Säkerhetspolisens behandling av personuppgifter

Betänkande av Utredningen om Säkerhetspolisens informationshantering

Stockholm 2025

STATENS OFFENTLIGA UTREDNINGAR

SOU 2025:49

SOU och Ds finns på regeringen.se under Rättsliga dokument.

Svara på remiss – hur och varför
Statsrådsberedningen, SB PM 2021:1.
Information för dem som ska svara på remiss finns tillgänglig på regeringen.se/remisser.

Layout: Kommittéservice, Regeringskansliet
Omslag: Elanders Sverige AB
Tryck och remisshantering: Elanders Sverige AB, Stockholm 2025

ISBN 978-91-525-1235-7 (tryck)
ISBN 978-91-525-1236-4 (pdf)
ISSN 0375-250X

Till statsrådet och chefen för Justitiedepartementet

Regeringen beslutade den 11 maj 2023 att tillkalla en särskild utredare med uppdrag att göra en översyn av de bestämmelser som reglerar Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet (dir. 2023:64). Till särskild utredare utsågs lagmannen Mikael Forsgren. Genom tilläggsdirektiv som beslutades den 24 oktober 2024 förlängdes utredningstiden (dir. 2024:99).

Som experter i utredningen förordnades den 29 maj 2023 seniora verksjuristen Charlotte Persson (Säkerhetspolisen), avdelningschefen Daniel Karlsson (Säkerhetspolisen) och enhetschefen Gunilla Berglund (Säkerhets- och integritetsskyddsnämnden). Som sakkunnig förordnades samtidigt kanslirådet Jonatan Lundqvist. Den 30 november 2023 förordnades före detta ordföranden i Försvarsunderrättelsedomstolen Lars Lundgren som expert i utredningen. Gunilla Berglund entledigades genom beslut den 11 december 2023. Den 4 april 2024 förordnades i hennes ställe enhetschefen Ia Hamlin (Säkerhets- och integritetsskyddsnämnden). Samma datum utsågs även juristen Lisa Zettervall (Integritetskyddsmyndigheten) till expert i utredningen. Daniel Karlsson entledigades den 2 september 2024 och i stället förordnades kommissarien Rami Hamdeh (Säkerhetspolisen) som expert i utredningen.

Som sekreterare anställdes den 15 maj 2023 hovrättsassessorn, numera utnämnda rådmannen, Jon Karlsson.

Utredningen har antagit namnet Utredningen om Säkerhetspolisens informationshantering.

Utredningen överlämnar nu betänkandet *Säkerhetspolisens behandling av personuppgifter* (SOU 2025:49). Experterna och den sakkunnige ställer sig i allt väsentligt bakom de bedömningar och förslag som redovisas i betänkandet, även om olika uppfattningar kan

ha funnits i enskilda delar. Betänkandet är därför formulerat i vi-form.

Umeå i mars 2025

Mikael Forsgren

Jon Karlsson

Innehåll

Sammanfattning

Uppdraget

Utredningens uppdrag har varit att genomföra en översyn av bestämmelserna om Säkerhetspolisens personuppgiftsbehandling inom området nationell säkerhet. Sådana regler finns i den så kallade säpodatalagen. Målet har varit att utforma ett modernare och mer ändamålsenligt regelverk anpassat till dagens förhållanden. I uppdraget har ingått att:

- Kartlägga Säkerhetspolisens rättsliga möjligheter att behandla personuppgifter.
- Identifiera hur nuvarande regelverk försvårar effektiv informationshantering.
- Utarbeta förslag för effektivare informationshantering med bibehållet skydd för personlig integritet.
- Säkerställa en effektiv tillsyn.

En central målsättning för utredningen har varit att finna en lämplig balans mellan Säkerhetspolisens behov och skyddet för grundläggande fri- och rättigheter enligt regeringsformen och Europakonventionen. Enligt direktiven ska förslagen även vara anpassade till Europarådets moderniserade dataskyddskonvention från år 2018 (dataskyddskonventionen 108+).

Reformbehovet

Säkerhetspolisens uppdrag är främst att förebygga, förhindra och upptäcka brott mot nationell säkerhet

Säkerhetspolisens uppdrag som nationell säkerhetstjänst är att skydda Sveriges grundläggande demokratiska funktioner och den nationella säkerheten. Dess kärnverksamhet syftar till att förebygga, förhindra och upptäcka brottslig verksamhet som innefattar brott mot rikets säkerhet eller terroristbrott. I myndighetens uppdrag ingår även att utreda och lagföra sådan brottslighet. Denna brottslighet utmärks av att den kan få mycket stora konsekvenser för samhället och för enskilda individer. Målet för verksamheten är därför att förhindra att brott överhuvudtaget begås genom att exempelvis avslöja en spion eller en terrorist innan några brottsliga gärningar ens har begåtts.

Såväl spionerи som terrorism bedrivs med nödvändighet i det fördolda och i former som till sin natur är slutna. Det innebär att det sällan finns några anmälningar eller uppslag från allmänheten att utgå ifrån. Säkerhetspolisen måste därför bedriva ett aktivt underrättelsearbete inriktat på att kartlägga personer och miljöer i syfte att förebygga, förhindra och upptäcka brottslig och säkerhetshotande verksamhet.

En förändrad hotbild

Sverige står inför en bredare och alltmer komplex hotbild. Auktoritära stater som Ryssland, Kina och Iran bedriver omfattande säkerhetshotande verksamhet mot Sverige genom underrättelseinhämtning, påverkansoperationer, cyberangrepp samt olovlig teknik- och kunskapsanskaffning. Samtidigt har hotet från våldsbejakande extremism förändrats. Extremistiska budskap får större spridning via digitala plattformar och gränserna mellan våldsbejakande extremism och annan extremism har blivit mer otydliga.

Den nuvarande lagstiftningen är inte anpassad till Säkerhetspolisens verksamhet eller dagens informationsmängder

Säkerhetspolisen har ett särpräglat uppdrag i förhållande till de andra brottsbekämpande myndigheterna. Kärnan i Säkerhetspolisens verksamhet är att som säkerhetstjänst skydda Sveriges säkerhet och det svenska statsskicket mot säkerhetshotande verksamhet. Brottsutredande verksamhet, bestående i att utreda brott och bedriva förundersökning, utgör endast en liten del av detta uppdrag. Säkerhetspolisen intar därför en särställning inom brottsbekämpningen med ett uppdrag som nationell säkerhetstjänst. Trots de stora skillnaderna i myndigheternas uppdrag, mål och metoder har Säkerhetspolisen i stora delar identisk lagstiftning vad gäller behandling av personuppgifter som övriga brottsbekämpande myndigheter.

Säkerhetspolisens uppdrag förutsätter att myndigheten på ett effektivt sätt kan bearbeta och analysera stora mängder information, för att på ett tidigt stadium kunna förebygga, förhindra och upptäcka säkerhetshotande verksamhet. Säpodatalagen reglerar stora delar av denna verksamhet och är därmed påtagligt styrande för myndighetens underrättelseverksamhet och -förmåga.

Informationsmängderna i samhället ökar exponentiellt. Det har förändrat förutsättningarna för Säkerhetspolisens verksamhet. Stora delar av den nuvarande säpodatalagen har överförts från tidigare lagstiftningar och har sitt ursprung i en tid då tekniken och informationsmängderna såg väsentligt annorlunda ut. År 1992 skickades världens första sms. I dag skickas det cirka 500 miljarder textmeddelanden, över olika plattformar, varje dag. Ett it-beslag av en telefon eller dator kan innebära att hundratusentals meddelanden, bilder och dokument behöver bearbetas. Det finns även hot mot Sveriges säkerhet som uppstår och utvecklas i mer öppna former på internet och i olika sociala medier. Både terroristrekrytering, destabiliserande påverkanskampanjer och försök av främmande makt att olovligt anskaffa information sker i dag över internet. För att upptäcka och motverka sådana säkerhetshot krävs att stora informationsmängder behandlas.

Dagens regelverk är emellertid snarare anpassat till 1990-talets informationsmängder än 2020-talets och har svårt att hantera de miljöer där säkerhetshot i dag uppstår och utvecklas. Den nuvarande lagstiftningen tvingar ofta Säkerhetspolisen att radera betydande

mängder inhämtad information som kan vara av stor betydelse för myndighetens möjlighet att lösa sitt uppdrag. Den nuvarande säpodatalagen medför nämligen att varje enskild personuppgift ska granskas och bedömas för sig för att få behandlas. Det innebär att myndigheten avstår från att hämta in uppgifter som i och för sig behövs för verksamheten.

Som tydliga begränsningar i nuvarande regelverk kan nämnas:

- Krav på konkret behov och ändamål för varje enskild personuppgift utan beaktande av sammanhang.
- Krav på att alla känsliga personuppgifter ska identifieras och prövas för sig. Sådana uppgifter får behandlas endast om uppgiften är absolut nödvändig.
- För kort längsta tid för behandling med hänsyn till Säkerhetspolisens uppdrag, vilket innebär att viktig information riskerar att gå förlorad.
- Begränsad möjlighet att behandla referensdatabaser eller utveckla moderna tekniska verktyg (som AI).

Reformens inriktning

Avvägning mot grundläggande fri- och rättigheter

Säkerhetspolisens behov av att behandla personuppgifter måste noggrant balanseras mot skyddet för grundläggande fri- och rättigheter. Det svenska statsskickets grunder slås fast i regeringsformen. Där framgår bland annat att den svenska folkstyrelsen bygger på fri åsiktsbildning, att den offentliga makten ska utövas med respekt för alla människors lika värde och för den enskilda människans frihet och värdighet. Vidare anges att det allmänna ska värna den enskildes privatliv och familjeliv.

Utökade möjligheter för Säkerhetspolisen att, genom att bevara information, kartlägga enskildas aktiviteter kan medföra risker för den personliga integriteten. Dessa risker påverkar inte enbart rätten till privatliv utan indirekt även yttrandefriheten och andra opinionsfriheter. Om medborgare uppfattar att olika former av åsiktsyttringar registreras och bevaras av säkerhetstjänsten, kan det få en

avhållande inverkan på viljan att använda sina demokratiska rättigheter.

En lagstiftning som syftar till att skydda de demokratiska kärnvärdena får inte samtidigt riskera att undergräva dem. Enligt regeringsformen får begränsningar av grundläggande fri- och rättigheter endast göras genom lag och endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Begränsningarna får inte gå utöver vad som är nödvändigt med hänsyn till ändamålet och inte heller sträcka sig så långt att de utgör ett hot mot den fria åsiktsbildningen. Utredningen har lagt stor vikt vid att analysera det förslag som lämnas mot detta krav.

Principerna för en ny lagstiftning

Utredningen föreslår en genomgripande reform av regleringen för Säkerhetspolisens personuppgiftsbehandling. Det centrala elementet är en helt ny säpodatalag som utgår från dataskyddskonventionen 108+ och Europakonventionen i stället för EU-rätten. Detta bygger på ställningstagandet att skyddet av nationell säkerhet är en nationell angelägenhet, där unionen saknar lagstiftningskompetens. Det är därför möjligt att föreslå en lagstiftning som bättre balanserar säkerhetsbehov med integritets- och rättighetsskydd.

Den nya lagstiftningen bygger på följande centrala principer:

- **Proportionalitetsprincipen** införs som grundläggande krav, där varje behandlingsåtgärd måste vara proportionerlig i förhållande till ändamålet och intrånget i den enskildes fri- och rättigheter.
- **Situationsanpassade krav:** Mer flexibla regler för ändamål, behov och behandlingstider som bättre motsvarar hur en underrättelse- och säkerhetstjänst faktiskt fungerar. Detta innebär att även till synes perifer information kan sparas över tid när den förekommer i relevanta sammanhang, eftersom sådan information senare kan visa sig avgörande för att upptäcka säkerhetshot.
- **Teknikneutral utformning** som möjliggör användning av moderna tekniker samtidigt som riskerna med dessa begränsas genom robusta skyddsmekanismer.

- **Systemorienterad tillsyn** snarare än tillsyn av behandlingen av enskilda personuppgifter, vilket ger en mer effektiv och realistisk tillsyn av stora informationsmängder.

Som ett komplement till säpodatalagen föreslår utredningen en särskild lag, anpassad för behandling av stora informationsmängder. Denna lag innebär ett proportionerligt undantag från vissa dataskyddsprinciper, vilket utredningen bedömt nödvändigt för att skydda nationell säkerhet. Säkerhetspolisen ges därigenom ökade möjligheter att behandla stora mängder information och även uppgifter som inte direkt behövs för uppdraget men som förekommer i sammanhang som är befogade att behandla.

För att motverka riskerna med denna utökade förmåga föreslås förstärkta mekanismer för tillsyn och kontroll med omfattande krav på förhandsprövning av domstol. Tillsynsmyndigheterna ges utökade befogenheter och resurser. De nya lagarna ställer nya krav på hur tillsynen utövas, med större fokus på hur personuppgifter behandlas och behandlingens potentiella effekter än på att granska formalia.

Förslagen skapar ett sammanhängande regelverk som ger Säkerhetspolisen moderna verktyg för att möta en komplex hotbild samtidigt som det upprätthåller rättssäkerhet och värnar grundläggande fri- och rättigheter i ett demokratiskt samhälle.

Huvudsakliga förslag

Ny lag om Säkerhetspolisens behandling av personuppgifter

Utredningen föreslår en ny säpodatalag som helt ersätter den nuvarande lagen från år 2019. De centrala förslagen innebär:

- **En proportionalitetsprincip:** Införs som ett grundläggande krav för all behandling. Skälet för behandlingen ska väga tyngre än intrånget i enskilda och allmänna intressen.
- **Inledande behandling och granskning:** Begreppet *inledande behandling* (insamling, inhämtning etc.) införs. Det ställs lägre krav för inledande behandling än annan behandling. Det får ske om det är befogat för ett ändamål. Efter den inledande behandlingen regleras hur uppgifterna ska *granskas* (under max sex

månader) för att säkerställa att de får fortsätta att behandlas enligt högre krav. Fortsatt behandling får ske om det behövs för ett särskilt, uttryckligt angivet och berättigat ändamål.

- **Ändamål för underrättelseverksamhet:** Nuvarande uppräkning av rättslig grund ersätts med verksamheter för personuppgiftsbehandling. Ändamål för behandling ska bestämmas inom någon av dessa verksamheter. Underrättelseverksamheten förtydligas genom att det framgår att personuppgifter får behandlas för att bland annat kartlägga och klarlägga brottslig verksamhet. Det medger behandling av uppgifter som är relevanta på grund av sammanhang och kontext.
- **Längre och mer flexibla behandlingstider:** Behandlingstid för personuppgifter bestäms vid registrering utifrån behov och proportionalitet. Den längsta behandlingstiden som får bestämmas är 25 år, med undantag för kontraspionage (60 år) och teknisk utveckling (5 år). Förlängning utöver dessa tider kräver ett särskilt beslut och en underrättelse till Säkerhets- och integritetsskyddsnämnden. Det införs en särskild regel om att barns uppgifter ska ges ett särskilt starkt skydd vid bestämmande av behandlingstid.
- **Kvalitetskrav:** Kraven på adekvans, relevans och uppgiftsminimering bibehålls men tillämpas inte före det att uppgifterna kunnat granskas.
- **Känsliga personuppgifter:** Ett förbud mot behandling som enbart grundar sig på känsliga personuppgifter. Dagens krav på *absolut nödvändighet* tas bort, men förekomst av känsliga uppgifter ska påverka proportionalitetsprövningen. Ett högre krav ställs för sökningar och sammanställningar grundade på känsliga uppgifter. Sådant urval får endast ske om skälen *uppenbart* överväger intrånget.
- **Privilegierade uppgifter:** Ett absolut förbud införs mot att behandla uppgifter som omfattas av meddelarskydd enligt tryckfrihetsförordningen och yttrandefrihetsgrundlagen. Detsamma gäller förtrolig kommunikation mellan en misstänkt och dennes försvarare. Detta utgör en nyhet i den nya lagen som begränsar Säkerhetspolisens möjligheter att samla information som är särskilt känslig från ett rättighetsperspektiv.

- **Teknikutveckling:** Tillåts uttryckligen som ändamål för personuppgiftsbehandling, men uppgifter som samlats in enbart för detta ändamål får inte användas operativt.
- **Automatiserat beslutsfattande:** Förbjuds om det har betydande påverkan på den enskilde.

Förändringarna innebär att Säkerhetspolisen får en lag som är anpassad till myndighetens uppdrag. Utredningen har strävat efter en transparent lag som ska reglera den faktiska verksamheten och som inte innehåller bestämmelser som leder till omotiverade administrativa uppgifter. Förslaget frångår den nuvarande lagstiftningens koppling till EU-rättens förlagor och vad som gäller för övriga brottsbekämpande myndigheter. Lagförslaget innebär en avvägning på nationell nivå mellan behovet av skydd för nationell säkerhet och skydd för andra enskilda eller allmänna intressen. Utredningen bedömer att lagen är förenlig med dataskyddskonventionen 108+.

Ny lag om behandling av personuppgifter i särskilda uppgiftssamlingar

Utredningen föreslår även en helt ny lag med kompletterande bestämmelser om behandling av personuppgifter i särskilda uppgiftssamlingar:

- **Syfte:** Möjliggöra hantering av stora, inledningsvis ofta ostrukturerade, informationsmängder där granskning enligt säpodatalagen inte är möjlig. Lagen kompletterar och gör undantag från den nya säpodatalagen. Lagen innebär att Sverige utnyttjar möjligheten till undantag från vissa av dataskyddskonventionens bestämmelser. Sådana undantag är nödvändiga för att skydda nationell säkerhet.
- **Registrering:** Uppgifter får registreras i en *särskild uppgiftssamling* efter ett motiverat beslut. Samma krav ska gälla för registrering som för inledande behandling (befogat). Beslutet ska bland annat beskriva källan, ändamålet, och vilket intrång i enskilda och allmänna intressen som behandling av uppgifterna kan antas medföra. Behandlingstid bestäms vid registrering

(max 10 år, förlängning möjlig upp till 25 år, eller längre vid synnerliga skäl).

- **Framtagningsförbud:** Huvudregeln är att uppgifter i en särskild uppgiftssamling inte får tas fram (läsas, tillgängliggöras). Detta utgör den centrala skyddsmekanismen.
- **Tillstånd för framtagning:** Uppgifter får tas fram endast efter tillstånd från Försvarsunderrättelsedomstolen. Av ansökan ska bland annat framgå ändamål, behov samt vilka sökbegrepp och teknik för urval som ska användas. Domstolen gör en fullständig legalitets-, behovs- och proportionalitetsprövning. Alla tillstånd är tidsbegränsade.
- **Sekretess:** Absolut sekretess föreslås gälla för uppgifterna så länge de behandlas i en särskild uppgiftssamling, både till skydd för enskild och för verksamheten.
- **Användningsbegränsning:** Uppgifter som tagits fram från en särskild uppgiftssamling får inte användas för att utreda brott, exempelvis i en förundersökning.

De rättssäkerhetsmekanismer som införs är omfattande och minst lika starka som de som gäller för signalspaning (ett system som har prövats i Europadomstolen). Utredningen bedömer därför att förslaget är förenligt med Europakonventionen.

Förstärkt tillsyn

De utökade möjligheterna att behandla personuppgifter förutsätter en förstärkning av tillsynen. Utredningen föreslår att den nuvarande parallella tillsynen genom Integritetsskyddsmyndigheten och Säkerhets- och integritetsskyddsnämnden bibehålls, men med tydligare roller och förstärkta befogenheter:

- Säkerhets- och integritetsskyddsnämnden utpekas i lagen som särskild tillsynsmyndighet.
- Nämnden och Säkerhetspolisen får en skyldighet att löpande samverka i frågor som rör Säkerhetspolisens skyldigheter som personuppgiftsansvarig.

- För att möta utmaningarna med ökad teknisk komplexitet får Säkerhetspolisen en skyldighet att i skälig omfattning vidta nödvändiga tekniska åtgärder för att möjliggöra effektiv tillsyn.
- Nämnden och Försvarsunderrättelsedomstolen utgör delar av samma kontrollsystem. Nämnden ska yttra sig över Säkerhetspolisens ansökan om tillstånd till att ta fram uppgifter ur en särskild uppgiftssamling. En sekretessbrytande bestämmelse införs för att domstolen ska kunna ta del av all relevant utredning vid prövningen.
- Nämnden får en ny korrigerande befogenhet att besluta om omedelbar radering av uppgifter som tagits fram från en särskild uppgiftssamling utan tillstånd eller i strid med tillstånd.
- Beslut om förelägganden eller förbud från Integritetsskyddsmyndigheten ska överklagas till Försvarsunderrättelsedomstolen.
- Nämnden tillförs betydande ekonomiska resurser och ges möjlighet att förstärka sig med teknisk kompetens för att kunna utöva en effektiv tillsyn över bland annat nya behandlingsmetoder.

Förändringarna syftar till ett robust och oberoende tillsynssystem som säkerställer att personuppgiftsbehandlingen sker i enlighet med de nya lagkraven. En effektiv tillsyn bidrar därmed till att upprätthålla rättssäkerheten och det allmänna förtroendet för Säkerhetspolisens personuppgiftsbehandling.

Ikraftträdande och övergångsbestämmelser

Utredningen föreslår att de nya lagarna träder i kraft den 1 januari 2027. Detta ger Säkerhetspolisen och tillsynsmyndigheterna tillräcklig tid att genomföra nödvändiga anpassningar av tekniska system, rutiner och arbetssätt. Även Försvarsunderrättelsedomstolen får nya uppgifter med anledning av förslaget. Reformen innebär omfattande förändringar både organisatoriskt och tekniskt, vilket kräver grundlig förberedelse.

För att säkerställa en smidig övergång föreslås att personuppgifter som redan behandlas vid ikraftträdandet får fortsätta att behandlas enligt den äldre lagen fram till och med den 31 december 2029. Under denna treåriga övergångsperiod ska Säkerhetspolisen

successivt anpassa sin befintliga personuppgiftsbehandling till de nya regelverken. För nya personuppgifter som behandlas efter ikraftträdandet ska dock de nya lagarna tillämpas omedelbart.

Detta stegvisa införande balanserar behovet av att snabbt införa ett modernare regelverk mot Säkerhetspolisens förmåga att upprätthålla sin verksamhet under övergångsperioden.

Summary[1]

The Assignment

The purpose of this investigation has been to conduct a review of the provisions regarding the Security Police's processing of personal data in the field of national security. Such rules are found in the Security Police Data Act. The goal has been to develop a more modern and appropriate regulatory framework adapted to current conditions. The assignment has included:

- Mapping the Security Police's legal authority to process personal data.
- Identifying how the current regulatory framework hinders efficient information management.
- Developing proposals for more efficient information management while maintaining protection of personal privacy.
- Ensuring effective supervision.

A central objective of the investigation has been to find an appropriate balance between the Security Police's needs and the protection of fundamental rights and freedoms under the Instrument of Government and the European Convention on Human Rights. According to the directives, the proposals should also be adapted to the Council of Europe's Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, from 2018 (Data Protection Convention 108+).

[1] The translation was initially drafted with AI assistance but subsequently reviewed, edited and approved by humans.

The Need for Reform

The Security Police's mission is primarily to prevent, pre-empt and detect crimes against national security

The Security Police's mission as a national security service is to protect Sweden's fundamental democratic functions and national security. Its core activities aim to prevent, pre-empt and detect criminal activities that include crimes against national security or terrorist offenses. The authority's duties also include investigating and prosecuting such crimes. These crimes are characterized by their potential to have very severe consequences for society and individuals. Therefore, the goal of the operations is to prevent crimes from being committed at all, for example by exposing a spy or a terrorist before any crime has even been committed.

Both espionage and terrorism are necessarily using methods that are inherently covert. This means that there are rarely any reports or leads from the public. The Security Police must therefore conduct active intelligence work focused on mapping individuals and environments with the aim of preventing, pre-empting and detecting criminal and security -threatening activities.

A changed threat landscape

Sweden faces a broader and increasingly complex threat landscape. Authoritarian states such as Russia, China, and Iran conduct extensive security-threatening activities against Sweden through intelligence gathering, influence operations, cyberattacks, and illegal acquisition of technology and knowledge. At the same time, the threat from violent extremism has evolved. Extremist messages spread more widely via digital platforms, and the boundaries between violent extremism and other forms of extremism have become increasingly blurred.

The current legislation is not adapted to the Security Police's operations or today's information volumes

The Security Police has a distinctive mission compared to other law enforcement agencies. The core of the Security Police's operations is to protect Sweden's security and constitutional order against security-threatening activities, acting in its capacity as a security service. Criminal investigative activities, consisting of investigating crimes and conducting preliminary investigations, constitute only a small part of this mission. The Security Police therefore holds a special position within law enforcement, with a mission as a national security service. Despite the major differences in the authorities' missions, goals, and methods, the Security Police is largely subject to the same legislation regarding the processing of personal data as other law enforcement authorities.

The Security Police's mission requires that the authority be able to efficiently process and analyze large volumes of information in order to prevent, pre-empt and detect security-threatening activities at an early stage. The Security Police Data Act regulates large parts of this activity and is therefore significant in shaping the authority's intelligence operations and capabilities.

The volume of information in society is increasing exponentially. This has changed the conditions for the Security Police's operations. Large parts of the current Security Police Data Act have been carried over from previous legislation and originate from a time when technology and information volumes were substantially different. In 1992, the world's first SMS was sent. Today, approximately 500 billion text messages are sent across different platforms every day. An IT seizure of a phone or computer can result in hundreds of thousands of messages, images, and documents that must be processed. There are also threats to Sweden's security that arise and develop in more open environments on the internet and across various social media platforms. Today, terrorist recruitment, destabilising influence campaigns, and attempts by foreign powers to unlawfully acquire information occur online. To detect and counter such security threats, large volumes of information must be processed.

However, the current regulatory framework is designed for the information volumes of the 1990s rather than those of the 2020s and struggles to cope with the environments where security threats

now emerge and develop. The current legislation often forces the Security Police to delete significant amounts of collected information that could be of great importance for the authority's ability to fulfil its mission. The current Security Police Data Act requires that each personal data item be reviewed and assessed individually in order to be processed. This means that the authority refrains from collecting data that is, in fact, necessary for its operations.

Clear limitations in the current regulatory framework include the following:

- Requirements for a specific need and purpose for each personal data item, without consideration of context.
- Requirements that all sensitive personal data shall be identified and assessed individually. Such data may only be processed if the specific data item is strictly necessary.
- A maximum processing time that is too short given the Security Police's mission, which means that important information risks being lost.
- Limited ability to process reference databases or to develop modern technical tools (including AI).

The Direction of Reform

Balance against fundamental rights and freedoms

The Security Police's need to process personal data must be carefully balanced against the protection of fundamental rights and freedoms. The foundations of Sweden's constitutional order are established in the Instrument of Government. It states, among other things, that Swedish democracy is founded on the free formation of opinion, that public power shall be exercised with respect for the equal worth of all people and for the freedom and dignity of the individual. Furthermore, it states that the public sector shall protect the privacy and family life of individuals.

Enhanced capabilities for the Security Police to map individuals' activities by retaining information can pose risks to personal privacy. These risks affect not only the right to privacy but indirectly also freedom of expression and other freedoms of opinion. If citizens

perceive that different forms of expression of opinion are registered and preserved by the security service, it can discourage citizens from exercising their democratic rights. Legislation aimed at protecting democratic core values must not simultaneously risk undermining them. According to the Instrument of Government, restrictions on fundamental rights and freedoms may only be made by law and only to satisfy purposes that are acceptable in a democratic society. The restrictions must not go beyond what is necessary with regard to the purpose, nor extend so far as to constitute a threat to the free formation of opinion. The investigation has placed great emphasis on analyzing the proposal against this requirement.

Principles for new legislation

The investigation proposes a comprehensive reform of the regulations for the Security Police's processing of personal data. The central element is an entirely new Security Police Data Act based on Data Protection Convention 108+ and the European Convention on Human Rights instead of EU law. This is based on the position that the protection of national security is a national matter, in which the union lacks legislative competence. It is therefore possible to propose legislation that better balances security needs with privacy and the protection of rights.

The new legislation is based on the following central principles:

- **The principle of proportionality** is introduced as a fundamental requirement, where each processing measure must be proportionate to the purpose and the intrusion into the individual's rights and freedoms.
- **Situation-specific requirements** providing more flexibility regarding purpose, need, and processing times that better reflect how an intelligence and security service functions. This means that even seemingly peripheral information can be retained over time when it appears in relevant contexts, because such information may later prove crucial for detecting security threats.

- **Technology-neutral design** that enables the use of modern technologies while limiting the risks through robust protective mechanisms.
- **System-oriented supervision** rather than supervision of individual personal data processing, which provides more effective and realistic oversight of large volumes of information.

As a complement to the Security Police Data Act, the investigation proposes a special law, adapted for processing large volumes of information. This law represents a proportionate exception to certain data protection principles, which the investigation has deemed necessary to protect national security. The Security Police is therefore granted expanded possibilities to process large amounts of information, including data that is not directly needed for the mission but appears in contexts that are justified to process.

To counter the risks associated with this enhanced capability, strengthened mechanisms for supervision and control, with extensive requirements for preliminary judicial review, are proposed. The supervisory authorities are given expanded powers and resources. The new laws place new demands on how supervision is exercised, with greater focus on how personal data is processed and the potential effects of the processing, rather than on reviewing formalities.

The proposals create a coherent regulatory framework that gives the Security Police modern tools to meet a complex threat landscape while maintaining the rule of law and safeguarding fundamental rights and freedoms in a democratic society.

Main Proposals

New law on the Security Police's processing of personal data

The investigation proposes a new Security Police Data Act that completely replaces the current law from 2019. The central provisions include:

- **A principle of proportionality:** Introduced as a fundamental requirement for all processing. The reason for processing must outweigh the intrusion into individual and public interests.

- **Initial processing and review:** The concept of initial processing (collection, acquisition, etc.) is introduced. Lower requirements are set for initial processing than for subsequent processing. It may occur if it is justified for a purpose. After the initial processing, regulations specify how the data should be reviewed (for a maximum of six months) to ensure that it may continue to be processed, according to stricter requirements. Continued processing may occur if it is needed for a specific, explicitly stated, and legitimate purpose.
- **Purposes for intelligence activities:** The current enumeration of legal grounds is replaced with defined categories of activities for personal data processing. Purposes for processing must be linked to one of these activities. Intelligence activities are clarified by stating that personal data may be processed to, among other things, map and clarify criminal activities. This allows for the processing of data that is relevant due to context and connections.
- **Longer and more flexible processing times:** Processing time for personal data is determined at registration based on need and proportionality. The maximum processing time that may be determined is 25 years, with exceptions for counterespionage (60 years) and technical development (5 years). Extensions beyond these times require a special decision and notification to the Swedish Commission on Security and Integrity Protection. A special rule is introduced that children's data shall be given particularly strong protection when determining the processing period.
- **Quality requirements:** The requirements for adequacy, relevance, and data minimization are maintained but not applied before the data has been reviewed.
- **Sensitive personal data:** A prohibition is introduced against processing solely based on sensitive data. Today's requirement for absolute necessity is removed, but the presence of sensitive data shall affect the proportionality assessment. A stricter requirement is placed on searches and compilations based on sensitive data. Such processing may only occur if the reasons clearly outweigh the intrusion.

- **Privileged personal data:** An absolute prohibition is introduced against processing data covered by source protection under the Freedom of the Press Act and the Fundamental Law on Freedom of Expression. The same applies to confidential communication between a suspect and their defence counsel. This constitutes a new feature in the new law that limits the Security Police's ability to collect information that is particularly sensitive from a rights perspective.
- **Technology development:** Explicitly allowed as a purpose for personal data processing, but data collected solely for this purpose may not be used operationally.
- **Automated decision-making:** Prohibited if it has a significant impact on the individual.

The changes mean that the Security Police will have a law adapted to the authority's mission. The investigation has aimed to create a transparent law that regulates the actual operations and does not contain provisions that lead to unjustified administrative tasks. The proposal deviates from the current legislation's connection to EU law frameworks and from what applies to other law enforcement authorities. The legislative proposal represents a balance at the national level between the need for protection of national security and the protection of other individual or public interests. The investigation concludes that the law is compatible with Data Protection Convention 108+.

New law on processing of personal data in special data collections

The investigation also proposes an entirely new law with supplementary provisions on the processing of personal data in special data collections:

- **Purpose**: To enable the handling of large, initially often unstructured, volumes of information where review in accordance with the Security Police Data Act is not possible. The law complements and provides exceptions to the new Security Police Data Act. It allows Sweden to make use of the possibility of exemptions from

certain provisions of the Data Protection Convention. Such exceptions are necessary to protect national security.

- **Registration:** Data may be registered in a special data collection based on a justified decision. The same requirements shall apply to registration as to initial processing (justified). The decision shall, among other things, describe the source, purpose, and the expected impact on individual and public interests resulting from the processing of the data. The Processing time is set at registration (maximum 10 years, extendable up to 25 years, or longer in extraordinary circumstances).
- **Retrieval prohibition:** The main rule is that data in a special data collection may not be retrieved (read, made available). This constitutes the central protective mechanism.
- **Permission for retrieval:** Data may only be retrieved with permission from the Swedish Foreign Intelligence Court (Försvarsunderrättelsedomstolen). The application shall, among other things, state the purpose, need, and what search terms and selection technology will be used. The court conducts a comprehensive assessment of legality, necessity, and proportionality. All permissions are time-limited.
- **Secrecy:** Absolute secrecy is proposed to apply to the data as long as it is processed in a special data collection, to protect both individuals and operations.
- **Usage limitation:** Data retrieved from a special data collection may not be used to investigate crimes, for example in a preliminary investigation.

The rule-of-law safeguards that are introduced are extensive and at least as strong as those that apply to signals intelligence (a system that has been tested before the European Court of Human Rights). The investigation therefore concludes that the proposal is compatible with the European Convention on Human Rights.

Strengthened supervision and court control

The enhanced possibilities to process personal data require a strengthening of supervision. The investigation proposes that the current parallel supervision through the Swedish Authority for Privacy Protection and the Swedish Commission on Security and Integrity Protection be maintained, but with clearer roles and strengthened powers:

- The Commission on Security and Integrity Protection is designated by law as a special supervisory authority.
- The Commission and the Security Police have a duty to collaborate continuously on issues concerning the Security Police's obligations as a data controller.
- To meet the challenges of increased technical complexity, the Security Police is required to take necessary technical measures to a reasonable extent to enable effective supervision.
- The Commission and the Foreign Intelligence Court are parts of the same oversight system. The Commission shall issue an opinion on the Security Police's application for permission to retrieve data from a special data collection. A statutory exemption from confidentiality is introduced so that the court can access all relevant material during the review.
- The Commission is given a new corrective power to decide on immediate deletion of data that has been retrieved from a special data collection without permission or in violation of permission.
- Decisions on injunctions or prohibitions issued by the Swedish Authority for Privacy Protection shall be appealed to the Foreign Intelligence Court.
- The Commission is provided with significant financial resources and given the possibility to strengthen its capacity with technical expertise, in order to exercise effective supervision of, among other things, new methods of processing.

The changes aim at a robust and independent supervisory system that ensures that personal data processing is carried out in accordance with the new legal requirements. Effective supervision thus

contributes to maintaining the rule of law and public confidence in the Security Police's processing of personal data.

Entry into force and transitional provisions

The investigation proposes that the new laws enter into force on 1 January 2027. This gives the Security Police and supervisory authorities sufficient time to implement necessary adaptations to technical systems, routines, and working methods. The Foreign Intelligence Court also receives new tasks as a result of the proposal. The reform involves extensive changes both organizationally and technically, which requires thorough preparation.

To ensure a smooth transition, it is proposed that personal data already being processed at the time the new laws take effect may continue to be processed under the older law until 31 December 2029. During this three-year transitional period, the Security Police shall gradually adapt its existing personal data processing to the new regulatory frameworks. For new personal data processed after the entry into force, however, the new laws shall apply immediately.

This gradual introduction strikes a balance between the need to swiftly establish a more modern regulatory framework and the Security Police's ability to maintain operational continuity during the transitional period.

1 Författningsförslag

1.1 Förslag till lag om Säkerhetspolisens behandling av personuppgifter

Härigenom föreskrivs följande.

1 kap. Allmänna bestämmelser

Lagens syfte

1 § Syftet med lagen är att skydda fysiska personers grundläggande rättigheter och friheter i samband med behandling av personuppgifter och att säkerställa att Säkerhetspolisen kan behandla personuppgifter på ett ändamålsenligt sätt.

Lagens tillämpningsområde

2 § Denna lag gäller vid behandling av personuppgifter som rör nationell säkerhet i Säkerhetspolisens brottsbekämpande verksamhet.

Lagen gäller även vid Polismyndighetens behandling av personuppgifter, när myndigheten har övertagit en uppgift från Säkerhetspolisen inom denna lags tillämpningsområde.

När Polismyndigheten har övertagit en uppgift enligt andra stycket, ska vad som i denna lag sägs om Säkerhetspolisen i stället gälla Polismyndigheten.

3 § Lagen gäller vid sådan behandling av personuppgifter som är helt eller delvis automatiserad och för annan behandling av personuppgifter som ingår i eller är avsedda att ingå i en strukturerad samling

av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

4 § Om en annan lag innehåller någon bestämmelse som avviker från denna lag, tillämpas den bestämmelsen.

I lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar finns bestämmelser om Säkerhetspolisens behandling av personuppgifter i vissa fall.

Definitioner

5 § I denna lag används följande uttryck med nedan angiven betydelse.

Uttryck	Betydelse
Behandling av personuppgifter	En åtgärd eller kombination av åtgärder som vidtas i fråga om personuppgifter eller uppsättningar av personuppgifter, oavsett om det görs automatiserat eller inte, t.ex. insamling, granskning, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämnande, spridning eller tillhandahållande på annat sätt, justering, sammanföring, begränsning, radering eller förstöring.
Biometriska uppgifter	Personuppgifter som rör en persons fysiska, fysiologiska eller beteendemässiga kännetecken, som tagits fram genom särskild teknisk behandling och som möjliggör eller bekräftar unik identifiering av personen.
Genetiska uppgifter	Personuppgifter som rör en persons nedärvda eller förvärvade genetiska kännetecken och

	som härrör från analys av ett spår av eller ett prov från personen.
Inledande behandling	Behandling av personuppgifter som innebär att personuppgifter samlas in, hämtas in, tas emot eller på något annat sätt kommer Säkerhetspolisen till handa eller att personuppgifter nedtecknas, upprättas eller på något annat sätt skapas inom myndigheten, eller att personuppgifter tas fram från en särskild uppgiftssamling enligt lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftsinsamlingar.
Känsliga personuppgifter	Biometriska uppgifter, genetiska uppgifter och uppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning.
Personuppgift	Varje upplysning om en identifierad eller identifierbar fysisk person som är i livet.
Personuppgiftsansvarig	Den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter.
Personuppgiftsbiträde	Den som behandlar personuppgifter för den personuppgiftsansvariges räkning.
Registrerad	Den fysiska person som personuppgiften gäller.

Personuppgiftsansvar

6 § Säkerhetspolisen är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.

Den personuppgiftsansvarige är ansvarig för all behandling av personuppgifter som utförs under dennes ledning eller på dennes vägnar.

2 kap. Behandling av personuppgifter

Grundläggande krav på behandling

Proportionalitet

1 § All behandling av personuppgifter ska vara proportionerlig. En behandling är proportionerlig, om skälet för att utföra den överväger intrånget i de enskilda eller allmänna intressen som kan påverkas.

Rättslig grund

2 § Personuppgifter får endast behandlas för att bedriva verksamhet som följer av lag, förordning, internationella åtaganden eller särskilt beslut av regeringen.

Författningsenlig och korrekt behandling

3 § Personuppgifter ska behandlas författningsenligt och på ett korrekt sätt.

Verksamheter för behandling av personuppgifter

Underrättelse- och säkerhetstjänst

4 § I sin uppgift att förebygga, förhindra och upptäcka brottslig verksamhet får Säkerhetspolisen behandla personuppgifter för att

1. kartlägga och klarlägga brottslig verksamhet, eller
2. vidta åtgärder som hindrar eller försvårar brottslig verksamhet.

Brottsutredning och lagföring

5 § Personuppgifter får behandlas för att utreda och lagföra brott.

Övrig verksamhet

6 § Personuppgifter får behandlas för annan verksamhet som bedrivs enligt 2 §.

7 § Säkerhetspolisen får behandla personuppgifter för att fortlöpande utveckla den teknik och metodik som behövs inom denna lags tillämpningsområde (utvecklingsändamål).

Personuppgifter som behandlas endast för utvecklingsändamål får inte behandlas för något annat ändamål.

Inledande behandling

8 § Inledande behandling av personuppgifter får ske, om det är befogat för ett ändamål inom någon av de verksamheter som anges i 4–7 §§.

Vid inledande behandling tillämpas inte 13–16 §§.

Inledande granskning

9 § Efter inledande behandling ska personuppgifter granskas, om det behövs för att säkerställa författningsenlig behandling. Innan granskningen har genomförts får personuppgifterna behandlas endast för granskningsändamål.

Granskningen enligt första stycket ska ske så snart det är möjligt och får inte pågå längre än nödvändigt. Sådan behandling får pågå i högst sex månader.

Granskningen ska utföras av särskilt angivna tjänstemän som har tillräckliga kunskaper för uppgiften. Under granskningen ska tillgången till uppgifterna vara begränsad till vad var och en behöver för att fullgöra uppgiften.

10 § De befattningshavare vid Säkerhetspolisen som regeringen föreskriver får besluta att personuppgifter som behandlas med stöd av 9 § även får behandlas av andra tjänstemän och för andra ändamål än granskning, om det är absolut nödvändigt för att fullgöra en uppgift av synnerlig vikt.

Behandling enligt första stycket får pågå i högst trettio dagar och tillgången till sådana personuppgifter ska vara strikt begränsad till vad var och en behöver för att fullgöra uppgiften.

Beslut enligt första stycket ska dokumenteras och omedelbart anmälas till den särskilda tillsynsmyndigheten.

Fortsatt behandling

11 § Efter inledande granskning får personuppgifter behandlas endast om det behövs för ett särskilt, uttryckligt angivet och berättigat ändamål.

Finalitetsprincipen

12 § Personuppgifter får inte behandlas för ett ändamål som är oförenligt med ändamålet för den inledande behandlingen.

Första stycket hindrar dock inte att personuppgifter som behandlas enligt 4–6 §§ behandlas för

1. utvecklingsändamål enligt 7 §,
2. vetenskapliga, statistiska eller historiska ändamål inom denna lags tillämpningsområde, eller
3. diarieföring, handläggning och liknande verksamhet inom denna lags tillämpningsområde.

Personuppgifters kvalitet

Korrekta uppgifter

13 § Personuppgifter som behandlas ska vara korrekta och, om det är nödvändigt, uppdaterade.

Uppgiftsminimering

14 § Personuppgifter som behandlas ska vara adekvata, relevanta och inte för omfattande i förhållande till ändamålet med behandlingen.

Särskilda upplysningar

15 § Om det ändamål som personuppgifter behandlas för inte framgår av sammanhanget eller på något annat sätt, ska det tydliggöras genom en särskild upplysning.

16 § När personuppgifter behandlas för att utreda och lagföra brott som Säkerhetspolisen ansvarar för, ska personuppgifter som rör olika kategorier av registrerade så långt det är möjligt särskiljas. Genom särskiljningen ska det framgå om personen är misstänkt, dömd för brott, brottsoffer eller någon annan som berörs av ett brott.

Om det inte framgår av sammanhanget eller på annat sätt till vilken kategori personen hör, ska det tydliggöras genom en särskild upplysning.

Särskilda kategorier av personuppgifter

Känsliga personuppgifter

17 § Uppgifter om en person får inte behandlas enbart utifrån sådant som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller uppgifter som rör hälsa, sexualliv eller sexuell läggning.

Första stycket hindrar inte behandling av personuppgifter som har lämnats till Säkerhetspolisen i en anmälan, ansökan eller liknande.

18 § Genetiska uppgifter får inte behandlas.

Privilegierade uppgifter

19 § Säkerhetspolisen får inte behandla personuppgifter

1. för vilka tystnadsplikt gäller enligt 3 kap. 3 § tryckfrihetsförordningen eller 2 kap. 3 § yttrandefrihetsgrundlagen, eller som omfattas av efterforskningsförbudet i 3 kap. 5 § tryckfrihetsförordningen eller 2 kap. 5 § yttrandefrihetsgrundlagen, eller

2. i sådana meddelanden mellan en person som är misstänkt för brott och hans eller hennes försvarare vilka skyddas enligt 27 kap. 22 § första stycket rättegångsbalken.

Sökbegränsningar

20 § Sökning i syfte att få fram ett urval av personer får grundas på känsliga personuppgifter endast om skälen för att utföra behandlingen uppenbart överväger intrånget i de enskilda eller allmänna intressen som kan påverkas av den.

21 § Om en förundersökning mot en person har lagts ner, om ett åtal har lagts ner eller om en frikännande dom har fått laga kraft, får personen inte längre vara sökbar som misstänkt avseende det brottet.

Automatiserat beslutsfattande

22 § En persons personuppgifter får inte användas för att fatta automatiserade beslut som har en betydande påverkan för honom eller henne.

3 kap. Informationsutbyte

Behandling för att tillhandahålla information

1 § Uppgifter som behandlas enligt 2 kap. 4–6 §§ får även behandlas för att tillhandahålla information

1. om uppgifterna behövs i

a) brottsbekämpande verksamhet hos en myndighet,

b) en myndighets verksamhet, om informationen tillhandahålls inom ramen för myndighetsöverskridande samverkan mot brott,

c) Försvarsmaktens militära säkerhetstjänst, eller

d) Försvarsmaktens eller Försvarets radioanstalts försvarsunderrättelseverksamhet, eller

2. om uppgifterna behövs i

a) brottsbekämpande verksamhet hos en utländsk myndighet,

b) brottsbekämpande verksamhet hos en mellanfolklig organisation,

c) verksamhet hos utländsk underrättelse- eller säkerhetstjänst, eller

d) ett säkerhets- eller underrättelseorgan i en mellanfolklig organisation som Sverige är medlem i, eller

3. till riksdagen eller regeringen, eller

4. om det sker i överensstämmelse med lag eller förordning.

2 § Personuppgifter som behövs för att framställa rättsstatistik ska lämnas till den myndighet som ansvarar för att framställa sådan statistik.

Utlämnande av personuppgifter till annat land

3 § Om det är förenligt med svenska intressen, får personuppgifter som behandlas med stöd av 2 kap. 4–6 §§ lämnas ut

1. enligt 1 § 2, eller

2. till en annan utländsk myndighet eller mellanfolklig organisation, om utlämnandet följer av en internationell överenskommelse som Sverige har tillträtt efter riksdagens godkännande.

Utlämnande av personuppgifter enligt första stycket får bara ske till mottagare som kan garantera ett tillräckligt skydd för personuppgifterna.

4 § Personuppgifter som behandlas med stöd av 2 kap. 4–6 §§ får i ett enskilt fall lämnas ut till annan utländsk mottagare än vad som anges i 3 § om

1. sekretess inte hindrar utlämnandet, och

2. skälen för att lämna ut uppgifterna uppenbart överväger intrånget i de enskilda eller allmänna intressen som kan påverkas av utlämnandet.

Elektroniskt utlämnande

5 § Personuppgifter får lämnas ut elektroniskt på annat sätt än genom direktåtkomst, om det inte är olämpligt.

6 § Direktåtkomst får medges för personuppgifter som behandlas enligt 2 kap. 4–6 §§ och som

1. Polismyndigheten behöver för att

a) förebygga, förhindra eller upptäcka brottslig verksamhet,

b) utreda eller lagföra brott, eller

c) fullgöra uppgifter enligt utlänningslagen (2005:716) eller lagen (2022:700) om särskild kontroll av vissa utlänningar,

2. Försvarsmakten behöver i sin försvarsunderrättelseverksamhet eller militära säkerhetstjänst, eller

3. Försvarets radioanstalt behöver i sin försvarsunderrättelseverksamhet.

7 § En underrättelse- eller säkerhetstjänst i en stat som omfattas av avtalet om Europeiska ekonomiska samarbetsområdet, i Förenade kungariket eller i Schweiz får medges direktåtkomst till personuppgifter

1. som behandlas för att förebygga, förhindra och upptäcka brottslig verksamhet som innefattar terrorbrott, och

2. om det behövs för samarbetet mot terrorism.

Innan direktåtkomst medges en utländsk underrättelse- eller säkerhetstjänst ska Säkerhetspolisen informera regeringen.

Sekretessbrytande bestämmelser

8 § Trots sekretess enligt 21 kap. 3 § första stycket, 35 kap. 1 § och 37 kap. 1 § offentlighets- och sekretesslagen (2009:400) har

1. Polismyndigheten rätt att ta del av personuppgifter som behandlas med stöd av 2 kap. 4–6 §§, om myndigheten behöver uppgifterna för att

a) förebygga, förhindra eller upptäcka brottslig verksamhet,

b) utreda eller lagföra brott, eller

c) fullgöra uppgifter enligt utlänningslagen (2005:716) eller lagen (2022:700) om särskild kontroll av vissa utlänningar,

2. Försvarsmakten rätt att ta del av personuppgifter som behandlas med stöd av 2 kap. 4 eller 5 §, om myndigheten behöver uppgifterna i sin försvarsunderrättelseverksamhet eller militära säkerhetstjänst, och

3. Försvarets radioanstalt rätt att ta del av personuppgifter som behandlas med stöd av 2 kap. 4 eller 5 §, om myndigheten behöver uppgifterna i sin försvarsunderrättelseverksamhet.

Rätt att meddela föreskrifter

9 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om omfattningen av direktåtkomst enligt 6 och 7 §§ och om behörighet och säkerhet vid sådan åtkomst.

Regeringen kan också meddela föreskrifter om begränsning av möjligheten att lämna ut personuppgifter elektroniskt enligt 5 §.

4 kap. Längsta tid som personuppgifter får behandlas

Bestämmande av behandlingstid

1 § När personuppgifter registreras för ett ändamål eller börjar behandlas för ett nytt ändamål ska Säkerhetspolisen bestämma hur lång tid uppgifterna får behandlas för det ändamålet.

Tiden enligt första stycket får inte vara längre än vad som behövs för ändamålet med behandlingen och inte vara längre än

1. sextio år, om ändamålet för behandlingen hänför sig till sådan säkerhetshotande verksamhet som avses i 18 och 19 kap. brottsbalken och som utövas av främmande makt,

2. fem år, om uppgifterna behandlas endast för utvecklingsändamål, och

3. tjugofem år, om uppgifterna behandlas för något annat ändamål enligt denna lag.

Behandlingstiden får bestämmas gemensamt för personuppgifter som är förenade av sammanhanget. Behandlingstiden ska avse antingen viss tid eller räknas från den senaste registreringen avseende personens anknytning till ändamålet för behandlingen.

Behandlingens upphörande

2 § Personuppgifter får inte behandlas för något ändamål inom denna lags tillämpningsområde efter utgången av det kalenderår då behandlingstiden enligt 1 § löper ut. Om behandlingstiden är kortare än ett år, får uppgifterna inte behandlas efter att den tiden löpt ut. Personuppgifter får inte heller behandlas om det framgår att uppgifterna inte längre behövs för ändamålet med behandlingen.

Bestämmelsen i första stycket hindrar inte att Säkerhetspolisen arkiverar och bevarar allmänna handlingar eller att arkivmaterial lämnas till en arkivmyndighet.

Förlängning av behandlingstid

3 § Säkerhetspolisen får i ett enskilt fall bestämma att personuppgifter får behandlas under längre tid än vad som följer av 1 § första stycket, om uppgifterna fortfarande behövs för det ändamål som de behandlas för.

Vid ett beslut enligt första stycket får behandlingstiden förlängas med som längst den tid som anges i 1 § andra stycket.

Om den behandlingstid som bestäms enligt första stycket innebär att uppgifter behandlas längre än vad som anges i 1 § andra stycket, ska ett särskilt beslut fattas och den särskilda tillsynsmyndigheten underrättas om det.

Bestämmande av behandlingstid för uppgifter om barn

4 § När Säkerhetspolisen bestämmer längsta tid för behandling av personuppgifter enligt 1 och 3 §§, ska särskilt beaktas att personuppgifter som rör barn ska omfattas av ett särskilt starkt personuppgiftsskydd.

Rätt att meddela föreskrifter

5 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

1. att personuppgifter får behandlas för arkivändamål av allmänt intresse eller vetenskapliga, statistiska eller historiska ändamål enligt 2 § andra stycket, och
2. begränsning av behandlingen av personuppgifter för ändamål inom denna lags tillämpningsområde vid digital arkivering.

5 kap. Säkerhetspolisens skyldigheter

Skyldighet att vidta åtgärder

1 § Om det framgår att personuppgifter behandlas i strid med lag eller annan författning, ska Säkerhetspolisen vidta de åtgärder som krävs för att behandlingen ska bli författningsenlig. Detsamma gäller om åtgärden krävs för att utföra en rättslig förpliktelse.

Om det till följd av första stycket krävs att personuppgifter raderas men uppgifterna behöver finnas kvar av bevisskäl, ska behandlingen av uppgifterna i stället utan onödigt dröjsmål begränsas till detta ändamål.

Tekniska och organisatoriska åtgärder

2 § Säkerhetspolisen ska, genom lämpliga tekniska och organisatoriska åtgärder, säkerställa och kunna visa att behandlingen av personuppgifter är författningsenlig och att registrerades rättigheter skyddas.

3 § Säkerhetspolisen ska när medlen för behandlingen bestäms och vid behandlingen, genom lämpliga tekniska och organisatoriska åtgärder, se till att nödvändiga skyddsåtgärder integreras i behandlingen (inbyggt dataskydd).

4 § Säkerhetspolisen ska se till att det i automatiserade behandlingssystem som regel inte är möjligt att behandla andra personuppgifter än de som behövs för varje särskilt angivet ändamål med behandlingen (dataskydd som standard).

5 § Säkerhetspolisen ska säkerställa att det i automatiserade behandlingssystem förs loggar över personuppgiftsbehandling i den utsträckning det behövs eller är särskilt föreskrivet.

För behandling som avses i 2 kap. 20 § ska loggar föras.

Tillgången till personuppgifter

6 § Säkerhetspolisen ska se till och kunna visa att tillgången till personuppgifter begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Säkerhetsåtgärder

7 § Säkerhetspolisen ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas, särskilt mot obehörig eller otillåten behandling och mot förlust, förstöring eller annan oavsiktlig skada.

Konsekvensbedömning

8 § Om en ny typ av behandling, eller betydande förändringar av redan pågående behandling, kan antas medföra särskild risk för intrång i den registrerades personliga integritet, ska Säkerhetspolisen innan behandlingen påbörjas eller förändringen genomförs bedöma konsekvenserna för skyddet av personuppgifter.

Förhandssamråd

9 § Om konsekvensbedömningen visar att det finns en särskild risk för intrång i den registrerades personliga integritet, eller om typen av behandling innebär en särskild risk för intrång, ska Säkerhetspolisen samråda med tillsynsmyndigheten i god tid innan behandlingen påbörjas eller betydande förändringar genomförs (förhandssamråd).

Samarbetsskyldighet

10 § Säkerhetspolisen ska samarbeta med de myndigheter som utövar tillsyn över personuppgiftsbehandling enligt denna lag och föreskrifter som har meddelats i anslutning till lagen.

Dataskyddsombud

11 § Säkerhetspolisen ska inom myndigheten utse ett eller flera dataskyddsombud och anmäla till tillsynsmyndigheten och den särskilda tillsynsmyndigheten när dataskyddsombud utses och entledigas.

12 § Dataskyddsombud ska

1. självständigt kontrollera att Säkerhetspolisen behandlar personuppgifter författningsenligt och på ett korrekt sätt och i övrigt fullgör sina skyldigheter,
2. informera och ge råd till Säkerhetspolisen och de som behandlar personuppgifter under myndighetens ledning om deras skyldigheter vid behandling av personuppgifter,
3. på begäran ge Säkerhetspolisen råd vid en konsekvensbedömning och kontrollera att den genomförs på korrekt sätt,
4. vara kontaktpunkt för enskilda i frågor som rör Säkerhetspolisens behandling av personuppgifter, och
5. samarbeta med tillsynsmyndigheten och den särskilda tillsynsmyndigheten och vara kontaktpunkt för dessa vid förhandssamråd och andra frågor som rör behandling av personuppgifter.

Personuppgiftsbiträden

13 § Säkerhetspolisen får, om det är lämpligt, anlita personuppgiftsbiträden för behandling av personuppgifter på myndighetens vägnar. Innan ett personuppgiftsbiträde anlitas ska Säkerhetspolisen försäkra sig om att biträdet kommer att vidta de lämpliga tekniska och organisatoriska åtgärder som krävs för att behandlingen av personuppgifter ska vara författningsenlig och för att skydda registrerades rättigheter.

Personuppgiftsbiträdets behandling av personuppgifter ska regleras i ett skriftligt avtal eller annan skriftlig överenskommelse mellan Säkerhetspolisen och biträdet.

14 § Ett personuppgiftsbiträde får inte anlita ett annat personuppgiftsbiträde utan skriftligt tillstånd från Säkerhetspolisen.

15 § Ett personuppgiftsbiträde och de som arbetar under biträdets ledning ska behandla personuppgifter i enlighet med instruktioner från Säkerhetspolisen.

Om ett personuppgiftsbiträde bestämmer ändamålen med och medlen för behandlingen, ska biträdet anses vara personuppgiftsansvarig för den behandlingen.

16 § Det som sägs om Säkerhetspolisens skyldigheter i 2–8 §§ och 10 § gäller även för personuppgiftsbiträden.

6 kap. Den registrerades rättigheter

Rätt till registerutdrag

1 § På begäran av en enskild ska Säkerhetspolisen lämna skriftligt besked om personuppgifter som rör honom eller henne behandlas. Om sådana uppgifter behandlas, ska sökanden få skriftlig information om

1. vilka personuppgifter om sökanden som behandlas,
2. varifrån personuppgifterna kommer,
3. den rättsliga grunden och ändamålen med behandlingen,
4. mottagare eller kategorier av mottagare av personuppgifterna, och
5. hur länge personuppgifterna får behandlas.

Uppgifter enligt första stycket, som den sökanden inte redan tagit del av, ska lämnas utan kostnad en gång per år. I andra fall får Säkerhetspolisen ta ut en rimlig avgift.

2 § Säkerhetspolisens skyldighet att lämna information enligt 1 § gäller inte i den utsträckning det är särskilt föreskrivet i lag eller annan författning eller annars framgår av beslut som har meddelats med stöd av författning att uppgifter inte får lämnas ut till den registrerade.

Om förutsättningarna i första stycket är uppfyllda, är Säkerhetspolisen inte skyldig att lämna ut skälen för beslutet. Säkerhetspolisen ska i dessa fall informera sökanden om andra möjligheter att pröva om dennes personuppgifter behandlas författningsenligt.

Skadestånd

3 § Den personuppgiftsansvarige ska ersätta den registrerade för den skada och kränkning av den personliga integriteten som orsakats av behandling av personuppgifter i strid med denna lag, eller föreskrifter som har meddelats i anslutning till den.

7 kap. Tillsyn

Tillsynsmyndighetens uppgifter

1 § Tillsynsmyndigheten ska

1. utöva allmän tillsyn över personuppgiftsbehandling, och
2. vid förhandssamråd enligt 5 kap. 9 § och när det i övrigt är påkallat ge råd och stöd till Säkerhetspolisen och personuppgiftsbiträden om deras skyldigheter enligt lag eller annan författning.

Undersökningsbefogenheter

2 § Tillsynsmyndigheten har rätt att av Säkerhetspolisen och personuppgiftsbiträdet på begäran få

1. tillgång till alla personuppgifter som behandlas,
2. upplysningar om och dokumentation av behandlingen av personuppgifter och säkerhets- och skyddsåtgärder,
3. tillträde till lokaler som Säkerhetspolisen eller personuppgiftsbiträdet disponerar samt tillgång till utrustning och andra medel för behandling av personuppgifter, och
4. den hjälp och den information som behövs för tillsynen.

Förebyggande befogenheter

3 § Om tillsynsmyndigheten bedömer att det finns risk för att personuppgifter kan komma att behandlas i strid med lag eller annan författning, ska myndigheten genom råd, rekommendationer eller påpekanden försöka förmå Säkerhetspolisen eller personuppgiftsbiträdet att vidta åtgärder för att motverka den risken.

4 § Tillsynsmyndigheten får utfärda en skriftlig varning för att planerad behandling av personuppgifter riskerar att stå i strid med lag eller annan författning. Detsamma gäller om pågående behandling riskerar att stå i strid med lag eller annan författning.

Korrigerande befogenheter

5 § Om tillsynsmyndigheten konstaterar att personuppgifter behandlas i strid med lag eller annan författning eller att Säkerhetspolisen eller personuppgiftsbiträdet på något annat sätt inte fullgör sina skyldigheter, får tillsynsmyndigheten

1. genom sådana åtgärder som anges i 3 § försöka förmå Säkerhetspolisen eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig, eller att uppfylla andra skyldigheter,
2. förelägga Säkerhetspolisen eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller att uppfylla andra skyldigheter, eller
3. förbjuda fortsatt behandling om bristen är allvarlig.

Om ett föreläggande utfärdas, ska det av föreläggandet framgå när åtgärderna senast ska vara genomförda och, om det är lämpligt, vilka åtgärder som ska vidtas.

6 § Tillsynsmyndighetens beslut får inte verkställas omedelbart.

Särskild tillsyn

7 § Bestämmelser om särskild tillsyn över Säkerhetspolisens behandling av personuppgifter finns i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet.

8 § Den myndighet som utövar tillsyn enligt 7 § (särskild tillsynsmyndighet) och Säkerhetspolisen ska löpande samverka i frågor som rör Säkerhetspolisens skyldigheter enligt lag eller annan författning.

9 § Säkerhetspolisen ska i skälig omfattning vidta de tekniska åtgärder som är nödvändiga för att den särskilda tillsynsmyndigheten ska kunna utföra sina arbetsuppgifter på ett ändamålsenligt sätt.

Den särskilda tillsynsmyndigheten har utöver de befogenheter som följer av särskild lagstiftning även de befogenheter som följer av 2 §.

8 kap. Överklagande

Överklagande av den personuppgiftsansvariges beslut

1 § Beslut om att inte lämna information eller att ta ut avgift enligt 6 kap. 1 § får överklagas till kammarrätt.

Överklagande av tillsynsmyndighetens beslut

2 § Tillsynsmyndighetens beslut enligt denna lag får överklagas till Försvarsunderrättelsedomstolen.

3 § Vid prövning enligt 2 § ska Försvarsunderrättelsedomstolen tillämpa 2–8, 10–15, 17–26, 28–32 och 38–53 §§ förvaltningsprocesslagen (1971:291) i tillämpliga delar samt 9 §, 10 § första stycket 1 och 15 § lagen (2009:966) om Försvarsunderrättelsedomstol.

Muntliga förhandlingar i domstolen är inte offentliga. Rätten får besluta att en förhandling ska vara offentlig i de delar där det står klart att inga uppgifter för vilka det hos domstolen gäller sådan sekretess som avses i offentlighets- och sekretesslagen (2009:400) kommer att uppenbaras.

När ett beslut överklagas är tillsynsmyndigheten motpart i domstolen. Den särskilda tillsynsmyndigheten ska beredas tillfälle att yttra sig i målet om det behövs.

Överklagandeförbud

4 § Försvarsunderrättelsedomstolens avgöranden får inte överklagas.

5 § Övriga beslut enligt denna lag får inte överklagas.

---

1. Denna lag träder i kraft den 1 januari 2027.

2. Genom denna lag upphävs lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter.

3. För behandling av personuppgifter som påbörjats innan lagen trätt i kraft får lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter tillämpas fram till och med den 31 december 2029 i stället för den nya lagen.

4. Äldre föreskrifter gäller fortfarande för överklagande av beslut som har meddelats före ikraftträdandet.

1.2 Förslag till lag om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar

Härigenom föreskrivs följande.

1 kap. Allmänna bestämmelser

Lagens tillämpningsområde

1 § Denna lag gäller utöver lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter. Lagen är tillämplig för automatiserad behandling av personuppgifter som registreras eller har registrerats i en särskild uppgiftssamling.

Vid tillämpning av denna lag ska följande bestämmelser i lagen om Säkerhetspolisens behandling av personuppgifter inte tillämpas

– 2 kap. 5, 11, 13–16, 20 och 21 §§,
– 3 kap.,
– 4 kap.,
– 6 kap. 1 och 2 §§, samt
– 7 kap. 2 § 1.

Definitioner

2 § I denna lag används följande uttryck med nedan angiven betydelse.

Uttryck	Betydelse
Särskild uppgiftssamling	En samling med uppgifter som inte får tas fram utan tillstånd och där tillgången till uppgifterna är begränsad genom tekniska eller organisatoriska åtgärder.
Registrering	Införande av uppgifter i en särskild uppgiftssamling.
Framtagning	Tillgängliggörande av personuppgifter som innebär att innehållet i eller innebörden av dem avslöjas.

2 kap. Registrering

Registreringsbeslut

1 § Säkerhetspolisen får besluta att personuppgifter ska registreras i en särskild uppgiftssamling, om det är befogat för ett ändamål inom någon av de verksamheter som anges i 2 kap. 4, 6 eller 7 § lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter.

Säkerhetspolisen ska utse de personer som får fatta beslut enligt första stycket. Sådana personer ska ha de särskilda kunskaper och den erfarenhet som uppgiften kräver.

Dokumentation

2 § Ett beslut enligt 1 § ska dokumenteras. Av ett registreringsbeslut ska framgå

1. vad de registrerade uppgifterna i huvudsak avser och från vilken källa eller vilka källor de härrör,
2. vilket intrång i enskilda och allmänna intressen som behandling av uppgifterna kan antas medföra,
3. för vilket eller vilka ändamål uppgifterna registreras,
4. hur länge uppgifterna som längst får behandlas (behandlingstid), och
5. de skäl och omständigheter i övrigt som föranlett registreringen.

Varje uppgift i en särskild uppgiftssamling ska kunna spåras till ett beslut enligt första stycket.

Behandlingstid

3 § Behandlingstiden i ett registreringsbeslut får inte bestämmas till längre än tio år.

Om behandlingstiden bestäms så att personuppgifter sammanlagt behandlas längre än fem år, ska skälen till det anges särskilt. Den särskilda tillsynsmyndigheten ska underrättas om sådana beslut.

Förlängd behandlingstid

4 § Säkerhetspolisen får besluta att förlänga behandlingstiden, om fortsatt behandling av uppgifterna är befogad för något ändamål som anges i 1 § första stycket.

Vid ett beslut om förlängning av behandlingstiden ska 2 och 3 §§ tillämpas.

Den sammanlagda behandlingstiden får överstiga tjugofem år endast om det finns synnerliga skäl.

3 kap. Framtagning och annan behandling

Framtagning

1 § Uppgifter som är registrerade i en särskild uppgiftssamling får tas fram endast efter tillstånd.

2 § Säkerhetspolisen får ansöka om tillstånd till framtagning, om det behövs för ett särskilt ändamål inom någon av de verksamheter som anges i 2 kap. 4, 6 och 7 §§ lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter.

3 § De befattningshavare vid Säkerhetspolisen som regeringen föreskriver får besluta om tillstånd till framtagning, om ett inhämtande av domstolens tillstånd skulle medföra en fördröjning som är av väsentlig betydelse för att avvärja en omedelbart förestående fara för människors liv, hälsa eller omfattande förstörelse av egendom.

Ett tillstånd enligt första stycket ska vara förenligt med 5 § och beslutet ska utformas enligt 4 kap. 6 §. Den särskilda tillsynsmyndigheten ska omedelbart underrättas om beslutet. Beslutet ska senast dagen efter att det fattats anmälas till domstolen. Om ett beslut inte anmälts i rätt tid, får det inte ligga till grund för framtagning och personuppgifter som tagits fram med stöd av beslutet får inte längre behandlas.

Övrig behandling

4 § Annan personuppgiftsbehandling än registrering och framtagning får ske

1. för att tekniskt möjliggöra, effektivisera eller förenkla en framtagning,
2. om det behövs för att personuppgifter ska behandlas författningsenligt och på ett korrekt sätt, eller
3. om det behövs för ett särskilt, uttryckligt angivet och berättigat ändamål.

Förutsättningar för tillstånd till framtagning

5 § Tillstånd till framtagning får lämnas endast om

1. behandlingen står i överensstämmelse med lag och Sveriges internationella åtaganden,
2. behandlingen behövs för ändamålet, och
3. det står klart att skälet för att utföra behandlingen överväger intrånget i de enskilda eller allmänna intressen som kan påverkas av den.

En framtagning enligt första stycket får inte förväntas leda till att fler personuppgifter än vad som behövs för ändamålet behandlas.

Ett tillstånd till framtagning ska gälla för viss tid.

4 kap. Handläggningen i domstol

Ansökan om framtagning

1 § Ansökan om tillstånd till framtagning görs hos Försvarsunderrättelsedomstolen.

2 § I ansökan ska sökanden ange

1. vilka kategorier av uppgifter framtagningen ska avse och från vilka typer av källor framtagning ska ske,
2. det särskilda ändamålet med och behovet av framtagningen,
3. vilka sökbegrepp, kategorier av sökbegrepp eller andra urvalskriterier som är avsedda att användas vid framtagningen och, om det finns skäl, med vilken teknik urvalet ska ske,
4. under vilken tid tillståndet ska gälla, och

5. de skäl och omständigheter i övrigt som sökanden vill åberopa till stöd för sin ansökan.

Om sökbegrepp ska innehålla känsliga personuppgifter, eller om urvalet av annan anledning förväntas ske utifrån sådana uppgifter, ska det anges särskilt.

3 § Ett beslut om framtagning enligt 3 kap. 3 § som anmälts till domstolen ska anses vara en ansökan om framtagning. En sådan anmälan ska prövas skyndsamt.

Domstolen får bestämma att ett beslut som avses i första stycket inte får ligga till grund för framtagning. Domstolen får också besluta att personuppgifter som tagits fram med stöd av ett anmält beslut inte längre får behandlas.

Domstolen får fatta beslut enligt andra stycket innan ansökan slutligen har prövats.

Sammanträde

4 § När en ansökan om framtagning har inkommit ska domstolen, om det behövs, hålla sammanträde. Till sammanträdet ska Säkerhetspolisen och den särskilda tillsynsmyndigheten kallas.

Den särskilda tillsynsmyndighetens yttrande

5 § Innan domstolen avgör en tillståndsfråga ska den särskilda tillsynsmyndigheten ges tillfälle att yttra sig, om det inte är obehövligt.

Tillstånd till framtagning

6 § Försvarsunderrättelsedomstolen får lämna tillstånd till framtagning. I tillståndet ska domstolen ange

1. från vilka kategorier av uppgifter och från vilken typ av källor som framtagning får ske,
2. de sökbegrepp, kategorier av sökbegrepp eller andra urvalskriterier som får användas vid framtagning samt, om det finns skäl, med vilken teknik urvalet får ske,
3. under vilken tid tillståndet gäller,

4. de villkor i övrigt som behövs för att begränsa intrånget i enskilda eller allmänna intressen samt för att möjliggöra en effektiv tillsyn, och

5. de skäl som bestämt utgången.

Ändring av tillstånd

7 § Domstolen får besluta om ändring av vad som föreskrivits i ett tillstånd.

Domstolen

8 § I fråga om domförhet gäller 9 § lagen (2009:966) om Försvarsunderrättelsedomstol.

9 § En ordförande eller en vice ordförande får ensam

1. företa förberedande åtgärder och besluta om avskrivning,
2. fatta beslut enligt 3 § tredje stycket, och
3. besluta om ändring enligt 7 §, om ändringen är av enkel beskaffenhet.

Ordföranden får förordna en lagfaren tjänsteman vid domstolen att ensam på domstolens vägnar vidta förberedande åtgärder.

10 § Om inte annat följer av denna lag, gäller 3–5, 8, 14, 17–26, 29–32 och 38–53 §§ förvaltningsprocesslagen (1971:291) i tillämpliga delar vid förfarandet i domstolen.

11 § Muntliga förhandlingar i domstolen är inte offentliga.

Rätten får besluta att en förhandling ska vara offentlig i de delar där det är uppenbart att inga sekretessbelagda uppgifter enligt offentlighets- och sekretesslagen (2009:400) kommer att avslöjas.

12 § Domstolens avgörande av saken sker genom dom. Andra avgöranden sker genom beslut.

13 § I fråga om omröstning gäller 16 kap. rättegångsbalken i tillämpliga delar.

Överklagandeförbud

14 § Domstolens avgöranden enligt denna lag får inte överklagas.

5 kap. Tillsyn

Radering

1 § Den särskilda tillsynsmyndigheten får besluta att framtagna uppgifter ska raderas, om det kan konstateras att framtagningen inte har varit förenlig med ett tillstånd enligt denna lag.

Framtagning för tillsyn

2 § Den särskilda tillsynsmyndigheten har rätt att ansöka om tillstånd till framtagning för tillsynsändamål. I ett enskilt fall har också tillsynsmyndigheten rätt att ansöka om framtagning för ett sådant ändamål.

Säkerhetspolisen ska ges tillfälle att yttra sig över ansökan.

Denna lag träder i kraft den 1 januari 2027.

1.3 Förslag till lag om ändring i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet

Härigenom föreskrivs i fråga om lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet att 1 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 §[1]	
Säkerhets- och integritetsskyddsnämnden (nämnden) ska utöva tillsyn över	
1. brottsbekämpande myndigheters användning av hemliga tvångsmedel och kvalificerade skyddsidentiteter,	
2. brottsbekämpande myndigheters användning av andra tvångsmedel enligt lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott än de som avses i 1, om inte den som åtgärden utförts hos eller annars riktats mot har närvarat vid åtgärden,	
3. Säkerhetspolisens användning av hemliga tvångsmedel vid särskild kontroll av vissa utlänningar, och	
4. därmed sammanhängande verksamhet.	
Nämnden ska även utöva tillsyn över den behandling av personuppgifter som utförs av Polismyndigheten, Säkerhetspolisen och Ekobrottsmyndigheten enligt brottsdatalagen (2018:1177) och lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område för de syften som anges i 1 kap. 1 § i den sistnämnda lagen, och lagen *(2019:1182)* om Säkerhetspolisens behandling av personuppgifter. Tillsynen ska särskilt avse behandling enligt 2 kap. 11 § brottsdatalagen *och 2 kap. 9 §*	Nämnden ska även utöva tillsyn över den behandling av personuppgifter som utförs av Polismyndigheten, Säkerhetspolisen och Ekobrottsmyndigheten enligt brottsdatalagen (2018:1177) och lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område för de syften som anges i 1 kap. 1 § i den sistnämnda lagen, och lagen *(2026:000)* om Säkerhetspolisens behandling av personuppgifter. Tillsynen ska särskilt avse behandling enligt 2 kap. 11 § brottsdatalagen.

[1] Senaste lydelse 2024:563.

lagen om Säkerhetspolisens behandling av personuppgifter.	
Nämnden ska också utöva tillsyn över Polismyndighetens och Säkerhetspolisens tillämpning av lagen (2019:547) om förbud mot användning av vissa uppgifter för att utreda brott.	Nämnden ska också utöva tillsyn över Polismyndighetens och Säkerhetspolisens tillämpning av lagen (2019:547) om förbud mot användning av vissa uppgifter för att utreda brott. *Nämnden ska även utöva tillsyn över Säkerhetspolisens behandling av personuppgifter enligt lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar.*

Tillsynen ska särskilt syfta till att säkerställa att verksamhet enligt första–tredje styckena bedrivs i enlighet med lag eller annan författning.

---

1. Denna lag träder i kraft den 1 januari 2027.

2. Äldre föreskrifter gäller fortfarande för nämndens tillsyn över Säkerhetspolisens personuppgiftsbehandling som utförts före ikraftträdandet eller som sker med stöd av övergångsbestämmelser till lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter.

1.4 Förslag till lag om ändring av offentlighets- och sekretesslagen (2009:400)

Härigenom föreskrivs i fråga om offentlighets- och sekretesslagen (2009:400)

dels att 18 kap. 2 §, 35 kap. 1 och 10 §§ ska ha följande lydelse,

dels att rubriken närmast före 42 kap. 5 § i stället ska sättas närmast före den nya 42 kap. 4 d §,

dels att det ska införas nya paragrafer, 18 kap. 2 a §, 35 kap. 1 a § samt 42 kap. 4 d och 4 e §§, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
18 kap.	
2 §[1]	
Sekretess gäller för uppgift som hänför sig till sådan verksamhet som avses i 2 kap. 1 § 1 lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område, om det inte står klart att uppgiften kan röjas utan att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas.	
Sekretess gäller, under motsvarande förutsättningar som anges i första stycket, för uppgift som hänför sig till sådan verksamhet som avses i	
1. 2 kap. 1 § 1 lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område,	
2. 2 kap. 1 § 1 lagen (2018:1695) om Kustbevakningens behandling av personuppgifter inom brottsdatalagens område,	
3. 2 kap. 1 § 1 lagen (2018:1696) om Skatteverkets behandling av personuppgifter inom brottsdatalagens område, eller	
4. 2 kap. *1 § 1* lagen *(2019:1182)* om Säkerhetspolisens behandling av personuppgifter.	4. 2 kap. *4 §* lagen *(2026:000)* om Säkerhetspolisens behandling av personuppgifter.
Sekretess enligt första stycket gäller inte för uppgift som hänför sig till verksamhet hos Säkerhetspolisen och som har förts in i en allmän handling före år 1949.	
För uppgift i en allmän handling gäller sekretessen i högst sjuttio år	

[1] Senaste lydelse 2019:1184.

2 a §

Sekretess gäller för uppgift i särskilda uppgiftssamlingar, enligt lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar, som lämnar eller kan bidra till upplysning om Säkerhetspolisens verksamhet att förebygga, förhindra och upptäcka brottslig verksamhet.

För uppgift i allmän handling gäller sekretessen i sjuttio år.

Sekretess enligt första stycket hindrar inte en framtagning enligt lagen om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar.

35 kap.

1 §[2]

Sekretess gäller för uppgift om en enskilds personliga och ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider skada eller men och uppgiften förekommer i

1. utredning enligt bestämmelserna om förundersökning i brottmål,

2. angelägenhet som avser användning av tvångsmedel i brottmål eller i annan verksamhet för att förebygga brott eller i ärende enligt lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder,

3. angelägenhet som avser säkerhetsprövning enligt säkerhetsskyddslagen (2018:585),

4. annan verksamhet som syftar till att förebygga, uppdaga, utreda eller beivra brott eller verkställa uppbörd och som bedrivs av en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen, Skatteverket, Tullverket eller Kustbevakningen,

[2] Senaste lydelse 2024:788.

5. register som förs av Polismyndigheten enligt 5 kap. lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas med stöd av de bestämmelserna, eller uppgifter som behandlas av Säkerhetspolisen eller Polismyndigheten med stöd av lagen *(2019:1182)* om Säkerhetspolisens behandling av personuppgifter,	5. register som förs av Polismyndigheten enligt 5 kap. lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas med stöd av de bestämmelserna, eller uppgifter som behandlas av Säkerhetspolisen eller Polismyndigheten med stöd av lagen *(2026:000)* om Säkerhetspolisens behandling av personuppgifter,

6. register som förs enligt lagen (1998:621) om misstankeregister,

7. register som förs av Skatteverket enligt lagen (2018:1696) om Skatteverkets behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas där med stöd av samma lag,

8. särskilt ärenderegister över brottmål som förs av åklagarmyndighet, om uppgiften inte hänför sig till registrering som avses i 5 kap. 1 §,

9. register som förs av Tullverket enligt lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas där med stöd av samma lag, eller

10. utredning om självständigt förverkande.

Sekretessen enligt första stycket 2 gäller hos domstol i dess rättskipande eller rättsvårdande verksamhet endast om det kan antas att den enskilde eller någon närstående till honom eller henne lider skada eller men om uppgiften röjs. Vid förhandling om användning av tvångsmedel gäller sekretess för uppgift om vem som är misstänkt endast om det kan antas att fara uppkommer för att den misstänkte eller någon närstående till honom eller henne utsätts för våld eller lider annat allvarligt men om uppgiften röjs.

Första stycket gäller inte om annat följer av 2, 6 eller 7 §.

För uppgift i en allmän handling gäller sekretessen i högst sjuttio år.

1 a §

Sekretess gäller för uppgift om en enskilds personliga och ekonomiska förhållanden i särskilda uppgiftssamlingar enligt lagen (2026:000) om Säkerhetspolisens

behandling av personuppgifter i särskilda uppgiftssamlingar.

För uppgift i allmän handling gäller sekretessen i sjuttio år.

Sekretess enligt första stycket hindrar inte en framtagning enligt lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar.

10 §[3]

Sekretessen enligt 1 § hindrar inte att en uppgift lämnas ut

1. till en enskild enligt vad som föreskrivs i lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare,

2. till en enskild enligt vad som föreskrivs i säkerhetsskyddslagen (2018:585) och i förordning som har meddelats med stöd i den lagen,

3. till en enskild enligt vad som föreskrivs i 27 kap. 8 § rättegångsbalken,

4. enligt vad som föreskrivs i

– lagen (1998:621) om misstankeregister,

– lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område,

– lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område,

– lagen (2018:1695) om Kustbevakningens behandling av personuppgifter inom brottsdatalagens område,

– lagen (2018:1696) om Skatteverkets behandling av personuppgifter inom brottsdatalagens område,

– lagen (2018:1697) om åklagarväsendets behandling av personuppgifter inom brottsdatalagens område,

– lagen *(2019:1182)* om Säkerhetspolisens behandling av personuppgifter, eller

– lagen *(2026:000)* om Säkerhetspolisens behandling av personuppgifter, eller

förordningar som har stöd i dessa lagar.

[3] Senaste lydelse 2019:1184,

42 kap.

4 d §

Får Säkerhets- och integritetsskyddsnämnden en sekretessreglerad uppgift från en myndighet i mål om tillstånd enligt lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar blir sekretessbestämmelsen tillämplig på uppgiften även hos nämnden.

4 e §

Sekretess som gäller hos Säkerhets- och integritetsskyddsnämnden enligt 4 d §, 6–8 §§, 15 kap. eller 18 kap., hindrar inte att en uppgift lämnas till domstol, om uppgiften behövs för tillståndsprövning enligt lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar.

---

1. Denna lag träder i kraft den 1 januari 2027.

2. Äldre föreskrifter gäller fortfarande för uppgifter som behandlas med stöd av övergångsbestämmelser till lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter.

1.5 Förslag till lag om ändring i lagen (2009:966) om Försvarsunderrättelsedomstol

Härigenom föreskrivs i fråga lagen (2009:966) om Försvarsunderrättelsedomstol

dels att 1, 2, 4, 5, 9 §§ ska ha följande lydelse,

dels att rubriken närmast före 5 § ska lyda ”Integritetsskyddsombud i mål om signalspaning”,

dels att det ska införas en ny paragraf, 10 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 §	
Försvarsunderrättelsedomstolen ska pröva frågor om tillstånd till signalspaning enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.	
	Försvarsunderrättelsedomstolen ska även
	1. pröva frågor om tillstånd till framtagning enligt lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar,
	2. pröva beslut som ska överklagas dit enligt lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter.
2 §[1]	
Försvarsunderrättelsedomstolen består av *en* ordförande, *en eller* högst två vice ordförande samt minst två och högst *sex* särskilda ledamöter.	Försvarsunderrättelsedomstolen består av *högst två* ordförande, högst två vice ordförande samt minst två och högst *tio* särskilda ledamöter. *En av ordförandena ska vara chef för domstolen.*

Ledamöterna ska vara svenska medborgare och får inte vara underåriga eller i konkurstillstånd eller ha förvaltare enligt 11 kap. 7 § föräldrabalken. Innan en ledamot börjar tjänstgöra i domstolen, ska han eller hon ha avlagt domared.

[1] Senaste lydelse 2010:1399.

I lagen (2010:1390) om utnämning av ordinarie domare finns bestämmelser om utnämning av ordförande i domstolen. Vice ordförande och särskilda ledamöter förordnas av regeringen för fyra år.	I lagen (2010:1390) om utnämning av ordinarie domare finns bestämmelser om utnämning av *ordförande tillika chef och övriga* ordförande i domstolen. Vice ordförande och särskilda ledamöter förordnas av regeringen för fyra år.
4 §	
Är *ordföranden* förhindrad att tjänstgöra, *inträder* en vice ordförande i ordförandens ställe.	Är *en ordförande* förhindrad att tjänstgöra, *får* en vice ordförande inträda i ordförandens ställe.
5 §	
Ett integritetsskyddsombud ska bevaka enskildas integritetsintresse i mål vid domstolen. Ombudet har rätt att ta del av det som förekommer i målet och att yttra sig.	Ett integritetsskyddsombud ska bevaka enskildas integritetsintresse i mål vid domstolen *om tillstånd till signalspaning*. Ombudet har rätt att ta del av det som förekommer i målet och att yttra sig.
9 §	
Försvarsunderrättelsedomstolen är domför med ordförande och två särskilda ledamöter. Fler än tre ledamöter får inte delta i ett avgörande.	Försvarsunderrättelsedomstolen är domför med en ordförande och två särskilda ledamöter. Fler än tre ledamöter får inte delta i ett avgörande.
	10 a §
	I lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar finns regler om handläggningen av mål enligt den lagen.

Denna lag träder i kraft den 1 januari 2027.

1.6 Förslag till lag om ändring i lagen (2010:1390) om utnämning av ordinarie domare

Härigenom föreskrivs i fråga om lagen (2010:1390) om utnämning av ordinarie domare att 1 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 §[2]	
Denna lag avser utnämning av ordinarie domare. Dessa är	
1. justitieråd tillika ordförande, justitieråd tillika avdelningsordförande och övriga justitieråd i Högsta domstolen och Högsta förvaltningsdomstolen,	
2. president, lagman samt råd tillika vice ordförande på avdelning och övriga råd i hovrätt och kammarrätt,	
3. lagman, chefsrådman och rådman i tingsrätt och förvaltningsrätt,	
4. tekniska råd,	
5. patentråd,	
6. ordförande tillika chef och övriga ordförande i Arbetsdomstolen,	
7. ordförande i Försvarsunderrättelsedomstolen.	7. ordförande *tillika chef och övriga ordförande* i Försvarsunderrättelsedomstolen.

Denna lag träder i kraft den 1 januari 2027.

[2] Senaste lydelse 2016:227.

1.7 Förslag till lag om ändring i lagen (2017:496) om internationellt polisiärt samarbete

Härigenom föreskrivs i fråga om lagen (2017:496) om internationellt polisiärt samarbete att 6 kap. 1 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
6 kap.	
1 §[1]	
Om inte annat följer av denna lag eller föreskrifter som regeringen har meddelat i anslutning till lagen gäller brottsdatalagen (2018:1177) och följande författningar för respektive myndighet för behandling av personuppgifter vid internationellt polisiärt samarbete:	
– lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område,	
– lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område	
– lagen (2018:1695) om Kustbevakningens behandling av personuppgifter inom brottsdatalagens område, eller	
– lagen (*2019:1182*) om Säkerhetspolisens behandling av personuppgifter.	– lagen (*2026:000*) om Säkerhetspolisens behandling av personuppgifter.

Denna lag träder i kraft den 1 januari 2027.

[1] Senaste lydelse 2018:1247.

1.8 Förslag till lag om ändring i lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning

Härigenom föreskrivs i fråga om lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning att 1 kap. 3 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 kap.	
3 §[1]	
Bestämmelserna i 2 § gäller inte i verksamhet som omfattas av	
1. lagen (2021:1171) om behandling av personuppgifter vid Försvarsmakten,	
2. lagen (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt, eller	
3. lagen (*2019:1182*) om Säkerhetspolisens behandling av personuppgifter.	3. lagen (*2026:000*) om Säkerhetspolisens behandling av personuppgifter.

1. Denna lag träder i kraft den 1 januari 2027.

2. Äldre föreskrifter ska fortsätta att tillämpas för personuppgifter som behandlas med stöd av övergångsbestämmelserna till lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter.

[1] Senaste lydelse 2021:114.

1.9 Förslag till lag om ändring i säkerhetsskyddslagen (2018:585)

Härigenom föreskrivs i fråga om säkerhetsskyddslagen (2018:585) att 3 kap. 13 och14 §§ ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
3 kap.	
13 §[1]	
Med registerkontroll avses att uppgifter hämtas från ett register som omfattas av lagen (1998:620) om belastningsregister eller lagen (1998:621) om misstankeregister. Med registerkontroll avses också att uppgifter hämtas som behandlas med stöd av	
1. lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område, eller	
2. lagen *(2019:1182)* om Säkerhetspolisens behandling av personuppgifter.	2. lagen (*2026:000*) om Säkerhetspolisens behandling av personuppgifter.
14 §[2]	
Registerkontroll ska göras om anställningen eller deltagandet i verksamheten har placerats i säkerhetsklass. Uppgifter ska löpande hämtas under den tid deltagandet i den säkerhetskänsliga verksamheten pågår.	
För säkerhetsklass 1 eller 2 får uppgifter om den kontrollerade som finns i belastningsregistret eller misstankeregistret eller som behandlas med stöd av lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område eller lagen (*2019:1182*) om Säkerhetspolisens behandling av personuppgifter hämtas. Motsvarande uppgifter får även hämtas	För säkerhetsklass 1 eller 2 får uppgifter om den kontrollerade som finns i belastningsregistret eller misstankeregistret eller som behandlas med stöd av lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område eller lagen (*2026:000*) om Säkerhetspolisens behandling av personuppgifter hämtas. Motsvarande uppgifter får även hämtas

[1] Senaste lydelse 2019:1187.
[2] Senaste lydelse 2019:1187.

om den kontrollerades make eller sambo.

om den kontrollerades make eller sambo.

För säkerhetsklass 3 får sådana uppgifter om den kontrollerade som finns i belastningsregistret eller misstankeregistret eller som behandlas hos Säkerhetspolisen med stöd av lagen om polisens behandling av personuppgifter inom brottsdatalagens område eller lagen om Säkerhetspolisens behandling av personuppgifter hämtas.

Om det finns synnerliga skäl får även andra uppgifter än sådana som anges i andra och tredje styckena hämtas.

---

1. Denna lag träder i kraft den 1 januari 2027.

2. Äldre föreskrifter ska gälla för personuppgifter som behandlas enligt övergångsbestämmelser till lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter.

1.10 Förslag till lag om ändring i kamerabevakningslagen (2018:1200)

Härigenom föreskrivs i fråga om kamerabevakningslagen (2018:1200) att 7 och 14 §§ ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
7 §[1]	
Vid utförande av en uppgift av allmänt intresse som följer av lag eller annan författning, kollektivavtal eller beslut som har meddelats med stöd av lag eller annan författning får kamerabevakning bedrivas om	
1. bevakningen är nödvändig för att utföra uppgiften, och	
2. förutsättningarna som följer av 8, 9, 11 och 13 §§ är uppfyllda.	
För kamerabevakning som en myndighet bedriver i en verksamhet för vilken personuppgiftsbehandlingen omfattas av brottsdatalagen (2018:1177) eller lagen (*2019:1182*) om Säkerhetspolisens behandling av personuppgifter gäller i stället bestämmelserna i 14 §	För kamerabevakning som en myndighet bedriver i en verksamhet för vilken personuppgiftsbehandlingen omfattas av brottsdatalagen (2018:1177) eller lagen (*2026:000*) om Säkerhetspolisens behandling av personuppgifter gäller i stället bestämmelserna i 14 §
14 §[2]	
I en verksamhet för vilken personuppgiftsbehandlingen omfattas av brottsdatalagen (2018:1177) eller lagen (*2019:1182*) om Säkerhetspolisens behandling av personuppgifter får kamerabevakning bedrivas av en myndighet om	I en verksamhet för vilken personuppgiftsbehandlingen omfattas av brottsdatalagen (2018:1177) eller lagen (*2026:000*) om Säkerhetspolisens behandling av personuppgifter får kamerabevakning bedrivas av en myndighet om
1. bevakningen är nödvändig för ett syfte som anges i de lagarna, och	
2. förutsättningarna som följer av 14 a–14 d §§ är uppfyllda.	

Denna lag träder i kraft den 1 januari 2027.

---

[1] Senaste lydelse 2025:220.
[2] Senaste lydelse 2025:220.

1.11 Förslag till lag om ändring i lagen (2019:547) om förbud mot användning av vissa uppgifter för att utreda brott

Härigenom föreskrivs i fråga om lagen (2019:547) om förbud mot användning av vissa uppgifter för att utreda brott att 1 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 §	
Uppgifter i underrättelser som Försvarets radioanstalt rapporterat till en annan myndighet i enlighet med lagen (2000:130) om försvarsunderrättelseverksamhet får inte användas för att utreda brott.	
	Uppgifter som Säkerhetspolisen tagit fram från en särskild uppgiftssamling enligt lag (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar får inte användas för att utreda brott.

Denna lag träder i kraft den 1 januari 2027.

1.12 Förslag till förordning om Säkerhetspolisens behandling av personuppgifter

Härigenom föreskrivs följande.

1 kap. Allmänna bestämmelser

1 § I denna förordning finns kompletterande föreskrifter om sådan behandling av personuppgifter som omfattas av lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter.

2 § Uttryck som används i denna förordning har samma innebörd och tillämpningsområde som i lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter

2 kap Behandling av personuppgifter

1 § Säkerhetspolisen ska besluta vilka tjänstemän som har tillräckliga kunskaper enligt 2 kap. 9 § tredje stycket lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter.

2 § Säkerhetspolischefen och biträdande säkerhetspolischefen får fatta beslut enligt 2 kap. 10 § lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter.

3 kap. Informationsutbyte

Direktåtkomst

1 § Av information enligt 3 kap. 7 § andra stycket lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter ska omfattningen av direktåtkomsten framgå.

2 § Säkerhetspolisen får ställa villkor i fråga om behörighet och säkerhet för att myndigheten ska medge direktåtkomst enligt 3 kap. 6 eller 7 § lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter.

Direktåtkomst får inte medges innan Säkerhetspolisen har försäkrat sig om att den mottagande myndigheten uppfyller kraven på behörighet och säkerhet.

3 § Polismyndigheten får medges direktåtkomst enligt 3 kap. 6 § 1 lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter till personuppgifter som behandlas enligt 2 kap 11 § i den lagen för att

1. förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar, brott mot Sveriges säkerhet eller terrorbrott,
2. utreda eller lagföra sådana brott,
3. fullgöra uppgifter

a) i samband med personskydd av den centrala statsledningen och andra som regeringen eller Säkerhetspolisen bestämmer, eller

b) enligt utlännings- och medborgarskapslagstiftningen.

4 § Försvarsmakten får medges direktåtkomst enligt 3 kap. 6 § 2 lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter till personuppgifter som behandlas enligt 2 kap 11 § i den lagen för att

1. förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar, brott mot Sveriges säkerhet eller terrorbrott, eller
2. utreda eller lagföra sådana brott.

5 § Försvarets radioanstalt får medges direktåtkomst enligt 3 kap. 6 § 2 lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter till personuppgifter som behandlas enligt 2 kap 11 § i den lagen för att

1. förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar, brott mot Sveriges säkerhet eller terrorbrott, eller
2. utreda eller lagföra sådana brott.

Utlämnande till mottagare utomlands

6 § Säkerhetspolisen ska dokumentera bedömningen av att de mottagare som avses i 3 kap. 3 § lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter kan garantera tillräckligt skydd för personuppgifterna.

Ett utlämnande enligt 3 kap. 3 § lagen om Säkerhetspolisens behandling av personuppgifter får bara ske om det finns en bedömning som är aktuell.

De bedömningar som avses i första stycket ska hållas tillgänglig för tillsynsmyndigheten och den särskilda tillsynsmyndigheten tillsammans med underlaget för bedömningen.

7 § Utlämnande av personuppgifter till utländska mottagare som sker med stöd av 3 kap. 4 § lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter ska dokumenteras. Av dokumentationen ska framgå vilka personuppgifter som överförts, datum och tidpunkt för överföringen, ändamålet med överföringen, till vem personuppgifterna överfördes. Av dokumentationen ska även Säkerhetspolisens bedömning enligt 3 kap. 4 § 1 och 2 lagen om Säkerhetspolisens behandling av personuppgifter framgå.

4 kap. Längsta tid som personuppgifter får behandlas

Rutiner för att säkerställa tidsfristerna

1 § Säkerhetspolisen ska se till att det finns rutiner för att säkerställa att de som behandlar personuppgifter respekterar tidsfristerna för när personuppgifter inte längre får behandlas.

Arkivering

2 § När uppgifter och handlingar arkiveras digitalt ska de avskiljas så att de inte kan behandlas för att utföra en uppgift enligt 1 kap. 2 § lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter.

Åtkomsten till arkiverade uppgifter och handlingar ska begränsas till särskilt angivna tjänstemän.

3 § Riksarkivet får, efter att ha gett Säkerhetspolisen tillfälle att yttra sig, meddela föreskrifter enligt 4 kap. 5 § 1 lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter om behandling för arkivändamål av allmänt intresse och vetenskapliga, statistiska eller historiska ändamål.

4 § Säkerhetspolisen får, efter att ha gett Riksarkivet tillfälle att yttra sig, meddela närmare föreskrifter om digital arkivering.

5 kap. Säkerhetspolisen skyldigheter

1 § Om det visar sig att sådana personuppgifter som anges i 5 kap. 1 § lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter har lämnats ut, ska mottagaren omedelbart underrättas om det.

Om sådana personuppgifter har gjorts tillgängliga ska, så långt det är möjligt, även den som har tagit del av personuppgifterna omedelbart underrättas.

Tekniska och organisatoriska åtgärder

2 § De tekniska och organisatoriska åtgärder som Säkerhetspolisen ska vidta enligt 5 kap. 2 och 3 §§ lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter ska vara rimliga med hänsyn till behandlingens art, omfattning, sammanhang och ändamål och de särskilda riskerna med behandlingen.

När Säkerhetspolisen vidtar åtgärder enligt 5 kap. 3 § samma lag ska även de tekniska möjligheterna och kostnaderna för åtgärderna beaktas.

Dokumentationsskyldighet

3 § De tekniska och organisatoriska åtgärder som avses i 5 kap. 2 § lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter ska innefatta antagande och dokumentation av interna strategier för dataskydd, om det inte är uppenbart obehövligt med hänsyn till verksamhetens begränsade omfattning.

4 § Säkerhetspolisen ska föra en förteckning över de kategorier av behandlingar av personuppgifter som myndigheten ansvarar för.

Förteckningen ska innehålla namnet på och kontaktuppgifter till myndigheten och dataskyddsombud.

Förteckningen ska dessutom, för varje kategori av behandling, innehålla följande uppgifter:

1. den rättsliga grunden för behandlingen,
2. ändamålen med behandlingen,
3. de kategorier av tjänstemän som har tillgång till de personuppgifter som behandlas,
4. de kategorier av mottagare som uppgifterna kan komma att lämnas ut till,
5. de kategorier av registrerade som berörs av behandlingen,
6. de kategorier av personuppgifter som kan komma att behandlas, och
7. om det är möjligt, en allmän beskrivning av vilka säkerhetsåtgärder som har vidtagits.

5 § Skyldigheten att föra loggar i automatiserade behandlingssystem enligt 5 kap. 5 § första stycket lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter ska omfatta
1. inledande behandling av personuppgifter,
2. ändring, läsning, sammanföring och radering av personuppgifter, och
3. utlämning av personuppgifter samt överföring till mottagare utomlands eller internationella organisationer.

Loggarna över läsning och utlämning ska visa datum och tidpunkt för behandlingen och, så långt det är möjligt, vem som har läst eller lämnat ut personuppgifterna och vem som har fått ta del av personuppgifterna.

6 § Loggning enligt 5 kap. 5 § andra stycket lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter ska visa datum och tidpunkt för sökningen, vem som har utfört sökningen och läst personuppgifterna och, så långt det är möjligt, vem som har fått ta del av personuppgifterna.

Tillgången till personuppgifter

7 § Vid tilldelning av behörighet för tillgång till personuppgifter ska, utöver behovet av uppgifterna, utbildning och erfarenhet särskilt beaktas.

8 § Säkerhetspolisen ansvarar för att det inom myndigheten finns rutiner för tilldelning, förändring, borttagning och regelbunden uppföljning av behörighet för tillgången till personuppgifter.

Säkerhetsåtgärder

9 § Säkerhetsåtgärder enligt 5 kap. 7 § lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter ska åstadkomma en skyddsnivå som är lämplig med hänsyn till

1. de tekniska möjligheterna,
2. kostnaderna för åtgärderna,
3. behandlingens art, omfattning, sammanhang och ändamål,
4. de särskilda riskerna med behandlingen,
5. om känsliga personuppgifter behandlas, och
6. hur integritetskänsliga övriga personuppgifter som behandlas är.

Konsekvensbedömningar och förhandssamråd

10 § Konsekvensbedömningar som avses i 5 kap. 8 § lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter ska dokumenteras och innehålla följande uppgifter:

1. en allmän beskrivning av den planerade behandlingen,
2. en bedömning av riskerna för intrång i registrerades personliga integritet,
3. vilka åtgärder som planeras för att hantera riskerna,
4. åtgärder och rutiner för att säkerställa skyddet av personuppgifterna,
5. rutiner för att visa att personuppgifter behandlas författningsenligt, och
6. skälet för att genomföra den planerade behandlingen överväger intrånget i de enskilda eller allmänna intressen som kan påverkas av den.

11 § Vid förhandssamråd enligt 5 kap. 9 § lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter ska Säkerhetspolisen lämna in konsekvensbedömningen till tillsynsmyndigheten och tillhandahålla den övriga information som begärs av myndigheten.

Vid bedömningen av om typen av behandling innebär en sådan risk för intrång i registrerades personliga integritet att förhandssamråd

ska äga rum ska ny teknik, nya rutiner eller nya förfaranden särskilt beaktas.

Anmälan om överträdelser

12 § Säkerhetspolisen ska ha interna rutiner för anmälan av överträdelser av bestämmelser om personuppgiftsbehandling som garanterar att anmälarens identitet skyddas.

Dataskyddsombud

13 § Säkerhetspolisen ska säkerställa att dataskyddsombud ges möjlighet att delta i de frågor som rör skyddet av personuppgifter.

Säkerhetspolisen ska se till att dataskyddsombud kan utföra de uppgifter som anges i 5 kap. 12 § lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter genom att tillhandahålla nödvändiga resurser, ge tillgång till dokumentation om behandling av personuppgifter och vid behov medge åtkomst till personuppgifter som behandlas.

Säkerhetspolisen ska också se till att dataskyddsombud har den sakkunskap som krävs och att de ges möjlighet att upprätthålla denna.

Personuppgiftsbiträden

14 § Ett avtal eller en annan överenskommelse enligt 5 kap. 13 § andra stycket lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter ska ange vad behandlingen av personuppgifter ska avse, hur länge behandlingen ska pågå, dess art och ändamål, typen av personuppgifter, kategorier av registrerade och Säkerhetspolisens skyldigheter och rättigheter.

I avtalet eller överenskommelsen ska det särskilt föreskrivas att personuppgiftsbiträdet ska

1. behandla personuppgifter bara enligt instruktioner från Säkerhetspolisen,

2. säkerställa att personer som har tillstånd att behandla personuppgifter antingen har förbundit sig att iaktta regler om tystnadsplikt eller omfattas av lagstadgad tystnadsplikt,

3. hjälpa Säkerhetspolisen att säkerställa att bestämmelserna om registrerades rättigheter följs,

4. radera eller återlämna alla personuppgifter till Säkerhetspolisen när uppdraget har slutförts och, om inte annat följer av lag eller förordning, radera befintliga kopior,

5. ge Säkerhetspolisen tillgång till den information som krävs för att visa att det som sägs i denna paragraf, 15 § och 5 kap. 13–15 §§ lagen om Säkerhetspolisens behandling av personuppgifter följs, och

6. respektera de villkor som framgår av denna paragraf, 15 § och 5 kap. 14 § lagen om Säkerhetspolisens behandling av personuppgifter när ett annat personuppgiftsbiträde anlitas.

15 § Om Säkerhetspolisen har lämnat ett generellt tillstånd enligt 5 kap. 14 § lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter, ska personuppgiftsbiträdet informera Säkerhetspolisen innan nya personuppgiftsbiträden anlitas.

16 § Varje personuppgiftsbiträde ska föra en förteckning över kategorier av behandlingar av personuppgifter som utförs för Säkerhetspolisens räkning. Förteckningen ska innehålla namnet på och kontaktuppgifter till personuppgiftsbiträdet och Säkerhetspolisen och dessutom, för varje kategori av behandling, följande uppgifter:

1. namnet på och kontaktuppgifter till eventuella underbiträden,

2. vilka uppgifter som har utlämnats och till vem, om utlämning av personuppgifter har gjorts till en mottagare utomlands eller en internationell organisation, och

3. om det är möjligt, en allmän beskrivning av de säkerhetsåtgärder som har vidtagits.

17 § Det som sägs om Säkerhetspolisens skyldigheter i 5,6 och 8 §§ gäller även för personuppgiftsbiträden.

Föreskrifter

18 § Innan Säkerhetspolisen meddelar föreskrifter med stöd av denna förordning, ska tillsynsmyndigheten ges tillfälle att yttra sig i frågor som berör särskilda risker för intrång i den personliga integriteten.

19 § Tillsynsmyndigheten får meddela ytterligare föreskrifter om

1. sådana åtgärder som avses i 5 kap. 2–4 och 7 §§ lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter,

2. krav och rutiner för loggning enligt 5 kap. 5 § lagen om Säkerhetspolisens behandling av personuppgifter, och

3. vilka typer av behandlingar som ska omfattas av förhandssamråd enligt 5 kap. 9 § lagen om Säkerhetspolisens behandling av personuppgifter.

6 kap. Den registrerades rättigheter

1 § Säkerhetspolisen ska göra följande allmänna information tillgänglig för allmänheten:

1. myndighetens identitet och kontaktuppgifter,

2. dataskyddsombudets kontaktuppgifter,

3. för vilka ändamål myndigheten får behandla personuppgifter,

4. rätten till registerutdrag enligt 6 kap. 1 § lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter, och

5. möjligheten att begära kontroll enligt 3 § lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet.

Informationen ska vara lättillgänglig och lättbegriplig och lämnas i lämplig form.

2 § En begäran enligt 6 kap. 2 § lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter ska göras skriftligen hos Säkerhetspolisen.

Säkerhetspolisen ska säkerställa att begäran görs av en behörig person.

3 § Beslut enligt 6 kap. 1 § andra stycket och 2 § första stycket lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter ska vara skriftliga. Beslut som går den registrerade emot ska motiveras om inte annat följer av 6 kap. 2 § andra stycket lagen om Säkerhetspolisens behandling av personuppgifter.

4 § Om den registrerade inte har rätt att ta del av uppgifter utan kostnad enligt 6 kap. 1 § andra stycket lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter ska Säkerhetspolisen tillämpa

11–14 §§ avgiftsförordningen (1992:191). En avgift för att ta del av uppgifter får tas ut med det belopp som anges för avgiftsklass B i 20 § avgiftsförordningen.

7 kap. Tillsyn

1 § Tillsynsmyndigheten ska informera Säkerhets- och integritetsskyddsnämnden om att förhandssamråd enligt 5 kap. 9 § lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter har begärts. Om det är lämpligt ska nämnden ges tillfälle att yttra sig till tillsynsmyndigheten inom ramen för förhandssamrådet.

Säkerhets- och integritetsskyddsnämnden har rätt att få tillgång till underlaget för förhandssamrådet och tillsynsmyndighetens yttrande

---

1. Denna förordning träder i kraft den 1 januari 2027.

2. Genom denna förordning upphävs förordningen (2019:1235) om Säkerhetspolisens behandling av personuppgifter.

3. Förordningen (2019:1235) om Säkerhetspolisens behandling av personuppgifter ska dock tillämpas för behandling av personuppgifter som sker enligt lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter även efter detta datum.

1.13 Förslag till förordning om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar

Härigenom föreskrivs följande.

1 kap. Allmänna bestämmelser

1 § I denna förordning finns kompletterande föreskrifter om sådan behandling av personuppgifter som omfattas av lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar.

2 § Uttryck som används i denna förordning har samma innebörd och tillämpningsområde som i lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar.

Gallring

3 § Uppgifter i särskilda uppgiftssamlingar enligt lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar ska gallras när de inte längre får behandlas enligt den lagen.

2 kap. Registrering av personuppgifter

1 § Säkerhetspolisen ska bestämma vilka tjänstemän som har de särskilda kunskaper och den erfarenhet som krävs enligt 2 kap. 1 § andra stycket lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar.

2 § Säkerhetspolisen ska samråda med den särskilda tillsynsmyndighetens om hur registreringsbeslut enligt 2 kap. 2 § lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar ska utformas.

3 kap. Framtagning och annan personuppgiftsbehandling

1 § Beslut enligt 3 kap. 3 § lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar får fattas av Säkerhetspolischefen eller dennes ställföreträdare.

4 kap. Säkerhetspolisens skyldigheter

1 § Skyldigheten att föra loggar i automatiserade behandlingssystem enligt 5 kap. 5 § första stycket lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter ska omfatta

1. registrering av personuppgifter enligt 2 kap. 1 § lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar,
2. behandling enligt 3 kap. 3 § lagen om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar, och
3. framtagning enligt lagen om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar.

2 § Loggarna över sådan behandling som avses i 1 § 1 ska visa datum och tidpunkt för behandlingen om vem som fattat beslut om registrering.

3 § Loggarna över sådan behandling som avses i 1 § 2 ska visa datum och tidpunkt för behandlingen och vad den avsåg.

4 § Loggarna över sådan behandling som avses i 1 § 3 ska visa datum och tidpunkt för framtagningen, vem som har utfört framtagningen och läst personuppgifterna och, så långt det är möjligt, vem som har fått ta del av personuppgifterna. Det ska även framgå med stöd av vilket tillstånd framtagningen skett.

5 § Om personuppgifter som tagits fram enligt lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar inte får behandlas, på grund av att ett beslut enligt 3 kap. 3 § inte anmälts i tid eller av ett beslut som domstolen meddelat med stöd av 4 kap. 3 § andra stycket i den lagen, ska personuppgifterna omedelbart begränsas enligt 5 kap. 1 § lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter.

Om sådana personuppgifter har lämnats ut ska mottagaren genast underrättas om att uppgifterna inte längre får behandlas.

Den särskilda tillsynsmyndigheten ska underrättas om att personuppgifterna inte längre får behandlas. Om den särskilda tillsynsmyndigheten eller tillsynsmyndigheten inte anser att personuppgifter som begränsats enligt första stycket behöver finnas kvar av bevisskäl ska de raderas.

5 kap. Tillsyn

1 § Radering enligt 5 kap. 1 § lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar ska ske vid den tid som anges i beslutet och på ett sådant sätt att uppgifterna inte kan återskapas.

Denna förordning träder i kraft den 1 januari 2027.

1.14 Förslag till förordning om ändring i förordningen (1995:1301) om handläggning av skadeståndsanspråk mot staten

Härigenom föreskrivs i fråga om förordningen (1995:1301) om handläggning av skadeståndsanspråk mot staten att 3 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

3 §[1]

Justitiekanslern handlägger anspråk på ersättning med stöd av

– 36 kap. 21 § brottsbalken,

– 2 kap. 1 § eller 3 kap. 1, 2 eller 4 § skadeståndslagen (1972:207), om anspråket grundas på ett påstående om felaktigt beslut eller underlåtenhet att meddela beslut,

– 23 § datalagen (1973:289),

– artikel 82 i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) och 7 kap. 1 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning,

– 7 kap. 1 § brottsdatalagen (2018:1177),

– *8* kap. *1* § lagen (*2019:1182*) om Säkerhetspolisens behandling av personuppgifter,	– *6* kap. *3* § lagen (*2026:000*) om Säkerhetspolisens behandling av personuppgifter,

– lagen (1998:714) om ersättning vid frihetsberövanden och andra tvångsåtgärder, dock inte anspråk som avses i 8 § i den lagen,

– 5 kap. 3 § lagen (2017:496) om internationellt polisiärt samarbete, om anspråket grundas på ett påstående om felaktigt beslut eller underlåtenhet att meddela beslut,

– 26 § lagen (2011:111) om förstörande av vissa hälsofarliga missbrukssubstanser,

– 46 kap. 20 § skatteförfarandelagen (2011:1244),

– 28 § kamerabevakningslagen (2018:1200),

– artikel 84 i Europaparlamentets och rådets förordning (EU) 2019/1896 av den 13 november 2019 om den europeiska gräns- och

[1] Senaste lydelse 2024:1024.

kustbevakningen och om upphävande av förordningarna (EU) nr 1052/2013 och (EU) 2016/1624, om anspråket grundas på ett påstående om felaktigt beslut eller underlåtenhet att meddela beslut, eller

– 19 kap. 4 § patentlagen (2024:945).

Justitiekanslern handlägger också andra anspråk på ersättning som grundas på ett påstående om överträdelse av unionsrätten.

Av 4 § följer att vissa anspråk på ersättning med stöd av 3 kap. 1, 2 eller 4 § skadeståndslagen handläggs av Kammarkollegiet.

---

1. Denna förordning träder i kraft den 1 januari 2027.

2. Äldre föreskrifter ska tillämpas för de ärenden som inletts före denna förordning träder i kraft.

1.15 Förslag till förordning om ändring i förordningen (2007:975) med instruktion för Integritetsskyddsmyndigheten

Härigenom föreskrivs i fråga om förordningen (2007:975) med instruktion för Integritetsskyddsmyndigheten att 2 a § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

2 a §[1]

Myndigheten är tillstånds- och tillsynsmyndighet enligt kreditupplysningslagen (1973:1173).

Myndigheten är tillsynsmyndighet enligt

– artikel 51.1 i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning),

– lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning och andra föreskrifter som kompletterar Europaparlamentets och rådets förordning (EU) 2016/679,

– artikel 41.1 i Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF,

– lagen (*2019:1182*) om Säkerhetspolisens behandling av personuppgifter,	– lagen (*2026:000*) om Säkerhetspolisens behandling av personuppgifter,
	– lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar,

– lagen (2021:1171) om behandling av personuppgifter vid Försvarsmakten och lagen (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt, och

[1] Senaste lydelse 2023:726.

– artikel 15.1 i Europaparlamentets och rådets direktiv (EU) 2016/681 av den 27 april 2016 om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet.

Myndigheten ska delta i Europeiska dataskyddsstyrelsens arbete.

---

1. Denna förordning träder i kraft den 1 januari 2027.

2. Äldre föreskrifter ska fortsätta att tillämpas för personuppgifter som behandlas med stöd av övergångsbestämmelserna till lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter.

1.16 Förslag till förordning om ändring i förordningen (2007:1141) med instruktion för Säkerhets- och integritetsskyddsnämnden

Härigenom föreskrivs i fråga om förordningen (2007:1141) med instruktion för Säkerhets- och integritetsskyddsnämnden att 1 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	1 §
Säkerhets- och integritetsskyddsnämnden är en myndighet som ansvarar för de uppgifter som framgår av 1 § lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet och av 2 och 3 §§ denna förordning.	
	Myndigheten ska även fullgöra de uppgifter som följer av lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar.

Denna förordning träder i kraft den 1 januari 2027.

1.17 Förslag till förordning om ändring i offentlighets- och sekretessförordningen (2009:641)

Härigenom föreskrivs i fråga om offentlighets- och sekretessförordningen (2009:641) att 2 och 3 §§ ska ha följande lydelse.

Föreslagen lydelse

2 §[1]

Följande myndigheter är i den utsträckning som framgår nedan undantagna från registreringsskyldigheten enligt 5 kap. 1 § offentlighets- och sekretesslagen (2009:400).

Myndighet	Handlingar som innehåller sekretessreglerade uppgifter och som inte behöver registreras
----------	----------
Säkerhetspolisen	– anteckningar om det löpande polisarbetet, – handlingar som utgör underlag för strukturerade uppgiftssamlingar som avser brottslig verksamhet och som förs med stöd av lagen (*2026:000*) om Säkerhetspolisens behandling av personuppgifter, och – underrättelser från Kriminalvården om permissioner
----------	----------

3 §[2]

Följande myndigheter ska i den utsträckning som framgår nedan inte tillämpa 5 kap. 2 § andra stycket offentlighets- och sekretesslagen (2009:400).

---

[1] Senaste lydelse 2022:652.
[2] Senaste lydelse 2024:1184.

Försvarsunderrättelsedomstolen	diarier över mål om tillstånd enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet *och tillstånd enligt lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar.*
Säkerhets- och integritetsskyddsnämnden	*diarier som rör mål, underrättelser eller yttranden enligt lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar*
Säkerhetspolisen	diarier över underrättelser inom den särskilda polisverksamheten för att hindra och uppdaga brott mot rikets säkerhet m.m. och diarier över ärenden om kvarhållande av försändelse på befordringsanstalt, om föreläggande att bevara en viss lagrad uppgift, om inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet och om hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning och hemlig dataavläsning samt över ärenden enligt lagen (2024:1180) om anonyma vittnen i brottmål, *diarier över beslut, ansökningar, yttranden eller underrättelser enligt lagen (2026:000) om Säkerhetspolisens*

behandling av personuppgifter i särskilda uppgiftssamlingar.

Denna förordning träder i kraft den 1 januari 2027.

1.18 Förslag till förordning om ändring i förordningen (2009:968) med instruktion för Försvarsunderrättelsedomstolen

Härigenom föreskrivs i fråga om förordningen (2009:968) med instruktion för Försvarsunderrättelsedomstolen

dels att 2,4 9, 11, 12, § ska ha följande lydelse,

dels att en ny paragraf 6 a ska införas av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
2 §	
Följande bestämmelser i myndighetsförordningen (2007:515) ska tillämpas på Försvarsunderrättelsedomstolen:	
3 och 4 §§ om ledningens ansvar,	
6 § om allmänna uppgifter,	
8 § om myndighetens arbetsgivarpolitik,	
19 § om kostnadsmässiga konsekvenser, och	
21 § om myndighetens beslut.	
Det som i dessa bestämmelser sägs om myndighetens ledning ska avse domstolens ordförande i enlighet med bestämmelsen i 11 §. Bestämmelsen i 21 § myndighetsförordningen ska tillämpas endast i administrativa ärenden.	Det som i dessa bestämmelser sägs om myndighetens ledning ska avse domstolens ordförande, *tillika chef*, i enlighet med bestämmelsen i 11 §. Bestämmelsen i 21 § myndighetsförordningen ska tillämpas endast i administrativa ärenden.
4 §	
I Försvarsunderrättelsedomstolen ska, förutom ordförande, vice ordförande och de särskilda ledamöter som anges i lagen (2009:966) om Försvarsunderrättelsedomstol, en kanslichef finnas.	
Försvarsunderrättelsedomstolens ordförande är domstolens administrative chef.	Försvarsunderrättelsedomstolens ordförande, *tillika chef*, är domstolens administrative chef
Kanslichefen ska ansvara för beredningsverksamheten i domstolen.	

	6 a §
	Bestämmelser om handläggningen av ansökningar om tillstånd till framtagning av uppgifter från särskilda uppgiftssamlingar finns i lagen (2026:000) Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar.
9 §	
Domstolens beslut ska expedieras till ansökande myndighet och till Statens inspektion för försvarsunderrättelseverksamheten.	Domstolens beslut *om signalspaning* ska expedieras till ansökande myndighet och till Statens inspektion för försvarsunderrättelseverksamheten. *Domstolens domar och beslut om framtagning från en särskild uppgiftssamling ska expedieras till Säkerhetspolisen och till Säkerhets- och integritetsskyddsnämnden.*
11 §	
Administrativa ärenden avgörs av domstolens *ordförande* om inte annat följer av arbetsordningen.	Administrativa ärenden avgörs av domstolens *chef* om inte annat följer av arbetsordningen.
12 §[1]	
Bestämmelser om utnämning av ordförande i Försvarsunderrättelsedomstolen finns i lagen (2010:1390) om utnämning av ordinarie domare. Bestämmelser om förordnande av vice ordförande och särskilda ledamöter finns i lagen (2009:966) om Försvarsunderrättelsedomstol.	Bestämmelser om utnämning av ordförande, *tillika chef*, *och andra ordförande* i Försvarsunderrättelsedomstolen finns i lagen (2010:1390) om utnämning av ordinarie domare. Bestämmelser om förordnande av vice ordförande och särskilda ledamöter finns i lagen (2009:966) om Försvarsunderrättelsedomstol.

[1] Senaste lydelse 2010:1811.

Försvarsunderrättelsedomstolen ska anmäla till Domarnämnden när det finns en ledig anställning som ordförande som behöver tillsättas.

Anställningen som kanslichef beslutas av regeringen. Kanslichefen ska vara lagfaren. Andra anställningar beslutas av Försvarsunderrättelsedomstolen.

För andra anställningar vid domstolen än anställning av ordförande behöver inte 6 § anställningsförordningen (1994:373) tillämpas.

Denna förordning träder i kraft den 1 januari 2027.

1.19 Förslag till förordning om ändring i utlänningsdataförordningen (2016:30)

Härigenom föreskrivs i fråga om utlänningsdataförordning (2016:30) att 11 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	11 §[1]
Säkerhetspolisens direktåtkomst ska begränsas till de personuppgifter som myndigheten behöver för att fullgöra sådana uppgifter som avses i 2 kap. *1 § 1 a* och b, 2, 3 a *och c och 4* lagen *(2019:1182)* om Säkerhetspolisens behandling av personuppgifter. Direktåtkomsten för att fullgöra uppgifterna i 2 kap. *1 § 2* lagen om Säkerhetspolisens behandling av personuppgifter gäller enbart *sådana brott som avses i 2 kap. 1 § 1 a och b samma lag.*	Säkerhetspolisens direktåtkomst ska begränsas till de personuppgifter som myndigheten behöver för att fullgöra sådana uppgifter som avses i 2 kap. *4–6 §§ lagen (2026:000)* om Säkerhetspolisens behandling av personuppgifter. Direktåtkomsten för att fullgöra uppgifterna i 2 kap. *5 §* lagen om Säkerhetspolisens behandling av personuppgifter gäller enbart *för att utreda brott mot Sveriges säkerhet eller terrorbrott.*

Denna förordning träder i kraft den 1 januari 2027.

[1] Senaste lydelse 2020:326.

1.20 Förslag till förordning om ändring i förordningen (2023:363) om samordningsnummer

Härigenom föreskrivs i fråga om förordningen (2023:363) om samordningsnummer att 5 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
5 §	
Samordningsnummer enligt 2 kap. 6 § lagen (2022:1697) om samordningsnummer får endast tilldelas för	
1. registrering i register som förs enligt lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister och lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område,	
2. annan behandling av uppgifter enligt lagen om polisens behandling av personuppgifter inom brottsdatalagens område eller lagen *(2019:1182)* om Säkerhetspolisens behandling av personuppgifter, eller i övrigt inom rättsväsendets informationssystem,	2. annan behandling av uppgifter enligt lagen om polisens behandling av personuppgifter inom brottsdatalagens område eller lagen (*2026:000*) om Säkerhetspolisens behandling av personuppgifter, eller i övrigt inom rättsväsendets informationssystem,
3. Migrationsverkets behandling av personuppgifter med stöd av utlänningsdatalagen (2016:27) när det gäller personer som omfattas av lagen (1994:137) om mottagande av asylsökande m.fl.,	
4. registrering i beskattningsdatabasen, eller	
5. Försäkringskassans behandling av personuppgifter med stöd av 114 kap. socialförsäkringsbalken.	

Denna förordning träder i kraft den 1 januari 2027.

2 Utredningens uppdrag och arbete

2.1 Utredningsuppdraget

Utredningens direktiv beslutades av regeringen den 11 maj 2023 (dir. 2023:64). Direktiven i dess helhet finns fogade till betänkandet som bilaga 1.

Enligt direktiven är vår huvudsakliga uppgift att göra en översyn av de bestämmelser som reglerar Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet. Syftet är att skapa ändamålsenliga regler som är anpassade efter dagens behov och möjligheter. Reglerna bör som utgångspunkt ge Säkerhetspolisen ökade möjligheter att behandla personuppgifter, särskilt vad gäller att samla in, sortera, lagra, bearbeta och analysera information med hjälp av tekniska hjälpmedel.

I direktiven anges att utredaren noga ska väga myndigheternas behov av att behandla personuppgifter mot den enskildes rätt till skydd för sin personliga integritet. I uppdraget ingår att lämna nödvändiga författningsförslag.

Inom ramen för en översyn av regleringen ska utredaren bland annat

- beskriva dagens rättsliga möjligheter för Säkerhetspolisen att behandla personuppgifter, särskilt vad gäller att samla in, sortera, lagra, bearbeta och analysera information med hjälp av tekniska hjälpmedel,
- undersöka i vilken utsträckning dagens regelverk försvårar en effektiv informationshantering i Säkerhetspolisens verksamhet,
- lämna förslag som gör att information kan hanteras av Säkerhetspolisen på ett mer ändamålsenligt sätt än i dag, och
- lämna nödvändiga författningsförslag.

2.2 Uppdragets genomförande

Vi har antagit namnet Utredningen om Säkerhetspolisens informationshantering. Arbetet har bedrivits på sedvanligt sätt och vi har haft 15 utredningssammanträden med expertgruppen, varav två sammanträden har genomförts i internatform med två mötesdagar. Vid internaten har vi bland annat genomfört rättegångsspel för att testa den föreslagna prövningsordningen i den nya lagen om hantering av stora informationsmängder.

Utöver expertgruppens sammanträden har utredningen haft enskilda möten och samrått med flera myndigheter och andra aktörer. Vi har på detta sätt haft kontakt med bland annat:

- Försvarsmakten (MUST),
- Försvarets radioanstalt,
- Försvarsunderrättelsedomstolen,
- Myndigheten för psykologiskt försvar,
- Regeringskansliet,
- Polismyndigheten,
- Integritetsskyddsmyndigheten,
- Säkerhetspolisen,
- Riksenheten för Säkerhetsmål,
- Säkerhets- och integritetsskyddsnämnden (SIN),
- Statens inspektion för försvarsunderrättelseverksamheten (Siun),
- Förvaltningsrätten i Stockholm och
- Kammarrätten i Stockholm.

Vi har även samrått med Underrättelseutredningen (Fö 2023:04) samt Utredningen om Förbättrade möjligheter att skydda Sveriges säkerhet (Ju 2023:23).

Utredningen har i samarbete med Juridiska institutionen och Centrum för Transdisciplinär AI (TAIGA) vid Umeå Universitet, arrangerat ett forskningsseminarium om dataskydd, AI och demo-

krati den 5 december 2023. Vid seminariet medverkade forskare och praktiker från flera nordiska länder.

I januari 2025 höll utredningen ett så kallat minilagråd, där bland annat professor Markus Naarttijärvi och ställföreträdande chefsrådmannen Mattias Nordell deltog. Syftet med minilagrådet var att granska lagförslagen från mer lagtekniska utgångspunkter.

2.3 Betänkandets disposition

Betänkandet är indelat i tretton kapitel. I kapitel 1 finns våra författningsförslag. Vårt uppdrag och arbete redovisas i kapitel 2 (detta kapitel). Därefter följer kapitel 3 som innehåller en allmän bakgrund med beskrivning av Säkerhetspolisens uppdrag, den nuvarande säpodatalagen samt en översiktlig redogörelse för relevanta delar av Försvarsmaktens underrättelsetjänst, Försvarets radioanstalt och Polismyndigheten.

I kapitel 4 redogörs för internationella förhållanden. Där redogörs helt kortfattat regelverken i vissa andra länder som kan tjäna som jämförelse vid vår översyn. Vidare beskrivs helt översiktligt Europarådets dataskyddskonvention, som är det internationella instrument som är av störst betydelse i sammanhanget.

Kapitel 5 innehåller en beskrivning av de aktuella hoten mot Sveriges säkerhet medan de reformbehov som vi identifierat beskrivs i kapitel 6. Kapitel 7 redogör för inriktningen för den reform vi föreslår.

Våra materiella överväganden och förslag presenteras i kapitel 8–10. Kapitel 8 innehåller förslag till en ny lag om Säkerhetspolisens behandling av personuppgifter, kapitel 9 beskriver en ny lag för behandling av stora informationsmängder och kapitel 10 behandlar tillsynsfrågor.

Ikraftträdande och övergångsbestämmelser behandlas i kapitel 11, och konsekvenserna av utredningens förslag gås igenom i kapitel 12. Slutligen innehåller kapitel 13 författningskommentaren till våra lagförslag.

3 Bakgrund

3.1 Inledning

I detta kapitel av betänkandet försöker vi teckna en allmän bakgrund till de rättsfrågor som omfattas av vår översyn. Det innebär att vi först redogör för Säkerhetspolisen och hur myndighetens uppdrag är reglerat. Vi kommer därutöver att försöka ge en översiktlig överblick av Säkerhetspolisens verksamhet. Vi kommer att återkomma till verksamhetens behov av ny lagstiftning i kapitel 6 och 7.

Vi kommer även att redogöra för det regelverk som vår översyn i huvudsak avser: Lag (2019:1182) om Säkerhetspolisens behandling av personuppgifter. Trots att vi har till uppdrag att bland annat beskriva dagens rättsliga möjligheter för Säkerhetspolisen att behandla personuppgifter kommer redogörelsen att hållas förhållandevis kort i detta kapitel. Vi har nämligen för avsikt att redogöra för gällande rätt i närmare detalj i samband med att vi analyserar behovet av att förändra enskilda bestämmelser och lämnar våra förslag. Detta görs i huvudsak i kapitel 8.

Vårt direktiv har som utgångspunkt att Säkerhetspolisens uppdrag som nationell säkerhetstjänst ger goda skäl för att myndigheten bör ha ett mer generöst regelverk kring personuppgiftsbehandlingen än många andra myndigheter. Vi har därmed haft skäl att undersöka hur några andra, till sin verksamhet närliggande, myndigheters personuppgiftsbehandling reglerats. Vi redogör kortfattat för vår undersökning i slutet av detta kapitel. Vi har begränsat undersökningen till Polismyndigheten, Försvarsmakten och Försvarets radioanstalt, som alla ägnar sig åt underrättelseverksamhet i någon form.

3.2 Säkerhetspolisens uppdrag

3.2.1 Rättslig reglering av Säkerhetspolisens uppgifter

Säkerhetspolisens huvudsakliga uppgifter och ansvar framgår av 3 § polislagen. Där framgår att Säkerhetspolisen ska

1. förebygga, förhindra och upptäcka brottslig verksamhet som innefattar brott mot rikets säkerhet eller terrorbrott,
2. utreda och beivra sådana brott,
3. fullgöra uppgifter i samband med personskydd av den centrala statsledningen och andra som regeringen eller Säkerhetspolisen bestämmer,
4. fullgöra uppgifter enligt säkerhetsskyddslagen (2018:585),
5. leda annan polisverksamhet om regeringen föreskriver det och i övrigt bedriva sådan verksamhet som framgår av lag eller förordning eller som regeringen uppdragit åt Säkerhetspolisen att i särskilda hänseenden ansvara för.

Sådan övrig verksamhet som avses i den femte punkten framgår av polisförordningen (2014:1104), förordningen (2022:1719) med instruktion för Säkerhetspolisen, andra författningar och särskilda beslut. Enligt utlänningslagen (2005:716) kan Säkerhetspolisen av skäl som rör Sveriges säkerhet eller som annars har betydelse för allmän säkerhet förorda att vissa beslut ska meddelas. Det kan exempelvis handla om att en utlänning ska avvisas eller utvisas eller att en utlännings ansökan om uppehållstillstånd ska avslås. Säkerhetspolisen utför även uppgifter enligt lagen (2022:700) om särskild kontroll av vissa utlänningar. Med stöd av den lagen kan myndigheten ansöka om att en utlänning ska utvisas ur landet om utlänningen kan antas komma att begå eller på annat sätt medverka till ett brott enligt terroristbrottslagen, eller kan utgöra ett allvarligt hot mot Sveriges säkerhet. Enligt lagen (2001:82) om svenskt medborgarskap kan Säkerhetspolisen förorda att en ansökan om svenskt medborgarskap ska avslås av skäl som rör Sveriges säkerhet eller allmän säkerhet.

Säkerhetspolisen arbetar även med frågor som rör icke-spridning och kontraanskaffning. Den verksamheten syftar till att för-

hindra spridning och anskaffning av produkter som kan användas för att producera massförstörelsevapen. Arbetet går främst ut på att förhindra att kunskaper, produkter, ämnen eller mikroorganismer förs från eller via Sverige till aktörer som har ambitioner att anskaffa eller vidareutveckla massförstörelsevapen.

Säkerhetspolisen är vidare tillsammans med Försvarsmakten samrådsmyndighet inför att Post- och telestyrelsen beviljar tillstånd att använda radiosändare enligt lagen (2022:482) respektive förordningen (2022:511) om elektronisk kommunikation. Samrådet syftar till att klarlägga om radioanvändningen kan antas orsaka skada för Sveriges säkerhet, eftersom tillstånd i sådana fall inte ska beviljas. Det är Säkerhetspolisen och Försvarsmakten som tillsammans har en helhetsbild när det gäller säkerhetsläget och hotbilden mot Sverige och har tillgång till de uppgifter som behövs för att bedöma om radioanvändning kan antas orsaka skada för Sveriges säkerhet.

Säkerhetspolisen har även uppdrag enligt lagen (2023:560) respektive förordningen (2023:624) om granskning av utländska direktinvesteringar. Säkerhetspolisen har möjlighet att yttra sig över utländska direktinvesteringar som sker i skyddsvärd verksamhet. Om Säkerhetspolisen anser att en utländsk direktinvestering kan innebära skadlig inverkan på säkerheten i Sverige, kan myndigheten meddela detta till Inspektionen för strategiska produkter. Av 2 § 3 Säkerhetspolisens instruktion följer att myndigheten ska följa händelseutvecklingen i omvärlden och ha förmåga att snabbt anpassa inriktningen av verksamheten när det behövs. Säkerhetspolisen ska även snarast möjligt informera Regeringskansliet om underrättelser som kan ha betydelse för Sveriges säkerhet eller som av någon annan anledning bör komma till regeringens kännedom.

Utöver dessa författningsreglerade uppgifter ger regeringen varje år Säkerhetspolisen andra uppdrag genom regleringsbrevet och särskilda regeringsbeslut. Säkerhetspolisen samverkar också med andra svenska och utländska myndigheter inom en mängd områden.

3.2.2 Förebygga, förhindra och upptäcka brottslig verksamhet som innefattar brott mot rikets säkerhet eller terrorbrott

Av polislagen följer att en av Säkerhetspolisens uppgifter är att *förebygga, förhindra och upptäcka* brottslig verksamhet som innefattar brott mot rikets säkerhet eller terrorbrott. Denna del av myndighetens uppdrag utgör kärnverksamheten och är definierande för Säkerhetspolisens uppdrag som nationell säkerhetstjänst. Uppdraget kommer även till uttryck genom de mer specifika uppgifterna att fullgöra uppgifter i samband med personskydd av den centrala statsledningen och att fullgöra uppgifter enligt säkerhetsskyddslagen, ytterst för att skydda säkerhetskänslig verksamhet mot spioneri, sabotage, terroristbrott och andra verksamhetshotande brott.

Uppdraget för en nationell säkerhetstjänst är att skydda landets säkerhet mot säkerhetshotande verksamhet som bedrivs inom landets gränser. Sådan säkerhetshotande verksamhet utgör ofta ett brott, till exempel spioneri, sabotage eller terroristbrott, eller ett förstadium till ett sådant brott. I Säkerhetspolisens instruktion förtydligas myndighetens uppdrag som nationell säkerhetstjänst. Enligt 1 § i instruktionen ska Säkerhetspolisen, i egenskap av säkerhetstjänst, bedriva underrättelse- och säkerhetsarbete.

Kärnan i säkerhets- och underrättelsearbetet är att upptäcka och reducera hot och sårbarheter. Säkerhetspolisens verksamhet som syftar till att upptäcka och reducera hot bedrivs framför allt inom verksamhetsområdena kontraspionage, kontraterrorism och författningsskydd. Reduktion av ett hot kan ske på många olika sätt där frihetsberövande och lagföring inom ramen för en förundersökning är ett sätt. Andra sätt som står till myndighetens förfogande är att initiera en utvisning av en utlänning som bedöms utgöra ett säkerhetshot eller påtala för regeringen att underrättelseofficerare som arbetar under diplomatisk täckmantel bör förklaras *persona non grata*. Säkerhetspolisen arbetar även proaktivt för att minska extremistmiljöerna i Sverige. Så sker till exempel genom så kallad outreach-verksamhet, som innebär att Säkerhetspolisen informerar och kontaktar personer som exempelvis riskerar radikalisering, eller genom yttranden till andra myndigheter inom ramen för bland annat utlänningslagstiftningen eller de olika regelverken om statsstöd.

Säkerhetspolisens verksamhet som syftar till att upptäcka och reducera sårbarheter bedrivs framför allt inom verksamhetsområdena säkerhetsskydd och personskydd.

3.2.3 Utreda och beivra sådana brott

Säkerhetspolisens nationella uppdrag som polismyndighet framgår av 1 § andra stycket polislagen. Där anges att polisverksamhet bedrivs av Polismyndigheten och Säkerhetspolisen. Av 3 § i samma lag framgår att till Säkerhetspolisens uppgifter hör att *utreda och beivra* brott mot rikets säkerhet eller terrorbrott samt att utreda andra brott och leda annan polisverksamhet om regeringen särskilt föreskriver det.

Dessa uppgifter utgör den brottsutredande och lagförande verksamheten som Säkerhetspolisen bedriver utöver säkerhetsunderrättelseverksamhet. På så sätt skiljer sig myndighetens uppgifter i en internationell jämförelse med många andra säkerhetstjänsters.

Det brottsutredande uppdraget preciseras i Säkerhetspolisens instruktion. De särskilda brottskategorier som Säkerhetspolisen ansvarar att utreda och beivra framgår av 3 § i instruktionen och utgörs bland annat av brott mot 18 eller 19 kap. brottsbalken samt brott enligt terroristbrottslagen och allmänfarliga brott, såsom sabotage eller allmänfarlig ödeläggelse om syftet är att framkalla fara för Sveriges säkerhet.

3.2.4 Särskilt allvarlig brottslighet med konsekvenser för nationell säkerhet

Säkerhetspolisens verksamhet knyter an till att myndigheten är en säkerhetstjänst med uppdrag att skydda Sveriges grundläggande demokratiska funktioner och den nationella säkerheten. Polismyndighetens uppdrag är inte detsamma. Huvudinriktningen för Polismyndigheten är att minska brottsligheten och att öka människors trygghet. Säkerhetspolisen, i sin egenskap av nationell säkerhetstjänst, intar därför en särställning inom polisväsendet med ett uppdrag som är tydligt skiljt från Polismyndigheten.[1]

[1] SOU 2012:77 *En tydligare organisation för Säkerhetspolisen*, s. 116.

Kärnan i Säkerhetspolisens verksamhet är att som säkerhetstjänst skydda Sveriges säkerhet och det svenska statsskicket mot säkerhetshotande verksamhet. Den brottslighet som Säkerhetspolisen har till uppgift att förebygga och avslöja utmärks av att den kan få mycket stora konsekvenser för samhället och för enskilda individer. Tyngdpunkten i uppdraget är därför att förebygga brott och syftet med verksamheten är följaktligen att förhindra att brott överhuvudtaget begås. Det brottsförebyggande arbetet har därför, framför allt historiskt, spelat en större roll i Säkerhetspolisens arbete än vid annat polisarbete; för myndigheten gäller det att avslöja en spion eller en terrorist innan något brott ens har begåtts.[2]

En annan skillnad i förhållande till övrig polisverksamhet är att Säkerhetspolisen arbetar med brott som till sin natur är svåra – ofta mycket svåra – att bekämpa. En spion lämnar sällan spår efter sig och inte heller föranleder dennes förehavanden vanligtvis några anmälningar eller uppslag från allmänheten, som polisarbetet kan utgå från. En stor del av Säkerhetspolisens arbete går därför ut på att ta reda på om brott över huvud taget har begåtts, och brottsutredningar i vanlig mening utgör således av en mindre del av i myndighetens verksamhet. I stället är myndighetens arbete till stor del inriktat på att kartlägga personer och miljöer med anknytning till brottslighet av den typ som Säkerhetspolisen ska bekämpa. Underrättelseverksamheten inriktas främst mot personer eller organisationer som det finns anledning att hålla under uppsikt i syfte att förhindra och lagföra terrordåd och brott mot rikets säkerhet. Det säger sig självt att det är svårt att få inblick i miljöer där sådan verksamhet förekommer. Såväl spionerи som terrorism bedrivs med nödvändighet i det fördolda och över huvud taget i former som till sin natur är slutna.[3]

Till skillnad från Polismyndighetens verksamhet initieras Säkerhetspolisens ärenden endast undantagsvis genom allmänhetens anmälningar om brott. Det i sig förutsätter att Säkerhetspolisen själv har förmåga att identifiera och att hämta in uppgifter om brottslig verksamhet. Uppdraget kräver att Säkerhetspolisen kan hämta in uppgifter på ett mycket tidigt stadium, innan en person eller en gruppering har konkreta planer eller har vidtagit åtgärder för att begå brott. Säkerhetspolisen bedriver därför omfattande säkerhets-

[2] SOU 1990:51 *Säkerhetspolisens arbetsmetoder, personalkontroll och meddelarfrihet*, s. 65.
[3] Ibid. s. 65.

underrättelseverksamhet för att ta fram hot- och sårbarhetsbedömningar. Dessa bedömningar tjänar som underlag för beslut om vilka åtgärder Säkerhetspolisen ska vidta i sitt förebyggande arbete. Bedömningarna ligger också till grund för beslut om till exempel personskydd eller säkerhetsskyddsåtgärder och tjänar också som underlag för regeringen och andra myndigheters bedömningar och åtgärder.[4]

3.3 Säkerhetspolisens verksamhet och arbetsmetoder

3.3.1 Säkerhetspolisens verksamhetsområden

Säkerhetspolisens kärnverksamhet är indelad i fem huvudsakliga verksamhetsområden: kontraspionage, kontraterrorism, författningsskydd, personskydd och säkerhetsskydd. Den största delen av Säkerhetspolisens verksamhet utgörs av säkerhetsunderrättelsearbetet inom verksamhetsområdena kontraspionage, kontraterrorism och författningsskydd. Verksamheten innebär att Säkerhetspolisen aktivt inhämtar uppgifter för att analysera och agera mot olika typer av säkerhetshotande verksamhet.

Kontraspionage

Säkerhetspolisens kontraspionageverksamhet syftar till att förebygga, förhindra och upptäcka säkerhetshotande verksamhet från främmande makt mot Sverige och svenska intressen utomlands samt att utreda och beivra brott mot Sveriges säkerhet från främmande makt. Hotet från främmande makt i Sverige riktas mot Sveriges ekonomiska välstånd och oberoende, mot den politiska och territoriella suveräniteten samt mot medborgarnas grundläggande fri- och rättigheter.

Den brottsliga verksamhet som kontraspionaget främst bekämpar består bland annat av de olika spioneribrotten, andra brott som innefattar otillåten hantering av hemliga uppgifter samt olika former av olovlig underrättelseverksamhet i 19 kap. brottsbalken.

Den övergripande strategin för kontraspionaget är att begränsa främmande makts handlingsutrymme, det vill säga förebygga och

[4] Se SOU 2012:77 *En tydligare organisation för Säkerhetspolisen*, s. 56.

förhindra främmande makts möjligheter att bedriva antagonistisk verksamhet dolt och förnekbart i Sverige. Det kan handla om att förhindra att individer som kan bli ett säkerhetshot uppehåller sig i Sverige eller att de får tillgång till skyddsvärd information. Det kan även inkludera åtgärder för att informera om hotbilden i syfte att skapa en vaksamhet och en motståndskraft mot hotet. En god lägesuppfattning om säkerhetshotande verksamhet från främmande makt är en förutsättning för att kunna göra tillförlitliga bedömningar och genomföra hotreducerande åtgärder för att begränsa handlingsutrymmet.

Kontraspionage omfattar inhämtning av underrättelser om och bedömning av andra staters spionage och annan säkerhetshotande verksamhet mot Sverige. Sådant underrättelsearbete skapar underlag för olika typer av åtgärder mot andra staters säkerhetshotande underrättelseverksamhet och är en del av Sveriges försvar. Det arbete som kontraspionaget bedriver för att reducera hotet från främmande makt är centralt även utifrån ett totalförsvarsperspektiv. Det nya totalförsvaret i Sverige är under uppbyggnad och både det civila och det militära försvaret är beroende av civila verksamheter och infrastruktur för att fungera. Främmande makts mål finns inte bara i Sverige utan även utomlands, exempelvis personal på ambassader, konsulat och vid svenska representationer inom organ som EU och FN. Det svenska Nato-medlemskapet medför anpassningar avseende vad det innebär att vara en del av en allians och främmande makts mål.

Verksamheten inom kontraspionage planeras utifrån en allvarlig hotbild från främmande makt, där Ryssland, Kina och Iran fortsatt är de stater som bedriver säkerhetshotande verksamhet med mest allvarliga konsekvenser för Sveriges säkerhet. Dessa staters säkerhetshotande verksamhet inbegriper bland annat underrättelseinhämtning riktad mot säkerhetskänslig verksamhet eller svenskt näringsliv, påverkan riktad mot den svenska regeringen, teknik- och kunskapsanskaffning, cyberangrepp och i vissa fall även attentatsplanering mot mål i Sverige.

För att kunna bedriva underrättelseverksamhet i Sverige använder främmande makt underrättelseofficerare under diplomatisk täckmantel eller inresande som i sin tur nyttjar agenter med tillgång till den information och miljöer som främmande makt har ett intresse av. Underrättelsearbete bedrivs med utgångspunkt från ambassader

och från dolda plattformar. Främmande makt använder även i högre utsträckning ombud, det vill säga andra aktörer i syfte att kunna agera dolt och förnekbart.

Kontraspionage kräver ett långsiktigt underrättelsearbete och ett fokus på nya arenor för säkerhetshotande verksamhet som rymdsektorn och Arktis. Säkerhetspolisens inriktning är att bygga säkerhet tillsammans med och genom andra. Detta avspeglas inom kontraspionaget både genom en mycket nära samverkan nationellt med huvudsakligen försvarsunderrättelsemyndigheterna och med internationella partners.

Under de senaste decennierna har teknikutveckling kommit att utgöra en central dimension av staters säkerhetspolitiska målsättningar med stor betydelse för militär förmågeuppbyggnad. Statliga aktörers intresse har ökat för anskaffning av forskning och teknik inom olika strategiskt framväxande teknikområden samt för kunskap, teknik och materiel för användning inom konventionell militärindustri. Icke-spridning innebär att förebygga och förhindra spridning av kunskap, produkter och teknologier som kan användas för att utveckla massförstörelsevapen. Säkerhetspolisen har regelbundet utbyte med utländska underrättelsetjänster, samverkande nationella myndigheter och företag i syfte att förhindra olovlig anskaffning av produkter och teknisk kunskap som kan användas i andra länders massförstörelsevapen eller för säkerhetshotande syften i övrigt.

Främmande makt använder i ökad utsträckning ekonomiska instrument för att nå säkerhetspolitiska målsättningar, exempelvis genom handelshinder eller strategiska investeringar eller uppköp. I syfte att förhindra uppköp av säkerhetskänslig verksamhet finns lagen om utländska direktinvesteringar enligt vilken Säkerhetspolisen utgör så kallad samverkansmyndighet. Skadliga utländska direktinvesteringar kan bland annat innebära ett beroendeförhållande för Sverige när det gäller viktiga varor eller tjänster, inflytande över svenskt beslutsfattande eller stärkandet av främmande makts militära förmåga.

Främmande makt utför cyberangrepp mot säkerhetskänsliga verksamheter, företag och enskilda privatpersoner för att få tillgång till information och it-system över hela världen. För att genomföra angrepp använder aktörerna cyberinfrastruktur som även återfinns i Sverige. För att förbättra möjligheterna att i ett tidigt skede upptäcka

cyberangrepp mot svenska skyddsvärden har Säkerhetspolisen en omfattande nationell samverkan med myndigheter, organisationer och företag som utgör potentiella mål för främmande makt. Internationell samverkan är även en förutsättning för att på cyberområdet få del av kunskap om aktörer och information om angrepp mot Sverige. Cyberangrepp begränsas sällan till endast ett land. Säkerhetspolisen deltar därför i ett antal multilaterala samarbetsfora för att dela information om pågående och genomförda cyberangrepp.

Kontraterrorism

Säkerhetspolisen ansvarar för att förebygga, förhindra, upptäcka, utreda och lagföra brott enligt terroristbrottslagen. Säkerhetspolisens uppdrag inom ramen för kontraterrorism bedrivs såväl kort- som långsiktigt. Arbetet inom kontraterrorism handlar främst om att förhindra att terrorattentat eller annan terrorrelaterad brottslighet inträffar. Det förebyggande arbetet är mycket viktigt för att på sikt minska terrorhotet.

Att förhindra terroristbrott handlar om att ligga steget före, både i det kortsiktiga arbetet med att upptäcka och avvärja terrorhot här och nu, och i det långsiktiga arbetet med att bryta tillväxten i de våldsbejakande extremistmiljöerna. Underrättelsearbetet med innefattande analysverksamhet är därför central. Säkerhetspolisen måste få in relevant information för att kunna vidta åtgärder för att bryta tillväxten till och begränsa handlingsutrymmet i extremistiska miljöer.

Terrorbrott riktar sig mot mer än det enskilda brottsoffret och för att en gärning ska anses utgöra ett terroristbrott krävs att gärningen allvarligt kan skada ett land eller en mellanstatlig organisation. Brotten utförs av individer som av olika anledningar anser sig ha rätt att bruka våld för att ändra eller destabilisera samhället. Terrorbrott kan vara religiöst eller på annat sätt ideologiskt motiverade.

Såväl hotbilden som de våldsbejakande extremistmiljöerna är komplexa. Inom varje extremistmiljö finns individer, grupper, nätverk och organisationer med olika motiv och bevekelsegrunder för sina åsikter och sitt agerande. I dag är det ofta över internet som aktiviteten inom dessa miljöer sker, oavsett om det handlar om rekrytering, radikalisering, gemenskaper, motiv eller ökad förmåga.

Tillsammans med att internet också erbjuder en rad olika världsbilder och förenklade förklaringar till det som upplevs vara ”fel” i samhället, innebär detta att det finns en stor mängd potentiella mål som våldsbejakande extremister skulle kunna agera mot.

Dessutom tycks gränsen mellan den våldsbejakande och den icke våldsbejakande extremismen bli alltmer diffus, vilket bland annat innebär att de som enbart uttrycker åsikter också direkt eller indirekt påverkar de våldsbejakande delarna av extremismen. Säkerhetspolisen gör löpande bedömningar av de olika våldsbejakande extremistmiljöerna och olika företeelser som kan påverka hotbilden. Målet är att på kort sikt förhindra terroristattentat och andra grova våldsbrott och på lång sikt minska miljöernas tillväxt, handlingsutrymme och förmåga att underblåsa hotet mot Sverige.

Utmaningen för Säkerhetspolisen är att upptäcka och bedöma de individer som kan utgöra ett hot. Det vill säga de som agerar helt på egen hand, de som inspireras av andra eller de som blir styrda och agerar i en terrororganisations namn. Det är inte nödvändigtvis de som tillhör en specifik organisation som är mest benägna att begå brott. Det kan också vara ensamagerande som, till exempel utifrån en virtuell gemenskap och ett narrativ som både formar hat och försvarar användandet av våld, agerar för att förändra samhällsordningen. Uppmaningen och plikten att ”göra vad du kan, med de medel du har, där du är nu” förmedlas på flera olika sätt och avser såväl attentat och grova våldsbrott som aktiviteter som syftar till att polarisera, underblåsa och hetsa fram en samhällskollaps eller destabilisera det demokratiska systemet.

Författningsskydd

Inom författningsskyddet bedrivs den verksamhet som arbetar för att motverka aktörer som med hot, våld och tvång försöker påverka det demokratiska statsskickets grundläggande funktioner. Verksamheten syftar bland annat till att motverka påverkan på det centrala beslutsfattandet eller verkställandet av nationella beslut.

Säkerhetspolisens uppdrag gällande författningsskyddet är nära kopplat till arbetet med kontraterrorism, då aktörerna som ägnar sig åt författningshotande verksamhet ofta drivs av ideologiska eller religiösa skäl. Även främmande makt kan vara involverad i verksam-

het som syftar till att försvaga eller destabilisera det svenska demokratiska statsskicket, vilket innebär att verksamheten inom författningsskyddet delvis överlappar kontraspionaget. Den författningshotande brottsligheten kan rikta sig mot olika aktörer i samhället. Arbetet med författningsskydd behöver därför ske långsiktigt och i nära samarbete med andra samhällsfunktioner.

Personskydd

Personskyddsverksamheten utgörs av den del av Säkerhetspolisens uppdrag som innebär bevaknings- och säkerhetsarbete för den centrala statsledningen, främmande stats beskickningsmedlemmar samt vid statsbesök och liknande händelser.

Personskyddet består av många olika delar för att höja säkerheten, där den yttersta skyddsåtgärden är livvaktsskydd. Verksamheten handlar till stor del om förebyggande arbete för att en skyddsperson ska kunna genomföra sitt uppdrag tryggt och säkert, samtidigt som han eller hon ska kunna röra sig fritt och ha nära kontakt med allmänheten.

Säkerhetspolisen ansvarar för den övergripande utformningen av personskyddet och för skyddet närmast skyddspersonen. Polismyndigheten ansvarar för distansskyddet. Skyddet kring en skyddsperson utformas efter behov. Säkerhetspolisen gör löpande bedömningar som ligger till grund för vilka skyddsåtgärder som sedan vidtas. Säkerhetspolisens personskyddsarbete bygger på bedömningar av skyddsvärde, hotbild och sårbarheter:

- *Skyddsvärdet* beskriver hur allvarliga konsekvenserna skulle bli för Sverige om funktionen inte skulle kunna utföra sitt uppdrag. Det kan till exempel handla om hur viktig funktionen är för det demokratiska systemets förmåga att fungera, men också om funktionens symbolvärde.
- *Hotbilden* är en samlad bedömning av de konkreta och potentiella hoten mot en skyddsperson. Ett hot utgörs i det här sammanhanget av en aktörs avsikt och förmåga att utföra ett fysiskt angrepp mot skyddspersonen.

- *Sårbarheter* är egenskaper hos eller aspekter kring en skyddsperson som kan utnyttjas av en aktör med avsikt och förmåga att realisera ett hot mot skyddspersonen.

Inför att skyddspersoner deltar vid evenemang gör Säkerhetspolisen dessutom särskilda bedömningar för att se om det finns någon hotbild mot evenemanget.

Vid Säkerhetspolisen arbetar livvakter, säkerhetschaufförer, administratörer, analytiker, handläggare, psykologer och utredare nära varandra i frågor som rör skyddspersonernas säkerhet. Stora mängder information hämtas in, bearbetas och analyseras för att sedan ligga till grund för de löpande bedömningarna. Utifrån dem planeras sedan lämpliga åtgärder.

Skyddsåtgärderna ska förebygga, förhindra och försvåra ett angrepp. En skyddsåtgärd är information och rådgivning, till exempel att Säkerhetspolisen ger skyddspersonen råd om försiktighetsåtgärder att vidta i vardagen eller informerar Polismyndigheten om att en aktivitet ska genomföras på en viss plats. Andra exempel på skyddsåtgärder kan vara säkra transporter i form av en säkerhetschaufför, tekniska skyddsåtgärder som lås och larm i bostaden eller livvaktsskydd.

I samband med att skyddsåtgärder planeras bedömer Säkerhetspolisen vilken förmåga en angripare har. Dessa förmågor, till exempel att utöva hot eller använda fysiskt våld, kan förändras och utvecklas. Många gånger är dessa förändringar inte kända eller kan inte bedömas. För särskilt skyddsvärda funktioner tillämpar Säkerhetspolisen därför en dimensionerande hotbeskrivning. En dimensionerande hotbeskrivning beskriver en viss förmodad förmåga som skyddet ska motstå och som ska kunna stå sig över tid.

Säkerhetsskydd

Om vissa myndigheter och företag i Sverige utsätts för antagonistiska handlingar, kan det orsaka allvarliga konsekvenser för Sveriges säkerhet. Det kan till exempel handla om verksamheter inom rättsväsendet, energi- eller vattenförsörjningen, telekommunikationer eller transportsektorn.

Dessa verksamheter kan i sitt uppdrag behöva hantera uppgifter som är av betydelse för Sveriges säkerhet. Om dessa uppgifter röjs, förstörs eller ändras kan det inverka på Sveriges säkerhet. Det är därför verksamheter som behöver ett särskilt skydd: säkerhetsskydd. Säkerhetsskyddsåtgärder kan delas in i tre huvudområden: personalsäkerhet, fysisk säkerhet och informationssäkerhet. Säkerhetsskydd handlar om att respektive verksamhetsutövare ska skydda den information och de verksamheter som är av betydelse för Sveriges säkerhet mot spionerі, sabotage, terroristbrott och vissa andra hot. Det handlar även om att skydda verksamhet som omfattas av ett internationellt åtagande om säkerhetsskydd som är förpliktande för Sverige.

Säkerhetspolisens verksamhet inom säkerhetsskyddet bedrivs genom olika åtgärder som innebär att myndigheten bedömer och reducerar sårbarheter i verksamheter som är av betydelse för Sveriges säkerhet eller som omfattas av internationella säkerhetsskyddsåtaganden (säkerhetskänslig verksamhet). De sårbarhetsreducerande aktiviteterna består huvudsakligen av tillsyn, samråd och vägledning.

Säkerhetsskyddet ansvarar även för att hantera anmälan om säkerhetshotande händelser, upprätta nationella lägesbilder och att genomföra registerkontroller efter ansökan från verksamheter som bedriver säkerhetskänslig verksamhet.

3.3.2 Säkerhetspolisens underrättelseverksamhet

Målet med underrättelseverksamheten

Säkerhetspolisens huvudsakliga verksamhet består av underrättelsearbete. Underrättelsearbetet bedrivs inom alla Säkerhetspolisens verksamhetsgrenar. För att Säkerhetspolisen ska kunna fullgöra sitt uppdrag måste myndighetens verksamhet inriktas utifrån den hotbild som finns mot de företeelser som Säkerhetspolisen ska skydda.

Det är fråga dels om en strategisk hotbild för att inrikta verksamheten långsiktigt, dels om hotbilder som är knutna till en viss person, en viss gruppering, en viss händelse eller vissa företeelser. Tillförlitliga hotbedömningar och relevanta hot- och sårbarhetsreducerande åtgärder förutsätter att underrättelseverksamheten kan förse myndigheten med information om potentiella aktörer och fånga upp varningssignaler redan innan konkreta åtgärder för att

begå ett brott har vidtagits. Hotbilden utgår bland annat från en bedömning av en aktörs avsikt och förmåga att bedriva aktuell brottslig verksamhet. Det kan exempelvis handla om att kartlägga utländsk underrättelseverksamhet i Sverige eller om att upptäcka indikationer på terrorverksamhet. För att ha en sådan förmåga krävs att myndigheten kan uppfatta trender och tendenser som kan vara säkerhetshotande, utan att det alltid i detta skede rör sig om ett specifikt brott.

Säkerhetspolisens arbete är alltså främst inriktat mot att identifiera brottslig verksamhet i form av planer på och tidiga förstadier till brott. När Säkerhetspolisen identifierar brottslig verksamhet i ett så tidigt skede kan brottsligheten normalt förhindras innan konkreta brottsliga gärningar går att urskilja.

Säkerhetspolisen behöver kunna samla in, sammanställa och analysera uppgifter inom kontraspionageverksamheten, kontraterrorismverksamheten och författningsskyddsverksamheten även om uppgifterna inte kan hänföras vare sig till något visst konkret brott eller till någon mer konkret definierad brottslig verksamhet. Som exempel kan nämnas behovet av att inom kontraspionaget fortlöpande kunna följa utvecklingen när det gäller främmande makts underrättelsenärvaro här i landet och att kunna övervaka personer som bedriver sådan verksamhet. Säkerhetspolisen behöver också, med utgångspunkt i svenska intressen, följa den politiska utvecklingen i andra länder, verksamheten inom vissa grupper eller hos vissa personer som kan utgöra ett hot mot det svenska samhället eller som kan komma att göra sig skyldiga till terroristbrott. Inom författningsskyddet kan Säkerhetspolisen exempelvis behöva kartlägga hot som riktar sig mot vissa grupper i samhället och fortlöpande följa hotbilden mot vissa myndigheter eller organ. Inom ramen för detta arbete måste Säkerhetspolisen kunna dokumentera och analysera både information av underrättelsekaraktär och annan information av olika slag, såväl från allmänt tillgängliga källor som från Säkerhetspolisens eget arbete och från andra myndigheter.

Säkerhetspolisens huvudsakliga inriktning att identifiera förstadier av brott är en avgörande skillnad i Säkerhetspolisens verksamhet och arbetsmetoder jämfört med Polismyndighetens. Av Säkerhetspolisens operativa resurser är en överväldigande majoritet inriktad på underrättelsearbete. När Säkerhetspolisen har identi-

fierat brottslig verksamhet i ett så tidigt skede är det sällan som brottsligheten fullbordas.

Fokus i Säkerhetspolisens verksamhet är inte heller lagföring, utan i stället att inhämta underlag för beslut om hot- och sårbarhetsreducerande åtgärder. Denna underrättelseverksamhet tjänar därför i första hand som underlag för beslut om vilka åtgärder Säkerhetspolisen ska vidta i sitt brottsförebyggande arbete. Den ligger också till grund för beslut om till exempel personskydd eller säkerhetsskyddsåtgärder. Ett övergripande mål med underrättelseverksamheten är att hämta in kunskap som kan omsättas i operativ verksamhet. Det internationella samarbetet är ett väsentligt inslag i detta arbete.

Syftet med underrättelseverksamheten är alltså i huvudsak att upptäcka om en viss, inte närmare specificerad, brottslighet har ägt rum, pågår eller kan antas komma att begås. Underrättelser kan bland annat läggas till grund för beslut om att inleda förundersökning eller beslut om att vidta särskilda åtgärder för att förebygga, förhindra eller upptäcka brott. Exempelvis kan ett visst brottsligt tillvägagångssätt uppmärksammas genom media och därmed förebyggas. En annan form av förebyggande verksamhet innebär att berörda personer kontaktas och därigenom blir medvetna om myndighetens intresse, vilket många gånger leder till att den planerade brottsliga verksamheten aldrig kommer till stånd. Samverkan sker också med andra myndigheter för att de ska kunna vidta hotreducerande åtgärder samt med samverkande myndigheter i andra länder.

Metoder för underrättelseverksamheten

Underrättelseprocessen

Säkerhetspolisens uppdrag innebär att bekämpa särskilt allvarliga och svårutredda brott. För att kunna fullgöra detta uppdrag måste myndigheten själv identifiera aktörer som kan tänkas komma att begå till exempel terrorismrelaterad brottslighet samt bedöma förutsättningarna för att planerad brottslighet sätts i verket.

En stor del av myndighetens arbete består därför av kartläggning av individer och nätverk som kan komma att ägna sig åt brottslighet i eller utanför Sverige samt att upprätthålla en lägesbild över utvecklingen av potentiella hot genom att följa trender och tenden-

ser. Säkerhetspolisen måste vidare inrikta sitt arbete utifrån den hotbild som kan finnas mot de personer, särskilt skyddsvärda verksamheter och svenska intressen i övrigt som myndigheten har i uppdrag att skydda.

Underrättelseverksamhet bedrivs enligt en viss process. Det första ledet i processen är planerings- eller *inriktningsfasen*. I denna fas beslutas bland annat vilka områden som är prioriterade och vilka uppgifter som ska hämtas in. Nästa steg är *inhämtningen*, som kan ske på flera olika sätt. När information har hämtats in *bearbetas* den genom att struktureras, systematiseras och värderas, till exempel genom jämförelser med sedan tidigare kända uppgifter. Därefter vidtar *analysen*. Det kan handla om exempelvis hot- och riskanalys, analys av brottsmönster och kartläggning av kriminella nätverk och grupperingar. Efter inhämtning, bearbetning och analys är ambitionen att det framtagna underrättelsematerialet ska kunna användas i operativt arbete. Detta brukar benämnas *delgivning* av information.

Inhämtning och bearbetning

Inhämtning av underrättelser sker bland annat genom spaningsåtgärder, förhörsinformation, informationsutbyte med utländska säkerhets- och underrättelsetjänster och kontakter med Polismyndigheten, andra myndigheter och organisationer och från öppna källor, till exempel internet.

Andra källor för inhämtning utgörs av de hemliga tvångsmedlen enligt lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott eller inhämtning av uppgifter om elektronisk kommunikation enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet. För att kartlägga hot mot landet får Säkerhetspolisen under vissa förutsättningar även inrikta den signalspaning som utförs av Försvarets radioanstalt. Finansiell inhämtning sker också med stöd av lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism.

Inhämtning av information sker också från fysiska källor, personer som lämnar information. Att Säkerhetspolisen tar hjälp av fysiska källor är en mycket viktig del i underrättelsearbetet. Det bidrar till Säkerhetspolisens förmåga att skydda den svenska demokratin och

den nationella säkerheten, främst inom områdena kontraspionage, kontraterrorism och författningsskydd.

Inhämtade underrättelser bearbetas, och det görs en bedömning av hur trovärdig källan är och huruvida informationen är tillförlitlig. Efter det analyseras informationen.

Analys och delgivning

När inhämtade uppgifter har analyserats lämnas informationen till berörda funktioner inom Säkerhetspolisen eller andra myndigheter och lämpliga åtgärder vidtas eller så inriktas fortsatt inhämtning. Med utgångspunkt i informationen beslutas alltså om operativa åtgärder, extern informationsspridning eller förnyad underrättelseinriktning.

Till skillnad från utredningsarbete i en förundersökning som har en tydlig början och ett slut består underrättelseverksamhet i stället av att ständigt fylla informationsluckor och förse beslutsfattare med underlag som gör det möjligt att rikta in kommande inhämtning.

Att bearbeta, bedöma och analysera information och underrättelser ingår i kärnan av en säkerhetstjänsts uppgifter. Säkerhetspolisen jobbar dygnet runt med att lägga pussel, söka mönster och dra slutsatser utifrån det ständiga inflödet av underrättelser till myndigheten.

Säkerhetspolisens analysarbete sker på flera olika nivåer: strategisk, operativ och taktisk.

Strategisk analys syftar till att ta fram beslutsunderlag för den långsiktiga inriktningen av myndighetens verksamhet. *Operativ analys* kan till exempel handla om att utifrån bearbetande av underrättelseinformation hitta ingångar för att reducera hot och sårbarheter, utvecklingen i specifika miljöer eller att bedöma en statlig aktörs förmågor. *Taktisk analys* handlar om att ta fram beslutsunderlag för hur Säkerhetspolisen ska agera i enskilda ärenden, där tidsperspektivet ofta är kritiskt och beslut om åtgärder måste fattas snabbt.

När uppgifterna sedan har analyserats lämnas informationen till berörda enheter inom Säkerhetspolisen. Med utgångspunkt från analysen beslutas om exempelvis operativa åtgärder eller förnyad underrättelseinriktning.

Regleringen av Säkerhetspolisens underrättelseverksamhet

Vad som utgör underrättelseverksamhet är inte klart definierat i någon rättsakt. Med underrättelseverksamhet i stort avses insamling, bearbetning och analys av information i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet när det ännu inte finns konkreta misstankar om att ett visst brott har begåtts. Finns sådana misstankar består verksamheten i stället av att utreda brott, typiskt sett enligt reglerna om förundersökning i brottmål.

Brottsbekämpande verksamhet anses i dag omfatta både att förebygga, förhindra och upptäcka brottslig verksamhet samt att utreda och beivra/lagföra brott. I motsats till hur det förhåller sig med den brottsutredande verksamheten är dock stora delar av myndigheternas underrättelseverksamhet inte lagreglerad. I stället sätter polislagens och regeringsformens allmänna principer för olika former av ingripanden, som behovs- och proportionalitetsprinciperna, en ram för verksamheten.

Säkerhetspolisens underrättelseuppdrag har i öppna rättsliga källor beskrivits främst genom uttalanden i anslutning till de olika personuppgiftslagstiftningar som berört Säkerhetspolisen och i lagstiftningar som reglerar användandet av olika inhämtningsmetoder, som hemliga tvångsmedel. Instruktioner om den närmare inriktningen av Säkerhetspolisens uppdrag ger regeringen i regleringsbrev, som är sekretessbelagda med hänsyn till Sveriges säkerhet.

Underrättelseverksamhet består i mycket stor utsträckning av personuppgiftsbehandling. I brist på en generell rättslig reglering av underrättelseverksamhetens syfte, omfång och metoder är därför personuppgiftslagstiftningen i praktiken styrande för verksamheten, på samma sätt som rättegångsbalken är för brottsutredning och lagföring. Det finns även särskilda regler angående användning av mer ingripande metoder för underrättelseinhämtning, som hemliga tvångsmedel i brottspreventivt syfte. Dessa specialregleringar innehåller dock inte några mera generella regler av hur inhämtade uppgifter därefter får behandlas i verksamheten. En ändamålsenlig utformning av personuppgiftslagstiftningen är alltså av helt central betydelse för att Säkerhetspolisen ska kunna utföra sitt uppdrag och utnyttja den information som myndigheten har rätt att hämta in.

Av 3 § i den äldre polisdatalagen (1998:622) framgick att polisens, och då även Säkerhetspolisens, underrättelseverksamhet är ”att samla,

bearbeta och analysera information för att klarlägga om brottslig verksamhet har utövats eller kan komma att utövas och som inte utgör förundersökning". All underrättelseverksamhet som inte bedrevs av Säkerhetspolisen betecknades i den lagen som kriminalunderrättelseverksamhet och var något strängare reglerad. I den efterföljande polisdatalagen (2010:361) ersattes definitionen av underrättelseverksamheten med det mer generella ändamålet som uttrycks i polislagen; att förebygga, förhindra eller upptäcka brottslig verksamhet. I Säkerhetspolisens nuvarande personuppgiftslag, kvarstår polislagens definition av det brottsförebyggande uppdraget, att förebygga, förhindra eller upptäcka brottslig verksamhet, som en övergripande rättslig grund. Inom denna del av uppdraget inryms underrättelseverksamheten.

Begreppet *brottslig verksamhet* är central för att särskilja underrättelsearbete i förhållande till förundersökning. Begreppet förekommer inom både straff-[5] och processrätten,[6] men framför allt inom en rad personuppgiftslagstiftningar[7] samt i lagstiftningar som reglerar straffprocessuella tvångsmedel[8] för att markera att det rör sig om underrättelseverksamhet och inte förundersökning.

Begreppet brottslig verksamhet saknar en tydlig och allmängiltig definition, vilket har kritiserats.[9] Uttrycket används typiskt sett för att markera att det inte krävs misstankar av samma konkretion som för att inleda förundersökning. Ändå är kravet för att inleda förundersökning mycket lågt. Det räcker med ett antagande att brott av visst angivet slag har begåtts, men några närmare detaljer om brottet behöver inte vara kända. Skillnaden mellan misstankar som rör brottslig verksamhet och brott, särskilt i fråga om de osjälvständiga brottsformerna, får betecknas som svårfångad.

Allmänna misstankar om att det förekommer brottslig verksamhet i någon form är dock inte tillräckligt för att det ska kunna inledas

[5] Se bland annat 16 kap. 10 a § och 16 kap. 5 a § brottsbalken samt 3 § lag (2014:307) om straff för penningtvättbrott. Brottslig verksamhet har dock tidigare ansetts för vagt och oprecist för att kunna användas som straffrättsligt rekvisit; se prop. 1998/99:19 s. 29.
[6] Se bland annat 24 kap. 1 § och 28 kap. 3 § rättegångsbalken.
[7] Se bland annat Polisens (2018:1693), Tullverkets (2018:1694) och Kustbevakningens (2018:1695) respektive så kallade registerlagstiftningar inom brottsdatalagens område.
[8] Se lag (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott, lag (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet och lag (2020:62) om hemlig dataavläsning.
[9] Se Lindberg, Gunnel, *Straffprocessuella tvångsmedel*, JUNO version: 5, Publicerad digitalt: 2022, s. 813 samt Naarttijärvi, Markus, *För din och andras säkerhet*, Diss. Umeå universitet, 2013, s. 319.

förundersökning. Rättegångsbalkens bestämmelser om inledande av förundersökning är utformad utifrån en tanke om att en konkret brottslig gärning angivits eller anmälts. Gemensamt för hur begreppet brottslig verksamhet används i olika lagstiftningar är att det inte förutsätter kännedom om konkreta gärningar. Däremot måste verksamheten avse en viss typ av brottslighet, som dock inte behöver vara närmare specificerad i fråga om omfattning eller detaljer. Misstankar om bagatellartade gärningar som kan utgöra rena bötesbrott brukar inte anses kunna konstituera en brottslig verksamhet.[10]

Polismyndigheten har definierat brottslig verksamhet som sammanhängande aktiviteter som var för sig eller tillsammans innefattar att de som deltar i verksamheten kommer att utföra, eller förmå andra att utföra, gärningar som straffrättsligt är att anse som brott.[11]

Den brottsbekämpande underrättelseverksamheten som helhet går ut på att avslöja om en viss, inte närmare specificerad brottslig verksamhet har förekommit, pågår eller kan förväntas inträffa. I dessa sammanhang talas det om ”underrättelsemisstankar” om pågående brottslig verksamhet som inte kan konkretiseras eller om allmänna misstankar om framtida brott. Underrättelsemisstankarna om brottslig verksamhet kan avse fragmenterad, opreciserad och osäker information om aktiviteter som kan antas komma att leda till konkreta brott. De personer som är föremål för underrättelseutredningar kallas ibland för underrättelsemisstänkta eller riskpersoner.

Även i underrättelseverksamheten förekommer således ”misstänkta” i språklig mening, med den reservationen att personerna i fråga inte nödvändigtvis är misstänkta för ett redan inträffat brott som kan beskrivas med den konkretion som regleringen i brottsbalken och rättegångsbalken förutsätter. Misstanken avser i stället en viss brottslig verksamhet. Begreppet ”misstänkt brottslig verksamhet” används också i lagstiftning om de brottsbekämpande myndigheternas behandling av personuppgifter.[12] Även ”misstanke” utgör därmed en naturlig del av begreppsapparaten när underrättelse-

[10] Se Ds 2006:17 s. 94–97 och exempelvis prop. 2015/16 s. 18, prop. 2014/15 s. 34, prop. 2022/23:53 s. 84.
[11] *Polismyndighetens handbok för underrättelsetjänst – verksamhet, process och begrepp*, PM 2021:17 saknr 493, s. 9 f.
[12] Se 3 kap. 2 § 1 p. lag (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område samt 3 kap. 4 § i samma lag angående personer som är misstänkta för att ha utövat eller komma att utöva misstänkt brottslig verksamhet.

verksamhet i allmänhet och särskilt preventiv tvångsmedelsanvändning diskuteras.[13]

Den brottsliga verksamhet som Säkerhetspolisen har till uppdrag att bekämpa har exemplifierats i förarbeten till polisdatalagen (2010:361). Där anges verksamheter, sammanslutningar och annat som kan utvecklas till konkreta hot mot det svenska samhällsskicket eller mot enskilda personer i statsledningen som ett exempel. Ett annat exempel är att en främmande stat misstänks bedriva underrättelseverksamhet av visst slag, utan att några konkreta brott kan urskiljas. Även företeelser i det svenska samhället som kan komma att utvecklas till brott mot bestämmelser i 18 eller 19 kap. brottsbalken ansåg regeringen kunna utgöra brottslig verksamhet utan att närmare specificera hur riskbedömningen eller prognosen är tänkt att utföras.

Vidare anses begreppet medge att Säkerhetspolisen följer den politiska utvecklingen i andra länder och verksamheten inom vissa grupper, som kan utgöra ett hot mot det svenska samhället eller som kan komma att göra sig skyldiga till terroristbrott. Regeringen har uttalat att det normalt inte går att urskilja lika tydliga kopplingar till brottslig verksamhet i Säkerhetspolisens verksamhet. Den underrättelseverksamhet som bedrivs inom Säkerhetspolisen är till sin natur ofta sådan att den ligger på ett tidigare stadium än den som bedrivs av polisen i övrigt.[14] Klart är att avsikten är att Säkerhetspolisens underrättelseverksamhet ska tillåtas ha en bredare inriktning än motsvarande verksamhet hos andra brottsbekämpande myndigheter. Detta får anses följa av den brottskatalog som Säkerhetspolisen ansvarar för snarare än av den likalydande regleringen av underrättelseuppdraget.

3.3.3 Säkerhetspolisens brottsutredande verksamhet

Säkerhetspolisens brottsutredande uppdrag är av liten omfattning i förhållande till övriga uppdrag. De förundersökningar som främst aktualiseras inom myndigheten avser brott mot Sveriges säkerhet enligt 19 kap. brottsbalken, olika former av terroristbrott samt brott riktade mot personer i den centrala statsledningen. Eftersom Säker-

[13] Se SOU 2022:52 s. 146 f.
[14] Prop. 2009/10:85 s. 256 och 362 f.

hetspolisens mål är att förhindra allvarlig brottslighet innan den genomförs ingriper myndigheten ofta i ett tidigt skede vid information om misstänkt brottslighet. De brottsrubriceringar Säkerhetspolisen utreder utgörs därför många gånger av de så kallade osjälvständiga brottsformerna, som stämpling, förberedelse och anstiftan till brott.

De utredningar som bedrivs leder till förhållandevis få lagföringar. Den typ av brottslighet det är fråga om är ofta svår att bevisa i en straffrättslig process. De osjälvständiga brottsformerna, som av nämnda skäl främst aktualiseras, kräver ofta en omfattande utredning, om bland annat avsikter med ett handlande. Redan av det skälet föreligger bevissvårigheter, som inte är unika för Säkerhetspolisens verksamhet. Det finns dock ytterligare utredningssvårigheter som är särskilt utmärkande för förundersökningar som bedrivs av en myndighet som samtidigt är den nationella säkerhetstjänsten. En sådan svårighet är eventuella användningsbegränsningar som kan uppställas vad gäller uppgifter som Säkerhetspolisen har fått från en annan stat eller mellanfolklig organisation.[15]

Fällande domar är emellertid inte alltid huvudsyftet med en brottsutredning som genomförs av Säkerhetspolisen. Exempelvis kan aktörer som är misstänkta för spionerі agera i Sverige under en diplomatisk täckmantel. Den diplomatiska immuniteten innebär att det inte går att åtala dessa aktörer för brott. Det viktiga är i stället att Säkerhetspolisen på ett effektivt sätt avbrutit verksamheten innan ett allvarligt brott såsom spionage har genomförts.

Verksamhet för att utreda och lagföra brott omfattar åtgärder inom ramen för förundersökningar. En förundersökning ska inledas så snart det på grund av angivelse eller av annat skäl finns anledning att anta att ett brott som hör under allmänt åtal har förövats (23 kap. 1 § rättegångsbalken). Bestämmelsen ger uttryck för den principiella förundersökningsplikt som gäller i Sverige. När en förundersökning har inletts, blir ett omfattande regelverk som innefattar både förpliktelser för Säkerhetspolisen och rättigheter för den misstänkte tillämpligt. Förundersökningar vid Säkerhetspolisen leds som regel av åklagare vid Riksenheten för säkerhetsmål.

Förundersökningens syfte är att det ska utredas vem som kan misstänkas för ett aktuellt brott och om det finns tillräckliga skäl för åtal samt att målet ska förberedas så att bevisningen kan presen-

[15] Se 6 kap. lag (2017:496) om internationellt polisiärt samarbete.

teras i ett sammanhang vid en domstolsförhandling (23 kap. 2 § rättegångsbalken). Förundersökningsarbetet består till stor del i hållande av förhör samt hantering av eventuella beslag och information som inhämtats genom hemliga tvångsmedel. Under förundersökningen hämtas också annan utredning in.

För att den misstänkte ska kunna ta tillvara sina rättigheter och intressen under en förundersökning genom att till exempel begära att utredningen ska kompletteras med olika åtgärder, är det av avgörande betydelse att han eller hon får reda på att misstankarna finns. När förundersökningen har kommit så långt att någon skäligen kan misstänkas för brottet, ska den misstänkte därför underrättas om misstanken när han eller hon hörs (23 kap. 18 § rättegångsbalken). Genom underrättelsen uppkommer bland annat en rätt till insyn enligt rättegångsbalken. Rätten till insyn är central för den enskildes rättssäkerhet och möjlighet att försvara sig. Underrättelsen innebär självklart också slutet på Säkerhetspolisens möjlighet att utreda brottet utan den misstänktes kännedom.

3.4 Nationellt och internationellt samarbete

3.4.1 Nationellt samarbete

Nationellt samarbetar Säkerhetspolisen främst med de försvarsanknutna underrättelsemyndigheterna, de brottsbekämpande myndigheterna samt med Migrationsverket. Säkerhetspolisen har ett nära samarbete med den militära underrättelse- och säkerhetstjänsten, och med Försvarets radioanstalt. Samarbetet omfattar både strategisk, operativ och taktisk nivå för den verksamhet som bedrivs. Samverkan mellan de olika underrättelsemyndigheterna är helt avgörande för att Säkerhetspolisen ska lyckas med sitt uppdrag och ett effektivt informationsutbyte är en förutsättning för myndigheternas respektive uppdrag. Samarbetet är nödvändigt för att skapa helhetsbilder om bland annat hotutvecklingen och hur den påverkar Sveriges säkerhet. Uppgifter som behandlas av en underrättelsemyndighet kan tillsammans med uppgifter som behandlas av en annan ge en helhetsbild som inte framträder om de analyseras var för sig.

Därutöver finns sedan länge det etablerade samarbetet mellan myndigheterna inom *Nationellt centrum för terrorhotbedömning*

(NCT). Centret är en permanent arbetsgrupp med personal från Säkerhetspolisen, FRA och den militära underrättelse- och säkerhetstjänsten. Centrets uppgift är att göra strategiska bedömningar av terrorhotet mot Sverige och svenska intressen, på kort och lång sikt.

Säkerhetspolischefen, generaldirektören för Försvarets radioanstalt och chefen för den militära underrättelse- och säkerhetstjänsten ingår också i det *nationella underrättelserådet*. Underrättelserådets syfte är att säkerställa en god samordning av underrättelser och bidra till informationsutbytet mellan Regeringskansliet och underrättelsemyndigheterna.

Säkerhetspolisen har ett väl utvecklat samarbete med Polismyndigheten. En stor del av samarbetet handlar om informations- och erfarenhetsutbyte, men det är också operativt. Till exempel lämnar Säkerhetspolisen stöd till Polismyndigheten i brottsutredningar i form av expertkunskaper, hotbilder, spaning och analys. Säkerhetspolisen samverkar med Polismyndigheten och andra brottsbekämpande myndigheter vad gäller frågor om till exempel hemliga tvångsmedel och för att motverka grov organiserad brottslighet.[16]

Myndigheten är även sammankallande i *Samverkansrådet mot terrorism* vilket är ett samarbete mellan svenska myndigheter som syftar till att stärka Sveriges förmåga att motverka och hantera terrorism.

Säkerhetspolisen är etablerad i sammanhang som berör användandet av ekonomiska uppgifter för att upptäcka och förebygga brottslighet, inte minst genom aktivt deltagande i den så kallade *svenska regimen* som syftar till att motverka penningtvätt och finansiering av terrorism.[17] Det övergripande syftet med myndighetens deltagande är att stärka Sveriges motståndskraft i förhållande till penningtvätt och finansiering av terrorism. Säkerhetspolisen deltar även i sådan samverkan mot penningtvätt och finansiering av terrorism.[18] Syftet med samverkan är att genom informationsutbyte förebygga, förhindra eller upptäcka om aktörer och nätverk som Säkerhetspolisen misstänker har kopplingar till våldsbejakande extremism eller olovlig verksamhet i främmande makts regi ägnar sig åt penningtvätt eller finansiering av terrorism.

[16] Se 2 § 4 i Säkerhetspolisens instruktion.
[17] Regeringens skrivelse 2013/14:245.
[18] Se 4 a kap. lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terror.

Inom personskyddsarbetet finns ett nära samarbete med den lokala polisen vid planering och genomförande av skyddsåtgärder inom deras geografiska områden. Säkerhetspolisen samverkar också med de parter som omfattas av säkerhetsskyddslagstiftningen. Det vill säga myndigheter, kommuner, regioner samt vissa företag.

3.4.2 Internationellt samarbete

Det internationella samarbetet är ett väsentligt inslag i Säkerhetspolisens arbete med att inhämta underlag för beslut om hot- och sårbarhetsreducerande åtgärder och för att vidta sådana åtgärder. Informationsutbyte är en central del av Säkerhetspolisens samarbete med andra stater.

Samarbetet berör stater både inom och utanför EU. Händelser i utlandet kan få konsekvenser i Sverige och kan komma att påverka den nationella hotbilden och säkerheten. Den säkerhetshotande och brottsliga verksamhet som Säkerhetspolisen har i uppdrag att bekämpa är ofta gränsöverskridande. Säkerhetspolisen har därför ett väl utvecklat samarbete med andra länders säkerhets- och underrättelsetjänster och deltar i olika internationella forum. Myndigheten samverkar även med brottsbekämpande internationella organisationer så som EU:s brottsbekämpande organ Europol och den internationella polisorganisationen Interpol. Beslut och aktiviteter inom FN och EU har ofta bäring på Säkerhetspolisens uppdrag varför Säkerhetspolisen bevakar relevanta konventioner och rättsakter samt bistår regeringen med underlag och resurser i internationella sammanhang kopplat till organen. Säkerhetspolisen har även en roll i det informationsutbyte som sker inom Nato.

Lagen (2017:496) om internationellt polisiärt samarbete tillämpas på det polisiära samarbetet mellan Sverige och andra stater vad gäller frågor om åtaganden såsom operativt samarbete och informationsutbyte som följer av vissa internationella överenskommelser, till exempel Schengensamarbetet.

3.5 Reglering av Säkerhetspolisens behandling av personuppgifter

3.5.1 Bakgrund till säpodatalagen

Säkerhetspolisen var fram till och med år 2014 en del av dåvarande Rikspolisstyrelsen (RPS/Säk). Historiskt har Säkerhetspolisens verksamhet därför av naturliga skäl omfattats av samma personuppgiftslagstiftning som polisväsendet i stort, med vissa särbestämmelser. I den äldre polisdatalagen (1998:622) fanns avvikande bestämmelser som gällde Säkerhetspolisens verksamhet angående information från nedlagda förundersökningar. I övrigt fick Säkerhetspolisen behandla personuppgifter, i det så kallade SÄPO-registret, enligt den dåvarande personuppgiftslagen. Det innebar färre restriktioner än för kriminalunderrättelsetjänsten, som reglerades av polisdatalagen.

I förarbetena till den efterföljande polisdatalagen (2010:361) konstaterades att Säkerhetspolisens verksamhet i stor utsträckning bedrevs på liknande sätt som verksamheten vid polisen i övrigt. Särdragen i Säkerhetspolisens verksamhet motiverade dock att vissa bestämmelser utformades på ett sätt som var mer anpassat till den verksamheten och tillägnades därför ett eget kapitel i lagen. Tanken med regleringen av Säkerhetspolisens personuppgiftsbehandling var att den skulle tillåta hantering på ett i huvudsak oförändrat sätt mot tidigare.[19] Att Säkerhetspolisen år 2015 blev en fristående myndighet föranledde endast vissa formella ändringar i polisdatalagen som alltjämt omfattade både Polismyndighetens och Säkerhetspolisens verksamhet.[20]

År 2016 antog EU dels den så kallade dataskyddsförordningen,[21] dels det så kallade brottsdatadirektivet.[22] Den senare avsåg brottsbekämpande myndigheters behandling av personuppgifter och genomfördes i svensk rätt i huvudsak genom brottsdatalagen (2018:1177). Brottsdatalagen gäller behandling av personuppgifter

[19] Prop. 2009/10:85 s. 250–251.
[20] Prop. 2013/14:110 s. 480 f.
[21] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).
[22] Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF.

som utförs av de brottsbekämpande myndigheterna i deras brottsbekämpande verksamhet och i verksamhet som syftar till att upprätthålla allmän ordning och säkerhet. Dataskyddsförordningen reglerar all annan verksamhet än den som avses i brottsdatadirektivet.

Varken dataskyddsförordningen eller brottsdatadirektivet omfattar dock verksamhet som rör nationell säkerhet, vilket följaktligen inte heller brottsdatalagen gör. Då brottsdatalagen ersatte polisdatalagen, men inte omfattade brottsbekämpning som rör nationell säkerhet, saknades en modern personuppgiftslagstiftning för merparten av Säkerhetspolisens verksamhet. Genom övergångsbestämmelser fortsatte Säkerhetspolisen därför att tillämpa den upphävda polisdatalagen och personuppgiftslagen till dess att det år 2020 infördes en särskild lag för Säkerhetspolisens personuppgiftsbehandling, lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter (i det följande säpodatalagen).

I förarbetena till säpodatalagen betonades att Säkerhetspolisens och Polismyndighetens verksamhet i stor utsträckning bedrivs på liknande sätt men att Säkerhetspolisens uppdrag skiljer sig från Polismyndighetens. Säkerhetspolisen har en betydligt mer begränsad verksamhet, inriktad på några få områden där tyngdpunkten ligger på att förebygga och förhindra brott som rör nationell säkerhet, vilket förutsätter att myndigheten också har förmåga att identifiera och kartlägga sådan brottslig verksamhet. Enligt förarbetena behöver Säkerhetspolisen för detta ändamål kunna behandla personuppgifter på ett tidigt stadium, innan en person eller en gruppering har konkreta brottsplaner eller har vidtagit åtgärder för att begå brott. Det innebär att Säkerhetspolisens arbete främst är inriktat mot att identifiera planer på och förstadier av brottslig verksamhet, i ett så tidigt skede att konkreta brottsliga gärningar kan vara svåra att urskilja. I propositionen angavs att detta innebär att det finns avgörande skillnader i Säkerhetspolisens verksamhet och arbetsmetoder jämfört med Polismyndighetens.[23]

På samma sätt som gällt tidigare, då Polismyndigheten och Säkerhetspolisen omfattades av samma lag, är säpodatalagen både till sitt innehåll och sin struktur likartad med de regleringar som gäller för andra brottsbekämpande myndigheter. I motiven betonades även att de tidigare bestämmelserna i polisdatalagen i allt väsentligt fungerat som avsett. Bestämmelserna i polisdatalagen ansågs därför till

[23] Prop. 2018/19:163 s. 47 f.

stor del kunna bilda mönster för den nya lagen.[24] Säpodatalagen var därmed inte avsedd att medföra några större förändringar i hur Säkerhetspolisen skulle få behandla personuppgifter, utan syftade till att myndigheten i det avseendet skulle ha förutsättningar att fortsätta på i huvudsak samma sätt som tidigare.

3.5.2 Allmänt om personuppgiftsbehandling

För att förstå säpodatalagens uppbyggnad, eller någon annan dataskyddsreglering, är det viktigt att förstå begreppet personuppgiftsbehandling.

Av säpodatalagens definitioner i 1 kap. 5 § framgår att behandling av personuppgifter innefattar en åtgärd eller en kombination av åtgärder som vidtas i fråga om personuppgifter eller en uppsättning av personuppgifter, oavsett om det görs automatiserat eller inte. Som exempel anges i lagtexten insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämnande, spridning eller tillhandahållande på annat sätt, justering, sammanföring, begränsning, radering eller förstöring. Dessa exempel är inte uttömmande utan är avsedda att illustrera att det i praktiken inte finns något sätt att hantera personuppgifter som inte träffas av begreppet behandling.

I samma paragraf definieras en personuppgift som varje upplysning om en identifierad eller identifierbar fysisk person som är i livet. Varje upplysning som kan hänföras till en fysisk person är en personuppgift, som exempelvis namn eller passbild. Det gäller även upplysningar som kan hänföras till en individ om denna kan identifieras med hjälp av informationen, exempelvis oidentifierade fingeravtryck, alias eller e-postadress. Det krävs inte att den personuppgiftsansvarige ska förfoga över samtliga uppgifter som gör identifieringen möjlig. Det är därmed tillräckligt att det ska vara möjligt att koppla informationen till en levande individ för att det ska utgöra personuppgifter.

Information som kan utgöra personuppgifter omfattar därmed allt från uppgifter som direkt beskriver en person som namn, bild eller personnummer till uppgifter som indirekt går att koppla till en person som adress, ljudklipp, ip-adress eller GPS-information.

[24] Se SOU 2017:74 s. 598 och prop. 2018/19:163 s. 49.

I exempelvis ett telefonsamtal förekommer som regel en mängd personuppgifter, både avseende de personer som kommunicerar med varandra och om andra som direkt eller indirekt omnämns i samtalet.

Personuppgiftsbehandling har sedan länge använts som en heltäckande beskrivning av all slags hantering av uppgifter som direkt eller indirekt kan hänföras till en levande person. Begreppet i svensk rätt har sitt ursprung i personuppgiftslagen (1998:204). Personuppgiftslagen genomförde EU:s dataskyddsdirektiv[25] som innehöll en motsvarande definition av begreppet behandling. Dataskyddsdirektivet var i sin tur inspirerat av dataskyddskonventionen[26] från 1981 som innehåller en definition av *automatisk behandling* [eng. automatic processing], av liknande lydelse (som dock inte innefattade insamling av personuppgifter). Syftet med ett så generellt begrepp är att lagar där begreppet används ska bli så teknikneutrala som möjligt och inte stå i vägen för eller skapa oreglerade kryphål för nya eller oförutsedda sätt att bearbeta eller komma åt personuppgifter.

Problemet med den beskrivna lagstiftningstekniken är att de lagar som reglerar personuppgiftsbehandling omfattar en stor variation av både information och åtgärder. Det innebär att harmlös hantering, som att upprätta en lista med e-postadresser för utskick i en idrottsförening, och starkt integritetskänslig behandling, som genetisk profilering, regleras inom samma rättsliga ram. Sådana lagar behöver andra sätt att hantera det faktum att olika former av behandling kan utgöra olika grader av intrång i den personliga integriteten.

Lösningen går ut på att dataskyddsregelverk på olika sätt strävar efter att minimera antalet personuppgifter som behandlas och säkerställa att endast de uppgifter som är nödvändiga för ett visst på förhand uttalat ändamål får behandlas, och endast i detta syfte. Det ändamål som ska vägleda vilka personuppgifter som får behandlas måste komma från en på förhand definierad grund. Inom näringslivet bygger grunden för personuppgiftsbehandling ofta på avtal eller samtycke. För myndigheter utgörs grunden normalt av ett rätts-

[25] Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.
[26] Europarådets konvention 108 av den 28 januari 1981 om skydd för enskilda vid automatisk databehandling av personuppgifter, SÖ 1982:50.

ligt fastställt uppdrag, som brottsbekämpning och annan myndighetsutövning eller ett allmänt intresse.

En prövning av vilka personuppgifter som är nödvändiga att behandla för ett visst ändamål är inte sällan svår att utföra och läggs på den personuppgiftsansvariga myndigheten eller företaget att göra själv, i de fall då det inte är möjligt eller önskvärt med specifik lagstiftning i frågan. Den grundläggande tanken bakom kravet på ändamål är att ingen har rätt att samla på sig uppgifter om individer, hur obetydliga de än kan framstå, utan giltig anledning. En annan säkerhetsmekanism är att ett antal särskilt integritetskänsliga uppgifter endast tillåts att behandlas om behovet överskrider ett visst högre krav. I Sverige benämns dessa som känsliga personuppgifter, men inom EU- och Europarätten brukar motsvarande uppgifter sägas utgöra särskilda kategorier av uppgifter [eng. special categories].

Av 1 kap. 2 § säpodatalagen framgår att lagen gäller vid behandling av personuppgifter som rör nationell säkerhet i Säkerhetspolisens brottsbekämpande och lagförande verksamhet. Inom denna verksamhet är lagen därmed tillämplig på såväl insamling som lagring, sökning och läsning av personuppgifter, där annan specialreglering saknas. Hur Säkerhetspolisens personuppgiftsbehandling regleras har därmed stor betydelse för en myndighet vars uppdrag till största del består av att samla in och på olika sätt bearbeta och analysera information om människor.

I det följande beskrivs hur vissa delar av säpodatalagen är utformad. Redogörelsen är inriktad på de centrala bestämmelserna i lagen och gör inte anspråk på att vara heltäckande. Säpodatalagen är relativt ny och för en mer utförlig redogörelse för samtliga bestämmelser i lagen hänvisas till lagens förarbeten.[27]

3.5.3 Säpodatalagens tillämpningsområde

Behandling av personuppgifter som rör nationell säkerhet i brottsbekämpande och lagförande verksamhet

Säpodatalagen gäller behandling av personuppgifter som rör nationell säkerhet i Säkerhetspolisens brottsbekämpande och lagförande verksamhet (1 kap. 2 §).

[27] SOU 2017:74, prop. 2018/19:163, bet. 2019/20:JuU9, rskr. 2019/20:44.

Avgränsningen till nationell säkerhet följer av att det EU-rättsliga dataskyddsregelverket omfattar all personuppgiftsbehandling som sker inom områden där unionen har lagstiftningskompetens. Inom det område som går under beteckningen *nationell säkerhet* har medlemsstaterna däremot i princip exklusiv kompetens. Det innebär att varken dataskyddsförordningen eller brottsdatadirektivet är tillämpliga inom detta område, vilket det erinras om i respektive rättsakt.[28]

Trots sina likheter med brottsdatalagen utgör säpodatalagen ett exempel på att Sverige utnyttjat sin exklusiva lagstiftningskompetens inom området nationell säkerhet. Detta kommer till uttryck bland annat genom att säpodatalagen, på samma sätt som de tidigare polisdatalagarna, avgränsar tillämpningsområdet till brottsbekämpande *verksamhet*. Detta är en skillnad mot brottsdatalagens tillämpningsområde som avgränsas genom det brottsbekämpande *syftet* med personuppgiftsbehandlingen. Säpodatalagen omfattar därför behandling även för andra syften än brottsbekämpning, men som sker i brottsbekämpande verksamhet.

Om Säkerhetspolisen behandlar personuppgifter i brottsbekämpande syfte i verksamhet som inte rör nationell säkerhet tillämpas i stället brottsdatalagen och polisens brottsdatalag (1 kap. 4 § brottsdatalagen). Sådan behandling kan ske bland annat då Säkerhetspolisen bistår Polismyndigheten i enskilda fall eller efter överenskommelse enligt 13 § i Säkerhetspolisen instruktion.

All operativ verksamhet som bedrivs av Säkerhetspolisen har ansetts vara i någon mån brottsbekämpande. Det innebär exempelvis att även Säkerhetspolisens yttranden i medborgarskapsärenden har ansetts falla inom lagens tillämpningsområde.[29] I den verksamhet som inte rör brottsbekämpning ska EU:s dataskyddsförordning tillämpas, oavsett om verksamheten omfattas av unionsrätten eller inte (1 kap. 2 § dataskyddslagen). Detta område har ansetts omfatta eventuell personuppgiftsbehandling i den interna verksamheten, som framtagande av interna föreskrifter, handböcker och policydokument. Även den administrativa verksamheten, där personalfrågor och ekonomihantering hanteras, har ansetts falla utanför lagens brottsbekämpande tillämpningsområde och merparten av

[28] Se förklaringssats 16 till dataskyddsförordningen respektive 14 till brottsdatadirektivet.
[29] Prop. 2009/10:85 s. 255 f.

den administrativa personuppgiftsbehandlingen har inte heller antagits utgöra frågor som rör nationell säkerhet.[30]

Automatiserad behandling och strukturerade samlingar

Föremålet för olika personuppgiftslagstiftningar har alltid varit *automatiserad behandling*, vilket innebär att personuppgifter ska vara sökbara med dator. Sveriges (och världens) första personuppgiftslag, datalagen (1973:289), begränsades till denna då nya typ av behandling, som även ansågs medföra helt nya faror för otillbörligt intrång i den personliga integriteten.[31] När datalagen efter 25 år ersattes med personuppgiftslagen (1998:204) utvidgades tillämpningsområdet, både avseende automatiserad behandling och till behandling av personuppgifter i sökbara manuella register. Personuppgifter som hanterades i pappersform omfattades av samma regler som automatiserad behandling så länge uppgifterna ingår i en *strukturerad samling* av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier. Det senare innebär att det förs register över olika personuppgifter som exempelvis gör det möjligt att söka efter en akt eller ett dokument med hjälp av ett personnamn eller personnummer.

I tekniskt avseende är säpodatalagens tillämpningsområde detsamma som för den 25 år gamla personuppgiftslagen. Säpodatalagen ska därmed, enligt 1 kap. 3 §, tillämpas på sådan behandling av personuppgifter som är helt eller delvis automatiserad och på annan behandling som ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Subsidiär lagstiftning

Enligt 1 kap. 4 § är säpodatalagen subsidiär, inte bara till annan lag, utan även till förordning. Detta är en skillnad mot den tidigare polisdatalagen som endast var subsidiär till vissa utpekade lagar och förordningar meddelade med stöd av dessa.

[30] Prop. 2018/19:163 s. 54.
[31] Se till exempel prop. 1973:33 s. 89.

Det huvudsakliga skälet till bestämmelsen, som framgår av förarbetena, är att den insynsrätt för enskilda som säpodatalagen innehåller i viss mån kan anses stå i strid med straffprocessuella regler om målsägande och misstänkts insyn. Regeringen ansåg att subsidiaritetsbestämmelsen borde vara generell, och inte begränsas till bland annat rättegångsbalkens regler eller förordningen om internationellt polisiärt samarbete.

Säpodatalagen innehåller därmed en generell bestämmelse om att avvikelser från lagen är möjliga, antingen genom bestämmelser i annan lag eller i förordning, oavsett om de har beslutats med stöd av regeringens restkompetens eller följer av ett bemyndigande. Likalydande subsidiaritetsbestämmelse finns i brottsdatalagen (1 kap. 5 §) vilket bland annat beror på att den lagstiftningen är en ramlag som medger att särskilda bestämmelser meddelas i de så kallade registerlagarna. I dessa lagar, bland annat 1 kap. 3 § lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område (polisens brottsdatalag), saknas emellertid motsvarande bestämmelser om subsidiaritet i annat avseende än till vissa särskilt utpekade lagar.

3.5.4 Rättslig grund och ändamål

Rättslig grund

Vad innebär rättslig grund?

Att personuppgifter endast får behandlas av en myndighet om det finns rättsligt stöd är en sedan länge etablerad princip för skyddet av personlig information. Den rättsliga grunden utgör den ram inom vilken myndigheten överhuvudtaget får behandla personuppgifter. Begreppet *rättslig grund* för personuppgiftsbehandling används i EU:s rättsakter, som dataskyddsförordningen och genomgående i de lagar som bygger på EU-rättsliga förlagor, som brottsdatalagen och lag (2018:218) med kompletterande bestämmelser om EU:s dataskyddsförordning (dataskyddslagen). Det förekommer ofta att en myndighets verksamhet omfattas av olika personuppgiftsregleringar, där EU:s dataskyddsförordning med kompletterande svensk lagstiftning är tillämplig för exempelvis personaladministration och speciallagstiftning tillämpas i kärnverksamheten. Om en rättslig

grund anges i en personuppgiftslag, överensstämmer den med den del av myndighetens verksamhet som lagen är tänkt att reglera.

I lagar som föregår EU-regleringen eller reglerar områden som ligger utanför EU:s kompetens har begreppet *ändamål* i stället använts, men med samma betydelse: att personuppgifter endast får behandlas om det är nödvändigt för att myndigheten ska kunna utföra de uppgifter som åligger den. Behovet av att uttrycka en särskild rättslig grund, eller ett övergripande ändamål för personuppgiftsbehandling beror på vilken myndighet det handlar om och vilka personuppgifter som myndigheten kommer att behandla. Kravet på en uttrycklig rättslig grund, som är annat än en hänvisning till myndighetens uppdrag, beror dels på om myndighetens uppgifter är så specifika att det redan av dessa går att förutse vilka uppgifter om personer som är nödvändiga för myndigheten att behandla, dels på hur kännbart intrång i den personliga integriteten behandlingen är och om den kan sägas utgöra en kartläggning av enskildas personliga förhållanden. Om en myndighets verksamhet är väl reglerad kan det räcka att som ändamål eller rättslig grund ange att myndigheten får behandla personuppgifter om det är nödvändigt för att myndigheten ska kunna utföra sina uppgifter enligt lag eller förordning.[32] Om det däremot rör sig om uppgifter som är känsligare ur integritetssynpunkt eller innebär en sådan kartläggning som avses i 2 kap. 6 § andra stycket regeringsformen kan ställas högre krav på förutsebarhet och i lag uttryckt rättsligt stöd i personuppgiftslagstiftningen.

I 2 kap. 1 § säpodatalagen anges uttryckliga rättsliga grunder för Säkerhetspolisens personuppgiftsbehandling. Där räknas Säkerhetspolisens uppgifter som rör nationell säkerhet upp i ett antal punkter, vilka i princip korresponderar med polislagens 3 §. Av bestämmelsen framgår även *nödvändighetsrekvisitet* som innebär att personuppgiftsbehandlingen ska vara nödvändig för att uppgiften ska gå att fullgöra på ett effektivt sätt.

[32] Jfr art. 6.1 c i dataskyddsförordningen och 2 kap. 2 § lag om kompletterande bestämmelse till EU:s dataskyddsförordning.

Underrättelseverksamheten

Av de uppräknade grunderna för personuppgiftsbehandling återkommer, i *första punkten*, begreppet förebygga, förhindra eller upptäcka brottslig verksamhet som samlingsbegrepp för Säkerhetspolisens brottsförebyggande arbete. Den verksamhet som avses är huvudsakligen Säkerhetspolisens underrättelseverksamhet. Den första punken är därmed avsedd att ge rättsligt stöd för att bland annat samla in information samt analysera och bearbeta den i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet när det ännu inte finns misstankar om att något konkret brott har begåtts, se avsnitt 3.3.2.

I begreppet ingår bland annat Säkerhetspolisens kartläggning och kontroll av personer, företeelser och annat som kan belysa riskerna för de brott som Säkerhetspolisen har att beivra. Exempel på detta som anges i förarbetena är insamling av uppgifter om verksamheter och annat som kan utvecklas till konkreta hot mot det svenska samhället eller mot enskilda personer i statsledningen samt spaning i syfte att uppdaga sådan brottslig verksamhet som Säkerhetspolisen bekämpar.[33] Inom den rättsliga grunden som avser underrättelseverksamhet ryms också handläggning av frågor om till exempel preventiva tvångsmedel och överskottsinformation enligt 27 kap. 23 a § rättegångsbalken, så länge syftet i förlängningen är att förhindra brott.

Den brottsliga verksamhet som Säkerhetspolisen ska förebygga, förhindra eller upptäcka framgår av polislagen och återkommer även i denna punkt: brott mot Sveriges säkerhet och terrorbrott. Därutöver anges, i första punkten c, *tryckfrihetsbrott och yttrandefrihetsbrott med rasistiska eller främlingsfientliga motiv*. Denna särskilda brottskategori är en kvarleva från polisdatalagen och har sitt ursprung i den tidigare polisorganisationen. Rikspolisstyrelsen hade i en särskild författning[34] föreskrivit att förundersökningar avseende yttrandefrihetsbrott och tryckfrihetsbrott med rasistiskt eller främlingsfientligt motiv alltid skulle handhas av Säkerhetspolisen eller under medverkan av Säkerhetspolisen i de fall där Justitiekanslern är ensam åklagare. Denna föreskrift upphävdes år 2015[35] efter att Säkerhetspolisen blev en fristående myndighet och någon mot-

[33] Prop. 2018/19:163 s. 217 f.
[34] RPSFS 1999:10, FAP 403–3.
[35] PMFS 2015:02.

svarighet finns inte i de föreskrifter[36] som ersatt den tidigare. Bestämmelsen har trots detta överförts till den nuvarande säpodatalagen.

Utreda eller lagföra brott

Av 2 kap. 1 § *andra punkten* framgår att Säkerhetspolisen även får behandla personuppgifter för att utreda eller lagföra de brott som anges i föregående punkt eller efter särskilt beslut annat brott. I praktiken innebär det att Säkerhetspolisen får behandla personuppgifter under förundersökningsstadiet efter det att konkreta brott har kunnat identifierats och rättegångsbalkens regler börjat tillämpas. Med brott avses både gärningar som bevisligen har skett och sådana som det bara finns misstankar om.

Person- och säkerhetsskydd samt uppgifter enligt utlännings- och medborgarskapslagstiftningen

Av den *tredje punkten* följer att Säkerhetspolisen får behandla personuppgifter i samband med personskydd, säkerhetsskydd och då uppgifter utförs enligt utlännings- och medborgarskapslagstiftningen. De två första uppgifterna framgår av 3 § polislagen. Det kan handla om att personuppgifter för skyddspersoner och deras anhöriga kan vara nödvändiga att samla in och behandla vid livvaktsskydd eller att utföra registerkontroller avseende personer som ska delta i säkerhetskänslig verksamhet Uppgifter enligt utlännings- och medborgarskapslagstiftningen omfattar till exempel så kallade säkerhetsärenden, där Säkerhetspolisen bland annat behöver samla in uppgifter och göra sökningar i sina register.

Gemensamt för de tre särskilt uppräknade grunderna i den tredje punkten är att dessa uppgifter, och då särskilt avseende uppgifter enligt utlännings- och medborgarskapslagstiftningen, inte uppenbart utgör brottsbekämpning som rör nationell säkerhet. Det har vid flera tillfällen uttalats att i princip all operativ verksamhet hos Säkerhetspolisen i någon mening är brottsbekämpande. Regeringen ansåg att det fanns behov av att upplysa om att även dessa uppgifter

[36] PMFS 2015:02, PMFS 2018:10 och nu gällande PMFS 2023:6.

rör nationell säkerhet och därför faller inom lagens tillämpningsområde.[37]

Övriga rättsliga grunder

Den *fjärde punkten* anger att Säkerhetspolisen även får behandla personuppgifter om myndigheten ska utföra en annan uppgift som rör nationell säkerhet enligt lag, förordning eller efter särskilt beslut av regeringen. Bestämmelsen innebär att tillkommande uppgifter för Säkerhetspolisen som innebär personuppgiftsbehandling inte kräver ändring i säpodatalagen.[38]Av bestämmelsen erinras om att uppgiften ska röra nationell säkerhet. Trots att det inte nämns i paragrafen, kan det även anmärkas att den rättsliga grunden därutöver ska avse brottsbekämpning, för att säpodatalagen över huvud taget ska vara tillämplig.

Många andra myndigheters personuppgiftslagstiftningar innehåller har en motsvarighet till punkten fyra för att ange att det krävs en rättslig grund för personuppgiftsbehandling. I samband med att denna punkt tillfördes de särskilt angivna uppgifterna blev uppräkningen inte längre uttömmande och därmed inte heller begränsande.[39] De specifika uppgifterna som nämns i de övriga punkterna kan därför anses vara mer av upplysningskaraktär eftersom behandling även för andra, motsvarande uppgifter, kan följa av särskild lagstiftning. Säkerhetspolisen kan exempelvis med stöd av denna punkt behandla personuppgifter då myndigheten samverkar vid granskning av utländska direktinvesteringar i svensk skyddsvärd verksamhet.[40]

Internationella åtaganden

Av den *femte punkten* i bestämmelsen om rättslig grund följer att Säkerhetspolisen får behandla personuppgifter om det är nödvändigt för att fullgöra förpliktelser som följer av internationella åtaganden. Punkten avser att träffa bland annat åtgärder som Säkerhetspolisen vidtar för brottsbekämpande verksamhet i andra länder efter formell

[37] Prop. 2018/19:163 s. 66.
[38] Prop. 2014/15:94 s. 83.
[39] Jfr prop. 2009/10:85 s. 254.
[40] Se prop. 2022/23:116 s. 142.

begäran om rättslig hjälp eller informationsutbyte som enbart gagnar den utländska myndigheten.

Diarieföring med mera

Enligt 2 kap. 2 § i lagen får personuppgifter även behandlas om det är nödvändigt för diarieföring eller för handläggningen om uppgifterna har lämnats till Säkerhetspolisen i en anmälan, ansökan eller liknande. I dessa fall är det tillåtet att behandla personuppgifter oberoende av om förutsättningarna för behandling i föregående paragraf föreligger.

Som tidigare nämnts framgår av 1 kap. 2 § att säpodatalagen endast gäller vid behandling av personuppgifter som rör nationell säkerhet i Säkerhetspolisens brottsbekämpande och lagförande verksamhet. Det innebär att 2 kap. 2 § inte tillämpas för alla former av ansökningar eller all diarieföring, utan endast sådan som faller inom säpodatalagens tillämpningsområde.

Särskilt, uttryckligt angivna och berättigade ändamål

Enligt 2 kap. 3 § får personuppgifter endast behandlas för särskilt, uttryckligt angivna och berättigade ändamål. Vidare följer av bestämmelsen att personuppgifter inte får behandlas för något ändamål som är oförenligt med det ändamål de ursprungligen behandlades för.

Bestämmelsen är helt central för Säkerhetspolisens personuppgiftshantering och i förlängningen även för hur verksamheten kan bedrivas inom myndigheten. Ändamålsbestämmelsen i 2 kap. 3 § kompletteras av och måste läsas tillsammans med flera andra bestämmelser i säpodatalagen.

Som framgått av det föregående ger den rättsliga grunden en ram inom vilken Säkerhetspolisen får behandla personuppgifter. Det innebär att ändamålet aldrig får vara något annat än vad som följer av en rättslig grund, vilket också framgår av att ändamålet måste vara *berättigat*. Av 2 kap. 3 § följer även att det inte är tillräckligt om det på ett mer övergripande plan kan vara nödvändigt att bevara information om en viss person för att exempelvis upptäcka någon ännu inte konkretiserad brottslig verksamhet mot Sveriges säkerhet. Det krävs ett *särskilt, uttryckligt angivet*, ändamål med

denna behandling som måste vara mer konkret. För Säkerhetspolisens del handlar ändamålet för verksamheten i mycket stor utsträckning om att upptäcka brottslig eller säkerhetshotande verksamhet av visst slag. Det är därför naturligt att ändamålet uttrycks som en misstanke om att personen kan ha en koppling till brottslighet. Exempelvis att personen förekommer i ett sammanhang där terrorbrott planeras.

Av 3 kap. 3 § följer även att om det ändamål som gemensamt tillgängliga personuppgifter behandlas för inte framgår av sammanhanget eller på något annat sätt, ska det tydliggöras genom en särskild upplysning. Som framgår nedan, angående hur begreppet gemensamt tillgängliga uppgifter ska tolkas, innebär det i praktiken ett krav på dokumentation genom en särskild upplysning av det mer konkreta ändamålet för i princip alla personuppgifter som behandlas inom Säkerhetspolisen.

Skälet till att ändamålet ska vara särskilt uttryckt och dokumenterat är att det är av stor betydelse för andra bestämmelser i lagen. Av 2 kap. 8 § framgår att personuppgifter som behandlas ska vara *adekvata* och *relevanta* i förhållande till ändamålen med behandlingen. Där framgår också att inte fler uppgifter får behandlas än vad som är nödvändigt med hänsyn till ändamålen, vilket i dataskyddssammanhang brukar betecknas som principen om *uppgiftsminimering*. För att bedöma vilka uppgifter som är tillräckliga, adekvata och relevanta måste en prövning alltså ske mot det ändamål för vilket de ska behandlas.

Av 2 kap. 9 § framgår att *känsliga personuppgifter*, som avslöjar bland annat etniskt ursprung, eller politiska åsikter eller som utgör biometriska uppgifter, bara får behandlas om det är absolut nödvändigt för ändamålet med behandlingen. Denna prövning utgår ifrån att ändamålet med att behandla uppgifter om en viss person är tillräckligt konkret för att det ska gå att bedöma om en känslig personuppgift, om exempelvis etniskt ursprung, är absolut nödvändig att tillföra.

Av propositionen till säpodatalagen framgår att ändamålet inte får vara så vagt eller vittomfattande att någon prövning av adekvans, relevans, uppgiftsminimering och absolut nödvändighet i praktiken inte blir möjlig. Ett pågående underrättelsearbete om viss, närmare angiven brottslig verksamhet kan, enligt förarbetsuttalandet, utgöra ett ändamål. Regeringen konstaterade dock att eftersom Säkerhets-

polisens personuppgiftsbehandling till övervägande del utförs i myndighetens underrättelseverksamhet är det inte alltid möjligt att i ett tidigt stadium av processen ange ändamålen för behandlingen lika preciserat som i annan brottsbekämpande verksamhet. Inledningsvis kan därför ändamålen behöva anges mer övergripande för att sedan konkretiseras.[41] I praktiken tillämpar Säkerhetspolisen ändamålsbestämmelsen utifrån det ovan nämnda uttalandet i propositionen genom att det inledningsvis, då personuppgifter behandlas i en *särskild uppgiftssamling för bearbetning och analys*, som ändamål endast anges inom vilket verksamhetsområde uppgifterna behandlas. Allt eftersom uppgifterna bearbetas och analyseras förväntas ändamålet konkretiseras.

Ändamålsprincipen förutsätter att prövningar om personuppgifter är relevanta, adekvata, inte onödigt omfattande eller i fallet med känsliga personuppgifter att de är absolut nödvändiga, sker kontinuerligt och inför varje ytterligare behandling. När ursprungliga misstankar förstärks eller avtar ska alla personuppgifter prövas mot detta nya ändamål. På samma sätt ska ändamålsprövningen göras inför varje ytterligare behandling, exempelvis när uppgifter ska delas med andra. Det medför att bland annat att känsliga personuppgifter ska undantas från delning om de inte är absolut nödvändiga och att inte fler uppgifter ska ingå i överföringen än nödvändigt.

3.5.5 Känsliga personuppgifter

Uppgifter om etniskt ursprung, politiska åsikter, religiös övertygelse med mera

Som framgår i det föregående ställs särskilda krav på behandling av känsliga personuppgifter. Av 2 kap. 9 § första stycket framgår att personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning inte får behandlas. Av andra stycket följer att om uppgifter om en person behandlas får de dock kompletteras med sådana uppgifter om det är *absolut nödvändigt* för ändamålet med behandlingen. Motsvarande bestämmelser för andra brottsbekämpande myndigheter finns i brottsdatalagen.[42]

[41] Prop. 2018/19:163 s. 220.
[42] 2 kap. 11–12 §§ brottsdatalagen (2018:1177).

Kategorin av vilka uppgifter som ska anses särskilt känsliga har sitt ursprung i bland annat dataskyddskonventionen från 1981,[43] Den ursprungliga uppräkningen avsåg de uppgifter alla Europarådets medlemsstater kunde enas om som särskilt känsliga.[44] Den särskilda regleringen, som förekommer i all slags personuppgiftslagstiftning, syftar till att skydda de uppgifter som är särskilt känsliga ur integritetssynpunkt. Tillgången till sådana känsliga personuppgifter anses ge möjlighet till otillbörlig maktutövning mot enskilda och till att på olika sätt kränka en individs värdighet. En myndighet som har tillgång till känsliga personuppgifter kan också komma att misstänkliggöra individer på fördomsfulla grunder.[45] I 2 kap. 3 § regeringsformen finns förbudet mot att registreras i ett allmänt register enbart på grund av politisk åskådning.

Bestämmelserna om känsliga personuppgifter innebär att Säkerhetspolisen får behandla sådana uppgifter som anges i 2 kap. 9 § säpodatalagen endast om uppgifter om personen redan behandlas på någon annan grund och om behandlingen av de känsliga personuppgifterna är absolut nödvändig för ändamålet. Med hänsyn till den restriktivitet som ligger i uttrycket ”absolut nödvändigt” måste behovet av att göra sådana kompletteringar prövas noga i det enskilda fallet.[46]

Säkerhetspolisens uppdrag innebär att exempelvis islamistiska terrormiljöer eller våldsbejakande politisk extremism behöver kartläggas. Att känsliga personuppgifter om religiös övertygelse eller politiska åsikter i dessa fall registreras är nästan undantagslöst absolut nödvändigt för att kartlägga dessa miljöer. Undantagsregeln måste därför många gånger i praktiken tillämpas som en huvudregel, men kräver en motiverad prövning för varje enskild känslig personuppgift. Det finns däremot inte något utrymme för Säkerhetspolisen att exempelvis föra särskilda register över personer baserat på enbart de registrerades religiösa övertygelse. Känsliga personuppgifter om en person får endast tillföras andra uppgifter som behandlas för något ändamål.

[43] Europarådets konvention 108 om skydd för enskilda vid automatisk databehandling av personuppgifter.
[44] Europarådet, *Explanatory Report – ETS 108 – Automatic Processing of Personal Data (Convention)*, av den 28 januari 1981, p. 43.
[45] Europarådet, *Explanatory Report – CETS 223 – Automatic Processing of Personal Data (Amending Protocol)*, av den 10 oktober 2018, p. 55.
[46] Prop. 2018/19:163 s. 225.

Biometriska uppgifter

Av 2 kap. 10 § säpodatalagen framgår att Säkerhetspolisen får behandla biometriska uppgifter om det är absolut nödvändigt för ändamålet med behandlingen. Enligt samma bestämmelse får genetiska uppgifter inte behandlas.

Biometriska uppgifter tillfördes kategorin känsliga uppgifter genom EU:s dataskyddsförordning och brottsdatadirektivet. En biometrisk personuppgift avser en persons fysiska, fysiologiska eller beteendemässiga kännetecken. Det kan exempelvis röra sig om en persons utseende, fingeravtryck eller andra särskiljande detaljer i fysiologin. Av definitionen[47] framgår emellertid att en sådan uppgift inte utgör en biometrisk uppgift om den inte tagits fram genom särskild teknisk behandling som möjliggör eller bekräftar unik identifiering av en person. Det innebär att 2 kap. 10 § inte är tillämplig på exempelvis insamling och bevarande av bilder av ansikten som en analytiker använder för att jämföra manuellt. Däremot är den tillämplig på bearbetning och resultat av en datoriserad automatiserad ansiktsigenkänning. En biometrisk uppgift är nämligen resultatet av en automatisk process som mäter exempelvis ansiktsgeometri, fingeravtrycksmönster eller särskilda kännetecken i ögat. Även automatiska gångstilsanalyser från rörliga bilder eller röstanalys utgör biometriska uppgifter, trots att filmen eller ljudinspelningen alltså inte gör det. Det resultat som kommer från en särskild teknisk behandling består i normalfallet av ett resultat i form av bokstäver eller siffror som behöver tolkas genom en dator för att kunna användas. Uppgifter som kan vara föremål för en särskild teknisk behandling som avses i bestämmelsen, exempelvis fotografier eller fingeravtryck, brukar i stället betecknas biometriskt underlag och omfattas inte av någon särskild reglering.[48]

Biologiskt material från en människa, i form av exempelvis blod eller vävnadsprov, utgör också ett biometriskt underlag eftersom det går att använda för att genom en särskild form av dna-analys identifiera en person genom att ta fram en unik *dna-profil*. En dna-profil innehåller endast information om 15 så kallade STR-markörer, som är unika för en individ men inte förknippade med någon känd egenskap hos människan. Statistiskt är det i princip omöjligt att

[47] Se i 1 kap. 5 § säpodatalagen, som motsvarar artikel 3.13 i brottsdatadirektivet och artikel 4.14 i dataskyddsförordningen.
[48] Se prop. 2017/18:232 s. 86 och SOU 2023:32 s. 248 f.

samtliga 15 markörer från två prov skulle överensstämma om de inte har samma eller identiskt genetiska ursprung, varav det senare endast är fallet med enäggstvillingar. Den dna-profil som kan tas fram för att exempelvis knyta ett biologiskt spår från en brottsplats till en viss person utgör därmed en biometrisk uppgift.

Genetiska uppgifter

Med genetiska uppgifter avses enligt 1 kap. 5 § säpodatalagen personuppgifter som rör en persons nedärvda eller förvärvade genetiska kännetecken och som härrör från analys av ett spår av eller ett prov från personen. Säkerhetspolisen får enligt 2 kap. 10 § inte behandla genetiska uppgifter.

Från en standardiserad dna-profil som nämnts ovan kan inga nedärvda eller förvärvade kännetecken utläsas, då den endast består av en bokstavs- eller sifferkombination.[49] Förbudet avser därför inte behandling av dna-profiler. Förbudet mot behandling avser i stället uppgifter om exempelvis hårfärg eller uppgifter om en persons biogeografiska ursprung som kan tas fram efter en mer komplex analys än vad som krävs för en dna-profil. Förbudet för Säkerhetspolisen mot behandling av genetiska uppgifter avser att träffa sådana analyser. Motsvarande reglering finns för alla brottsbekämpande myndigheter, med undantag för Nationellt Forensiskt Centrum (NFC) inom Polismyndigheten och Rättsmedicinalverket. Forensiska analyser, undersökningar eller jämförelser utförs av NFC, på uppdrag av bland annat Säkerhetspolisen. NFC får då behandla genetiska uppgifter om det är absolut nödvändigt för ändamålet med behandlingen.[50]

Genetiska uppgifter är mycket strängt reglerat i Sverige. Utöver att uppgifterna är förbjudna att behandla är även definitionen av vad som utgör en genetisk uppgift betydligt bredare i brottsdatalagen och säpodatalagen än i det EU-direktiv som utgör förlaga. I brottsdatadirektivet krävs dels att det genetiska kännetecknet ger ”unik information” dels att det ska avse en persons ”fysiologi eller

[49] Se definitionen i 1 kap. 5 § polisens brottsdatalag. Sedan en tid tillbaka ingår emellertid även en 16 markör (kallad Amelogenin) i de dna-profiler som används inom polisen. Denna markör avslöjar könet hos den person som profilen avser, vilket skulle kunna tolkas som ett genetiskt kännetecken hos individen.
[50] Se 6 kap. 4–5 §§ lag (2018:1693) polisens brottsdatalag.

hälsa”. En genetisk uppgift i de svenska lagstiftningarna omfattar å andra sidan alla genetiska kännetecken, det vill säga även de som inte ger unik information för varje person och även sådana som avser annat än fysiologi eller hälsa. Skälet till detta är att regeringen ansåg att även andra uppgifter, som exempelvis en persons biogeografiska ursprung, som kan tas fram genom motsvarande analys förtjänade samma skydd som fysiologiska uppgifter om bland annat hud- eller hårfärg. Däremot finns inget motiv till varför den svenska definitionen innebär en överimplementering som omfattar alla kännetecken, även sådana som inte är unika för en person. Vid sidan av att i princip alla brottsbekämpande myndigheter är förbjudna att behandla genetiska uppgifter träffar följaktligen förbudet även fler uppgifter än vad som följer av brottsdatadirektivet.

Behandling av känsliga personuppgifter genom sökning i syfte att få fram ett urval av personer

Ett av de få undantag från säpodatalagens behandlingsneutrala utformning återfinns i 2 kap. 12 §. Där anges, i första stycket, att det är förbjudet att *utföra sökningar* i syfte att få fram ett urval av personer grundat på känsliga personuppgifter. I andra stycket förklaras att brottsrubriceringar, uppgifter om tillvägagångssätt vid brott eller uppgifter som beskriver en persons utseende inte ska utgöra hinder mot sökning även om det innefattar känsliga personuppgifter. Av tredje stycket framgår de undantag från förbudet som är särskilt anpassade för Säkerhetspolisens verksamhet: Sökningar i syfte att få fram ett urval av personer grundat på etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller uppgifter som rör hälsa, sexualliv eller sexuell läggning får göras om sökningen är absolut nödvändig för någon av de rättsliga grunder som anges i 2 kap. 1 §.

Undantaget från förbudet omfattar inte alla känsliga personuppgifter i 2 kap. 9 §. Uppgifter om ras och medlemskap i fackförening får nämligen inte alls användas som sökbegrepp[51] och det finns inte heller något undantag avseende biometriska uppgifter. När det kommer till ansiktsigenkänning genom särskild teknisk behandling ansåg

[51] Detta motiverades av det inte finns någon vetenskaplig grund för att dela in människor i skilda raser och att Säkerhetspolisen inte hade något behov av att göra sökningar på medlemskap i fackföreningar, prop. 2018/19:163 s. 80.

regeringen att det skulle vara tillåtet under förutsättning att syftet inte var att få fram ett urval av personer. Regeringen ansåg nämligen att behandling av en ansiktsbild i ett ansiktsigenkänningsprogram, inte utgjorde sökning i syfte att få fram ett visst personurval, även om det resulterade i en träfflista med flera möjliga kandidater. Trots att det skulle kunna hävdas att resultatet blir just ett personurval grundat på biometriska uppgifter ansåg regeringen att det i dessa fall är fråga om normal behandling av biometriska uppgifter som är tillåtet enligt 2 kap. 10 § om det är absolut nödvändigt.[52]

Den 1 juli 2025 träder emellertid en ny lag i kraft som ger Säkerhetspolisen möjlighet att utföra sökningar för att få fram ett urval av personer grundat på biometriska uppgifter i nya så kallade biometriregister.[53] Lagen innebär att tre nya biometriregister, ett över misstänkta, ett över dömda och ett över spår, ska föras av Polismyndigheten. Registren ska innehålla bland annat biometriska uppgifter och biometriskt underlag för att kunna identifiera personer med hjälp av biometrisk analys. De nya biometriregistren ersätter de nuvarande register som förs över dna-profiler, fingeravtryck och signalement.

Säkerhetspolisen ska enligt lagförslaget, genom direktåtkomst, få utföra sökningar i Polismyndighetens biometriregister i syfte att få fram ett urval av personer grundat på biometriska uppgifter, om det är absolut nödvändigt för ändamålet.

3.5.6 Särskilda upplysningar för gemensamt tillgängliga personuppgifter

Uppgifter som endast ett fåtal personer har rätt att ta del av

Enligt 3 kap. 1 § säpodatalagen är uppgifter som endast ett fåtal personer har rätt att ta del av inte att anse som gemensamt tillgängliga. Lagen innehåller i vissa avseenden olika regleringar för personuppgifter som endast ett fåtal personer har rätt att ta del och för sådana uppgifter som är gemensamt tillgängliga för en vidare krets medarbetare vid myndigheten. Inom vilken kategori personuppgifterna hänför sig påverkar bland annat kravet på särskilda upplysningar, behandlingstiden och om de får delas med mottagare utanför myn-

[52] Se prop. 2018/19:163 s. 80 och SOU 2017:74 s. 630, jfr dock SOU 2023:32 s. 395.
[53] Prop. 2024/25:37, bet. 2024/25:JuU18.

digheten genom direktåtkomst. Syftet med att särreglera uppgifter som en vidare krets har tillgång till är att risken för otillbörliga intrång i den personliga integriteten anses större när personuppgifter används av flera gemensamt i verksamheten än när personuppgifter behandlas av endast enstaka eller ett fåtal personer.[54]

Begreppet gemensamt tillgängliga personuppgifter infördes genom 2010 års polisdatalag för att avgränsa personuppgiftsbehandling där mer begränsande regler ansågs nödvändiga. I tidigare lagstiftningar hade begreppen register och databas använts för att definiera de uppgifter som gjorts tillgängliga för en större krets. Till de olika registerna fanns särskilda regler om bland annat innehåll, åtkomst och sökmöjligheter. I 2010 års polisdatalag övergavs register- och databasbegreppen för ett mer teknikneutralt begrepp som bättre skulle spegla datoriserad informationshantering. Skälet var att det inte längre är nödvändigt att strukturera och organisera information på ett visst sätt i en databas för att kunna hantera den effektivt. Begreppet gemensamt tillgängliga uppgifter infördes därför för att tydliggöra att det var den faktiskt åsyftade tillgängligheten som var väsentligt och inte på vilket sätt uppgifter tekniskt lagras.

Gemensamt tillgängliga uppgifter är ett rättsligt begrepp och därför teknikneutralt. Att en uppgift är tillgänglig för en person innebär att denna har såväl faktisk möjlighet som rättslig behörighet att ta del av uppgiften. Det spelar i sammanhanget inte någon roll om personen utnyttjar sin behörighet och faktiskt tar del av uppgiften. Att uppgifter som finns tillgängliga för hela eller stora delar av myndigheten är gemensamma råder det ingen tvekan om. Även om endast en bestämd och avgränsad personkrets har tillgång till uppgifterna innebär det dock att uppgifterna ska omfattas av begreppet gemensamt tillgängliga, om denna personkrets är tillräckligt stor. I propositionen till 2010 års polisdatalag angavs som tumregel att uppgifter i polisens verksamhet normalt bör anses som gemensamt tillgängliga när fler än ett tiotal personer har tillgång till dem. Om det står klart att det rör sig om uppgifter som kommer behandlas under lång tid ansåg regeringen att uppgifterna redan av det skälet ska anses som gemensamma. Det följer av att den mindre personkrets som har tillgång till uppgifterna kan komma att bytas ut efterhand. Regeringen uttalade även att personuppgifter alltid

[54] Prop. 2009/10:85 s. 125 och 263 samt prop. 2018/19:163 s. 87.

ska anses vara gemensamt tillgängliga om syftet är att de ska vara åtkomliga för en i förväg obestämd krets av anställda eller där det inte på förhand har bestämts vilka personer som får ha tillgång. Att olika personalkategorier kan ha olika behörighet, och att en uppgift därför i praktiken vid en viss tidpunkt är åtkomlig enbart för ett begränsat antal personer, innebär alltså inte att uppgiften inte kan anses vara gemensamt tillgänglig.[55] Förarbetsuttalandena från 2010 års polislag angående gemensamt tillgängliga uppgifter ansågs fortfarande vara aktuella när säpodatalagen beslutades. De tidigare reglerna infördes därför med likartad lydelse utan att någon förändring i sak var avsedd i detta avseende.[56]

Alltjämt omfattar begreppet gemensamt tillgängliga uppgifter därmed alla uppgifter som fler än ett fåtal har eller kan komma att få åtkomst till över tid. När det kommer till antalet personer som ska anses utgöra ett fåtal har Säkerhetspolisen att förhålla sig till förarbetsuttalandet om ”ett tiotal personer” och Säkerhets- och integritetsskyddsnämndens uttalanden i frågan. Gränsdragningsfrågor om vad som kan anses vara gemensamt tillgängliga uppgifter och inte har vid flertalet tillfällen varit föremål för nämndens tillsyn. Frågan har bedömts med hänsyn till omständigheterna i det enskilda fallet och med beaktande av nämnda förarbetsuttalanden.[57]

Nedan redogörs för den särskilda reglering som gäller gemensamt tillgängliga uppgifter.

Särskilda upplysningar om ändamål med behandlingen

Som framgår ovan får personuppgifter, enligt 2 kap. 3 § säpodatalagen, endast behandlas för särskilda, uttryckligt angivna och berättigade ändamål. Av 3 kap. 3 § följer att om det ändamål som de gemensamt tillgängliga personuppgifterna behandlas för inte framgår av sammanhanget eller på något annat sätt, ska det tydliggöras genom en särskild upplysning.

Bestämmelsen har sitt ursprung i det krav på att grunder för registrering skulle anges för uppgifter som fördes in i det så kallade SÄPO-registret, som reglerades i den äldre polisdatalagen. Den

[55] Prop. 2009/10:85 s. 128 f., 264 och 334.
[56] Prop. 2018/19:163 s. 87.
[57] Se Säkerhets- och integritetsskyddsnämndens uttalande i dnr 137-2017, 38-2017 samt 197-2016.

nuvarande bestämmelsen i 3 kap. 3 § säpodatalagen innebär att en särskild upplysning om ändamål måste införas manuellt för alla de personuppgifter som Säkerhetspolisen behandlar, om det inte framgår av sammanhanget. När ytterligare uppgifter tillförs redan kända personer kan ändamålet i många fall framgå av sammanhanget. När det däremot handlar om ostrukturerad information, som Säkerhetspolisen inhämtar genom exempelvis beslag eller hemliga tvångsmedel, handlar det om ett mycket omfattande arbete att särskilja det mer konkreta ändamålet för uppgifter som hör till olika individer. Vissa uppgifter kan vara relevanta för ett visst ändamål, då de exempelvis har koppling till ett befarat terrordåd som planeras i någon viss miljö. Andra uppgifter kan i och för sig vara relevanta för underrättelseverksamheten, exempelvis angående den misstänktes kontakter inom en extremistisk miljö, men kan inte direkt kopplas till det ursprungliga ärendet. Sådana uppgifter, som kan vara relevanta för att kartlägga misstankar om annan brottslig verksamhet, behöver regelmässigt förses med en särskild upplysning om ändamål.

Särskild upplysning om misstanke, trovärdighet och sakriktighet

Av 3 kap. 4 § första stycket säpodatalagen framgår att om uppgifter som har gjorts gemensamt tillgängliga direkt kan hänföras till en person som inte är misstänkt för brott eller för att ha utövat eller komma att utöva brottslig verksamhet som faller inom Säkerhetspolisens ansvarsområde, ska det genom en särskild upplysning eller på något annat sätt framgå att personen inte är misstänkt. Första stycket av paragrafen innebär att det genom en så kallad misstankemarkering måste framgå om en person är exempelvis en uppgiftslämnare och alltså inte föremål för Säkerhetspolisens intresse på grund av inblandning i brottslig verksamhet.

Bestämmelsen motiveras av att det är av stor betydelse för skyddet av den personliga integriteten vid brottsbekämpning att personuppgifter behandlas på ett sådant sätt att det framgår om personen är misstänkt eller inte. Särskilt i underrättelseverksamhet kan en persons roll vara otydlig och den särskilda upplysningen är avsedd att tydliggöra detta när uppgiften används utanför sitt sammanhang. Kravet gäller endast om det inte finns några som helst misstankar mot den aktuella personen avseende brottslighet inom Säkerhets-

polisens ansvarsområde. Förekommer det någon form av misstanke – vare sig det handlar om skälig misstanke eller om någon annan misstankegrad – behöver någon upplysning inte lämnas.[58] I de fall det inte går att precisera någon brottslig verksamhet inom Säkerhetspolisens ansvarsområde bör personen märkas som inte misstänkt även om personen är misstänkt för någon annan brottslighet. Upplysningen om huruvida personen är misstänkt eller inte tar endast sikte på den brottsliga verksamhet som undersöks.[59]

Av bestämmelsens andra stycke framgår att uppgifter om en person som kan antas ha direkt samband med brottslig verksamhet ska förses med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak, om det inte på grund av omständigheterna är onödigt. En sådan upplysning anses dels stärka skyddet för den enskildes integritet, dels förhindra att uppgifter, vilkas tillförlitlighet och trovärdighet är begränsad, läggs till grund för bedömningar och åtgärder som inte är sakligt motiverade. Reglerna om särskild misstankemarkeringen och trovärdigs- och sakriktighetsbedömning är i princip desamma för Säkerhetspolisen som för Polismyndigheten.[60]

Kravet om särskild upplysning om trovärdighet och sakriktighet behövs endast om det inte på grund av omständigheterna är onödigt. Med det avses exempelvis uppgifter som lämnats av en polisman vars trovärdighet redan är känd. Det finns dock ytterligare ett undantag. Av 3 kap. 4 § tredje stycket följer nämligen att sådan särskild upplysning inte behöver lämnas om uppgifterna ingår i en *uppgiftssamling för att bearbeta och analysera* information och någon bearbetning inte har genomförts. Undantaget för uppgifter som genomgår bearbetning är tänkt att möjliggöra att uppgifter kan göras gemensamt tillgängliga inom Säkerhetspolisen i brådskande fall även utan särskild upplysning om trovärdighet och sakriktighet.

Undantaget har motiverats med att Säkerhetspolisen ibland måste kunna reagera snabbt på händelseutvecklingen och att Säkerhetspolisens personal är van vid att hantera svårbedömd information. Risken för felbedömningar har därför ansetts liten och vid intresseavvägningen mellan verksamhetens behov och enskildas

[58] Prop. 2009/10:85 s. 340 och 370.
[59] Se Säkerhets- och integritetsskyddsnämndens uttalande den 17 februari 2016, dnr 50-2015 och den 14 juni 2018, dnr 197-2017.
[60] Se 3 kap. 4 § polisens brottsdatalag.

integritet ansågs verksamhetsintresset väga tyngre.[61] Så snart bearbetningen är genomförd och uppgifterna kopplats till annan information måste personuppgifterna dock kompletteras med sådana upplysningar, om det behövs.

3.5.7 Längsta tid för personuppgiftsbehandling

Huvudregeln

Hur länge Säkerhetspolisen får behandla personuppgifter regleras i 4 kap. säpodatalagen. 1 § innehåller en allmän bestämmelse om att personuppgifter inte får behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Denna bestämmelse gäller all personuppgiftsbehandling, oavsett om det rör sig om behandling på papper eller i automatiserade system. Motsvarande bestämmelser utgör ett grundläggande krav i många dataskyddsregelverk och bygger vidare på principen om behov, adekvans och relevans. Om uppgiften inte längre behövs eller inte längre är adekvat eller relevant för det ändamål som det ursprungligen behandlats för, ska den inte längre behandlas.

Huvudregeln om längsta tid för behandling har med vissa förändringar överförts från 2010 års polisdatalag. I polisdatalagen angavs att personuppgifter inte får bevaras under längre tid än vad som behövs för något eller några av de i lagen angivna ändamålen. Även om det i förarbetena till säpodatalagen anfördes att någon ändring i sak inte var avsedd har bestämmelsen i säpodatalagen en väsentligt annan innebörd än den tidigare.

De primära ändamål som polislagens bestämmelse hänvisade till är nämligen det som i säpodatalagen benämns som rättslig grund. I polisdatalagen var det därmed inte behovet att bevara personuppgifterna för det särskilda och uttryckligt angiva ändamålet som var styrande. Avgörande var i stället om uppgiften behövdes för att lösa någon av Säkerhetspolisens mer övergripande brottsbekämpande uppgifter. Säpodatalagens bestämmelse tar i stället sikte på det eller de särskilda ändamål som uppgiften behandlas för, som ska anges med en betydligt högre grad av konkretion.

[61] SOU 2017:74 s. 641 f.

Behandlingstider för automatiserad behandling

För automatiserad behandling av personuppgifter finns kompletterande bestämmelser. Om uppgiften inte är gemensamt tillgänglig får den, enligt 4 kap. 2 § säpodatalagen, behandlas i ett år efter att ärendet avslutats eller från det att den registrerats, om uppgiften inte behandlas i ett ärende. Denna bestämmelse har ingen större praktisk betydelse för Säkerhetspolisen som behandlar i princip alla uppgifter som gemensamt tillgängliga.

Av huvudsakligt intresse är därför de regler om längsta tid för behandling för uppgifter som behandlas automatiserat och är gemensamt tillgängliga. Det finns särskilda regler för längsta behandlingstid för personuppgifter som behandlas i ärenden om utredning av eller lagföring för brott.

Enligt 4 kap. 3 § får personuppgifter i en brottsanmälan som inte lett till en förundersökning behandlas till dess att åtalspreskription inträtt. Om skälet till att förundersökning inte inletts är att den påstådda gärningen inte utgör brott får uppgifter från anmälan dock inte längre behandlas enligt säpodatalagen. Enligt 4 kap. 4 § får personuppgifter i förundersökningar som längst behandlas i fem år från det att dom vunnit laga kraft eller förundersökningen lagts ner. Dessa särskilda bestämmelser avser personuppgifter som förekommer i vissa ärenden och alltså inte personuppgifter som behandlas för vissa ändamål. Regleringen har i princip ordagrant överförts från 2010 års polisdatalag.[62] Redan i den tidigare polisdatalagen från 1998 fanns regler om fortsatt behandling av uppgifter om kvarstående misstankar efter att en förundersökning lagts. Dessa regler gällde dock inte Säkerhetspolisen.[63]

Med hänsyn till Säkerhetspolisens uppdrag och verksamhet är reglerna i 4 kap. 7–10 §§ säpodatalagen av störst intresse. De gäller hur länge andra personuppgifter än de som finns i en brottsanmälan eller i en förundersökning får behandlas. Det finns tre huvudsakliga behandlingstider för uppgifter som används i underrättelseverksamheten. Huvudregeln, i 4 kap. 7 § är att uppgifter inte får behandlas längre än tio år efter utgången av det kalenderår då den senaste registreringen gjordes avseende personen. Om uppgiften avser en person som är under 18 år vid registreringstillfället, gäller dock en

[62] 3 kap. 9–12 §§ och 6 kap. 13 § polisdatalagen (2010:361).
[63] 10–12 §§ polisdatalagen (1998:622).

behandlingstid om fem år. För personuppgifter som registreras inom kontraspionaget gäller enligt 4 kap. 9 § en längsta behandlingstid om 40 år efter den senaste registreringen avseende personens anknytning till brott eller brottslig verksamhet. Denna behandlingsfrist gäller personuppgifter som hänför sig till sådan säkerhetshotande verksamhet som avses i 18 och 19 kap. brottsbalken och som utövas av främmande makt.

Vid sidan av dessa generella bestämmelser finns en särskild reglering, i 4 kap. 8 §, avseende uppgiftssamling för bearbetning och analys. För uppgifter i sådana uppgiftssamlingar gäller en behandlingsfrist om tre år efter den senaste registreringen avseende personen.

I 4 kap. 10 § finns regler om att Säkerhetspolisen, om det finns särskilda skäl, får besluta att förlänga behandlingstiden om uppgifterna fortfarande behövs för det ändamål som de behandlas för. Denna möjlighet är dock begränsad till de behandlingstider som avses i 7–9 §§ och omfattar därmed inte personuppgifter som finns i en nedlagd förundersökning.

Kontinuerlig behovsprövning

Av huvudregeln framgår att inga personuppgifter får behandlas under längre tid än vad som är nödvändigt för ändamålet. Därutöver gäller särskilda regler om längsta behandlingstid för uppgifter som behandlas automatiserat. Bestämmelser om längsta behandlingstid är, vilket framgår direkt av 4 kap. 1 § tredje stycket säpodatalagen, en ytterligare begränsning i förhållande till huvudregeln.

Det innebär, vilket nyligen slagits fast i ett uttalande från Säkerhets- och integritetsskyddsnämnden,[64] att Säkerhetspolisen kontinuerligt måste pröva om behovet av uppgifterna som behandlas alltjämt kvarstår. Om det inte längre finns ett behov av uppgifterna ska behandlingen avslutas, även om de yttersta tidsfrister som följer av lag inte har överskridits. I tillsynsärendet menade Säkerhetspolisen att myndigheten i regel har behov av att behandla alla personuppgifter fram till dess att de lagstadgade tidsfristerna för längsta tid för behandling faller ut. Nämnden ansåg dock att prövningen av behovet av uppgifterna ska prövas mot ändamålet för

[64] Säkerhets- och integritetsskyddsnämndens uttalande med beslut den 12 december 2023, *Säkerhetspolisens tillämpning av den allmänna bestämmelsen om längsta tid för behandling (s.k. behovsgallring) av personuppgifter i det centrala underrättelsesystem*, dnr 160-2022.

behandlingen i det enskilda fallet trots att någon tidsfrist för längsta tid för behandling inte passerats.

Nämnden riktade kritik mot Säkerhetspolisens tillämpning av lagen, som innebär att behovet av uppgifterna endast prövas när de först registreras samt inför att tidsfristen löper ut, i syfte att bedöma om det finns skäl att fatta ett beslut om förlängd behandlingstid. Nämnden hade förståelse för Säkerhetspolisens uppfattning att det i många fall är nödvändigt att behandla uppgifter under hela den lagstadgade tidsfristen, men att detta förutsätter att Säkerhetspolisen i vart fall med viss regelbundenhet under tidsperioden prövar behovet av uppgifterna. Säkerhets- och integritetsskyddsnämnden bedömde att Säkerhetspolisen vid tillsynen inte uppfyllde kravet i 4 kap. 1 § första stycket säpodatalagen på att kontinuerligt pröva det fortsatta behovet av att behandla personuppgifter. Nämnden poängterade att detta är särskilt anmärkningsvärt mot bakgrund av att Säkerhetspolisen tillåts registrera uppgifter i ett mycket tidigt skede och därefter behandla uppgifterna under lång tid.

När det gäller behandlingsfrister är säpodatalagen till sin utformning snarlik sin föregångare polisdatalagen. Eftersom kontinuerlig behovsprövning bygger på huvudregeln i 4 kap. 1 § säpodatalagen kvarstår emellertid den skillnad som redogjorts för i inledningen av detta avsnitt. Enligt polisdatalagen prövades behovet av fortsatt behandling mot det som motsvaras av säpodatalagens rättsliga grunder. Enligt säpodatalagen ska behovet däremot prövas mot det specifika, konkretiserade ändamålet, till exempel särskilda misstankar eller ett visst underrättelseärende.

Utredningen som bland annat lämnade förslag till säpodatalag föreslog en bestämmelse som motsvarade den tidigare, vilket innebar att behovet av att behandla en uppgift under behandlingstiden skulle bedömas efter uppgiftens allmänna värde för Säkerhetspolisens verksamhet.[65] Det var Säkerhetspolisen som föreslog att säpodatalagen skulle få den mer begränsande regleringen, som även gäller enligt brottsdatalagen.[66] Av den lydelse som slutligen kom att införas framgår att fortsatt behandling ska prövas mot ett specifikt ändamål och inte en rättslig grund.[67]

[65] Se SOU 2017:74 s. 801.
[66] Se prop. 2018/19:163 s. 118.
[67] Ibid. s. 235.

3.5.8 Enskildas rättigheter

Rätt till insyn, rättelse, radering och skadestånd enligt säpodatalagen

I 6 kap. säpodatalagen finns ett relativt omfattande regelverk som avser enskildas rättigheter. Dessa rättigheter omfattar bland annat rätten för en enskild att få besked om och i så fall vilka personuppgifter behandlas, varifrån dessa uppgifter kommer och till vem uppgifterna har lämnats ut, inom eller utom landets gränser. Vidare finns en rätt att på begäran få sina personuppgifter rättade eller kompletterade om de är felaktiga eller ofullständiga med hänsyn till ändamålet med behandlingen. Slutligen ska Säkerhetspolisen på begäran av den registrerade utan onödigt dröjsmål radera personuppgifter som rör honom eller henne, om de behandlas i strid med bland annat reglerna om ändamål och längsta behandlingstid.

När det gäller rätten till information om vilka personuppgifter som behandlas anges i 6 kap. 3 § att den inte gäller i den utsträckning det är särskilt föreskrivet i lag eller annan författning att uppgifter inte får lämnas ut till den registrerade. Rätten till information begränsas därmed av offentlighets- och sekretesslagen.

Säkerhetspolisens verksamhet omfattas i stor utsträckning av sekretess. Enligt 18 kap. 2 § offentlighets- och sekretesslagen gäller sekretess för uppgift som hänför sig till Säkerhetspolisens verksamhet att förebygga, förhindra och upptäcka brottslig verksamhet. Denna, så kallade underrättelsesekretess gäller, i högst 70 år, om det inte står klart att uppgiften kan röjas utan att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas.

Rätten till information infördes för första gången genom 1998 års polisdatalag, genom att den absoluta sekretessen för bland annat uppgifter i SÄPO-registret då avskaffades. Det konstaterades dock att det ligger i underrättelseverksamhetens natur att det endast i speciella fall kan komma i fråga att lämna ut uppgifter som hör till denna verksamhet. Det innebär att även uppgifter om att en person inte förekommer som regel omfattas av underrättelsesekretess.[68] En enskild har alltjämt små möjligheter att praktiskt utnyttja sin rätt till insyn, i vart fall när det kommer till information som behandlats

[68] Se prop. 1997/98 s. 68 och RÅ 2000 ref. 15.

inom underrättelseverksamheten. Det gäller oavsett om det avser en begäran om utlämnande av allmän handling, enligt 2 kap. tryckfrihetsförordningen, eller insyn i personuppgiftsbehandling, enligt 6 kap. 3 § säpodatalagen.

Enligt 8 kap. 1 § säpodatalagen ska Säkerhetspolisen ersätta den skada och kränkning av den personliga integriteten som orsakats av behandling av personuppgifter som sker i strid med säpodatalagen. Denna specialreglering tar över skadeståndslagens bestämmelser om det allmännas ansvar. Bestämmelsen ger rätt till ersättning inte endast för till exempel ren förmögenhetsskada utan även för den ideella skada som kränkningen av den personliga integriteten kan medföra.[69]

Indirekt insyn

Den omfattande sekretessen som omgärdar Säkerhetspolisens verksamhet innebär i praktiken mycket begränsade möjligheter för enskilda att bedöma om en personuppgiftsbehandling inneburit en rättighetskränkning. Eftersom det ofta saknas full insyn i behandlingen är det även svårt att vidta åtgärder för rättelse eller kompensation. I syfte att skapa ett fristående och självständigt organ som säkerställer rätten till effektivt rättsmedel, som den garanteras i artikel 13 i Europakonventionen, inrättades år 2008 Säkerhets- och integritetsskyddsnämnden.

Vid sidan av sina andra tillsynsuppgifter (se nedan) har nämnden till uppdrag att på begäran av enskild kontrollera om han eller hon varit föremål för personuppgiftsbehandling av Säkerhetspolisen och om den har utförts i enlighet med lag eller annan författning. Sådan kontroll kan ske utan hinder av sekretess. Däremot kan sekretessen medföra att resultatet av kontrollen inte kan lämnas ut till den enskilde. En kontroll på begäran av enskild som inte varit föremål för någon personuppgiftsbehandling alls kommer därför som regel resultera i samma besked från nämnden som en begäran av en person vars uppgifter har behandlat på ett korrekt sätt.

Om nämnden uppmärksammar felaktigheter vid en kontroll som kan medföra skadeståndsansvar för staten gentemot en enskild, ska nämnden anmäla det till Justitiekanslern. Om Justitiekanslern

[69] Prop. 2018/19:163 s. 257.

finner att det som har förekommit kan föranleda skadeståndsansvar, ska Justitiekanslern bereda den som berörs tillfälle att framställa skadeståndsanspråk mot staten. Förhållanden som kan utgöra brott ska anmälas till Åklagarmyndigheten eller annan behörig myndighet.[70]

3.5.9 Tillsyn

Allmänt om tillsynen över Säkerhetspolisens personuppgiftsbehandling

Tillsynen över Säkerhetspolisens behandling av personuppgifter enligt säpodatalagen utövas av både Integritetsskyddsmyndigheten och Säkerhets- och integritetsskyddsnämnden. Den parallella tillsynen motiverades bland annat av att två tillsynsmyndigheter med olika uppdrag och fokus kan komplettera och förstärka varandra. Det ansågs särskilt värdefull i Säkerhetspolisens verksamhet som omfattas av stark sekretess och där allmänheten och enskilda har begränsad insyn.[71]

Integritetsskyddsmyndighetens tillsyn regleras i 7 kap. säpodatalagen. För nämndens motsvarande tillsyn gäller i huvudsak lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet (tillsynslagen).

Säkerhets- och integritetsskyddsnämnden

En myndighet under regeringen med en stark parlamentarisk anknytning

Säkerhets- och integritetsskyddsnämnden består av högst tio ledamöter som samtliga utses av regeringen för en bestämd tid, dock högst fyra år. Ordföranden och vice ordföranden ska vara eller ha varit ordinarie domare eller ha annan motsvarande juridisk erfarenhet. De övriga, högst åtta, ledamöterna ska utses bland sådana personer som har föreslagits av partigrupperna i riksdagen.

Nämndens sammansättning är motiverad av att ett organ av detta särskilda slag bör representera allmänheten och garantera en med-

[70] 20 § förordningen (2007:1141) med instruktion för Säkerhets- och integritetsskyddsnämnden.
[71] Prop. 2018/19:163 s. 168–170.

borgerlig insyn i verksamheten. Att de folkvalda i riksdagen lämnar förslag till ledamöter i nämnden ansågs vara det bästa sättet att åstadkomma sådan medborgerlig insyn. Trots att riksdagens partigrupper därmed har ett starkt inflytande över dess sammansättning utgör inte nämnden ett parlamentariskt organ, utan är en myndighet under regeringen. Nämndens starka parlamentariska anknytning följer dock av att den inrättats genom lag, av vilken även nämndens sammansättning och tillsynsuppgifter framgår.[72]

Nämndens tillsyn

Enligt tillsynslagen ska nämnden utöva tillsyn bland annat över de brottsbekämpande myndigheternas användning av hemliga tvångsmedel och användning av kvalificerade skyddsidentiteter samt Polismyndighetens, Säkerhetspolisens och Ekobrottsmyndighetens behandling av personuppgifter inom brottsbekämpningen.

Nämnden ska utöva sin tillsyn genom inspektioner och andra undersökningar och har omfattande undersökningsbefogenheter. Enligt 4 § tillsynslagen har nämnden rätt att få de uppgifter och upplysningar, den information och det biträde som nämnden begär från den myndighet som tillsynen avser. Dessutom har även domstolar och andra myndigheter som inte omfattas av tillsynen en skyldighet att lämna nämnden de uppgifter som den begär.

Nämnden får, enligt 2 § tillsynslagen, uttala sig om förhållanden som den konstaterat vid en inspektion eller annan undersökning och om sin uppfattning om behov av förändringar i den verksamhet som tillsynen avser. Nämnden har även till uppgift att verka för att brister i lag eller annan författning avhjälps.

Nämndens rekommendationer är inte bindande och kan inte överklagas. Däremot har nämnden, enligt sin instruktion, en skyldighet att anmäla förhållanden som kan utgöra brott till åklagare samt att anmäla sådana brister i personuppgiftsbehandlingen som kan aktualisera korrigerande befogenheter till Integritetsskyddsmyndigheten.

Till skillnad från många andra tillsynsmyndigheter har nämnden inte till uppgift att utreda anmälningar och nämnden får sällan in tips om eventuella felaktigheter. Nämnden måste därför i regel själv

[72] Prop. 2006/07:133 s. 64 f.

komma fram till vad som bör granskas och hur det ska göras. Urvalet sker främst utifrån en bedömning av var risken för felaktig rättstillämpning är som störst eller där nya system eller ny lagstiftning börjat tillämpats. Av tillsynslagen följer även att tillsynen avseende personuppgiftsbehandling särskilt ska avse behandling av känsliga personuppgifter.

Nämnden använder sig i huvudsak av en så kallad tematisk tillsynsmetodik. Vid den tematiska tillsynen analyseras först gällande författningar och tillsynsobjektens interna föreskrifter. Därefter undersöks rutiner och praktisk tillämpning. Tillsynen bedrivs genom bland annat inspektioner på plats hos Säkerhetspolisen och skrivbordsgranskningar.

Ett initiativärende inleds vanligen genom att myndighetens kansli upprättar ett skriftligt förslag till granskning, som innehåller uppgifter om genomförande, hur lång tid granskningen kan förväntas ta, relevanta författningar och frågeställningar. På grundval av förslaget fattar nämnden sitt beslut om att inleda viss tillsyn. När nämnden har beslutat att inleda ett initiativärende är det tjänstemän vid kansliet som utför själva granskningen. Många initiativärenden innefattar en eller flera inspektioner. Ofta måste skriftliga frågor ställas till den granskade myndigheten för att klarlägga de närmare förhållandena. Kansliet upprättar därefter ett förslag till uttalande som presenteras vid nämndens sammanträde, innan nämnden därefter fattar beslut i ärendet.[73]

Nämnden har, som tidigare nämnts en skyldighet att på begäran av enskild kontrollera lagligheten av eventuell hemlig tvångsmedelsanvändning och personuppgiftsbehandling som den enskilde varit föremål för. Nämndens tillsynsverksamhet kan därmed sägas bestå av två ärendetyper: initiativärenden och kontrollärenden. Av tillsynskapaciteten fördelas ungefär hälften på egeninitierade tillsynsärenden och hälften på att utföra kontroller på begäran av enskild. Trenden är att alltmer resurser krävs för att uppfylla nämndens uppdrag avseende kontrollärenden, vilka blivit alltmer omfångsrika och komplexa till sin natur.

[73] Se Säkerhets- och integritetsskyddsnämnden, *Årsredovisning 2023,* dnr 168-2023, s. 6 f.

Integritetsskyddsmyndigheten

I förhållande till Säkerhets- och integritetsskyddsnämndens mer specialiserade uppdrag har Integritetsskyddsmyndigheten fler uppgifter och utövar en generell tillsyn personuppgiftsbehandling.

Av 7 kap. 1 § säpodatalagen framgår att Integritetsskyddsmyndigheten ska utöva allmän tillsyn över personuppgiftsbehandling, och vid förhandssamråd och när det i övrigt är påkallat, ge råd och stöd till Säkerhetspolisen.

Integritetsskyddsmyndigheten har vid sin tillsyn, enligt 7 kap. 3 § säpodatalagen, bland annat rätt att få tillgång till alla personuppgifter som behandlas, till utrustning och andra medel för behandling av dessa, tillträde till lokaler och den hjälp och den information som behövs för tillsynen.

Integritetsskyddsmyndigheten ges vidare, i 7 kap. 4 §, förebyggande befogenheter, som innebär att myndigheten genom råd, rekommendationer och påpekanden ska försöka förmå Säkerhetspolisen att motverka risker för att personuppgifter behandlas felaktigt. Integritetsskyddsmyndigheten kan även utfärda en skriftlig varning för att planerad eller pågående personuppgiftsbehandling riskerar att stå i strid med lag eller annan författning. Att Integritetsskyddsmyndigheten kan utfärda råd även för planerade behandlingsåtgärder hör samman med den skyldighet som Säkerhetspolisen har att, enligt 5 kap. 6 § andra stycket säpodatalagen, samråda med tillsynsmyndigheten. Ett så kallat förhandssamråd ska ske bland annat innan Säkerhetspolisen påbörjar en ny typ av behandling, där det bedömts finnas en särskild risk för intrång i registrerades personliga integritet.

Slutligen kan Integritetsskyddsmyndigheten, enligt 7 kap. 5 §, besluta om korrigerande åtgärder. Till sitt förfogande har Integritetsskyddsmyndigheten möjligheten att lämna råd och rekommendationer, men även att besluta om förelägganden att vidta åtgärder eller att förbjuda fortsatt behandling.

Tillsynsmyndighetens befogenheter, indelade i förebyggande och korrigerande, är utformade efter mönster från brottsdatalagen och brottsdatadirektivet. Integritetsskyddsmyndigheten har därmed i princip samma befogenheter vid tillsyn över Säkerhetspolisens personuppgiftsbehandling som då tillsynen vilar på lagstiftningar som genomför brottsdatadirektivet eller på dataskyddsförordningen.

Det är endast sanktionsavgift som inte tillämpas i förhållande till Säkerhetspolisen.

3.6 Hur regleras andra myndigheters behandling av personuppgifter?

3.6.1 Polismyndighetens brottsbekämpande verksamhet

Brottsdatadirektivet och brottsdatalagen

Brottsdatadirektivet är en del av EU:s dataskyddsreform och syftar till att säkerställa en enhetlig, hög skyddsnivå för personuppgifter som behandlas i myndigheters brottsbekämpande och lagförande verksamhet samt verksamhet som rör straffverkställighet. Genom att direktivet garanterar enhetliga rättigheter för enskilda inom hela unionen gynnas även utbytet av personuppgifter mellan myndigheter i olika länder.

Brottsdatadirektivet genomfördes i huvudsak genom en ny ramlag, brottsdatalagen (2018:1177). Brottsdatalagen gäller när *behöriga myndigheter* behandlar personuppgifter i brottsbekämpande syfte, för att upprätthålla allmän ordning och säkerhet eller för att verkställa straffrättsliga påföljder. Behöriga myndigheter är de myndigheter som direkt har till uppgift att bedriva sådan verksamhet eller andra aktörer som anförtrotts sådan myndighetsutövning. I Sverige gäller brottsdatalagen bland annat Polismyndigheten, Tullverket, Skatteverket och Kriminalvården. Säkerhetspolisen är behörig myndighet när myndigheten ägnar sig åt brottsbekämpande verksamhet som inte rör nationell säkerhet. Det förekommer exempelvis då Säkerhetspolisen biträder Polismyndigheten med särskilda utredningsinsatser eller då ett brott som Säkerhetspolisen normalt inte utreder upptäckts i samband med annan att verksamhet utreds eller sker mot en skyddsperson.[74]

Brottsdatalagen utgör en ramlag som kompletteras av flera så kallade registerförfattningar som är tillämpliga för olika myndigheter: Polisen, Tullverket, Kustbevakningen, Skatteverket, åklagarväsendets, domstolarna och Kriminalvården har alla sådana egna registerförfattningar.

[74] Se 3 § andra och tredje stycket i förordningen (2022:1719) med instruktion för Säkerhetspolisen.

Den följande framställningen koncentreras kring brottsdatalagen och lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område (polisens brottsdatalag). Som nämnts i samband med redogörelsen för säpodatalagen finns mycket stora likheter mellan den och polisens brottsdatalag. Lagarna tillkom i nära anslutning till varandra och togs fram inom ramen för samma utredningsarbete: *Utredningen om 2016 års dataskyddsdirektiv*. Fokus på redogörelsen nedan kommer i första hand vara det som skiljer de båda lagarna åt och hur detta påverkar tillämpningen.

Personuppgiftsbehandling för nya ändamål

Av polisens brottsdatalag framgår att myndigheten får behandla personuppgifter om det är nödvändigt för att utföra de brottsbekämpande uppgifter som ålagts den, bland annat att förebygga, förhindra och upptäcka brottslig verksamhet eller utreda brott. Dessa uppgifter är det som numera benämns som rättslig grund, vilket markerar inom vilka ramar som personuppgiftsbehandling är tillåten. Varje enskild behandling måste dock ha stöd i ett mer specifikt ändamål. Det följer av kravet att personuppgifter endast får behandlas för särskilda, uttryckligt angivna och berättigade ändamål. Polismyndigheten har därmed inte rätt att exempelvis kartlägga personer för breda ändamål som ”allvarlig brottslig verksamhet av länsövergripande karaktär” eller liknande.[75]

I detta avseende är brottsdatalagen ändamålsbestämmelse likalydande med säpodatalagen. Av förarbetena till brottsdatalagen framgår emellertid att polismyndigheten redan vid insamlandet av personuppgifter måste ha klart för sig för vilket närmare preciserat ändamål som insamlingen sker.[76] Bestämmelsen tar sikte på ändamålen i det enskilda fallet som till exempel en förundersökning om ett visst brott. Även om denna principiella utgångspunkt även gäller för Säkerhetspolisens verksamhet framgår av förarbetena till säpodatalagen att insamling av uppgifter i underrättelseverksamhet in-

[75] Prop. 2017/18:232 s. 123 och Säkerhets- och integritetsskyddsnämndens uttalande den 15 november 2013, dnr 173-2013, *Polismyndigheten i Skånes behandling av personuppgifter i uppgiftssamlingen benämnd ”Kringresande”*. Se även uttalandet den 12 december 2023, *Polismyndighetens behandling av personuppgifter i uppgiftssamlingar som rör utsatta områden*, dnr 127-2022.
[76] Ibid. s. 121 och prop. 2009/10:85 s. 98.

riktad mot Säkerhetspolisens brottskatalog inledningsvis får ske mot breda ändamål, se avsnitt 3.5.4 ovan. Polismyndigheten är därmed mer begränsad, framför allt i vilka uppgifter som får samlas in i underrättelseverksamheten.

Brottsdatalagen reglerar behandling av personuppgifter för nya ändamål än insamlingsändamålet på ett annat sätt än säpodatalagen. Av 2 kap. 4 och 22 §§ brottsdatalagen framgår att personuppgifter får behandlas för ett nytt ändamål endast om behandlingen är *nödvändigt och proportionerligt*.

Brottsdatalagen reglerar därmed inte behandling för nya ändamål genom den så kallade finalitetsprincipen. Skälet är att alla ändamål som omfattas av lagen ansetts vara förenliga med varandra. Det fanns därför inte något behov av att ange att ändamål för ursprunglig och ny behandling inte får vara oförenliga. Däremot följer av direktivet ett uttryckligt krav på att en proportionalitetsprövning ska göras innan behandling för nya ändamål. Det innebär att skälen för att personuppgifterna behandlas för det nya ändamålet ska väga tyngre än det intrång som behandlingen innebär för den enskilde.

För proportionalitetsbedömningen är det av betydelse vilka personuppgifter det är fråga om och i vilken verksamhet de används. Att exempelvis behandla en adressuppgift för nya ändamål har generellt setts som mer harmlöst än att behandla en uppgift som rör hälsa eller sexualliv. I den brottsutredande verksamheten kan det vara nödvändigt att till exempel göra sökningar i olika register där det förekommer uppgifter om personer som kan ha begått likartade brott tidigare. Uppgifterna i dessa register behandlas då för ett nytt ändamål vilket innebär ett utökat intrång för de registrerade. Uppgifter från en förundersökning kan också behöva användas i underrättelseverksamhet.

Syftet med ett krav på proportionalitet är alltså att det ska göras en bedömning av behovet av att behandla personuppgifter för nya ändamål ställt i relation till intrånget. För att underlätta tillämpningen i det enskilda fallet ansåg regeringen att vissa typer av nya ändamål generellt sett kan anses vara av så stort värde att de alltid väger upp integritetsintrånget och det därför kan förekomma proportionalitetsbedömningar som avser typsituationer.[77]

Av 2 kap. 4 och 22 §§ följer vidare att prövning av nödvändighet och proportionalitet inte ska göras om det i lag eller förordning

[77] Prop. 2017/18:232 s. 129.

finns en sekretessbrytande uppgiftsskyldighet. Då har lagstiftaren redan tagit ställning till att uppgiftslämnandet är nödvändigt och proportionerligt. Om det i lag eller förordning bara föreskrivs en möjlighet, men ingen skyldighet, att lämna uppgifter ska myndigheten däremot pröva om det är nödvändigt och proportionerligt att lämna dem, eftersom lagstiftaren då inte har gjort den prövningen.[78]

Gemensamt tillgängliga uppgifter i Polismyndighetens underrättelseverksamhet

I polisens brottsdatalag regleras, i 3 kap., vilka personuppgifter som får göras gemensamt tillgängliga. Uppdelningen mellan gemensamt tillgängliga uppgifter och uppgifter som endast är tillgängliga för ett fåtal följer inte av brottsdatadirektivet. Regleringen har överförts från tidigare polisdatalagen och grundas på att registerbegreppet där övergavs till förmån för ett mer teknikneutralt begrepp.

En av de största skillnaderna mellan säpodatalagen och polisens brottsdatalag är regleringen av vilka uppgifter som får göras gemensamt tillgängliga. Säpodatalagen har ingen begränsning i denna del. Enligt säpodatalagen får personuppgifter göras gemensamt tillgängliga om det behövs för att utföra någon av de uppgifter som anges som rättslig grund.

I polisens brottsdatalag finns däremot, i 3 kap. 2 § en detaljerad uppräkning av när personuppgifter får göras gemensamt tillgängliga. Till exempel får personuppgifter i förundersökningar eller uppgifter som har rapporterats till Polismyndighetens ledningscentraler regelmässigt göras gemensamt tillgängliga. I kriminalunderrättelseverksamheten krävs däremot att uppgifterna kan antas ha samband med misstänkt brottslig verksamhet, om den misstänkta verksamheten

a) innefattar brott för vilket det är föreskrivet fängelse i ett år eller mer, eller

b) sker systematiskt.

Eftersom lagstiftningen uppställer särskilda krav för att uppgifter inom underrättelseverksamheten ska få göras gemensamt tillgäng-

[78] Ibid. s. 138.

liga hanteras de inledningsvis i så kallade *underrättelsedeskar*. En desk utgörs av ett fåtal medarbetare, eftersom det inte är tillåtet att hantera information som gemensamt tillgänglig innan vissa åtgärder har vidtagits, bland annat avseende särskilda upplysningar och bedömningar av vilka brott som ingår i den brottsliga verksamheten. Eftersom varje desk inte får bemannas med mer än ett fåtal personer och på grund av det stora inflödet av underrättelseinformation har ett stort antal underrättelsedeskar upprättats över hela landet. Deskverksamhetens målsättning är att hitta samband mellan olika underrättelseuppslag för att på sikt möjliggöra att uppgifterna kan göras gemensamt tillgängliga.

Innan underrättelseuppgifter görs gemensamt tillgängliga kan de behandlas på ett friare sätt, eftersom den brottsliga verksamheten inte behöver vara preciserad. I likhet med säpodatalagen finns även det särskilda krav, om bland annat misstankemarkering samt trovärdighets- och sakriktighetsbedömning för gemensamt tillgängliga uppgifter.

Till skillnad mot Säkerhetspolisens underrättelseverksamhet är det vanligt förekommande att det inkommer tips till Polismyndigheten. Det kan handla om att allmänheten ringer in eller lämnar tips via polisens hemsida. Tips hanteras initialt vid deskarna.[79]

I polisens brottsdatalag finns även detaljerade bestämmelser om vilka personuppgifter som får tas fram när det utförs en sökning på gemensamt tillgängliga personuppgifter. En sökning på ett personnamn eller ett personnummer får som regel endast resultera i en träffbild där det framgår uppgifter om personen är misstänkt, vittne, målsägande, anmäld försvunnen, efterlyst eller bedöms kunna möta ett polisingripande med våld och liknande. Det finns dock vissa undantag från dessa bestämmelser bland annat för särskilt utvalda tjänstemän som utför vissa uppgifter i underrättelseverksamheten och vid utredning av allvarliga brott.

Polismyndigheten har beskrivit att bestämmelserna om gemensamt tillgängliga uppgifter medför stora tillämpningsproblem och på ett betydande sätt påverkar myndighetens förmåga att på ett effektivt sätt utöva sitt brottsbekämpande uppdrag. Myndigheten har därför hemställt till regeringen om vissa ändringar i dessa re-

[79] Nationella operativa avdelningen, PM 2021-03-11, *Underrättelseperspektivet på frågan om tipshantering inom Polismyndigheten*.

gler.[80] Bland annat föreslås att begränsningen till ett fåtal ska ersättas med att uppgifterna ska vara tillgängliga för *en avgränsad krets*. Vidare lämnas förslag på att de särskilda villkor för att göra uppgifter inom underrättelseverksamheten gemensamt tillgängliga, som beskrivs ovan, ska tas bort. Polismyndighetens förslag remitterades den 6 december 2024.

Längsta tid för behandling av personuppgifter

Av 2 kap. 17 § brottsdatalagen framgår att personuppgifter inte får behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Om det inte finns särskilda regler om när en viss kategori av personuppgifter inte längre får behandlas ska den personuppgiftsansvarige årligen se över behovet av att fortsätta behandla personuppgifterna.

Polisens brottsdatalag innehåller, i 4 kap., en rad bestämmelser med särskilda behandlingsfrister, som bär likheter med säpodatalagens motsvarande bestämmelser. Uppgifter som inte gjorts gemensamt tillgängliga får som längst behandlas ett år efter att ärendet de behandlats i avslutats eller efter att de behandlades första gången. Denna regel tillämpas hos Polismyndigheten eftersom fler uppgifter endast är tillgängliga för ett fåtal och det krävs arbete för att göra uppgifter gemensamt tillgängliga. Hos Säkerhetspolisen förekommer detta endast i undantagsfall då i princip alla uppgifter är gemensamt tillgängliga. Det finns även regler om behandling av uppgifter i brottsanmälningar och från förundersökningar som är likalydande med säpodatalagens. Det innebär att uppgifter från förundersökningar som regel får behandlas i fem år efter dom eller att förundersökningen lagts ner.

För uppgifter som är gemensamt tillgängliga inom underrättelseverksamheten gäller en generell behandlingstid på tre eller fem år, beroende på straffskalan för de brott som ingår i den brottsliga verksamheten. Behandlingstiden räknas från registreringen, men kan förlängas för alla personuppgifter om en ny registrering beträffande personens anknytning till brottslig verksamhet görs före utgången av tidsfristen. Det finns även en särskild bestämmelse om

[80] Skrivelse den 5 juli 2024, *Hemställan om ändring av bestämmelserna om gemensamt tillgängliga uppgifter i lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område*, dnr A286.201/2024.

att den tid som en person är frihetsberövad inte ska räknas in i behandlingsfristen. Gemensamt tillgängliga uppgifter som behandlas i ett ärende får behandlas som längst ett år efter att ärendet avslutats.

Till skillnad mot säpodatalagen innehåller polisens brottsdatalag en rad bestämmelser om olika register; bland dem tillträdesförbudsregistret och penningtvättsregistret som innehåller särskilda bestämmelser om behandlingstid. Därutöver finns i specialreglering, om bland annat belastningsregister, misstankeregister och passagerarregister, särskilda bestämmelser om behandlingstid för uppgifter som behandlas med stöd av respektive lag.

3.6.2 Försvarsmakten och Försvarets radioanstalt

Försvarsunderrättelseverksamhet och militär säkerhetstjänst

Säkerhetspolisen brukar kategoriseras med de andra myndigheterna med brottsbekämpande uppdrag. Det finns givetvis goda skäl för att de polisiära myndigheterna ska regleras på liknande sätt. Det finns dock även klara paralleller mellan Säkerhetspolisens verksamhet som rör nationell säkerhet och Försvarsmaktens säkerhetstjänst. De båda verksamheterna använder likartade metoder och har liknande mål. Där Säkerhetspolisens verksamhet avgränsas mot brottslig verksamhet av visst slag är Försvarsmaktens fokus på skydda verksamheten mot olika säkerhetshot. Dessa säkerhetshot kan dock ofta även utgöra brottslig verksamhet.

Inom den militära säkerhetstjänsten bedrivs underrättelseverksamhet för att kartlägga bland annat verksamhet som innefattar brott som kan hota Sveriges säkerhet eller terroristbrott och för att kartlägga underrättelseverksamhet som riktas mot Försvarsmakten och dess säkerhetsintressen.

Inom Försvarsmakten, men även andra myndigheter under Försvarsdepartementet bedrivs försvarsunderrättelseverksamhet. Försvarsunderrättelseverksamhet fick tidigare bedrivas för att kartlägga yttre militära hot mot landet. Sedan år 2007 begränsas inte verksamheten till militära hot, utan avser numera yttre hot mot landet.

Slutligen är jämförelsen mellan Säkerhetspolisen och de myndigheter som bedriver försvarsunderrättelseverksamhet och militär

säkerhetstjänst relevant på grund av avsaknad av bindande EU-rättsakter. EU:s lagstiftningskompetens är begränsad avseende frågor som rör försvar och nationell säkerhet. Därmed finns inte någon dataskyddslagstiftning på EU-nivå som binder den nationella lagstiftaren. Området försvar och nationell säkerhet omfattas dock av Europakonventionen och flera andra av Europarådets konventioner.

Försvarsunderrättelseverksamhet

Av lag (2000:130) om försvarsunderrättelseverksamhet framgår att försvarsunderrättelseverksamhet ska bedrivas till stöd för svensk utrikes-, säkerhets-, och försvarspolitik samt i övrigt för kartläggning av yttre hot mot landet. Det är regeringen som ska bestämma försvarsunderrättelseverksamhetens inriktning och de myndigheter som regeringen bestämmer får inom denna ram ange en närmare inriktning av verksamheten. De myndigheter som ska bedriva försvarsunderrättelseverksamhet är Försvarsmakten, Försvarets radioanstalt (FRA), Försvarets materielverk och Totalförsvarets Forskningsinstitut. Inom Försvarsmakten bedrivs försvarsunderrättelseverksamhet vid den militära underrättelse- och säkerhetstjänsten, ofta förkortad MUST.

Av lagen framgår uttryckligen att försvarsunderrättelseverksamhet endast får avse utländska förhållanden. Avgränsningen till utländska förhållanden innebär att försvarsunderrättelseverksamheten typiskt sett ska inhämta, bearbeta, analysera och delge sådan information om företeelser och förhållanden i andra länder som ger svenska beslutsfattare ett förbättrat underlag för beslut och bedömningar i utrikes-, säkerhets- och försvarspolitiska frågor eller för att skydda svensk personal som deltar i internationella insatser. Verksamheten kan under vissa förhållanden även avse företeelser inom landet exempelvis om en organisation med verksamhet som utgör ett hot mot landet har sitt ursprung i ett annat land, men verkar genom representanter i Sverige eller genom att på annat sätt utnyttja resurser i Sverige. Det handlar då om att följa upp utländska förhållandens koppling till Sverige för att kunna bedöma hotbilden mot landet. Exempel på vad som utgör försvarsunderrättelseverksamhet är säkerhetspolitiska och militärstrategiska bedömningar,

analyser av pågående och framtida konflikter, internationella terroristgrupper, cyberhot, massförstörelsevapen samt biografiska underrättelser som avser utländsk militär personal eller andra viktiga befattningshavare.

Försvarsunderrättelseverksamheten går ofta ut på att upptäcka på förhand okända företeelser. Till exempel uppgifter om nya hot mot svenska säkerhetsintressen, samhällsviktiga funktioner, eller mot säkerhetsskyddsklassificerade uppgifter som inte får hamna hos främmande makt. Verksamheten innebär även att kartlägga redan kända företeelser och följa förändringar i dessa för att tidigt få kunskap om aktörers nya ambitioner, avsikter och förmågor. Försvarsunderrättelseverksamhet är också ett centralt verktyg vid kartläggning i efterhand av händelser som oförutsett inträffat, i syfte att finna förklaringar till det inträffade samt för att kartlägga eventuella ännu inte identifierade inslag i en inträffad händelse. Genom sådan uppföljning kan ytterligare underrättelseinformation produceras som ger dels bättre förståelse för orsakerna bakom det inträffade, dels kompletterande information om inslag som ännu inte identifierats, till exempel kvarvarande oupptäckta hot.[81]

Militär säkerhetstjänst

Försvarsmakten ska enligt sin instruktion leda och bedriva militär säkerhetstjänst. Syftet är att skydda de säkerhetsintressen som berör Försvarsmakten och dess tillsynsområde enligt säkerhetsskyddslagen. Den militära säkerhetstjänsten ska

– förebygga, upptäcka, motverka och avvärja säkerhetshotande verksamhet,
– klarlägga och analysera den säkerhetshotande verksamhetens mål, medel och metoder, och
– utifrån hotbild och säkerhetshotande verksamhet vidta åtgärder för att säkerställa relevant skydd i form av informationssäkerhet, fysisk säkerhet och personalsäkerhet.

Med militär säkerhetstjänst avses såväl verksamheten som dess organisation. Försvarsmakten är bedrivs militär säkerhetstjänst

[81] Se SOU 2018:63 s. 95–96 samt prop. 2020/21:224 s. 43–45.

av den militära underrättelse- och säkerhetstjänsten, operationsledningen och vid militärregionerna. Den militära säkerhetstjänsten består av säkerhetsunderrättelsetjänst, säkerhetsskyddstjänst och signalskyddstjänst.

Säkerhetsunderrättelsetjänsten har till uppgift att klarlägga och analysera den säkerhetshotande verksamhetens mål, medel och metoder. Säkerhetshotande verksamhet mot Sverige eller mot insatta förband och insatser i andra länder kan förekomma i form av främmande underrättelseverksamhet, sabotage, subversiv verksamhet, terrorism och kriminalitet. Säkerhetsunderrättelsetjänst bedrivs genom planläggning, inhämtning, bearbetning och analys samt delgivning av säkerhetsunderrättelser. Verksamheten sker i stort under samma arbetsformer och med utnyttjande av samma typ av källor som används i försvarsunderrättelseverksamheten.

Säkerhetsskyddstjänstens uppgift är att ta fram åtgärder som syftar till att hindra eller försvåra säkerhetshotande verksamhet såsom exempelvis obehörigt röjande av hemliga uppgifter som rör Sveriges säkerhet, sabotage, stöld och terrorism. Säkerhetsskyddstjänsten ska, utifrån hotbild och säkerhetshotande verksamhet vidta relevanta säkerhetsskyddsåtgärder.

Signalskyddstjänsten syftar till att förhindra obehörig insyn i och påverkan av telekommunikations- och it-system med hjälp av kryptografiska metoder och övriga signalskyddsåtgärder. Signalskyddstjänsten är en säkerhetsskyddsangelägenhet som omfattar hela totalförsvaret och syftet är att säkerställa säker kommunikation. Säkerhetsskyddstjänsten och signalskyddstjänsten syftar gemensamt till att förebygga, förhindra och motverka säkerhetshotande verksamhet.

Försvarsmakten bedriver även underrättelsetjänst för att kunna lösa militära uppgifter som inte utgör försvarsunderrättelseverksamhet eller militär säkerhetstjänst. Denna underrättelseverksamhet syftar främst till att skapa en lägesbild och ge beslutsunderlag för militära chefer för myndighetens lösande av militära uppgifter enligt Försvarsmaktens instruktion, regleringsbrev eller särskilda regeringsbeslut.[82]

[82] Prop. 2020/21:224 s. 39–40.

Försvarets radioanstalt

Försvarets radioanstalt, FRA, är en civil myndighet under Försvarsdepartementet vars verksamhet i huvudsak utgörs av signalspaning i försvarsunderrättelseverksamhet. Myndigheten bildades redan år 1942 och bedrev ursprungligen endast signalspaning mot eterburna signaler. Sedan år 2009, när lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet trädde i kraft, bedriver myndigheten även signalspaning mot trådburna signaler.

Signalspaning är en form av teknisk inhämtning som ofta tar sikte på innehållet i kommunikationer och annan information som hanteras i elektronisk form. Det kan till exempel röra sig om textmeddelanden, talad kommunikation eller dokument. Andra delar av signalspaningen avser att fastställa tekniska detaljer rörande framför allt radarsignaler från fartyg eller flygplan. Försvarets radioanstalts försvarsunderrättelseverksamhet tar bland annat sikte på att upptäcka ännu okända hotaktörer och företeelser.

Signalspaning i försvarsunderrättelseverksamhet sker med stöd av lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet (i det följande signalspaningslagen). Enligt 1 § första stycket i den lagen får signalspaning i försvarsunderrättelseverksamhet endast ske i de fall regeringen eller någon av de myndigheter som anges i lagen har bestämt en närmare inriktning för signalspaning. FRA utför endast signalspaning på uppdrag åt andra och får inte initiera någon signalspaning utanför uppdragsgivarens inriktning.

Signalspaningslagen innehåller en uppräkning av de syften för vilka kartläggning genom signalspaning i försvarsunderrättelseverksamhet får ske.[83] Bland dem finns syften som tydligt avser Försvarsmaktens ansvarsområde, som kartläggning av yttre militära hot mot landet eller hot mot svenska intressen vid genomförandet av internationella insatser. Signalspaning får emellertid även inriktas mot frågor som helt eller delvis avser Säkerhetspolisens verksamhet, som kartläggning av strategiska förhållanden avseende internationell terrorism eller främmande underrättelseverksamhet mot svenska intressen. Följaktligen är Säkerhetspolisen en av de myndigheter som får besluta om en närmare inriktning av FRA:s signalspaning.

Enligt 2 § signalspaningslagen får inhämtning som sker i tråd endast avse signaler som förs över Sveriges gräns. Dessutom får,

[83] Se 1 § andra stycket signalspaningslagen.

enligt 2 a §, signalspaning som huvudregel inte avse signaler mellan en avsändare och mottagare som båda befinner sig i Sverige. Förbudet är försett med undantag för bland annat signaler från eller till utländsk krigsmakt som befinner sig i Sverige. Det finns emellertid förslag, om möjlighet till ytterligare undantag från denna begränsning. I betänkandet *Signalspaning i försvarsunderrättelseverksamhet – en modern och ändamålsenlig lagstiftning*, SOU 2024:59, föreslås bland annat att även inhemska kommunikation ska få inhämtas i sådana brådskande situationer som innebär fara för människors liv eller hälsa eller för omfattande förstörelse av egendom.

Den inhämtning genom signalspaning som FRA får bedriva kräver tillstånd av Försvarsunderrättelsedomstolen. Bestämmelserna om ansökan finns i 4 a § signalspaningslagen. En ansökan ska bland annat innehålla uppgifter om det inhämtningsuppdrag som ansökan avser, med en närmare redogörelse för det behov som föranleder ansökan och uppgifter om vilken inriktning uppdraget hänför sig till samt de sökbegrepp eller kategorier av sökbegrepp som är avsedda att användas vid inhämtningen.

Försvarsunderrättelsedomstolen får meddela tillstånd under förutsättning att vissa krav är uppfyllda. Det krävs bland annat att uppdraget är förenligt med lagen om försvarsunderrättelseverksamhet och signalspaningslagen att syftet med inhämtningen inte kan tillgodoses på ett mindre ingripande sätt och att uppdraget beräknas ge information vars värde är klart större än det integritetsintrång som inhämtning i enlighet med ansökan kan innebära.

Signalspaning får inte inriktas mot endast en viss fysisk person vilket är en avgörande skillnad i förhållande till straffprocessuella tvångsmedel. Vidare får de underrättelserapporter som FRA redovisar till inriktande myndighet endast innehålla de personuppgifter som är av betydelse för försvarsunderrättelseverksamheten. Det är därmed inte tillåtet att redovisa överskottsinformation om annan brottslig verksamhet än sådan som kan vara föremål för försvarsunderrättelseverksamhet. Inte heller får uppgifter i underrättelser från FRA användas i förundersökning vilket följer av en särskild lag; lag (2019:547) om förbud mot användning av vissa uppgifter för att utreda brott. Signalspaningsinformation utgör därför inte ett redskap i den brottsutredande verksamheten, utan är i första hand ett verktyg för underrättelseverksamheten.

Försvarsmaktens och FRA:s personuppgiftslagstiftning

År 2022 fick både Försvarsmakten och FRA ny personuppgiftslagstiftning: Lag (2021:1171) om behandling av personuppgifter vid Försvarsmakten (försvarsdatalagen) respektive lag (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt (FRA-datalagen).[84]

Trots att all den verksamhet som regleras i nämnda lagar ansetts falla utanför området för EU-rätten har lagarna i stor utsträckning samma struktur som närliggande EU-reglering. Detta ansågs vara en fördel i tillämpningshänseende för såväl Försvarsmakten och FRA som tillsyns- och kontrollmyndigheterna, liksom för enskilda ur ett integritetsskyddsperspektiv.[85]

FRA-datalagen innehåller bland annat bestämmelser för myndighetens försvarsunderrättelseverksamhet och utvecklingsverksamhet. För Försvarsmaktens del regleras både den generella verksamheten som avser att upprätthålla ett militärt försvar som ytterst kan möta ett väpnat angrepp mot Sverige (försvar och säkerhet) samt de mer specifika verksamheterna försvarsunderrättelseverksamheten och den militära säkerhetstjänsten i samma lag.

I det följande redogörs för några av de bestämmelser som reglerar Försvarsmaktens och FRA:s personuppgiftsbehandling och som avser områden av intresse för jämförelsen med Säkerhetspolisens lagstiftning. Redogörelsen gör därmed inte anspråk på att vara heltäckande.

Ändamål och rättslig grund

Försvarsmaktens försvarsunderrättelseverksamhet

I 2 kap. 3 § försvarsdatalagen anges att personuppgifter får behandlas i Försvarsmaktens försvarsunderrättelseverksamhet om det är nödvändigt för att bedriva den verksamhet som anges i lagen (2000:130) om försvarsunderrättelseverksamhet.

Ändamålen för personuppgiftsbehandlingen inom försvarsunderrättelseverksamheten måste bestämmas inom det bredare underrättelseuppdraget som anges i lagen om försvarsunderrättelseverk-

[84] SOU 2018:63 samt SOU 2020:68, prop. 2020/21:224, bet. 2021/22:FöU2, rskr. 2021/22:45.
[85] Prop. 2020/21:224 s. 59.

samhet. Ytterst ska behandlingen därmed vara nödvändig för att stödja svensk utrikes-, säkerhets- och försvarspolitik samt i övrigt för kartläggning av yttre hot mot landet.[86] De personuppgifter som behandlas är bland annat uppgifter om personer som verkar inom andra staters försvars- eller underrättelseväsende, ledande utländska politiska företrädare och andra opinionsbildare samt andra personer som förekommer i underrättelserapporter eller kan komma att få ett underrättelsevärde.[87]

I tidigare lagstiftning begränsades behandlingen av personuppgifter till personer som hade anknytning till en preciserad inriktning för försvarsunderrättelseverksamheten. Av den nya bestämmelsen i 2 kap. 4 § försvarsdatalagen följer att de personuppgifter som Försvarsmakten har fått tillgång till i myndighetens försvarsunderrättelseverksamhet får fortsätta att behandlas i den verksamheten, om det behövs för att fullgöra den. Bestämmelsen i 2 kap. 4 § försvarsdatalagen innebär alltså att Försvarsmakten numera fortsatt kan behandla personuppgifter som Försvarsmakten har fått tillgång till i myndighetens försvarsunderrättelseverksamhet i enlighet med en tidigare inriktning, såvida det behövs för att fullgöra försvarsunderrättelseverksamheten. Förändringen, som medger en utökad möjlighet att fortsätta att behandla personuppgifter av mer perifer betydelse för nuvarande hotbilder, motiverades bland annat av att kunskapen om historiska skeenden och normalbilder är av väsentlig betydelse för tolkning av nya observationer. I förarbetena konstaterade regeringen att framåtsyftande försvarsunderrättelseverksamhet behöver kunna förvarna om bland annat avsikter, aktiviteter och hot. För att kunna förstå ett skeende eller en aktörs agerande behöver det som observeras emellertid ofta sättas in i ett kontextuellt och historiskt sammanhang. Först därefter kan bedömningar om underrättelserelevans göras. För vissa företeelser behöver sådana jämförelser kunna göras med observationer som har gjorts långt tillbaka i tiden, inte sällan 10–20 år.[88]

Dessa regler innebär, tillsammans med avsaknaden av en lagstadgad, yttersta tidsgräns för bevarande av personuppgifter inom verksamheten, att personuppgifter kan behandlas under mycket lång tid inom Försvarsmakten. Lagen ställer endast upp den begränsningen

[86] Se 1 § lag om försvarsunderrättelseverksamhet.
[87] Se prop. 2006/07:46 s. 64.
[88] SOU 2018:63 s. 163 och prop. 2020/21:224 s. 71.

att personuppgifter inte får behandlas under längre tid än vad som behövs med hänsyn till ändamålen med behandlingen (2 kap. 21 §). Behoven kan utgöras av personuppgifter om exempelvis utländsk militär personal, politiker eller andra viktiga befattningshavare. Regeringen ansåg att sådana uppgifter är nödvändiga för att informationsunderlaget för svensk utrikes-, försvars- och säkerhetspolitik ska bli komplett.[89]

Personuppgifter i försvarsunderrättelseverksamheten som är gemensamt tillgängliga för fler än ett fåtal personer inom Försvarsmakten ska behandlas i uppgiftsamlingar.

Militär säkerhetstjänst

Enligt 2 kap. 5 § försvarsdatalagen får personuppgifter behandlas i Försvarsmaktens militära säkerhetstjänst för att *upptäcka, förebygga och avvärja* säkerhetshotande verksamhet som riktas mot Försvarsmakten och dess säkerhetsintressen, om det är nödvändigt att

1. klarlägga verksamhet som innefattar hot mot Sveriges säkerhet, eller
2. vidta åtgärder som hindrar eller försvårar säkerhetshotande verksamhet.[90]

Begreppet *klarlägga* i den första punkten är avsedd att markera säkerhetsunderrättelseverksamheten som ändamål och innebär att personuppgifter får behandlas för att klarlägga verksamhet som innefattar hot mot rikets säkerhet. Vid sådan underrättelseverksamhet får därmed uppgifter om personer med anknytning till sådan verksamhet också behandlas. Den andra punkten avser säkerhetsskyddstjänst, vilket inkluderar signalskyddstjänst.

Dessa vida ändamål i 2 kap. 5 § försvarsdatalagen begränsas och specificeras i 2 kap. 6 §. Där anges att personuppgifter får behandlas för de ändamål som anges i 5 § endast om uppgifterna är nödvändiga för något av den fem uppräknade ändamål. Bland dem finns ändamålet att ”kartlägga verksamhet som innefattar brott som kan hota Sveriges säkerhet eller terroristbrott” (1 p.) och att ”kartlägga

[89] Prop. 2020/21:224 s. 176.
[90] Jfr 7 § förordningen (2024:1333) med instruktion för Försvarsmakten.

underrättelseverksamhet som riktas mot Försvarsmakten och dess säkerhetsintressen" (2 p.).

Personuppgifter som behandlas för den militära säkerhetstjänsten ska förses med en upplysning om på vilken av de angivna grunderna uppgiften behandlas (2 kap. 7 §). I likhet med säpodatalagen ska en så kallad misstankemarkering göras för att särskilja uppgifter som inte rör personer som är misstänkta för brottslig verksamhet samt, i vissa fall, en uppgift om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak.

Särskilt, uttryckligt angivet och berättigat ändamål

Försvarsdatalagen och FRA-datalagen innehåller, båda i 2 kap. 1 §, samma ändamålsprincip som säpodatalagen, med ett krav på att personuppgifter bara får behandlas för särskilda, uttryckligt angivna och berättigade ändamål. Av förarbetena framgår emellertid att krav på ett *särskilt* ändamål anses uppfyllt genom att behandlingen kan hänföras till något av de ändamål som angetts i respektive lag.[91]

Behandling av personuppgifter inom den militära säkerhetstjänsten ska ske för något av de fem särskilda ändamål som räknas upp i 2 kap. 6 § i försvarsdatalagen. Dessa ändamål i försvarsdatalagen motsvarar vad som i säpodatalagen benämnts rättslig grund. Sådana, så kallade primära ändamålsbestämmelser, ansågs inte vara tillräckligt preciserade för att utgöra ett särskilt och uttryckligt angivet ändamål då säpodatalagen beslutades.[92]

Det finns därmed inte något krav på att ändamålet för behandling av personuppgifter inom Försvarsmakten ska bestämmas individuellt. Vi har även fått bekräftat att det är det sätt på vilken lagen tillämpas. Det är tillräckligt att behandlingen i fråga är nödvändig för någon av de ändamål som angetts i lagen. Denna, praktiskt mycket betydelsefulla skillnad mellan Försvarsmaktens och FRA:s respektive datalagar och säpodatalagen kommer dock inte till uttryck genom hur ändamålsprincipen formulerats i respektive lag. De tre lagarna har helt överensstämmande lagtext såvitt avser ändamålsprincipen.

[91] Prop. 2020/21:224 s. 65 ff.
[92] Prop. 2018/19:163 s. 61–63.

Även om utredningen inte har någon djupare insyn i den personuppgiftsbehandling som rent faktiskt sker i försvarsunderrättelseverksamheten eller den militära säkerhetstjänsten, framstår det utifrån förarbetena som att de breda ändamålen för vilken behandling kan ske inte begränsar informationshanteringen på samma sätt som för Säkerhetspolisen. Principerna om adekvans, relevans och uppgiftsminimering återfinns även i försvarsdatalagen och FRA-datalagen. Vilka uppgifter som är nödvändiga, relevanta, adekvata och inte onödigt omfattande för ändamålet med behandlingen beror givetvis på vilket ändamål som prövningen sker mot. Hur dessa principer påverkar behandlingen av personuppgifter skiljer sig därmed åt beroende på hur konkret ändamålet måste formuleras. Hur verksamhetsstyrande dessa principer är skiljer sig därför sannolikt åt mellan bland annat den militära säkerhetstjänsten och hur motsvarande bestämmelser påverkar Säkerhetspolisens verksamhet, trots att de lagfästs på samma sätt.

Allmänt tillgänglig information

Av 2 kap. 10 § i försvarsdatalagen respektive 2 kap. 9 § FRA-datalagen framgår uttryckligen att myndigheterna får behandla personuppgifter som utgör allmänt tillgänglig information om det är nödvändigt för att bland annat bedriva underrättelseverksamhet. Syftet är bland annat att komplettera den information som Försvarsmakten och FRA inhämtat genom särskilda metoder och sätta dessa uppgifter i sitt sammanhang.

Den särskilda regleringen för allmänt tillgänglig information tar bland annat sikte på att upprätta referensdatabaser av uppgifter som är publikt tillgängliga, antingen på internet eller genom köp av en kommersiell produkt. Det kan exempelvis röra sig om uppgifter som finns med i elektroniska telefonkataloger eller förteckningar över ip-adresser i olika länder. Eftersom den underrättelseverksamheten omfattas av sekretess är det inte lämpligt att myndigheterna exponerar sitt underrättelsearbete genom att själv göra sökningar i olika publika databaser. Sökningar på internet riskerar att röja vad som är föremål för myndigheternas intresse (inriktning) samt metod. I stället måste databaserna i sin helhet anskaffas av myndigheterna.

I propositionen anges att de ändamål som framgår av de båda lagarna, enligt regeringen, i och för sig omfattar behandling av allmänt tillgängliga personuppgifter i referensdatabaser. Regeringen bedömde dock att det stora antalet personuppgifter som sådana referensdatabaser kan innehålla utgör en form av integritetsintrång, även om de är allmänt tillgängliga. För att undvika oklarheter i rättstillämpningen ansågs därför att stödet för sådan behandling bör komma till tydligt uttryck i lagtexten.[93] Motiven till bestämmelsen är dock något otydliga i fråga om hur lagens övriga bestämmelser, om bland annat uppgiftsminimering och känsliga personuppgifter, är tänkta att tillämpas för de så kallade referensdatabaserna. Hur Försvarsmakten och FRA i praktiken tillämpar bestämmelsen som medger behandling av allmänt tillgänglig information är okänt för utredningen.

Det finns särskilda regler för FRA:s gemensamt tillgängliga uppgiftssamling för allmänt tillgänglig information som anger att den får endast innehålla information som finns eller har funnits på internet eller i öppna databaser.[94] Någon motsvarande reglering finns inte för Försvarsmakten.

Känsliga personuppgifter

I likhet med säpodatalagen innehåller både FRA-datalagen och försvarsdatalagen ett förbud att behandla personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning. Förbudet kompletteras med ett undantag som medger att personuppgifter får kompletteras med sådana uppgifter om det är absolut nödvändigt med hänsyn till ändamålen med behandlingen. Vidare framgår att biometriska uppgifter får behandlas om det är absolut nödvändigt med hänsyn till ändamålet med behandlingen. Biometriska uppgifter behöver inte utgöra ett komplement utan får registreras självständigt. I likhet med bland annat säpodatalagen framgår av samma paragraf även ett förbud mot behandling av genetiska uppgifter.[95]

[93] Prop. 2020/21:224 s. 85–86 samt SOU 2018:63 s. 172.
[94] 3 kap. 9 § förordning (2021:1208) om behandling av personuppgifter vid Försvarets radioanstalt.
[95] Se 2 kap. 13–14 §§ FRA-datalagen och 2 kap. 15–16 försvarsdatalagen.

Både FRA-datalagen och försvarsdatalagen innehåller likalydande regler om hur känsliga personuppgifter får användas som sökbegrepp av respektive myndighet. Till skillnad mot säpodatalagen innehåller lagarna inte något förbud mot sådana sökningar. Känsliga personuppgifter får dock endast utgöra sökbegrepp om det är absolut nödvändigt med hänsyn till ändamålet med behandlingen.[96]

När det gäller behandling av känsliga personuppgifter i allmänhet konstaterade regeringen uppgifter om bland annat etnisk härkomst eller religiös övertygelse, kan vara nödvändiga att behandla i samband med exempelvis humanitära insatser där en viss minoritet ska skyddas. I försvarsunderrättelse- och säkerhetstjänstsynpunkt är det ofta av grundläggande betydelse att registrera uppgifter om att en person tillhör ett politiskt parti eller annan organisation. Även om sådana personuppgifter ska behandlas restriktivt, och endast utgöra komplement till annan uppgift, ansåg regeringen att det ligger i verksamhetens natur att sådana uppgifter kan ha betydelse för den slutliga analysen. Avseende biometriska uppgifter får det exempelvis inom signalspaningen betraktas som självklart att en persons röstprofil behöver kunna behandlas i identifieringssyfte. Att kunna göra korrekta identifieringar är även av avgörande betydelse vid bedömning av olika källors trovärdighet och informations sakriktighet.[97]

I både FRA-datalagen och försvarsdatalagen finns även ett undantag från kravet på absolut nödvändighet vid behandling av känsliga uppgifter. Av försvarsdatalagen framgår nämligen att sådana uppgifter får behandlas om den registrerade har lämnat sitt uttryckliga samtycke eller på ett tydligt sätt har offentliggjort uppgifterna. Samtyckessituationer kan tänkas förekomma främst i Försvarsmaktens militära säkerhetstjänst vid säkerhetsprövningar.

I försvarsunderrättelseverksamhet aktualiseras inte några samtyckessituationer och för FRA:s del anges därför endast att undantaget gäller tydligt offentliggjorda uppgifter.[98]

Ett tydligt offentliggörande av en känslig personuppgift kan ske exempelvis genom att den registrerade gör uppgifterna tillgängliga på internet. Om en känslig personuppgift inhämtats på det sättet

[96] Se 2 kap. 15 § FRA-datalagen respektive 2 kap. 17 § försvarsdatalagen.
[97] Prop. 2020/21:224 s. 90–93.
[98] Se 2 kap. 17 § FRA-datalagen och 2 kap. 19 § försvarsdatalagen.

behöver myndigheten alltså inte pröva om behandlingen av den är absolut nödvändig.

Undantag för behandling då det ännu inte har kunnat fastställas vilka personuppgifter som informationen innehåller

Både FRA-datalagen och försvarsdatalagen innehåller en särskild bestämmelse som anger att hantering av information inte anses oförenlig med bestämmelserna om bland annat ändamål, kvalitet eller kraven som ställs på känsliga personuppgifter – i det skede av behandlingen då det ännu inte har kunnat fastställas vilka personuppgifter som informationen innehåller.[99]

Bestämmelsen fanns även i FRA:s tidigare personuppgiftslag, i en delvis annan lydelse. Syftet med bestämmelsen var att lagen inte skulle hindra inhämtning av personuppgifter genom signalspaning, lagring av uppgifter omedelbart därefter och bearbetning i form av kryptoforcering och språklig översättning, innan det var möjligt att fastställa att det ens rörde sig om personuppgiftsbehandling. Bestämmelsens utformning gjorde emellertid undantaget verkningslöst eftersom det vid signalspaning i princip går att förutsätta *att* det förekommer personuppgifter i de inhämtade signalerna. Bestämmelsens utformning ändrades därför till att undantaget gäller till dess att det går att fastställa *vilka* personuppgifter som förekommer i materialet.[100]

I förarbetena framhölls att dessa situationer även kan förekomma då Försvarsmakten inhämtat eller mottagit uppgifter. Där förklarades att när Försvarsmakten får in en rapport från en annan myndighet som rör exempelvis försvarsunderrättelseverksamhet eller militär säkerhetstjänst tas denna normalt in i informationssystemet, tillsammans med en notering om att det förekommer personuppgifter i handlingen. Någon prövning utifrån bestämmelserna om grundläggande krav, tillåtlighet och känsliga personuppgifter görs inte förrän personuppgifterna manuellt behandlas i respektive verksamhet. Det är först när handlingarna granskas av personal i de respektive verk-

[99] Se 2 kap. 18 § FRA-datalagen och 2 kap. 20 § försvarsdatalagen.
[100] Se prop. 2020/21:224 s. 95 samt Datainspektionens tillsynsbeslut 24 oktober 2016, dnr 2331-2015.

samheterna som en bedömning görs om personuppgifterna är bland annat nödvändiga och relevanta för ett visst ändamål. [101]

Motsvarande bestämmelse som för FRA infördes därför i den nya försvarsdatalagen i syfte att bland annat möjliggöra detta arbetssätt. I förarbetena framhölls att bestämmelsen är tillämplig då personuppgifter som behandlas automatiserat inte blir föremål för manuell granskning och även vid insamling av sådana uppgifter.[102]

Längsta tid för personuppgiftsbehandling

I de personuppgiftslagar som gäller för Försvarsmakten och FRA finns ingen uttrycklig tidsgräns för behandling av personuppgifter. I stället ska behandlingen fortlöpande prövas utifrån om behandling av personuppgifterna fortsatt är nödvändig utifrån för ändamålet med behandlingen. Av respektive lag framgår därmed endast att personuppgifter inte får behandlas under längre tid än vad som behövs med hänsyn till ändamålen med behandlingen.

Regeringen eller den myndighet regeringen bestämmer har möjlighet att meddela föreskrifter om att personuppgifter endast får behandlas under viss tid eller att de ska fortsätta att behandlas för exempelvis historiska ändamål. Sådana föreskrifter finns i de till respektive lag anslutna förordningarna såvitt avser uppgifter som är gemensamt tillgängliga i uppgiftssamlingar. Där anges för Försvarsmaktens del bland annat att personuppgifter i en uppgiftssamling för signalkontroll inte får behandlas längre än ett år efter att behandlingen av uppgifterna påbörjades. Vidare framgår att personuppgifter i uppgiftssamlingar för försvarsunderrättelseverksamhet och militär säkerhetstjänst ska fortsätta att bevaras för bland annat arkivändamål efter att de inte längre är nödvändiga för verksamheten.[103] För FRA anges att behandlingstiden för obearbetat och automatiskt bearbetat material vars relevans för verksamheten ännu inte har bedömts begränsats till ett år.[104]

I försvarsunderrättelseverksamheten och den militära säkerhetstjänsten behöver personuppgifter inte sällan behandlas under mycket

[101] Se SOU 2018:63 s. 195 och prop. 2020/21:224 s. 96.
[102] Prop. 2020/21:224 s. 96.
[103] Se 3 kap. 5 § tredje stycket, 2 § andra stycket respektive 3 § tredje stycket i förordning (2021:1207) om behandling av personuppgifter vid Försvarsmakten.
[104] Se 3 kap. 1 § tredje stycket förordning (2021:1208) om behandling av personuppgifter vid Försvarets radioanstalt.

lång tid. I förarbetena till den tidigare personuppgiftslagen för Försvarsmaktens underrättelseverksamhet och Försvarets radioanstalt angavs att det kan det förekomma att uppgifter som är så gamla som 40–70 år kan ha betydelse för bedömningar i frågor som rör den svenska utrikes-, försvars- och säkerhetspolitiken. Som exempel anfördes bland annat biografiska underrättelser om militära befattningshavare, där det i inledningen av personens karriär inhämtas uppgifter vilkas betydelse för verksamheten i framtiden då inte kan förutses. På motsvarande sätt ansågs uppgifter om en politisk makthavare under personens hela livstid – och i vissa fall även därefter – kunna vara av värde. Beträffande personuppgifter inom den militära säkerhetstjänsten exemplifierades behoven med att uppgifter om en anställd som genomgått registerkontroll måste kunna behandlas under hela anställningstiden, som kan uppgå till mer än 40 år.[105] Eftersom bestämmelsen om bevarande av personuppgifter överfördes utan några större sakliga ändringar till de nya lagstiftningarna torde detta uttalande alltjämt kunna beskriva synen på hur länge personuppgifter får bevaras inom de olika verksamheterna.

Särskilda regler angående signalspaning

I lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet (signalspaningslagen) finns även vissa bestämmelser som rör personuppgiftsbehandling. Dessa bestämmelser tillämpas parallellt med FRA-datalagen och gäller skyldighet att förstöra vissa uppgifter. Av 2 a och 7 §§ signalspaningslagen följer att en upptagning eller uppteckning av uppgifter som har inhämtats eller som FRA har fått från ett annat land eller en internationell organisation under vissa förhållanden ska förstöras om innehållet

- har bedömts sakna betydelse för försvarsunderrättelse- eller utvecklingsverksamheten,
- utgör så kallad privilegierad kommunikation eller
- avser signaler mellan en avsändare och mottagare som båda befinner sig i Sverige.

[105] Prop. 2006/07:46 s. 110 f.

Det förstnämnda kravet om betydelselös information är lägre än det nödvändighetsrekvisit som följer av FRA-datalagen och avser att träffa uppgifter som inte utgör underlag till försvarsunderrättelser, exempelvis uppgifter som endast rör inhemska förhållanden. Om en upptagning innehåller både betydelselösa uppgifter och uppgifter av intresse för verksamheten gäller inte bestämmelsen. Det finns inte heller något krav enligt signalspaningslagen på att en upptagning eller uppteckning ska redigeras så att endast betydelsefull information får kvarstå. Det har inte ansetts praktiskt genomförbart.[106] I stället begränsas vilken information som FRA får delge till inriktande myndigheter. Enligt 8 § signalspaningslagen får rapportering endast ske av personuppgifter som är av betydelse för försvarsunderrättelseverksamheten. Sedan år 2024 omfattar bestämmelsen om betydelselös information, efter att Sverige fått kritik från Europadomstolen i detta avseende, även andra uppgifter än personuppgifter.[107]

I lagens uppräkning av sådan privilegierad kommunikation som ska förstöras återfinns

- meddelanden som omfattas av tystnadsplikten och efterforskningsförbudet för meddelare enligt tryckfrihetsförordningen och yttrandefrihetsgrundlagen,
- meddelanden mellan en misstänkt och dennes försvarare samt
- uppgifter lämnade under bikt eller enskild själavård.

Förstöringsplikten för sistnämnd kommunikation, avseende bikt eller själavård, gäller dock inte om det finns synnerliga skäl för att behandla uppgifterna, exempelvis för att kartlägga internationella terrornätverk.[108] Andra meddelanden som utgör privilegierad kommunikation ska förstöras även om de till sitt innehåll eller sammanhang är av betydelse för verksamheten.

Förstöringsskyldigheten för signaler mellan en avsändare och mottagare som båda befinner sig i Sverige är försedd med undantag för kommunikation som sänds från eller till utländsk militär personal, utländska statsfartyg, statsluftfartyg eller militära fordon och vissa signaler som inte innehåller personuppgifter. *Utredningen om över-*

[106] Prop. 2006/07:63 s. 109.
[107] Se prop. 2023/24:136.
[108] Se 7 § signalspaningslagen och prop. 2008/09:201 s. 81.

syn av lagen om signalspaning i försvarsunderrättelseverksamhet har år 2024 lämnat förslag om ytterligare undantag från förstöringsskyldigheten avseende inhemsk kommunikation, bland annat vid krig och krigsfara och i brådskande situationer som innebär fara för människors liv eller hälsa eller för omfattande förstörelse av egendom.[109]

Av lagen (2019:547) om förbud mot användning av vissa uppgifter för att utreda brott gäller vidare att uppgifter som FRA rapporterat till en annan myndighet inte får användas för att utreda brott. De brottsbekämpande myndigheterna, däribland Säkerhetspolisen, ska se till att tillgången till uppgifter som rapporterats till dem begränsas inom organisationen med särskilt beaktande av att uppgifterna inte får användas för att utreda brott.

Av 10 och 10 a §§ framkommer att den så kallade *kontrollmyndigheten*, som utgörs av Statens inspektion för försvarsunderrättelseverksamheten, ska kontrollera bland annat att förstörningsplikten upprätthålls. Kontrollmyndigheten får även besluta att inhämtade uppgifter ska förstöras, om det vid kontroll framkommer att inhämtningen inte varit förenlig med tillstånd.

Försvarets radioanstalts tekniska utvecklingsverksamhet

Försvarets radioanstalt ska enligt sin instruktion särskilt följa förändringen av signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet. Myndigheten ska också fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamheten enligt signalspaningslagen. Myndigheten ska enligt sin instruktion även utföra matematiska bedömningar av kryptosystem för totalförsvaret samt biträda andra myndigheter vid värdering, utveckling, anskaffning och drift av signalspaningssystem.

När teknik utvecklas och när nya metoder för forcering av krypterad information arbetas fram används oftast autentiskt signalspaningsmaterial för att man ska kunna vara säker på teknikens riktighet. Det autentiska materialet kan innehålla personuppgifter. Stöd för denna behandling finns i 2 kap. 5 § FRA-datalagen. Där anges att myndigheten, om det är nödvändigt för försvarsunderrättelseverksamheten, får behandla personuppgifter för att

[109] Se SOU 2024:59.

1. följa förändringar i signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet, och
2. fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamheten.

Detta ändamål speglar möjlighet som myndigheten, enligt 1 § signalspaningslagen, har att inhämta signaler för detta syfte. I signalspaningslagens förarbeten konstaterades att sådan inhämtning av teknisk karaktär sker för myndighetens egna behov av att kunna anpassa sina tekniska system och följaktligen inte genererar någon underrättelserapportering. Intrånget i den personliga integriteten bedömdes bli marginellt i jämförelse med sådan signalspaning som sker i underrättelsesyfte. Även denna inhämtning är dock underkastad lagens övriga krav, om bland annat förhandstillstånd eftersom det, enligt regeringen, inte går att utesluta att verksamheten kan komma att innefatta inhämtning av information som är känslig ur integritetssynpunkt.[110]

Tillsyn

Statens inspektion för försvarsunderrättelseverksamheten

Statens inspektion för försvarsunderrättelseverksamheten är en nämndmyndighet som består av en nämnd som fattar myndighetens beslut och ett kansli som stödjer nämnden i dess arbete. Nämndens ledamöter utses av regeringen för en bestämd tid, minst fyra år. Ordföranden och vice ordföranden ska vara eller ha varit ordinarie domare. Övriga ledamöter ska utses bland personer som föreslagits av partigrupperna i riksdagen.

Statens inspektion för försvarsunderrättelseverksamheten har till uppgift att kontrollera försvarsunderrättelseverksamheten hos de myndigheter som bedriver sådan verksamhet. Inspektionen ska kontrollera att dessa myndigheter, i den försvarsunderrättelseverksamhet som utförs, efterlever lagar och förordningar samt i övrigt fullgör sina skyldigheter.

Statens inspektion för försvarsunderrättelseverksamheten är kontrollmyndighet enligt signalspaningslagen och har ska enligt

[110] Prop. 2006/07:63 s. 72.

den lagen kontrollera att FRA följer tillstånd vid signalspaning. Inspektionen har som kontrollmyndighet befogenhet att besluta om att uppgifter som inhämtats utan stöd av tillstånd ska raderas.

Enligt 10 a § signalspaningslagen ska de finnas ett särskilt beslutandeorgan i kontrollmyndigheten som på begäran av en enskild kontrollera om hans eller hennes meddelanden har inhämtats i samband med signalspaning. Om meddelanden har inhämtats ska organet, benämnt *Delegationen för kontroll på begäran av enskild*, kontrollera huruvida inhämtningen och behandlingen av inhämtade uppgifter har skett i enlighet med lag. Det finns, till skillnad mot den motsvarande kontrollen som Säkerhets- och integritetsskyddsnämnden utför på begäran av enskild, inte någon möjlighet att få en prövning av personuppgiftsbehandlingen som inte har samband med signalspaningen.

Inspektionen ska även granska sådan behandling av personuppgifter som utförs i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst och FRA:s försvarsunderrättelse- och utvecklingsverksamhet. Vid sidan av att besluta om förstöring av uppgifter som FRA inhämtat i strid med tillstånd om signalspaning har inte inspektionen några befogenheter att fatta beslut eller förlägga om rättelse vid denna granskning. Inspektionen är dock skyldig att anmäla vissa förhållanden som kan utgöra brott till brottsutredande myndigheter eller felaktigheter som kan medföra skadeståndsansvar för staten till Justitiekanslern. Om inspektionen finner omständigheter som Integritetsskyddsmyndigheten bör uppmärksammas på, ska nämnden anmäla det till den myndigheten.[111]

Inspektionens granskningsuppgift inskränker inte Integritetsskyddmyndighetens övergripande tillsynsansvar, utan utgör en särskild granskning i syfte att kompensera för enskildas begränsade möjligheter till insyn i personuppgiftsbehandlingen inom försvarsunderrättelseverksamheten. Inspektionens fokus för tillsynen är att granska att behandlingen av enskilda personuppgifter följer regelverket.[112]

[111] Se förordningen (2009:969) med instruktion för Statens inspektion för försvarsunderrättelseverksamheten.
[112] Se https://www.siun.se/uppgifter.html (hämtad: 2025-03-23).

Integritetsskyddsmyndigheten

I 6 kap. i både FRA-datalagen och försvarsdatalagen regleras tillsyn. Det är Integritetsskyddsmyndigheten som är tillsynsmyndighet över båda dessa lagar. Tillsynsmyndighetens ska, när det är motiverat, ge råd och stöd till FRA och Försvarsmakten i frågor som gäller deras skyldigheter enligt lag eller annan författning. De båda lagarna saknar dock regler om konsekvensbedömning och förhandssamråd. Därmed kommer inte Integritetsskyddsmyndigheten att göras medveten om planerade behandlingsåtgärder. Det finns inte heller någon möjlighet för enskilda att begära att tillsynsmyndigheten ska kontroller hur de personuppgiftsansvariga myndigheterna behandlar personuppgifter i något visst avseende. Integritetsskyddsmyndighetens tillsyn är därmed i huvudsak inskränkt till initiativärenden.

Integritetsskyddsmyndigheten har i stort sett samma tillsynsbefogenheter som enligt säpodatalagen, med den skillnaden att myndigheten inte kan förbjuda fortsatt behandling vid allvarliga överträdelser.[113]

[113] Jfr bestämmelserna om korrigerande befogenheter i 7 kap. 5 § 3 säpodatalagen med 6 kap. 5 § FRA-datalagen respektive 6 kap. 4 § försvarsdatalagen.

4 Internationella förhållanden

4.1 Inledning

I detta kapitel redovisas hur personuppgiftsbehandling inom säkerhets- och underrättelsetjänster regleras i ett antal europeiska länder: Danmark, Finland, Norge, Förenade kungariket och Nederländerna. De nordiska länderna har valts ut på grund av deras närhet till Sverige och likheter i rättstradition. Övriga länder är utvalda eftersom vi uppmärksammat att frågor kring bulkdatahantering har behandlats på olika sätt i dessa.

Framställningen är översiktlig och koncentreras till de aspekter som är av störst intresse för utredningen: den rättsliga grunden för hantering av stora datamängder, relevanskrav och behovskriterier, skyddsmekanismer för känsliga personuppgifter, lagringstider samt tillsynsarrangemang. I kapitlet ingår även en beskrivning av Europarådets dataskyddskonvention, som utgör en viktig internationell rättslig ram på området.

Beskrivningarna är en sammanfattning av den rättsutredning som gjorts avseende de jämförda ländernas rättsordningar. De är inte avsedda att ge en uttömmande redogörelse, utan syftar till att identifiera olika lösningar och modeller som kan tjäna som referenspunkt vid utformningen av ett svenskt regelverk. Särskilt intresse ägnas ländernas olika sätt att balansera säkerhetsintresset mot skyddet för den personliga integriteten vid hantering av stora datamängder.

4.2 Danmark

Politiets Efterretningstjeneste (PET) är Danmarks civila säkerhets- och underrättelsetjänst och *Forsvarets Efterretningstjeneste* (FE) dess militära motsvarighet. PET är organisatoriskt placerad under Rigspolitiet (Rikspolisstyrelsen). Sedan 2013 regleras PET:s verk-

samhet och personuppgiftsbehandling i en särskild lag, PET-loven, som ersatte tidigare styrning genom regleringsbrev och regeringsinstruktioner. Samtidigt inrättades en oberoende tillsynsmyndighet, *Tilsynet med Efterretningstjenesterne* (TET).

4.2.1 Uppdrag och verksamhet

PET:s huvudsakliga uppgifter är att förebygga, utreda och motverka brott mot nationell säkerhet. Sedan 2016 har PET:s uppdrag renodlats mot kontraterrorism och kontraspionage, medan bekämpning av grov organiserad brottslighet, som tidigare ingick i tjänstens uppgifter, överförts till den reguljära polisen.

PET driver normalt inte egna ärenden till domstol utan överlämnar förundersökningar till den reguljära polisen i samband med gripanden, även om PET kan bistå under fortsatt utredning.

4.2.2 Personuppgiftsbehandling

PET-loven undantar uttryckligen underrättelsetjänsterna från den danska motsvarigheten till brottsdatalagen, men vissa principer görs tillämpliga genom hänvisningar i lagen. Ett viktigt särdrag i PET-loven är distinktionen mellan:

- **Insamling och inhämtning:** Får ske redan när uppgifterna *kan ha betydelse* för verksamheten. Detta är ett lågt ställt relevansvillkor som innebär att det inte på förhand ska kunna uteslutas att informationen är relevant. Insamling avser öppet tillgängliga uppgifter medan inhämtning gäller uppgifter som kräver särskilda åtgärder för åtkomst.
- **Vidare behandling:** Kräver att uppgifterna *kan antas ha betydelse* för underrättelseverksamheten eller *är nödvändiga* för PET:s övriga verksamhet. Detta innebär att lagring, bearbetning och spridning av personuppgifter kräver en högre grad av relevans än den initiala insamlingen.

PET har tillgång till straffprocessuella tvångsmedel och får även samla in allmänt tillgänglig information oavsett format och källa. Det finns vidare en lagreglerad skyldighet för andra myndigheter

att lämna information till PET när denna kan antas ha betydelse för arbetet mot nationella säkerhetshot.

Känsliga personuppgifter

Regleringen av känsliga personuppgifter är begränsad jämfört med svensk personuppgiftslagstiftning. Det huvudsakliga skyddet gäller uppgifter om lovlig politisk verksamhet, där PET inte får behandla personuppgifter enbart på denna grund, vilket liknar det svenska förbudet mot åsiktsregistrering.

För övrigt ska personuppgiftsbehandlingen avseende känsliga personuppgifter följa sedvanliga principer om ändamålsbundenhet, relevans och dataminimering, uppdatering och korrekthet samt informationssäkerhet.

Längsta tid för personuppgiftsbehandling

PET ska som huvudregel radera personuppgifter avseende personer i utredning eller förundersökning när inga nya uppgifter har tillkommit inom de senaste 15 åren. Radering behöver dock inte ske om det på grund av väsentliga hänsyn är nödvändigt att de bevaras för fullgörandet PET:s uppgifter. Om PET får kännedom om att uppgifter inte längre uppfyller behovskriteriet ska de raderas oavsett om fristen löpt ut eller inte. PET behöver dock inte regelbundet granska uppgifterna i syfte att göra denna bedömning. Det följer även av lagen att PET inte är skyldig att radera personuppgifter som ingår i handlingar eller liknande om handlingen i övrigt uppfyller behovskriteriet för att bevaras. Det gäller även uppgifter som exempelvis inte är relevanta för det ändamål de ursprungligen samlats in. Reglerna som innebär skyldighet att radera personuppgifter är därmed olika på uppgiftsnivå i förhållande till det som i Danmark betecknas som dokumentnivå.

Dessa regler i PET-loven kompletteras av ytterligare bestämmelser i förordning. Där anges att PET ska föra vissa register. Uppgifter som inte utgör personuppgifter, och därmed inte omfattas av personuppgiftslagstiftningen, ska raderas inom tio år från det att ett ärende inletts. Radering kan dock undvaras om fortsatt behandling av uppgifterna är nödvändig för verksamheten. För personuppgifter i

register för den operativa verksamheten ska PET vid registrering själv ange en tidsfrist för radering. Fristen får inte vara längre än fem år annat än i undantagsfall, och som längst får lagens 15-årsgräns anges, med de där angivna undantagen om längre lagringstid för uppgifter som på grund av väsentlig hänsyn är nödvändiga att lagra längre. Frångås femårsgränsen ska tillsynsmyndigheten underrättas.

För rådata, som befinner sig i det som PET betecknar som transitsystem och ännu inte förts in i någon av PET:s register för operativa eller administrativa uppgifter, är den längsta lagringstiden fyra veckor enligt förordningen. PET har vid upprepade tillfällen kritiserats av tillsynsmyndigheten för att inte följa fyraveckorsfristen i dessa så kallade transitsystem.

4.2.3 Behandling av stora datamängder

PET använder systemet PET-INTEL (en anpassad version av Palantirs Gotham-plattform) för dataanalys. Systemet, som sedan 2017 även används inom den reguljära polisen, möjliggör sökning i olika register och analytisk bearbetning av information. I samband med införandet av systemet har den danska polislagen ändrats för att ge stöd för ”tvärgående informationsanalyser” och insamling av öppet tillgänglig information.

PET-loven utvärderades år 2022. Då identifierades att nuvarande regelverk utgör ett hinder för effektiv hantering av stora datamängder (bulkdata). Kravet på att varje enskild personuppgift ska antas vara av betydelse för verksamheten ansågs begränsa möjligheten att hantera omfattande informationsmängder där merparten av uppgifterna kan vara irrelevanta.

I utvärderingen efterfrågade PET lagändringar som skulle tillåta:

- Relevansbedömning på aggregerad nivå för stora datamängder i stället för på individnivå.
- Längre bevarandetider för rådata.
- Direkt tillgång till vissa myndighetsregister.

Det danska justitsministeriet har uttalat att dessa frågor bör övervägas vid en framtida översyn av lagstiftningen, men några lagändringar har ännu inte genomförts.

4.2.4 Tillsyn

TET utövar tillsyn över PET:s personuppgiftsbehandling och prövar enskildas klagomål genom indirekt insyn. TET är både till sin organisation och sin verksamhet jämförbar med Säkerhets- och integritetsskyddsnämnden i Sverige.

TET:s tillsynsbefogenheter är likartade med den svenska motsvarighetens och innebär att TET:

- Har tillgång till samtliga uppgifter och lokaler hos PET.
- Kan begära skriftliga yttranden i sak- och rättsfrågor.
- Har egna lokaler hos underrättelsetjänsterna med möjlighet att söka självständigt i IT-system.
- Utövar även indirekt insyn genom kontroll på begäran av enskild.
- Saknar befogenhet att förelägga PET att vidta åtgärder, men kan avge yttranden och hänskjuta frågor till ministern och i förlängningen till Folketingets underrättelseutskott.

Den danska regeringen beslutade i december 2023 om en översyn av tillsynssystemet med inriktning på att utvidga TET:s mandat till att omfatta även laglighetsövervakning av operativ verksamhet.

4.3 Finland

Skyddspolisen (Skypo) är Finlands nationella säkerhets- och underrättelsetjänst med ansvar för både inrikes och vissa utrikes förhållanden. Skypo är en del av polisväsendet men är organisatoriskt placerad direkt under inrikesministeriet, till skillnad från övriga polisiära enheter som lyder under den centrala Polisstyrelsen.

4.3.1 Uppdrag och verksamhet

Skypo har till uppgift att inhämta information för att skydda den nationella säkerheten samt att upptäcka, förhindra och avslöja verksamhet som kan hota statsskicket, samhällsordningen eller rikets säkerhet. Till skillnad från Säkerhetspolisen i Sverige är Skypo en renodlad underrättelsetjänst utan förundersökningsbefogenheter, men med skyldighet att anmäla vissa brott till den ordinarie polisen.

I Finland finns en samlad reglering av Skypos verksamhet i polislagen. Civil underrättelseinhämtning definieras som inhämtande och nyttjande av information för att skydda nationell säkerhet, stödja statsledningens beslutsfattande och hjälpa andra myndigheter med deras säkerhetsrelaterade uppgifter. Lagen räknar upp elva typer av företeelser som kan vara föremål för sådan underrättelseinhämtning, bland annat terrorism, utländsk underrättelseverksamhet, massförstörelsevapen och hot mot den demokratiska samhällsordningen.

Skypo har genom lagstiftningen särskilda befogenheter att inhämta personuppgifter från andra myndigheters register, även genom teknisk anslutning eller i form av större datamängder, utan hinder av sekretessbestämmelser. Även uppgifter från privata aktörer kan inhämtas med stöd av vitesföreläggande när det gäller exempelvis passageraruppgifter.

Ett viktigt särdrag i det finska systemet är att Skypos underrättelseverksamhet utgår från abstrakta samhällshot snarare än från brottsmisstankar. Denna modell infördes när Skypo förlorade sin förundersökningsbefogenhet, för att möjliggöra inhämtning av information i ett tidigare skede och om verksamhet som inte nödvändigtvis är kriminaliserad eller har nått stadiet där konkreta brottsmisstankar kan riktas mot enskilda. Skypos civila underrättelseverksamhet syftar till att skaffa information om verksamhet som inte är kopplad till någon brottsmisstanke. Om brottsmisstanke uppstår ska bestämmelserna om polisens underrättelseinhämtning för att förhindra och avslöja brott i stället tillämpas.

4.3.2 Personuppgiftsbehandling

Skypos personuppgiftsbehandling regleras främst genom den finska brottsdatalagen och ett särskilt kapitel i polisens registerlagstiftning. Skypo får behandla personuppgifter som behövs för att:

- Skydda den nationella säkerheten.
- Förhindra, avslöja och utreda verksamhet som hotar stats- och samhällsordningen.
- Förhindra och avslöja brott mot statens säkerhet.

Den finska lagstiftningen tillämpar brottsdatadirektivets principer även på nationell säkerhet, inklusive kraven på ändamålsbundenhet, uppgifters kvalitet och uppgiftsminimering.

Känsliga personuppgifter

Finland har valt en annan modell än Sverige för reglering av personuppgifter i underrättelseverksamhet. Den finska lagstiftningen innehåller en positiv uppräkning av vilka typer av personuppgifter som får behandlas, såsom identifieringsuppgifter, familjeförhållanden och uppgifter om resande.

För känsliga personuppgifter, och vissa andra mer privata uppgifter, gäller ett förhöjt skydd. Sådana uppgifter får endast behandlas när det är *nödvändigt* för Skypos uppgifter, vilket är en högre tröskel än det allmänna kravet om att uppgifter ska *behövas*. Behandling av känsliga personuppgifter får dessutom endast ske om det finns *godtagbart skäl*.

Längsta tid för personuppgiftsbehandling

Skypo ska radera personuppgifter i underrättelseverksamheten senast 25 år efter att den sista uppgiften om personen registrerats. Vid särskilda skäl kan behandlingstiden förlängas, men detta kräver omprövning minst vart femte år.

4.3.3 Behandling av stora datamängder

Det finns i dagsläget inte någon särskild reglering för så kallad bulkdatabehandling. Finland har nyligen (december 2023) beslutat att revidera lagstiftningen om civil underrättelseinhämtning och polisens personuppgiftslag. Ett av de områden som särskilt ska under-

sökas är hanteringen av stora, öppet tillgängliga datamängder i underrättelseverksamheten. Målsättningen är att lägga fram en proposition i denna del under år 2025. Reformen motiveras av det förändrade säkerhetsläget, Finlands Nato-medlemskap och den tekniska utvecklingen.

4.3.4 Tillsyn

Tillsynen över Skypos personuppgiftsbehandling sker genom *Dataombudsmannens byrå*, som har samma befogenheter avseende Skypo som för andra personuppgiftsansvariga myndigheter. Dataombudsmannen hanterar även ärenden om indirekt insyn för enskilda.

I det finska systemet finns också en parallell tillsynen genom *Underrättelsetillsynsombudsmannen*, som är organisatoriskt samordnad med Dataombudsmannens byrå, men har ett särskilt mandat att granska lagenligheten av de metoder som används i underrättelseverksamheten. Underrättelsetillsynsombudsmannen ska bland annat granska inhämtande och insamlande av personuppgifter, men inte den efterföljande behandlingen.

I likhet med andra europeiska rättsstater finns det i Finland domstolsprövning för användandet av de mest integritetskänsliga hemliga tvångsmedlen. Utmärkande för det finska systemet är att Underrättelsetillsynsombudsmannen ska ges tillfälle att yttra sig innan ett tillståndsärende avgörs. Underrättelsetillsynsombudsmannen kan även utan tidsgräns överklaga domstolens beslut.

Att tillsynsmyndigheten på detta sätt getts yttrande- och överklaganderätt i tillståndsförfarandet har motiverats av att underrättelsetillsynsombudsmannen har befogenhet att avbryta underrättelseinhämtning också om den grundar sig på tillstånd av domstol. Ett sådant interimistiskt ingripande kan motiveras exempelvis av att inhämtning sker i strid med beslutade villkor. Dessa tillsynsbeslut underställs därefter domstolen. När tillsynsmyndigheten på detta sätt tolkar domstolens beslut och agerar på grundval av detta har det ansetts finnas skäl att även ge myndigheten rätt att yttra sig inför domstolen och överklaga.

Att Underrättelsetillsynsombudsmannen har yttranderätt i domstolen även vid den ursprunglig ansökan ersätter behovet av att, som i exempelvis Sverige, förordna om särskilda allmänna eller

offentliga ombud som ska agera motvikt mot underrättelsetjänsten i processen, vilket annars ansetts motiverat utifrån europarättspraxis.

4.4 Norge

4.4.1 Uppdrag och verksamhet

Politiets sikkerhetstjenest (PST) är Norges nationella säkerhets- och underrättelsetjänst. PST:s uppdrag regleras i den norska polislagen och omfattar att förebygga och utreda brott mot Norges självständighet och andra grundläggande nationella intressen. Detta inkluderar förräderi- och spioneribrott, terrorbrott samt brott mot den norska säkerhetslagen, som syftar till att skydda information, informationssystem och infrastruktur av nationellt intresse. PST är i likhet med Säkerhetspolisen även en polismyndighet och ingår i det nationella polisdirektoratet.

PST:s uppdrag som inhemsk underrättelsetjänst har nyligen formaliserats i polislagen. Där anges att PST ska utarbeta analyser och underrättelsebedömningar om förhållanden i Norge som kan hota landets suveränitet, territoriella integritet, demokratiska styrelseform och andra nationella säkerhetsintressen. PST har även ansvar för att utarbeta hotbildsbedömningar, samarbeta med utländska säkerhets- och underrättelsetjänster samt utföra personell säkerhetsprövning.

4.4.2 Personuppgiftsbehandling

PST:s personuppgiftshantering regleras i den norska polisregisterlagen. Lagstiftningen är gemensam för hela polisväsendet och genomför EU:s brottsdatadirektiv. Direktivet är tillämpligt för Norge genom EES-avtalet. De delar av PST:s personuppgiftsbehandling som rör nationell säkerhet, och således inte omfattas av direktivet, regleras särskilt i polisregisterlagen. Regleringen bär likheter med säpodatalagen och bygger på samma dataskyddsprinciper som brottsdatadirektivet.

För PST:s personuppgiftshantering finns sedvanliga krav på att uppgifterna ska vara adekvata och relevanta för ändamålet samt vara korrekta och aktuella. Uppgifter ska i möjligaste mån förses med

information om till vilken personkategori de hänför sig (till exempel dömd, misstänkt, målsägande) och om de är grundade på faktiska förhållanden eller utgör bedömningar. Behovskriteriet är detsamma som i Sverige, det ska vara *nödvändigt* att behandla uppgifterna för det angivna ändamålet.

Längsta tid för personuppgiftsbehandling

Det finns inte någon angiven längsta behandlingstid i lag. I stället anges att personuppgifter inte får behandlas längre än vad som är nödvändigt för ändamålet med behandlingen. Den personuppgiftsansvarige är skyldig att upprätta rutiner för att säkerställa att behovet av radering av registrerade uppgifter regelbundet bedöms.

I polisregisterlagen finns en reglering av inledande granskning av personuppgifter. PST har, i likhet med den övriga polismyndigheten, som längst fyra månader på sig att behandla personuppgifter för att avgöra om kraven på ändamål, behov och uppgifternas kvalitet är uppfyllda.

Behandling av känsliga personuppgifter

Känsliga personuppgifter som rör exempelvis ras, etniskt ursprung, politisk eller religiös övertygelse, sexuell läggning eller genetiska och biometriska uppgifter får endast behandlas om det är absolut nödvändigt för ändamålet med behandlingen. Detta gäller för PST:s ordinarie verksamhet, men särskilda undantag finns för behandling av bulkdata (se nedan om 65 a §).

4.4.3 Behandling av stora datamängder

År 2023 beslutades en ny bestämmelse (65 a §) i polisregisterlagen som ger PST betydligt utvidgade möjligheter att hantera *öppet tillgänglig information*. Med öppet tillgänglig information avses sådan som är tillgänglig för allmänheten och inte kräver att ett lösenord eller andra liknande skyddsmekanismer forceras. Även om paragrafen har en delvis teknikneutral utformning är det underförstått att bestämmelsen i dagsläget avser att träffa information som finns

publicerad på internet; exempelvis webbsidor, sociala medier eller det så kallade ”darknet”. Den föreslagna 65 a § har dock ännu inte trätt i kraft. Den beslutade lagändringen tillåter bland annat PST att:

- Samla in och lagra stora mängder öppet tillgängliga data från internet, sociala medier och andra offentliga källor.
- Behandla dessa uppgifter med automatiserade analysverktyg (exempelvis AI och algoritmer).
- Göra undantag från ordinarie krav på uppgifternas kvalitet, relevans och korrekthet.
- Behandla även känsliga personuppgifter utan ordinarie begränsningar.

En central del vid insamlingen av öppna källor är att behovskriteriet har sänkts betydligt. För insamling räcker det med att uppgifterna *kan antas vara nödvändiga* för underrättelseverksamheten – en betydligt lägre tröskel än det generella nödvändighetskravet. Den behandling som anges ovan innebär att uppgifterna behandlas automatiserat. Den insamlade informationen ska vara ”spärrad” och hållas åtskild från PST:s övriga register. Spärrad information får endast behandlas i förskrivna fall:

– För att utarbeta underrättelseanalyser och -bedömningar.
– I ärenden om förebyggande av brott inom PST ansvarsområde.
– Vid förundersökning av vissa brott.

Information som samlas in enligt 65 a § ska raderas efter fem år, men lagringstiden kan förlängas med fem år i taget upp till maximalt 15 år.

Kritik mot 65 a §

Införandet av 65 a § har mött betydande kritik från flera remissinstanser:

Datatilsynet (norska dataskyddsmyndigheten) anser att lagen medför:

- Allvarliga konsekvenser för yttrandefrihet, mötesfrihet och integritet.
- Risk för ”avkylande effekt” på det offentliga samtalet.
- Att norsk rätt inte står i överenstämmelse med europarättslig praxis om massövervakning (Europadomstolens avgöranden i målen *Big Brother Watch m.fl. mot Förenade kungariket* och *Centrum för Rättvisa mot Sverige* respektive EU-domstolens dom i målet *La Quadrature du Net m.fl.*).
- Avsaknad av nödvändiga rättssäkerhetsgarantier, särskilt oberoende förhandstillstånd.

EOS-utskottet (se nedan) har framhållit att:

- Den parlamentariska tillsynen endast består av stickprovskontroller och inte utgör en garanti mot missbruk.
- Lagen ger PST kraftfullare verktyg än vad lagtexten ger sken av.
- Det saknas tillräckliga rättssäkerhetsgarantier i linje med Europadomstolens praxis.

Myndigheter och organisationer inom IT och media har lyft:

- Risker med automatiserad analys och AI.
- Faran för bias i algoritmer baserade på känsliga personuppgifter.
- Att olika hotbildsscenarier borde mötas med olika datainsamlingsmetoder snarare än en bred ansats.
- Att datakvaliteten inte kan garanteras när öppen information behandlas utan urskiljning.

UTSYN (forskningscenter för säkerhetspolitik) föreslår att:

- Lagen bör begränsa vilken typ av information som får samlas in för olika ändamål.
- Insamlingen bör fokuseras på specifika miljöer (till exempel extremistiska forum) i stället för allmän övervakning.
- Moderna språkmodeller kan användas för att rikta insamlingen mer precist.

Sammantaget har kritiken tagit sikte på spänningen mellan säkerhetsbehov och integritetsskydd samt behovet av tydligare begränsningar, förhandskontroll och löpande utvärdering vid bulkdatahantering.

I Norge har lagändringen trots kritiken lett till ett beslut om lagändring. Den nya lagstiftningen träder dock i kraft först när så beslutas och det har ännu inte skett.

4.4.4 Tillsyn

Till skillnad från övrig personuppgiftshantering inom polisen, som övervakas av den norska *Datatilsynet*, kontrolleras PST:s verksamhet av ett parlamentariskt organ, *Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjenesten* (EOS-utskottet).

Stortinget väljer bland sina ledamöter sju personer som ska utgöra EOS-utskottet, vilka i sin tur utser ett sekretariat. Utskottet har mandat att utföra sitt arbete självständigt, men Stortinget har även möjlighet att förelägga utskottet att vidta riktad tillsyn.

EOS-utskottets uppgifter är att:

- Utöva regelbunden tillsyn över underrättelse-, övervaknings- och säkerhetstjänsterna.
- Ta emot klagomål från enskilda.
- På eget initiativ ta upp frågor som det finner anledning att behandla.

Utskottet har omfattande befogenheter, inklusive:

- Rätt att kräva tillgång till arkiv, register, lokaler och anläggningar.
- Rätt att kalla personer till förhör, med skyldighet för dem att infinna sig och vittna under straffansvar.
- Möjlighet att hålla bevisupptagning inför domstol.

Utskottets tillsyn syftar till att utreda om och förhindra att enskildas rättigheter kränks, vilket innefattar bland annat att inte mer ingripande åtgärder vidtas av myndigheterna än vad förhållandena påkallar, samt kontrollera att de mänskliga rättigheterna respekteras inom de olika verksamheterna. Utskottets tillsyn kan resultera i yttranden som rapporteras till Stortinget. Några korrigerande befogenheter finns inte. Utskottet har även möjlighet att informera allmänheten om sina iakttagelser så länge ingen hemlig information röjs.

4.5 Förenade kungariket

4.5.1 Uppdrag och verksamhet

Förenade kungarikets nationella säkerhets- och underrättelsetjänst utgörs av Security Service (MI5). Därutöver finns Secret Intelligence Service (MI6) som utgör landets utrikes underrättelsetjänst samt Government Communications Headquarters (GCHQ) som främst ägnar sig åt signalspaning.

Security Service har enligt Security Service Act 1989 till uppgift att skydda den nationella säkerheten mot hot från spionage, terrorism och sabotage, aktiviteter från främmande makt samt åtgärder som är avsedda att undergräva den parlamentariska demokratin. Myndigheten ska även skydda Storbritanniens ekonomiska intressen mot hot från utlandet och stödja brottsbekämpande myndigheter i att förebygga och avslöja grov brottslighet.

4.5.2 Personuppgiftsbehandling

De brittiska säkerhets- och underrättelsetjänsterna omfattas av den fjärde avdelningen i Data Protection Act (2018), som är modellerad efter Europarådets dataskyddskonvention (108). Personuppgifts-

regleringen för de underrättelse- och säkerhetstjänsterna utgörs av sex dataskyddsprinciper:

1. **Författningsenlighet, korrekthet och transparens** – Behandlingen ska ha rättslig grund och vara öppen.
2. **Ändamålsbegränsning** – Insamling ska ske för specifika, uttryckliga och legitima ändamål.
3. **Dataminimering** – Uppgifter ska vara adekvata, relevanta och inte onödigt omfattande.
4. **Korrekthet** – Uppgifter ska vara korrekta och uppdaterade.
5. **Lagringsbegränsning** – Uppgifter får inte bevaras längre än nödvändigt.
6. **Säkerhet** – Lämpliga tekniska och organisatoriska skyddsåtgärder ska vidtas.

Tillsynsmyndigheten *Information Commissioner's Office (ICO)* har i sin vägledning framhållit att underrättelseverksamhetens särskilda karaktär ibland gör det nödvändigt att bevara information vars värde inte omedelbart kan bedömas, men betonat att insamling och bevarande aldrig får ske urskillningslöst.

Data Protection Act innehåller ett särskilt undantag för nationell säkerhet. De flesta dataskyddsprinciper och bestämmelser får åsidosättas om det är nödvändigt för att skydda den nationella säkerheten. Undantag kan formaliseras genom ett ”national security certificate” utfärdat av regeringsföreträdare, vilket får retroaktiv verkan.

Vissa grundläggande krav kan dock inte undantas, exempelvis kravet på rättslig grund och särskilda krav för behandling av känsliga personuppgifter. Security Service har genom undantagsbeslut medgetts undantag från vissa transparenskrav och insyn för registrerade, men är fortfarande skyldig att redovisa för tillsynsmyndigheten hur lagstiftningens krav uppfylls.

Känsliga personuppgifter

För känsliga personuppgifter finns ytterligare krav på att behandlingen ska vara nödvändig för att bland annat skydda en enskilds vitala intressen eller för lagföring, under förutsättning att den känsliga uppgiften inte offentliggjorts av den registrerade själv.

Behandlingstid

Den femte dataskyddsprincipen innebär att uppgifter inte får behandlas längre än nödvändigt. Tillsynsmyndigheten ICO har betonat att avsaknaden av lagstadgade tidsgränser innebär att det ofta krävs att den personuppgiftsansvarige utarbetar policys för den tid som uppgifter får bevaras. En sådan policy ska kunna rättfärdigas på objektiva grunder. Av förarbetena framgår även att det antingen bör fastställa tidsfrister för radering eller för periodisk översyn.

4.5.3 Behandling av stora datamängder

Hanteringen av stora datamängder regleras mer utförligt i *Investigatory Powers Act 2016 (IPA)*. Lagen reglerar fyra huvudsakliga metoder för hantering av bulkdata:

- Odifferentierad signalspaning (bulk interception).
- Massinsamling av kommunikationsuppgifter (bulk acquisition).
- Massdataavläsning (bulk equipment interference).
- Stora personuppgiftssamlingar (bulk personal datasets).

Ett utmärkande drag för det brittiska systemet är principen om ”dubbla lås” (double-lock). Processen innebär att:

– Ansvarig minister fattar beslut om tillstånd efter att ha bedömt nödvändighet och proportionalitet.

– Beslutet underställs granskning av en särskild domare (Judicial Commissioner) inom tillsynsorganet IPC (se nedan) som laglighetsprövar beslutet.

Samtliga tillståndstyper för bulkdata omfattar både metoden för insamling och den efterföljande behandlingen. Tillstånden är tidsbegränsade till sex månader, med möjlighet till förlängning.

Särskilt relevant för utredningen är regleringen av stora personuppgiftssamlingar som inhämtats från andra källor än signalspaning eller dataavläsning. Enligt IPA omfattas sådana dataset när:

- De innehåller personuppgifter om ett flertal individer.
- Majoriteten av individerna inte är av intresse för underrättelsetjänsten.
- Uppgiftssamlingen behålls för analys i underrättelseverksamheten.

Underrättelsetjänsterna får, under en begränsad tid, göra en initial analys av en sådan uppgiftssamling för att bedöma dess värde. För fortsatt behandling krävs tillstånd enligt systemet med dubbla lås. Uppgiftssamlingar kategoriseras utifrån känslighetsgrad:

- *Lägre känslighetsgrad*: Rena identifikationsuppgifter som namn eller adress i elektroniska telefonkataloger etc.
- *Högre känslighetsgrad*: Privata och känsliga uppgifter som rör enskildas privat- eller familjeliv, exempelvis privata meddelanden.

För dataset med lägre känslighet kan tillstånd ges för en viss typ av uppgiftssamlingar (class warrant). För dataset med högre känslighet krävs specifika tillstånd (specific warrant) med särskilda villkor för åtkomst och sökningar för varje dataset.

Ett centralt inslag i det brittiska systemet är begränsningarna för hur insamlad data får sökas igenom. Sökningar i stora dataset:

- Får endast ske för operativa ändamål som uttryckligen angivits i tillståndet.
- Måste vara nödvändiga och proportionerliga i varje enskilt fall.
- Ska dokumenteras med skriftliga motiveringar.
- Är föremål för särskild kontroll, när det gäller personer som befinner sig på brittiskt territorium.
- Underkastas särskilda regler för känsliga kategorier (till exempel journalister).

4.5.4 Tillsyn

Tillsyn över underrättelsetjänsternas generella personuppgiftshantering utförs av den brittiska datatillsynsmyndigheten Information Commissioner (ICO). Den generella tillsynen kan beskäras genom särskilda undantag, motiverade av nationell säkerhet, som tillgång till vissa lokaler, dokument eller utrustning vid inspektion.

Tillsynen över de särskilda befogenheter som regleras i IPA, bland annat stora personuppgiftssamlingar utförs av Investigatory Powers Commissioner (IPC). IPC:s tillsyn kompletterar ICO:s mer generella personuppgiftstillsyn. Till skillnad från ICO:s tillsyn kan IPC:s tillsynsbefogenheter dock inte begränsas genom undantag för nationell säkerhet. Vid allvarliga överträdelser kan IPC informera den berörda individen om möjligheten att klaga till en särskild domstol för indirekt insyn och klagomål om övervakningsåtgärder, Investigatory Powers Tribunal. IPC organiserar de domare som laglighetsprövar beslut om bland annat signalspaning och behandling av stora personuppgiftssamlingar.

Tillsynsarbetet vid IPC stöds av en särskild, lagreglerad, rådgivande panel (Technology Advisory Panel) som bistår med expertkunskap om teknisk utveckling och möjligheter att minska integritetsintrång genom nya tekniska lösningar.

4.6 Nederländerna

4.6.1 Uppdrag och verksamhet

I Nederländerna finns två underrättelsetjänster med ansvar för nationell säkerhet: den civila Allmänna underrättelse- och säkerhetstjänsten (AIVD) och Militära underrättelse- och säkerhetstjänsten (MIVD). Båda lyder under lagen om underrättelse- och säkerhetstjänster från 2017, kallad Wiv 2017, som reglerar deras organisation, metoder och personuppgiftsbehandling i verksamhet som gäller nationell säkerhet.

AIVD bedriver underrättelsearbete om organisationer och individer som kan misstänkas utgöra hot mot demokratin eller nationell säkerhet. Till skillnad från Säkerhetspolisen i Sverige saknar AIVD polisiära befogenheter.

4.6.2 Personuppgiftsbehandling

I Nederländerna regleras underrättelsetjänsternas personuppgiftsbehandling i samma lagstiftning som deras allmänna uppdrag och befogenheter, utan separat personuppgiftslag. Generellt gäller för personuppgiftsbehandling att:

- Personuppgifter endast får samlas in om det är proportionerligt i förhållande till motstående intressen.
- Behandling ska vara nödvändigt för ett specifikt ändamål.
- All behandling ska ske författningsenligt, korrekt och noggrant.
- Alla personuppgifter ska förses med upplysning om sakriktighet eller källhänvisning.

Behandling i form av *insamling* av personuppgifter ska uttryckligen ske efter en proportionalitetsbedömning. Det innebär att det minst ingripande sättet för datainsamling ska ske utifrån hotets allvar och de värden som ska skyddas. Vidare ska åtgärden vara proportionerlig både i förhållande till den skada eller olägenhet som den kan komma att orsaka och i förhållande till syftet med åtgärden.

Om en mindre ingripande åtgärd är möjlig måste den användas. Insamling av personuppgifter får enligt lagen ske från öppna källor, kommersiellt tillgängliga databaser eller sådan information som underrättelsetjänsten har tillgång till med stöd av författning, som exempelvis passagerardata. Uppgifter får även inhämtas från informanter, genom att använda särskilt reglerade hemliga tvångsmedel och genom samarbete med andra underrättelsetjänster eller myndigheter. Andra källor för inhämtning får utnyttjas endast efter tillstånd från ansvarig minister.

Insamling är ett begrepp som i lagen ofta används åtskilt från begreppet behandling, som i övrigt har den vedertagna betydelsen, vilken innefattar i princip alla åtgärder som vidtas med personuppgifter.

Det finns en särskild uppräkning av de personer vars personuppgifter AIVD får behandla. Bland annat personer som kan misstänkas utgöra en fara för nationell säkerhet. Personuppgifter får även behandlas om det är nödvändigt för att upprätta en hot- och riskanalys eller om informationen har samlats in av en annan underrättelse-

tjänst. Ett viktigt undantag är att personuppgiftsbehandling även är tillåten avseende andra personer om uppgifterna utgör ”en logisk och oskiljaktig del av en databas som tillhandahålls eller förvärvats”. Detta undantag är centralt för hanteringen av stora datamängder.

Känsliga personuppgifter

Behandling av personuppgifter får inte ske på grundval av känsliga personuppgifter, men sådana uppgifter får behandlas om det sker utöver behandlingen av andra uppgifter och om det är nödvändigt för ändamålet.

Behandlingstid

När det gäller lagringstid för personuppgifter medger Wiv 2017 att personuppgifter får behandlas så länge de är nödvändiga för sitt ändamål. Om uppgiften har förlorat sin betydelse för ändamålet måste den raderas. Denna bestämmelse kompletteras av det allmänna stadgandet om författningsenlig, korrekt och noggrann personuppgiftsbehandling och är behäftad med vissa undantag för uppgifter som samlats in med särskilda metoder.

Genom signalspaning, hemlig dataavläsning och andra särskilda befogenhet kan underrättelsetjänsterna komma att samla in mycket stora mängder personuppgifter. Huvudregeln är att dessa uppgifter så snart möjligt, dock senast inom ett år, ska bedömas för att avgöra om de är relevanta för de ändamål för vilka de samlats in eller något annat lagligt ändamål. Myndighetschefen kan förlänga ettårsfristen för en viss kategori uppgifter till maximalt ett år och sex månader. Personuppgifter som inte bedömts efter denna tid ska omedelbart raderas.

4.6.3 Behandling av stora datamängder

Wiv 2017 skiljer mellan allmänna och särskilda befogenheter. Särskilda befogenheter avser integritetskänsliga metoder som kräver tillstånd. Av de allmänna befogenheterna har två särreglerats: systematisk insamling från öppna källor och insamling genom informanter.

Systematisk insamling av öppen information

För systematisk insamling av öppet tillgänglig information krävs tillstånd från ansvarig minister (eller i vissa fall myndighetschefen genom delegation). Tillståndet omfattar tre månader och kräver beskrivning av ändamål och motivering av nödvändighet. Denna reglering motiveras av att systematisk insamling från olika öppna källor enligt nederländsk tolkning av europarättspraxis utgör ett allvarligt integritetsintrång som kräver särskilda rättssäkerhetsgarantier.

Bulkdata från informanter

En särskild möjlighet i Wiv 2017 är att underrättelsetjänsterna kan ta del av information genom ”informanter”, vilket i lagen avser såväl andra myndigheter som privata aktörer. En viktig aspekt är att informanter kan tillhandahålla data i form av datafiler eller genom direktåtkomst till databaser.

Detta har gett AIVD möjlighet att:

- Få direktåtkomst till data hos privata företag via samarbetsvilliga anställda.
- Förvärva stora datamängder från datamäklare eller internet, som exempelvis läckt från dataintrång (även anonyma fildelningssajter betraktas som ”informanter”).

Tillsynsmyndigheter har rapporterat att AIVD med stöd av dessa befogenheter har förvärvat stora dataset tillgängliga på darknet, med uppgifter om hundratals miljoner individer, där endast en liten del av personuppgifterna är direkt relevanta för myndighetens verksamhet.

”Inside box – outside box”-modellen för stora datamängder

Det är den nederländska signalspaningsmyndigheten som behandlar stora datamängder enligt en särskild modell, ursprungligen utformad som en intern policy men senare formaliserad i en temporär föreskrift. En lagstiftningsprocess pågår för att reglera behandlingen på lagnivå.

Den temporära regleringen bygger på principen om ”inside box – outside box” och utgörs av en process i flera steg:

1. **Initialbedömning:** När stora datamängder förvärvas görs en bedömning av om den innehåller sådana uppgifter som innebär intrång i privatlivet.
2. **Kategorisering:** Baserat på bedömningen kategoriseras datasetet som antingen *tillgängligt*, *begränsat* eller *strikt begränsat*.
3. **Outside box-hantering:** Stora datamängder som kategoriserats som begränsade placeras i en så kallad ”outside box” till vilken endast ett fåtal tekniker har tillgång. Andra tjänstemän kan göra sökningar i outside-box men endast få ett binärt resultat: träff/icke-träff.
4. **Ansökan om tillgång:** I datamängder som är begränsade eller strikt begränsade kan tillgång medges endast efter en skriftligt motiverad begäran. Vilka krav som ställs beror på om det är en begränsad eller strikt begränsad uppgiftssamling.
5. **Inside box:** När uppgifter efter godkänd begäran flyttas till ”inside box” blir de gemensamt tillgängliga för verksamheten och behandlas enligt de regler som gäller i övrigt.

Behovet av de stora dataset som behandlas enligt denna reglering ska omprövas med jämna mellanrum. Beroende på hur känsliga uppgifterna bedömts vara vid kategoriseringen ska detta göras med olika intervall: Dataset som kategoriserats som tillgängliga efter 36 månader, begränsade efter 24 månader och strikt begränsade efter 12 månader.

Automatisk analys

Wiv 2017 reglerar även automatisk analys av stora datamängder. Underrättelsetjänsterna får använda automatisk dataanalys på uppgifter från:

- Egna samlingar.
- Öppen information.
- Databaser med direktåtkomst.

- Uppgifter från tredje part.
- Metadata från signalspaning.

Den automatiska analysen, som kan innefatta profilering och mönsterigenkänning, är dock begränsad genom att resultatet inte ensamt får leda till åtgärder mot enskilda. Stordataanalyser måste kompletteras med annan bekräftande information innan myndigheten vidtar åtgärder mot en viss person, vilket förhindrar så kallad ”predictive policing” baserad enbart på automatiserad analys.

4.7 Europarådets dataskyddskonvention

4.7.1 Konventionens ställning och syfte

Europarådets konvention 108 av den 28 januari 1981 om skydd för enskilda vid automatisk databehandling av personuppgifter (ETS 108), den så kallade dataskyddskonventionen, utgör en central internationell rättslig ram för personuppgiftsskydd. Konventionen, som trädde i kraft den 1 oktober 1985, har ratificerats av samtliga Europarådets 46 medlemsstater.[1] Därutöver har flera icke-europeiska länder anslutit sig, däribland Argentina, Kap Verde, Marocko, Mauritius, Mexiko, Senegal, Tunisien och Uruguay.

Dataskyddskonventionen brukar betraktas som en precisering av artikel 8 i Europakonventionen när det gäller automatisk databehandling av personuppgifter. Den syftar till att säkerställa respekten för grundläggande fri- och rättigheter, särskilt den enskildes rätt till personlig integritet vid automatiserad personuppgiftsbehandling. Medan EU:s dataskyddsförordning har övertagit konventionens roll som grundläggande dokument för automatiserad behandling av personuppgifter inom stora delar av EU:s kompetensområde, är konventionen fortsatt av särskild betydelse för områden som ligger utanför unionsrätten, såsom nationell säkerhet, försvar och statens säkerhet.

[1] För Sveriges del se SÖ 1982:50.

4.7.2 Grundläggande principer

Dataskyddskonventionen omfattar automatiserad behandling av personuppgifter inom både allmän och enskild verksamhet. De grundläggande principerna i konventionen inkluderar:

- Krav på att uppgifter ska inhämtas och behandlas författningsenligt och på ett korrekt sätt, lagras endast för särskilda och berättigade ändamål och inte därefter behandlas på ett sätt som är oförenligt med dessa ändamål (artikel 5 a–b).
- Krav på uppgifternas kvalitet som innebär att uppgifter ska vara
  - adekvata, relevanta och inte för omfattande i förhållande till ändamålet (artikel 5 c),
  - korrekta och om nödvändigt uppdaterade (artikel 5 d).
- Krav på att uppgifter inte ska behandlas längre än vad som är nödvändigt för ändamålet (artikel 5 e).
- Särskilt skydd för känsliga personuppgifter som avslöjar ras, politisk tillhörighet, religiös övertygelse, sexualliv samt uppgifter om brott (artikel 6).
- Rätt för registrerade, bland annat, att få veta vilken information som lagras och att få den korrigerad (artikel 8).

Från de ovanstående principerna får dock medlemsstaterna göra undantag, så länge det är nödvändigt i ett demokratiskt samhälle för att bland annat skydda nationell säkerhet.

Europarådets ministerkommitté antog år 2001 ett tilläggsprotokoll till dataskyddskonventionen (ETS 181), som trädde i kraft den 1 juli 2004. Protokollet, som Sverige har ratificerat, innehåller två huvudsakliga kompletteringar:

Krav på tillsynsmyndigheter. Varje konventionsstat ska inrätta en eller flera oberoende tillsynsmyndigheter för att kontrollera efterlevnaden av dataskyddsprinciperna. Myndigheterna ska ha utrednings- och ingripandebefogenheter samt kunna delta i rättsliga förfaranden.

Gränsöverskridande dataflöden. Bestämmelser som reglerar överföring av personuppgifter till länder som inte är parter till kon-

ventionen. Sådan överföring får bara ske om mottagarlandet säkerställer en adekvat skyddsnivå för de aktuella uppgifterna.

4.7.3 Moderniserad konvention (108+)

Efter en omfattande översyn antog Europarådets medlemsstater den 18 maj 2018 ett ändringsprotokoll till dataskyddskonventionen (CETS 223), informellt kallad *dataskyddskonventionen 108+*. Protokollet innebär en modernisering av konventionen som syftar till att harmonisera den med EU:s dataskyddsreform och andra internationella instrument.

Bland de viktigaste förändringarna i den moderniserade konventionen kan nämnas:

- Stärkta krav på proportionalitet och rättslig grund för behandling.
- Krav på inbyggt dataskydd och konsekvensbedömningar.
- Förstärkta rättigheter för registrerade, bland annat avseende automatiskt beslutsfattande.

Ändringsprotokollet träder i kraft när det har ratificerats av samtliga Europarådets medlemsstater, men tillåter även ett partiellt ikraftträdande. Sverige har undertecknat men ännu inte ratificerat ändringsprotokollet. Dataskyddskonventionen 108+ har (i mars 2025) ratificerats av 33 medlemsstater och kommer träda i kraft partiellt när dessa följts av ytterligare fem medlemsstater.

Den moderniserade konventionen kommer få betydelse för underrättelsetjänsternas personuppgiftsbehandling

Dataskyddskonventionen gäller även för personuppgiftsbehandling som rör nationell säkerhet, men medger undantag från alla centrala principer. Detta gäller inte för den moderniserade konventionen 108+. För kraven på proportionalitet, rättslig grund och författningsenlig behandling är det inte möjligt att göra undantag. Detsamma gäller för bestämmelserna om särskilt skydd för känsliga personuppgifter; en kategori som dessutom utökats genom tilläggsprotokollet. Det finns dessutom endast begränsade möjligheter att undanta

behandling som rör nationell säkerhet från kravet på oberoende tillsyn.

Detta gör den moderniserade dataskyddskonventionen till ett viktigt rättsligt instrument för underrättelsetjänsters verksamhet. Konventionens principer för dataskydd kommer att utgöra en bindande minimistandard som medlemsstaterna måste iaktta i sin nationella lagstiftning. Avvägningen mellan dataskydd och nationell säkerhet är dock fortsatt en fråga som hanteras på nationell nivå inom de ramar konventionen sätter upp.

5 En komplex hotbild mot Sverige

5.1 Inledning

I detta kapitel tecknar vi en ögonblicksbild av Säkerhetspolisens bedömning av det säkerhetsläge som råder då detta betänkande avlämnas. Beskrivningen är naturligtvis inte heltäckande.

Hotbilden mot Sverige blir alltmer komplex och det ställer förändrade krav på Säkerhetspolisens förmåga. För att lösa sitt uppdrag behöver myndigheten ha tillgång till relevant information och på ett effektivt sätt kunna hantera och bearbeta de stora informationsmängderna. Syftet med denna utredning är att ge Säkerhetspolisen effektivare verktyg i detta avseende.

Beskrivningen i detta kapitel avser att ge en ökad förståelse för de säkerhetshot som riktas mot Sverige och vilka nationella säkerhetsintressen som står på spel. Genom att förstå hoten är det lättare att avgöra vilka verktyg som behövs för att motverka dem.

5.2 Hotbilden i dag

5.2.1 Allmänt om säkerhetsläget

Säkerhetsläget i omvärlden och i Sveriges geografiska närområde har allvarligt försämrats, vilket även har betydelse för Sveriges inre säkerhet. Det försämrade säkerhetsläget har både breddat och förändrat hotbilden mot Sverige och därigenom också gjort den mer komplex. Auktoritära stater har blivit allt mer offensiva i sitt agerande samtidigt som våldsbejakande extremister och statliga aktörer opportunistiskt utnyttjar händelseutvecklingen i Sverige och omvärlden för att driva och legitimera aktiviteter och verksamhet som riskerar att hota grundläggande demokratiska principer och undergräva förtroendet för staten och demokratin.

Våldsbejakande extremister såväl som statliga aktörer söker ständigt efter sårbarheter att utnyttja för att i förlängningen stärka sina egna positioner. Dessa aktörer nyttjar i dag ett brett spektrum av metoder för att försvaga det svenska samhället. Ryssland, Kina och Iran är de statliga aktörer som i dagsläget är mest offensiva och aktiva i att bedriva säkerhetshotande verksamhet mot Sverige. Genom att kontinuerligt bedriva underrättelseverksamhet, påverkansaktiviteter, cyberangrepp och olovlig teknik- och kunskapsanskaffning försöker statliga aktörer att tillskansa sig fördelar och påverka individer, politiskt beslutsfattande såväl som den allmänna opinionen.

Våldsutövning, antingen genom ombud eller genom egna initiativ, kan även riktas mot Sverige eller mot mål i Sverige för att uppnå givna målsättningar. Sverige är ett intressant mål för statliga aktörer i synnerhet avseende den framstående forsknings- och industrisektorn. Likväl är Sverige en arena för statliga aktörer att agera på inom ramen för en större konflikt, vilket i förlängningen har en inverkan på Sveriges säkerhet. Generellt har det förändrade omvärldsläget förändrat karaktären av hotet från statliga aktörer, som i dag utgör ett allvarligt hot mot Sveriges säkerhet.

Även hotet från våldsbejakande extremism har förändrats över tid. Attentatshotet består samtidigt som mycket av den verksamhet och aktivitet som bedrivs utgör ett bredare hot mot demokratin. Detta berör inte nödvändigtvis enbart brottsliga handlingar, utan utgörs även av verksamhet inom demokratins ramar men som syftar till att underminera och utmana staten och samhället. Till viss del nyttjar våldsbejakande extremister liknande metoder som statliga aktörer för att öka splittringen och polariseringen i samhället för att i förlängningen uppnå mål inom ramen för den ideologiska uppfattningen, exempelvis genom subversiv verksamhet och påverkan.

Gränserna mellan våldsbejakande extremism och extremism är även mer otydliga i dag jämfört med tidigare. Konspirationsteorier, alternativa världsåskådningar och desinformation sprids och anammas av såväl våldsbejakande extremister som av övriga samhällsmedborgare vilket gör att extremistiska och våldsbejakande budskap får ett bredare fäste i samhället. Tillsammans med möjligheten att genom digitala plattformar nå en bred publik nås fler personer i dag av extremistiska budskap vilket i förlängningen bidrar till en normalisering och legitimering av våld och avhumanisering av meningsmotståndare. Det sänker tröskeln för engagemang i våldsbejakande

extremistiska miljöer. Polarisering och omvärldsutvecklingen bidrar även det till en växande extremism och ett bredare hot mot samhället.

Nyttjandet av digitala plattformar är många gånger centralt för att bedriva säkerhetshotande verksamhet då dessa erbjuder möjligheter till effektiv och snabb spridning av våldsbejakande och extremistiska budskap, internationalisering av rörelser och narrativ samt förmågan att kunna verka i det dolda och undgå motåtgärder. Sett till den generella digitaliseringen kommer mörkertalet av hotaktörer som primärt är verksamma online sannolikt att öka framöver. Aktivitetsnivån online tillsammans med en generell normalisering av vissa våldsbejakande budskap gör det även svårt att bedöma aktörers avsikt att realisera potentiella hot som de ger uttryck för.

5.2.2 Främmande makts säkerhetshotande verksamhet

Främmande makt bedriver en systematisk och omfattande säkerhetshotande verksamhet mot Sverige i syfte att stärka sin ställning och sina förmågor på bekostnad av Sverige och svenska intressen. Den säkerhetshotande verksamheten utgörs av en bredd av aktiviteter såsom exempelvis underrättelseinhämtning, teknikanskaffning, påverkansaktiviteter, cyberangrepp och attentat mot individer i Sverige. Säkerhetspolisen har identifierat Ryssland, Kina och Iran som de aktörer som utgör de allvarligaste hoten mot Sverige och svenska intressen.

Ryssland bedriver kontinuerlig och omfattande säkerhetshotande verksamhet mot Sverige och svenska intressen utomlands. Det handlar huvudsakligen om underrättelseinhämtning och teknikanskaffning, men även olika former av påverkan, i syfte att stärka Rysslands geopolitiska, ekonomiska, teknologiska och militära mål. Uppdraget inbegriper också att undanröja hot mot den egna regimen. Rysk säkerhetshotande verksamhet i Sverige riktas bland annat mot politiker och tjänstemän, det svenska totalförsvaret, civil och militär industri samt individer i Sverige som kritiserar den ryska regimen. Ryska statliga aktörer agerar även opportunistiskt på händelser i omvärlden för att nå sina mål. Det innebär bland annat att ryska statliga aktörer bedriver påverkanskampanjer utifrån händelser som de själva kanske inte ligger bakom men som kan passa in på det egna syftet. Centrala aktörer för rysk säkerhetshotande verksamhet

i Sverige är de ryska underrättelse- och säkerhetstjänsterna. I Sverige utgår de ryska tjänsternas verksamhet från de ryska beskickningarna i Stockholm, icke-officiella plattformar såsom företag och organisationer samt tillfälligt inresande underrättelseofficerare. De ryska tjänsterna rekryterar också agenter och ombud i Ryssland och i tredje land. Tekniska förmågor såsom cyberspionage och signalspaning används kontinuerligt för att spionera på svenska mål. Därtill förfogar Ryssland över förmågor som vid behov kan användas för sabotage.

Även de kinesiska underrättelsetjänsterna bedriver en omfattande säkerhetshotande verksamhet mot Sverige och svenska intressen. Målet är att nå Kinas långsiktiga ambition att positionera sig som en global stormakt. Svensk teknik, produkter, kunskap och information bedöms vara av stort värde för att uppnå detta. Kinesiska investeringar och nyetableringar inom sektorer som är prioriterade av den kinesiska staten har under det senaste decenniet ökat i Sverige. De sker bland annat i syfte att tillgodogöra sig teknik och kunskap samt för att få tillgång till nätverk och utvecklingsplattformar, men även för att möjliggöra påverkan av svenskt beslutsfattande. Kinesisk verksamhet i form av strategiska uppköp och nyetableringar, anskaffning av teknik, produkter och särskild kunskap utgör ett allvarligt hot mot Sverige och svenska intressen. Underrättelseaktiviteter mot regimkritiker för att hota och reducera deras yttrande- och handlingsfrihet bedrivs kontinuerligt av Kina mot individer i Sverige. Det finns en mycket hög förmåga hos kinesiska aktörer gällande elektroniska angrepp och Kina använder i stor utsträckning cyberangrepp för att inhämta information.

Iran bedriver säkerhetshotande verksamhet i och mot Sverige och svenska intressen i form av underrättelseinhämtning, påverkan mot oppositionella och genom anskaffningsverksamhet. Den säkerhetshotande verksamheten omfattar även hot och våld mot individer. I Sverige har Irans underrättelseverksamhet i första hand varit riktad mot ledande oppositionella inom den iranska diasporan. Iran har tidigare använt våld i andra länder i Europa i syfte att tysta kritiska röster och upplevda hot mot den egna regimen. För att utföra dessa säkerhetshotande aktiviteter har den iranska regimen vid tillfällen använt sig av kriminella nätverk. På senare år sker detta även i Sverige. Svensk teknologi som produkter med dubbla användningsområden och kritiska spetsprodukter för både civil och militär

användning är av intresse för Iran. Iran anskaffar både teknik och kunskap genom olovliga metoder, och utvecklar bland annat sin egen förmåga på svenska universitet och lärosäten. Iran bedriver industrispionage som främst riktas mot svensk högteknologisk industri

5.2.3 Cyberangrepp

I takt med den digitala utvecklingen ökar både främmande makts och kriminella grupperingars möjligheter att använda cyberangrepp för att nå sina mål. Kriminella aktörer använder cyberangrepp för att stjäla information och utpressa offer på pengar vilket ofta medför stora och svåra konsekvenser för den drabbade.

Främmande makts underrättelse- och säkerhetstjänster använder inhämtning via cyberangrepp som ett verktyg för informationsinhämtning/underrättelseinhämtning/spioneri. En del av dessa aktörer har också förmåga att använda förstörande angrepp som en del i pågående väpnad konflikt. Rysslands cyberangrepp mot Ukraina är ett bra exempel på detta som visar hur dessa typer av angrepp kan användas för att försöka slå ut samhällsviktiga funktioner och infrastruktur.

5.2.4 Subversiv verksamhet i Sverige

Motståndet mot staten, samhället och dess företrädare har alltid varit en grundbult i den våldsbejakande extremismen oavsett ideologisk drivkraft. Säkerhetspolisen beskriver att det även finns ett samhällshot i dag som inte utgår från brottsliga handlingar utan snarare handlar om spridande av desinformation som kan hämta sin grund från olika konspirationsteorier om att staten är illegitim och korrupt. Sådana konspirationsteorier återfinns även utanför de våldsbejakande extremistmiljöerna och extrema idéer och antistatliga narrativ har fått fäste i ett bredare samhällsskikt. Detta kan i sin tur utnyttjas av såväl våldsbejakande extremister som främmande makt vilket i förlängningen kan utgöra ett säkerhetshot. Två sentida exempel är stormningen av Kapitolium i USA i januari 2021 och tillslaget i Tyskland år 2022 som grundandes på misstankar om en planerad statskupp.

Säkerhetspolisen har även beskrivit hur våldsbejakande extremister uppmanar till att infiltrera olika delar av samhället för att kunna höja sin förmåga, till exempel i strid och vapenhantering, men även för att kunna påverka olika beslut eller inriktningar. Uppmaningar till infiltration kan även handla om att långsiktigt, i det fördolda eller lågmält, undergräva förtroendet för samhället.

5.2.5 Radikalisering

Säkerhetspolisen beskriver att de aktörer som myndigheter följer har påverkats och förändrat sina arbetssätt i det uppkopplade samhället. I dag nås allt fler, särskilt unga personer, av våldsbejakande extremisters budskap där avhumanisering och legitimering av våld blir allt vanligare. Interaktionen sker främst på digitala plattformar där det finns stora möjligheter att verka i det fördolda. Hastigheten, räckvidden och möjligheten att både skapa nya allianser och att nå andra som delar samma världsbild sänker tröskeln för att engagera sig i en våldsbejakande extremistisk miljö. Extrema tankar och uttryck har i vissa kretsar normaliserats och i viss mån accepteras. Det kan därför vara svårt att veta vilka individer som är beredda att agera för att skada samhället och vilka som bara uttrycker sig extremt. Flera av de aktörer som på egen hand har planerat eller utfört attentat eller andra grova våldsbrott har ingått i digitala gemenskaper där de har interagerat med likasinnade i olika delar av världen. I flera fall sker detta i de krypterade delarna av internet, där information enbart är tillgänglig en kort tid.

Säkerhetspolisen har särskilt uppmärksammat hur radikaliserande krafter sänder ut sina budskap i kanaler där barn och unga spenderar tid, som populära sociala mediekanaler samt gaming- och streamingplattformar. Det beror delvis på att våldsbejakande extremister har en långsiktig målsättning med sin verksamhet och därför fokuserar på att rekrytera ungdomar som anses vara påverkningsbara. Men också på att många våldsbejakande extremister själva är unga och kan interagera relativt ostört med sina jämnåriga i sociala medier. Det kan exempelvis handla om att ideologiskt övertygade personer uttrycker hat mot samhället eller grupper på sådana forum och delar med sig av instruktioner och manualer om vapen- och sprängmedelstillverkning.

5.2.6 Terrorism

Terrorism och annan ideologiskt motiverad brottslighet syftar till att skada Sverige som stat, injaga fruktan i befolkningen och destabilisera demokratin. Denna typ av brottslighet utgör ett allvarligt hot mot den svenska samhällsordningen. Det traditionella attentatshotet mot Sverige utgörs främst av ensamagerande gärningspersoner som motiveras av våldsbejakande islamistisk extremism eller våldsbejakande högerextremism och som agerar för att förändra samhällsordningen. Dessa personer utgår inte sällan från en virtuell gemenskap där det finns ett narrativ som både formar hat och försvarar användandet av våld. Uppmaningen och plikten att *göra vad du kan, med de medel du har, där du är nu* förmedlas på flera olika sätt och avser såväl attentat och grova våldsbrott som aktiviteter som syftar till att polarisera, underblåsa och hetsa fram en samhällskollaps.

Säkerhetspolisen har under senare år sett ett ökat antal attentatshot mot Sverige och svenska intressen utomlands, där Sverige har stått i större fokus för våldsbejakande islamistisk extremism. Myndigheten beskriver att denna händelseutveckling även gynnar främmande makt och påverkar den våldsbejakande högerextremismen.

5.3 Hotbilden i framtiden

Den komplexa hotbilden mot Sverige från statliga aktörer och våldsbejakande extremism kommer sannolikt att bestå på kort och lång sikt. Statliga aktörer och våldsbejakande extremistiska aktörer kommer fortsättningsvis att agera opportunistiskt utifrån händelseutvecklingen i omvärlden och i Sverige för att uppnå sina målsättningar. Detta kan ta sig uttryck på flertalet olika sätt, både i form av brottsliga och icke-brottsliga handlingar, och kommer sannolikt att ske kontinuerligt och parallellt samt riktas mot flera olika delar av samhället vilket både breddar och intensifierar hotbilden mot Sverige.

Ryssland, Kina och Iran kommer fortsatt vara de stater som bedriver säkerhetshotande aktiviteter med de mest allvarliga konsekvenser för Sveriges säkerhet. Samtidigt kommer det vara utmanande för statliga aktörer att bedriva verksamhet utifrån officiella plattformar framöver med tanke på de motåtgärder som riktas mot dem, både i Sverige och internationellt. Därav kan statliga aktörer i större utsträckning komma att nyttja ombud och andra icke-officiella

plattformar för att bedriva säkerhetshotande verksamhet exempelvis i form av påverkan och underrättelseinhämtning eller i syfte att destabilisera och undergräva förtroendet för staten och samhället.

Nyttjandet av ombud och icke-officiella plattformar ger även statliga aktörer möjligheten att agera förnekbart och till viss del dölja sin aktivitet och verksamhet. I och med teknikutvecklingen har statliga aktörer även möjlighet att effektivisera sin verksamhet och utveckla både nya och befintliga metoder för att exempelvis agera förnekbart samt nyttja cyberangrepp och informationspåverkan i syfte att destabilisera det svenska samhället.

Teknikutvecklingen och den digitala arenan är även central för hotet från våldsbejakande extremism framöver. Radikalisering och spridandet av våldsbejakande och extremistiska budskap på digitala plattformar kommer fortsatt att ha en central betydelse för såväl attentatshotet mot Sverige som för tillväxten i våldsbejakande miljöer. Händelser i omvärlden och i Sverige kommer att nyttjas opportunistiskt av aktörer i Sverige såväl som av internationella terrororganisationer för att uppmana till och legitimera attentat och våldsdåd mot Sverige och svenska mål.

Internationaliseringen och den breda spridningen av hotdrivande narrativ och alternativa världsåskådningar inom våldsbejakande miljöer gör att kopplingen till Sverige inte alltid behöver vara tydlig för att verka hotdrivande för våldsbejakande extremister som har för avsikt att agera mot Sverige. Vid sidan om attentatshotet kommer våldsbejakande extremister fortsatt att bedriva och utveckla stödverksamhet som finansiering, rekrytering, radikalisering och spridandet av propaganda. Den tekniska utvecklingen och möjligheterna detta ger för att effektivisera dessa typer av aktiviteter kommer att utnyttjas av våldsbejakande extremister också framöver.

Våldsbejakande extremister såväl som statliga aktörer kommer även fortsättningsvis ha för avsikt att bedriva verksamhet som inte direkt är att betrakta som brottslig men som likväl påverkar Sveriges säkerhet negativt. Detta utgörs exempelvis av engagemang och verksamhet inom ramen för demokratiska plattformar samt informationspåverkan, där avsikten är att påverka individer, politiskt beslutsfattande och den allmänna opinionen samt inspirera till handlingar som hotar grundläggande demokratiska rättigheter och principer.

6 Reformbehoven

6.1 Säpodatalagen är inte anpassad till Säkerhetspolisens verksamhet

Bedömning: Den nuvarande säpodatalagen innehåller bestämmelser som i stort överförts utan ändringar från tidigare lagstiftning och härstammar från en tid då hoten mot Sveriges säkerhet, den tekniska utvecklingen och informationsmängderna såg annorlunda ut. Säpodatalagen är varken anpassad efter dagens förhållanden eller Säkerhetspolisens nuvarande uppdrag, verksamhet och framtida utmaningar.

På grund av de krav som nuvarande lagstiftning uppställer behöver Säkerhetspolisen ofta radera betydande mängder information som inhämtats, eller helt avstå från att hämta in uppgifterna. Detta trots att informationsmängden typiskt sett är relevant och ofta avgörande för att myndigheten ska kunna fullgöra sitt uppdrag.

6.1.1 Nuvarande regelverk är anpassat till tidigare arbetssätt

Säkerhetspolisen har fått en rad nya personuppgiftslagstiftningar under de senaste decennierna (se avsnitt 3.5.1 ovan). Gemensamt för dem har varit en ambition att inte ändra på de grundläggande villkoren för Säkerhetspolisens behandling av personuppgifter. Säpodatalagen bygger i sak vidare på den tidigare polisdatalagen och har i stora delar getts samma struktur och materiellt innehåll som brottsdatalagen och polisens brottsdatalag. Både säpodatalagen och dess föregångare har avsett att ge ramverket för ett existerande arbetssätt.

Det har i de olika lagstiftningsärendena i princip inte gjorts några nya överväganden angående frågan om hur integritetskänsligt eller

vilket slags intrång i privatlivet en personuppgiftsbehandling ska anses utgöra. Personuppgiftsbehandling enligt dagens lagstiftning bygger därför i stor utsträckning på samma principer som en registrering i det tidigare SÄPO-registret enligt den första polisdatalagen. Lagstiftningen från 1990-talet reglerade hanteringen av person- och sakakter där, ofta integritetskänsliga, uppgifter om enskilda samlades. Förekomsten av en personakt som upprättats på grund av en misstanke om brottslig verksamhet får anses ha utgjort ett påtagligt intrång i den registrerades personliga integritet och motiverade därför ett visst regelverk.

När detta arbetssätt, med manuellt förda personakter, övergetts till förmån för automatiserad behandling har de mekanismer som avsett att förhindra att belastande personakter felaktigt upprättats kommit att få andra konsekvenser. Säkerhetspolisen tillämpar nämligen i dag ett snarlikt krav för behandling av varje enskild personuppgift, som för att upprätta en personakt enligt tidigare lagstiftning. Det innebär bland annat att varje personuppgift måste bedömas individuellt. När Säkerhetspolisen bedömer hur ett dokument eller ett stort it-beslag ska hanteras prövas i princip varje enskild personuppgift för sig enligt dessa krav, till exempel ett personnamn som omnämns i en konversation, en person som syns i bakgrunden på ett fotografi, ett ip-nummer som förekommer som metadata eller en adressuppgift.

Dagens lagstiftning bygger på synsättet att behandling av enskilda personuppgifter motsvarar intrånget av att upprätta en personakt och att det är belastande i sig om Säkerhetspolisen behandlar en uppgift om en person. Detta innebär en begränsning av Säkerhetspolisens förmåga.

År 1998 fattade regeringen beslut om att överlämna propositionen *Polisens register* till riksdagen. Den polisdatalagen (1998:622), som följde propositionen, innehöll bestämmelser om bland annat Säkerhetspolisen personuppgiftsbehandling. Förändringarna hade föranletts av att datorer introducerats i verksamheten. Följande citat från propositionen återspeglar den tidens syn på den nya teknikens förhållande till den personliga integriteten.

> Inom Säkerhetspolisen pågår förberedelser för övergång till ett system som medger en helt elektronisk ärendehantering. Om den samlade informationen i databaserna görs tillgänglig genom ett sökprogram skulle varje person som finns med i någon undersökning hos Säkerhetspolisen göras sökbar. Förutsättningar skulle kunna uppkomma

> att kombinera lagrade uppgifter i obegränsad omfattning. Det är ur integritetssynpunkt inte godtagbart.[1]

Detta synsätt har även präglat mycket av den efterföljande lagstiftningen, där det lagts stor vikt vid att det är mycket känsligt att förekomma i ett register hos Säkerhetspolisen. Den nuvarande lagstiftningen innehåller därför en stor mängd garantier för att enbart personer som är direkt relevanta för Säkerhetspolisens verksamhet finns registrerade hos myndigheten. Dagens lagstiftning utgår från ett i viss mån förlegat synsätt vad gäller informationshantering och ett tidigare arbetssätt där myndigheten hanterar personuppgifter i register och där personuppgiftsbehandlingen enbart utgick från en aktiv inhämtning. Detta är inte förenligt med hur informationsmängderna ser ut i dag.

Den oro som regeringen uttryckte i propositionen *Polisens register* för 25 år sedan, angående riskerna med att jämföra och kombinera lagrade uppgifter, får numera anses vara ett etablerat arbetssätt inom modern underrättelsemetodik. När Säkerhetspolisen exempelvis behandlar information som inhämtats från en misstänkt terrorist förväntas det att myndigheten ska kunna använda teknik för att snabbt och effektivt bearbeta och analysera dessa uppgifter för att förebygga, förhindra och upptäcka brottslig verksamhet. I detta ingår att göra sökningar mot uppgifter som förekommer i olika register men även att kunna jämföra de uppgifter som förekommer i större sammanhang. Det finns dock i dagsläget rättsliga hinder både mot att utnyttja existerande teknik och att utveckla nya tekniska förmågor.

6.1.2 Granskningsfunktionens bedömningar av information

I dagsläget hanteras alla handlingar som kommer in till Säkerhetspolisen inledningsvis av administratörer som överför handlingar till myndighetens dokument- och ärendehanteringssystem där den ankomstregistreras. Därefter fördelas handlingen till *tematiserade mottagningsfunktioner* där den diarieförs. Handlingen hanteras av operativ personal på dessa mottagningsfunktioner som gör en första bedömning av informationen.

[1] Prop. 1997/98:97 s. 146.

Om informationen bedöms vara operativt relevant görs en bedömning om handlingen bör tillgängliggöras för övrig operativ personal genom att överföras till Säkerhetspolisens underrättelsesystem eller bearbetas ytterligare. Denna bedömning följer en standardiserad process som innebär ett *beslut om tillgängliggörande*. Processen tillämpas både för inkommen information och sådan operativ information som upprättats inom Säkerhetspolisen. I processen tar den operativa handläggaren ställning till på vilket sätt informationen ska tillgängliggöras, med vilken tidsprioritering och till vilken personalkrets uppgifterna ska delas. Ett sådant beslut innebär att uppgifterna behandlas i en särskild *uppgiftssamling för bearbetning och analys*.

Den information som finns i uppgiftssamlingen för bearbetning och analys ska passera en särskild *granskningsfunktion*. Granskningsfunktionen tillser bland annat att personuppgifter behandlas enligt säpodatalagens bestämmelser. Om informationen bedöms uppfylla kraven får informationen fortsätta att behandlas för bearbetning och analys. Den information som ska tillföras Säkerhetspolisens centrala underrättelseregister lyfts därefter, enligt olika prioriteringar upp från en av uppgiftssamlingarna för bearbetning och analys till det centrala underrättelseregistret. Granskning fyller, vid sidan av att säkerställa författningsenlig och korrekt personuppgiftsbehandling, även en operativ funktion genom att uppgifter struktureras och kopplas samman i olika informationssystem som kan nyttjas av annan personal inom myndighetens olika verksamhetsgrenar. Information som lyfts upp till det centrala underrättelseregistret blir tillgänglig för operativ personal utifrån tilldelade behörigheter.

Arbetssättet som innebär att uppgifter måste passera en granskningsfunktion har gällt sedan länge.[2] Processen har sitt ursprung i en tid då den samlade informationsmängden i samhället och i verksamheten var betydligt mindre, samtidigt som det var svårare att strukturera information i automatiserade system.

Mängden information som kommer Säkerhetspolisen till del har ökat markant bara de senaste åren. För att den obligatoriska granskningsfunktionen ska kunna hålla jämn takt med inflödet av information måste Säkerhetspolisen vara mycket selektiv med vilken information som överhuvudtaget ska genomgå den process som

[2] Se SOU 2017:74 s. 639.

beskrivs ovan. Redan i den tematiska mottagningsfunktionen görs därför en initial bedömning av vilken information som är mest relevant att behandla. De uppgifter som initialt bedöms ha ett lägre värde prioriteras inte för att genomgå den relativt mödosamma processen som ett *beslut om tillgängliggörande* innebär och raderas utan att genomgå någon bearbetning eller analys. I takt med att mängden information som kommer in till granskningsfunktionen har ökat har denna funktion tilldelats betydande resurser och fått en allt större betydelse för att upprätthålla Säkerhetspolisens förmåga. Arbetsmetoden innebär dock en stor risk för att en flaskhals för informationsflödet inom myndigheten skapas. Sådana flaskhalsar kan vara kritiska för Säkerhetspolisens förmåga att fullgöra sitt uppdrag.

6.1.3 Varje enskild personuppgift bedöms

Det ovan beskrivna flödet är anpassat för en ordning där Säkerhetspolisen i huvudsak bedriver en egen aktiv inhämtning; som innebär att myndigheten själv genererar den information som ska registreras och på så sätt helt kan styra innehåll och omfattningen av de personuppgifter som behandlas.

Information som lämnats muntligt till en tjänsteman vid Säkerhetspolisen nedtecknas vid behov i en promemoria. Att i denna promemoria från början utelämna eller maskera irrelevanta uppgifter och känsliga personuppgifter som inte är absolut nödvändiga, om exempelvis sexuell läggning eller etniskt ursprung, är naturligt. Information som Säkerhetspolisen själv genererar kan redan från början kontrolleras för att uppfylla krav på korrekt personuppgiftsbehandling. Den ytterligare granskningen som utförs av granskningsfunktionen innan uppgifterna kan tillgängliggöras operativt är i dessa fall en relativt enkel åtgärd. Av all information som kommer Säkerhetspolisen tillhanda utgör dock sådan lättöverskådlig och begränsad information som i detta exempel en liten del.

Mycket information kommer i stället Säkerhetspolisen till del från externa källor, exempelvis genom tips från allmänheten eller information från andra nationella och internationella myndigheter eller utländska säkerhets- och underrättelsetjänster. Denna informationsmängd består till viss del av dokument med text. Ett enskilt

dokument som kommer Säkerhetspolisen tillhanda kan innehålla en stor mängd personuppgifter och även många känsliga personuppgifter, vilka var och en måste bedömas särskilt och där bedömningen i vissa fall ska dokumenteras.

Även om uppgifter alltjämt kommer in till Säkerhetspolisen i form av promemorior och dokument så inkommer eller inhämtas information i allt större utsträckning i annan form och format. Ett sådant exempel är att information som granskningsfunktionen ska bedöma utgörs av ett antal datafiler från en telefontömning eller spegling av en hårddisk från en person som misstänks vara inblandad i någon form av brott. Den informationsmängd som kan inrymmas i ett sådant it-beslag kan motsvara en lastbil full av pärmar och papper, men lagstiftningens principer om granskning och bedömning av varje enskild uppgift gäller alltjämt. En analys av en mobiltelefon kan innebära att hundratusentals personuppgifter måste bedömas.

Personuppgifterna granskas var och en och prövas mot kravet på rättslig grund respektive nödvändighet. I inkommande information kan det förekomma mer perifera personuppgifter som inte direkt berörs av det sammanhang som den inkommande informationen handlar om eller som har en vid tillfället osäker koppling till myndighetens uppdrag. Dessa måste också genomgå samma granskning och bedömning. Om inte ändamålen med behandlingen framgår av sammanhanget måste det även tydliggöras genom en särskild upplysning. Samtliga förekommande känsliga personuppgifter måste identifieras, bedömas och maskas om de vid tillfället inte kan anses vara absolut nödvändiga att behandla. Det behöver också framgå genom en särskild upplysning eller på annat sätt om personer inte är misstänkta för brott eller brottslig verksamhet. Dessutom måste uppgifter om uppgiftslämnares trovärdighet tillföras, tillsammans med en bedömning av uppgifternas riktighet i sak.

Av den information som kan vara relevant, och alltså inte måste raderas utan dröjsmål, krävs ytterligare handpåläggning och bedömningar på uppgiftsnivå. Inledningsvis måste även samtliga känsliga personuppgifter i denna mängd identifieras och prövas mot kravet på absolut nödvändighet. Om det exempelvis rör sig om brottslig verksamhet i form av islamistiskt motiverad terrorism eller olovlig kårverksamhet i en högerextrem miljö, kan uppgifter som avslöjar religiös övertygelse eller politiska åsikter förväntas förekomma.

I alla sammanhang, även när det inte rör sig om inhämtning riktad mot en uttalad extremistisk miljö, kan dock känsliga personuppgifter förväntas förekomma i en inte oansenlig mängd.

Känsliga personuppgifter är vanligt förekommande bland den information som personer själva väljer att dela med sig av öppet på internet, bland annat i profilinformation på sociala medier, blogginlägg, öppna diskussionstrådar och konversationer samt i privat kommunikation mellan människor. Uppgifterna kan även framgå av bilder, filmer och ljudfiler. Exempelvis kan bilder och filmer innehålla religiös klädsel eller symboler; vardagliga konversationer kan röra graviditet, sjukdom eller öppenhet kring sexuell läggning och sexuella relationer; incheckningar, taggade bilder eller liknande på sociala medier kan avse religiösa byggnader eller politiska engagemang. Samtliga känsliga personuppgifter måste identifieras och bedömas. När en känslig personuppgift inte framstår som absolut nödvändig måste den som tidigare nämnts maskeras eller raderas under granskningsskedet. Bedömningen kring förekomsten av känsliga personuppgifter i bilder ställer höga krav på granskning eftersom identifiering av varje förekommande religiös symbol, klädsel eller plats måste ske, liksom granskning av större mängder text. Kravet på bedömning av samtliga känsliga personuppgifter som kan förekomma i det insamlade materialet medför därför mycket omfattande och resurskrävande administrativt arbete. Om inhämtning skett exempelvis från en våldsbejakande extremistisk miljö är som regel alla uppgifter absolut nödvändiga att behandla. Trots detta måste varje personuppgift bedömas och annoteras för sig.

Som nämnt görs det hårda prioriteringar i informationsflödet för att endast den mest relevanta informationen ska genomgå den ovan beskrivna processen för *beslut om tillgängliggörande.* Skälet är att det krävs omfattande resurser för att säkerställa bland annat att varje personuppgift annoteras korrekt med en upplysning om varför just dessa personuppgifter behandlas hos Säkerhetspolisen. Säpodatalagens krav innebär att Säkerhetspolisen ofta raderar betydande mängder information eller helt avstår från att hämta in information för att inte överbelasta den särskilda granskningsfunktionen, trots att det finns ett operativt behov.

6.1.4 Konkret behov, ändamål och särskilda upplysningar,

Granskningsfunktionen måste även göra en bedömning om vissa särskilda upplysningar behöver anges. För både direkta och indirekta personuppgifter som ska användas i verksamheten måste en särskild upplysning tillföras som anger för vilket specifikt ändamål uppgiften ska behandlas, om det inte framgår av sammanhanget. Om personen i fråga inte kan anses vara misstänkt för brottslig verksamhet, måste även det anges.

De höga krav som nuvarande lagstiftning ställer på konkretion av behovet utgör ett problem. Ändamålen för behandling av personuppgifter måste vara tillräckligt preciserade för att det ska kunna avgöras om personuppgifter som behandlas är adekvata och relevanta för ändamålet med behandlingen, eller om för många personuppgifter behandlas. Behovet ska avse varje enskild personuppgift. Om exempelvis meddelanden mellan två personer som misstänks för brottslig verksamhet behandlas ska behovet av alla där förekommande personuppgifter prövas. Det innebär att det inte endast är behovet av att behandla uppgifter om de två misstänkta personerna som måste prövas, utan även alla personer som de omnämner i konversationen. Det kan givetvis, utifrån Säkerhetspolisens brottsbekämpande uppdrag, vara svårt att motivera ett konkret behov av att behandla personuppgifter om kändisar, släktningar eller vänner som endast omnämns i förbifarten under en konversation. Det har ingen betydelse om meddelandena bedöms vara relevanta att behandla i sin helhet för underrättelseändamål. Kan ett ändamål för att behandla även sådana perifera personuppgifter inte konkretiseras får de inte behandlas. Det innebär att de måste maskeras eller raderas från handlingen, vilket kan vara en mycket omfattande administrativ process. Säkerhetspolisens resurser måste ofta prioriteras till annat än sådan administration. Hela konversationen kan då komma att raderas trots att det finns operativa behov av att bevara den för en bredare kartläggning av brottslig verksamhet.

Ett annat exempel kan vara bedömningar inom personskyddsverksamheten. Vid en bedömning av en hotaktör kan historiska uppgifter vara av stort värde. Det kan exempelvis vara information om hur en individs kontaktförsök mot någon i centrala statsledningen har sett ut över tid. Att ha en historisk kontext skiljer sig avsevärt från att enbart utgå från en ögonblicksbild. Om kontakt-

försöken innebär en eskalering genom att de förändrats, intensifierats eller blivit mer aggressiva kan det vara av betydelse för bedömningen av individens avsikt att begå brott. De tidiga kontaktförsöken i en sådan eskalering, som inte utgör hot eller uttrycker hat, är typiskt sett inte sådana att de kan motivera registrering enligt säpodatalagen. Avsaknad av historik påverkar kvalitén av bedömningen av senare tillkommen information. Historiken behövs ofta för att kontextualisera enskilda underrättelser.

Säpodatalagen bygger i stor utsträckning på den polisiära utgångspunkten att registrering av personuppgifter sker först efter att Säkerhetspolisen har påbörjat ett arbete som är inriktat mot viss närmare angiven brottslig verksamhet. Till skillnad mot Polismyndighetens verksamhet anmäls dock mycket få brott till Säkerhetspolisen. Myndigheten kan inte heller förlita sig på tips eller andra externa inspel för att identifiera brottslig verksamhet. Det finns en förväntan om att Säkerhetspolisen, i betydligt större utsträckning än övriga brottsbekämpande myndigheter, själv ska identifiera potentiella hot mot nationell säkerhet och annan brottslig verksamhet genom ett aktivt underrättelsearbete.

Enligt de nuvarande förarbetena får ändamålen för behandling av personuppgifter inledningsvis anges mer övergripande för att sedan konkretiseras.[3] Även om detta uttalande medför att Säkerhetspolisen har möjlighet att inhämta personuppgifter för att upptäcka okända hot, som inte behöver konkretiseras närmare, finns en förväntan om att det ska ske genom en linjär ärendehandläggning.

Tröskeln för att behandla personuppgifter i gemensamt tillgängliga operativa system är relativt hög. Det kan ställas i relation till de rättsliga förutsättningarna för att bedriva underrättelseverksamhet. Som framgår av avsnitt 3.3.2 utgörs underrättelseverksamhet av inhämtning, bearbetning och analys av information i syfte att upptäcka brottslig verksamhet när det ännu inte finns konkreta misstankar om att ett visst brott har begåtts. Förarbetena nämner att personuppgifter, efter en inledande behandling för vida ändamål, får behandlas exempelvis för ett pågående underrättelsearbete om viss, närmare angiven brottslig verksamhet.[4] Den konkretisering av ändamålet som krävs för att information ska få behandlas inom

[3] Prop. 2018/19:163 s. 68 och 220.
[4] Ibid. s. 220.

underrättelseverksamheten efter att uppgifterna hämtats in kräver att det okända hotet ska definieras, trots att den fortsatta behandlingen syftar till att upptäcka just detta. Misstankar om brottslig verksamhet måste formuleras som hypoteser som endast kan bekräftas genom att personuppgifter behandlas. Information som är relevant inom myndighetens underrättelseverksamhet är i många fall inte så konkret eller lättbedömd som nuvarande lagstiftning förutsätter.

Det kan vara uppenbart att Säkerhetspolisen har behov av att behandla personuppgifter utifrån det sammanhang som uppgifterna kom in till myndigheten, men det kan vara desto svårare att motivera varje enskild personuppgift utifrån den grad av konkretion som lagstiftningen kräver. Exempelvis framstår det som självklart att de personuppgifter som återfunnits i en dömd spions eller terrorists mobiltelefon ska få behandlas. Det krävs emellertid att varje enskild sådan personuppgift bedömts vara nödvändig att behandla för ett särskilt och uttryckligt angivet ändamål för att sådan behandling ska få ske inom underrättelseverksamheten.

Behovet av varje enskild personuppgift måste också prövas kontinuerligt. Även denna syn baseras på polisiära utgångspunkter och att en relation till viss, närmare angiven brottslig verksamhet kan anges kontinuerligt över tid för varje personuppgift som Säkerhetspolisen har registrerat i underrättelsesystemen. Dessa prövningar får anses vara grundade i ett tidigare arbetssätt där misstankar samlades i personakter som följde en given process, som bar vissa likheter med förundersökning. En sådan process bygger på tanken att personuppgifter antecknas och behandlas i en personakt som successivt fylls på med underrättelser till dess att misstankarna antingen kan avskrivas eller bedöms tillräckliga för att inleda förundersökning. Dessa utgångspunkter tar dock inte hänsyn till att personuppgifter förekommer i stor mängd i nästan allt material som hämtas in i det operativa arbetet. En personuppgift som förekommer i ett textmeddelande eller i ett samtal kan med dagens teknik sökas fram och sammanställas med andra uppgifter som rör samma person på ett effektivt sätt. Att däremot manuellt sammanställa olika källor, genom att klippa ut de personuppgifter som hör till en person och sammanföra dessa till en akt som i sin helhet kan behovsprövas, är dock mycket ineffektivt.

6.1.5 Den längsta tiden för behandling är för kort

Den nuvarande säpodatalagen innehåller olika regler om hur länge personuppgifter får behandlas, se avsnitt 3.5.7. Huvudregeln är att personuppgifter längst får behandlas i tio år eller, för uppgifter som hänför sig till säkerhetshotande verksamhet som utövas av främmande makt, i 40 år. Inom Säkerhetspolisens verksamhet finns ofta behov av att kunna behandla personuppgifter operativt under längre tid än inom andra brottsbekämpande verksamheter. De antagonistiska aktörer som Säkerhetspolisen har att motverka bedriver sin verksamhet på ett annat sätt än vad som är typiskt för annan kriminalitet. De fenomen som Säkerhetspolisen är satt att motverka finns ofta kvar under lång tid även om de under vissa tidpunkter kan ha minskat i omfattning. Samtidigt kan sådana fenomen eller miljöer med kort varsel bli aktuella igen. Säkerhetspolisen kan då redan ha förlorat värdefullt arbete som utförts längre tillbaka i tiden. Säkerhetsläget i Sveriges närområde har pendlat kraftigt de senaste decennierna. Terrorhotet har skiftat i intensitet och haft olika ideologiska förtecken. Främmande makts ambitioner, verksamhet och mål avseende svenska intressen har också förändrats över tid. Att en viss terrorgruppering är på tillbakagång eller att exempelvis Iran eller Ryssland haft fokus på annat håll under ett antal år innebär inte att Säkerhetspolisen kan utgå från att detta förhållande består. Det finns gott om exempel på att kartläggning av ledarskiktet i en viss gruppering eller uppgifter om främmande makts agentnätverk och underrättelseofficerare kommit till nytta långt senare. Vi uppfattar att underrättelseverksamhet ställer krav på kontinuerlig uppföljning ”över tid” och att detta inte fullt ut medges med dagens lagstiftning.

Ett exempel på att den nuvarande behandlingstiden framstår som otillräcklig givet Säkerhetspolisen uppdrag är de så kallade terroresenärerna som under 2010-talet lämnade Sverige för att ansluta sig till olika grupperingar utomlands. Av Säkerhetspolisens årsbok från 2014 framgår bland annat följande.

> I december 2014 kunde Säkerhetspolisen bekräfta att fler än hundra personer rest från Sverige till Syrien eller Irak och anslutit sig till al-Qaida-inspirerade grupper. Flera av dessa personer har återvänt och ett flertal har dödats i konflikterna. Resandet till Syrien från Sverige för att ansluta sig till al-Qaidainspirerade grupper är exceptionellt omfattande i förhållande till tidigare al-Qaidainspirerat resande. Tidigare har

> personer från Sverige också rest till Afghanistan/Pakistan, Irak, Somalia och Jemen. Från 2006 till idag handlar det om minst ett 30-tal som rest till Somalia, ett tiotal till Afghanistan/Pakistan och ett fåtal till Jemen. Säkerhetspolisen ser inga tecken på att resandet till Syrien och Irak håller på att avta. (Säkerhetspolisens årsbok 2014, s. 56)

När detta betänkande avlämnas har det gått mer än tio år sedan dessa personer lämnat Sverige. Huvudregeln är därför att dessa personuppgifter inte längre ska behandlas såvida det inte under den aktuella perioden har inkommit ny information. Dagens regler medför att Säkerhetspolisen i vart fall behövt fatta ett aktivt beslut för att inte de uppgifter om de personer som rest utomlands för att ansluta sig till olika terrorsekter ska ha raderats vid utgången av år 2024.

De personer som för ett decennium sedan lämnat Sverige för att ansluta sig till olika våldsbejakande grupperingar utomlands har potential att utgöra hot mot nationell säkerhet under lång tid. Det finns en risk att någon av dessa personer återvänder till Sverige utan att Säkerhetspolisen längre har kännedom om skälet för att personen utvandrade.

Tioårsfristen kan även komma att påverka andra myndigheters beslut. För medborgarskapsärenden, där Säkerhetspolisen är en viktig remissinstans beträffande frågan om den som ansöker om medborgarskap haft ett hederligt levnadssätt, finns vissa karenstider.[5] Karenstiden för ett hederligt levnadssätt är mycket sällan kortare än femton år men kan vara avsevärt längre. I vissa fall kan tidigare brottslighet även innebära att svenskt medborgarskap är uteslutet. Bland annat följer det av praxis att en person som varit verksam i en organisation som ägnat sig åt systematiska, omfattande och grova övergrepp som regel inte kan beviljas medborgarskap förrän 25 år förflutit sedan personen lämnade organisationen eller verksamheten upphörde. Det krävs därmed inte att personen själv deltagit i någon sådan brottslighet.[6] Även om Säkerhetspolisen har information om att en person exempelvis anslutit sig till en internationell terrororganisation som ägnar sig åt sådana övergrepp, är det inte säkert att denna kunskap består i Säkerhetspolisens register under hela denna karenstid.

[5] Se 11 § 5 punkten lag (2001:82) om svenskt medborgarskap.
[6] Se regeringens beslut 2004-09-02, Ju 2003/262 samt MIG 2007:40 och MIG 2019:11.

Det kan också konstateras att mycket av den allvarligaste brottsliga verksamhet som Säkerhetspolisen har till uppgift att upptäcka, och i förlängningen utreda, har långa preskriptionstider. För bland annat terroristbrott enligt 4 § terroristbrottslagen saknas preskriptionstid. Om det krävs att underrättelseuppgifter tillförs en brottsutredning kan den tioåriga behandlingstiden i vissa fall innebära att brott inte går att utreda och att gärningsmän undgår straff.

Mot bakgrund av den stora mängd information vars behandlingsfrist utgår vid varje årsskifte enligt nuvarande lagstiftning finns det en betydande risk att viktiga och alltjämt relevanta uppgifter raderas utan att de hinner granskas. Beslut om att förlänga behandlingstid måste även ses mot bakgrund av den i övrigt tunga administrativa börda som följer av säpodatalagens bestämmelser. Kombinationen av krav på individuell bedömning och volymerna som det handlar om innebär att personuppgifter ofta raderas i stället för att behandlingstiden förlängs. Säkerhetspolisen måste i dag kontinuerligt radera information utan att först ha bedömt huruvida uppgifterna vore relevanta att spara. När väl uppgifter raderas är de oåterkalleligen raderade från Säkerhetspolisens operativa system. Vi anser att den nuvarande lagstiftningen medför oacceptabla risker för att information väsentlig för rikets säkerhet raderas i förtid.

6.1.6 En telefonkatalog får inte behandlas enligt dagens regelverk

En stor del av underrättelsearbetet går ut på att utifrån Säkerhetspolisens uppdrag identifiera intressanta personer eller organisationer i det material som har hämtats in. Det kan exempelvis handla om att koppla telefonnummer eller id-nummer i en inhämtad telefonlista till personer för att därefter kontrollera om dessa personer deltar i säkerhetshotande verksamhet.

För att kunna göra dessa bearbetningar på ett effektivt sätt behöver Säkerhetspolisen använda olika referensdatabaser. Om Säkerhetspolisen använder öppna referensdatabaser, som exempelvis webbplatsen Eniro, i sitt arbete riskerar myndigheten att röja vilka personer och organisationer som är intressanta. Det får förutsättas att Säkerhetspolisens verksamhet är intressant för främmande makt att kartlägga. Det kan ske på olika sätt, bland annat genom att signalspaning riktas mot Sverige, genom cyberoperationer eller genom

att företag eller organisationer infiltreras. Säkerhetspolisen kan därmed aldrig utgå från att information som tillförs andra system än de egna är säker. Den informationssäkerhet som krävs för att upprätthålla skyddet för den egna verksamheten medger därför inte att exempelvis ett telefonnummer delges med ett företag som Eniro genom en sökning på den öppna webbplatsen.

För att inte riskera att avslöja vilka personer och fenomen som är intressanta behöver olika referensdatabaser som innehåller personuppgifter därför lagras lokalt hos Säkerhetspolisen. Så som säpodatalagen är utformad och tillämpas inom myndigheten kräver varje personuppgift ett särskilt, uttryckligt angivet och berättigat ändamål. En referensdatabas över exempelvis adresser, telefonnummer eller ip-nummer kommer innehålla information som endast till en bråkdel är tillräckligt intressant för att uppfylla säpodatalagens krav. Trots att uppgifterna får betraktas som harmlösa och är tillgängliga för var och en är Säkerhetspolisens bedömning att myndigheten är förhindrad att behandla sådana uppgifter.

6.2 Teknikutvecklingen och allt större informationsmängder

Bedömning: Informationsmängderna i samhället ökar mycket snabbt. Säkerhetspolisens uppdrag förutsätter att myndigheten på ett effektivt sätt kan hantera stora informationsmängder för att på ett tidigt stadium kunna förebygga, förhindra och upptäcka brottslig verksamhet. Nuvarande regelverk begränsar Säkerhetspolisens möjligheter att behandla dagens informationsmängder och därmed utföra sitt uppdrag.

6.2.1 En explosionsartad utveckling av mängden information i samhället

Internet har de senaste decennierna kommit att påverka samhället på ett sätt som skulle framstått som ofattbart för endast något decennium sedan. Det finns nu cirka åtta miljarder människor på jorden. Det finns samtidigt över fem miljarder mobiltelefoner och nästan lika många konton på sociala medier. Trenden med att allt

fler människor blir uppkopplade och får möjlighet att kommunicera med varandra på ett helt annat sätt än tidigare är tydlig. Tillväxten av nya mobilabonnemang i världen är dubbelt så hög som befolkningsökningen och antalet nya användarkonton på sociala medier det tredubbla.

I december 1992 skickades världens första sms-meddelande. Tio år senare skickades det cirka 20 miljarder sms-meddelanden per månad. Nu, drygt tre decennier efter att det första sms-meddelandet skapats, skickas det cirka 23 miljarder sms – varje dag. Därutöver skickas det dagligen cirka 50 miljarder meddelanden via WhatsApp, ytterligare 50 miljarder meddelanden via Facebook Messenger och 5 miljarder meddelanden via SnapChat. Till det kommer de cirka 350 miljarder dagliga e-postmeddelanden och den kommunikation som sker via andra sociala medier, som Telegram eller Signal.[7] De som använder internet spenderar i snitt cirka sju timmar per dygn uppkopplade. Sökmotorn Google har cirka 142 miljarder besök per månad.[8]

Den informations- och kommunikationsmängd som nu färdas över jorden är till sin omfattning i en helt annan skala än vad vi ens kunde föreställa oss vid millennieskiftet. År 2010 uppskattades det att cirka två *zettabyte* data genererades i världen. En zettabyte motsvarar 1 000 miljarder gigabyte. Mängden data som genereras[9] ökar exponentiellt för varje år och under 2024 uppskattas det att cirka 147 zettabyte (147 000 miljarder gigabyte) data har genererats. Det innebär, enligt vissa uppskattningar, att av den totala informationsmängden som genererats sedan skriftspråket utvecklades för cirka 5 000 år sedan har ungefär 90 procent genererats under de senaste två åren. En stor del av den explosionsartade utvecklingen av genererad data de senaste åren kan förklaras med den ökande konsumtionen av strömmande video i allt högre upplösning, vilket i dag står för ungefär hälften av internettrafiken. Med hänsyn till den enorma skalan på datatrafiken är dock även den återstående delen oöverskådligt stor.[10]

[7] https://www.sellcell.com/blog/how-many-text-messages-are-sent-a-day-2023-statistics/.
[8] https://datareportal.com/reports/digital-2023-october-global-statshot.
[9] Med generering av data avses här skapande, mottagande, kopiering och konsumering.
[10] https://explodingtopics.com/blog/data-generated-per-day.

6.2.2 Underrättelseverksamhet kräver förmåga att behandla stora mängder information

Den allt större samlade informationsmängden i samhället påverkar hur Säkerhetspolisen kan bedriva sin underrättelseverksamhet. Vi har i föregående avsnitt redogjort för problemen som uppkommit i tillämpningen genom att varje registrering av en enskild personuppgift kräver en manuell granskning, bedömning och annotering innan uppgiften kan komma till operativ nytta. Vår uppfattning är att lagstiftningens utformning haft utgångspunkten att Säkerhetspolisen i huvudsak bedriver polisiär verksamhet i form av brottsutredning eller annan ärendehandläggning.

Det som är unikt för Säkerhetspolisen, och andra myndigheter som har ett omfattande underrättelseuppdrag, är att verksamheten kräver en förmåga att på olika sätt inhämta, bearbeta och analysera stora mängder information. En säkerhetstjänst är helt beroende av snabb och effektiv hantering av information som innefattar personuppgifter. När de informationsmängder som genereras och behandlas på olika sätt ökar, både i samhället i stort och i var och ens privata digitala liv, växer även behovet av denna förmåga. Vår uppfattning är att Säkerhetspolisens underrättelseuppdrag och förväntningarna som ställs på myndigheten sedan länge passerat vad som är möjligt med nuvarande lagstiftning.

Förväntningarna på Säkerhetspolisen är att myndigheten ska kunna upptäcka brottslig verksamhet som innebär hot mot samhällets grundfunktioner. Sådana hot kan förekomma både i mer eller mindre öppna samtal, exempelvis genom radikalisering och terrorrekrytering via sociala medier, och i det fördolda, genom bland annat krypterade meddelandetjänster. Som framkommit ovan krävs mycket hårda prioriteringar genom alla delar av underrättelseprocessen för att det ska vara möjligt att begränsa informationen till en mängd som är möjlig att hantera enligt nuvarande lagstiftning.

Det innebär att Säkerhetspolisen aktivt måste avstå från att exempelvis analysera vissa it-beslag eller bedriva spaning mot internetforum där ungdomar radikaliseras, trots att den operativa bedömningen är att sådan analys krävs för att myndigheten till fullo ska kunna utföra sitt uppdrag eller uppnå sina mål.

6.2.3 Vanliga it-beslag kan i dag vara för stora för att kunna hanteras

De stora informationsmängderna får även konsekvenser i den taktiska underrättelseanalysen, som handlar om att ta fram beslutsunderlag för Säkerhetspolisens agerande i enskilda ärenden. I samband med gripanden och andra tvångsåtgärder mot misstänkta görs alltid beslag av mobiltelefoner, datorer och andra enheter. Det är inte ovanligt att varje enskilt ärende innehåller flera aktörer och att varje aktör har flera telefoner och andra enheter. På senare år har lagringskapaciteten på privatpersoners digitala enheter ökat kraftigt, vilket resulterat i att de datamängder som behöver bearbetas och granskas har ökat i samma takt. För tio år sedan kunde ett it-beslag innehålla ett antal tusen kommunikationer i form av telefonsamtal, sms eller e-postmeddelanden. Dessa gick att överblicka genom att analytiker manuellt gick igenom materialet och på så sätt sorterade ut den relevanta informationen. I dag är det inte ovanligt att ett it-beslag omfattar hundratusentals konversationer och meddelanden över ett stort antal plattformar. Totalt rör det sig alltså om betydande datamängder i varje enskilt ärende. Gömt i denna datamängd kan den pusselbit som Säkerhetspolisen behöver för att förhindra ett terrorattentat, hitta en agent, kartlägga och klarlägga viss brottslig verksamhet över tid eller utreda ett brott finnas.

Säkerhetspolisen har rätt att, efter beslut från åklagare, använda överskottsinformation för underrättelseändamål. Eftersom en personuppgiftsgranskning och -bedömning av sådant material är oerhört tidskrävande enligt nuvarande lagstiftning – det kan röra sig om en tidsåtgång motsvarande många årsarbetskrafter – är det i praktiken inte görbart. Mycket information som inte hinner granskas på föreskrivet vis förstörs därför, ofta utan att sparas i Säkerhetspolisens underrättelsesystem. Att överskottsinformation inte kan behandlas effektivt begränsar Säkerhetspolisens förmåga att identifiera okända hotaktörer och upptäcka hot mot Sverige i ett tidigare skede. I förlängningen innebär detta också en mer begränsad förmåga för Säkerhetspolisen att motverka hoten.

6.2.4 Säkerhetspolisen saknar förmåga att behandla uppgifter om brott och brottslig verksamhet som finns öppet tillgängliga

Den kommunikation som tidigare gick över telefon har i stor utsträckning flyttat ut på internet och sker oftast med någon grad av anonymitet. De aktörer som Säkerhetspolisen är intresserade av kommunicerar ofta på forum och plattformar som inte är allmänt åtkomliga. Ibland kan information från dessa forum och plattformar läcka ut, exempelvis genom att ett forum blir hackat, och informationen läggs ut publikt på internet. Ett exempel på detta var ett forum för IS-resenärer som hackades och publicerades öppet på internet. Säkerhetspolisen utnyttjade denna läcka genom att göra sökningar mot aktörer som redan var kända för myndigheten och där behov och ändamål redan var givet. I underrättelsesystemet tillfördes dessa individer uppgifter om dem från det läckta forumet. För att Säkerhetspolisen skulle få den största effekten av den läckta databasen skulle den dock behöva sparas i sin helhet och över tid för att kunna utgöra underlag vid jämförelser med andra liknande datakällor.

Med nuvarande lagstiftning måste behovet av varje enskild personuppgift i den läckta databasen motiveras innan den sparas. Eftersom den särskilda granskningsfunktionen inte kan hantera sådana informationsmängder, tvingades Säkerhetspolisen att radera hela datamängden strax efter att den förvärvats. Behovet av att behandla personuppgifter som tillhör tidigare okända aktörer visar sig ofta först när informationen korskörs eller läggs samman med ny information. Eftersom databasen inte kunde bevaras, är det sannolikt att uppgifter om personer som förekom där inte heller kommer att bevaras nästa gång de påträffas. Mer perifera uppgifter som tillhör en okänd aktör får endast behandlas för ett särskilt, uttryckligt angivet ändamål, trots att det aktuella sammanhanget får betecknas som relevant för att behålla uppgifterna i sin helhet.

Inte bara kommunikationsvägarna, utan också de sätt som personer radikaliseras på, har förändrats. Teknikutvecklingen och den digitala arenan är central för hotet från våldsbejakande extremism. Radikalisering och spridandet av våldsbejakande och extremistiska budskap på digitala plattformar har en avgörande betydelse för såväl attentatshotet mot Sverige som för tillväxten i våldsbejakande miljöer.

Förr kunde Säkerhetspolisen ofta upptäcka nya, tidigare okända aktörer i redan kända miljöer, eller i kontakt med för Säkerhetspolisen kända individer. I dag har många av dem som radikaliserats inte kopplingar till dessa kända personer och miljöer och trenden går mer mot ensamagerande och självradikaliserade aktörer som har kontakt med likasinnade individer online. För att hitta dessa individer behöver arbetssättet ändras och sökningarna ske i bredare sammanhang, exempelvis i online-forum som finns publikt tillgängliga. Sådana sökningar kan ske med hjälp av olika indikatorer som pekar på självradikalisering, exempelvis genom jämförelser med mönster från tidigare händelser utförda av ensamagerande aktörer. Utifrån dessa indikatorer kan för myndigheten tidigare okända personer upptäckas innan de genomför ett attentat. Sådan behandling kräver dock behandling av stora datamängder då det inte på förhand går att känna till vilken del av informationen som kommer att bli avgörande. Även om Säkerhetspolisen redan i dag har tekniska och juridiska förutsättningar att hämta in många av de datakällor som skulle behövas för att hitta personer som radikaliseras, är det i praktiken svårt att använda dem. Mängden information i varje enskild datakälla är för stor för att kunna bedömas enligt säpodatalagens krav.

I praktiken kan Säkerhetspolisen endast motivera konkret behov av de personuppgifter från sådana stora informationsmängder som är möjliga att koppla till tidigare bedömd information. Det innebär att redan kända individer och företeelser kan tillföras information men att resten av den data som inhämtas måste raderas. Säkerhetspolisen saknar därmed förmåga att identifiera personer eller företeelser som är intressanta trots att de förekommer i flera datakällor, som var och en stärker misstankarna mot personen. Med nuvarande arbetssätt kan Säkerhetspolisen alltså bygga ut kunskapen om redan kända aktörer, men har svårt att upptäcka dem som inte är kända sedan tidigare.

6.2.5 Säpodatalagen begränsar Säkerhetspolisens förmåga till operativ och strategisk underrättelseanalys

Öppen information, exempelvis sådan som finns tillgänglig för alla internetanvändare på sociala plattformar, i nyhetsmedia eller genom andra källor behöver inte endast behandlas för att upptäcka kon-

kreta hot eller för att bedöma en hotaktörs avsikt och förmåga. Informationen kan också vara nödvändig för att bevaka och analysera omvärldsläget eller för att ta fram en hotbild i syfte att dimensionera skyddet för skyddspersoner i den centrala statsledningen. En förståelse för normalbilden i de miljöer som är relevanta för Säkerhetspolisens uppföljning är avgörande för att i ett tidskritiskt skede kunna notera avvikelser som myndigheten behöver agera på.

Det är i dag omöjligt att följa ett flöde på internet enbart med det mänskliga ögat för att få en överblick eller för att kunna göra kvalificerade bedömningar och analyser av trender eller förändringar. För en strategisk underrättelseanalys krävs ofta att stora mängder information inhämtas, bearbetas och analyseras över tid.

Säkerhetspolisen har med dagens regelverk goda möjligheter att inhämta information. En informationsmängd som inhämtas raderas dock som regel kort efter att den bearbetning som krävs för ärendet avslutats. Vid sidan av relevant information finns det som regel också personuppgifter där ett konkret behov saknas för att motivera fortsatt behandling. I nästa ärende, när det finns behov av samma informationsmängd, måste inhämtningen göras om. Mycket av den information som är relevant för Säkerhetspolisens analys och uppföljning finns dock inte tillgänglig på internet över tid. Vid en uppföljning dagar, månader eller år senare kan samma informationsmängd vara omöjlig att komma åt.

6.2.6 Teknikutvecklingen begränsas av säpodatalagens krav

Teknikutvecklingen inom informationsbehandling går mycket snabbt och har inom vissa områden nyligen passerat avgörande utvecklingströsklar för att kunna tillämpas operativt. Ett sådant utvecklingsområde är artificiell intelligens (AI) och maskininlärning. De senaste åren har många kraftfulla verktyg och AI-modeller för analys av stora datamängder utvecklats; modeller och verktyg som skulle göra stor nytta i analysen av underrättelseinformation. Dessa verktyg kan exempelvis hjälpa till med automatiserad inhämtning, att strukturera text, filtrera ut intressanta motiv i en stor mängd bilder eller att transkribera långa röstinspelningar.

Några av dessa verktyg kan köpas in och användas redan i dag, men i många fall krävs specifika anpassningar efter den speciella typ

av information som Säkerhetspolisen har behov av att behandla. Som exempel kan nämnas de kraftfulla så kallade språkmodeller som lanserats på senare år. Dessa skulle kunna vara till stor hjälp för att bearbeta och analysera information hos Säkerhetspolisen. Den data som dessa modeller har tränats på ser dock ofta inte ut som den text eller språkbruk som Säkerhetspolisen bearbetar i vardagen. Modellerna är ofta tränade på tidningsartiklar, Wikipedia och officiella rapporter. Den text som Säkerhetspolisen behöver bearbeta är emellertid sällan av sådant slag. För att kunna användas fullt ut inom Säkerhetspolisens operativa verksamhet skulle dessa modeller i stället behöva tränas på autentiskt data. Sådan information finns i viss mån hos Säkerhetspolisen i form av chatkonversationer i it-beslag och uppgifter som inhämtas genom hemlig dataavläsning.

Dagens lagstiftning innehåller ingen tydlig rättslig grund för insamling och behandling av personuppgifter i syfte att utveckla tekniska system eller förmågor. Säkerhetspolisen har möjlighet att samla in sådana data i sitt operativa arbete som skulle kunna användas för teknikutveckling. Dagens lagstiftning kräver dock en omfattande radering av överflödiga personuppgifter innan uppgifter får behandlas. Som träningsdata för teknik- och metodutveckling är det dock stora, ofiltrerade och autentiska informationsmängder som är användbara. Det går också att ifrågasätta om all den metodutveckling som Säkerhetspolisen är i behov av kan anses vara förenlig med finalitetsprincipen som den uttrycks i säpodatalagen.

Säkerhetspolisen har i dag inte de rättsliga förutsättningarna för att utveckla teknisk förmåga som kräver en omfattande personuppgiftsbehandling, som AI. Det innebär att Säkerhetspolisen i dag inte kan vidareutveckla eller skräddarsy sådan mjukvara.

Att använda publikt tillgängliga modeller, som inte anpassats till Säkerhetspolisens verksamhet, kan innebära en sårbarhet för myndigheten. Genom att analysera svagheter i dessa modeller skulle en angripare i värsta fall kunna justera vilka resultat användningen av en modell ska ge, och därmed manipulera underrättelseanalysen. Genom att träna egna modeller, på data som Säkerhetspolisen har kontroll över, minskar risken för denna typ av angrepp drastiskt. Innan ny teknik införs och används behöver den också kunna utvärderas på ett objektivt sätt. Genom att testa olika verktyg mot samma uppgift är det möjligt att jämföra hur bra de presterar; innan

en ny AI-modell införs behöver modellen visa att den är bättre än en redan befintlig modell. För att kunna göra den här typen av utvärdering måste ett ”facit” för varje uppgift (så kallat utvärderingsdata) sparas över tid. Denna data ska representera den faktiska uppgiften så bra som möjligt. Om målet med verktyget är att effektivt översätta texter från it-beslag, ska helst utvärderingsdata vara från just it-beslag.

Dagens lagstiftning innebär att Säkerhetspolisen är förhindrad att hämta in, vidarebehandla och lagra data för att på ett effektivt sätt arbeta med nya AI-verktyg. Samtidigt som Säkerhetspolisen halkar efter i teknisk förmåga kan det med säkerhet konstateras att antagonistiska aktörer kommer utnyttja den nya tekniken till fullo för sina syften.

6.3 Ökad förmåga för Säkerhetspolisen att behandla personuppgifter kan påverka grundläggande fri- och rättigheter

Bedömning: Säkerhetspolisens behov av att behandla personuppgifter är så stort att de åtgärder som krävs för att möta det kan medföra en risk för betydande intrång eller kränkning av mänskliga rättigheter. Rätten till privatliv och skyddet för den personliga integriteten påverkas av att personuppgifter samlas in och bevaras hos en säkerhetstjänst. Om enskilda uppfattar att olika former av opinionsyttringar kan medföra att Säkerhetspolisen registrerar dessa och behandlar dem över tid, kan det få en avhållande effekt på viljan att yttra sig offentligt.

6.3.1 Skyddet för personuppgifter utgör ett grundläggande demokratiskt värde

I vår grundlag framgår bland annat de principer som ska vägleda samhället och samhällsutvecklingen. En av de viktigaste principerna i det svenska statsskicket framgår av regeringsformens portalparagraf, i 1 kap. 1 §. Där anges att det demokratiska styrelseskicket bygger på fri åsiktsbildning. Vidare framgår, genom stadgandet att den offentliga makten utövas under lagarna, att Sverige är en rätts-

stat. Av den följande paragrafen följer att den offentliga makten ska utövas med respekt för alla människors lika värde och för den enskilda människans frihet och värdighet samt att det allmänna ska värna den enskildes privatliv och familjeliv.

Dessa bestämmelsers centrala placering i regeringsformen visar att dessa värden – rättsstaten, den fria åsiktsbildningen och respekten för medborgarens frihet och privatliv – utgör helt nödvändiga hörnstenar i den svenska demokratin.

Genom utökade möjligheter för staten att övervaka medborgares åsiktsyttringar och kartlägga enskildas privatliv i syfte att värna de grundläggande fri- och rättigheterna kan en intressemotsättning uppstå mellan mål och medel. Det krävs därför stor aktsamhet då en lagstiftning genomförs som ytterst syftar till att skydda de demokratiska kärnvärdena men samtidigt riskerar att erodera desamma.

Den svenska demokratin präglas även av en stor tillit mellan stat och medborgare, där staten i stor utsträckning avstår från att övervaka det normala samhällslivet och medborgare i hög grad litar på att rättsstaten fungerar. Om tilliten mellan stat och medborgare urholkas i alltför hög grad, finns inte förutsättningar för ett öppet och fritt demokratiskt samhälle.

6.3.2 Den personliga integriteten påverkas av Säkerhetspolisens personuppgiftsbehandling

Bestämmelsen i 1 kap. 2 § regeringsformen om att det allmänna ska värna den enskildes privatliv och familjeliv förtydligas i regeringsformens rättighetskatalog. Där anges, i 2 kap. 6 § andra stycket, att var och en gentemot det allmänna är skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden.

I propositionen *En reformerad grundlag* framhålls att det är naturligt att det läggs stor vikt vid uppgifternas karaktär vid bedömningen av hur ingripande intrånget i den personliga integriteten kan anses vara i samband med insamling, lagring och bearbetning eller utlämnande av uppgifter om enskildas personliga förhållanden. Ju känsligare uppgifterna är, desto mer ingripande anses det allmännas hantering av uppgifterna normalt vara. Även hantering av ett fåtal uppgifter kan med andra ord innebära ett betydande intrång i den

personliga integriteten, om uppgifterna är av mycket känslig karaktär. Vid bedömningen av intrångets karaktär är det också naturligt att stor vikt läggs vid ändamålet med behandlingen. En hantering som syftar till att utreda brott kan enligt förarbetena normalt anses vara mer känslig än till exempel en hantering som uteslutande sker för att ge en myndighet underlag för förbättringar av kvaliteten i handläggningen. Mängden uppgifter kan också vara en betydelsefull faktor i sammanhanget.[11]

Av 2 kap. 3 § följer även att ingen svensk medborgare utan samtycke får antecknas i ett allmänt register enbart på grund av sin politiska åskådning. Det innebär att en persons politiska uppfattning endast får registreras om denna har samband med någon annan omständighet som föranlett registreringen.

Enligt artikel 8.1 i Europakonventionen har var och en har rätt till skydd för sitt privat- och familjeliv, sitt hem och sin korrespondens. Av FN:s allmänna förklaring om de mänskliga rättigheterna följer, av artikel 12, att ingen får utsättas för godtyckligt ingripande i fråga om privatliv, familj, hem eller korrespondens och inte heller för angrepp på sin heder eller sitt anseende. Var och en har rätt till lagens skydd mot sådana ingripanden och angrepp.

Av dessa rättskällor framgår en begreppsapparat där begreppen personlig integritet och privatliv används, till synes synonymt. Det finns inte skäl att i detta sammanhang närmare utveckla de eventuella skillnaderna dem emellan.[12] Det är tillräckligt att konstatera att både svensk grundlag och internationella konventioner skyddar rätten att inte utan tungt vägande allmänna intressen övervakas och kartläggas av staten genom insamlande och bevarande av uppgifter om en persons privata förhållanden.

När det kommer till Säkerhetspolisens informationshantering bör det därför vara detta som är utgångspunkten när det kommer till *vad* skyddet för den personliga integriteten avser, och i förlängningen därmed även den personuppgiftslagstiftning som denna utredning har att lämna förslag om.

Internetstiftelsen gör årliga undersökningar om svenskarnas internetvanor och tankar om bland annat personlig integritet i det uppkopplade samhället. I undersökningen från 2023 svarade ungefär hälften av de tillfrågade att de upplever att deras integritet kränks

[11] Prop. 2009/10:80 s. 183.
[12] För en utförlig redogörelse, se SOU 2007:22 s. 53 ff.

när någon samlar in personliga data från deras internetanvändning. Nästan åtta av tio anser att ”även de som har rent mjöl i påsen bör tänka på vilken personlig data deras internetanvändning genererar”. Av dem angav en fjärdedel att de oroade sig för att myndigheter kan se ”var jag är och vad jag gör”, men endast en åttondel oroade sig för att arbetsgivaren gör detsamma.

I både 2023 och 2024 års enkät ställdes frågan om synen på om myndigheter vid misstanke om brott ska få tillgång till privata konversationer på nätet och synen på kameraövervakning med biometrisk identifiering. Över 90 procent av de tillfrågade ansåg att polisen skulle få tillgång till exempelvis Facebook Messenger vid misstanke om brott eller allvarliga brott. Sju av tio ansåg att kameraövervakning med ansiktsigenkänning ska vara tillåtet på allmän plats för att underlätta brottsbekämpningen.

En slutsats från Internetstiftelsens undersökningar är att det finns en stor förståelse för att den personliga integriteten får stå tillbaka om intrånget är motiverat av brottsbekämpning. Samtidigt går det inte att bortse från att en stor majoritet av svenskarna anser sig kränkta av att personliga data från internetanvändning samlas in eller att en fjärdedel uttrycker oro över att myndigheter använder sådan data för att kartlägga dem.

6.3.3 Opinionsfriheterna kan indirekt komma att påverkas av en utökad möjlighet till behandling av personuppgifter

De för en demokrati avgörande medborgerliga rättigheterna framgår av regeringsformens rättighetskatalog. I 2 kap. 1 § räknas de så kallade opinionsfriheterna upp. Motsvarande friheter skyddas även av artiklarna 9–11 i Europakonventionen samt av FN:s allmänna förklaring om de mänskliga rättigheterna i artiklarna 18–20.

Yttrandefrihet är frihet att i tal, skrift eller bild eller på annat sätt meddela upplysningar samt uttrycka tankar, åsikter och känslor. Informationsfrihet innebär frihet att inhämta och ta emot upplysningar samt att i övrigt ta del av andras yttranden. Yttrandefriheten utgör en helt integrerad del av samtliga de övriga opinionsfriheterna och utgör den enskilt viktigaste hörnstenen i det demokratiska statsskicket. Mötesfrihet är friheten att anordna och delta i sammankomster för upplysning, meningsyttring eller annat liknande syfte eller för framförande av konstnärligt verk. Demonstrationsfrihet är

frihet att anordna och delta i demonstrationer på allmän plats och föreningsfrihet utgörs av frihet att sammansluta sig med andra för allmänna eller enskilda syften. Religionsfrihet är frihet att ensam eller tillsammans med andra utöva sin religion. Skyddet för opinionsfriheterna har en lång tradition i Sverige.

Utövandet av dessa friheter har kommit att påverkas av teknikutvecklingen, på samma sätt som andra aspekter av våra liv. Det är nu i hög grad möjligt att dela tankar och åsikter, ge uttryck för sin religiösa övertygelse eller manifestera sympatier med vissa organisationer genom internet. Demonstrationer, möten och föreningsliv organiseras och offentliggörs ofta via internet. Denna förflyttning innebär att uttryck för opinionsfriheterna i större utsträckning än tidigare manifesteras globalt och bevaras över tid. Det ger även en möjlighet att i stor skala kartlägga en befolkning eller en individ. Många förefaller ha accepterat detta och den minoritet som inte gör det avstår från vissa tjänster eller använder sig av olika former av anonymisering för att undgå att bli kartlagda.

Att många frikostigt delar med sig av personliga uppfattningar, även i mer känsliga ämnen, via olika digitala plattformar kan anses vara ett gott betyg för det demokratiska samhällskontraktet, som innebär att medborgarna litar på att de inte övervakas av staten och inte riskerar repressalier för sina åsiktsyttringar.

Individer kartläggs dagligen, exempelvis genom att kommersiella aktörer profilerar kunder eller användare för att rikta reklammeddelanden som denne är mottaglig för. Profilering brukar sägas utgöra möjligheten att kategorisera enskilda personer på grundval av vissa synliga egenskaper för att dra slutsatser om andra egenskaper som inte är synliga. Tanken att sådan kartläggning ska ske även av myndigheter, för att på motsvarande sätt som de kommersiella aktörerna, använda sig av profilering för att försöka skapa sig en bild av exempelvis enskilda individers brottsbenägenhet har börjat rota sig i vissa länder. Metoden är kontroversiell och har visat sig bära på många risker. En av dem är risken för diskriminerande urval där personer med viss etnicitet eller religion stigmatiseras. Efter terroristattacken i New York den 11 september 2001 tillämpade exempelvis tyska myndigheter en metod för att profilera eventuellt ”sovande terrorister” i landet. Denna profilering innebar att 200 000–300 000 personers uppgifter behandlades varav nästan 32 000 personer ansågs uppfylla alla kriterier i profilen. Denna

omfattande kartläggning avsåg endast muslimer. Profileringen, som inte resulterade i något gripande, underkändes sedermera av tyska författningsdomstolen som ansåg att den bland annat bröt mot den tyska grundlagens skydd för mänsklig värdighet.[13]

När väl tanken börjat få fäste om att yttranden, ageranden och uttryck som görs på internet kan vara övervakade och att detta kan få framtida konsekvenser, finns i förlängningen en risk för att en kultur av självcensur etableras. En självcensur, som kan få effekt även avseende helt legitima åsiktsyttringar trots att avsikten varit något annat. Det finns därmed en risk för att en avkylande effekt skapas avseende medborgares vilja att utnyttja sina opinionsfriheter.[14] Riskerna för sådana avhållande effekter har lett till en skepsis hos bland annat Europadomstolen och EU-domstolen mot allt för omfattande övervakningsmetoder såsom signalspaning och hemliga tvångsmedel eller att hålla register om exempelvis enskildas politiska sympatier.[15]

6.3.4 Förutsättningar för att inskränka de grundläggande fri- och rättigheterna

Skyddet mot betydande intrång i den personliga integriteten, yttrandefriheten, informationsfriheten, mötesfriheten, demonstrationsfriheten och föreningsfriheten får begränsas genom lag, men endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Enligt 2 kap. 20 och 21 §§ regeringsformen får en begränsning inte gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen.

Begränsningen får inte heller göras enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning. Det innebär att det krävs ett formellt lagstöd för ingrepp som begränsar rättigheterna och att lagstiftaren därtill öppet och noggrant ska redovisa skälen för ett ingrepp och varför det krävs. Varken religionsfriheten eller

[13] Europeiska unionens byrå för grundläggande rättigheter, *Mot ett effektivare polisarbete, Förstå och förhindra diskriminerande etnisk profilering: en vägledning,* 2010, s. 13 f.
[14] Se om begreppet ”avkylande effekt” bl.a. Harvard Law Review, volym 133, nr 4, februari, 2020, *The Establishment Clause and the Chilling Effect*, s. 1338–1359.
[15] Se t.ex. Europadomstolens dom den 24 april 2019, *Catt mot Förenade kungariket*, mål nr 43514/15, p. 123 och den 25 maj 2021, *Big Brother Watch m.fl. mot Förenade kungariket*, mål nr 58170/13 m.fl., p. 449 samt EU-domstolens dom den 6 oktober 2020, *La Quadrature du Net*, mål nr C-511/18 m.fl. p. 118, med hänvisningar.

skyddet mot att utan samtycke antecknas i ett allmänt register enbart på grund av sin politiska åskådning är möjliga att inskränka.

Europakonventionen gäller som lag och skyddet för privat- och familjeliv, hem och korrespondens i artikel 8 får inte inskränkas om det inte i ett demokratiskt samhälle är nödvändigt med hänsyn till bland annat den nationella säkerheten. En inskränkning i en konventionsskyddad rättighet ska ha stöd i lag. Lagen ska vara så preciserad att inskränkningarna är förutsebara och att lagen är allmänt tillgänglig. Europadomstolen har i sin praxis slagit fast att intrånget ska syfta till att uppnå ett angeläget samhälleligt behov. Inskränkningen ska stå i rimlig proportion till det syfte som ska tillgodoses.

Enligt 2 kap. 19 § regeringsformen får en lag eller annan föreskrift får inte meddelas i strid med Sveriges åtaganden på grund av Europakonventionen.

Vi kommer att göra våra överväganden med beaktande av de huvudsakliga perspektiv som beskrivits i detta kapitel. Det finns således dels ett konkret och tydligt behov av att förbättra Säkerhetspolisens möjligheter att behandla personuppgifter, dels måste detta ske på ett sätt som uppfyller grundlagens och Europakonventionens krav och minimerar påverkan på de grundläggande fri- och rättigheterna.

7 Inriktningen för en reform

Bedömning: Det behövs en ny säpodatalag som på ett bättre sätt är anpassad till Säkerhetspolisens särskilda uppdrag och behov av att behandla personuppgifter samtidigt som enskildas grundläggande rättigheter och friheter i samband med sådan behandling tryggas.

Skyddet av nationell säkerhet är en nationell fråga och verksamhet rörande nationell säkerhet omfattas inte av unionsrätten. Lagstiftningen bör därför inte vila på EU-rättslig grund utan utformas för att tillgodose nationella prioriteringar. Lagstiftningen ska vara förenlig med Europakonventionen och den moderniserade dataskyddskonventionen (CETS nr 223).

Säkerhetspolisen bör få en ny förmåga att behandla vissa informationsmängder. Automatiserad behandling av personuppgifter i ostrukturerade informationsmängder är en nödvändig förmåga för att Säkerhetspolisen ska kunna utföra sitt uppdrag i dag och i framtiden.

Behandling av stora informationsmängder är ofta inte förenligt med de principer som bör vägleda en personuppgiftslag. En lag som ger Säkerhetspolisen denna förmåga måste därför utgöra ett undantag från de principer som gäller i övrigt, motiverat av skyddet för nationell säkerhet. Behandling av sådana informationsmängder bör därför specialregleras och omgärdas av särskilda skyddsmekanismer för att undantaget ska uppfylla kraven på att vara nödvändigt och proportionerligt i ett demokratiskt samhälle.

7.1 En ny säpodatalag bör införas

Förslag: Det införs en ny lag om Säkerhetspolisens personuppgiftsbehandling. Lagen utgår ifrån de krav och principer som framgår genom dataskyddskonventionen 108 med tilläggsprotokoll (CETS nr 223) samt de krav som kan anses följa av Europakonventionen.

7.1.1 EU-rätten bör inte bilda utgångspunkt för den nya lagen

Nuvarande regelverk tillkom i samband med och är präglat av EU:s dataskyddsreform. I Fördragen om den Europeiska unionen anges i artikel 4.2 bland annat att unionen ska respektera medlemsstaternas väsentliga statliga funktioner, särskilt funktioner vars syfte är att hävda deras territoriella integritet, upprätthålla lag och ordning och skydda den nationella säkerheten. Artikeln slår vidare fast: I synnerhet ska den nationella säkerheten också i fortsättningen vara varje medlemsstats eget ansvar. I bland annat dataskyddsförordningen och brottsdatadirektivet hänvisas till medlemsstaternas exklusiva kompetens inom området nationell säkerhet.[1] Det EU-rättsliga dataskyddet är därmed inte bindande när Sverige ska lagstifta om personuppgiftsreglering som uteslutande rör nationell säkerhet.

Brottsdatadirektivet har i svensk rätt genomförts genom brottsdatalagen (2018:1177), som utgör en ramlagstiftning för de brottsbekämpande myndigheternas personuppgiftsbehandling. Mot bakgrund av att Säkerhetspolisens verksamhet som rör nationell säkerhet inte omfattas av EU-rätten har denna verksamhet även undantagits från brottsdatalagens tillämpningsområde (1 kap. 4 § brottsdatalagen). Trots detta är säpodatalagen uppbyggd på samma sätt som brottsdatalagen och de båda lagstiftningarna delar både begreppsapparat, systematik och i stora delar materiellt innehåll. Skälet till detta är att överensstämmande regler dels ansågs underlätta tillämpningen, både för Säkerhetspolisen och för tillsynsmyndigheten, dels för att Sverige, genom att följa den EU-rättsliga regleringen även ansågs uppfylla kraven i dataskyddskonventionen med tilläggsprotokoll.[2]

[1] Se skäl (16) i dataskyddsförordningen och skäl (14) i brottsdatadirektivet.
[2] Prop. 2018/19:163 s. 49–50.

De skäl som talar för att låta regleringen av Säkerhetspolisens personuppgiftsbehandling ligga nära det EU-rättsliga regelverket kan alltjämt anses ha samma bärkraft. Det har sedan säpodatalagens tillkomst utvecklats en praxis kring de begrepp som används i det EU-rättsliga ramverket vilket underlättar tillsynen även över säpodatalagen. Att tillsynsmyndigheten har uppdrag avseende andra likartade lagstiftningar som bygger på samma grund medför synergieffekter vid tillsynen. Vidare har det EU-rättsliga dataskyddet höga ambitioner vilket innebär att det med viss marginal kan antas uppfylla andra internationella åtaganden som följer av bland annat Europakonventionen och dataskyddskonventionen. Det finns därmed skäl som talar för att lägga en ny personuppgiftslag för Säkerhetspolisen nära den nuvarande lagstiftningen och därmed även det regelverk som gäller för bland annat Polismyndighetens brottsbekämpande verksamhet som inte rör nationell säkerhet.

Det finns emellertid starka argument för att inte låta det EU-rättsliga dataskyddet vara utgångspunkten för en ny lagstiftning. Brottsdatadirektivet är inte anpassat särskilt för den verksamhet som bedrivs av underrättelse- och säkerhetstjänster. De förväntningar som ställs på att dessa myndigheter ska skydda den nationella säkerheten bygger på andra premisser än vad som kan göras gällande för brottsbekämpning i stort. De intressen som står på spel kan i vissa fall motivera mer långtgående befogenheter. EU-domstolen har avseende nationell säkerhet bedömt att begreppet avser skyddet av ”statens väsentliga funktioner och samhällets grundläggande intressen och inbegriper förebyggande och beivrande av verksamhet som allvarligt kan störa de grundläggande konstitutionella, politiska, ekonomiska eller sociala strukturerna i ett land och i synnerhet direkt hota samhället, befolkningen eller staten som sådan, såsom bland annat terrorverksamhet.” Domstolen konstaterade att sådana hot skiljer sig både till sin art och sitt allvar från brottslighet i allmänhet, även om den kan betecknas som grov. Målet att skydda nationell säkerhet kan därför, enligt EU-domstolen, motivera åtgärder som innebär mer långtgående ingrepp i de grundläggande rättigheterna.[3]

Intresset att värna den personliga integriteten genom ett starkt dataskydd har därför i den EU-rättsliga kontexten inte fullt ut prö-

[3] Se EU-domstolens dom den 6 oktober 2020 i de förenade målen C 511/18, C 512/18 och C 520/18, *La Quadrature du Net*, punkt 135–136.

vats mot intresset av nationell säkerhet. Denna avvägning förväntas ske på nationell nivå utifrån hotbilden i medlemsstaten och behoven av att kunna möta dessa hot. Det går att argumentera för att frågan om skyddet för nationell säkerhet är tillgodosedd inte prövades i tillräcklig utsträckning när säpodatalagen beslutades. I avsnitt 6.1 och 6.2 framgår hur den nuvarande lagstiftningen begränsar Säkerhetspolisens verksamhet. Vår bedömning är att säpodatalagen i vissa delar inte utgör en rimlig avvägning mellan verksamhetens behov och de intressen den är till för att skydda. I delar innebär den nuvarande lagstiftningen att Säkerhetspolisen begränsas på ett sätt som inte kan ha varit avsikten och inte speglar samhällets förväntningar på hur myndigheten ska utföra sitt uppdrag. Lagstiftningen tillåter helt enkelt inte all sådan verksamhet som det finns en samhällelig förväntan på att Säkerhetspolisen ska bedriva.

Att låta EU-rätten få genomslag inom Säkerhetspolisens primära verksamhetsområde har vidare den nackdelen att de bedömningar som görs avseende bekämpande av brottslighet i allmänhet även får genomslag avseende det starkare skyddsintresset som finns avseende nationell säkerhet. Att medlemsstaterna själva är bäst lämpade att bedöma och möta hoten mot nationell säkerhet är en viktig princip som kommer till uttryck i artikel 4.2 i Fördraget om den Europeiska unionen. Det är i princip omöjligt för EU-domstolen att ta del av hela bilden när en dataskyddsrättslig fråga i en nationell säkerhetskontext prövas. Det framstår som osannolikt att en medlemsstat skulle offentliggöra alla skäl som kan motivera en viss personuppgiftsbehandling till andra än mycket betrodda samarbetspartners utanför rikets gränser.

Även om det inte varit avsikten med den nuvarande lagstiftningen kan EU-domstolens avgöranden därför komma att påverka tillämpningen och tillsynen av Säkerhetspolisens personuppgiftslagstiftning. Detta eftersom lagens nära koppling till angränsande EU-rätt gör att EU-rättsliga tolkningar och bedömningar ofrånkomligen kommer påverka även tolkningen av säpodatalagen. Vi anser att det finns goda argument för att på ett tydligare sätt än tidigare särskilja detta område från det där EU-rätten har ett bestämmande inflytande och låta den svenska lagstiftaren göra avvägningen mellan intresset av nationell säkerhet och andra intressen.

Vårt ställningstagande ska dock inte uppfattas som att skyddet för bland annat den personliga integriteten helt och hållet är en

nationell angelägenhet. Sverige har andra internationella åtaganden som ålägger landet en långtgående skyldighet att skydda enskildas grundläggande fri- och rättigheter. Andemeningen i det EU-rättsliga dataskyddet och skyddet för den personliga integriteten som följer av Europakonventionen är detsamma. Skillnaden är att det EU-rättsliga regelverket är tänkt att på en betydligt större detaljnivå harmonisera bland annat de brottsbekämpande myndigheternas personuppgiftslagstiftning. Europakonventionen medger en större frihet i hur skyddet för enskilda ska lagfästas, men medger inte avsteg från detta skydd på ett sätt som inte är godtagbart i ett demokratiskt samhälle.

7.1.2 En ny lagstiftning måste vara förenlig med kraven i dataskyddskonventionen och Europakonventionen

Europakonventionen tillförsäkrar, genom sin artikel 8, var och en rätt till skydd för sitt privat- och familjeliv, sitt hem och sin korrespondens. Offentlig myndighet får inte ingripa i denna rättighet annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till den nationella säkerheten, den allmänna säkerheten eller landets ekonomiska välstånd, till förebyggande av oordning eller brott, till skydd för hälsa eller moral eller till skydd för andra personers fri- och rättigheter.

Även om Sverige frångår den systematik som följer av EU-rätten när det kommer till Säkerhetspolisens verksamhet, krävs att lagstiftningen innehåller tillräckliga skyddsmekanismer för att alltjämt vara förenlig med Europakonventionens krav. Det är ytterst Europadomstolen som uttolkar vilka krav som konventionen ställer på medlemsstaterna i detta avseende. Det finns inte tillräcklig domstolspraxis för att kunna bygga ett nationellt regelverk enbart kring Europakonventionens bestämmelser. Vi återkommer dock i kapitel 9 till hur vi tolkar Europadomstolens praxis avseende behandling av stora informationsmängder.

Sverige har anslutit sig till Europarådets dataskyddskonvention (CETS nr 108) som i stora delar anses utgöra ett förtydligande av Europakonventionens artikel 8. Dataskyddskonventionen är från år 1981 och är även förlagan till det EU-rättsliga dataskyddet. Konventionen bygger på samma grundläggande principer om exempel-

vis ändamålsbundenhet och uppgiftsminimering som EU:s dataskyddsregler, se avsnitt 4.7.1–2.

År 2018 beslutade Europarådets ministerkommitté om ett tilläggsprotokoll till dataskyddskonventionen (CETS nr 223). Tilläggsprotokollet innebär att konventionens materiella innehåll uppdateras. Moderniseringen av konvention 108 hade två huvudmål: att hantera utmaningar till följd av användningen av ny informations- och kommunikationsteknik och att stärka konventionens genomslag. Den moderniserade konventionen i sin lydelse efter tilläggsprotokollet brukar benämnas dataskyddskonventionen 108+. Dataskyddskonventionen 108+ har ännu inte trätt i kraft. Se avsnitt 4.7.3.

Det finns vissa grundläggande principer i konventionen som är absoluta oavsett för vilket ändamål personuppgifter behandlas. Det är till exempel inte möjligt för medlemsstaterna att göra undantag från proportionalitetskravet vid all personuppgiftsbehandling eller från kravet på rättslig grund. Andra artiklar i konventionen medger att konventionsstaterna gör nödvändiga och proportionerliga undantag, för att bland annat tillgodose intresset av nationell säkerhet. Sådana undantag ska följa av lag, respektera grundläggande demokratiska fri- och rättigheter samt utgöra en nödvändig och proportionerlig åtgärd i ett demokratiskt samhälle.

Vi anser att den nya lagen bör utgå från den systematik som följer av dataskyddskonventionen 108 i dess lydelse efter det att 2018 års tilläggsprotokoll trätt i kraft, dvs. dataskyddskonventionen 108+. Konventionen, som är tillämplig även inom området nationell säkerhet, har som syfte att bilda europeisk praxis för dataskydd. I Sverige är den del av Säkerhetspolisens verksamhet som rör nationell säkerhet ett av de få områden där konventionen gäller i stället för EU:s dataskyddsregelverk. Konventionen är generell i sin utformning och tillräckligt flexibel för en lagstiftning som både medger en effektiv verksamhet för Säkerhetspolisen och ger ett adekvat skydd för enskildas grundläggande medborgerliga fri- och rättigheter.

Dataskyddskonventionen 108+ kan ses som en precisering av de krav som uppställs enligt Europakonventionens artikel 8, om rätten till respekt för enskildas privat- och familjeliv. En lagstiftning som tydligt utgår från de krav som ställs enligt dataskyddskonventionen kan därför förutsättas vara förenlig med Europa-

konventionen så länge de grundläggande och ovillkorliga principerna bakom de båda konventionerna respekteras.

7.1.3 En proportionerlig lag

Avvägning mellan verksamhetsbehov och intrång i enskildas fri- och rättigheter

Säkerhetspolisen är Sveriges nationella säkerhetstjänst med uppdrag att skydda landet mot säkerhetshotande verksamhet som bedrivs inom landets gränser. Den brottslighet som myndigheten ska bekämpa är sådan som kan få mycket stora konsekvenser, både för samhället och för enskilda. Säkerhetspolisens uppdrag är därför i första hand att förebygga och förhindra att brott begås. Samtidigt utmärks den brottslighet som är Säkerhetspolisens ansvar, som terrorism och spionerі, av att den är mycket svårupptäckt och sällan kommer till myndighetens kännedom genom anmälan. Det ställs därför stora krav på att myndigheten själv ska upptäcka brottslig verksamhet genom att bedriva underrättelseverksamhet.

Vår uppfattning är att det finns en betydande skillnad mellan Säkerhetspolisen och andra brottsbekämpande myndigheter. Skillnaderna framträder både vad gäller den tyngd som kan tillmätas verksamhetens behov och vad gäller de integritetsrisker som verksamheten kan ge upphov till. Lagstiftningen vi förslår måste därför balansera mellan olika intressen, och medföljande risker, där det ena innebär att lagstiftningen inte ger Säkerhetspolisen förmågan att utföra sitt uppdrag och där det andra utgörs av att lagstiftningen inte innehåller tillräckligt skydd för grundläggande fri- och rättigheter, som därmed riskerar att urholkas.

Vi anser att det är möjligt att utforma en lagstiftning som tillgodoser å ena sidan det allmänna intresset av att skydda nationell säkerhet och å andra sidan det enskilda intresset av att inte övervakas eller kartläggas utan starka och berättigade skäl samt det allmänna intresset av fri åsikts- och opinionsbildning.

Verksamhetens behov måste tillgodoses i större utsträckning genom den nya lagen

Av avsnitt 6.1 och 6.2 framgår att Säkerhetspolisens förmåga begränsas av ett regelverk som inte i alla delar är utformat för behoven i verksamheten. Vi uppfattar att det är mycket angeläget att stärka Säkerhetspolisens förmåga i flera avseenden. Den underrättelseverksamhet som Säkerhetspolisen bedriver avser att kartlägga hot mot centrala nationella intressen. Stora delar av samhället förlitar sig på Säkerhetspolisens förmåga att upptäcka, förebygga och förhindra dessa hot. Säkerhetspolisen är en av flera svenska myndigheter med ett utpräglat underrättelseuppdrag. En av Försvarsmaktens grenar består av den militära underrättelse- och säkerhetstjänsten som både har i uppdrag att identifiera yttre hot mot landet och inre hot mot Försvarsmaktens verksamhet. Den svenska signalspaningsmyndigheten FRA bedriver ett avancerat underrättelsearbete, bland annat på uppdrag av Säkerhetspolisen. Dessa båda verksamheter har nyligen fått en mer verksamhetsanpassad personuppgiftslagstiftning. Med hänsyn till de likheter som finns i uppdrag och verksamhet mellan myndigheterna finns skäl att dra lärdom av och, om lämpligt, harmoniera lagstiftningarna.

Säkerhetspolisen har bland annat tillgång till högt kvalificerad personal, de tekniska resurser som krävs och ett utbyggt internationellt samarbete. Det som saknas för att fullt ut utnyttja Säkerhetspolisens förmåga i dag är de rättsliga förutsättningarna för att effektivt behandla personuppgifter i olika avseenden. Det är i första hand underrättelseverksamhetens behov som ska tillgodoses genom våra förslag.

Vi anser att det bör ske genom att frångå utgångspunkten att varje enskild personuppgift som behandlas av Säkerhetspolisen ska bedömas för sig i fråga om behandlingen utgör ett intrång i den personliga integriteten med mera Det måste vara möjligt att se på sammanhang i stället för att i detalj pröva varje enskild personuppgift. Att i allt för stor utsträckning dekonstruera och pröva uppgifter utanför sitt sammanhang är inte en metod väl lämpad för underrättelseverksamhet, vars mål ofta är att just sätta in uppgifter i en kontext. Detta gäller för den taktiska såväl som för den strategiska underrättelseanalysen.

Vidare måste det var möjligt för Säkerhetspolisen att behandla personuppgifter under längre tid än i dag. Av avsnitt 6.1.5 framgår att konsekvenserna av dagens behandlingstider kan innebära oacceptabla risker för medborgare och samhället och att dessa brister kan komma att påverka andra myndigheters beslutsfattande.

Lagstiftningen vi föreslår behöver även tillåta att ny teknik används och utvecklas. Det är väsentligt att Säkerhetspolisen kan möta hot som den tekniska utvecklingen innebär och samtidigt dra nytta av ny teknik i den egna verksamheten. Det måste därför finnas förutsättningar att behandla personuppgifter för teknisk utveckling.

Utgångspunkten är att verksamheten inte ska hindras av regler som saknar ett tydligt integritetshöjande syfte

I avsnitt 6.1 har vi redogjort för vilka hinder den nuvarande lagstiftningen ställer upp för Säkerhetspolisens verksamhet. Flera av dessa hinder är medvetna begränsningar för att på olika sätt reducera integritetsintrång och minska risken för rättighetskränkningar. Exempelvis avser den förhöjda behandlingströskeln för känsliga personuppgifter att minimera risken för att sådana uppgifter behandlas felaktigt eller sprids (se avsnitt 3.5.5).

Andra begränsningar kan utgöra oavsiktliga konsekvenser av regler som påverkar verksamheten på ett påtagligt sätt, utan att det tillgodoser bestämmelsens primära syfte. Ett exempel på det är att Säkerhetspolisen anser sig förhindrad att hålla en egen kopia av en referensdatabas, som exempelvis en digital telefonkatalog (se avsnitt 6.1.6). Skyddet av personuppgifter är i dessa fall verksamhetshindrande utan att det i samma utsträckning kan anses vara integritetshöjande.

Vi har även identifierat en rad bestämmelser som innebär ett påtagligt administrativt merarbete genom att de förutsätter granskning, annotering och bedömning av krav, utan att det finns någon uppenbar integritetsvinst. Varje sådant krav innebär att resurser måste fördelas från operativ till administrativ verksamhet. Flera av dessa bestämmelser har sitt ursprung i en reglering som avsåg ett annat arbetssätt, ett annat informationsflöde och med andra tekniska förutsättningar. Ett exempel är huruvida lagstiftningen ska vara tillämplig för uppgifter om juridiska personer. Denna bestämmelse är motiverad av bland annat tekniska skäl som inte längre är

giltiga, men innebär alltjämt en omotiverad förmågesänkning. Det finns även flera detaljregleringar, exempelvis en individuell notering i systemen av personer som inte är misstänkta för brottslig verksamhet. Bestämmelsen har sitt ursprung i ett annat system och är nu inte längre motiverad utifrån det merarbete regleringen medför för verksamheten.

Intrånget ska balanseras

Kartläggning av enskildas personliga förhållanden, utan samtycke och ofta utan konkret brottsmisstanke, utgör en verksamhet av särskilt integritetskänsligt slag. En stor del av Säkerhetspolisens verksamhet är till sin natur sådan att det kan leda till ett betydande intrång i den personliga integriteten. Frågan om en lagstiftning som medger ett sådant intrång i grundläggande rättigheter är proportionerlig innebär en prövning i flera steg. Att lagstiftningen möter ett faktiskt och genuint behov som inte kan tillgodoses genom mindre ingripande åtgärder är en del av denna prövning. Prövningen kan emellertid inte stanna vid att pröva behoven. Även intrånget måste vägas in i bedömningen.

De behov som våra förslag ska möta har vi redogjort för i bland annat avsnitt 6.1 och 6.2. Vi kommer i de enskilda bestämmelserna göra ytterligare överväganden angående behoven och huruvida de kan tillgodoses genom mindre ingripande åtgärder. Här redovisas några ingångsvärden vi haft vid dessa överväganden.

En integritetsintrångsanalys av en lagstiftning ska typiskt sett innehålla en bedömning av vilken typ av personuppgifter som kommer att behandlas till följd av förslaget. Denna fråga är svår att besvara när det kommer till Säkerhetspolisens brottsbekämpande verksamhet. Säkerhetspolisen har getts ett relativt brett mandat att inhämta personuppgifter och har tillgång till en mängd olika inhämtningsmetoder. I princip kan därför alla tänkbara personuppgifter komma att behandlas.

Att lösa integritetsrisker genom att förbjuda behandling av vissa personuppgifter eller föreskriva vilket slag av personuppgifter som får behandlas uppfattar vi inte vara en framkomlig väg, eftersom det förutsätter en individuell granskning och bedömning av varje

enskild uppgift, något som inte låter sig göras på ett rimligt effektivt sätt.

Om kraven på granskning av enskilda personuppgifter minskar är dock den mest sannolika följden att antalet personuppgifter som behandlas ökar. Vår uppfattning är att de integritetsrisker som detta medför ska motverkas genom mekanismer som innebär att systemet och behandlingens faktiska effekter i högre grad ska bedömas och om nödvändigt kunna korrigeras. Vi anser exempelvis att riskerna med att behandla känsliga personuppgifter i Säkerhetspolisens verksamhet inte i första hand utgörs av risken för att obehörig personal ska få tillgång till dem eller att de sprids genom exempelvis en dataläcka. De risker som registrering av uppgifter som avslöjar en persons religiösa övertygelse, etniska ursprung eller sexuella läggning är mest framträdande om dessa uppgifter utgör sökkriterier eller på annat sätt används för att göra ett urval av personer. Att göra ett urval av personer baserat på enbart känsliga personuppgifter har potential att leda till diskriminering eller ett ogrundat misstänkliggörande av individer. Vi ser därför starka skäl att i lag särskilt reglera förutsättningarna för sådan behandling.

Vad som utgör känsliga personuppgifter är en generell uppräkning, som gäller över i princip hela samhället, se avsnitt 3.5.5. Vi har dock uppfattat att det även finns andra uppgifter som kan vara minst lika integritetskänsliga men som inte ingår i den uppräkning som följer av bland annat dataskyddskonventionen eller dataskyddsförordningen. Personuppgifter som kan påverka anonymitetsskyddet för så kallade meddelare enligt tryckfrihetsförordningen eller yttrandefrihetsgrundlagen samt uppgifter om vad som förekommit i förtroliga samtal mellan en misstänkt och dennes försvarare anser vi förtjänar ett starkt skydd. Riskerna för kränkning av grundläggande fri- och rättigheter får anses vara så betydande vid behandling av sådana uppgifter att ett eventuellt behov för verksamheten får stå tillbaka.

Det finns vidare starka skäl att överväga vilka potentiella risker som följer av att implementera ny teknik i verksamheten. En lag som tillåter utveckling av exempelvis artificiell intelligens i en så känslig verksamhet som Säkerhetspolisens anser vi även måste innehålla försäkringar om att tekniken inte ska kunna ges ett självständigt bestämmande inflytande.

En robust tillsyn

Säkerhetspolisens personuppgiftsbehandling står i dag under tillsyn av två oberoende organ, Säkerhets- och integritetsskyddsnämnden och Integritetsskyddsmyndigheten. Den kontinuerliga tillsynen bedrivs av Säkerhets- och integritetsskyddsnämnden men det är Integritetsskyddsmyndigheten som har befogenheter att korrigera missförhållanden.

Vi anser att tillsynen utgör en helt avgörande komponent för att värna enskildas integritet. Säkerhetspolisen är ansvarig för att myndigheten följer gällande lagstiftning men det krävs även en robust tillsyn av att så sker. Vår ambition är därför att så långt möjligt bidra till att tillsynen blir effektiv. En effektiv tillsyn ska syfta till att personuppgifter behandlas författningsenligt av Säkerhetspolisen. Vår ambition är att dataskyddet inte ska grundas på förutsättningar för att registrera enskilda personuppgifter utan ska gälla på en mer systematisk nivå. En sådan förflyttning innebär även att tillsynen kommer att behöva anpassas och i större utsträckning inriktas på *hur* personuppgifter behandlas och behandlingens faktiska eller potentiella effekter.

Vårt förslag innehåller därför flera bestämmelser som syftar till att stärka tillsynen i dessa avseenden.

En mer transparent lag

Personuppgiftslagar i allmänhet är ofta svårgenomträngliga. För att kunna bedöma intrånget krävs en förförståelse av rättspraxis, tillämpningen i verksamheten och vilka faktiska möjligheter som verksamhetsutövaren har att genomföra olika åtgärder. En teknikneutral och flexibel lagstiftning kräver ett visst mått av abstraktion. Det är heller inte möjligt att i klartext förklara exakt hur Säkerhetspolisen behandlar personuppgifter i verksamheten.

Vi anser däremot att det ska vara möjligt att förstå lagens uppbyggnad utan att behöva känna till verksamheten i detalj. Ett exempel på att detta inte är möjligt i nuvarande lagstiftning är att det finns en inbyggd motsättning i att det ställs krav för att överhuvudtaget få behandla personuppgifter som endast kan uppfyllas genom att behandla dem. Säkerhetspolisen behöver, för att uppfylla dessa krav, på förhand känna till innehållet i alla uppgifter som samlas

eller hämtas in. Förutsättningarna för att Säkerhetspolisen ska få samla in personuppgifter ska lämpligen framgå direkt av lagen.

Vi avser därför att så långt som möjligt lämna förslag till en lag som är möjlig att tillämpa, och därmed även utöva tillsyn över, och som bättre speglar hur personuppgifter faktiskt måste kunna behandlas i verksamheten.

7.1.4 En proportionerlig tillämpning

Ändamål och rättslig grund

Den lag vi föreslår kommer att ställa höga krav på tillämparen. Vi anser att en myndighet som Säkerhetspolisen, vars kärnverksamhet består av informationshantering, kan anförtros uppgifter som kräver svåra bedömningar inom detta område.

En sådan bedömning är att formulera ändamål för personuppgiftsbehandling. Det är endast Säkerhetspolisen som vet vilka ändamål som är relevanta för verksamheten. Vi anser därför att lagen endast ska uppställa de yttre ramarna för personuppgiftsbehandling och, i likhet med dagens lagstiftning, inte i detalj ange ändamålen för behandling. En utgångspunkt är att Säkerhetspolisen ska få behandla personuppgifter för samtliga ändamål som behövs för den brottsbekämpande verksamheten. När det kommer till kärnverksamheten, som består i underrättelseverksamhet, finns det anledning att särskilt överväga vad denna verksamhet omfattar.

Behandlingströskel

Det är i dagsläget endast de uppgifter som är nödvändiga för en rättslig grund som får behandlas. Det finns anledning att titta närmare på hur denna bestämmelse överensstämmer med Säkerhetspolisens uppdrag. Kraven på att varje uppgift ska vara nödvändig innebär att en uppgiftsmängd, exempelvis ett fotografi eller ett dokument, inte kan bedömas som nödvändigt i sin helhet. Eftersom det i dagsläget är olika behandlingströsklar för känsliga personuppgifter och andra uppgifter måste en detaljerad granskning och bedömning göras för att både identifiera känsliga personuppgifter och bedöma om behandling av dem är absolut nödvändig.

Detta medför problem i tillämpningen och är inte en ordning som är anpassad för verksamheten, där känsliga personuppgifter är vanligt förekommande.

Vi uppfattar inte heller att endast pröva behovet av att behandla en känslig personuppgift i och för sig utgör ett adekvat skydd mot kränkning. En personuppgiftslag ska skydda mot risken för intrång i grundläggande fri- och rättigheter. Det är en bedömning som kräver mer än ett konstaterande av att det är absolut nödvändigt att behandla en uppgift. Det kan finnas anledning att överväga om en högre behandlingströskel är det mest effektiva skyddet eller om riskerna eller den faktiska effekten av behandlingen bör få större genomslag.

Proportionalitetsavvägning

En nyhet i dataskyddskonventionen 108+ är bestämmelsen, i artikel 5.1, som säger att all personuppgiftsbehandling ska vara proportionerlig och utgöra en skälig avvägning mellan intresset av att utföra behandlingen och andra allmänna och enskilda intressen. Denna proportionalitetsprincip ska tillämpas genom alla steg av behandlingen: från insamling och registrering till sökning, läsning och delgivning.

Av 2 kap. 21 § regeringsformen följer en liknande proportionalitetsprincip som anger att en begränsning av en fri- eller rättighet inte får gå längre än nödvändigt. Proportionalitetsprincipen har i svensk förvaltningsrätt ansetts innebära att en myndighet måste avstå från att meddela ett betungande beslut om de negativa konsekvenserna för den enskilde inte står i rimlig proportion till det allmänna intresse som ska tillgodoses. Principen gäller även om det i och för sig finns författningsstöd för åtgärden.[4]

Säkerhetspolisen har getts ett brett mandat att inhämta personuppgifter och har tillgång till flera olika inhämtningsmetoder. I princip kan därför alla tänkbara personuppgifter komma att behandlas i verksamheten. I praktiken innebär detaljkraven i nuvarande personuppgiftslagstiftning att det inte är möjligt för Säkerhetspolisen att behandla all information som myndigheten har rätt att inhämta. Vi uppfattar att det är en brist att mycket starka verksamhetsbehov

[4] NJA 2016 s. 868 p. 15. Se även t.ex. NJA 2012 s. 400 p. 19 och 2018 s. 753 p. 20.

inte kan tillgodoses på ett mer effektivt sätt än i dag. Samtidigt kan integritetsintrånget med nuvarande lagstiftning bli omotiverat stort genom behandling av personuppgifter med låg eller ingen verksamhetsnytta. Det framstår som mer lämpligt med en lagstiftning som medger större intrång om det kan motiveras av tungt vägande ändamål, än att alla uppgifter som passerar en viss behandlingströskel ska behandlas lika.

Hur tungt ändamål som krävs för att ett visst intrång ska få ske är inte möjligt att förutse och inte heller lämpligt att slå fast i lag. Det är inte heller nödvändigt med på förhand givna trösklar vid en sådan prövning. Polislagens allmänna principer om ingripanden, i 8 §, är ett exempel på hur en proportionalitetsprövning är en del av det dagliga arbetet i andra delar av verksamheten. Bestämmelsen föreskriver bland annat att ett polisingripande ska vara försvarligt med hänsyn till åtgärdens syfte och övriga omständigheter och att mer tvång inte får användas än som behövs för att uppnå avsett resultat. Bestämmelsen ger både möjlighet att tillgripa tvång då det krävs men samtidigt en möjlighet att ifrågasätta ett ingripande som inte framstår som proportionerligt.

Vi anser att en proportionalitetsprövning för varje behandlingsåtgärd kan vara ett lämpligt sätt att reglera personuppgiftsbehandling som kan innebära övervakning eller kartläggning av den enskildes personliga förhållanden. Vi uppfattar att det möjliggör en prövning som bättre tillgodoser skyddet för fri- och rättigheter än att lämna detaljerade, formella förutsättningar för personuppgiftsbehandling på uppgiftsnivå. Proportionalitet som en förutsättning för behandling innebär också att tillsynsmyndigheten kommer kunna utöva tillsyn av åtgärders faktiska eller potentiella effekter på ett annat sätt än i dag. En ny lagstiftning bör utformas från dessa utgångspunkter. De närmare övervägandena om en sådan ny allmän personuppgiftslagstiftning för Säkerhetspolisen finns i kapitel 8.

7.2 En ny lag som möjliggör för Säkerhetspolisen att behandla vissa informationsmängder

Förslag: Det är inte möjligt att behandla vissa stora informationsmängder enligt säpodatalagens bestämmelser om bland annat behov, adekvans och uppgiftsminimering. Säpodatalagen ska därför kompletteras av en särskild lag som reglerar behandling av stora, ostrukturerade informationsmängder som är befogade för myndigheten att behandla. Lagen ska medge att uppgiftsmängder registreras och behandlas i sin helhet för ett övergripande ändamål.

Behandling av stora mängder personuppgifter bär med sig risker för den personliga integriteten och andra grundläggande fri- och rättigheter. För sådan behandling som kan innebära en kränkning eller en betydande påverkan av rättigheten krävs starka skyddsmekanismer.

7.2.1 Säkerhetspolisen måste ges ny förmåga att hantera information

Samhället har genom digitaliseringen och den tekniska utvecklingen förändrats i grunden. Förändringen har inneburit att det varje dag produceras enorma och komplexa mängder information. I avsnitt 6.2.1 redogörs för hur informationsflödena har utvecklats under de senaste decennierna. I tillägg kan nämnas att under de dryga fem år som säpodatalagen varit i kraft till att detta betänkande avlämnats (januari 2020 till april 2025) har det genererats uppskattningsvis fyra gånger så mycket data som den sammanlagda mängd som genererats från skriftspråkets tillkomst fram till att säpodatalagen beslutades. Även om denna siffra inte är direkt överförbar till en ökning av den informationsmängd som är relevant för Säkerhetspolisen att behandla, ger den en fingervisning om att det inte längre är möjligt att tillämpa samma metoder för att hantera information som när tidigare personuppgiftslagstiftningar beslutats.

Säkerhetspolisens uppdrag som nationell säkerhetstjänst skiljer sig från andra brottsbekämpande myndigheters på så sätt att huvudfokus i den brottsbekämpande verksamhet ligger på underrättelsearbete. Den säkerhetshotande verksamhet som Säkerhetspolisen

ansvarar för att bekämpa är per definition hot mot själva statens suveränitet och funktionalitet. Säkerhetstjänstens primära uppgift är därför att förebygga och förhindra sådan verksamhet innan ett brott har begåtts. Den säkerhetshotande brottslighet som Säkerhetspolisen ansvarar för att bekämpa utmärks även av att den är mycket svårupptäckt. För att upptäcka det okända hotet är det naturligt att underrättelsearbetet måste ske med en större bredd än om det redan på förhand finns en lägesbild eller mer konkretiserade misstankar. Säkerhetspolisen har därför ett, i förhållande till andra brottsbekämpande myndigheter, särpräglat uppdrag. För att lösa sitt uppdrag behöver Säkerhetspolisen ha tillgång till relevant information och förmåga att på ett effektivt sätt hantera och bearbeta denna. Förmågan att snabbt kunna kontrollera och förstå stora mängder information är avgörande för en säkerhetstjänst.

Det finns en förväntan om att Säkerhetspolisen ska ha förmågan att identifiera brottslig verksamhet som förekommer på olika öppna plattformar på internet som i sociala medier eller i andra mer ljusskygga forum. Redan av den exponentiella informationstillväxten som sker på internet följer att den spaning som bedrivs i öppna källor, för att vara effektiv, måste kunna ske genom automatiserad behandling av stora informationsmängder. Det finns flera exempel i närtid på personer med en extremistisk agenda som på förhand aviserat sin avsikt att begå terrorbrott. Som framgår av avsnitt 5.1.5 förväntas olika digitala plattformar vara av fortsatt central betydelse för såväl attentatshotet mot Sverige som för tillväxten av våldsbejakande miljöer. I dag krävs att Säkerhetspolisen har förmåga att få tidiga varningar om eller upptäcka bland annat terrorhot eller brottsplaner som publicerats på internet.

Vår uppfattning är att den nationella säkerhetstjänsten även i andra sammanhang förväntas ha förmåga att hantera information effektivt och över tid. Ett exempel på behovet av ny förmåga i detta avseende kan hämtas från en av Säkerhetspolisens förundersökningar inom kontraspionaget. Inom ramen för brottsutredningen inhämtades uppgifter genom hemlig dataavläsning avseende en individ som misstänktes vara en aktiv agent för främmande makt. Utifrån den samlade informationsbilden bedömdes individen ingå i ett nätverk av agenter som fick uppdrag av samma underrättelseofficer. Säkerhetspolisen hade kännedom om några men troligtvis inte alla agenter verksamma i nätverket. Det inhämtade materialet

var mycket omfattande och innehöll sannolikt uppgifter som sammantaget med annan information skulle kunna bidra till att fler agenter inom samma nätverk kunde identifieras och vars säkerhetshotande aktiviteter därmed skulle kunna motverkas. Trots att betydande resurser lades på granskning och bearbetning av det inhämtade materialet var det inte möjligt att i tid granska och bedöma alla personuppgifter enligt säpodatalagens krav. Stora delar av informationen förstördes därför utan att ha tillförts Säkerhetspolisens underrättelsesystem. I uppföljningen av det aktuella nätverket inhämtades senare, i en annan förundersökning, omfattande itbeslag. Informationen från den första förundersökningen kunde dock inte komplettera den nya, eftersom den raderats. Även den information som inhämtades i den nya förundersökningen förstördes då informationsmassan innehöll ett mycket stort antal personuppgifter som inte var möjliga att bedöma var för sig. Säkerhetspolisens konsekvensanalys är att oförmågan att behandla informationen som inhämtats medförde en sämre förmåga att identifiera okända individer som bedriver olovlig underrättelseverksamhet eller kontakter till dem.

Ett annat exempel är de uppgifter som behövs inom Säkerhetspolisens personskyddsverksamhet. Inom denna verksamhet finns behov bland annat av att kontinuerligt och över tid kunna hämta in och behandla öppet tillgänglig information. För att kunna följa utvecklingen av potentiellt hotdrivande kommunikation och uppmärksamhet kring skyddspersoner i den centrala statsledningen behöver Säkerhetspolisen löpande analysera uppgifter från sociala medier. Detta för att kunna göra mer träffsäkra bedömningar av den sammantagna hotbilden mot skyddspersoner och fatta välavvägda beslut om dimensioneringen av personskyddet. Genom att analysera avvikelser, trender och mönster i sociala medier är det möjligt att tydligare kunna urskilja och förstå bakomliggande orsaker till potentiellt hotdrivande kommunikation och känslostämningar. Möjligheten att inhämta och behandla större datamängder över tid skulle också stärka myndighetens förmåga att utvärdera och lära av tidigare händelser, då information från exempelvis sociala medier kan vara en viktig pusselbit för att förstå varför ett skeende kom att se ut som det gjorde. Med befintlig lagstiftning har Säkerhetspolisen inte möjlighet att bedriva sådan inhämtning givet att den typ av information som inhämtningen skulle riktas mot inne-

håller en stor mängd personuppgifter, ibland även känsliga personuppgifter, som var och en måste granskas och bedömas enligt Säpodatalagens bestämmelser. Konsekvenserna av detta blir en sämre förmåga för Säkerhetspolisen att, utifrån en helhetsbild, identifiera konkreta och potentiella hot mot Säkerhetspolisens skyddspersoner. Konsekvenserna blir också en sämre förmåga att känna igen och upptäcka förändringar i uppmärksamhet och kommunikation kopplat till en skyddsperson där dessa förändringar i sig skulle kunna utgöra en varningssignal för att hotbilden mot skyddspersonen redan har eller kan komma att förändras. Eftersom Säkerhetspolisen saknar historiska uppgifter kan inte nya observationer sättas in i ett kontextuellt och historiskt sammanhang. Det innebär att nya observationer om företeelser inte kan jämföras eller analyseras med tidigare observationer vilket försvårar bedömningar avseende de nya observationernas underrättelserelevans.

Säkerhetspolisen har ett behov av att kunna bearbeta och analysera information snabbare i dag än vad som var nödvändigt förr. När exempelvis ett terrorattentat inträffat genereras i dag en mycket stor mängd information som behöver samlas in, tips behöver hanteras och information utbytas med nationella och internationella partners. Informationsflödet är vid sådana händelser mycket omfattande. Ett annat exempel är den spridning av desinformation som skett på senare tid i det svenska samhället, exempelvis i samband med de så kallade koranbränningarna. För att ha möjlighet att upptäcka källan till informationen, som skulle kunna vara en statlig aktör som vill skapa en oro och misstro i det svenska samhället, måste Säkerhetspolisen i realtid kunna följa hur informationen spridits, vem som är ursprunget och hur informationsflödesprocessen ser ut. För att förstå vilka som eventuellt radikaliseras av den desinformation som sprids, och som därför kan befaras komma att begå terrorhandlingar, behöver Säkerhetspolisen också förstå vilka mottagarna av desinformationen är. Säkerhetspolisen måste, för att kunna hantera denna uppgift, bearbeta och analysera informationsmängder under stark tidspress.

Det finns även behov att behandla uppgifter över tid eftersom det inte alltid är möjligt att identifiera vad som är relevant förrän informationen kopplas samman med annan information. I en nätverkskartläggning kan det krävas komplex analys för att koppla samman aktörer. Personer som inledningsvis framstått som mindre

relevanta i förhållande till Säkerhetspolisens uppdrag kan flera år senare, då kartläggningen kompletterats med ytterligare underlag, visa sig vara centrala gestalter. En person som inledningsvis framstått som perifer i ett nätverk kan visa sig vara den som kopplar samman ett nätverk med ett annat. Personuppgifter som var för sig inte är ägnade att väcka misstanke kan efter att ha analyserats över tid visa sig utgöra olika identiteter för en och samma antagonistiska aktör.

Vår uppfattning är att dagens regelverk inte ger tillräcklig förmåga för Säkerhetspolisen att utföra sitt underrättelseuppdrag eftersom det saknas medel för att effektivt behandla de allt större informationsmängderna. Det kan vara bland de uppgifter som framstår som perifera, och som därför i normalfallet måste raderas, som det dolda hotet kan uppstå och utvecklas utan att Säkerhetspolisen i dag har möjlighet att upptäcka det. I den information som Säkerhetspolisen tvingas lämna obearbetad och radera utan granskning kan det med säkerhet sägas finnas uppgifter som skulle kunna bidra till att skydda Sveriges eller våra allierades nationella säkerhet. Möjligheten att inhämta och behandla större datamängder över tid skulle också stärka myndighetens förmåga att utvärdera och lära av tidigare händelser, då information från exempelvis sociala medier kan vara en viktig pusselbit för att förstå varför ett skeende kom att se ut som det gjorde.

7.2.2 Behandling av vissa informationsmängder kräver undantag från dataskyddskonventionen

Nödvändiga åtgärder för att skydda nationell säkerhet

När det kommer till hotet mot nationell säkerhet och terrorism anser vi att det finns en betydande skillnad mellan förväntningarna på Säkerhetspolisens förmåga att upptäcka okända hot och myndighetens rättsliga möjligheter till ett effektivt underrättelsearbete. EU:s dataskyddsregelverk är inte tillämpligt för nationella säkerhets- och underrättelsetjänsters verksamhet och det finns betydande möjligheter till undantag motiverade av nationell säkerhet från de principer som följer av dataskyddskonventionen. Detta visar på att det finns en betydande skillnad mellan personuppgiftsrättens generella tillämpning och hur man ser på avvägningen mellan allmänna

och enskilda intressen som påverkas och behovet av att förebygga nationella säkerhetshot.

Det finns i dag ingen rättslig möjlighet för Säkerhetspolisen att över tid behandla stora mängder information för att analysera vilka uppgifter som kan vara relevanta för att exempelvis upptäcka spionibrottslighet eller förhindra terroristattentat. I en stor informationsmängd saknar ofta en majoritet av de personuppgifter som förekommer koppling till något ändamål för vilket Säkerhetspolisen får behandla personuppgifter. Som framgår av avsnitt 6.1 kan inte Säkerhetspolisen hantera all information som inkommer till myndigheten. Då mängden information ständigt växer och flödar i allt snabbare takt blir gapet mellan Säkerhetspolisens förmåga och behov med tiden allt större. Förmågan att snabbt kunna kontrollera och förstå stora mängder information är avgörande för en säkerhetstjänst.

Personuppgiftsrätten i allmänhet innehåller flera principer vars syfte är att förhindra att fler uppgifter än nödvändigt behandlas. Principerna om behov, ändamål, adekvans, relevans och uppgiftsminimering syftar till att säkerställa att endast uppgifter som behövs för ett på förhand uttalat ändamål får behandlas. I de flesta verksamheter i samhället finns inte några skäl att frångå dessa dataskyddsprinciper. Vi har i föregående avsnitt bedömt att det finns skäl att införa en ny säpodatalag uppbyggd enligt de principer som framgår av dataskyddskonventionen 108+. Dataskyddskonventionen utgör ett ramverk och lämnar inte detaljerade instruktioner om hur en nationell lagstiftning ska utformas. Vi anser att det finns goda möjligheter att tillämpa de flesta av konventionens grundläggande principer även inom en verksamhet som Säkerhetspolisens. När det gäller att bygga upp en förmåga att behandla informationsmängder som inte är möjliga att granska manuellt är det inte möjligt att på något meningsfullt sätt uppställa krav på relevans, adekvans eller uppgiftsminimering. Som vi har påpekat i föregående avsnitt finns det ett stort behov att inom alla Säkerhetspolisens verksamhetsgrenar behandla sådana uppgiftsmängder. Dataskyddskonventionen medger också undantag från flera centrala bestämmelser om det är nödvändigt och proportionerligt för att bland annat skydda nationell säkerhet (artikel 11).

Underrättelsetjänster över hela världen bygger nu upp förmågan att analysera stora datamängder i olika syften. Även inom Europa

finns det flera exempel på detta, exempelvis finns i Förenade kungariket särskild lagstiftning om behandling av så kallade ”bulk personal dataset”. Vi anser att det finns starka skäl som talar för att även Sverige ska göra vissa undantag från några av konventionens bestämmelser i syfte att stärka Säkerhetspolisens förmåga att behandla information. Säkerhetspolisen saknar i dag förmågor som är väsentliga för att förebygga, förhindra och upptäcka säkerhetshotande och brottslig verksamhet som innebär hot mot nationell säkerhet eller terrorism. Vi anser att denna förmåga är nödvändig för att Säkerhetspolisen ska kunna fullgöra sitt uppdrag och att det behövs anpassade regler för att hantera personuppgiftsbehandling av vissa stora informationsmängder.

Proportionerliga undantag som respekterar grundläggande fri- och rättigheter genom bestämmelser i en särskild lag

Vi anser att vårt förslag till ny säpodatalag bör gälla generellt för personuppgiftsbehandling som sker inom Säkerhetspolisens brottsbekämpande verksamhet som rör nationell säkerhet. Från denna lagstiftning bör vissa undantag göras för att kunna behandla vissa informationsmängder som behövs i verksamheten men inte kan hanteras enligt den nya säpodatalagen. Undantagen bör medge behandling inom vissa ramar som respekterar de grundläggande fri- och rättigheter som kommer till uttryck i dataskyddskonventionen och Europakonventionen.

När det kommer till hur de undantag som vi anser vara nödvändiga ska utformas, finns det inte något tydligt ramverk att förhålla sig till. De vägledningar som finns angående behandling av stora datamängder har sällan beaktat den särskilda avvägning som bör gälla då ändamålet med behandling är skyddet av nationell säkerhet. Det gäller exempelvis den rekommendation till dataskyddskonventionen som rör behandling av stora datamängder.[5] Rekommendationen är generell till sin utformning och har inte fokus på brottsbekämpning och i synnerhet inte sådan brottsbekämpning som gäller nationell säkerhet. Det finns dock flera principer i riktlinjen som lämpligen kan utgöra en utgångspunkt för den lagstiftning vi här föreslår. Exempelvis att det ska finnas möjligheter till test och

[5] Europarådet, *Guidelines on the Protection of Individuals with regard to the Processing of Personal Data in a World of Big Data*, 17 januari 2017.

träning genom simulering innan ett system används operativt eller att olika medel för behandling ska ha inbyggt dataskydd.

Det sker en mycket snabb teknisk utveckling i samhället. Genom att göra lagstiftningen så långt som möjligt teknikneutral kan den förbli hållbar över tid. Samtidigt kommer nya tekniker med nya risker. Lagen behöver därför balansera flexibiliteten att kunna utnyttja tekniska framsteg samtidigt som den måste innehålla tillräckliga kontrollmekanismer för att bibehålla sin rättsstatliga legitimitet. Mekanismer som skapar legitimitet anser vi vara helt avgörande för att förtroendet både för Säkerhetspolisen och för de nya metoder som teknikutvecklingen medför.

Samma tekniker som ibland utmålas som en stor samhällelig risk och ett vapen för antagonister kan och bör även användas som ett skydd för samhället som minimerar detta hot och skapar ökad trygghet. I detta syfte finns ett stort behov av att kunna hantera stora datamängder. I flera utvecklade demokratier sker sådan behandling redan i dag. Även Sverige behöver ett robust system för att Säkerhetspolisen ska kunna utnyttja denna möjlighet under robust, rättsstatlig kontroll. En hörnsten i en ny lagstiftning på området är att den innehåller robusta tillsynsmekanismer. Det är en förutsättning för tilltron till att rättsstaten har förmåga att hantera den tekniska utvecklingen på ett ansvarsfullt sätt.

7.2.3 Behandling av stora datamängder innebär en ökad risk för integritetsintrång och för avhållande inverkan på opinionsfriheterna

Personlig integritet vid behandling av stora informationsmängder

Även om det inte finns någon koppling mellan den lagstiftning vi föreslår och EU-rätten, finns anledning att nämna praxis från EU-domstolen avseende hantering av stora mängder information i form av generell datalagring av uppgifter om elektronisk kommunikation. Datalagring innebär en skyldighet för tillhandahållare av elektroniska kommunikationsnät och kommunikationstjänster, t.ex. mobiloperatörer, att lagra uppgifter om elektronisk kommunikation. Domstolen har ansett att lagring av trafik- och lokaliseringsuppgifter från elektronisk kommunikation utgör ett ingrepp i de grundläg-

gande rättigheter till respekt för privatlivet och skydd av personuppgifter. Detta oberoende av om de uppgifter som avser privatlivet är av känslig art eller ej eller om de berörda har fått utstå eventuella olägenheter på grund av ingreppet. Det är inte heller relevant huruvida de lagrade uppgifterna därefter används eller inte.

EU-domstolen har motiverat sin slutsats med att trafik- och lokaliseringsuppgifter kan avslöja information om ett stort antal aspekter av de berörda personernas privatliv, inbegripet känslig information, såsom sexuell läggning, politisk åskådning, religiös, filosofisk eller annan övertygelse, samhällsåskådning samt hälsotillstånd. Dessa uppgifter kan sammantagna göra det möjligt att dra mycket precisa slutsatser om privatlivet för de personer vilkas uppgifter har lagrats, såsom deras vanor i vardagslivet, deras stadigvarande och tillfälliga uppehållsorter, deras dagliga förflyttningar och förflyttningar i övrigt, de aktiviteter de utövar, deras sociala relationer och de umgängeskretsar de rör sig i. Sådana uppgifter gör det möjligt att kartlägga de berörda personerna på ett sätt som är lika känsligt med avseende på rätten till respekt för privatlivet som själva innehållet i kommunikationerna.[6]

Även Europadomstolen har i flera mål kunnat konstatera att polisens eller olika nationella säkerhetsmyndigheters lagring av personuppgifter i sig utgör ett intrång av rätten till privatliv som garanteras enligt artikel 8.1 i Europakonventionen.[7] Många domar har handlat om hur medlemsstaterna motiverat dessa intrång och en bedömning av om dessa motiv utgör en proportionerlig avvägning mellan enskildas rätt till privatliv och statens intressen av registreringen. Vi anser att detta synsätt bör avspeglas i den lagstiftning vi nu föreslår på området.

Avhållande inverkan på opinionsfriheterna

Med integritetsriskerna av att utöka möjligheten till kartläggning följer även riskerna att människor börjar anpassa sitt beteende för att undvika kartläggning. EU-domstolen har vid flera tillfällen påpekat att en omfattande insamling av uppgifter om elektronisk

[6] EU-domstolens dom den 6 oktober 2020 i de förenade målen C 511/18, C 512/18 och C 520/18, *La Quadrature du Net*, p. 115–117.
[7] Se bland andra *Leander mot Sverige*, nr 9248/81, 26 mars 1987, *M.M. mot Förenade kungariket*, nr 24029/07, 13 november 2012, *M.K. mot Frankrike*, nr 19522/09, 18 april 2013.

kommunikation kan ha en avhållande inverkan på hur medborgare väljer att utöva sin yttrandefrihet genom sådana kommunikationskanaler.[8] Med en lagstiftning som mer generellt tillåter behandling av uppgifter kan resonemanget överföras även till andra källor och även allmänt tillgänglig information.[9]

I avsnitt 6.2.2 och 6.2.4.resonerar vi om att det finns ett behov, en förväntan och ett berättigat intresse för Säkerhetspolisen att kartlägga bland annat extremistiska och våldsbejakande miljöer på internet. Det kan handla om exempelvis stängda eller öppna chattforum där det förekommer radikalisering, rekrytering och annan brottslig verksamhet. I sådana datamängder finns information som är relevant för Säkerhetspolisens verksamhet och erfarenhet från andra länder visar att en strukturerad bearbetning av den här typen av data har resulterat i att tidigare okända hotaktörer upptäckts. Materialet innehåller också en betydande mängd personuppgifter som inte är relevanta för Säkerhetspolisens uppföljning.

Den brottsbekämpande verksamheten i allmänhet, så även förmågan att behandla större datamängder på ett strukturerat sätt, kan verka avhållande i förhållande till yttranden eller manifestationer som utgör brottsliga gärningar. Att upptäcktsrisken verkar brottspreventivt är inte något problem. Riskerna med den ökade förmågan är att den även verkar avhållande i förhållande till yttranden som inte är kriminaliserade eller kan anses utgöra brottslig verksamhet. Om det upplevs medföra en risk för kartläggning att nämna vissa ord eller ge uttryck för en kontroversiell politisk uppfattning eller att förespråka en viss religiös tolkning är påverkan på opinionsfriheterna ett faktum, se avsnitt 6.3.3.

En lagstiftning som medger behandling av fler uppgifter än vad som kan anses direkt relevanta för bekämpande av säkerhetshotande verksamhet anser vi inte utgöra ett direkt intrång i exempelvis yttrande- eller religionsfriheten. Människor är oförhindrade att utöva sina fri- och rättigheter och många uppfattar sannolikt redan i dag att vissa kontroversiella ämnen kan väcka myndigheters intresse. En sådan lagstiftning får ändå anses medföra ett indirekt intrång, som följer av risken att yttranden eller uttryck, nu eller i framtiden,

[8] Se bland annat EU-domstolens dom, *La Quadrature du Net*, p. 118.
[9] Se avsnitt 4.4.3 om den kritik som riktats mot den norska lagstiftning som tillåter lagring av allmänt tillgänglig information.

kan ge negativa konsekvenser för enskilda som inte är proportionerliga i ett demokratiskt samhälle.

Sammanfattande utgångspunkter för den nya lagstiftningen

Det kan mot den nu skisserade bakgrunden konstateras att en lagstiftning måste balansera mellan olika var för sig starka intressen. Den nya lagen ska å ena sidan skapa rättsliga förutsättningar för Säkerhetspolisen att hantera vissa stora informationsmängder som behövs i verksamheten men i dag inte kan behandlas. Samtidigt medför en sådan behandling, å andra sidan, ett intrång i de registrerades personliga integritet och medför risker för en påverkan på opinionsfriheten. Vi kommer i kapitel 9 att redovisa våra överväganden hur de beskrivna behoven kan uppfyllas med bibehållet skydd för den personliga integriteten och opinionsfriheterna.

8 En ny lag om Säkerhetspolisens behandling av personuppgifter

8.1 Lagens syfte och tillämpningsområde

8.1.1 Lagens syfte

Förslag: Syftet med lagen ska vara att skydda fysiska personers grundläggande rättigheter och friheter i samband med behandling av personuppgifter och att säkerställa att Säkerhetspolisen kan behandla personuppgifter på ett ändamålsenligt sätt.

Av artikel 1 i dataskyddskonventionen 108+ framgår att syftet med konventionen är att skydda enskilda med avseende på behandling av dennes personuppgifter och därigenom bidra till respekten för de mänskliga rättigheterna och grundläggande friheterna, särskilt avseende rätten till privatliv.

I nuvarande säpodatalag anges att syftet med lagen är att skydda fysiska personers grundläggande rättigheter och friheter i samband med behandling av personuppgifter och att säkerställa att Säkerhetspolisen kan behandla och utbyta personuppgifter på ett ändamålsenligt sätt (1 kap. 1 §). Lagens syfte är dubbelt. Vi anser att detta syfte återspeglar att en central målsättning för all personuppgiftslagstiftning är att skydda den personliga integriteten och andra grundläggande fri- och rättigheter. Detta skydd är emellertid inte ovillkorligt. Det är en nödvändig förutsättning för Säkerhetspolisens verksamhet att det sker en avvägning mellan skyddet för den personliga integriteten och det allmänna intresset av att Säkerhetspolisen kan bedriva sin verksamhet effektivt. I likhet med den tidigare lagstiftningen bör lagens syfte återspegla att den utgör en sådan avvägning; mellan enskildas fri- och rättigheter och det nationella säker-

hetsintresset. Även säkerhetsintresset syftar ju ytterst till att säkerställa fri- och rättigheter i Sverige.

Den nuvarande säpodatalagen syftar även till att Säkerhetspolisen ska kunna *utbyta* personuppgifter på ett ändamålsenligt sätt. Skälet till att utbyte av personuppgifter särskilt nämns hör samman med att säpodatalagen är uppbyggd efter samma modell som EU:s brottsdatadirektiv. Direktivet avsåg att harmonisera medlemsstaternas skyddsnivå för personuppgifter bland annat i syfte att underlätta det fria flödet av personuppgifter mellan unionens brottsbekämpande myndigheter.[1] Detta syfte återspeglas inte lika tydligt i dataskyddskonventionen 108+ vars syfte är att skydda enskildas fri- och rättigheter vid behandling av personuppgifter, vilket kan bidra till det fria flödet av information.[2] Vi anser därför, till skillnad mot nuvarande ordning, att säpodatalagen inte bör ha som syfte att säkerställa informationsutbyte. I övrigt bör den nuvarande lagens syfte även gälla för vårt förslag.

8.1.2 Lagens tillämpningsområde

Förslag: Lagen ska vara tillämplig vid behandling av personuppgifter i Säkerhetspolisens brottsbekämpande verksamhet som rör nationell säkerhet.

Lagen ska även gälla Polismyndigheten då den övertagit en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen.

Bedömning: Lagen bör inte vara tillämplig vid behandling av andra uppgifter än personuppgifter.

Säpodatalagens nuvarande tillämpningsområde

Den nuvarande säpodatalagen gäller behandling av personuppgifter i Säkerhetspolisens brottsbekämpande och lagförande verksamhet som rör nationell säkerhet (1 kap. 2 §). Om Säkerhetspolisen behandlar personuppgifter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott som inte rör natio-

[1] Se bl.a. förklaringssats 4 och 7 samt artikel 1.2 b brottsdatadirektivet.
[2] Se artikel 1 i dataskyddskonventionen 108+ samt 6 stycket i preambeln.

nell säkerhet tillämpas i stället brottsdatalagen (1 kap. 4 §). Sådan behandling kan ske då Säkerhetspolisen bistår Polismyndigheten i enskilda fall eller efter överenskommelse enligt 13 § i Säkerhetspolisens instruktion. För verksamhet som inte rör brottsbekämpning ska EU:s dataskyddsförordning tillämpas, oavsett om verksamheten omfattas av unionsrätten eller inte (1 kap. 2 § dataskyddslagen).

Vad ingår i brottsbekämpande och lagförande verksamhet?

När det gäller frågan om säpodatalagens tillämpningsområde konstaterade regeringen i förarbetena till nuvarande lag att *syftet* med personuppgiftsbehandling inte nödvändigtvis behöver utgöra begränsningen, eftersom brottsdatadirektivet inte är tillämpligt. Regeringen ansåg i stället att *verksamheten* där behandlingen sker utgjorde en lämplig avgränsning, i likhet med den tidigare polisdatalagens tillämpningsområde. Trots att all Säkerhetspolisens verksamhet har ansetts vara ”i viss utsträckning brottsbekämpande” ansåg regeringen att vissa gränsdragningsfrågor kunde uppkomma. Delar av verksamheten har inte ett lika tydligt brottsbekämpande syfte som övrig verksamhet, vilket beror på att Säkerhetspolisen också är en säkerhetstjänst. Eftersom denna verksamhet är inriktad på att förebygga att säkerhetshot skapas och kan förverkligas ansåg regeringen att den indirekt kan sägas ha brottsbekämpande syfte. För att markera att lagen skulle omfatta även denna, mer indirekt brottsbekämpande verksamhet, diskuterades om lagens tillämpningsområde skulle omfatta exempelvis ”brottsbekämpande och annan operativ verksamhet”. Regeringen stannade dock vid att låta lagen endast omfatta Säkerhetspolisens brottsbekämpande (och lagförande) verksamhet. Skälet var att inarbetade begrepp inte bör ändras utan starka skäl. Några sådana hade inte framförts i lagstiftningsärendet, även om regeringen såg fördelar med ett utvidgat tillämpningsområde.[3]

Syftet med den nuvarande säpodatalagen är därmed att den ska anses omfatta all operativ verksamhet inom Säkerhetspolisen. Det innefattar kärnverksamheten som nationell säkerhetstjänst där det brottsbekämpande uppdraget till stor del innebär underrättelseverksamhet i syfte att förebygga, förhindra och upptäcka brottslig verksamhet. Brottsbekämpning i form av det brottsutredande uppdraget

[3] Prop. 2018/19:163 s. 53.

är förhållandevis litet men innebär att Säkerhetspolisen även utgör en polismyndighet. Vid sidan av dessa delar har Säkerhetspolisen även flera andra uppdrag knutna till sin roll som säkerhetstjänst, bland annat person- och säkerhetsskydd samt uppgifter inom utlännings- och medborgarskapslagstiftningen. Sådana övriga uppgifter har det gemensamt att de alla kan innebära hantering av mycket känslig information och att de drar nytta av Säkerhetspolisens samlade lägesbild över företeelser som kan innebära hot mot nationell säkerhet. Alla dessa övriga uppgifter anses utgöra brottsbekämpning, men kopplingen till brott inom Säkerhetspolisens ansvarsområde är svagare och tyngdpunkten mot att förebygga säkerhetshotande verksamhet får anses starkare.[4] I polislagen anges dessa uppdrag även vid sidan av de renodlat brottsförebyggande och brottsutredande uppdragen.

Vad ingår i nationell säkerhet?

I sitt remissvar till den nuvarande säpodatalagen efterfrågade Polismyndigheten en definition av begreppet nationell säkerhet, i syfte att kunna underlätta bedömningen av när lagen är tillämplig. Regeringen konstaterade att det rör sig om ett EU-rättsligt begrepp som avgränsar EU:s kompetens gentemot medlemsstaterna. I förlängningen är det upp till EU-domstolen att avgöra begreppets närmare innebörd och det är därför inte lämpligt att definiera uttrycket.[5]

Från dataskyddsförordningens tillämpningsområde undantas endast behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten. Det är därför möjligt att gränserna för EU:s kompetens, och begreppet skydd av nationell säkerhet kan komma att prövas i frågor som rör skyddet av personuppgifter.[6]

Sedan säpodatalagen beslutades har också EU-domstolen prövat ett antal fall som rör dataskyddsförordningens tillämpningsområde och förklarat att undantaget ska tolkas restriktivt. Undantaget avser enligt domstolen behandling av personuppgifter som statliga myndigheter utför som ett led i en verksamhet som syftar till att upprätt-

[4] Jfr prop. 2018/19:163 s. 66.
[5] Prop. 2019/20:163 s. 52 och prop. 2017/18:232 s. 104.
[6] Se t.ex. EU-domstolens dom den 5 juni 2023 i mål C–204/21 p. 318–319 och den 20 oktober 2022 i mål C–306/21 p. 40–41.

hålla nationell säkerhet eller andra kategorier av verksamheter som på grund av sin art inte omfattas av unionsrätten. Sådan verksamhet utmärks bland annat av att den syftar till att skydda statens grundfunktioner och samhällets grundläggande intressen.[7]

Vi delar regeringens tidigare bedömning av att det varken är lämpligt eller ens möjligt att definiera begreppet nationell säkerhet i lag. Nationell säkerhet är ett begrepp som behöver innehålla ett visst mått av flexibilitet. Tolkning och tillämpning av begreppet måste därför i någon mån vara en fråga för praxis.[8] Vår tolkning är dock att begreppet kan omfatta hela verksamheter, så länge verksamheten är ägnad att skydda eller upprätthålla nationell säkerhet. Vår bedömning är att alla Säkerhetspolisens nuvarande uppgifter i princip uteslutande ingår som ett led i en verksamhet som syftar till att skydda nationell säkerhet.

Vad omfattas inte av säpodatalagen?

Att den nuvarande säpodatalagen är begränsad till behandling av personuppgifter som rör nationell säkerhet i Säkerhetspolisens brottsbekämpande och lagförande verksamhet innebär att vissa delar av myndighetens verksamhet i stället omfattas av dataskyddsförordningens utvidgade tillämpningsområde.[9]

Enligt förarbetena till den nuvarande säpodatalagen gäller dataskyddsförordningen och den kompletterande svenska lagstiftningen i första hand då Säkerhetspolisen behandlar personuppgifter i den interna och administrativa verksamheten. Som exempel på interna åtgärder angavs framtagande av interna föreskrifter, handböcker och policydokument. Administrativ verksamhet exemplifierades där som personalfrågor och ekonomihantering. Regeringen ansåg att viss behandling av personuppgifter som utförs i Säkerhetspolisens interna eller administrativa verksamhet kan vara av sådan karaktär att den gäller nationell säkerhet. Det ska exempelvis inte vara möjligt för främmande makt att med hjälp av offentliga uppgifter kartlägga

[7] EU-domstolens dom den 22 juni 2021 i mål C–439/19 *Latvijas Republikas Saeima*, p. 66 och dom den 16 januari 2024 i mål C–33/22, *Österreichische Datenschutzbehörde mot WK*, p. 50–52.
[8] Se även Europarådets kommission för de mänskliga rättigheterna avgörande den 2 april 1993 *Esbester mot Förenade kungariket*, mål nr 18601/91.
[9] Se 1 kap. 2–3 §§ lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

Säkerhetspolisens organisation. Det konstaterades dock att Säkerhetspolisens organisation i större utsträckning än normalt omfattas av bland annat försvars- och underrättelsesekretess. Regeringen ansåg likväl att merparten av den personuppgiftsbehandling som sker i intern och administrativ verksamhet hos Säkerhetspolisen inte var av sådan karaktär att den kan anses röra nationell säkerhet.[10]

Tillsynen över den interna och administrativa verksamheten sker av Integritetsskyddsmyndigheten, och faller utanför Säkerhets- och integritetsskyddsnämndens tillsynskompetens.[11]

Finns det skäl att utvidga säpodatalagens tillämpningsområde?

Personuppgiftsbehandling för teknisk utveckling bör ske med stöd av säpodatalagen

Det finns som ovan beskrivits vissa problem att tolka lagens nuvarande tillämpningsområde, både avseende begreppet brottsbekämpande verksamhet och begreppet nationell säkerhet. Det följer av att inget av dessa begrepp är vare sig möjliga eller lämpliga att uttömmande definiera i lag. Det finns dock en naturlig korrelation mellan Säkerhetspolisens uppdrag och lagens tillämpningsområde, där utgångspunkten måste vara att i princip alla uppdrag som läggs på myndigheten är sådana att personuppgiftsbehandling ska kunna ske med stöd av säpodatalagen. Det finns sällan skäl att lägga en uppgift på Säkerhetspolisen som inte, i vid mening, rör brottsbekämpning avseende nationell säkerhet.

I vissa fall kan det dock finnas verksamhet inom myndigheten som inte direkt följer av något uttryckligt uppdrag men som behövs för att utföra en uppgift. En sådan verksamhet som identifierats under utredningen är den tekniska utvecklingsverksamheten som bedrivs inom myndigheten. Det handlar framför allt om utveckling av nya eller befintliga it-system, där personuppgiftsbehandling kan spela en central roll, se avsnitt 6.2.6.

Den tekniska utvecklingsverksamheten faller inte uppenbart inom den nuvarande lagens tillämpningsområde; behandling av personuppgifter som rör nationell säkerhet i Säkerhetspolisens brottsbekämpande och lagförande verksamhet. I likhet med andra myndig-

[10] Prop. 2018/19:163 s. 54.
[11] 1 § lag (2007:980) om tillsyn över viss brottsbekämpande verksamhet.

heter måste Säkerhetspolisen verksamhet ständigt ses över, förbättras och vidareutvecklas mot bakgrund av bland annat teknikutvecklingen, ändrade förutsättningar eller förväntningar för verksamheten.[12] För Säkerhetspolisen finns ett stort behov och en stor potential att strukturera, organisera och även i viss mån analysera information med ny teknik. Uppgiften att effektivisera och förenkla informationshanteringen inom myndigheten är inte ny. It-system och olika behandlingsmetoder har kontinuerligt utvecklats och vidareutvecklats i syfte att effektivisera myndighetens kärnverksamhet. Sådan teknisk utveckling har inte ansetts nödvändig att härleda till något uttryckligt uppdrag eller någon särskild rättslig grund, då det ansetts följa indirekt av andra uppdrag eller varit en nödvändig förutsättning för att myndighetens förvaltning och funktion.[13]

Vi anser att it-utveckling som syftar till att öka myndighetens förmåga att bearbeta och analysera personuppgifter utgör en del av den brottsbekämpande verksamheten. Teknisk utveckling som är inriktad mot brottsbekämpning utgör därmed även ett led i Säkerhetspolisens verksamhet som syftar till att upprätthålla nationell säkerhet. Vi bedömer därmed att det inte finns några hinder mot att tillämpa säpodatalagen för den personuppgiftsbehandling som behövs för att utveckla tekniska verktyg med en tydlig koppling till Säkerhetspolisens kärnverksamhet.

Övriga uppdrag som rör brottsbekämpning i vid bemärkelse

Säkerhetspolisens huvudsakliga brottsbekämpande uppdrag avser gärningar som är straffbelagda enligt 18 och 19 kap. brottsbalken och terroristbrottslagen. Myndigheten har emellertid många uppdrag som kan sägas röra brottsbekämpning utan att de för den delen är kopplade till den brottskatalog som myndigheten ansvarar för. Det kan exempelvis röra brottsbekämpning avseende brott eller brottslig verksamhet som inte omfattas av svensk jurisdiktion eller direkt rör svenska intressen men där Säkerhetspolisen har ett uppdrag att hjälpa utländska partners.

Säkerhetspolisen åläggs kontinuerligt nya uppgifter, senast genom en uppgiftsskyldighet i förhållande till Polismyndigheten angående

[12] Se 3 och 6 § myndighetsförordningen (2007:515) och 1 kap. 3 § budgetlagen och t.ex. prop. 2009/10:175 s. 24.
[13] Jfr prop. 2017/18:105 s. 59 f., prop. 2019/20:113 s.19 ff. och prop. 2023/24:29 s. 45 f.

terrorisminnehåll på internet enligt kompletterande bestämmelser till EU:s så kallade TCO-förordning.[14] Förordningen ålägger Sverige att utse en behörig myndighet som bland annat ska kunna förelägga så kallade värdtjänstleverantörer att avlägsna terrorisminnehåll från internet. I Sverige är Polismyndigheten utsedd att utföra dessa uppgifter och Säkerhetspolisen har fått uppdraget att lämna Polismyndigheten de uppgifter som den behöver för att fullgöra sitt uppdrag enligt TCO-förordningen.[15] Det kan i dessa fall röra sig om terrorisminnehåll som finns tillgängligt för svenskar att ta del av men som inte avser någon brottslig verksamhet i Sverige eller ens Europa. Denna uppgift kan tjäna som exempel på uppdrag som saknar direkt anknytning till eventuell brottslig verksamhet avseende svenska intressen.

Lagen bör vara tillämplig då Säkerhetspolisen ägnar sig åt brottsbekämpning som rör nationell säkerhet utan att lagens tillämpningsområde är kopplat till en viss brottskatalog. Som tidigare nämnts har det vid upprepade tillfällen uttalats att all operativ verksamhet vid Säkerhetspolisen i någon mån är brottsbekämpande. När det gäller begreppet nationell säkerhet har även klargjorts att det inte endast är Sveriges säkerhet som avses.[16]

Det har inte framförts något behov att utöka säpodatalagens tillämpningsområde utanför det nuvarande. Inom den brottsbekämpande verksamheten inryms all brottslighet som Säkerhetspolisen ska bekämpa med stöd av någon rättslig grund – oavsett om brotten angår svenska eller utländska förhållanden (under förutsättning att den omfattas av EU-domstolens definition av nationell säkerhet). När det gäller utländska förhållanden måste detta avgöras från fall till fall.

Intern och administrativ verksamhet som rör nationell säkerhet

I dagsläget omfattas inte Säkerhetspolisens administrativa verksamhet, som rör bland annat personalfrågor och ekonomihantering, av säpodatalagen eftersom detta område i många fall tydligt faller utanför myndighetens brottsbekämpande uppdrag, och därmed säpodata-

[14] Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorisminnehåll online (TCO-förordningen).
[15] 12 § lagen (2023:319) med kompletterande bestämmelser till EU:s förordning om åtgärder mot spridning av terrorisminnehåll online.
[16] Prop. 2018/19:163 s. 53.

lagens tillämpningsområde. Detsamma gäller annan intern verksamhet som exempelvis framtagande av interna regler, handböcker eller policydokument. För personuppgiftsbehandling som faller utanför brottsbekämpningen tillämpas dataskyddsförordningen fullt ut. Även den tidigare polisdatalagens tillämpningsområde var begränsad till brottsbekämpande verksamhet. Även tidigare saknades därmed särskild personuppgiftsreglering för Säkerhetspolisens administrativa och interna verksamhet som rör nationell säkerhet, som reglerades enligt den dåvarande personuppgiftslagen.

Det finns utrymme att lagstifta om att alla uppgifter som rör nationell säkerhet ska omfattas av säpodatalagen. Det innebär att det inte finns några hinder mot att låta administrativ och intern verksamhet som rör nationell säkerhet ingå vid sidan av de brottsbekämpande uppgifterna. Då Försvarsmakten och FRA fick ny personuppgiftslagstiftning år 2021 ansåg regeringen att det fanns övervägande skäl som talade för att lagstiftningen skulle vara heltäckande inom det område där Sverige har exklusiv lagstiftningskompetens.[17] För Försvarsmaktens del innebär den nya personuppgiftslagstiftningen att behandling av personuppgifter i all verksamhet som rör Sveriges försvar och säkerhet samt internationellt försvars- och säkerhetssamarbete omfattas av särregleringen. Tidigare hade endast Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst varit reglerad på annat sätt än genom personuppgiftslagen. Den nya lagstiftningen omfattar därmed även intern och administrativ verksamhet, så länge verksamheten rör Sveriges försvar.[18] Exempelvis omfattas numera Försvarsmaktens personuppgiftsbehandling i samband med personalrekrytering eller ekonomihantering av den särskilda regleringen, till skillnad från motsvarande verksamhet hos Säkerhetspolisen.

Det finns inget egensyfte av att utvidga säpodatalagens tillämpningsområde så långt det är möjligt. Den nuvarande ordningen har beskrivits som fungerande och Säkerhetspolisens behov avser i första hand myndighetens operativa verksamhet. Vårt fokus har därför inte varit att utreda frågan om dataskyddsförordningens utsträckta tillämpningsområde.

Nackdelen med att Säkerhetspolisen måste tillämpa två olika regelverk på verksamhet som rör nationell säkerhet, säpodatalagen

[17] Prop. 2020/21:224 s. 57–60.
[18] Ibid. s. 168.

för det som kan anses utgöra brottsbekämpning och dataskyddsförordningen för övrig verksamhet, ska inte överdrivas. Det finns även fördelar med att dataskyddsförordningen gäller för all personuppgiftsbehandling inom den interna och administrativa verksamheten och inte endast för de uppgifter som inte rör nationell säkerhet. En sådan är att det inte uppkommer gränsdragningsproblem vid bedömningen av om viss personuppgiftsbehandling rör nationell säkerhet och därmed faller utanför dataskyddsförordningens egentliga tillämpningsområde.[19] Det kan även underlätta att renodlat administrativa åtgärder hanteras inom samma regelverk hos i princip alla myndigheter.[20] Vi har sammantaget inte funnit skäl att frångå den nuvarande ordningen att begränsa säpodatalagens tillämpning till brottsbekämpande verksamhet som rör nationell säkerhet.

Polismyndigheten bör liksom i dag tillämpa lagen då den övertar en uppgift från Säkerhetspolisen

Enligt 15 § i Säkerhetspolisens instruktion[21] får en förundersökning eller annan uppgift i den brottsbekämpande verksamheten i ett enskilt fall lämnas över till Polismyndigheten för fortsatt handläggning. Enligt 25 § i Polismyndighetens instruktion[22] ska myndigheten även bistå vid polisverksamhet som leds av Säkerhetspolisen, om Säkerhetspolisen i ett enskilt fall begär det och det inte finns särskilda skäl mot det eller om Polismyndigheten och Säkerhetspolisen kommer överens om det.

Av 1 kap. 2 § andra stycket säpodatalagen framgår att lagen gäller vid Polismyndighetens behandling av personuppgifter när myndigheten har övertagit en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen. Av förarbetena framgår tydligt att bestämmelsen är avsedd att träffa både situationen att Polismyndigheten tagit över och då den biträder Säkerhetspolisen med en uppgift inom säpodatalagens tillämpningsområde.[23]

[19] Prop. 2017/18:105 s. 29–30.
[20] Försvarsdatalagen ska tillämpas på all personuppgiftsbehandling som sker vid Försvarsmakten som inte omfattas av unionsrätten. Även behandlingen av personuppgifter i Försvarsmaktens interna och administrativa verksamhet som rör myndighetens personal omfattas av lagen, se prop. 2020/21:224 s. 168.
[21] Förordning (2022:1719) med instruktion för Säkerhetspolisen.
[22] Förordning (2022:1718) med instruktion för Polismyndigheten.
[23] Prop. 2017/18:232 s. 105 f. samt prop. 2018/19:163 s. 55 och 211.

Polisens brottsdatalag bär stora likheter med den nuvarande säpodatalagen. Det kan antas ha underlättat Polismyndighetens förståelse och tillämpning av säpodatalagen. Den lag vi föreslår kommer avvika från brottsdatalagens systematik och avvika även i materiellt hänseende. Det innebär att det inte går att förutsätta att personal från Polismyndigheten lika sömlöst kan påbörja behandling enligt säpodatalagen. Det kan samtidigt konstateras att de situationer då Polismyndigheten tar över ett ärende från Säkerhetspolisen ofta sker i det skede då personuppgiftsbehandlingen även är förenlig med polisens brottsdatalag eller följer av särskilda bestämmelser i förundersökningskungörelsen och rättegångsbalken som gäller för båda myndigheterna. Om det i andra fall finns behov av att överlämna ett ärende som kräver behandling enligt säpodatalagen, får frågan lösas genom utbildningsinsatser eller stöd från Säkerhetspolisen.

Vi anser därmed att den nuvarande ordningen har skäl för sig och det har inte framkommit några skäl för att inskränka eller utvidga säpodatalagens tillämpningsområde i denna del.

Behandling av uppgifter om juridiska personer

Dataskyddsregler syftar ytterst till att säkerställa enskilda individers fri- och rättigheter. Det finns inga krav enligt dataskyddskonventionen 108+ som innebär att juridiska personers uppgifter ska omfattas av samma dataskydd som gäller för fysiska personers personuppgifter. Konventionsstaterna är emellertid fria att lagstifta om skydd även för juridiska personers uppgifter.[24]

När säpodatalagen infördes avhandlades inte frågan om vilket dataskydd som var nödvändigt för juridiska personers uppgifter annat än helt översiktligt. I förarbetena konstaterades att dessa uppgifter ofta utgjorde indirekta personuppgifter något som innebar att det kunde diskuteras om inte även sådana uppgifter borde skyddas. Eftersom det tidigare ansetts att sådant skydd var nödvändigt, bedömdes inte någon förändring i detta avseende påkallad då den nya säpodatalagen beslutades.[25] I den tidigare lagstiftningen, 2010 års polisdatalag, motiverades att vissa av lagens bestämmelser skulle göras tillämpliga

[24] Se artikel 3 samt artikel 13 i dataskyddskonventionen 108+ och p. 30 i *Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*.
[25] Prop. 2017/18:269 s. 113 och prop. 2018/19:163 s. 61.

även på juridiska personer främst med att personuppgifter om ägare eller ställföreträdare kunde vara svåra att särskilja från uppgifter om juridiska personer i den elektroniska hanteringen. Det konstaterades dock samtidigt att juridiska personer inte har samma behov av integritetsskydd som fysiska personer.[26] Liknande tekniska argument har använts för att motivera att juridiska personer omfattas av flera andra personuppgiftslagstiftningar, både inom det brottsbekämpande området[27] och i andra sektorer.[28] När den nyinrättade Utbetalningsmyndigheten fick en registerförfattning föreslog utredningen att juridiska personer borde omfattas av vissa bestämmelser, i huvudsak mot bakgrund av samma skäl som tidigare anförts i andra personuppgiftslagar.[29] Regeringen ansåg emellertid inte att det fanns tillräckliga skyddsskäl för uppgifter om juridiska personer för att låta delar av lagstiftningen utvidgas till att gälla utanför dataskyddsförordningens tillämpningsområde.[30] Samma ställningstagande förefaller ligga bakom att domstolsdatalagen (2015:728), trots utredningens förslag, inte omfattar juridiska personer.[31]

Vi har funnit skäl att överväga behovet av att juridiska personer omfattas av dataskyddsregler som tillkommit till skydd för den personliga integriteten. Om det fortfarande, i något avseende, finns tekniska svårigheter att särskilja uppgifter om juridiska personer från personuppgifter får det konsekvenser för hur Säkerhetspolisen kan behandla uppgifterna. Sådana tekniska svårigheter bör dock inte vara ett skäl till att personuppgiftslagen ska omfatta även uppgifter om juridiska personer. Uppgifter om exempelvis bolagsföreträdare, styrelsemedlemmar eller liknande är personuppgifter och får som sådana endast behandlas i den utsträckning personuppgiftslagstift-

[26] Prop. 2009/10:85 s. 78 och Ds 2007:43 s. 100 (där begreppet juridisk person emellertid missuppfattats). Att låta juridiska personers uppgifter omfattas av lagen var inspirerat av den samtida lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet (prop. 2004/05:164 s. 56).
[27] 1 kap. 6 polisens brottsdatalag och motsvarande registerförfattningar för Tullverket (2018:1694), Kustbevakningen (2018:1695) åklagarväsendet (2018:1697) och Skatteverket (2018:1696).
[28] Se bland annat 1 kap. 1 § andra stycket lag (2001:181) om behandling av uppgifter i Skatteverkets beskattningsverksamhet, 5 § kustbevakningsdatalag (2019:429), 1 kap. 1 § andra stycket lag (2001:185) om behandling av uppgifter i Tullverkets verksamhet, 1 kap. 3 § vägtrafikdatalag (2019:369).
[29] SOU 2020:35 s. 348 f.
[30] Prop. 2022/23:34 s. 121.
[31] Se Ds 2013:10 s. 52 och prop. 2014/15:148 s. 25. Jfr SOU 2001:100 s. 104–105.

ningen tillåter det.[32] Även indirekta uppgifter om enskilda personer är uppgifter som skyddas i personuppgiftslagstiftningen.

Det kan givetvis finnas skäl att låta juridiska personer omfattas av ett visst dataskydd. Det kan exempelvis ifrågasättas ur ett mer allmänt fri- och rättighetsperspektiv att Säkerhetspolisen samlar uppgifter om föreningar av olika slag. På samma sätt skulle en omfattande registrering av vilka bolag som handlar med vissa främmande stater kunna uppfattas som ett onödigt intrång i näringsfriheten. Vi anser samtidigt att det finns skäl som talar emot att låta den nuvarande ordningen bestå. Det kan finnas anledning för Säkerhetspolisen att övervaka vissa juridiska personers förehavanden. Juridiska personer kan bedriva säkerhetshotande verksamhet exempelvis i form av ideella föreningar vars mål är att med våld störta det demokratiska samhället. Det kan också röra sig om föreningar eller bolag som används för att organisera eller finansiera terrorism eller som används vid rekrytering till våldsbejakande miljöer. I dessa fall är Säkerhetspolisens intresse av den juridiska personen avhängigt hur fysiska personer på olika sätt nyttjar dessa juridiska personer för att bedriva säkerhetshotande verksamhet. I andra fall kan det vara den juridiska personen, exempelvis ett bolag, som är av direkt intresse. Det kan röra sig om att Säkerhetspolisen måste hålla sig informerad om vissa utländska bolag som verkar i Sverige eller i vårt närområde och ägarstrukturerna i dessa juridiska personer. Så kan vara fallet då en annan stat eller dess säkerhetstjänst har ett direkt inflytande över bolaget eller kan verka genom det. Det kan röra sig om olika bolagskonstruktioner som främmande makt kan sätta upp för att dölja olovlig teknikanskaffning i Sverige eller som används som täckmantel vid underrättelseinhämtning. Det kan även finnas andra skäl för Säkerhetspolisen att registrera uppgifter om juridiska personer inom bland annat säkerhetsskyddslagens tillämpningsområde eller lag (2023:560) om granskning av utländska direktinvesteringar.

Att säpodatalagen delvis är tillämplig för uppgifter om juridiska personer orsakar ett administrativt merarbete för myndigheten. Det finns exempelvis vissa svårigheter att definiera vad som är en juridisk person. I Sverige gäller det framför allt ideella föreningar, som inte behöver registrera sig hos någon myndighet utan kan bildas mer

[32] Se motsvarande argument i SOU 2023:10 s. 372 som föreslår att kompletterande registerförfattningar till Dataskyddsförordningen för Skatteverkets, Tullverkets och Kronofogdens icke-brottsbekämpande verksam inte längre ska omfatta juridiska personer.

formlöst genom att anta stadgar och utse en styrelse. Det stora problemet uppstår emellertid när det kommer till att bedöma om olika slags associationer i andra länder kan anses vara juridiska personer enligt utländsk rätt. Särskilt gäller det olika nätverk, lösa sammanslutningar och andra mer formlösa organisationer. Frågan om en association har rättskapacitet är enligt nuvarande lagstiftning avgörande att besvara för att veta vilka regler som ska tillämpas och i vissa fall om uppgifterna får samlas in och bevaras. Detta medför betydande tillämpningssvårigheter.

Vi anser sammantaget att det saknas tillräckliga skäl att låta lagen omfatta även behandling av uppgifter om juridiska personer. Vi uppfattar att den nuvarande bestämmelsen innebär en överreglering som inte medför tillräckligt substantiella integritetsvinster. Den skapar däremot tydliga verksamhetshinder och påverkar därmed myndighetens förmåga. Att lagen är tillämplig på direkta och indirekta personuppgifter om exempelvis föreningsmedlemmar och bolagsföreträdare anser vi ger ett tillräckligt skydd för den personliga integriteten. I den praktiska tillämpningen kommer skyddet för juridiska personer i många fall upprätthållas genom de indirekta personuppgifter som information om bland annat föreningar och bolag innehåller. Det bör därför inte införas någon bestämmelse om att lagen, helt eller delvis, ska vara tillämplig på uppgifter även om juridiska personer.

8.1.3 Förhållandet till annan lagstiftning

Förslag: Lagen ska vara subsidiär till bestämmelser i annan lag.

Den nuvarande säpodatalagen är, enligt 1 kap. 4 §, subsidiär till annan lag eller förordning. Bestämmelsen är motiverad i huvudsak av att enskildas rättigheter enligt säpodatalagen ansågs riskera att stå i strid med enskildas rätt till insyn i brottsutredningar och straffrättsliga förfaranden. Regeringen såg därför ett behov av att förtydliga att, i första hand, straffprocessuella men även andra regler skulle ha företräde framför säpodatalagen.

Att bestämmelser i speciallagstiftning som rör viss personuppgiftsbehandling ska ha företräde framför motsvarande bestämmelser i den generella personuppgiftslagstiftningen är inte anmärknings-

värt. Däremot kan omfattningen av den nuvarande bestämmelsen ifrågasättas. Den generella utformningen av 1 kap. 4 § innebär att även bestämmelser i förordning kan sätta lagens bestämmelser åt sidan. Det kan sättas i fråga om dagens bestämmelse är förenlig med den formella lagkraftens princip (8 kap. 18 § regeringsformen). För det fall en förordning i något avseende ska ha företräde framför en skyddslagstiftning bör det inte ske genom en så generell bestämmelse. Det kan däremot komma i fråga att riksdagen delegerar till regeringen att genom förordning reglera vissa avgränsade områden.[33] Sådan delegation bör enligt vår mening följa av respektive bestämmelse.

Den tidigare polisdatalagen var subsidiär i förhållande till lagen (2017:496) om internationellt polisiärt samarbete och de föreskrifter som regeringen har meddelat i anslutning till den lagen. Det framgår dock redan av 6 kap. 1 § lagen om internationellt polisiärt samarbete att den lagen och den till lagen knutna förordningen har företräde framför bland annat säpodatalagen.

Vi har inte uppmärksammat någon annan förordning som kan vara motiverad att ge företräde framför säpodatalagen. Det finns dock alltjämt ett behov att lagen ska vara subsidiär till bland annat rättegångsbalken eller speciallagstiftningar som rör inhämtning genom hemliga tvångsmedel. Med hänsyn till att säpodatalagen reglerar en integritetskänslig verksamhet bör endast lag kunna sätta skyddslagstiftningen åt sidan. Möjligheten att göra detta genom förordning bör därför inte överföras till den nya lagen.

8.2 All personuppgiftsbehandling som omfattas av lagen ska vara proportionell

8.2.1 Dataskyddskonventionens bestämmelser

Proportionalitet vid behandling av personuppgifter är en utgångspunkt i dataskyddskonventionen 108+:

> **Article 5 – Legitimacy of data processing and quality of data**
>
> 1. Data processing shall be proportionate in relation to the legitimate purpose pursued and reflect at all stages of the processing a fair balance

[33] Jfr Lagrådets yttrande i prop. 2017/18:269 s. 600.

between all interests concerned, whether public or private, and the rights and freedoms at stake.

Bestämmelsen saknar motsvarighet i konventionens tidigare lydelse och innebär att en behandling bara får ske om den är lämplig för att uppnå ändamålet. Det innebär att personuppgiftsbehandling inte får leda till ett oproportionerligt intrång i den registrerades fri- och rättigheter eller i något allmänt intresse. Proportionalitetsprincipen ska respekteras i alla skeden av behandlingen, även i det inledande skedet, när beslut fattas om huruvida behandlingen ska utföras eller inte.[34]

8.2.2 Den nuvarande regleringen

Proportionalitetsprincipen utgör en konstitutionell princip, som kommer till uttryck i 2 kap. 21 § regeringsformen. Där anges att inskränkningar i grundläggande fri- och rättigheter aldrig får gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den. Principen kommer, vid sidan av regeringsformen, till uttryck i ett stort antal bestämmelser i lagstiftning och i praxis från de högsta domstolarna. Numera anses proportionalitetsprincipen även utgöra en allmän rättsprincip inom förvaltningsrätten vid avvägningen mellan olika, men var för sig skyddsvärda, intressen.

I svensk förvaltningsrätt innebär principen att en myndighet måste avstå från att meddela ett betungande beslut för vilket man i och för sig kan ha författningsstöd, om de negativa konsekvenserna för den enskilde inte står i rimlig proportion till det allmänna intresse som ska tillgodoses.[35]

Det finns inte någon allmän föreskrift i säpodatalagen som innebär att de intressen som talar för respektive mot en behandling ska vägas mot varandra och vara utslagsgivande i fråga om en behandling ska utföras eller inte. Det finns emellertid ett exempel då Säkerhetspolisen uttryckligen ska tillämpa en proportionalitetsprincip. Det gäller vissa av de särskilda situationer då personuppgifter får överföras till ett annat land trots att det saknas garantier om ett adekvat dataskydd för uppgifterna. Då ska Säkerhetspolisen, enligt 9 kap.

[34] Se p. 40 i *Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.*
[35] Se bl.a. prop. 1987/88:65 s. 72, HFD 2012 ref. 12, HFD 2017 ref. 5 och NJA 2016 s. 868 p. 16.

4 § andra stycket säpodatalagen, först väga den registrerades intresse av skydd mot kränkning av rättigheter och friheter mot det allmänna intresset av överföringen. Detsamma gäller om en överföring, med stöd av 9 kap. 5 § ska göras till exempelvis ett privat företag eller en myndighet som inte har ett brottsbekämpande uppdrag i ett annat land.

Den proportionalitetsprincip som kommer till uttryck i artikel 5.1 i dataskyddskonventionen liknar den som Säkerhetspolisen tillämpar i många andra situationer, som inte direkt rör behandling av personuppgifter. För de straffprocessuella tvångsmedlen framgår principen direkt av de olika bestämmelserna och i polislagen finns en proportionalitetsprincip för polisingripanden.

I brottsdatadirektivet återfinns inte någon motsvarande proportionalitetsprincip som ska tillämpas vid alla behandlingsåtgärder. Enligt vissa särskilda bestämmelser ska dock motsvarande avvägningar göras. Exempelvis får, enligt artikel 4.2 b, personuppgiftsbehandling för andra ändamål än brottsbekämpning ske endast om sådan behandling är nödvändig och står i proportion till detta andra ändamål. Proportionalitetsbedömningar ska även ske i vissa fall enligt dataskyddsförordningen. Om en ny typ av behandling sannolikt innebär en hög risk för enskildas fri- och rättigheter, ska en konsekvensbedömning göras. Enligt artikel 35.7 b är en beståndsdel av en sådan konsekvensbedömning en prövning av proportionaliteten av behandlingen i förhållande till syftena.

8.2.3 Finns det behov av en uttrycklig proportionalitetsprincip i säpodatalagen?

Bedömning: Dataskyddskonventionen 108+ ställer upp krav på att all behandling av personuppgifter ska vara proportionerlig. Kravet kan genomföras antingen genom att lagen uppställer olika krav som innebär att proportionalitet uppnås eller genom att det föreskrivs att tillämparen ska göra en sådan avvägning.

Genom ett krav på att all personuppgiftsbehandling ska vara proportionerlig kan ändamålet vägas mot intrånget i varje enskilt fall. Det möjliggör en tillämpning som överensstämmer med lagens syfte: att skydda fysiska personers grundläggande rättigheter och friheter i samband med behandling av personuppgifter och

att säkerställa att Säkerhetspolisen kan behandla personuppgifter på ett ändamålsenligt sätt.

Teknikneutralitet vid insamling, inhämtning och vidarebehandling

Sådan övervakning och kartläggning av enskildas personliga förhållanden som omfattas av 2 kap. 6 § andra stycket regeringsformen eller sådana intrång i privatlivet som avses i artikel 8.1 i Europakonventionen, kan ske på olika sätt. Det görs inte någon skillnad på vilket sätt ett intrång i den personliga integriteten sker. Det är snarare åtgärdens effekter som är relevanta att bedöma för att avgöra om ett intrång också utgör en kränkning av en rättighet. Det kan därför vara lämpligt med ett teknikneutralt rättighetsskydd för att det inte ska vara möjligt att kringgå skyddsmekanismer genom att justera metoder eller för att inte skyddet efter en tid ska bli verkningslöst på grund av teknikutvecklingen. Vi anser att personuppgiftslagstiftningen på så sätt kan utgöra en teknikneutral skyddsmekanism som förhindrar att teknik och metoder som inte omfattas av särskild lagstiftning lämnas oreglerad i fråga om proportionalitet.

Tidigare personuppgiftslagar har reglerat behandlingsåtgärder i form av exempelvis insamling, bevarande, sökning, delning och radering av uppgifter. Det har också med relativt god träffsäkerhet varit möjligt att vid lagstiftningens beredning förutse hur information kommer att behandlas och vilka konsekvenser behandlingen kan få för enskilda. Exempelvis är det naturligt att personuppgifter som finns lagrade kan hittas genom sökning under hela tiden de behandlas.[36] Även om detaljerna i Säkerhetspolisens it-system är i ständig utveckling och förbättringar skett bland annat i träffsäkerheten vid sökning eller hur information presenteras, har det grundläggande intrånget i den skyddade rättigheten som sker genom sådana behandlingsåtgärder varit likartad ända sedan myndigheten övergick till datoriserad informationshantering.

I samband med att nya tekniker utvecklats kan intrånget i den personliga integriteten vara mer svårförutsägbar. Utvecklingen kan medföra att det nu eller i framtiden är möjligt att behandla personuppgifter på ett sätt som utgör ett större intrång än vad som varit

[36] Jfr exempelvis prop. 1997/98:97 s. 146.

förväntat då uppgifterna samlades in. Ett exempel är bildmaterial som numera är sökbart på ett annat sätt än tidigare. Denna teknikutveckling innebär att det numera kan anses mer känsligt att exempelvis behandla stora mängder bildmaterial. Teknik för automatiska jämförelser och sökningar av sådant material gör att det som tidigare inte varit möjligt med hänsyn till den manuella arbetsinsats som krävts nu kan göras snabbt, enkelt och träffsäkert. Om sökningar efter individer i ett videomaterial dessutom kan ske i realtid, kan övervakningskameror användas på ett helt annat sätt än som varit möjligt tidigare. Denna teknikutveckling och den potentiella effekten för den personliga integriteten som den har inneburit har föranlett särskild regleringen av bland annat behandling av biometriska uppgifter.

I framtiden kan det vara möjligt att vidta andra liknande behandlingsåtgärder med personuppgifter som innebär ett större intrång än vad som tidigare varit möjligt. Det potentiella intrånget i enskildas rättigheter kan vara likartat, men regleringen kan skilja sig mycket åt beroende på om lagstiftaren hunnit ta ställning till och reglera behandlingen i fråga. Uppgifter som framstod som skäliga att samla in och bevara vid insamlingstidpunkten kan senare visa sig vara mycket integritetskänsliga, då tekniska landvinningar möjliggjort att de behandlas på ett annat sätt. Europadomstolen har exempelvis identifierat att så kallad metadata, uppgifter som omgärdar det egentliga kommunikationsinnehållet vid elektronisk kommunikation, kan utgöra mycket skyddsvärda uppgifter. Sådan data kan enligt domstolen numera användas för att teckna ”en intim bild av en person” genom kartläggning av dennes kontakter, sociala nätverk, platsdata, webhistorik och kommunikationsmönster. Domstolen ansåg att behandling av sådan data, som inte utgör kommunikationsinnehåll och därför inte omfattas av särskild tvångsmedelslagstiftning i alla länder (i Sverige krävs dock beslut av åklagare eller domstol), inte nödvändigtvis utgör ett mindre intrång i den personliga integriteten än själva innehållet i en kommunikation.[37]

Vi har uppfattat att den tekniska utvecklingen är mycket svår att förutse. Att interagera med de stora språkmodellerna, som Chat-GPT, på det sätt som görs i dag tycktes som en omöjlighet för endast några år sedan. Om utvecklingen fortsätter att accelerera, inom bland annat artificiell intelligens, framstår det som svårt för lagstiftaren

[37] Se Europadomstolens dom, *Centrum för Rättvisa mot Sverige*, p. 256 och 277.

att följa med i utvecklingen och reglera framtida integritetsrisker var för sig. Riskerna med nya behandlingsmetoder inom Säkerhetspolisens verksamhet är givetvis särskilt höga eftersom myndigheten förfogar över en stor mängd personuppgifter som kan vara av känslig art. Uppgifter över vilka enskilda, av naturliga skäl, inte har möjlighet att ha kontroll.

Omvänt kan även sägas att det kan komma att finnas teknik tillgänglig som det finns ett starkt samhälleligt intresse av att Säkerhetspolisen använder. För att Säkerhetspolisen på ett effektivt sätt ska kunna utföra sitt uppdrag behöver myndigheten tillgodogöra sig och använda ny teknik. Det är inte önskvärt att lagstiftningen är så statisk att Säkerhetspolisen hindras från i och för sig rimliga och proportionerliga behandlingsåtgärder.

Den proportionalitetsprincip som följer av artikel 5.1 i dataskyddskonventionen 108+ kan utgöra ett hinder mot att ny teknik används på ett sätt som inte är förenligt med grundläggande värderingar i vårt samhälle. Samtidigt medger denna princip tillräcklig flexibilitet för att tillåta att ändamål av stor vikt motiverar större intrång i andra skyddsvärda intressen än ändamål som är av lägre dignitet. Proportionalitetsprincipen kan därför öppna för en teknikneutral och flexibel lagstiftning, både för verksamhetens behov och för de intressen som dataskyddet värnar.

Styrkan hos ändamålet bestämmer omfattningen av behandlingen

I avsnitt 6.2 redogör vi för några av de problem som identifierats med nuvarande lagstiftning. Ett av dem är att uppgifter med en uppenbar verksamhetsnytta, som exempelvis uppgifter från forum för IS-resenärer eller uppgifter som inhämtats från en person som misstänktes vara aktiv agent för främmande makt, inte kunnat behandlas på grund av alltför strikta krav enligt nuvarande regelverk. Det finns förväntningar på att Säkerhetspolisen ska ha en hög förmåga att samla in och bearbeta information, i syfte att förhindra brott som kan påverka nationell säkerhet. Denna förväntan ökar naturligen i händelse av ett kraftigt försämrat säkerhetsläge. Det framstår på samma sätt som självklart att polisen dimensionerar en insats och bestämmer vilken utrustning som ska användas beroende på vilket brott eller vilken ordningsstörning det är fråga om.

Nuvarande säpodatalag medger emellertid inte att någon hänsyn tas till de allmänna intressen som kan motivera att Säkerhetspolisen har behov av att utföra en viss behandling. Regleringen bygger på synsättet att all behandling måste passera samma prövning, utan tydlig hänsyn till hur tungt ändamålet för behandlingen väger. I princip kan samma personuppgifter behandlas för ett ändamål med mycket låg aktualitet som för ett som avser avvärjande av en akut samhällsfara.

Detta något formalistiska synsätt kan också innebära omotiverat omfattande personuppgiftsbehandling för ändamål som framstår som mindre angelägna. Så länge de formella kraven är uppfyllda finns inte någon tydlig mekanism som innebär att skäligheten prövas. Denna brist på proportionalitetsprövning i personuppgiftsbehandlingen har också föranlett fällanden av Europadomstolen.[38]

En proportionalitetsprövning kan motivera behandling för tungt vägande ändamål, som inte bör tillåtas för mindre angelägna syften. Säkerhetspolisens brottsbekämpande verksamhet i stort avser det synnerligen tungt vägande allmänintresset nationell säkerhet. Det skulle kunna motivera en mycket tillåtande lagstiftning. Samtidigt kan konstateras att all Säkerhetspolisens verksamhet inte avser de mest allvarliga säkerhetshoten. En generellt tillåtande lagstiftning skulle därför kunna vara oproportionerlig i förhållande till mindre allvarliga eller mer avlägsna hotbilder. En bedömning för varje behandlingsåtgärd framstår därför som mer lämplig än att försöka anpassa lagen till någon form av mellanläge, som kan framstå som oproportionerlig i förhållande både till det allmänna intresset av att behandla uppgifter och intresset av att inte finnas registrerad hos myndigheten.

Styrkan hos andra intressen kan begränsa behandlingen

Nuvarande lagstiftning har en på många sätt neutral utformning när det gäller bedömningen av vilka personuppgifter som är skyddsvärda. Alla känsliga personuppgifter skyddas på samma sätt och uppgifter som inte innefattas i denna kategori omfattas i princip av samma regler.

[38] Se *Segerstedt-Wiberg m.fl. mot Sverige* där bristen på proportionalitet vid Säkerhetspolisens behandling av personuppgifter särskilt framhölls.

Hur stort intrång behandling av personuppgifter kan anses innebära för den personliga integriteten eller för bland annat yttrandefriheten beror på flera faktorer. Vi uppfattar att det exempelvis är ett väsentligt mycket större intrång i den personliga integriteten att behandla uppgifter om en enskilds sexualliv eller sexuell läggning än att behandla hälsouppgifter om en persons benbrott. Det är också stor skillnad mellan att en säkerhetstjänst aktivt samlar in politiska eller religiösa yttringar från sociala medier än att det i ett enskilt fall framgår mer indirekt. Ändå regleras dessa behandlingar i princip på samma sätt enligt nuvarande lagstiftning. Enligt säpodatalagen är det behovet som styr möjligheten till behandling av känsliga personuppgifter. Om det är absolut nödvändigt får i princip behandlingen utföras och skyddet ge vika.

Även om det i vissa fall kan finnas ett absolut behov av att kartlägga exempelvis politiska åsikter eller religiös övertygelse är det långt ifrån säkert att det är rimligt att genomföra en sådan kartläggning. Det är fullt rimligt att sådan känslig behandling även ska underkastas en mer allmän bedömning av de faktiska eller potentiella effekterna och inte endast verksamhetsbehovet. Det kan också konstateras att känsliga personuppgifter utgör ett trubbigt instrument för att bedöma vilken behandling som är den mest integritetskänsliga. Den mycket breda palett av uppgifter som inryms i detta begrepp kan alla graderas på olika sätt. En hälsouppgift som avser en stukad fot kan exempelvis inte jämföras med en som avser en psykiatrisk diagnos. För en präst i Svenska kyrkan är knappast religiös övertygelse en lika känslig uppgift som för en person som riskerar förföljelse på grund av sin tro.

I vissa andra länder kompletteras de känsliga personuppgifterna av andra skyddsmekanismer. I den tyska grundlagen skyddas exempelvis ”privatlivets innersta kärna” (Kernbereich persönlicher Lebensgestaltung). Skyddet gäller särskilt icke-offentlig kommunikation med betrodda personer och som ska kunna ske under rimliga förväntningar på att ingen övervakning sker.[39] Enligt nuvarande säpodatalag krävs det inte någon särskild avvägning mellan vilka uppgifter som behandlas, så länge de inte ingår bland de särskilt uppräknade känsliga personuppgifterna. Att bedömningen av om en uppgift får behandlas eller inte sker så binärt som säpodatalagen ger uttryck

[39] Se Tysklands federala författningsdomstols (Bundesverfassungsgerich) avgörande den 26 april 2022 i mål 1619/17, punkt 276.

för framstår inte som helt ändamålsenligt. Särskilt inte mot bakgrund av den låga graden av insyn i verksamheten.

Som framgår i inledningen av detta avsnitt finns det i och för sig en allmän proportionalitetsprincip i svensk förvaltningsrätt som är avsedd att förhindra åtgärder som innebär negativa konsekvenser för den enskilde som inte står i rimlig proportion till det allmänna intresse som ska tillgodoses. Tröskeln för att tillämpa denna oskrivna regel får dock anses relativt hög och sker i praktiken sannolikt främst på klagan av enskild. De åtgärder vi anser bära på de största riskerna är sådana där enskilda är omedvetna om intrånget eller som avser allmänna intressen, som intrång i opinionsfriheterna, där enskilda inte har något direkt klagorätt. Att det direkt av lag framgår att en proportionalitetsprövning ska göras vid all behandling av personuppgifter innebär både ett förtydligande av en viktig princip och att orimliga effekter av personuppgiftsbehandling kan motverkas.

Helhetssyn i stället för detaljreglering

Säpodatalagen tillämpas på så sätt att varje personuppgift prövas var för sig mot en rad olika bestämmelser. Om en personuppgift, som ett namn, förekommer i en chattkonversation mellan två personer, kommer uppgiften först behöva kopplas till ett konkret ändamål, som i vissa fall måste framgå genom en särskild upplysning. Därefter måste det prövas om uppgiften är nödvändig för ändamålet och dessutom adekvat, relevant och inte onödigt omfattande. Vid prövningen kommer det inte bedömas hur relevant chattkonversationen som sådan är för Säkerhetspolisens verksamhet. Den ovan beskrivna prövningen ska göras för enskilda uppgifter även om det kan vara helt uppenbart att konversationen i sin helhet behövs för att kartlägga exempelvis ett terroristnätverk (se avsnitt 6.1.5).

I praktiken bidrar denna granskning, som framgår av avsnitt 6.1.3, till att minska den faktiska mängden information som behandlas av Säkerhetspolisen. Den detaljnivå som präglar tillämpningen av säpodatalagen kan på så sätt sägas bidra till ett högt dataskydd, beroende på att personuppgiftsbehandling är förenad med en hög kostnad, i form av granskningsresurser. Samtidigt kan en mycket stor mängd uppgifter om en enskild person behandlas, så länge myndigheten lagt ner sådana resurser för att tillgodose formella förutsättningarna

för behandlingen. Ett välformulerat ändamål och en oklanderlig genomförd personuppgiftsgranskning kan medge en mycket omfattande kartläggning av en enskilds privatliv. Det kan vara svårt för tillsynsmyndigheten eller den enskilde att ifrågasätta lagligheten av sådan behandling, även om den skulle framstå som överdriven i det enskilda fallet.

Ett proportionalitetskrav öppnar för möjligheten att både bedöma relevanta sammanhang i sin helhet samtidigt som den samlade personuppgiftsbehandlingen går att ifrågasätta på ett annat sätt än i dag. Det kan till exempel innebära att Säkerhetspolisen kan granska och vidarebehandla ett it-beslag i sin helhet snarare än att pröva varje enskild uppgift i ett sådant beslag. Det kan också innebära att en sådan granskning som Europadomstolen använder för att pröva proportionaliteten av personuppgiftsbehandling i det enskilda fallet kan integreras i verksamheten och även vara föremål för tillsyn.

Vi anser att ett uttryckligt krav på proportionalitet innebär att lagens syften kan uppnås: att skydda fysiska personers grundläggande rättigheter och friheter i samband med behandling av personuppgifter och att säkerställa att Säkerhetspolisen kan behandla personuppgifter på ett ändamålsenligt sätt.

8.2.4 Det bör införas en uttrycklig proportionalitetsprincip i säpodatalagen

Förslag: Ett grundläggande krav för all behandling av personuppgifter med stöd av lagen ska vara att behandlingen är proportionerlig.

En personuppgiftsbehandling är proportionerlig om skälet för att utföra behandlingen överväger intrånget i de enskilda eller allmänna intressen som kan påverkas av den.

Det finns skäl för en proportionalitetsprincip

Enligt artikel 5.1 i dataskyddskonventionen 108+ ska all personuppgiftsbehandling vara proportionerlig. Detta konventionskrav kan uppfyllas genom att lagstiftningen utformas genom att olika intressen vägs mot varandra så att endast de behandlingsåtgärder

som är proportionerliga tillåts. Det kan exempelvis ske genom en mycket strikt reglering av vilka personuppgifter som får behandlas eller ett krav på att känsliga uppgifter endast får behandlas under en kort tid. Det är även möjligt att sätta upp olika trösklar, där exempelvis brottsmisstankar av viss styrka eller avseende vissa utpekade brott, kan ge möjlighet till en mer omfattande personuppgiftsbehandling. Då har kravet uppfyllts på lagstiftningsnivå.

Det andra sättet, som vi förordar, är att införa ett uttryckligt proportionalitetskrav för all personuppgiftsbehandling inom säpodatalagens tillämpningsområde. Vi har kommit till slutsatsen att det finns goda skäl som talar för att Säkerhetspolisen inför varje behandlingsåtgärd ska pröva om skälen för åtgärden väger tyngre än den påverkan på enskilda eller allmänna intressen som åtgärden innebär. Det gäller både vid beslut om att samla in personuppgifter, som att lagra dem under viss tid och om vilka olika behandlingsåtgärder som ska vidtas. Vi kommer i förslag till enskilda bestämmelser längre fram i betänkandet förklara hur en proportionalitetsprövning kan få genomslag och påverka utfallet i det enskilda fallet.

Sammanfattningsvis kan konstateras att kravet på att all personuppgiftsbehandling ska vara proportionerlig ger ett större utrymme att behandla uppgifter när ändamålet är tillräckligt specificerat och av sådan tyngd att det anses väga över de andra intressena av att inte behandla uppgifterna i fråga. Ett vagt formulerat ändamål kan däremot inte ge tillräcklig ledning för en sådan prövning. En proportionalitetsprövning innebär att mycket allvarliga samhällshot kvalitativt kan motivera en kartläggning av högre kvantitet. Om ändamålet endast avser en klart avgränsad fråga, exempelvis frågor som rör medborgarskap är utrymmet för personuppgiftsbehandling begränsat till de uppgifter som är proportionerliga att behandla för detta ändamål, vilket måhända inte innebär en så stor förändring mot hur uppgifter behandlas i dag. Vår bedömning är att proportionalitetsprövningen kommer få störst betydelse vid den underrättelseverksamhet som syftar till att upptäcka brott mot rikets säkerhet eller terrorbrott.

Är det möjligt att införa en proportionalitetsprövning vid all personuppgiftsbehandling?

Att tillämpa en uttrycklig och generell proportionalitetsprincip på det sätt vi föreslår är en nyhet i svensk personuppgiftsrätt. Det finns därför skäl att noga överväga hur en sådan bestämmelse kan komma att påverka verksamheten och om den är möjlig att införa i praktiken.

Ett proportionalitetskrav för varje enskild behandling kan framstå som en tung materiell prövning i den dagliga verksamheten hos en myndighet vars kärnverksamhet i stor utsträckning består av personuppgiftsbehandling. Det finns emellertid en hög kompetens hos både Säkerhetspolisen och tillsynsmyndigheterna, som i många andra sammanhang måste tillämpa en proportionalitetsprincip. Åtgärder som vidtas för särskild utlänningskontroll får endast ske efter en avvägning mellan det enskilda och det allmänna intresset.[40] För hemliga tvångsmedel och andra straffprocessuella tvångsmedel utgör en proportionalitetsavvägning en självklar rättsstatlig förutsättning. I likhet med den prövning som ska göras i dessa fall är proportionalitetsavvägningen det sista steget i en samlad bedömning av om intrånget i rättigheten är godtagbart i ett demokratiskt samhälle. De steg som föregår den slutliga avvägningen är inga nyheter för Säkerhetspolisen. Ett första grundläggande krav är *legalitet*. Detta krav om lagstöd för intrånget följer av säpodatalagens krav på rättslig grund för behandling av personuppgifter. Därutöver måste intrånget i den grundläggande fri- och rättigheten syfta till att uppnå ett *berättigat ändamål*. Att ändamålet för behandlingen ska vara tydligt för den som hanterar personuppgifter inom myndigheten är en naturlig del av det nuvarande arbetssättet. Slutligen ska åtgärden som inskränker den enskildes rätt vara *nödvändig* för att uppnå ändamålen. Den behandlingströskel som följer av all personuppgiftslagstiftning är ett utflöde av detta krav, tillsammans med bestämmelser om uppgiftsminimering, relevans och adekvans. Om alla dessa krav är uppfyllda återstår den slutliga prövningen av om skälen för åtgärden överväger andra intressen.

Myndigheten kommer behöva bedöma om en behandlingsåtgärd är proportionerlig. Vi föreslår dock inget särskilt dokumentationskrav av bedömningen. Däremot innebär förstås en lagreglering att

[40] 1 kap. 8 § lag (2022:700) om särskild kontroll av vissa utlänningar.

Säkerhetspolisen även i enskilda fall kan behöva förklara sin proportionalitetsbedömning inför tillsynsmyndigheten, på samma sätt som att behov, adekvans och relevans måste kunna motiveras i dag. Eftersom proportionalitet, enligt vårt förslag, är en förutsättning för att få behandla uppgifter måste utgångspunkten vara att all behandling genomgått denna prövning. En del av tillsynen kommer därför vara att pröva om Säkerhetspolisen haft fog för sin bedömning i denna del.

Sammantaget framstår det för oss som att en proportionalitetsprövning är möjlig att införa i Säkerhetspolisens verksamhet som innefattar personuppgiftsbehandling utan att den i sig utgör en betungande administrativ pålaga. Tvärtom kan en sådan prövning motivera att uppgifter inte behöver granskas på den nivå som gäller i dag. En samlad proportionalitetsprövning bedömer vi vara en nödvändig komponent i en lagstiftning som både kan medge en effektiv och ändamålsenlig personuppgiftsbehandling som tillgodoser Säkerhetspolisens behov och samtidigt utgör ett adekvat skydd för de enskilda och allmänna intressen som kan påverkas.

Vår uppfattning är att prövningen kommer att kunna integreras i verksamheten på ett naturligt sätt, i likhet med de ingripanden som görs med stöd av polisära befogenheter och som regleras genom 8 § polislagen. I förarbetena till polislagen framhölls att det närmast var en självklarhet att en uttrycklig behovs- och proportionalitetsprincip ska framgå av lagtexten. De allmänna befogenheterna för polisingripande som framgår av denna bestämmelse ska även tillämpas vid exempelvis val av olika spaningsmetoder.[41]

Hur bör proportionalitetsprincipen utformas

När det kommer till utformningen av principen finns det anledning att ge paragrafen en lydelse som ligger nära konventionstexten. Det förklarar att paragrafen avser att införliva artikel 5.1 direkt i lagen.

En direktöversättning av artikel 5.1 skulle kunna ha följande lydelse. ”Behandlingen av uppgifter ska vara proportionerlig i förhållande till det berättigade ändamål som eftersträvas och i alla skeden återspegla en skälig avvägning mellan alla berörda intressen, både de enskilda och allmänna, och de rättigheter och friheter som står på spel.” Denna lydelse framstår som omständlig och inte fullt

[41] Prop. 1983/84:111 s. 76–78.

ut förenlig med svensk lagstiftningstradition. Andemeningen och syftet med bestämmelsen måste dock vara att föreskriva dels att all behandling ska vara proportionerlig, dels förklara vilka intressen som ska vägas mot varandra. Paragrafen kan därför lämpligen delas in i två meningar när den första meningen slår fast att en proportionalitetsprincip ska tillämpas för all behandling av personuppgifter. Den andra meningen ska innebära att en avvägning ska göras mellan det allmänna intresset av att Säkerhetspolisen utför behandlingen och de enskilda och allmänna intressen som kan påverkas av den. De grundläggande fri- och rättigheterna ingår i begreppet enskilda och allmänna intressen. Att det ska ske en avvägning mellan mål och medel vid behandling av personuppgifter är centralt och måste framgå tydligt. Det kan finnas anledning formulera denna avvägning på liknande sätt som andra svenska lagar.

Proportionalitetsprincipen förekommer även i annan lagstiftning. I regeringsformen slås, i 2 kap. 21 §, fast att en begränsning av en fri- och rättighet aldrig få gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen såsom en av folkstyrelsens grundvalar. I förvaltningslagen (2017:900) har principen utformats som att en åtgärd aldrig får vara mer långtgående än vad som behövs och får vidtas endast om det avsedda resultatet står i rimligt förhållande till de olägenheter som kan antas uppstå för den som åtgärden riktas mot. I rättegångsbalken uttrycks den, i bland annat 24 kap. 1 § om häktning: skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den misstänkte eller för något annat motstående intresse. I 8 § polislagen (1984:387) anges principen på ett annat sätt. Där förklaras att en polisman som ska verkställa en tjänsteuppgift ska göra på ett sätt som är försvarligt med hänsyn till åtgärdens syfte och övriga omständigheter. I 15 § lagen (2023:421) om ordningsvakter finns motsvarande regel, men uttryckt på ett modernare sätt: ett ingripande ska ske på ett sätt som står i rimlig proportion till åtgärdens syfte och omständigheterna i övrigt.

Av detta axplock ur svensk rätt framkommer att det inte finns något enhetligt sätt att uttrycka principen om att det ska ske en avvägning mellan olika intressen. Detta bör uttryckas så enkelt som möjligt. Vi anser att avvägningen ska beskrivas som att skälet för att

utföra behandlingen ska överväga intrånget i de enskilda eller allmänna intressen som kan påverkas av den. Då framgår att det är ändamålet för att behandla personuppgifter som ska vägas mot de grundläggande fri- och rättigheterna eller andra enskilda eller allmänna intressen som kan påverkas av behandlingen. Bestämmelsen ska tillämpas före en behandling utförs, vilket innebär att den kommer utgöra en prognos.

Vilket genomslag kan proportionalitetsprincipen få i det enskilda fallet?

Dataskydd handlar i stor utsträckning om skyddet för den personliga integriteten. Vi anser dock att det för en nationell säkerhetstjänst även finns skäl att noggrant överväga hur insamling och annan behandling av personuppgifter kan komma att påverka andra grundläggande fri- och rättigheter än de som rör enskildas privatliv. Vi tänker i detta sammanhang främst på direkt eller indirekt påverkan på yttrandefriheten och andra opinionsfriheter (se avsnitt 6.3.3). Detta är en skillnad mot de proportionalitetsbedömningar som är föreskrivna för straffprocessuella tvångsmedel där avvägningen företrädesvis görs mot enskilda intressen.

Personuppgifter får bara behandlas om det behövs för ett ändamål. Prövningen av behovet att utföra behandlingen föregår alltid proportionalitetsprövningen, eftersom det aldrig kan vara proportionerligt att behandla uppgifter, eller på annat sätt begränsa en grundläggande fri- och rättighet, om det inte behövs för ett ändamål som är godtagbart i ett demokratiskt samhälle.

Frågan om proportionalitet innebär en prövning av om dessa ändamål i det enskilda fallet väger tyngre än de andra intressena som påverkas. Eftersom lagstiftaren gett Säkerhetspolisen i uppdrag att bland annat förebygga, förhindra och upptäcka ett visst slags brottslig verksamhet är behandling av de personuppgifter som direkt behövs för att utföra uppdraget ofta proportionerligt i och för sig. Proportionalitet syftar till att förhindra att grundläggande fri- och rättigheter kränks. Syftet är förstås inte att på ett allmänt plan försvåra för myndigheten att utföra sitt uppdrag.

Proportionalitetsprincipen ger emellertid möjlighet att gradera skälen för att utföra behandlingen efter ändamålens tyngd. Om det exempelvis rör sig om personuppgifter som återfunnits i ett it-beslag från en dömd terrorist får den brottsliga gärningen i det fallet sägas

föranleda att det krävs en avsevärd styrka i de andra intressena för att behandling av de personuppgifter som återfinns i beslaget ska undvaras. Det framstår som uppenbart att alla uppgifter i beslaget kommer att behöva behandlas över tid för att kunna jämföras och kopplas samman med andra uppgifter (jämför avsnitt 6.2.3).

På motsvarande sätt kan en kartläggning av en inte fullt så allvarlig brottslighet eller brottslig verksamhet som inte är lika specifik innebära att vikten av de andra intressena inte behöver vara fullt så tunga, för att de ska påverka Säkerhetspolisens beslut i fråga om behandlingsåtgärden. Ett sådant beslut innebär dock inte nödvändigtvis att insamling av uppgifter vid sådan kartläggning inte får ske; det finns olika sätt att minska intrånget av åtgärden för att uppnå proportionalitet.

Den lag vi föreslår kommer ge Säkerhetspolisen flera verktyg för att kunna förverkliga en proportionalitetsprövning på ett effektivt sätt. Ändamålsbestämmelserna, uppgiftsminimering och behandlingstid utgör viktiga komponenter för att uppnå proportionalitet vid behandling. Den lagstiftning vi föreslår innehåller olika verktyg för att kompensera intrånget i syfte att nå en skälig balans mellan myndighetens behov och andra skyddsvärda intressen. Vår intention och lagstiftningens syfte är att ge Säkerhetspolisen ett större utrymme att behandla de personuppgifter som krävs för att skydda nationell säkerhet, men att sådan behandling inte får riskera att medföra ett oskäligt intrång i de grundläggande medborgerliga fri- och rättigheterna.

Sådana verktyg kan påverka prövningen exempelvis då Säkerhetspolisen går igenom uppgifter som inhämtats med stöd av preventiva tvångsmedel. Ofta kan det vid sådan tvångsmedelsanvändning inhämtas ett omfattande material som endast delvis är av direkt intresse för den brottsliga verksamhet som undersöks. Frågan kan då uppkomma om det i materialet finns uppgifter som behövs för att upptäcka ännu okänd brottslig verksamhet. Om det bedöms finnas ett sådant behov, måste det göras en proportionalitetsprövning för behandlingen. Det kan exempelvis röra sig om kommunikationsinnehåll mellan anhöriga eller vänner, där en stor mängd känsliga och intima personuppgifter kan förekomma. Trots att det finns ett operativt behov av att behandla uppgifterna under till exempel tio år kan prövningen utmynna i att det skulle innebära ett alltför stort integritetsintrång. Då finns i vår föreslagna lag en möjlighet att redan

då uppgifterna registreras fastställa en kortare behandlingstid, i exempelvis tre år. Integritetsintrånget för en kortare behandlingstid är lägre, vilket kan utmynna i att behandlingen är proportionerlig i förhållande till ändamålet.

Ett annat exempel från Säkerhetspolisens verksamhet är personskyddet av den centrala statsledningen. Inför en händelse med möjlig hög risk, exempelvis Almedalsveckan i Visby, kan aktiviteter som rör Säkerhetspolisens skyddspersoner behöva kartläggas. En omfattande informationsinhämtning kan då vara motiverad för att bedöma aktuell hotnivå för skyddspersonerna. Om inhämtning sker i exempelvis sociala medier eller på olika internetforum i detta syfte, kan det förutsättas att ett omfattande material som innehåller känsliga personuppgifter kommer att behandlas. Detta kan antas utgöras av helt legitima opinionsyttringar kring skyddspersonerna. En kartläggning av sådana yttranden får sägas riskera att utgöra ett stort intrång i opinionsfriheterna. Samtidigt krävs en bred inhämtning för att kunna bedöma hotbilden. För att kunna motivera en sådan behandling krävs ett specifikt ändamål av stor vikt och att behandlingen inte pågår under längre tid än vad som är absolut nödvändigt. Vi anser att Säkerhetspolisen i detta fall skulle kunna motivera en bred inhämtning från sociala medier i syfte att kartlägga exempelvis kvantiteten av och allvaret i hotfulla uttalanden kring de aktuella skyddspersonerna, men att behandlingen måste upphöra omedelbart efter att hotbilden kunnat utvärderas eller händelsen avslutats. Det skulle kunna innebära att behandlingstiden begränsas till några månader och därmed utgör en skälig personuppgiftsbehandling i förhållande till intrånget i yttrandefriheten som kartläggningen kan innebära.

Ett annat sätt att minska intrånget är att tillämpa olika mekanismer för uppgiftsminimering. Det kan ske manuellt eller med automatiserad programvara som identifierar tecken på våldsbejakande extremism genom lingvistiska markörer.[42]

En proportionalitetsprövning ger även en möjlighet att ge allvaret i säkerhetshotet genomslag vid avvägningen. För terrorbrottslighet är det exempelvis klart att behovens tyngd kan medge en mer extensiv personuppgiftsbehandling än brott som utgör ett mindre konkret eller mera avlägset hot mot nationell säkerhet. För allvarliga säkerhets-

[42] Se exempelvis Johansson, Fredrik m.fl., *Detecting Linguistic Markers of Violent Extremism in Online Environments*, tillgänglig via https://www.researchgate.net/.

hot kan även behandling av mer perifera uppgifter eller omfattande behandling av känsliga uppgifter över längre tid vara proportionerligt.

Uppgifternas karaktär kan även beaktas i större utsträckning. Redan med nuvarande lagstiftning anses det exempelvis proportionerligt att behandla uppgifter om främmande makts underrättelseofficerare och agenter under mycket lång tid. Att Säkerhetspolisen behandlar uppgifter om de diplomater och annan personal som arbetar på vissa länders ambassader, utgör inte ett särskilt påtagligt integritetsintrång för de registrerade. De individer som bedriver underrättelseverksamhet mot Sverige under diplomatisk täckmantel måste förutsätta att de övervakas och kartläggs. Motsvarande bedömning av både säkerhetshotet och intrång kan göras i andra fall, exempelvis avseende de personer som rest utomlands för att ansluta sig till en terroristorganisation. Att uppgifter om sådana personer, som utgör uppenbara hot mot nationell säkerhet, behandlas under lång tid är godtagbart och i det närmaste förväntat i demokratiska rättsstater. I andra vågskålen kan förekomsten av känsliga personuppgifter, mycket privat kommunikation, eller sammanhang där det i hög grad förekommer uttryck för opinionsfriheterna tillåtas få större tyngd vid en proportionalitetsprövning.

Av det ovanstående följer att ändamålet med personuppgiftsbehandlingen i många fall blir helt avgörande vid proportionalitetsprövningen. Vi inledde detta avsnitt med att konstatera att Säkerhetspolisen endast får behandla de uppgifter som behövs för något av myndighetens uppdrag. När ett behov kunnat konstateras finns det naturligtvis en viss tyngd i ändamålet, eftersom Säkerhetspolisens uppdrag rör frågor om nationell säkerhet. Behandling för sådana ändamål innebär att det som regel finns ett utrymme att begränsa andra allmänna och enskilda intressen på ett annat sätt än vad som gäller för de flesta andra myndigheters personuppgiftsbehandling. Proportionalitetsprövningen måste därför ske i den kontext som gäller för Säkerhetspolisens verksamhet och de politiska överväganden som gjorts avseende myndighetens uppdrag, metoder och befogenheter i övrigt.

Det innebär också att en mer schabloniserad tillämpning kan tillåtas för exempelvis breda underrättelseändamål. Proportionalitetsprövning ger dock gott om utrymme att frångå schabloner när ändamålet är mer precist. Detta gäller både insamling och vidarebehandling av personuppgifter. Vi kommer återkomma till hur proportionalitetsprövningen

kan tillämpas i samband med andra bestämmelser i den av oss föreslagna lagen.

Vi föreslår av dessa skäl att det införs en grundläggande bestämmelse om proportionalitet i den nya lagen.

8.3 Rättslig grund för personuppgiftsbehandling

8.3.1 Dataskyddskonventionens bestämmelser

Av dataskyddskonventionen 108+ följer att personuppgiftsbehandling som sker utan samtycke måste vila på en rättslig grund:

> **Article 5 – Legitimacy of data processing and quality of data**
>
> 2. Each Party shall provide that data processing can be carried out on the basis of the free, specific, informed and unambiguous consent of the data subject or of some other legitimate basis laid down by law.

Enligt kommentaren till bestämmelsen avses med annan rättslig grund fastställd i lag, bland annat de lagliga grunder för behandling som anges i dataskyddsförordningen: som behandling till följd av avtal, för att skydda den registrerades eller annans intressen av grundläggande betydelse, för att uppfylla en rättslig förpliktelse, för ett allmänt intresse eller för den personuppgiftsansvariges berättigade intressen.

8.3.2 Den nuvarande regleringen

I avsnitt 3.5.4 redogör vi för den nuvarande bestämmelsen om rättslig grund. Sammanfattningsvis anges under rubriken rättslig grund, i 2 kap. 1 § säpodatalagen bland annat att personuppgifter får behandlas om det är nödvändigt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott mot Sveriges säkerhet, terrorbrott, eller tryckfrihetsbrott och yttrandefrihetsbrott med rasistiska eller främlingsfientliga motiv.[43] Vidare framgår att personuppgifter får behandlas för att utreda eller lagföra sådana brott eller efter särskilt beslut annat brott.

[43] Se avsnitt 3.5.4 angående 2 kap. 1 § 1 punkten c som oavsiktligt medger behandling av personuppgifter för brottsbekämpning utanför Säkerhetspolisens ansvarsområde.

I paragrafen framgår även att Säkerhetspolisens uppgifter i samband med personskydd, enligt säkerhetsskyddslagen eller utlännings- och medborgarskapslagstiftningen är rättsliga grunder för personuppgiftsbehandling. Slutligen anges att personuppgifter även får behandlas om det är nödvändigt för att fullgöra någon annan uppgift som rör nationell säkerhet och som anges i lag eller förordning eller särskilt beslut av regeringen eller fullgöra förpliktelser som följer av internationella åtaganden.

8.3.3 Den rättsliga grunden bör inte definieras i säpodatalagen

Bedömning: Säkerhetspolisens brottsbekämpande uppdrag som rör nationell säkerhet anges och avgränsas i annan författning. Det finns därför inte något behov av att i säpodatalagen upprepa för vilka rättsliga grunder personuppgifter får behandlas.

Förslag: Av lagen ska framgå att Säkerhetspolisen endast får behandla personuppgifter för att bedriva verksamhet som rör nationell säkerhet och som följer av lag, förordning, internationella åtaganden eller särskilt beslut av regeringen.

Den rättslig grunden för Säkerhetspolisens personuppgiftsbehandling

Det finns ett allmänt konstitutionellt krav på att intrång i enskildas rättighetssfär endast får ske med stöd av lag eller annan författning. Denna legalitetsprincip följer direkt både av 2 kap. 20 § regeringsformen och av artikel 8.2 i Europakonventionen.

I likhet med andra myndigheter, och brottsbekämpande myndigheter i synnerhet, kan Säkerhetspolisen endast i undantagsfall tillämpa samtycke som grund för personuppgiftsbehandling. Det finns därför ett krav på att personuppgiftsbehandling ska ske för att utföra en uppgift som har stöd av lag eller annan författning. Säkerhetspolisen rättsliga grund för att behandla personuppgifter finns samlad i flera olika rättsakter (se avsnitt 3.2.1).

Myndighetens huvudsakliga uppgifter följer av polislagen. Där framgår Säkerhetspolisens övergripande brottsbekämpande uppdrag och vissa uppgifter som är utmärkande för en säkerhetstjänst. Av 1 § förordningen (2022:1719) med instruktion för Säkerhetspolisen framgår även att Säkerhetspolisen i egenskap av säkerhetstjänst bedriver underrättelse- och säkerhetsarbete. Av instruktionen framgår även den brottskatalog som myndigheten ansvarar för i det brottsbekämpande och lagförande arbetet, vilka som omfattas av det personskydd som Säkerhetspolisen ansvarar för och hur säkerhetsskyddsarbetet får bedrivas.

Begreppet *rättslig grund* för personuppgiftsbehandling används i EU:s rättsakter, som i dataskyddsförordningen och genomgående i de lagar som bygger på EU-rättsliga förlagor. Begreppet återfinns även i brottsdatalagen och dataskyddslagen. I samband med att EU:s dataskyddsdirektiv för brottsbekämpning genomfördes och en ny säpodatalag beslutades, diskuterades skillnaden mellan ändamål och rättslig grund.

Regeringen kunde konstatera att det som i den tidigare polisdatalagen angetts som primära, övergripande ändamål var allt för oprecisa för att kunna betecknas som ändamål. I stället ansågs den tidigare uppräkningen av primära ändamål som en definition av den rättsliga grunden för personuppgiftsbehandling.[44] Denna uppräkning överfördes därför i stort sett oförändrad till säpodatalagen, men under en annan rubrik.

Det finns inte anledning att räkna upp vissa rättsliga grunder i säpodatalagen

Säkerhetspolisens brottsbekämpande verksamhet är specifik och inriktad på några få, särskilt allvarliga och svårupptäckta säkerhetshot som rör nationell säkerhet. Detta följer av både polislagen och myndighetens instruktion. En förutsättning för att Säkerhetspolisen ska få behandla personuppgifter är att Säkerhetspolisen har ålagts att utföra en viss arbetsuppgift. Dessa arbetsuppgifter framgår av lag, förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att utföra uppgiften.

[44] Se prop. 2018/19:163 s. 62 f. och prop. 2017/18:232 s. 123 f.

Kravet på att det finns en rättslig grund för behandling av personuppgifter kan uppfyllas genom att det i lagen framgår att personuppgifter endast får behandlas då Säkerhetspolisen utför en sådan uppgift. Att i Säkerhetspolisens personuppgiftslagstiftning räkna upp samtliga rättsliga grunder som ålägger myndigheten ett brottsbekämpande uppdrag som rör nationell säkerhet fyller inte någon egentlig funktion. Som framgår av avsnitt 8.1.2 ovan är det heller inte möjligt att exakt definiera lagens tillämpningsområde, men utgångspunkten måste vara att de uppdrag som åläggs myndigheten är sådana att säpodatalagen ska tillämpas.

Att räkna upp rättsliga grunder även i personuppgiftslagen kan inte heller anses vara något rättsstatligt legalitetskrav eller medföra någon ökad förutsebarhet för medborgare. Att som nu upprepa Säkerhetspolisens uppgifter både i polislagen och i säpodatalagen ger nämligen inte någon ytterligare ledning om vilken typ av personuppgiftsbehandling som kan förväntas ske av Säkerhetspolisen. Den nuvarande uppräkningen framstår både som specifik, avseende exempelvis uppgifter inom personskyddet, men också som väldigt generell då den även innehåller en hänvisning till ”övriga uppgifter”.

Vi bedömer att de rättsakter som reglerar Säkerhetspolisens uppdrag redan är så tydliga som kan krävas för att medborgarna ska kunna förutse inom vilka områden myndigheten verkar och har ett behov av att kunna behandla personuppgifter. Att upprepa uppdraget i personuppgiftslagstiftningen fyller inte någon ytterligare funktion än den avgränsning som redan följer av lagens tillämpningsområde.

Det bör framgå att personuppgifter endast får behandlas med stöd av någon rättslig grund inom lagens tillämpningsområde

Försvarsmakten och FRA:s lagstiftning är av senare datum än de lagar som följde EU:s dataskyddsreform, bland dem säpodatalagen. Regeringen vände sig i det lagstiftningsärende mot att införa begreppet rättslig grund även inom försvarsområdets personuppgiftslagstiftning. Regeringen förklarade att de rättsliga grunderna för Försvarsmaktens och FRA:s behandling av personuppgifter finns i de regelverk som ligger till grund för myndighetens verksamheter.[45]

[45] Prop. 2020/21:224 s. 68.

Vi anser att det bör vara tillräckligt att ange att det är genom lag, förordning, särskilt beslut av regeringen eller för Sverige bindande internationella åtaganden som Säkerhetspolisens nationella säkerhetsuppdrag definieras och att det är inom detta uppdrag som personuppgifter får behandlas. Det innebär att bland annat att polislagens uppräkning av Säkerhetspolisens uppgifter inte behöver återupprepas i personuppgiftslagstiftningen.

En sådan lagstiftning är enklare att anpassa till nya uppdrag och mål för myndigheten och det riskerar inte att bli otydligt vilken rättsakt som har företräde när det kommer till att beskriva uppdraget. Alternativet är att som i dag räkna upp några av de mest centrala uppgifterna för Säkerhetspolisen. Vi kan dock inte se att en sådan ordning har några uppenbara fördelar.

Däremot anser vi att det kan finnas behov av att det i lagen ska framgå inom vilka övergripande verksamhetsområden personuppgiftsbehandlingen får ske. Som rättslig grund anser vi däremot att det är tillräckligt att ange att Säkerhetspolisen endast får behandla personuppgifter då myndigheten bedriver verksamhet som rör nationell säkerhet som följer av lag, förordning, internationella åtaganden eller särskilt beslut av regeringen. Vi föreslår därför att bestämmelserna om rättslig grund får denna utformning i den nya lagen.

8.4 Verksamheter för behandling av personuppgifter

8.4.1 Dataskyddskonventionens bestämmelser

Av dataskyddskonventionen 108+ framgår att personuppgifter måste behandlas transparent.

> **Article 5 – Legitimacy of data processing and quality of data**
>
> 4. a Personal data undergoing processing shall be processed fairly and in a transparent manner;

Kravet om en korrekt och transparent behandling utgör en förutsättning för att behandling av personuppgifter ska vara förenliga med dataskyddskonventionen 108+. Bestämmelsen om transparens innebär bland annat att personuppgifter inte ska behandlas på ett sätt som kan uppfattas som oväntat. I artikel 8 följer även att den personuppgiftsansvarige bland annat ska ange de ändamål för vilka personuppgifter kan behandlas.

8.4.2 Måste det framgå för vilka ändamål personuppgifter får behandlas?

Bedömning: Den nuvarande lagens uppräkningen av rättsliga grunder bör ersättas med ett annat sätt att tydliggöra inom vilka ramar lagen medger behandling av personuppgifter.

Syftet med de rättsliga grunder som nuvarande lag innehåller är att ge medborgare en beskrivning av den yttre ram inom vilken personuppgifter får behandlas med stöd av lagen. Hur dessa bestämmelser formuleras kan dock även ha betydelse för den myndighet som regleringen avser. Lagstiftningen kan på detta sätt avgränsa vilka ändamål som får bestämmas med stöd av en rättslig grund. Behovet av att i lag beskriva inom vilka ramar ett ändamål för personuppgiftsbehandling kan bestämmas får sägas bero på vilken myndighet det handlar om och vilka personuppgifter som myndigheten kommer att behandla. Om en myndighets verksamhet är väl reglerad kan det räcka att det framgår att myndigheten får behandla personuppgifter om det är nödvändigt för att myndigheten ska kunna utföra sina uppgifter.

Vi har bedömt att Säkerhetspolisen uppgifter i och för sig är tillräckligt välavgränsade i de olika rättsakter som är styrande för myndighetens verksamhet. Det är därför inte nödvändigt att, som i dag, exemplifiera vissa av dessa rättsliga grunder och inte heller lämpligt att uttömmande räkna upp dem för att sammanfatta myndighetens uppdrag.

Säkerhetspolisens verksamhet rör dock i stor utsträckning personuppgiftsbehandling som är känslig ur integritetssynpunkt och som kan utgöra en sådan kartläggning av enskilda som avses i 2 kap. 6 § andra stycket regeringsformen. Under dessa förhållanden ställs högre krav på förutsebarhet och i lag uttryckta ändamål för intrånget i den skyddade rättigheten. Även om vi inte uppfattar att det finns ett behov av att ange rättsliga grunder i detalj bör det övervägas om det i lagen ska anges övergripande ändamål för behandling.

I dataskyddsammanhang har begreppet ändamål olika betydelse beroende på i vilket sammanhang det förekommer. En brett formulerad ändamålsbestämmelse pekar ut ramarna för den personuppgiftsbehandling som en författning reglerar. Ändamålen utgör där en slags sammanfattande beskrivning av den rättsliga grunden och där-

med de särskilda ändamål som kan komma att aktualiseras inom författningens materiella tillämpningsområde. Breda ändamålsbestämmelser tydliggör därmed de syften där personuppgiftsbehandling som kan komma i fråga för en viss myndighet.[46]

Vi anser att det finns goda skäl för att det alltjämt ska framgå inom vilka, brett formulerade, ändamål eller särskilt angivna rättsliga grunder som det närmare, mer specifika ändamålet för behandling av personuppgifter får ske.

8.4.3 De verksamheter inom vilka personuppgifter får behandlas bör anges i lagen

Förslag: Av lagen ska framgå inom vilka verksamheter Säkerhetspolisen får behandla personuppgifter.

Syftet med övergripande ändamålsbestämmelser eller att särskilt ange vissa rättsliga grunder i personuppgiftslagstiftning är alltså att förtydliga inom vilka verksamheter som personuppgifter får behandlas med stöd av lagen.

En sådan uppräkning syftar därmed inte till att ersätta kravet på en rättslig grund. De rättsliga grunderna för personuppgiftsbehandling ska anges i en annan rättsakt än personuppgiftlagen och behöver inte upprepas om de inte avser att begränsa lagens tillämpningsområde (se avsnitt 8.3.3).

Uppräkningen ska inte heller utgöra ett särskilt, uttryckligt angivet och berättigat ändamål. Sådana mer precisa ändamål ska som regel bestämmas av den personuppgiftsansvarige och inte av lagstiftaren. Kravet på konkretion är sådant att det sällan lämpar sig att ange i lag, i vart fall inte för den verksamhet som Säkerhetspolisen bedriver. Då säpodatalagen beslutades konstaterade regeringen också att rättsliga grunder för behandling och ändamålsbestämmelser ibland har blandats samman.[47]

Vi anser att det är viktigt att det varken framstår som att lagen begränsar vilka rättsliga grunder som personuppgifter får behandlas för eller blandas samman med de särskilda ändamålsbestämmelserna. För att undvika att uppräkningen sammanblandas med begreppet

[46] Se även SOU 2023:100 s. 509–512.
[47] Jfr prop. 2018/19:163 s. 62 f.

rättslig grund, som har en självständig betydelse eller ett särskilt ändamål, som ska bestämmas och preciseras av tillämparen, bör ett annat begrepp användas.

Vi anser att det bör anges inom vilka *verksamheter* som personuppgifter får behandlas. Det är det som är själva syftet med uppräkningen; medborgare ska kunna bilda sig en uppfattning om inom vilka verksamheter som behandling av personuppgifter kommer att kunna ske. De särskilda ändamålen ska bestämmas av den personuppgiftsansvarige. De uppräknade verksamheterna syftar till att förtydliga inom vilka ramar dessa ändamål får bestämmas. Verksamheterna måste därför vara tillräckligt brett angivna för att inrymma de ändamål som behövs för att myndigheten ska kunna utföra sitt uppdrag.

I försvarsdatalagen anges bland annat att personuppgifter får behandlas för att planera, förbereda och genomföra verksamhet som rör Sveriges försvar och säkerhet, i försvarsunderrättelseverksamhet och i Försvarsmaktens militära säkerhetstjänst. Denna uppräkning ger en bild av vad som är Försvarsmaktens kärnverksamhet och inom vilka delar av denna verksamhet som det är nödvändigt att behandla personuppgifter. En liknande uppräkning kan vara lämplig för Säkerhetspolisens del.

När det kommer till vilka verksamheter som ska anges i lagstiftningen anser vi att det är särskilt viktigt att Säkerhetspolisens uppdrag som nationell säkerhetstjänst framgår. I denna egenskap bedriver myndigheten underrättelse- och säkerhetsverksamhet. Vidare bör det framgå att Säkerhetspolisen är en polismyndighet som bedriver brottsutredande verksamhet. Behandling av personuppgifter för brottsbekämpning anser vi vara så känslig att dessa verksamheter bör framgå direkt av personuppgiftslagstiftningen.

Med hänsyn till att det tydliggörs att personuppgifter får behandlas för uttryckliga brottsbekämpande ändamål måste det av lagen även framgå att behandling även medges för uppdrag enligt rättsliga grunder där det brottsbekämpande inslaget inte är lika tydligt. Det bör därför även framgå att Säkerhetspolisen får behandla personuppgifter enligt andra ändamål som rör nationell säkerhet. Dessa områden utvecklas i det följande.

8.4.4 Säkerhetspolisens verksamhet som nationell säkerhetstjänst bör förtydligas

Förslag: Säkerhetspolisens personuppgiftsbehandling i säkerhets- och underrättelseverksamheten ska förtydligas. Av lagen ska framgå att Säkerhetspolisen i sin uppgift att förebygga, förhindra och upptäcka brottslig verksamhet får behandla personuppgifter för att kartlägga och klarlägga brottslig verksamhet, eller för att vidta åtgärder som hindrar eller försvårar brottslig verksamhet.

Den rättsliga regleringen av Säkerhetspolisens brottsförebyggande uppdrag

Av polislagen följer som nämnts att Säkerhetspolisen bland annat ska förebygga, förhindra och upptäcka brottslig verksamhet som innefattar brott mot rikets säkerhet eller terrorbrott. I myndighetens instruktion preciseras uppdraget i denna del. Enligt 1 § ska Säkerhetspolisen, i egenskap av säkerhetstjänst, bedriva underrättelse- och säkerhetsarbete.

En säkerhetstjänst arbetar för att höja säkerhetsnivån i det egna landet. Detta görs dels genom att avslöja och reducera säkerhetshot som riktas mot landet och dess skyddsvärda verksamheter, dels genom att reducera sårbarheter i dessa verksamheter. Säkerhetspolisens arbete är alltså främst inriktat mot att identifiera brottslig verksamhet som ännu inte konkretiserats till straffbara gärningar. När Säkerhetspolisen identifierar brottslig verksamhet i ett så tidigt skede kan brottsligheten normalt avvärjas. Säkerhetspolisen behöver därmed kunna behandla personuppgifter på ett tidigt stadium, innan en person eller en gruppering har konkreta brottsplaner eller har vidtagit åtgärder för att begå brott, se avsnitt 3.3.

Denna del av Säkerhetspolisens kärnverksamhet är lagtekniskt reglerad på samma sätt som det brottsförebyggande arbete som bedrivs hos andra brottsbekämpande myndigheter, genom uppdraget att förebygga, förhindra och upptäcka brottslig verksamhet, se avsnitt 3.3.2. Detta trots att Säkerhetspolisens uppdrag i denna del får betraktas som mycket särpräglat i förhållande till exempelvis Polismyndighetens eller Tullverkets uppdrag. Det gäller både avseende

de befogenheter som finns tillgängliga för respektive myndighet och det samhällsintresse som verksamheten avser att skydda.

Det har funnits en ovilja att lagtekniskt särskilja Säkerhetspolisens brottsförebyggande arbete i förhållande till övriga brottsbekämpande myndigheters. I propositionen till polisdatalagen angavs att Säkerhetspolisen behöver kunna samla in, sammanställa och analysera uppgifter inom kontraspionageverksamheten, kontraterrorismverksamheten och författningsskyddsverksamheten även om uppgifterna inte kan hänföras vare sig till något visst konkret brott eller till någon mer konkret definierad brottslig verksamhet. Som exempel nämndes behovet av att inom kontraspionaget fortlöpande följa utvecklingen när det gäller andra nationers närvaro i form av underrättelseagenter här i landet, att kunna övervaka sådana personer och även behandla personuppgifter. Regeringen ansåg även att Säkerhetspolisen behöver följa den politiska utvecklingen i andra länder och verksamheten inom vissa grupper, som kan utgöra ett hot mot det svenska samhället eller som kan komma att göra sig skyldiga till terroristbrott. Regeringen konstaterade att Säkerhetspolisens behov av att kunna genomföra och dokumentera olika typer av undersökningar och analyser är stort och att det i flera avseenden skiljer sig från de behov som finns inom den övriga polisen. Säkerhetspolisens brottsförebyggande arbete ansågs särpräglat på så sätt att det normalt inte går att urskilja lika tydliga kopplingar till konkreta brott eller till brottslig verksamhet. Den underrättelseverksamhet som bedrivs inom Säkerhetspolisen är till sin natur ofta sådan att den ligger på ett tidigare stadium. Å andra sidan är den, genom Säkerhetspolisens instruktion, inriktad mot ett fåtal, väl avgränsade företeelser av särskilt samhällsfarlig karaktär. Trots denna skillnad ansåg regeringen att den brottförebyggande ändamålsbestämmelsen skulle utformas på samma sätt som motsvarande bestämmelse för polisen, med den skillnaden att Säkerhetspolisens brottskatalog skulle anges.[48] Då säpodatalagen beslutades ansåg regeringen att det inte fanns skäl att ändra bestämmelsen om rättslig grund (som motsvarade polisdatalagens tidigare bestämmelse om brottsförebyggande ändamål).[49]

[48] Prop. 2009/10:85 s. 256.
[49] Prop. 2018/19:163 s. 65.

Säkerhetspolisens förändrade uppdrag

Sedan de uttalanden som gjordes i samband med polisdatalagen, och som ligger till grund även för den nuvarande säpodatalagen, har stora förändringar skett i Säkerhetspolisens verksamhet. Den största förändringen är givetvis att Säkerhetspolisen sedan den 1 januari år 2015 är en egen myndighet. Även omvärlden och hotbilden har förändrats och Säkerhetspolisens organisation med den. Säkerhetspolisens uppdrag består i dag till mycket stor del av underrättelseverksamhet riktad mot hotaktörer med internationella kopplingar. Samverkan med andra länders underrättelsetjänster och med de nationella försvarsunderrättelsemyndigheterna har utvecklats. Säkerhetspolisens allt tydligare roll som säkerhetstjänst innebär att underrättelseverksamheten inte bär lika stora likheter med den kriminalunderrättelseverksamheten som tidigare kanske var fallet.

Säkerhetspolisens verksamhet har, på ett annat sätt än de andra brottsbekämpande myndigheternas verksamhet, också en tydlig koppling till svensk säkerhetspolitik. Annorlunda uttryckt är säkerhetstjänsten ett av många instrument för att säkerhetspolitiken i vid mening ska fungera. Vid en snabb eskalering av säkerhetshotet mot Sverige skulle Säkerhetspolisens inhämtning utgöra en viktig pusselbit i förståelsen av hotet och vara av betydelse för både regeringen och Försvarsmakten i deras beslutsfattande.

Säkerhetspolisen är Sveriges nationella säkerhetstjänst med ett brottsbekämpande uppdrag. Av olika skäl har uppdraget lagtekniskt reglerats med fokus på polisär brottsbekämpning snarare än på att förebygga säkerhetshot i bredare mening, som utmärker en säkerhetstjänst. Det har fått till följd att Säkerhetspolisens personuppgiftslagstiftning även fått stora likheter med andra brottsbekämpande myndigheters. Vi anser dock att Säkerhetspolisens uppdrag som nationell säkerhetstjänst bär vissa, och i många avseende större, likheter med det liknande uppdrag som anförtrotts Försvarsmaktens militära underrättelse- och säkerhetstjänst. Detta bör komma till uttryck i lag.

Försvarsmaktens verksamhet som avser säkerhetstjänst regleras i försvarsdatalagen. Där anges, i 2 kap. 5 §, som övergripande ändamål, att personuppgifter får behandlas i Försvarsmaktens militära säkerhetstjänst för att upptäcka, förebygga och avvärja säkerhetshotande verksamhet som riktas mot Försvarsmakten och dess säker-

hetsintressen, om det är nödvändigt för att 1. *klarlägga* verksamhet som innefattar hot mot Sveriges säkerhet, eller 2. vidta åtgärder som *hindrar eller försvårar* säkerhetshotande verksamhet.

För detta övergripande ändamål får personuppgifter behandlas om det är nödvändigt för vissa, i 2 kap. 6 § uppräknade, mer specifika ändamål. Bland annat om det är nödvändiga för att *kartlägga* verksamhet som innefattar brott som kan hota Sveriges säkerhet eller terroristbrott, för att kartlägga underrättelseverksamhet riktad mot Försvarsmakten och dess säkerhetsintressen eller för att kartlägga annan säkerhetshotande verksamhet som innefattar brott eller åsidosättande av skyldigheter i anställning hos Försvarsmakten.

Underrättelse- och säkerhetsarbete som verksamhet för behandling av personuppgifter

Det pågår löpande ett integrerat samarbete mellan Säkerhetspolisen och den militära underrättelse- och säkerhetstjänsten. Myndigheternas uppdrag är i vissa delar närliggande och i andra delar överlappande. Samarbetet mellan Säkerhetspolisen och den militära underrättelse- och säkerhetstjänsten är i vissa avseenden långtgående och inom underrättelseverksamheten finns en tydlig koppling. I denna verksamhet, som får betecknas som Säkerhetspolisens kärnverksamhet, är kopplingen tydligare med den militära underrättelse- och säkerhetstjänsten än mellan Säkerhetspolisen och Polismyndigheten. I Säkerhetspolisens uppdrag att förebygga, förhindra eller upptäcka brottslig verksamhet inryms även flera av de begrepp som uttryckligen angetts i lag för den militära underrättelse- och säkerhetstjänsten. I Säkerhetspolisens uppdrag ingår bland annat att klarlägga brottslig verksamhet och att kartlägga främmande makts underrättelseverksamhet. Av uppdraget följer även att Säkerhetspolisen ska vidta åtgärder för att hindra eller försvåra säkerhetshotande verksamhet inom Säkerhetspolisens ansvarsområde, bland annat avseende terrorism och spionage.

Både den militära och den civila underrättelse- och säkerhetstjänstens verksamhet förutsätter att personuppgifter kan delas och behandlas på ett likartat sätt i de områden där säkerhetshotet har både utländska och inhemska dimensioner. Ett exempel är gränsöverskridande terrorism, ett annat är utländsk underrättelseverksamhet som är inriktad både mot Försvarsmakten och dess säkerhetsintressen

och mot delar av civilsamhället. Vi anser därför att det finns goda skäl för att i större utsträckning än förut harmonisera lagstiftningen för den civila och militära säkerhetstjänsten avseende ändamålet som beskriver underrättelseverksamheten.

Kartlägga och klarlägga brottslig verksamhet

Säkerhetspolisens uppdrag att som säkerhetstjänst bedriva underrättelseverksamhet förutsätter att myndigheten har förmåga att kartlägga vissa typer av brottslig verksamhet. Av Säkerhetspolisens operativa resurser är en överväldigande majoritet inriktad på underrättelsearbete inom de olika verksamhetsgrenarna. Det är naturligt att det vid en kartläggning av brottslig verksamhet behöver behandlas en stor mängd personuppgifter. Det är i själva verket det som är utmärkande i den inledande fasen av underrättelseverksamhet, där enskilda aktörers koppling till brott eller ens till brottslig verksamhet ännu inte kunnat fastställas. Att i lagen särskilt ange att det i Säkerhetspolisen brottsbekämpande uppdrag ingår att kartlägga brottslig verksamhet som innefattar brott mot rikets säkerhet eller terrorbrott utgör därför ett förtydligande av det nuvarande uppdraget. I likhet med vad som gäller för den militära underrättelse- och säkerhetstjänsten bör det även framgå att syftet med underrättelseverksamheten är att klarlägga olika förhållanden. Detta kan ses som det nästa naturliga steget i underrättelsearbetet.

Genom begreppet kartlägga i ändamålsbestämmelsen framgår att personuppgifter kan behöva behandlas för att ge en helhetsbild. Det innebär att det kan behövas uppgifter om personer som i behandlingsögonblicket inte kan misstänkas för brottslig verksamhet men som ingår i en vidare krets kring misstänkta personer. Även uppgifter om andra personer som förekommer i en kontext som är nödvändig att kartlägga måste kunna behandlas för att ge en tillräcklig förståelse för företeelsen. Ett exempel kan vara att Säkerhetspolisen kartlägger en utländsk underrättelseofficers förehavanden här i landet. Det ligger i sakens natur att alla kontakter denna har med personer här i landet kan vara relevanta för att kartlägga brottslig verksamhet. Sett till underrättelseofficerens uppdrag här i landet går det att anta värvningsförsök eller kontakter med redan etablerade agenter kommer att ske. En kartläggning av dennes brottsliga verksamhet

kan röra sig om uppgifter om vilka bilar som parkerat på samma eller angränsande våningsplan i ett parkeringsgarage. Utan denna information är det inte möjligt att veta om bilar knutna till en viss person återkommande parkerar i närheten av underrättelseofficeren och att denne därmed kan misstänkas för att exempelvis dela känsliga uppgifter till främmande makt.

Denna typ av intensiv underrättelseverksamhet är i princip förbehållet säkerhetstjänsterna. Att beskriva underrättelseverksamheten på ett liknande sätt för Säkerhetspolisen som för den militära underrättelse- och säkerhetstjänsten markerar en skillnad mellan denna typ av kvalificerat underrättelsearbete i förhållande till andra brottsbekämpande myndigheter. Detta har tidigare uttryckts i lagförarbeten utan att närmare klargöras i lagtexten.[50]

Kartläggning är även ett begrepp som tidigare använts för att beskriva underrättelseverksamhet och som därför lämpar sig bra att återinföra i den nya lagstiftningen. Kartläggning av enskildas personliga förhållanden används också i 2 kap. 6 § regeringsformen där det anges att var och en gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Genom att uttryckligen hänvisa till begreppet kartläggning står det klart att lagen avser att utgöra en tillåten begränsning av denna rättighet enligt regeringsformen 2 kap. 20–21 §§, i syfte att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle.

Begreppet klarlägga har en delvis annan innebörd som medger att personuppgifter kan behandlas för att gå vidare med inledningsvis mycket svaga misstankar mot en person eller företeelse. I exemplet ovan skulle det kunna vara att utreda vem som står bakom de hyrbilar som återkommande återfinns i det parkeringsgaraget där Säkerhetspolisen misstänker att underrättelseofficeren träffar en svensk kontaktperson. På så vis kan misstankar som inledningsvis väckts på grund av slump avfärdas, men andra kan vara uppslag till ett ärende om misstänkt spionage. Begreppet klarlägga användes även i definition av underrättelseverksamhet i den äldre polisdatalagen. Där angavs att underrättelseverksamhet är ”polisverksamhet som består i att samla, bearbeta och analysera information för att klarlägga om brottslig verksamhet har utövats eller kan komma att

[50] Prop. 2018/19:163 s. 68.

utövas och som inte utgör förundersökning enligt 23 kap. rättegångsbalken” (se även avsnitt 3.3.2). I en underrättelsekontext får begreppet ”klarlägga” anses vara kvalificerat i förhållande till att ”kartlägga”. Klarläggning av förhållanden är så att säga målet med kartläggningen och markerar att underrättelsearbetet riktas in mot mer specifika omständigheter än vad som är fallet med en bredare kartläggning.

Hindra eller försvåra brottslig verksamhet

I Sverige är Säkerhetspolisen inte en civil underrättelsetjänst med ett uppdrag begränsat till att kartlägga olika förhållanden. Underrättelseverksamheten inom myndigheten bedrivs för att Säkerhetspolisen ska kunna utföra uppgifter som nationell säkerhetstjänst. Säkerhetspolisen har därmed inget självständigt intresse att samla information om brottslig verksamhet. Syftet med underrättelseverksamheten är att förebygga och förhindra brottslig verksamhet som innefattar brott mot rikets säkerhet eller terrorbrott. Detta uppdrag förutsätter att brottslig verksamhet först identifierats. Därefter följer åtgärder av olika slag för att förebygga hot eller, i förekommande fall förhindra brottslig verksamhet. Dessa åtgärder är det sista ledet i den brottsförebyggande verksamheten och resultatet av ett framgångsrikt underrättelsearbete. Det är dock sällan dessa åtgärder resulterar i en lagföring.

Säkerhetspolisens verksamhet som syftar till att upptäcka och reducera hot bedrivs framför allt inom verksamhetsområdena kontraspionage, kontraterrorism och författningsskydd. Reduktion av ett hot kan ske på många olika sätt där frihetsberövande och lagföring inom ramen för en förundersökning är ett sätt. Andra sätt som står till myndighetens förfogande är att initiera en utvisning av en utlänning som bedöms utgöra ett säkerhetshot eller att påtala för regeringen att underrättelseofficerare som arbetar under diplomatisk täckmantel bör förklaras *persona non grata*. Säkerhetspolisen arbetar även proaktivt för att minska extremistmiljöerna i Sverige. Så sker till exempel genom så kallad outreach-verksamhet och yttranden till andra myndigheter inom ramen för bl.a. utlänningslagstiftningen och de olika regelverken om statsstöd. Säkerhetspolisens verksamhet som syftar till att upptäcka och reducera sårbarheter bedrivs

i stället framför allt inom verksamhetsområdena säkerhetsskydd och personskydd.

Det bör i den nya lagen uttryckligen anges att denna del av verksamheten utgör ett ändamål för personuppgiftsbehandling. Säkerhetspolisens personuppgiftslag bör därför precisera det brottsförebyggande uppdraget genom att personuppgifter som behövs för att vidta åtgärder som hindrar eller försvårar sådan brottslig verksamhet omfattas. Även åtgärder för att hindra eller försvåra brottslig verksamhet är utmärkande för det kvalificerade uppdraget som nationell säkerhetstjänst och motsvarar inte andra brottsbekämpande myndigheters brottsförebyggande verksamhet. Detta bör komma till uttryck i lagtexten som ett förtydligande av det nuvarande uppdraget. Någon betydelseförskjutning avseende Säkerhetspolisens uppdrag är inte avsedd.

8.4.5 Brottsutredning som verksamhet för personuppgiftsbehandling

Förslag: Av lagen ska framgå att Säkerhetspolisen får behandla personuppgifter i sin brottsutredande och lagförande verksamhet.

Det brottsutredande uppdraget ska framgå

Av polislagen framgår att Säkerhetspolisen i likhet med Polismyndigheten bedriver polisverksamhet och att myndigheten har ett brottsutredande och lagförande uppdrag. Det innebär bland annat att Säkerhetspolisen inom sitt ansvarsområde får bedriva förundersökning och inom ramen för denna använda straffprocessuella tvångsmedel. Säkerhetspolisen bedriver alltså förutom säkerhets- och underrättelsearbete även brottsutredande verksamhet. På så sätt skiljer sig myndighetens uppgifter i en internationell jämförelse från många andra säkerhetstjänsters uppgifter. Att Säkerhetspolisen är polismyndighet med uppgift att utreda brott och kan behandla personuppgifter för detta ändamål bör framgå av lagstiftningen.

Personuppgifter som rör brott, straffrättsliga förfaranden, fällande domar och andra relaterade säkerhetsåtgärder anses i dataskyddskonventionen 108+ vara känsliga personuppgifter. För en brottsbekäm-

pande myndighet är det självklart att sådana personuppgifter måste kunna behandlas, då det utgör själva grunden för myndighetens verksamhet. Skälet till att det är angeläget att det framgår av lagstiftningen att uppgifter som myndigheten behandlar får användas för brottsutredande och lagförande ändamål är huvudsakligen för att allmänheten ska kunna förutse konsekvenserna av Säkerhetspolisens personuppgiftsbehandling. Vi anser att den nuvarande bestämmelsen, om den rättsliga grunden brottsutredning och lagföring bör överföras till den nya lagen. Som framgår nedan finns det dock skäl att justera lydelsen.

Brottskatalogen bör inte anges

Den nuvarande säpodatalagen anger vilka kategorier av brott som Säkerhetspolisen ansvarar för. Som framgått i avsnitt 8.3.3, anser vi att det inte är nödvändigt att upprepa de brott som Säkerhetspolisen ansvarar för som rättslig grund i den generella personuppgiftslagstiftningen. Av samma skäl anser vi inte att det är nödvändigt att ange vilka brott som ingår i den brottsutredande verksamheten. Det framstår som mer lämpligt att brottskatalogen anges i de rättsakter som primärt reglerar Säkerhetspolisens uppdrag: i huvudsak polislagen och Säkerhetspolisens instruktion. Det innebär givetvis inte någon utvidgning av Säkerhetspolisens uppdrag i denna del. Säkerhetspolisen ska även fortsättningsvis endast utreda de brott som följer av det uppdrag som getts myndigheten genom lag eller förordning. Däremot medför det att lagen blir mer neutral i sin utformning och möjliggör att uppdraget förändras utan onödiga följdändringar i personuppgiftslagstiftningen. Vår uppfattning är att den rättsliga grunden är tillräcklig för att avgränsa vilka brottsbekämpande ändamål som får bestämmas inom denna verksamhet.

Det tål att upprepas att säpodatalagens tillämpningsområde är begränsat till brottsbekämpning som rör nationell säkerhet. Sverige har ett stort utrymme att avgöra vilken brottslighet som utgör hot mot nationell säkerhet genom att den hotar statens grundfunktioner och samhällets grundläggande intressen. Trots detta är det endast EU-domstolen som i slutändan kan avgöra var gränsen för brottsbekämpning som rör nationell säkerhet går och därmed begränsa säpodatalagens tillämpningsområde. Även av denna anledning är

det lämpligt att inte närmare ange vilken brottslig verksamhet som lagen avser.

8.4.6 Övrig brottsbekämpande verksamhet som rör nationell säkerhet

Förslag: Av lagen ska framgå att personuppgifter får behandlas för andra ändamål inom lagens tillämpningsområde om det finns stöd för behandling i en rättslig grund.

Därutöver ska förtydligas att behandling av personuppgifter får ske för utveckling av teknik och metodik inom lagens tillämpningsområde.

Andra uppgifter med stöd av rättslig grund

Vid sidan av sitt brottsförebyggande och brottsutredande uppdrag har Säkerhetspolisen även andra uppgifter, som följer av lag, förordning eller särskilt beslut av regeringen. Av polislagen anges särskilt att Säkerhetspolisen ansvarar för personskyddet av den centrala statsledningen, av säkerhetsskyddslagen följer andra uppgifter, liksom av utlännings- och medborgarskapslagstiftningen. Alla dessa uppgifter anges uttryckligen som rättslig grund i den nuvarande lagstiftningen. Därutöver anges i säpodatalagen att personuppgifter får behandlas om det är nödvändigt för att fullgöra någon annan uppgift som rör nationell säkerhet, om det finns en rättslig grund för behandlingen. Vi anser att en uppräkning av vissa ytterligare uppgifter, vid sidan av de uttryckligt brottsbekämpande, inte fyller någon tydlig funktion. Särskilt inte om uppräkningen inte är uttömmande utan att det därutöver tillkommer en rad uppgifter som följer av andra, icke utpekade, författningar (se avsnitt 8.3.3).

Därför anser vi att de uttryckligt brottsbekämpande verksamheterna i lagen endast bör kompletteras på så sätt att det anges att det ändamålet för personuppgiftsbehandling även kan bestämmas i en annan verksamhet som följer av någon rättslig grund.

Teknikutveckling

Säkerhetspolisen har ett stort och växande behov av att utveckla, testa och utvärdera olika it-system och tekniska förmågor för informationshantering. Det inkluderar framtagande av AI-modeller, för att förbättra den tekniska förmågan. Vi har konstaterat att it-utveckling som sker i syfte att öka myndighetens förmåga att bearbeta och analysera personuppgifter inom den brottsbekämpande verksamheten inte kräver särskilt lagstöd utan sker med stöd av det övergripande uppdraget. Vi anser även att teknisk utveckling är sådan verksamhet som faller inom lagens tillämpningsområde (se avsnitt 8.1.2 ovan).

I de fall som test- och utvecklingsverksamhet sker med personuppgifter som Säkerhetspolisen redan behandlar med stöd av säpodatalagen utgör finalitetsprincipen i dag den yttersta ramen för vilken behandling som är tillåten. Personuppgiftsbehandling för att utveckla it-system är i normalfallet förenligt med det ändamål uppgifterna ursprungligen behandlades för, eller i vart fall inte oförenligt. Behandling av personuppgifter för teständamål, är också något som normalt inte brukar regleras i särskilda registerförfattningar. Det följer av att myndigheter generellt har en skyldighet att ha säkra tekniska lösningar för att kunna utföra de uppgifter som åligger dem. Regeringen har uttalat att det numera är en huvudprincip att testverksamhet inte behöver regleras som ett särskilt ändamål.[51]

FRA har i 2 kap. 5 § FRA-datalagen en ändamålsbestämmelse som medger att personuppgifter behandlas för utvecklingsändamål, om det är nödvändigt för försvarsunderrättelseverksamheten. Paragrafen innebär att FRA får behandla personuppgifter för att följa förändringar i signalmiljön, den tekniska utvecklingen och signalskyddet samt för fortlöpande utveckla den teknik och metodik som behövs för att bedriva signalspaning.

FRA:s särskilda bestämmelse för personuppgiftsbehandling för teknisk utveckling utgör därmed ett undantag från huvudregeln. Skälet är att det även finns en möjlighet för FRA att bedriva signalspaning för samma ändamål och därmed inhämta mycket stora mängder information och personuppgifter för att utveckla teknik och metodik. När nya metoder för forcering av krypterad information arbetas fram används exempelvis autentiskt signalspaningsmaterial.

[51] Prop. 2019/20:113 s. 20.

I målet Centrum för Rättsvisa mot Sverige uttalade sig Europadomstolen om FRA:s utvecklingsverksamhet. Domstolen framhöll uppgifter inom denna verksamhet inte intresserar myndigheterna på grund av de uppgifter de kan innehålla, utan endast på grund av den möjlighet de ger att analysera de tekniska systemen. Domstolen konstaterade att den grad av intrång i enskildas rättigheter enligt artikel 8 som sådan verksamhet medför ”förefaller vara av mycket låg intensitet med hänsyn till att de uppgifter som erhålls inte är avsedda att generera underrättelser”.[52]

Den nuvarande säpodatalagen medger att myndigheten i viss utsträckning kan använda bedömd information, som uppfyller kvalitetskraven i nuvarande 2 kap. 7–9 §§ säpodatalagen, som test- och träningsdata för att utveckla eller utvärdera AI-modeller. För att kunna utveckla, testa och utvärdera nya tekniska förmågor på ett ändamålsenligt sätt krävs emellertid behandling av stora, autentiska datamängder av olika uppgiftsslag.

Det finns i dag inte någon möjlighet för Säkerhetspolisen att samla in uppgifter för teknikutveckling. Det finns en god tillgång till autentiskt material, exempelvis olika slags överskottsinformation som hade kunnat användas som träningsdata eller på annat sätt inom utvecklingsverksamheten. Dagens regler innebär dock att uppgifterna måste granskas och uppfylla säpodatalagens krav innan de potentiellt skulle kunna användas för utvecklingsändamål. Eftersom detta är en väldigt tidskrävande process, kan bara begränsade delar av hela materialet hanteras enligt dessa krav. Verktyg som nyttjar moderna tekniker kräver ofta stora datamängder att utveckla, något som inte är möjligt att åstadkomma med nuvarande lagstiftning.

Det förutsätts att Säkerhetspolisen ska kunna möta dagens och framtidens hot genom en god teknisk förmåga; en förmåga som delvis måste utvecklas inom myndigheten (se avsnitt 6.2.6). Att Säkerhetspolisen inhämtar och behandlar personuppgifter i detta syfte måste dock ske transparent och inom lagens ram. Vi anser att det därför finns skäl att uttryckligen reglera teknisk utveckling som en verksamhet för vilket Säkerhetspolisen får behandla personuppgifter.

Genom att denna verksamhet tydliggörs i lagstiftningen framgår det att enskildas personuppgifter kan komma att behandlas inom myndigheten trots att det inte omedelbart sker för ett brottsbekämpande ändamål. Så kan vara fallet då exempelvis texter av olika slag

[52] Se Europadomstolens dom, *Centrum för Rättvisa mot Sverige*, p. 292.

används för att utvärdera eller vidareutveckla översättningstjänster eller att bildmaterial används för att träna mjukvara som kan identifiera vapen. Behandling för sådana utvecklingsändamål innebär normalt inte övervakning eller kartläggning av den enskildes personliga förhållanden. Det kan emellertid inte uteslutas att det i vissa fall kan behöva ske en kartläggning i utvärdering- och utvecklingssyfte.

Utvecklingsändamålen i lagen bör medge att uppgifter som ursprungligen inhämtats för ett operativt ändamål även behandlas för att utveckla tekniska system, men också att Säkerhetspolisen kan samla in uppgifter enbart för utvecklingsändamål.

Det är viktigt att de uppgifter som behandlas endast för utvecklingsändamål regleras särskilt avseende vilken vidarebehandling som är tillåten och avseende behandlingstid. Det bör inte vara tillåtet att behandla sådana uppgifter för något annat ändamål och heller under någon längre tid. Vi återkommer därför till dessa frågor.

8.5 Författningsenlig och korrekt behandling

8.5.1 Dataskyddskonventionens bestämmelse

Av dataskyddskonventionen 108+ framgår kravet på författningsenligt, transparent och korrekt personuppgiftsbehandling:

> **Article 5 – Legitimacy of data processing and quality of data**
>
> 3. Personal data undergoing processing shall be processed lawfully.
>
> 4. a Personal data undergoing processing shall be processed fairly and in a transparent manner.

Bestämmelsen om författningsenlighet, i artikel 5.3, utgör ett av de absoluta krav, där särskilda undantag, enligt artikel 11, inte är möjliga, oavsett syfte. Enskilda har även en rätt att kräva radering av personuppgifter som inte behandlats författningsenligt. Kravet i punkten 4 a omfattas däremot av möjligheterna till undantag.

I dataskyddskonventionen regleras dessa krav, på att personuppgifter ska behandlas författningsenligt, korrekt och öppet, i ett sammanhang (artikel 5.1 a).

8.5.2 Den nuvarande regleringen

Bestämmelser som motsvarar konventionens krav finns i nuvarande 2 kap. 6 § säpodatalagen. Där anges att personuppgifter ska behandlas författningsenligt och på ett korrekt sätt. Att personuppgifter ska behandlas författningsenligt innebär att det ska finnas en rättslig grund för behandlingen. Att personuppgifter ska behandlas korrekt innefattar att behandlingen inte bara formellt ska vara i enlighet med regleringen utan också spegla intentionerna med lagstiftningen.[53]

8.5.3 Den nuvarande bestämmelsen bör överföras

Förslag: Av lagen ska framgå att personuppgifter ska behandlas författningsenligt och på ett korrekt sätt.

Det finns inte några skäl att ändra på den nuvarande bestämmelsen som kräver att personuppgifter ska behandlas författningsenligt och på ett korrekt sätt, vilket får anses vara av upplysningskaraktär. Att en myndighet ska agera i enlighet med lag och att handläggningen ska ske på ett korrekt sätt framstår som en djupt förankrad självklarhet i den svenska förvaltningstraditionen.

I tidigare lagstiftningsärenden har begreppet *korrekt* ansetts motsvara det engelska begreppet *fairly*, även om det engelska ordet ansetts snarast böra översättas till rättvist, skäligt eller rimligt.[54] Begreppet *fairly* i dataskyddskonventionen bör ha samma betydelse som begreppet i de EU-rättsliga dataskyddet. I de svenska språkversionerna av dataskyddsförordningen och brottsdatadirektivet används begreppet korrekt. Även om det skulle vara önskvärt att implementera dataskyddskonventionen genom ett begrepp som stämmer bättre överens med konventionstexten anser vi att de begrepp som utvecklats inom svenskt dataskydd, med motsvarande innebörd, inte bör ändras när betydelsen avses vara densamma som tidigare.

Dataskyddskonventionens krav på öppenhet eller transparens kommer, i likhet med gällande rätt, främst att tillgodoses genom att det framgår av författning hur personuppgifter får behandlas vid

[53] Prop. 2018/19:163 s. 72.
[54] Prop. 2017/18:232 s. 142 f. och prop. 2018/19:163 s. 72.

myndigheten. Att de övergripande verksamheter för behandling anges bidrar till att uppnå detta krav, se avsnitt 8.4.

8.6 Inledande behandling av personuppgifter

8.6.1 Dataskyddskonventionens bestämmelser

En av de mest centrala bestämmelserna i dataskyddskonventionen 108+ är artikel 5.4 b. Där framgår bland annat:

> **Article 5 – Legitimacy of data processing and quality of data**
>
> 4. Personal data undergoing processing shall be:
>
> b. collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes […]

Denna ändamålsprincip vid personuppgiftsbehandling är en mycket viktig del av dataskyddet. Artikeln uttrycker att personuppgifter ska samlas in för ett särskilt, uttryckligt angivet och berättigat ändamål och inte behandlas på ett sätt som är oförenligt med det ändamålet.

Konventionen tillåter inte behandling för odefinierade, oprecisa eller vaga ändamål. Enligt kommentaren till konventionen är det som utgör ett legitimt ändamål beroende av omständigheterna kring behandlingen. Bestämmelsen syftar till att säkerställa proportionalitet mellan samtliga fri- och rättigheter och andra intressen som påverkas i det enskilda fallet. Med oförenlig behandling avses sådan behandling som kan vara oväntad, olämplig eller på annat sätt stötande för den registrerade. Det kan ha betydelse i vilket sammanhang personuppgifterna har samlats in och att det finns lämpliga skyddsåtgärder både för den ursprungliga och den avsedda vidare behandlingen.[55]

Principen, som får anses vara grunden för hela personuppgiftsskyddet, har i Sverige funnits med ända sedan den första datalagen från 1973. Ändamålsprincipen var en del av den första dataskyddskonventionen från 1981 och återfinns i motsvarande lydelse även i EU:s dataskyddsrätt.

[55] Se *Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, p. 48–49.

8.6.2 Den nuvarande regleringen

Den nuvarande säpodatalagen är utformad på samma sätt som övrig svensk personuppgiftslagstiftning i det avseendet att insamling av uppgifter inte längre är särreglerat i förhållande till övrig behandling.

Innan det lagstiftningsprojekt som genomförde brottsdatadirektivet i svensk rätt angavs i polisdatalagen att personuppgifter endast fick s*amlas in* för särskilda, uttryckligt angivna och berättigade ändamål.[56] Att insamlingsändamålen uttryckligen angavs i polisdatalagen motiverades av regeringen med att det är en central dataskyddsprincip att uppgifter endast får samlas in för specifika och legitima ändamål och att insamlade uppgifter inte får behandlas för något ändamål som är oförenligt med det ursprungliga ändamålet. Enligt regeringen kunde skyldigheten att ha ett preciserat ändamål för insamlingen visserligen sägas följa redan av de materiella bestämmelser som styr polisens verksamhet men valde ändå att särskilt ange insamlingsändamål.[57]

Den nuvarande säpodatalagen, tillsammans med alla de lagstiftningar som ingick i genomförandet av EU:s dataskyddsreform, har frångått metoden att särskilt ange och reglera personuppgiftsbehandling i form av insamling. Denna ordning motiverades med att det inte bara är när personuppgifter samlas in som det ska finnas ett särskilt, uttryckligt angivet och berättigat ändamål för behandlingen. Varje åtgärd som vidtas med insamlade uppgifter ska också uppfylla dessa krav.[58]

I förarbetena till säpodatalagen förklarade regeringen att det i underrättelseverksamhet, där personuppgifter behandlas på ett tidigt stadium i processen, inte alltid är möjligt att ange ändamålen för behandlingen lika tydligt och detaljerat som i annan brottsbekämpande verksamhet. Det innebär enligt regeringen att ändamålet till en början kanske inte kan anges mer preciserat än till vilken verksamhetsområde en viss uppgift hör, exempelvis kontraterrorism. Det får därför accepteras att beskrivningen av ändamålen inte alltid kan ha samma precision som i annan brottsbekämpande verksamhet. Det finns vidare inget som hindrar att det närmare ändamålet med behand-

[56] 9 § första stycket a personuppgiftslagen (1998:204) som genom 2 § första stycket 3 polisdatalagen (2010:631) gjordes tillämplig även för Säkerhetspolisen.
[57] Prop. 2009/10:85 s. 97 f.
[58] Prop. 2017/18:232 s. 121.

lingen inledningsvis är detsamma som anges i bestämmelsen om rättslig grund. Ändamålet får sedan preciseras mer när det blir möjligt.[59]

Dagens reglering kan därmed sägas innebära att det för Säkerhetspolisen i lagförarbetena har gjorts ett särskilt undantag avseende kravet på ett särskilt, uttryckligt angivet ändamål vid insamling. Undantaget medger att Säkerhetspolisen kan inhämta information för ett vagt formulerat ändamål, och att ändamålet i samband med att uppgifterna bearbetas och analyseras ska vara nödvändiga för ett särskilt, uttryckligt angivet ändamål. Detta möjliggör underrättelseinhämtning, men framgår alltså inte av lagtexten.

8.6.3 Särskilt angående underrättelseinhämtning

Bedömning: Inom Säkerhetspolisens verksamhet finns ett stort och för säkerhets- och underrättelsetjänster utmärkande behov av att aktivt samla in personuppgifter.

Att avslöja och avvärja hoten innan brotten begås är en säkerhetstjänsts främsta utmaning. En stor del av Säkerhetspolisens underrättelseverksamhet är beroende av att information inhämtas på olika sätt. Det kan röra sig om inhämtning med stöd av särskilda befogenheter, som exempelvis genom inriktning av signalspaning, hemlig dataavläsning eller avlyssning. I dessa fall finns regelverk som styr för vilka ändamål insamling av personuppgifter får ske och i vilken omfattning.

När inhämtning sker med stöd av särskilda befogenheter och särskilda regelverk finns ofta regler om hur länge och på vilket sätt de inhämtade uppgifterna får behandlas. Saknas det ska säpodatalagen tillämpas. Det gäller exempelvis egen insamling av personuppgifter från internet eller tips och uppslag som lämnas till Säkerhetspolisen eller uppgifter som lämnats från en samverkande tjänst i ett annat land. Om uppgifter inhämtats genom hemliga tvångsmedel, kan även åklagare, med stöd av 27 kap. 23 a § rättegångsbalken, besluta att uppgifter som har kommit fram får användas för ett annat ändamål än det som har legat till grund för åtgärden. Sådan, så kallad

[59] Prop. 2018/19:163 s. 68.

överskottsinformation, används ofta för underrättelseändamål och behandlas med stöd av säpodatalagen.

Säkerhetspolisens verksamhet utgörs till övervägande del av underrättelsearbete. Det bedrivs underrättelseverksamhet även inom andra brottsbekämpande myndigheter. Polismyndigheten har genom Nationella operativa avdelningen liknande möjligheter som Säkerhetspolisen att bedriva aktiv underrättelseinhämtning mot bland annat den grova organiserade gängbrottsligheten. Det finns emellertid en betydande skillnad i naturen hos underrättelseverksamheten som bedrivs av Polismyndigheten respektive Säkerhetspolisen. Polismyndigheten övervakar som regel en aktiv kriminell miljö där det finns åtskilliga indikatorer som pekar ut en riktning för underrättelseverksamheten. Även Säkerhetspolisen kan i vissa fall få indikationer som pekar ut en riktning, som att en viss våldsbejakande extremistmiljö håller på att radikaliseras.

En viktig del av Säkerhetspolisens uppdrag är emellertid att upptäcka, förebygga och förhindra mycket allvarlig brottslighet som inte sker i en aktiv kriminell miljö. Terrordåd riktade mot mål i västvärlden utmärks exempelvis ofta av att de planeras och förbereds i största hemlighet och utförs helt utan förvarning. Underrättelseverksamhet som syftar till att upptäcka och avvärja sådana okända hot måste därför ske utan att några närmare detaljer är kända då underrättelseinhämtningen påbörjas. Den preventiva uppgiften är den primära vilket innebär att Säkerhetspolisen inte kan förlita sig på polisanmälningar för att fullgöra sitt uppdrag. Myndigheten måste själv inhämta uppgifter för att identifiera om ett brott kan komma att begås. Uppdraget kräver således att Säkerhetspolisen på ett mycket tidigt stadium kan hämta in uppgifter inriktade mot brottslig verksamhet.

Den militära säkerhets- och underrättelsetjänsten har tillsammans med FRA ett liknande uppdrag. När FRA inhämtar signaler sker det utifrån ändamål som är brett formulerade genom beslut om försvarsunderrättelseverksamhetens inriktning och genom de inriktande myndigheternas närmare preciseringar (se avsnitt 3.6.2). När personuppgifter inhämtats med stöd av dessa breda ändamål påbörjas personuppgiftsbehandling för särskilda, uttryckligt angivna och berättigade ändamål. Detta sker bland annat genom att uppgifter som är av intresse struktureras och analyseras och att uppgifter som inte behövs för något berättigat ändamål raderas. Att den inledande behandlingen av personuppgifter genom inhämtning eller annan

insamling sker med stöd av ett bredare ändamål än den fortsatta behandlingen följer för FRA:s del av den särskilda bestämmelsen i 2 kap. 18 § FRA-datalagen. Där anges att flera av lagens krav inte ska gälla hantering av information i det skede av behandlingen då det inte har kunnat fastställas vilka personuppgifter som informationen innehåller.

Det är givetvis inte möjligt att inhämta uppgifter i syfte att förebygga okända hot, om det krävs att hotet ska anges som ändamål för inhämtning. Trots att den särskilda bestämmelsen i 2 kap. 18 § FRA-datalagen ursprungligen tillkom för att specifikt möta rättsliga hinder för signalspaning finns i 2 kap. 20 § försvarsdatalagen en likalydande bestämmelse som kan tillämpas av Försvarsmakten. Denna bestämmelse ger därmed klart lagstöd för den militära underrättelse- och säkerhetstjänsten att inhämta och inledningsvis behandla personuppgifter utan krav på särskilt, uttryckligt angivet och berättigat ändamål – i inhämtningsögonblicket.

Av avsnitt 6.1 och 6.2 följer att det finns ett stort behov för en myndighet med Säkerhetspolisens uppdrag att hantera de allt större informationsmängderna i samhället i syfte att identifiera hotaktörer och upptäcka tidigare okänd brottslig verksamhet. Det finns därför ett helt annat behov av att kunna samla in information och även en helt annan förväntan på att Säkerhetspolisen ska kunna agera i dagens informationsmiljö än vad som gäller för andra aktörer. Vi vill säkerställa att Säkerhetspolisen kan utföra sitt underrättelseuppdrag. Det behövs därför en reglering i säpodatalagen som tar hänsyn till det som utmärker myndighetens verksamhet och det faktum att det sker en exponentiell informationstillväxt i samhället.

8.6.4 Insamling och inhämtning bör särregleras

Bedömning: Insamling och liknande sätt att inleda behandling av personuppgifter bör regleras särskilt i säpodatalagen. Det ska inte ställas samma krav för sådan behandling som efterföljande behandlingsåtgärder.

I många verksamheter innebär den nuvarande ordningen inte något större problem. Normalt sett samlas inte uppgifter in i någon större omfattning av svenska myndigheter, och om det sker är det i så

liten utsträckning som möjligt. Ofta kommer personuppgifter till en myndighet till följd av en rättslig bestämmelse eller lämnas till myndigheten på dennas uppmaning. Någon regelrätt inhämtning eller insamling av information sker mer sällan av andra myndigheter än de som har någon form av underrättelseverksamhet knutet till sitt uppdrag. För en myndighet som Säkerhetspolisen som har ett uttalat och omfattande underrättelseuppdrag, anser vi att det finns en brist i denna systematik.

En mycket stor del av Säkerhetspolisens arbete går ut på att bedriva underrättelseverksamhet. En av myndighetens kärnuppgifter är därmed att samla in uppgifter som därefter bearbetas och analyseras. Det framstår därför som naturligt att insamling av uppgifter ska regleras särskilt och på ett transparent sätt. Det finns i huvudsak två skäl till att insamling av personuppgifter bör regleras särskilt.

Det går inte att ställa krav på uppgifters kvalitet innan uppgifterna är kända

För det första är det inte realistiskt, eller ens möjligt att, som den nuvarande lagstiftningen är formulerad, upprätthålla alla lagens krav på personuppgiftsbehandling under insamlingsskedet. Vid insamlingen, då uppgifterna fortfarande är okända till sitt innehåll går det nämligen inte att avgöra om personuppgifterna är nödvändiga, eller ifall de visar sig vara känsliga uppgifter, absolut nödvändiga för ett visst ändamål. Inte heller går det att i detta skede att avgöra om uppgifter är relevanta, adekvata och inte onödigt omfattande för ett visst ändamål. Prövningen av att personuppgifterna behandlas i enlighet med 2 kap. 3, 7–9 §§ säpodatalagen kan ske först efter att de finns tillgängliga hos myndigheten. Då har behandlingen redan påbörjats.

Den nuvarande lagstiftningen innebär i praktiken att Säkerhetspolisen inte kan följa säpodatalagen och samtidigt utföra sitt uppdrag som nationell säkerhetstjänst. Det är därmed svårt för medborgare att endast utifrån innehållet i lagen utläsa hur myndigheten behandlar personuppgifter i verksamheten. Denna otydlighet innebär också att effektiviteten i verksamheten kan lida av att det är osäkert med vilket rättsligt stöd en viss behandling sker.

Uppgifter måste kunna samlas in för att upptäcka okända hot

För det andra är det inte ett mål för Säkerhetspolisens verksamhet att insamling av uppgifter ska ske för på förhand bestämda, särskilda och uttryckligt angivna ändamål. En skillnad i förhållande till övrig brottsbekämpande verksamhet är att Säkerhetspolisen arbetar med brott som till sin natur är svåra – ibland mycket svåra – att bekämpa. En spion lämnar sällan spår efter sig och inte heller föranleder dennes förehavanden vanligtvis några anmälningar eller uppslag från allmänheten, som polisarbetet kan utgå från. En stor del av Säkerhetspolisens arbete är inriktat på att kartlägga personer och miljöer med anknytning till brottslighet av den typ som Säkerhetspolisen ska bekämpa. Föremål för Säkerhetspolisens arbete är främst personer eller organisationer som det finns anledning att hålla under uppsikt i syfte att förhindra brott mot rikets säkerhet. Det säger sig självt att det är svårt att få inblick i miljöer där sådan verksamhet förekommer. Såväl spioneri som terrorism bedrivs med nödvändighet i det fördolda och över huvud taget i former som till sin natur är slutna.

Det är givetvis inte möjligt att inhämta uppgifter i syfte att förebygga okända hot från sådana miljöer om det krävs att hotet ska anges som ändamål för inhämtning. Lösningen i den praktiska tillämpningen i dag är att kraven för med vilken precision ändamålen ska uttryckas är lägre i insamlingsskedet än för den efterföljande behandlingen. Enligt propositionsuttalanden finns inget som hindrar att det närmare ändamålet med behandlingen inledningsvis är exempelvis kontraterrorism för att sedan preciseras när det blir möjligt.[60] Denna tillämpning bör komma till uttryck i lagstiftningen.

8.6.5 Insamling och andra åtgärder som ger Säkerhetspolisen tillgång till personuppgifter bör betecknas som *inledande behandling*

Förslag: Personuppgiftsbehandling som innebär att Säkerhetspolisen inhämtar, samlar in eller på annat sätt får del av personuppgifter ska benämnas inledande behandling av personuppgifter.

[60] Prop. 2018/19:163 s. 68.

Vi har funnit skäl att återgå till att i lagen särskilt reglera insamling av personuppgifter. Enligt allmänt språkbruk innebär *insamling* att något samlas ihop genom en aktiv handling. Detta begrepp fångar dock inte hela spektrumet av hur Säkerhetspolisen kan komma i kontakt med personuppgifter. I begreppet insamling av uppgifter ligger ett antagande om att uppgifter kommit till myndigheten genom dess aktiva agerande. Regleringen som vi föreslår bör emellertid gälla även personuppgifter som kommer till Säkerhetspolisen på andra sätt, exempelvis genom att annan myndighet eller en samverkande tjänst i utlandet delar information utan att Säkerhetspolisen aktivt efterfrågat den. Som jämförelse kan vi se på hur olika myndigheter erhåller information. Medan exempelvis Skatteverket aktivt samlar in uppgifter genom deklarationer, kan Säkerhetspolisen både aktivt söka information och passivt ta emot den från olika källor. Begreppet insamling täcker inte in denna bredd av informationsflöden.

Insamling bör därför ersättas med ett lämpligt samlingsbegrepp. I 2 kap. 3 § säpodatalagen används begreppet *ursprunglig behandling* som ersättning för insamling för att förklara finalitetsprincipen. Begreppet används för den situation som vi avser att reglera. Det kan dock uppfattas som otydligt på så sätt att det går att tolka som att begreppet endast avser den första gången en personuppgift hanteras av Säkerhetspolisen. En personuppgift i form av exempelvis ett namn kan dock komma att samlas in många gånger och för olika ändamål. Vi föreslår att begreppet *inledande behandling* i stället ska användas. Begreppet som även ska framgå av definitionerna i lagen, innebär att personuppgifter kommer till eller görs tillgängliga för Säkerhetspolisen.

8.6.6 Inledande behandling bör kunna ske för ett brett formulerat ändamål

Förslag: Det ska inte ställas lika höga krav på att konkretisera ändamålet för den inledande behandlingen som för andra behandlingsåtgärder. Det ska därför inte ställas krav på ett *särskilt angivet* ändamål. Inledande behandling ska i stället få ske för ett ändamål som bestäms inom de i lagen angivna verksamheterna.

Syftet med regleringen av inledande behandling är i första hand att uppnå en transparens i lagstiftningen som på ett bättre sätt ska motsvara Säkerhetspolisens faktiska verksamhet. Lagen kommer på så sätt att avvika från brottsdatalagens struktur och materiella innehåll. För Säkerhetspolisens befogenhet att samla in uppgifter är ingen saklig förändring avsedd, men det tydliggörs att den verksamhet som Säkerhetspolisen ägnar sig åt är av ett särskilt kvalificerat slag, motiverat av nationell säkerhet. Innebörden av regleringen som vi föreslår är därmed att Säkerhetspolisen på samma sätt som sker i dag ska få samla in personuppgifter för breda ändamål.

Begreppet ändamål har förändrats över tid. Tidigare innehöll myndigheters personuppgiftslagstiftningar typiskt sett en uppräkning av primära ändamål, som mer eller mindre preciserat beskrev det myndighetsuppdrag för vilket uppgifter fick behandlas. I samband med EU:s dataskyddsreform gjordes bedömningen att det som tidigare betecknats som ändamål i stället var att anse som rättslig grund för behandling. De ändamål som avsågs med ändamålsprincipen förändrades därmed i vissa fall, eftersom det tidigare ofta ansetts tillräckligt att hänvisa till de primära ändamålen. Även i den tidigare lagstiftningen för Säkerhetspolisen gällde att personuppgifter bara fick samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Skillnaden var att med dessa ändamål avsågs de primära ändamålen, bland annat att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott mot rikets säkerhet eller terrorbrott.[61] Denna ordning antogs bestå även genom säpodatalagen, trots att det inte framgår uttryckligen av lagen.[62]

I avsnitt 8.4 har vi redogjort för varför det bör framgå inom vilka verksamheter som Säkerhetspolisen bör få behandla personuppgifter. Av lagen bör följa att det särskilda ändamålet för inledande behandling ska bestämmas inom någon av dessa verksamheter. Ändamålet för den inledande behandlingen måste vara tillräckligt specificerat för att ge ledning för bedömningen av behov och proportionalitet. Eftersom ändamålet för den inledande behandling även är avgörande för tillämpningen av finalitetsprincipen måste det även vara tillräckligt specifikt för att medge denna prövning.

[61] Se 6 kap. 1 §polisdatalagen (2010:361) och 9 § c personuppgiftslagen (1998:204) som enligt 2 kap. 2 § polisdatalagen skulle tillämpas.
[62] Prop. 2018/19:163 s. 220.

Det innebär sammantaget att det inte är tillräckligt med ett alltför vagt formulerat ändamål, som *brottsbekämpning* eller *kartläggning av brottslig verksamhet*. Det krävs en substans i ändamålet som innebär att en avvägning faktiskt kan göras mot andra skyddsvärda intressen och om efterföljande behandling är oförenlig med det inledande ändamålet.

De övergripande verksamheter som anges i lagen avser underrättelseverksamhet, säkerhetstjänst, brottsutredning och andra brottsbekämpande uppdrag. Därutöver finns utvecklingsverksamhet som sker i brottsbekämpande syfte. Det är inte tillräckligt att inleda behandling av personuppgifter endast med stöd av ändamålet kartlägga och klarlägga brottslig verksamhet. Detta begrepp syftar till att beskriva underrättelseverksamhet. Om ändamålet för den inledande behandlingen ska bestämmas inom denna verksamhet bör även typen av brottslighet anges. Ett godtagbart ändamål kan vara att uppgifterna ska behandlas för att kartlägga terrorhot mot Sverige. Då anges vilken brottslig verksamhet som underrättelseverksamheten ska bedrivas mot.

8.6.7 Behandlingströskeln för inledande behandling bör vara lägre än i dag

Förslag: Inledande behandling ska kunna ske av personuppgifter som är befogade för ändamålet.

Det är svårt för Säkerhetspolisen att följa säpodatalagen som den är formulerad i dag. Ett exempel på att lagstiftningen inte är förenlig med Säkerhetspolisens verksamhet är att endast uppgifter som är *nödvändiga* för ett ändamål får behandlas. Bedömningen av om en uppgift är nödvändig för ett ändamål är emellertid inte möjlig att göra förrän uppgiften redan har behandlats. Denna diskrepans mellan verksamhetens praktik och lagstiftning är inte unik för Säkerhetspolisen. Vi uppfattar dock att det är ett särskilt tydligt problem i en verksamhet som kan betecknas som integritetskänslig, vilket ställer höga krav på en transparent lagstiftning. Dessutom utgör inte det beskrivna problemet något särpräglat och sällan förekommande undantag. Säkerhetspolisens underrättelseverksamhet består i hög grad av aktiv insamling av personuppgifter. Lagstiftningen bygger

på premissen att behovet av vissa specifika uppgifter är känd på förhand. Det finns dock samtidigt en förväntan på att Säkerhetspolisen i sitt uppdrag som säkerhetstjänst ska upptäcka ännu okända hot.

I praktiken sker det en inhämtning av uppgifter, både av Säkerhetspolisen och andra myndigheter med liknande uppdrag, trots denna lagtekniska utformning. Denna pragmatiska tolkning av vad som är tillåtet enligt gällande rätt bygger på vissa förarbetsuttalanden och ett samförstånd mellan verksamhetsutövare och tillsynsmyndigheten. Vi anser att det är lämpligare att det framgår av lag att Sveriges nationella säkerhetstjänst får samla in personuppgifter för att upptäcka okända hot. En sådan lagstiftning är mer transparent och förutsägbar för medborgarna.

Vår uppfattning är att lagstiftningen bör vara tydlig med att underrättelseverksamhet får bedrivas mot vissa relevanta informationsmiljöer och att inledande behandling får ske av uppgifter som kan förväntas vara relevanta. Att inledande behandling får ske för övergripande ändamål, som exempelvis ”kartläggning av terrorhot” innebär att en viss typ av uppgifter typiskt sett kan antas vara relevanta att analysera. Det är däremot inte möjligt att behandla *endast* de uppgifter som är relevanta, eftersom bedömning av om en uppgift är relevant inte går att göra förrän uppgiften har behandlats genom exempelvis insamling. Europadomstolen har även accepterat att underrättelseverksamhetens natur är sådan att personuppgifter först måste samlas in, innan dess värde som underrättelser kan bedömas.[63] För att markera att underrättelseverksamhet får bedrivas genom aktiv insamling och inhämtning mot vissa miljöer i syfte att upptäcka okända hot bör en lägre behandlingströskel gälla för inledande behandling.

Vilken behandlingströskel bör väljas

I Danmark tillämpas olika behandlingströsklar för säkerhetstjänstens PET:s personuppgiftsbehandling beroende både på vilket ändamål och vilken behandling det är fråga om. PET får samla in och inhämta personuppgifter s*om kan ha betydelse (”kan have betydning”)* för verksamheten. När det gäller efterföljande behandlingsåtgärder, som

[63] Se Europadomstolens dom 24 januari 2019, *Catt mot Förenade kungariket*, mål nr 43514/18, p. 117.

lagring eller delning, är behovskriteriet för underrättelseverksamheten lägre än övrig verksamhet. För att förebygga och efterforska brott inom PET:s ansvarsområde, krävs att personuppgifter*n kan antas ha betydelse* (”*må antages at have betydning*”) vilket är ett betydligt lägre krav ä*n nödvändigt* som är behandlingströskeln för annan verksamhet (se även avsnitt 4.2.2).

Det finns oss veterligen ingen motsvarande lagstiftning i Sverige som direkt uppmärksammat ett behov av att särreglera inledande behandling i personuppgiftslagstiftningen. FRA behandlar en stor mängd personuppgifter i sin signalspaningsverksamhet. Enligt FRA-datalagen får myndigheten behandla personuppgifter som är nödvändiga för att bedriva den verksamhet som anges i lagen (2000:130) om försvarsunderrättelseverksamhet och lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet. Regeringen uttalade i författningskommentaren att det ligger i underrättelseverksamhetens natur att det inte går att på förhand göra tydliga avgränsningar av vilka uppgifter som måste inhämtas för att nå det slutliga målet att åstadkomma de underrättelser som uppdragsgivarna efterfrågar. Inhämtad information kan motivera inhämtning av annan information som man från början inte kände till. Verksamheten kan också gå ut på att söka efter företeelser och hot som är okända men som antas existera.[64] Denna beskrivning av underrättelseverksamhetens behov kan göras gällande även för Säkerhetspolisen och även för inhämtning som, till skillnad mot signalspaning, inte är särskilt reglerad.

För att åstadkomma en rimlig avgränsning av Säkerhetspolisens insamling av personuppgifter bör behandlingströskeln för inledande behandling vara lägre än för andra former av behandling, men inte så låg att oskäligt många uppgifter kan samlas in. Begreppet *skäligt* används i många andra sammanhang. Enligt vår bedömning passar skälig emellertid mindre väl som behandlingströskel. Skälig används exempelvis inom straffprocessen för angivande av en misstankegrad. Kravet för att Säkerhetspolisens ska få behandla personuppgifter bör dock vara betydligt lägre än vad som avses med exempelvis en skälig misstanke om brott. Ett annat begrepp som skulle kunna införas är *berättigad.* Berättigad innebär att något är välgrundat. Berättigad är emellertid närbesläktat med ordet rättighet och används ofta för att beskriva att någon har rätt till något. Denna åsyftning leder tankarna

[64] Prop. 2020/21:224 s. 214.

fel i detta sammanhang. Behandlingströskeln är inte avsedd att beskriva vilken behörighet som Säkerhetspolisen i och för sig har att inleda personuppgiftsbehandling utan vilken befogenhet som finns för sådan behandling i det enskilda fallet. Ett begrepp som enligt Svenska Akademiens ordlista ligger nära både skälig och berättigad är just ordet *befogad*. Enligt Svensk Ordbok har befogad betydelsen ”som grundas på övertygande skäl”. Befogad används i många andra lagar för att markera att något är skäligt.[65]

Enligt vår bedömning motsvarar ”befogad” väl det vi vill eftersträva med angivandet av en behandlingströskel för inledande behandling. Att en inledande behandling måste vara befogad för ett visst ändamål visar att åtgärden måste utgöra en skälig avgränsning i förhållande till ändamålet. Det får givetvis inte handla om att uppgifter som är helt onödiga för ändamålet behandlas. Om uppgifter förekommer i ett sammanhang eller en kontext som är relevant att analysera, är dock de där ingående personuppgifterna alltid befogade att inledningsvis behandla. Om den informationsmiljö eller den uppgiftsmängd som den inledande behandlingen avser inte är tillräckligt väl avgränsad kan det emellertid vara svårt för Säkerhetspolisen att motivera att behandlingströskeln är passerad för uppgiftsmängden som helhet.

Vad avses med befogade uppgifter?

Innebörden av begreppet ”befogad” bör vara att det finns någon indikation som ger stöd för att personuppgifterna i fråga är relevanta att behandla för ändamålet. Det bör däremot inte krävas någon visshet eller en sannolikhetsövervikt för att uppgifterna verkligen är det. Det finns därmed inget krav på att det på förhand ska finnas belagda misstankar om att någon för Säkerhetspolisen känd aktör förekommer i uppgiftsmängden. Det bör vara tillräckligt att det finns skäl att för det angivna ändamålet undersöka om någon känd aktör förekommer eller att det finns anledning att anta att företeelser eller hot som är okända men antas existera går att identifiera i materialet.

Uppgifter av visst slag eller som har visst ursprung kan typiskt sett vara befogade att behandla för ett inledande ändamål. Exempelvis

[65] Se exempelvis 1 § lag (1988:688) om kontaktförbud angående kontakter som är uppenbart befogade och i vapenlagstiftningen avseende befogade undantag från generella förbud.

kan överskottsinformation från hemliga tvångsmedel många gånger antas vara befogad för underrättelseverksamheten. Detsamma kan sägas om information som överlämnats av betrodda partner eller andra myndigheter. I dessa fall har någon annan redan bedömt att uppgifterna är relevanta för Säkerhetspolisen, vilket ofta innebär att det är befogat att undersöka uppgifterna vidare.

8.6.8 Det ska inte ställas krav på personuppgifternas kvalitet vid inledande behandling

Förslag: Kraven på personuppgifters kvalitet ska inte tillämpas vid inledande behandling.

Vi har i avsnitt 8.6.4 redogjort för skälen till att inledande behandling bör särregleras. Ett av dessa skäl är att det inte är rimligt att uppställa krav på uppgifters kvalitet innan de kunnat granskas. För att kunna granska en uppgift måste den först behandlas – men uppgiften får inte behandlas innan den granskats. Denna interna konflikt mellan dataskyddsrättsliga principer är inte unik för den nuvarande säpodatalagen och innebär att det i praktiken måste göras ett oreglerat undantag från vissa bestämmelser under en inledande granskningsperiod.

De flesta myndigheter har inte några större problem att motivera undantag från dessa principer under en kortare period efter att uppgifter inhämtas eller samlats in, eftersom de granskas i princip simultant med denna behandling.

För en myndighet vars uppdrag förutsätter inhämtning och insamling av stora, på förhand okända och osorterade informationsmängder, innebär en sådan inkonsekvens att lagen inte på ett korrekt sätt återspeglar tillämpningen. För att förtydliga att det inte uppställs något krav på personuppgifters kvalitet innan de kunnat granskas bör kvalitetskraven särskilt undantas vid inledande behandling.

8.6.9 Lättnaderna avseende inledande behandling är nödvändiga och proportionerliga

Bedömning: Lagens lägre krav för inledande behandling är proportionerligt och nödvändigt i demokratiskt samhälle för att skydda nationell säkerhet. Lagen respekterar andemeningen i skyddet för personuppgifter.

De generella personuppgiftsregelverken, som dataskyddsförordningen eller dataskyddskonventionen 108+, är inte särskilt anpassade för brottsbekämpande verksamhet. Det är skillnad på myndigheter och företag som inhämtar personuppgifter genom att den enskilda exempelvis skickar in en ansökan eller ger sitt samtycke till att uppgifter registreras och en säkerhetstjänst som har till uppdrag att upptäcka brott och brottslig verksamhet som pågår i det fördolda. Det är utmanande att tillämpa samma principer för så väsensskild verksamhet. Det finns anledning att se över om den föreslagna lösningen avseende inledande behandling är förenlig med dataskyddskonventionen.

Det finns inte någon praxis som direkt bidrar till tolkningen av de särskilda och uttryckligt angivna ändamålen för insamling i dataskyddskonventionen 108+. I den ursprungliga och alltjämt gällande konvention 108, från 1981, uppställs inte samma krav. Där anges, i artikel 5 a, att personuppgifter ska ”erhållas” (”be obtained”) och behandlas korrekt och författningsenligt. I nästa punkt i artikeln, 5 b, anges att ”lagring” av uppgifterna däremot ska ske för ”särskilda och berättigade ändamål”. Principerna om uppgifts- och lagringsminimering ska prövas mot detta särskilda ändamål.

Vår tolkning av den ursprungliga dataskyddskonventionen är att insamling får ske med stöd av det som i Sverige kallas primärt ändamål eller en rättslig grund men att endast de personuppgifter som behövs för ett särskilt ändamål får behållas. Skillnaderna i konvention 108 och 108+ i detta avseende är att den moderniserade konventionen kräver särskilt, uttryckligt angivet och berättigat ändamål för all behandling, inklusive insamling. Det talar emot att vår föreslagna lösning, där inledande behandling i princip ska kunna ske för ett primärt ändamål, är förenlig med konvention 108+. Det finns inte några detaljerade rapporter eller förarbeten om vad som legat bakom förändringen av dataskyddskonventionen i detta avseende.

Ändringen ligger dock i linje med hur det europeiska personuppgiftsrätten utvecklats i övrigt, då både brottsdatadirektivet och dataskyddsförordningen är utformade på samma sätt.

Vi ser ett stort värde i att det ställs höga krav på konkretion av det ändamål för vilket personuppgifter behandlas. Det gäller särskilt för integritetskänslig behandling, som exempelvis behandling som sker med stöd av säpodatalagen. Vilket krav som dataskyddskonventionen ställer på konkretionen av ett särskilt ändamål är emellertid svårt att bedöma. Det finns sannolikt olika tolkningar av vad som avses med ett särskilt, uttryckligt angivet ändamål mellan konventionsstaterna. Detsamma gäller begreppets uttolkning i olika svenska lagstiftningar.

Vår bedömning är att kravet på ett särskilt, uttryckligt angivet ändamål inte är relevant för insamling som sker i underrättelseverksamhet. Det huvudsakliga intrånget i den personliga integriteten sker enligt vår uppfattning efter inhämtningsskedet. Regeringsformens integritetsskydd avser personuppgifter som behandlas på ett sätt som innebär ett betydande intrång i den personliga integriteten och som utgör övervakning eller kartläggning av den enskildes personliga förhållanden. En kartläggning eller övervakning förutsätter i princip ytterligare behandling än insamling.

Vi anser att andemeningen i principen, som den kommer till uttryck i dataskyddskonventionen 108+ medger insamling för breda underrättelseändamål. Detta gäller så länge de insamlade uppgifterna endast får fortsätta att behandlas om det behövs för särskilda, uttryckligt angivna och berättigade ändamål. Denna tillämpning är en förutsättning för att förebygga, förhindra och i synnerhet upptäcka brottslig verksamhet som utgör hot mot nationell säkerhet. När en sådan förutsättning föreligger finns också möjlighet att göra undantag, enligt artikel 11 i konventionen.

Oavsett hur dataskyddskonventionen 108+ ska uttolkas i denna del, finns därmed utrymme för Sverige att utforma en lagstiftning i enlighet med vårt förslag. Vår uppfattning är att förslaget befinner sig inom Sveriges bedömningsmarginal när det kommer till frågan om vad som är nödvändigt i ett demokratiskt samhälle för att skydda nationell säkerhet.

8.7 Efterföljande behandlingsåtgärder

8.7.1 Efterföljande behandling bör få ske för särskilda, uttryckligt angivna och berättigade ändamål

Bedömning: Intrånget i rätten till privatliv och den personliga integriteten är större när personuppgifter fortsätter att behandlas efter insamlingen. Det krävs därför ett starkt dataskydd för sådan behandling.

Förslag: Den behandling av personuppgifter som följer efter den inledande behandlingen ska endast få ske för särskilda, uttryckligt angivna och berättigade ändamål.

I begreppet inledande behandling ingår alla de åtgärder som krävs för att myndigheten ska få tillgång till personuppgifter, exempelvis genom inhämtning med stöd av särskild lagstiftning, insamling från öppna källor eller att Säkerhetspolisen tar emot underrättelser från andra tjänster. Efter inledande behandling av uppgifter sker i princip undantagslöst ytterligare behandlingsåtgärder, i form av exempelvis lagring, granskning, läsning eller radering.

Regleringen av den efterföljande behandling av personuppgifter är helt avgörande för ett effektivt dataskydd. Ett betydande intrång och sådan kartläggning som avses i 2 kap. 6 § andra stycket regeringsformen uppstår ofta genom åtgärder som sökning eller sammanställning av lagrade personuppgifter, antingen ensamt eller i kombination. Vi anser att tyngdpunkten för dataskyddet bör ligga där risken för intrång är som störst. En viktig del i ett sådant skydd är ändamålsprincipen. Det etablerade uttrycket för ändamålsprincipen i dataskyddssammanhang är att personuppgifter bara får behandlas för särskilda, uttryckligt angivna och berättigade ändamål. Det finns ingen anledning att frångå denna princip när det gäller andra behandlingsåtgärder än inledande behandling.

Att ändamålet ska vara *särskilt* innebär att de måste vara tillräckligt specificerade för att ge ledning för andra bedömningar i lagen. Det krävs en bedömning av om personuppgifterna är adekvata och relevanta för ändamålet för behandlingen och inte mer omfattande än vad som behövs. Ett särskilt ändamål är avgörande för att bedöma avgränsningen av den personuppgiftsbehandling som kan motiveras.

Ett övergripande ändamål, som kan godtas vid den inledande behandlingen, är ofta inte tillräckligt för att göra en sådan prövning. Ett särskilt ändamål kan exempelvis vara en kartläggning av vissa terroristnätverk i Sverige eller utomlands. Det kan även röra sig om hotbildsbedömningar av vissa utpekade skyddspersoner. Något hinder mot att ange flera parallella ändamål för behandlingen finns inte. Samma krav ställs emellertid för varje ändamål som angivits.

Att ändamålen ska vara *uttryckligt angivna* är inte ett dokumentationskrav för behandling av enskilda personuppgifter. Som framgår av avsnitt 8.13.3 föreslår vi att det särskilda ändamålet, i likhet med i dag, ska anges som en särskild upplysning om ändamålet inte framgår på annat sätt. I många fall följer ändamålet av sammanhanget som uppgiften förekommer i. Om exempelvis någon form av textmeddelanden samlats in och bevarats från ett it-beslag, följer ändamålet för alla personuppgifter som återfinns i dessa av ändamålet med att beslaget överhuvudtaget bevaras. Kravet på uttryckligt angivande av ändamålet innebär att Säkerhetspolisen alltid måste kunna redogöra för vilket eller vilka ändamål uppgiften vidarebehandlas. Detta oavsett om det finns en särskild upplysning eller om det får anses följa av sammanhanget.

Att ändamålen ska vara *berättigade* innebär att de inte får gå utöver de breda ändamålen som anges i lagen och måste följa en rättslig grund. Exempelvis måste kartläggning av brottslig verksamhet avse verksamhet som innefattar brott som Säkerhetspolisen ansvarar för enligt polislagen och myndighetens instruktion. Kravet på att det särskilda ändamålet ska vara berättigat innebär därmed att det måste vara förenligt med Säkerhetspolisens verksamhet som den anges i lag, förordning, internationellt åtagande eller särskilt beslut av regeringen.

Givetvis kan en rättslig grund som står i strid med en överordnad norm inte berättiga en personuppgiftsbehandling. Av 12 kap. 10 § regeringsformen följer att om ett offentligt organ finner att en föreskrift står i strid med en bestämmelse i grundlag eller annan överordnad författning, får föreskriften inte tillämpas. En regeringsinstruktion som står i strid med exempelvis 2 kap. 21 § regeringsformen kan därför aldrig utgöra en berättigad rättslig grund. Kravet på att ändamålet för behandlingen ska vara berättigat innebär ett krav på att behandlingen ska vara förenlig med konstitutionella och andra rättsliga principer.

8.7.2 Särskilt om fortsatt behandling av uppgifter inom underrättelseverksamheten

Bedömning: När uppgifter behandlas för att kartlägga brottslig verksamhet går det inte att ställa krav på att varje enskild personuppgift i ett material ska behandlas för ett specifikt ändamål.

Behandlingen av enskilda personuppgifter bör i underrättelseverksamhet ses i förhållande till den kontext där de förekommer. Vid kartläggning innebär det att vissa personuppgifter bör kunna behandlas för att sätta andra, mer centrala, uppgifter i sitt sammanhang.

Kartläggning och klarläggning är en del av underrättelseprocessen

Syftet med särskilda regler för den inledande behandlingen är huvudsakligen att reglera Säkerhetspolisens underrättelseverksamhet under inhämtningsskedet. Underrättelsearbete bedrivs enligt en särskild process som innebär att en inhämtning följs av bearbetning, analys och slutligen delgivning av information. De efterföljande delarna i denna process innebär i stor utsträckning personuppgiftsbehandling som, till skillnad mot mycket av inhämtningen, inte omfattas av några särskilda regelverk.

Efter att information har hämtats in bearbetas den genom att struktureras, systematiseras och värderas, till exempel genom jämförelser med sedan tidigare kända uppgifter. Därefter vidtar analysen. Det kan handla om till exempel hot- och riskanalys, analys av brottsmönster och kartläggning av nätverk och grupperingar. Efter inhämtning, bearbetning och analys är ambitionen att det framtagna underrättelsematerialet ska kunna användas i operativt arbete. Det framtagna underrättelsematerialet kan till exempel läggas till grund för beslut om att inleda förundersökning eller om att vidta andra åtgärder för att avvärja brott. Brottsförebyggande åtgärder kan bestå i att berörda personer kontaktas och därigenom blir medvetna om myndighetens intresse, vilket många gånger leder till att den planerade brottsliga verksamheten aldrig kommer till stånd. Samverkan kan också ske med en annan myndighet för att den myndigheten ska kunna vidta hotreducerande åtgärder. Underrättelse-

information kan även delas med samverkande myndigheter i andra länder, se vidare avsnitt 3.3.2 och 3.3.3.

Inom ramen för detta arbete måste Säkerhetspolisen kunna dokumentera och analysera både information av underrättelsekaraktär och annan information. Detta trots att ändamålet inte går att konkretisera till exempelvis en utpekad aktör eller misstankar om att ett visst konkret brott kommer att begås i framtiden. Säkerhetspolisens behov av att kunna genomföra och dokumentera olika typer av undersökningar och analyser av bland annat företeelser, personer och platser är således stort. Detta behov skiljer sig även i flera avseenden från de behov som finns inom den övriga polisen. Den underrättelseverksamhet som bedrivs inom Säkerhetspolisen är till sin natur ofta sådan att den ligger på ett tidigare stadium än den som bedrivs av polisen i övrigt. Å andra sidan är den, genom Säkerhetspolisens instruktion, inriktad mot ett fåtal, väl avgränsade företeelser av särskilt samhällsfarlig karaktär.[66]

Trots denna skillnad mellan Säkerhetspolisens och Polismyndighetens brottsbekämpande uppdrag, har regleringen av underrättelseverksamhet varit likartad. Vi har i tidigare avsnitt föreslagit att lagen ska innehålla övergripande verksamheter som beskriver de yttre ramarna för de ändamål som kan föranleda personuppgiftsbehandling. En av dessa bestämmelser syftar till att särskilja underrättelseverksamheten. Det handlar om uppgifter som behandlas för att *kartlägga och klarlägga* den typ av brottslig verksamhet som Säkerhetspolisen ansvarar för.

Även om kravet för den inledande behandlingen inte är högre än att det ska anges ett brett formulerat inhämtningsändamål inom en verksamhet, måste ändamålet successivt förtydligas för de uppgifter som fortsätter att behandlas. Ofta sker detta per automatik genom processen med att bearbeta, sammanställa och analysera information. Strukturering av information i myndighetens olika system innebär att ändamålet ofta går att utläsa av sammanhanget. Ändamålsprincipens huvudsakliga syfte är emellertid att säkerställa att uppgifter som inte har en tydlig koppling till något ändamål inte heller fortsätter att behandlas.

[66] Prop. 2009/10:85 s. 256.

Kartläggning innebär att uppgifter kan behandlas i sitt sammanhang

Att uppgifter inte får behandlas om de inte kan kopplas till ett visst specifikt ändamål innebär inte att det i alla sammanhang går att ställa krav på att varje enskild personuppgift i ett material är nödvändig för ett specifikt ändamål. Behandlingen av enskilda personuppgifter måste i underrättelseverksamhet ses i förhållande till den kontext där de förekommer. Det innebär att enskilda personuppgifter, även om de är irrelevanta för att exempelvis avvärja ett terroristbrott, ändå kan behandlas för att sätta mer relevanta uppgifter i sitt sammanhang. Uppgiften kan behövas för den bredare kartläggningen av företeelsen. Detta är avsett att fångas av de nya ändamålsbestämmelserna som ger Säkerhetspolisen rätt att i sin underrättelseverksamhet kartlägga och klarlägga brottslig verksamhet.

Normalt sett ska i underrättelseverksamheten någon radering av enskilda personuppgifter inte behöva göras i ett sammanhållet dokument eller från det sammanhang där de naturligt förekommer. Om sammanhanget behövs för att kartlägga en brottslig verksamhet, bör ändamålet för personuppgiftsbehandlingen kunna gälla för samtliga däri ingående personuppgifter. Om personuppgifter i ett helt dokument eller (vilket är mer vanligt) i ett digitalt sammanhang ska behandlas, bör bedömningen av ändamålet för behandlingen få göras gemensamt för de uppgifter som förekommer där. Kravet på att ändamålen ska vara uttryckligt angivna bör därför inte heller anses innebära ett krav på att ändamålen ska dokumenteras i varje enskilt fall och för varje enskild personuppgift.

De första personuppgiftslagarna avsåg att reglera olika register. Innan digitaliseringen utgjordes sådana register av pappersakter i dokumentskåp. I ett sådant register krävdes det att varje individ av intresse tilldelades en personakt eller på annat sätt aktivt fördes in i ett system som möjliggjorde sökning. Att förekomma som en sådan sökbar aktör i register hos Säkerhetspolisen utgjorde regelmässigt ett allvarligt intrång i den personliga integriteten. Det är därför naturligt att ändamålsprincipen gällde fullt ut för varje enskild personakt. Det är rimligt att kräva ett särskilt och uttryckligt angivet ändamål för att få registrera en person och föra in information i dennes personakt. Varken då eller nu är det dock avsett att alla enskilda personuppgifter som finns hos en underrättelsetjänst individuellt ska prövas

för ett specifikt ändamål. Det förekom tidigare regelmässigt att tidningsurklipp, kontakter som den registrerade haft, eller fotografier där denne förekom tillsammans med andra bevarades i personakter. Europadomstolen har vid upprepade tillfällen prövat om personakter som olika säkerhetstjänster upprättat varit förenliga med artikel 8 i Europakonventionen och i flera fall kritiserat säkerhetstjänster för sådana personakter och deras innehåll. Det finns däremot, oss veterligen, inget uttalande från domstolen som innebär att samtliga individuella personuppgifter som ingår i en sådan personakt ska prövas för sig. Normalt sett utgår domstolen från att om det finns ett berättigat ändamål för att upprätta en sådan akt så innefattar det alla uppgifter som behövs för kartläggning av en individ eller ett fenomen.

Nu har registerbegreppet i stort sett övergetts och digitaliseringen har ersatt behovet av att behandla personuppgifter i akter av olika slag. Principen bör dock alltjämt vara densamma. Ändamålet för att behandla personuppgifter bör avse de uppgifter som är förenade av sitt naturliga sammanhang och inte varje personuppgift för sig.

Det bör vara möjligt att behandla en stor mängd personuppgifter genom att i en kartläggning av brottslig verksamhet behandla uppgifter i ett sammanhang. En sådan kartläggning som kräver efterföljande behandling av ett mer vidlyftigt material begränsas emellertid i den föreslagna lagstiftningen genom proportionalitetsprövningen. Behandlingen av informationen måste utgöra en rimlig avvägning mellan ändamålet för behandlingen och de andra skyddsvärda intressena som påverkas. Registrering och lagring av uppgifter om personer som endast har en avlägsen koppling till ändamålet kan vara möjlig, om ändamålet är mycket angeläget. Så är exempelvis fallet om ändamålet för kartläggningen är att förhindra ett allvarligt, verkligt och aktuellt hot mot Sveriges säkerhet. Om kartläggningen i stället sker för att möta mer långsiktiga och strategiska hot mot nationell säkerhet, kan proportionalitet uppnås på andra sätt. Exempelvis genom att uppgifterna endast behandlas under en kortare tid eller genom att färre uppgifter behandlas.

I likhet med gällande rätt bör kravet på uttryckliga ändamål kunna tillgodoses genom en särskild upplysning i de fall ändamålet inte framgår av sammanhanget. Ofta framgår sammanhanget klart av den kontext som personuppgifter förekommer i. Om det förekommer en personuppgift i ett dokument, en konversation eller på

ett fotografi, står det ofta klart utifrån sammanhanget för vilket ändamål samtliga personuppgifter där behandlas.

Det bör därför vara möjligt att fortsätta att behandla samtliga uppgifter som har ett naturligt samband trots att det endast är vissa personuppgifter som är relevanta för kartläggning av den brottsliga verksamheten i fråga.

8.8 Finalitetsprincipen

8.8.1 Dataskyddskonventionens bestämmelser

Som en del av ändamålsprincipen i artikel 5.4 b dataskyddskonventionen framgår även den så kallade finalitetsprincipen.

> **Article 5 – Legitimacy of data processing and quality of data**
>
> 4. b Personal data undergoing processing shall be collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is, subject to appropriate safeguards, compatible with those purposes;

Finalitetsprincipen i dataskyddskonventionen innebär som huvudregel att personuppgifter inte bör vidarebehandlas på ett sätt som den registrerade kan anse vara oväntat, olämpligt eller på annat sätt stötande. För att fastställa om ett nytt ändamål är förenligt med det ändamål för vilket personuppgifterna ursprungligen samlades in ska den personuppgiftsansvarige, enligt kommentaren till konventionen, bland annat beakta det sammanhang där personuppgifterna har samlats in, de registrerade personernas rimliga förväntningar och deras relation till den personuppgiftsansvarige. Personuppgifternas art kan också påverka bedömningen av om behandlingen är förenlig med insamlingsändamålet. Andra aspekter av prövningen är vilka konsekvenser den avsedda behandlingen kan få för de registrerade samt förekomsten av lämpliga skyddsåtgärder i både den ursprungliga och den avsedda ytterligare behandlingen.[67]

[67] *Explanatory Report – CETS 223 – Automatic Processing of Personal Data* (Amending Protocol), p. 49.

8.8.2 Den nuvarande regleringen

Finalitetsprincipen innebär att uppgifter inte får behandlas för nya ändamål som är oförenliga med det ändamål för vilket uppgifterna samlades in. Detta har sedan lång tid gällt för Säkerhetspolisens verksamhet. Säkerhetspolisen behöver kunna behandla personuppgifter för nya ändamål, till exempel använda information från en förundersökning för att senare förebygga nya brott.

Säpodatalagens ändamålsbestämmelse, i 2 kap. 3 § har en liknande utformning som dataskyddskonventionen i detta avseende. Där anges att personuppgifter inte får behandlas för något ändamål som är oförenligt med det ändamål som de ursprungligen behandlades för.

När Säkerhetspolisen ska behandla personuppgifter för nya ändamål, innebär finalitetsprincipen att myndigheten måste pröva om det nya ändamålet är förenligt med det ändamål för vilket personuppgifterna samlades in. Om det exempelvis krävs för att kartlägga främmande makts inblandning vid ett terroristattentat, kan uppgifter som inledningsvis behandlats för ändamål inom kontraspionaget behandlas för nya ändamål inom kontraterrorverksamheten. Eftersom Säkerhetspolisens brottsbekämpande verksamhet är inriktad på att bekämpa en viss typ av systemhotande brott, har Säkerhetspolisens behandling av personuppgifter för nya ändamål ansetts förenlig med ursprungsändamålet i de allra flesta fallen.[68]

8.8.3 Behandling för nya ändamål bör regleras på samma sätt som i dag

Förslag: Som huvudregel bör finalitetsprincipen gälla. Det innebär att personuppgifter inte får behandlas för ett ändamål som är oförenligt med ändamålet för den inledande behandlingen.

Finalitetsprincipen hindrar dock inte behandling för diarieföring och handläggning eller vetenskapliga, statistiska eller historiska ändamål.

[68] Prop. 2018/19:163 s. 221.

Finalitetsprincipen ska gälla

Vi har inte uppfattat att finalitetsprincipen utgör ett problem för den verksamhet som bedrivs inom myndigheten. Principen utgör en viktig del av ändamålsprincipen och utgör en relevant dataskyddsmekanism. Det finns därför inte skäl att reglera behandling för nya ändamål på annat sätt än enligt nuvarande lagstiftning. Vår föreslagna proportionalitetsprövning för all personuppgiftsbehandling innebär emellertid att finalitetsprincipen kompletteras av en liknande prövning som enligt 2 kap. 4 § brottsdatalagen gäller för övriga brottsbekämpande myndigheter.

Att behandling för nya ändamål både ska vara proportionerlig och inte oförenlig med ändamålet för den inledande behandlingen utgör enligt vår bedömning en rimlig ordning. Den information som Säkerhetspolisen behandlar kan vara mycket integritetskänslig och det är därför lämpligt att prövningen inte endast sker av ändamålen utan även av vilket intrång som behandlingen för det nya ändamålet kan medföra. Ett nytt ändamål av lägre tyngd kan vid prövningen medföra att behandlingen för detta ändamål inte är proportionerlig.

Behandling för andra än operativa ändamål

En särskild fråga är hur finalitetsprincipen förhåller sig till ändamål som sker i helt andra intressen än Säkerhetspolisens.

I nuvarande säpodatalag framgår, av 2 kap. 2 §, att personuppgifter får behandlas om det är nödvändigt för diarieföring eller handläggning av en anmälan, ansökan eller liknande. Vi anser att syftet med denna bestämmelse är något oklart. Att Säkerhetspolisen får behandla personuppgifter för att uppfylla sina förvaltningsrättsliga skyldigheter framstår som självklart. Det finns en rättslig grund för sådan behandling enligt bland annat förvaltningslagen, offentlighets- och sekretesslagen och tryckfrihetsförordningen. Däremot kan det inte anses lika klart att uppgifter som ursprungligen behandlats för ett brottsbekämpande ändamål utan hinder av finalitetsprincipen även får behandlas för ett administrativt. Det kan därför finnas skäl att klargöra att diarieföring och vissa handläggningsåtgärder får ske även enligt den nya lagen.

Av 2 kap. 5 § säpodatalagen följer vidare att Säkerhetspolisen får behandla personuppgifter för vetenskapliga, statistiska eller historiska

ändamål inom lagens tillämpningsområde. Motsvarande bestämmelser finns i många andra personuppgiftslagstiftningar och ger exempelvis förutsättningar att göra sökningar och sammanställningar av personuppgifter för brottsstatistiska ändamål eller för en vetenskaplig undersökning. Det ger även stöd för att lämna ut uppgifter för sådana ändamål. Det får däremot knappast antas ha varit syftet att Säkerhetspolisen ska ägna sig åt insamling eller inhämtning av personuppgifter för sådana ändamål. Det bör därför vara tillräckligt att ge möjlighet till behandling för sådana ändamål utan hinder av finalitetsprincipen.

8.8.4 Särskilt om personuppgifter som behandlas för utvecklingsändamål

Förslag: Personuppgifter som behandlas för ett brottsbekämpande ändamål ska få behandlas även för att utvecklingsändamål. Personuppgifter som inledningsvis behandlas endast för utvecklingsändamål får inte behandlas för något annat ändamål.

Ett ändamål som tidigare inte omnämnts i någon personuppgiftsreglering för Säkerhetspolisen är utvecklingsverksamhet. Vi har ansett att denna del av Säkerhetspolisens verksamhet är viktig och bör regleras särskilt för att klargöra rättsläget och ge myndigheten möjlighet att inleda personuppgiftsbehandling för utvecklingsändamål. Uppgifter för utvecklingsändamål kan samlas in på olika sätt, exempelvis genom sociala medier. Det kan handla om uppgifter som behövs för utvecklingsändamål, men som saknar koppling till myndighetens brottsbekämpande uppdrag. Ändamålet kan exempelvis vara att förbättra en automatisk översättningstjänst. Se vidare avsnitt 8.4.6 och 6.2.6.

Eftersom ändamålet inte direkt behöver ha med Säkerhetspolisens brottsbekämpande uppdrag att göra, finns skäl att förtydliga att uppgifterna inte får behandlas för andra ändamål än teknisk utveckling. Vi anser att det är rimligt att begränsa användning av personuppgifter som samlats in för utvecklingsändamål på så sätt att de inte får behandlas för något annat ändamål. Detta förhindrar att inledande behandling för utvecklingsändamål övergår till en övervakning eller kartläggning av enskildas personliga förhållanden. Finalitetsprincipen

bör därför vara absolut avseende uppgifter som inledningsvis behandlats för utvecklingsändamål.

Det finns däremot ingen anledning att begränsa behandling av personuppgifter som samlats in för något brottsbekämpande ändamål i förhållande till teknisk utveckling. Att en personuppgift som samlats in för ett visst brottsbekämpande ändamål fortsätter att behandlas en tid även för att utveckla tekniska system framstår inte som ett tillkommande intrång i den personliga integriteten av betydelse. Finalitetsprincipen kan dock förhindra att uppgifter vidarebehandlas för att utveckla eller testa tekniska system, med en mer perifer koppling till det brottsbekämpande ändamålet för vilket uppgiften inledningsvis behandlats. Att vidarebehandling för utvecklingsändamål får ske utan hinder av finalitetsprincipen bör därför framgå direkt av lag.

8.9 Behandlingströskeln

8.9.1 Behovsprincipen måste uppfyllas

Behovsprincipen innebär ett krav på att en åtgärd ska vara effektiv för att uppnå det eftersträvade målet och att det inte heller ska vara möjligt att uppnå målet med mindre ingripande alternativ. Att denna princip uppfylls är en förutsättning för att det alls ska vara tillåtet att begränsa fri- och rättigheter.

När en säkerhetstjänst behandlar personuppgifter i olika former av register sker ett intrång i enskildas rätt till privat- och familjeliv och en sådan behandling innebär i princip en kartläggning av enskildas personliga förhållanden. Både svensk grundlag och Europakonventionen ställer därför upp krav på att Säkerhetspolisens personuppgiftsbehandling som utgör ett intrång i dessa grundläggande fri- och rättigheter ska vara motiverad av ett starkt vägande allmänintresse.

I regeringsformen är det uttryckt som att begränsningen av enskildas rätt till personlig integritet aldrig får gå utöver vad som är *nödvändigt* med hänsyn till det ändamål som har föranlett den och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen såsom en av folkstyrelsens grundvalar (2 kap. 21 § regeringsformen). I Europakonventionen uttrycks samma grundläggande princip som att begräsningen ska vara *nödvändig* med hänsyn till bland annat den nationella säkerheten.

Behovsprincipen utgör en grundläggande konstitutionell förutsättning för en lagstiftning inom detta område och kan anses följa direkt av proportionalitetsprincipen. Principen bör betraktas som det första steget som en behandling av personuppgifter måste uppfylla. Om den föreslagna åtgärden inte klarar kravet på att effektivt kunna uppnå ändamålet, finns det inget skäl av att undersöka dess proportionalitet. Behov är en nödvändig, men inte tillräcklig, förutsättning för proportionalitet.

8.9.2 Dataskyddskonventionens bestämmelser

Att personuppgiftsbehandling endast får ske om det är *nödvändigt* följer inte av dataskyddskonventionen utan begreppet har sitt ursprung i det EU-rättsliga dataskyddet. Det finns inte skäl att använda begreppet inom området för nationell säkerhet.

Behovsprincipen kommer inte till uttryck direkt av dataskyddskonventionen. Det finns inget krav enligt dataskyddskonventionen 108+ som anger att endast personuppgifter som krävs för att fullgöra en uppgift på ett effektivt sätt får behandlas. Konventionen uttrycker däremot att personuppgiftsbehandlingen inte får vara oproportionerlig i förhållande till ändamålen.

I det ligger givetvis att en personuppgift som inte är behövs för att på ett effektivt sätt utföra en uppgift inte är proportionerlig att behandla. Men även personuppgifter som kan vara nödvändiga för att i framtiden kunna lösa en uppgift eller som är nödvändiga för att kunna sätta andra uppgifter i sitt sammanhang skulle enligt vår uppfattning kunna anses proportionerligt att samla in och lagra en tid enligt en konventionstolkning av behovskriteriet.

8.9.3 Den nuvarande regleringen

Behovsprincipen i säpodatalagen kommer till uttryck genom att det i bestämmelsen om rättslig grund för personuppgiftsbehandling, 2 kap. 1 §, anges att personuppgifter får behandlas om det är *nödvändigt* för att utföra en av de uppgifter som anges där. Nödvändighetsrekvisitet innebär, enligt författningskommentaren, att personuppgiftsbehandlingen ska behövas för att uppgiften ska gå att fullgöra på ett effektivt sätt.

Nödvändighetsrekvisitet återkommer i flera andra bestämmelser. I 2 kap. 8 § anges att fler personuppgifter inte får behandlas än vad som är nödvändigt med hänsyn till ändamålet. Av 4 kap. 1 § följer att personuppgifter inte får behandlas längre än vad som är nödvändigt med hänsyn till ändamålet.

I den tidigare polisdatalagen användes begreppet *behövs* för att uttrycka principen att det krävs ett konkret behov av att utföra personuppgiftsbehandlingen och att detta behov ska svara mot ändamålet med behandlingen. I förarbetena till polisdatalagen angavs att om ändamålet med personuppgiftsbehandlingen är underrättelseverksamhet kan det till exempel vara nödvändigt att sammanställa uppgifter om vem som hyr vissa lokaler eller vem som äger eller disponerar fordon som man misstänker används i den brottsliga verksamheten. Det kan också handla om att klarlägga vilka personer som regelbundet besöker en viss plats där man misstänker att allvarlig brottslig verksamhet förekommer. I underrättelseprojekt som rör en viss typ av allvarlig brottslighet bör inte underrättelseuppgifter som helt saknar samband med just det aktuella projektet få behandlas.[69]

8.9.4 Utformningen av behovsprincipen ändrades genom säpodatalagen

Bedömning: Nödvändighetsrekvisitet har en särskild EU-rättslig innebörd.

Skälen för bedömning

I samband med implementeringen av EU:s dataskyddsdirektiv för brottsbekämpning ändrades begreppet ”behövs” till *nödvändig*, både i brottsdatalagen och säpodatalagen. Polismyndigheten och Säkerhetspolisen anmärkte i remissbehandlingen att begreppet nödvändigt framstod som mer begränsande i förhållande till det tidigare begreppet *behövs*. I förarbetena till brottsdatalagen konstaterade regeringen att begreppet nödvändigt enligt Svenska Akademiens ordbok innebär att någonting absolut fordras eller inte kan underlåtas. Det hänvisades

[69] Prop. 2009/10:85 s. 317 f.

dock till att ordet nödvändigt i brottsdatadirektivet får anses en självständig EU-rättslig betydelse som innebär att det är fråga om något som ”behövs för att på ett effektivt sätt kunna utföra arbetsuppgiften”.

En enhetlig terminologi mellan dataskyddsförordningen och de lagar som avsåg att genomföra brottsdatadirektivet framhölls som ett skäl i förarbetena till brottsdatalagen.[70] Samma motiv angavs i förarbetena till säpodatalagen: att skälen för en enhetlig begreppsapparat ansågs överväga skälen för att behålla det tidigare behovskriteriet. Det fick till följd att begreppet nödvändigt, med sin särskilda EU-rättsliga innebörd, kom att tillämpas även för Säkerhetspolisen. Detta trots att säpodatalagen avser att reglera den del av myndighetens personuppgiftsbehandling som utgör ett led i en verksamhet som inte omfattas av unionsrätten. Regeringen framhöll emellertid att det för Säkerhetspolisens del, trots att terminologin ändrats, inte var fråga om någon ändring i förhållande till kraven enligt polisdatalagen (2010:361) i detta avseende.[71]

Det kan enligt vår uppfattning ifrågasättas om regeringens intentioner att någon saklig ändring inte var avsett verkligen uppfyllts. Förarbetena till polisdatalagen, som återgetts ovan, ger sken av att behovet som avgränsar personuppgiftsbehandling i underrättelseprojekt avseende viss allvarlig brottslighet är sådana uppgifter som inte ”helt saknar samband” med det aktuella projektet. Sådana särskilda underrättelseprojekt får anses vara typiskt för Säkerhetspolisens underrättelseverksamhet och uttalandet i propositionen ger bilden av att behovet av att registrera en personuppgift enbart måste vara faktiskt, men inte nödvändigt. I författningskommentaren till säpodatalagen anges i stället att nödvändighetsrekvisitet innebär att personuppgiftsbehandlingen ska behövas för att uppgiften ska gå att fullgöra på ett effektivt sätt.[72]

Oavsett om denna ändring i sak har någon praktisk betydelse för Säkerhetspolisen, ger förarbetsuttalandena inte någon tydlig vägledning till begreppets innebörd. Det får även sägas vara något av en motsättning att ändra ett begrepp för att harmonisera det mot annan lagstiftning men samtidigt behålla en äldre innebörd av begreppet endast för Säkerhetspolisens verksamhet. Risken för att

[70] Prop. 2017/18:232 s. 117.
[71] Prop. 2018/19:163 s. 65.
[72] Ibid. s. 217.

begreppet även för Säkerhetspolisen kommer att få samma innebörd som motsvarande begrepp i de andra lagar där det används får sägas vara överhängande.

8.9.5 Behandlingströskeln bör ändras från *nödvändigt* till *behövs*

Förslag: Annan personuppgiftsbehandling än inledande behandling får ske, om det behövs för ändamålet med behandlingen.

Hur regleras behovsprincipen i andra lagar?

I den norska polisregisterlagen, som i stora delar är tillämplig för PST:s verksamhet, finns ett nödvändighetsrekvisit. I förordning till lagen finns föreskrifter om hur kravet på nödvändighet ska tillämpas. Där framgår att ”vad som ska anses nödvändigt beror på en konkret bedömning i det enskilda fallet”. Vidare anges att ”vid prövningen av vad som är nödvändigt ska en proportionalitetsbedömning göras där det bland annat ska läggas vikt vid syftet med behandlingen, vilka uppgifter som ska behandlas, om behandlingen avser grov eller mindre allvarlig brottslighet samt hur många personer som får tillgång till uppgifterna som behandlas”. I de övriga nordiska länderna finns exempel på att andra begrepp än vad som motsvarar innebörden av det svenska nödvändighetsrekvisitet används i personuppgiftslagstiftning för just säkerhetstjänster. I Danmark får säkerhetstjänsten PET samla in och inhämta personuppgifter som *kan ha betydelse* för verksamheten. När det gäller efterföljande behandlingsåtgärder, som lagring eller delning, är behovskriteriet för underrättelseverksamheten lägre än övrig verksamhet. För att förebygga och efterforska brott inom PET:s ansvarsområde, krävs att personuppgifterna *kan antas ha betydelse.* Inom andra verksamhetsgrenar, som exempelvis säkerhetsskydd, krävs i stället att personuppgifterna är *nödvändiga*. Även i Finland finns en uppdelning av behovskriteriet, men i stället för ändamålet med behandlingen är det typen av uppgift som avgör tröskeln. Skypo får behandla bland annat identifikationsuppgifter, uppgifter om medborgarskap, bosättningsort och anställning om det *behövs* för myndighetens uppdrag som civil säkerhetsunderrättelse-

tjänst. För mer integritetskänsliga uppgifter, om en persons resande, verksamhet och beteende, krävs att uppgifterna är *nödvändiga*, vilket är samma krav som för behandling av känsliga personuppgifter. För den finska polisens kriminalunderrättelseverksamhet, som även innefattar brott som rör nationell säkerhet, är behovskriteriet i underrättelseverksamheten beroende på vems personuppgifter som behandlas. Polisen i Finland får behandla personuppgifter inom underrättelseverksamheten avseende personer som *med fog kan antas* ha gjort sig eller göra sig skyldiga till brott och under vissa omständigheter även dennes kontakter. Kravet för personuppgiftsbehandling är lägre än vad som krävs för att inleda förundersökning (skäl att misstänka).

Det finns uppenbara fördelar med en enhetlig begreppsapparat för lagstiftningar som avser att reglera samma typ av verksamhet. Bland annat kan praxis utvecklas gemensamt för olika verksamheter vilket skapar en förutsebarhet och underlättar både tillsyn och samarbetet mellan olika myndigheter. Det får även anses vara ett ställningstagande från lagstiftaren att harmoniseringen mellan säpodatalagen och brottsdatalagen i detta och flera andra avseenden medger att EU-rätten, om än indirekt, gjorts tillämplig inom området nationell säkerhet. Om EU-domstolen uttolkar, exempelvis begreppet nödvändigt,[73] krävs det mycket starka skäl för att inte denna uttolkning ska anses gälla även för säpodatalagen. Detta trots att ändamålen som rör nationell säkerhet av naturliga skäl sällan kommer under EU-domstolens prövning och att medlemsstaterna har en stor bedömningsmarginal i vad som avses med dessa ändamål.

Begreppet nödvändigt har redan etablerats i olika personuppgiftslagstiftningar i Sverige. Även Försvarsmakten och FRA:s respektive datalagar, som i likhet med säpodatalagen inte genomför något EU-direktiv, använder detta begrepp. Att frångå nödvändighetsrekvisitet kräver därför starka skäl.

Det finns nackdelar med att nödvändighetsrekvisitet har en EU-rättslig innebörd

EU-rätten har ett mycket starkt inflytande över skyddet för personuppgifter inom de områden där unionen har lagstiftningskompetens. Det sker en kontinuerlig utveckling av dataskyddet genom EU-dom-

[73] Vilket skett i t.ex. mål C–175/20 angående den lettiska skattemyndighetens tillgång till personuppgifter i försäljningsannonser avseende personbilar grundat på allmänt intresse.

stolens praxis. Att tillämpa ett EU-rättsligt begrepp i en lagstiftning som i sin helhet är avsedd att ligga utanför unionsrätten kan innebära att rättsutvecklingen inom EU kan få oväntade, oönskade och svårförutsebara konsekvenser för Säkerhetspolisens verksamhet. Vi har tidigare framfört att den nuvarande säpodatalagens nära koppling till brottsdatadirektivet innebär att den avvägning mellan nationell säkerhet och andra intressen inte fullt ut kunnat prövas på nationell nivå. Det finns goda skäl till att medlemsstaterna har behållit exklusiv lagstiftningskompetens inom området som rör skyddet av nationell säkerhet. Den rättspraxis som kan komma att påverka innebörden av begreppet ”nödvändigt” kommer att utgå från en annan intresseavvägning än den som bör göras beträffande sådana hot som både till sin art och sitt allvar skiljer sig från brottslighet i allmänhet.

Nödvändighetsrekvisitet bör bytas ut till ett behovsrekvisit

Det finns skäl att i lagen beskriva att behovsprincipen ska tillämpas i varje enskilt fall av personuppgiftsbehandling. Frågan är om detta lämpligen sker genom att i likhet med nuvarande och angränsade personuppgiftslagstiftning ange att behandlingen ska vara *nödvändigt* för ett särskilt, uttryckligt angivet och berättigat ändamål?

Att begreppet *nödvändigt* motsvarar *behövs* kan alltjämt ifrågasättas rent språkligt. Att det finns behov av en åtgärd, exempelvis att lagra personuppgifter under viss tid, uttrycks lämpligen som att personuppgiftsbehandlingen behövs för att fullgöra en uppgift. Att ange att behandlingen ska vara nödvändig indikerar att det inte är tillräckligt att den behövs. Det är lätt att tolka nödvändighetsrekvisitet som att behandlingen måsta vara oundgänglig eller att uppgiften inte går att utföra utan att registrera personuppgiften i fråga. Så är sällan fallet, vare sig i Säkerhetspolisens verksamhet eller i verksamhet som regleras av andra personuppgiftslagstiftningar.

Målet att skydda nationell säkerhet kan motivera åtgärder som innebär mer långtgående ingrepp i de grundläggande rättigheterna. Behandlingströskeln för att överhuvudtaget få behandla personuppgifter inom en verksamhet som rör nationell säkerhet anser vi vara av så grundläggande betydelse att den bör formuleras så att den kan få en självständig betydelse på nationell nivå. Skälet till att Säkerhetspolisen har en egen lagstiftning för den verksamhet som ligger utan-

för EU-rätten är att denna verksamhet kan behöva anpassas och att avvägningarna inom denna verksamhet i stor utsträckning ska vila på nationella överväganden.

Vår slutsats är därför att skälen för att byta ut nödvändighetsrekvisitet och i stället återgå till ett behovsrekvisit överväger skälen mot att behålla det nuvarande begreppet. Vi anser därför att Säkerhetspolisen ska få behandla personuppgifter om det *behövs* för särskilda, uttryckligt angivna och berättigade ändamål.

8.9.6 Vad avses med *behövs*?

Det har inte framförts några skäl som talar för en betydligt lägre behandlingströskel än i dag. Säkerhetspolisen har givetvis inte behov av att behandla personuppgifter som inte krävs för att utföra sina arbetsuppgifter. Begreppet behövs bör därför tolkas på samma sätt som enligt den tidigare polisdatalagen.

I förarbetena till den lagstiftningen angavs att begreppet innebär att det ska finnas ett konkret behov av att behandla personuppgifterna. Det kan exempelvis finnas behov av att klarlägga vilka personer som regelbundet besöker en viss plats där man misstänker att allvarlig brottslig verksamhet förekommer. Uppgifter som inte behövs är sådana som helt saknar intresse för det aktuella ändamålet.[74]

Det övergripande ändamålet för underrättelseverksamheten är att kartlägga och klarlägga brottslig verksamhet. Även för ett mer specifikt underrättelseändamål, exempelvis att kartlägga en närmare angiven företeelse, kan uppgifter behövas på en mer aggregerad nivå. I dessa fall följer redan av ändamålet att behovet inte behöver prövas för varje uppgift för sig, utan kan avse ett visst avgränsat material i sin helhet. Hur en informationsmängd i dessa fall ska avgränsas bestäms både av det konkreta behovet och av proportionalitetsprövningen. En kartläggning får inte innebära ett oproportionerligt intrång i de enskilda eller allmänna intressen som påverkas oavsett vilket behov Säkerhetspolisen kan ha av behandlingen i fråga. Den närmare innebörden av ”behövs” behandlas vidare i författningskommentaren.

[74] Prop. 2009/10:85 s. 317 f.

8.10 Personuppgifters kvalitet

8.10.1 Dataskyddskonventionens bestämmelser

Artikel 5.4 i dataskyddskonventionen innehåller bestämmelser som rör personuppgifters kvalitet.

> **Article 5 – Legitimacy of data processing and quality of data**
>
> 4. Personal data undergoing processing shall be:
>
> c. adequate, relevant and not excessive in relation to the purposes for which they are processed;
>
> d. accurate and, where necessary, kept up to date;

De krav som ställs upp i artikel 5 c är välbekanta inom europeisk dataskyddsrätt och innebär att personuppgifter ska vara adekvata, relevanta och inte onödigt omfattande i förhållande till de ändamål för vilka de behandlas. Denna bestämmelse brukar sammanfattas som principen om uppgiftsminimering.

I kommentaren till konventionen förklaras att kravet på att uppgifterna inte får vara onödigt omfattande innebär att behandlingen ska begränsas till vad som är nödvändigt för ändamålet. Personuppgiftsbehandling får bara ske om ändamålen inte rimligen kan uppfyllas genom att behandla information som inte utgör personuppgifter. Dessutom är kravet att uppgifterna inte får vara onödigt omfattande inte endast kvantitativt utan även kvalitativt. Proportionalitetsprincipen innebär att behandling av personuppgifter som i och för sig är adekvata och relevanta inte får ske om behandlingen skulle innebära ett oproportionerligt ingrepp i de grundläggande fri- och rättigheter som står på spel.[75]

Av punkten d framgår att uppgifter också ska vara korrekta och uppdaterade. Detta är ett krav som följer även av det EU-rättsliga personuppgiftsregelverket.

[75] *Explanatory Report – CETS 223 – Automatic Processing of Personal Data (Amending Protocol)*, p. 52.

8.10.2 Uppgiftsminimering

Bedömning: Regleringen om uppgiftsminimering bör justeras för att stämma bättre överens med dataskyddskonventionens krav.

Förslag: Personuppgifter som behandlas ska vara adekvata, relevanta och inte för omfattande i förhållande till ändamålet med behandlingen.

Adekvans och relevans

Den nuvarande regleringen

Dagens regelverk om personuppgifters kvalitet bygger i stor utsträckning på det som gäller enligt brottsdatadirektivet och den tidigare polisdatalagen.

När det kommer till adekvans och relevanskravet i nuvarande 2 kap. 8 § säpodatalagen angavs i förarbetena att det kan vara svårare att bedöma vilka uppgifter som är adekvata och i Säkerhetspolisens verksamhet än i annan polisverksamhet. Detta eftersom det som regel inte är lika tydligt vari den brottsliga verksamheten eller säkerhetshotet består. Vidare ansåg regeringen att det i vissa fall kan vara motiverat att utsträcka adekvans och relevans till personuppgifter som inte behövs för ändamålet, för att inte avslöja vem eller vilka personer som myndigheten intresserar sig för i sitt underrättelsearbete.[76]

Det finns inte skäl att ändra på nuvarande ordning

Det har inte framgått att kravet på att personuppgifter ska vara adekvata och relevanta för ändamålet med behandlingen medför tillämpningsproblem eller utgör ett otillräckligt personuppgiftsskydd. Principerna är viktiga för att markera att onödiga uppgifter inte får behandlas. Hur kraven på adekvans och relevans tillämpas beror på vilket ändamål som prövningen ska göras mot. Hur ändamålet formuleras är avgörande för bedömningen av vilka uppgifter som är relevanta att behandla. Ett vagt ändamål medger inte någon reell präv-

[76] Prop. 2018/19:163 s. 74 f.

ning. För att det ska vara möjligt att bedöma vilka uppgifter som får behandlas för ett ändamål krävs ett visst mått av konkretion och specifikation. Därmed är reglerna om adekvans och relevans även avgörande för det krav som ställs på ett ändamål. Ändamålet måste nämligen vara tillräckligt konkret för att det ska vara möjligt göra bedömningen.[77]

Om ett ändamål för behandling av personuppgifter är att kartlägga en viss företeelse är bedömningen av vilka uppgifter som är relevanta och adekvata en annan än om behandlingen sker för att exempelvis utreda ett brott. En viktig princip i nuvarande lag, som alltjämt bör gälla, är att Säkerhetspolisen måste kunna redogöra för på vilket sätt uppgifter som behandlas är relevanta och adekvata för ändamålet. Vi har därmed inte funnit skäl att ändra på nuvarande ordning. Det bör alltjämt ställas krav på att de personuppgifter som behandlas ska vara relevanta och adekvata i förhållande till ändamålet.

Inte för ”omfattande” eller ”inte fler” uppgifter?

Den nuvarande regleringen

I 2 kap. 8 § säpodatalagen framkommer vid sidan av kraven på att uppgifter ska vara adekvata och relevanta för ändamålet även, i andra meningen, att inte fler uppgifter än vad som är nödvändigt får behandlas. I säpodatalagen, men även i brottsdatalagen, har bestämmelsen om att inte fler uppgifter än nödvändigt får behandlas närmast ansetts utgöra en konsekvens av adekvans och relevanskravet. Om endast de relevanta och adekvata uppgifterna behandlas framstår det som att det tillkommande kravet på att inte fler uppgifter än nödvändigt får behandlas sällan får någon självständig betydelse. I förarbetena nämns däremot undantagen från principen. Det har ansetts tillåtet att samla in fler uppgifter än avseende misstänkta personer för att inte avslöja myndighetens intresse för dem.[78]

Bestämmelsen, om att inte *fler* uppgifter än vad som är nödvändigt med hänsyn till ändamålet, återfinns även i brottsdatalagen. Det kan anmärkas att både brottsdatadirektivet och dataskyddsförordningen har en annan formulering av principen om uppgiftsminimering. I dessa rättsakter anges att personuppgifter som behandlas inte får vara för

[77] Prop. 2018/19:163 s. 67.
[78] Ibid. s. 74 f.

omfattande i förhållande till ändamålet. Motsvarande lydelse följer även av det föregångaren till dataskyddsförordningen, det så kallade dataskyddsdirektivet från 1995. Direktivet implementerades genom personuppgiftslagen (1998:204) där direktivets begrepp ”inte för *omfattande*” byttes ut till ”inte *fler*”. Det finns inte några motiv till denna ändring som förefaller vara av språklig natur. Som framgår av dataskyddskonventionen 108+ artikel 5 c, som citerats ovan, används det engelska begreppet ”not excessive” för att beskriva principen om uppgiftsminimering. Samma begrepp används i de engelska språkversionerna av brottsdatadirektivet och dataskyddsförordningen, som alltså översatts till ”inte för omfattande”.

Kravet på uppgiftsminimering bör anpassas till dataskyddskonventionen

Den något justerade lydelsen av principen om uppgiftsminimering i svensk rätt, i förhållande till den som används inom den europeiska personuppgiftsrätten kan få viss betydelse. I kommentaren till dataskyddskonventionen, som i och för sig inte har någon formell rättslig status, förklaras att principen om uppgiftsminimering inte endast är ett kvantitativt krav. Det finns även en kvalitativ aspekt av att de personuppgifter som behandlas inte får vara onödigt omfattande i förhållande till ändamålet. Detta får anses vara en naturlig följd av att det kan göras skillnad i det intrång som behandling av olika slags personuppgifter innebär för enskilds fri- och rättigheter. Den kvalitativa aspekten innebär att mer integritetskänsliga uppgifter inte får behandlas om det är tillräckligt att behandla mindre känsliga uppgifter för ändamålet.

Mot bakgrund av det krav som vi uppfattar att datakonventionen 108+ innebär kan det finnas skäl att förändra det begrepp i den föreslagna lagen som ska motsvara ”not excessive”. Det finns flera möjliga översättningar. I den svenska språkversionen av både dataskyddsförordningen och brottsdatadirektivet översätts begreppet emellertid med ”inte för omfattande”. Detta begrepp får anses spegla dataskyddskonventionens artikel 5 c på det mest korrekta sättet och det finns ett uppenbart mervärde i en konsekvent översättning av utländska begrepp med samma betydelse. Det finns därför skäl att justera lydelsen av principen om uppgiftsminimering i den del som

framgår i nuvarande 2 kap. 8 § andra meningen säpodatalagen på så sätt att *inte fler* ska ersättas av *inte för omfattande*.

Uppgiftsminimering kan påverka proportionalitetsbedömningen

Kravet på att personuppgifterna inte får vara för omfattande gäller även sådana uppgifter som i och för sig är adekvata och relevanta för ändamålet. Huruvida uppgifterna är för omfattande eller inte beror på ändamålet med behandlingen.

Uppgifter som får behandlas för vissa ändamål kan vara för omfattande för andra. Både antalet och arten av uppgifter påverkar också proportionalitetsprövningen. Uppgiftsminimering utgör ett verktyg för att uppnå proportionalitet och det är därför inte endast behovet av uppgiften som ska prövas. Den ändrade lydelsen av principen om uppgiftsminimering är därmed inte endast språklig. För att uppnå proportionalitet kan krävas uppgiftsminimering; både genom att de mest integritetskänsliga uppgifterna raderas och genom att ett färre antal uppgifter behandlas.

8.10.3 Korrekta och uppdaterade uppgifter

Bedömning: Den nuvarande bestämmelsen om hur en persons utseende ska beskrivas följer redan av kraven på författningsenlig och korrekt behandling samt kraven på adekvans och relevans. Den nuvarande regleringen bör därför inte överföras till den nya lagen.

Förslag: Kravet på att personuppgifter som behandlas ska vara korrekta och om nödvändigt uppdaterade ska överföras till den nya lagen.

Den nuvarande regleringen

Kravet på korrekta och uppdaterade uppgifter följer av nuvarande 2 kap. 7 § första stycket säpodatalagen. Av andra stycket framgår ett ytterligare krav; att signalement ska utformas på ett objektivt sätt med respekt för människovärdet.

När det gäller kravet på korrekta och uppdaterade uppgifter framgår av förarbetena att det kan skilja sig mellan olika ändamål. Personuppgifter som behandlas i brottsanmälan får exempelvis betraktas som korrekta, om de stämmer överens med de inkomna uppgifterna oavsett hur de förhåller sig till de verkliga förhållandena. Uppgifter i underrättelseflödet får på samma sätt anses korrekta om de återger vad som inkommit även om det senare visar sig inte stämma överens med verkligheten. Om uppgifter måste hållas uppdaterade beror också på för vilket ändamål de behandlas. I ärenden kan det exempelvis finnas behov av att uppdatera kontaktuppgifter så länge handläggningen pågår.[79]

Bestämmelsen som anger att uppgifter som beskriver en persons utseende ska utformas på ett objektivt sätt med respekt för människovärdet överfördes från polisdatalagen och har inte sin grund i brottsdatadirektivet. Bestämmelsen infördes ursprungligen i lagen (2001:85) om behandling av personuppgifter i Tullverkets brottsbekämpande verksamhet. Det framstår, enligt den lagens förarbeten, som att bestämmelsen var ett svar på Diskrimineringsombudsmannens farhågor om hur känsliga personuppgifter, särskilt avseende ras och etnicitet, kunde komma att användas som signalement i tullens verksamhet. Syftet med bestämmelsen är att förhindra att personer allmänt beskrivs i förklenande ordalag som kan anses kränkande för individen, särskilt då känsliga personuppgifter används som signalement.[80]

Kravet på korrekta och uppdaterade uppgifter ska överföras till den nya lagen

Att uppgifter ska vara korrekta och om nödvändigt hållas uppdaterade kan vara viktiga för enskildas rätt. Det är exempelvis viktigt att uppgifter som kan ha betydelse vid den registerkontroll som ska utföras vid en säkerhetsprövning är korrekta.

Det finns även i övrigt skäl för att uppgifter som på något sätt kan vara kompromet terande för den enskilde ska vara korrekta. Det kan även innebära att uppgifter måste uppdateras för att motsvara förändrade förhållanden.

Bestämmelserna har till syfte att skydda enskildas personliga integritet. Om korrekta och uppdaterade uppgifter behövs eller inte

[79] Ibid. s. 73 f.
[80] Prop. 2004/05:164 s. 68 och 118.

för verksamheten, är därför av underordnad betydelse. Det saknas skäl att göra undantag från kraven i dataskyddskonventionen 108+ om korrekta och uppdaterade uppgifter. Den nuvarande bestämmelsen bör därför överföras till den nya lagen.

De särskilda bestämmelserna om signalement bör inte regleras särskilt

När det kommer till den särskilda och särpräglade bestämmelsen som avser hur en persons utseende ska beskrivas kan integritetsnyttan i viss mån ifrågasättas. Det får sägas vara en självklarhet inom svensk förvaltning att en persons utseende beskrivs objektivt och med respekt för människovärdet. Detta framgår även av 1 kap. 9 § regeringsformen och 5 § förvaltningslagen (2017:900). Bestämmelsen i den nuvarande säpodatalagen kan felaktigt ge bilden av att denna självklarhet inte skulle gälla om regeln inte fanns. Å andra sidan har en motsvarande bestämmelse införts för alla andra brottsbekämpande myndigheter. Att ta bort denna regel för Säkerhetspolisens del skulle kunna misstolkas och som upplysning för allmänheten kan regeln måhända ha sitt värde.[81]

Bestämmelsen är inte anpassad för Säkerhetspolisens uppdrag och utgör, enligt vår bedömning, en regel som gör lagen mer komplex utan att tillföra uppenbar integritetsnytta. Om Säkerhetspolisen beskriver en persons utseende ska det, enligt allmänna rättsgrundsatser inom svenska förvaltningsrätt ske på ett objektivt sätt och med respekt för människovärdet. Den nuvarande regleringen kan också medföra tillämpningsproblem. Det kan exempelvis handla om att Säkerhetspolisen avlyssnar ett samtal mellan personer i en kriminell miljö där en persons utseende beskrivs helt utan respekt för dennes människovärde. Sådana beskrivningar ska återges korrekt och inte anpassas efter denna bestämmelse. Om myndigheten får till sig en beskrivning av någons utseende, vilket inte alls är ovanligt, bör det inte ställas särskilda krav på tillrättalägganden i efterhand för att få behandla uppgiften.

Sammantaget anser vi att skälen som talar för att inte överföra det särskilda kravet på signalementsuppgifter överväger. Det följer av bland annat av kraven på korrekt personuppgiftsbehandling och

[81] Jfr prop. 2011/12:45 s. 95 f.

att personuppgifter ska vara adekvata för ändamålet att beskrivningar som Säkerhetspolisen själv är ansvarig för sker på ett objektivt sätt med respekt för människovärdet. Någon ändring i sak är därför inte avsedd.

8.11 Det nuvarande begreppet gemensamt tillgängliga uppgifter ska inte användas i den nya lagen

8.11.1 Den nuvarande regleringen är svårmotiverad

Vi redogör för innebörden och bakgrunden till den särskilda regleringen av gemensamt tillgängliga uppgifter i avsnitt 3.5.6.

Begreppet gemensamt tillgängliga uppgifter omfattar alla personuppgifter som fler än endast ett fåtal personer har eller kan komma att få åtkomst till över tid. Ett fåtal personer utgörs enligt förarbetena av ett tiotal medarbetare som har eller kan komma att få tillgång till uppgifterna över tid. Nuvarande lagstiftning är uppbyggd kring uppdelningen av uppgifter mellan de som är gemensamt tillgängliga och de som inte är det.

Inom Polismyndigheten bedrivs underrättelseverksamhet vid särskilda enheter med särskilt utbildade tjänstemän (se avsnitt 3.6.1). I propositionen till polisdatalagen uttalade regeringen att det är en naturlig del i underrättelsearbete att begränsa antalet tjänstemän som får del av viss information, till exempel när man kartlägger organiserad eller annan allvarlig brottslighet. Det innebär allmänt sett en risk att sprida uppgifter av underrättelsekaraktär till en vidare krets. För Polismyndighetens del har tillämpningen av reglerna som rör icke gemensamt tillgängliga personuppgifter exemplifierats som mindre underrättelseprojekt bestående av ett fåtal på förhand utpekade personer eller funktioner.

Säkerhetspolisens uppdrag, organisation och verksamhet innebär att det i praktiken inte är möjligt att begränsa kretsen av medarbetare som över tid har tillgång till underrättelseinformation till endast ett fåtal personer. I myndighetens verksamhet samarbetar ofta flera avdelningar och medarbetare måste kunna bytas ut över tid för att upprätthålla kontinuiteten i underrättelsearbetet. Det innebär att i stort sett samtliga personuppgifter behandlas som gemensamt till-

gängliga inom myndigheten från det att uppgifterna samlats in. Informationsinflödet är vidare så stort att det är svårt att med någon rimlig effektivitet begränsa åtkomsten till uppgifter som inte har bearbetats till endast ett tiotal personer. Bedömningen av relevanta tips och annan information förväntas ske dygnet runt alla årets dagar, vilket kräver en robust grundbemanning.

Säpodatalagen innehåller inte heller, till skillnad mot Polisens brottsdatalag, några begränsningar av vilka uppgifter som får göras gemensamt tillgängliga. Av 3 kap. 2 § följer att personuppgifter får göras gemensamt tillgängliga, om det behövs för att utföra någon av de uppgifter som angetts om rättslig grund. De intressen som Säkerhetspolisen har till uppgift att skydda ansågs motivera att Säkerhetspolisen skulle ges större handlingsfrihet i fråga om vilka uppgifter som får behandlas. Enligt regeringen talade verksamhetens särdrag för att de begränsningar som gäller för Polismyndigheten för att göra uppgifter gemensamt tillgängliga inte bör gälla för Säkerhetspolisen. I samma riktning ansågs svårigheten att förutse och i lag uttrycka de olika kategorier av personuppgifter som bör få göras gemensamt tillgängliga hos Säkerhetspolisen. Säkerhetspolisens verksamhet bedömdes till sin natur vara sådan att informationen sprids i mindre utsträckning än inom Polismyndigheten, vilket minskar risken för otillbörliga intrång i den personliga integriteten, trots att uppgifter kan användas av flera gemensamt.[82]

8.11.2 Begreppet gemensamt tillgängliga uppgifter bör inte användas i säpodatalagen

Bedömning: Den nya lagen bör inte innehålla särskilda regler som bygger på om personuppgifter är gemensamt tillgängliga eller endast tillgängliga för ett fåtal medarbetare.

Skälen för bedömning

Dagens säpodatalag bygger på principen att uppgifter antingen är gemensamt tillgängliga eller behandlas endast av ett fåtal personer. Att en uppgift är gemensamt tillgänglig har ansetts innebära en

[82] Prop. 2009/10:85 s. 264 och prop. 2018/19:163 s. 87.

förhöjd risk för att uppgiften missbrukas och ett större integritetsintrång. Tanken är därför att endast viss operativ information som har ett värde för en större del av organisationen ska behandlas i brett tillgängliga system, i vilka det ska vara säkerställt att endast uppgifter som uppfyller alla lagens krav behandlas. Som konstaterats ovan har uppdelningen mellan gemensamt tillgängliga uppgifter och uppgifter som endast ett fåtal personer har rätt att ta del av inte någon egentlig funktion för Säkerhetspolisen. Alla uppgifter får göras gemensamt tillgängliga och det finns mycket få, om ens några, uppgifter som endast är tillgängliga för de tiotal personerna som anses utgöra ett fåtal enligt bestämmelsen.

Det innebär dock inte att alla uppgifter faktiskt är tillgängliga för hela Säkerhetspolisens organisation. Tvärtom finns det antagligen få myndigheter som har lika strikta begränsningar gällande vilken information enskilda medarbetare har tillgång till och där uppföljningen av sökningar och slagningar i register sker lika noggrant. Dessa system är givetvis motiverade främst av informationssäkerhetsskäl hos Säkerhetspolisen, som har en mycket hög medvetenhet om riskerna som kan följa av att känsliga uppgifter sprids. Säkerhetspolisens verksamhet är till sin natur mer sluten än Polismyndighetens vilket, som regeringen konstaterade redan i samband med att reglerna infördes, innebär att risken för spridning och otillbörligt intrång i den personliga integriteten är mindre.

En av de principer som den nya lag vi föreslår ska följa är att vi inte ser något värde av regler som gör systemet mer komplext utan att vara påtagligt integritetshöjande. Vi har därför inte sett något större värde av att till en ny lag överföra det relativt komplexa systemet med uppdelningen av uppgifter som är gemensamt tillgängliga och endast tillgängliga för en handfull personer. Den ursprungliga tanken med att vissa uppgifter kan hanteras med lättnader i personuppgiftsregleringen så länge de endast är åtkomliga för ett fåtal personer har sedan länge spelat ut sin roll inom Säkerhetspolisens verksamhet. Det är inte heller möjligt att använda sig av ett fåtal personer för att granska om inkomna uppgifter är tillåtna att behandla. När uppgifter kommer in till Säkerhetspolisen kräver grundbearbetning och kvalitetssäkring av inkomna uppgifter normalt att en betydligt större arbetsgrupp har åtkomst till uppgifterna över tid för att den ska kunna ske tillräckligt effektivt. Se avsnitt 6.1.2.

Vi har övervägt att förändra det nuvarande systemet genom att ändra definitionen av när uppgifter ska anses vara åtkomliga för en mindre grupp medarbetare.[83] Den nuvarande regleringen om ett tiotal personer bygger emellertid på avvägningar avseende hur många personer som kan ha tillgång till information för att integritetsintrånget ska anses vara acceptabelt för behandling av uppgifter vars kvalitet inte ännu kunnat fastställas. Genom att utöka denna krets till en större enhet inom Säkerhetspolisen skulle syftet med begränsningen ändå inte uppfyllas. En lagstiftning som innebär en uppdelning mellan uppgifter som finns tillgängliga gemensamt och uppgifter som finns tillgängliga för ett femtiotal eller ett hundratal anställda vid en viss enhet fyller inte motsvarande funktion som det nuvarande begreppet är avsett för. Enligt förarbetena gör sig de integritetsskyddsintressen som motiverar särskilda regler för gemensamt tillgängliga uppgifter inte lika starkt gällande när bara ett fåtal personer har tillgång till uppgifterna som när många personer har tillgång till dem.[84]

Vi har sammantaget inte kunnat finna tillräckliga skäl för att dela in personuppgifter på samma sätt som gjorts tidigare med vissa lättnader för uppgifter som är tillgängliga för ett mindre antal. I stället anser vi att Säkerhetspolisen genom tekniska och organisatoriska åtgärder, som i dag, ska se till och kunna visa att tillgången till personuppgifter begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Det finns dock ett klart integritetshöjande värde av att uppgifter som kommer in till myndigheten granskas innan de görs brett tillgängliga operativt. Vi anser därför att den inledande granskningen och kvalitetssäkringen av uppgifter ska hanteras genom en ny, särskild och tydlig reglering som är avsedd för just detta.

[83] Jfr Polismyndigheten skrivelse den 5 juli 2024, *Hemställan om ändring av bestämmelserna om gemensamt tillgängliga uppgifter i lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område*, dnr A286.201/2024.
[84] Prop. 2009/10:85 s. 128.

8.12 Den inledande granskningen av insamlade personuppgifter

8.12.1 Olika krav på insamling och vidarebehandling

Vi har i avsnitt 8.6 lämnat förslag om att insamling och annan inledande behandling ska regleras på ett sätt som bättre motsvarar Säkerhetspolisens behov och faktiska verksamhet. Principen bakom förslaget är att behandling av personuppgifter i underrättelseverksamhet måste kunna ske på ett annat sätt än för andra verksamheter; bland annat genom att uttryckligen tillåta insamling av okänd information. Den reglering vi föreslår är att Säkerhetspolisen ska få inleda behandling av personuppgifter som är befogade för ett brett formulerat ändamål.

I avsnitt 8.7 lämnar vi förslag om att annan personuppgiftsbehandling än inledande behandling ska få ske för särskilda och uttryckligt angiva ändamål och i avsnitt 8.9 att uppgifterna ska behövas för detta, mer specifika ändamål. I avsnitt 8.10 lämnar vi förslag om att personuppgifter som behandlas ska vara förenliga bland annat med principen om uppgiftsminimering. I avsnitt 8.6.7 konstaterar vi att detta krav dock inte är möjligt att upprätthålla vid inledande behandling.

Det ställs därmed helt andra krav när personuppgiftsbehandlingen inleds, genom att uppgifter exempelvis samlas in jämfört med när de ska fortsätta att behandlas, genom att till exempel lagras i en databas.

Enligt såväl dataskyddskonventionen som det nuvarande och tidigare EU-rättsliga regelverket får personuppgifter endast *samlas in* för särskilda, uttryckligt angivna och berättigade ändamål.[85] Därefter får uppgifterna inte behandlas på ett sätt som står i strid med de ändamål för vilka de samlats in. Det finns inte någon uttrycklig reglering att insamlade uppgifter ska granskas mot insamlingsändamålet, eller något sekundärt ändamål, i förhållande till adekvans, relevant och principen om uppgiftsminimering. Underförstått finns det dock ett krav på granskning av att de insamlade personuppgifter uppfyller förutsättningarna för att få behandlas.

I den ursprungliga dataskyddskonventionen från 1981 ingår inte insamling i begreppet personuppgiftsbehandling, och kraven på

[85] Artikel 5.4.b dataskyddskonventionen 108+, artikel 5.1.b dataskyddsförordningen, artikel 4.1.b brottsdatadirektivet.

uttryckligt ändamål och uppgiftsminimering gäller de insamlade uppgifter som bevarades.

Article 5 – Quality of data

Personal data undergoing automatic processing shall be:

a) obtained and processed fairly and lawfully;

b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes;

c) adequate, relevant and not excessive in relation to the purposes for which they are stored;

d) accurate and, where necessary, kept up to date;

e) preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

Genom systematiken i dataskyddskonventionen framgår kraven som gäller för behandling av personuppgifter i en tydligare kronologi. Dataskyddskonventionen 108+ har behållit uppräkningen i denna ordning, men justerat kraven i vissa delar. Som framgått i bland annat avsnitt 8.6.1 ställer den moderniserade konventionen upp krav på att insamling ska ske för särskilda ändamål och kraven på författningsenlig och korrekt behandling gäller all behandling.

Principerna bakom säpodatalagen är desamma som i bland annat brottsdatalagen och innebär att personuppgifter endast får behandlas om de, under alla skeden av behandlingen, uppfyller lagens krav. Det innebär i teorin att ingen personuppgift får samlas in eller tas emot om den inte följer kraven på adekvans och relevans eller om den utgör en känslig personuppgift som inte är absolut nödvändig. Det innebär att det finns ett krav för att uppgifter ska få behandlas som inte går att kontrollera utan att de först behandlas.

Det faller sig mer naturligt, sett till uppbyggnaden av regelverket, att det finns ett krav på efterföljande granskning av insamlade uppgifter när insamling av uppgifter är särreglerat i förhållande till fortsatt lagring och andra former av personuppgiftsbehandling. Vi anser att det finns skäl att överväga att särskilt reglera granskningsförfarandet som följer på den inledande behandlingen.

8.12.2 Den nuvarande regleringen av inledande granskning

I avsnitt 6.1.2–6.1.4 redogörs för Säkerhetspolisens nuvarande arbetssätt avseende inledande granskning och tillgängliggörande av uppgifter i centrala register.

Enligt nuvarande ordning måste alla personuppgifter i ett tidigt skede granskas av någon som kan pröva om behandlingen är förenlig med säpodatalagen. Detta följer av 2 kap. 14 § säpodatalagen som anger att alla rimliga åtgärder ska vidtas för att personuppgifter som behandlas i strid med bestämmelser om rättslig grund, ändamål, kravet på adekvans och relevans eller är onödigt omfattande i förhållande till ändamålet *utan onödigt dröjsmål* ska raderas. Detsamma gäller känsliga uppgifter som inte är absolut nödvändiga för ändamålet med behandlingen.

Uppgifter som är gemensamt tillgängliga ska enligt 3 kap. 3 och 4 §§ säpodatalagen förses med särskilda upplysningar i vissa fall. Det finns dock, i 3 kap. 4 § tredje stycket, ett undantag för särskilda upplysningar om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak för uppgifter som ingår i en uppgiftssamling som har skapats för att bearbeta och analysera information. En sådan *uppgiftssamling för bearbetning och analys* får endast var åtkomlig för särskilt angivna tjänstemän och undantaget gäller så länge bearbetning av uppgifterna inte har genomförts.

Behovet av att behandla känsliga personuppgifter prövas särskilt och utgör en grannlaga uppgift. Känsliga personuppgifter som inte får behandlas tas bort genom maskning. Därefter bearbetas informationen genom att uppgifterna bryts ut och länkas samman med annan information, tematiseras och tillförs särskilda upplysningar om det krävs. Under bearbetningen i uppgiftssamlingen för bearbetning och analys behöver någon särskild upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak inte anges. Enheten som utför granskningen består dock av fler än ett fåtal personer och andra särskilda upplysningar, om ändamål och misstanke, förutsätts därför vara tillfogade personuppgifter under bearbetningen. När bearbetningen är klar kan uppgifterna föras över till uppgiftssamlingen med bedömd information eller tas bort. Enligt 4 kap. 8 § säpodatalagen får personuppgifter som behandlas i en uppgiftssamling för bearbetning och analys inte behandlas längre

än tre år efter utgången av det kalenderår då den senaste registreringen gjordes avseende personen.

Hur lång tid Säkerhetspolisen har på sig att bedöma om en uppgift ska raderas eller fortsätta att behandlas följer varken av lagen eller omnämns i något uttalande i förarbeten. När det gäller överskottsinformation från hemliga tvångsmedel uttalas dock att det är först när informationen är möjlig att ta del av, efter exempelvis teknisk bearbetning eller översättning, som någon faktisk granskning kan påbörjas. Kravet på att material som härrör från hemliga tvångsmedel och som är ovidkommande ska tas bort så snabbt som möjligt måste därför ses i ljuset av möjligheterna att på ett tidigt stadium kunna bedöma värdet av informationen.[86]

8.12.3 Det behövs tydligare regler för inledande granskning och behandling av insamlade personuppgifter

Bedömning: Initialgranskning av information som innehåller personuppgifter bör regleras. Det bör uttryckligen anges att det är tillåtet för Säkerhetspolisen att behandla information innan den hunnit granskas.

Eftersom vårt förslag på ny säpodatalag ställer olika krav för inledande och behandling måste glappet mellan kraven fyllas med någon form av granskningsfunktion. Syftet är att sålla och filtrerar bort den information som inte når upp till de strängare kraven för fortsatt behandling. Insamling, bearbetning och analys av information utgör Säkerhetspolisens kärnverksamhet. Det är därför lämpligt att det finns ett tydligt rättsligt ramverk för personuppgiftsbehandlingen under alla stegen i underrättelseprocessen; både för att myndigheten kunna utföra sina uppgifter på ett effektivt sätt och för att säkerställa tillräckligt skydd för personuppgifter.

Det finns flera olika sätt att hantera insamlad information i syfte att utföra personuppgiftsgranskning. Försvarsmakten och FRA har i sin lagstiftning en särskild regel som medger att uppgifter får behandlas innan de kunnat granskas. Av 2 kap. 18 § i FRA-datalagen respektive 2 kap. 20 § försvarsdatalagen framgår att hantering av information inte ska anses oförenlig med bestämmelserna om tillåt-

[86] Prop. 2018/19:163 s. 75.

lighet, grundläggande krav, känsliga personuppgifter och personnummer, i det skede av behandlingen då det ännu inte har kunnat fastställas vilka personuppgifter som informationen innehåller. Bestämmelsen var, för FRA:s del, en förutsättning för verksamheten. Regeringen konstaterade att det även för Försvarsmakten kunde finnas skäl att medge automatiserad hantering av uppgifter innan en manuell bedömning av dem kan göras.[87] Bestämmelsen för Försvarsmakten genomfördes trots att Lagrådet kritiserade bestämmelsens generösa utformning, särskilt att undantaget omfattar även ändamålet med personuppgiftsbehandling.[88]

Bestämmelsen i FRA och Försvarsmaktens personuppgiftslagar medger att myndigheterna bevarar information och successivt bedömer personuppgifternas förenlighet med respektive myndighets personuppgiftslag i samband med att uppgifterna granskas för första gången. Sådan granskning utförs därmed inte av en särskild enhet utan löpande av personal inom de olika verksamhetsgrenarna. Det finns inte någon särskild tidsgräns angiven för behandling enligt nämnda paragrafer.

Behovet att samla in och analysera allt större informationsmängder i den operativa verksamheten samtidigt som lagens krav på personuppgiftsbehandling upprätthålls är något som många underrättelsetjänster brottas med. I Danmark har säkerhetstjänsten PET under flera år kritiserats av tillsynsmyndigheten för att uppgifter som inhämtats eller insamlats sparas längre än de fyra veckor som är föreskrivet. Frågan togs även upp när det i Finland skulle beslutas om en ny personuppgiftslag, som omfattade bland annat underrättelsetjänsten Skypos verksamhet. I regeringens proposition fanns ett förslag om en inledande granskningsfrist om sex månader för att bedöma om uppgifter som samlats in kan ha betydelse för något ändamål. Denna bestämmelse föll emellertid i Grundlagsutskottet behandling av lagförslaget. Grundlagsutskottet ansåg att den föreslagna regleringen stred mot brottsdatadirektivet och endast kunde tillåtas till den del lagen faller utanför unionsrättens tillämpningsområde, till exempel när det gäller den nationella säkerheten. För att kunna medge en särskild granskningsfrist för grundbearbetning för Skypo, som i praktiken medgav insamling av uppgifter i strid med ändamålsprincipen, krävdes dock enligt utskottet att lagen

[87] Se prop. 2020/21:224 s. 95–96.
[88] Ibid. s. 320 (bilaga 8).

stiftades enligt den i Finland föreskrivna ordningen för grundlagsändring.

Säkerhetspolisen måste hantera stora mängder information på ett strukturerat sätt för att bygga upp de underrättelsesystem som behövs i den operativa verksamheten. Den tekniska utvecklingen innebär att det är möjligt att automatisera informationshanteringen i större utsträckning än tidigare. I verksamheten kan ostrukturerad information användas i betydligt högre grad genom komplexa sökningar och sammanställningar. Sådan teknik ersätter delvis behovet av person- och sakakter för att kunna ta del av information på ett strukturerat sätt. Oavsett hur information tekniskt hanteras, kvarstår emellertid kravet på att personuppgiftsbehandling inom Säkerhetspolisen måste uppfylla de grundläggande kraven som ställs upp i lagstiftningen.

De ovillkorliga krav som uppställs i dataskyddskonventionen är bland annat att personuppgiftsbehandling ska ske för ett berättigat ändamål, vara proportionerlig samt att den ska vara författningsenligt och korrekt. Till detta kommer regeringsformens krav på att personuppgiftsbehandling som innebär ett betydande intrång i den personliga integriteten måste tillgodose ändamål som är godtagbara i ett demokratiskt samhälle och inte går utöver vad som är nödvändigt med hänsyn till det ändamål som föranlett behandlingen. Prövning av bland annat proportionalitet och legitimitet får sitt närmare innehåll genom personuppgiftslagstiftningen. Denna bedömning är dock svår att automatisera. För detta krävs som regel att information läses av mänskliga ögon och att beslut fattas av en person med kunskaper om vad som ingår i prövningen och som i slutändan kan hållas ansvarig för sin bedömning, även om olika beslutsstöd kan underlätta prövningen.

Vi anser inte att dagens krav, som innebär att personuppgifter som behandlas så snart det är möjligt ska följa lagens krav, utgör en tillräcklig reglering för denna granskning. Den nuvarande bestämmelsen innebär i praktiken att personuppgiftsbehandling sker i strid med bestämmelserna om adekvans, relevans och uppgiftsminimering då de samlats in och att det är oreglerat hur länge denna otillåtna behandling får pågå. Denna ordning får anses vara otillfredsställande för den verksamhet som Säkerhetspolisen bedriver. Vi uppfattar att otydligheten i lagstiftningen på denna punkt inte

kan betecknas som transparent och öppen i förhållande till de registrerade.

Den mycket generösa reglering av särskilda fall av personuppgiftsbehandling som gäller för Försvarsmakten och FRA är anpassad i huvudsak för försvarsunderrättelseverksamhet och syftar till att tillåta bland annat kryptoforcering av insamlat material. Detta skäl görs sig inte gällande i samma utsträckning för Säkerhetspolisen. När det kommer till automatiserad behandling av vissa stora uppgiftsmängder som inte kan granskas manuellt föreslår vi, i kapitel 9, en särskild reglering.

Vi anser att det bör finnas en reglering som är särskilt anpassad för Säkerhetspolisens verksamhet och som anger hur personuppgifter får hanteras under den process som syftar till att granska, sortera och radera inkomna och inhämtade uppgifter för att lagens krav ska uppnås. Frågan om hur information som inte har granskats får behandlas bör därför regleras uttryckligen i den nya lagen. Regleringen bör ta hänsyn till Säkerhetspolisens uppdrag och utmaningar men samtidigt innebära ett adekvat dataskydd.

8.12.4 Hur bör reglerna utformas?

Förslag: Efter inledande behandling ska personuppgifter granskas, om det behövs för att säkerställa författningsenlig behandling. Innan detta skett får personuppgifterna endast behandlas för den granskningen.

Det ska under den inledande granskningen inte ställas krav på att samtliga uppgifter måste vara relevanta, adekvata och inte onödigt omfattande i förhållande till ändamålet med insamlingen.

Granskning ska ske så snart det är möjligt efter inledande behandling och får pågå i högst sex månader. Granskningen ska utföras av särskilt utbildad personal.

Grundläggande principer för initialgranskning

Det är viktigt för de intressen som en personuppgiftslag primärt har att värna, den personliga integriteten och andra grundläggande fri- och rättigheter, att det i myndighetens informationssystem

endast finns uppgifter som behövs för Säkerhetspolisens uppdrag samt att uppgifterna är adekvata, relevanta och inte onödigt omfattande i förhållande till ett berättigat ändamål. Medborgare måste ha förtroende för att Säkerhetspolisen inte har tillgång till uppgifter om dem, om de inte förekommer i något sammanhang som gett skäl till det. Det innebär att det i princip är förbjudet för Säkerhetspolisen att bevara uppgifter utan någon koppling till ett berättigat ändamål.

Det är samtidigt omöjligt för Säkerhetspolisen att endast behandla personuppgifter som uppfyller alla lagens bestämmelser. Redan insamling eller inhämtande av uppgifter, genom exempelvis behandling av överskottsinformation från hemliga tvångsmedel, uppgifter som delges från FRA eller uppgifter som tillhandahålls av en samverkande tjänst innebär en behandling. I det skedet är det inte klart vilka personuppgifter som finns i informationsmängden som hanteras. Att översätta, bearbeta, sammanställa, läsa och analysera dessa uppgifter för att kunna avgöra om de över huvud taget får behandlas innebär i sig personuppgiftsbehandling. Reglerna måste därför medge en temporär behandling under granskningsskedet, med andra krav än vad som gäller för att få fortsätta att behandla uppgifterna genom bland annat lagring. Reglerna bör gälla under en begränsad tid, som inte får vara längre än vad som är nödvändigt för att utföra granskningen. Den undantagssituation som aktualiseras under granskningsskedet får inte heller medge en behandling som riskerar att stå i strid med de centrala bestämmelserna i Europakonventionen, regeringsformen eller dataskyddskonventionen.

Granskning bör kunna ske mer effektivt i den nya lagen

Trots att säpodatalagen är relativt ny kan det konstateras att det i dag ställs helt andra krav på Säkerhetspolisens förmåga att hantera allt större informationsmängder än vad som kunde förutses vid lagens tillkomst, (se avsnitt 6.2). Säkerhetspolisens organisation har också genomgått förändringar och det är inte längre effektivt att endast låta ett fåtal eller en mindre grupp medarbetare hantera bearbetning av all information som myndigheten behöver i sitt operativa arbete.

Vår uppfattning är att den föreslagna lagstiftningen i många avseenden kommer göra det lättare för Säkerhetspolisen att avgöra om personuppgifter får behandlas. Personuppgifter som behövs inom underrättelseverksamheten för att kartlägga och klarlägga företeelser och verksamheter ska inte behöva granskas och annoteras på detaljnivå. Det är inte var och en av de personuppgifter som förekommer som ska bedömas, utan uppgifternas sammanhang. Genom att uppgifter som förekommer i ett relevant sammanhang kommer bedömas på en mer aggregerad nivå bör behovet att maskera eller anonymisera enskilda personuppgifter att minska eller upphöra (jämför avsnitt 6.1.3). Vi föreslår även att känsliga personuppgifter bör få behandlas enligt samma behandlingströskel som andra uppgifter, vilket även innebär att det inte som i dag behövs en särskild prövning för varje sådan uppgift som förekommer i ett material (se nedan i avsnitt 8.15.2). Behovet att anförtro granskning till en särskild enhet med hög kompetens inom personuppgiftslagstiftningen kommer därför inte vara lika tydligt som förut. Det bör därför vara möjligt för operativ personal inom de olika verksamhetsgrenarna att utföra granskning av uppgifterna direkt då de kommer in till myndigheten.

Från vilka bestämmelser bör undantag göras vid initialgranskning?

Som nämnts ovan är det inte möjligt att ställa krav på att Säkerhetspolisen ska ha kännedom om innehållet i de uppgifter som behandlats inledningsvis innan de hunnit granskats. Det är därför inte möjligt att ställa krav på att samtliga uppgifter ska vara relevanta, adekvata eller inte onödigt omfattande i förhållande till ändamålet med insamlingen.

Däremot finns det inga skäl till att göra undantag från ändamålsprincipen som sådan.[89] Vi har i avsnitt 8.6.6 kommit till slutsatsen att inledande behandling ska få ske för övergripande ändamål och i avsnitt 8.6.7 att behandlingströskeln ska vara lägre. Detta är motiverat utifrån Säkerhetspolisens behov av att kunna identifiera ännu okända hot och företeelser. Den inledande granskningen ska därför ske av uppgifter som samlats in för ett övergripande ändamål. Som

[89] Jfr även Lagrådets yttrande i prop. 2020/21:224, bilaga 8, på s. 320 f.

framgår av avsnitt 8.7 och 8.9 ska både ändamålet preciseras och en högre behandlingströskel passeras för att personuppgifter ska få fortsätta att behandlas. Den inledande granskningen sker i syfte att säkerhetsställa detta.

Personuppgifterna behandlas för ett övergripande ändamål då granskningen inleds och för ett särskilt, preciserat ändamål då den avslutas. Uppgifter som inte uppfyller kravet för efterföljande behandling ska givetvis raderas. Av avsnitt 8.6.8 framgår att det inte kan ställas några krav på uppgifters kvalitet innan de hunnit granskas i detta avseende. Det innebär att den inledande granskningen ska syfta till att säkerställa kvalitetskraven.

Vi föreslår således i den nya lagstiftningen ett undantag från de angivna kraven under den inledande granskningen.

Personuppgifter som inte granskats bör vara begränsade avseende det ändamål för vilka de får behandlas

Att vi i lagen förslår att information som kommer till Säkerhetspolisen ska kunna granskas på ett mer effektivt sätt och i stor utsträckning av operativ personal inom de olika verksamhetsgrenarna innebär inte uppgifterna omedelbart ska vara operativt tillgängliga. En sådan ordning är oförenlig med principerna bakom den föreslagna lagen. Granskningen syftar inte till att exempelvis utreda brott eller förebygga brottslig verksamhet. Granskningen syftar till att kontrollera om myndigheten får behandla uppgifterna för något operativt ändamål. Det innebär naturligtvis att granskning måste föregå all annan operativ behandling av personuppgifterna. Samtidigt är tanken att all information ska kunna behandlas operativt så fort det kunnat konstateras att personuppgifterna som granskats uppfyller kraven på ändamål, kvalitet och proportionalitet.

Uppgifter som kommer till Säkerhetspolisen genom inledande behandling får inte vara sökbara eller operativt tillgängliga innan de granskats. Operativt tillgängliga uppgifter måste även fortsättningsvis förutsättas vara granskade och uppfylla alla lagens krav. Vår uppfattning är att den lämpligaste regleringstekniken för att uppnå detta är att uppgifter, efter den inledande behandlingen, inte ska få behandlas för något annat ändamål än att säkerställa författningsenlig behandling.

Det innebär att de personer som tar emot uppgifter ska bedöma om fortsatt behandling är proportionerlig, om uppgifterna behövs samt om de är relevanta, adekvata och inte onödigt omfattande i förhållande till ett särskilt uttryckligt angivet ändamål. När allt detta väl konstaterats kan uppgifterna omedelbart behandlas för sitt ändamål. Typiskt sett innebär det att uppgifterna görs operativt tillgängliga genom datatekniska åtgärder. Det innebär att samma personal som granskar uppgifterna omedelbart kan gå vidare med de ytterligare åtgärder som föranletts av den information som kommit in till myndigheten. Att personal med sakkunskap inom de olika verksamheterna själva granskar uppgifter som kommer till enheten ger operativa fördelar. Ofta kan bakgrundskunskap om personer, företeelser eller verksamheter innebära att ändamålet med fortsatt behandling kan preciseras i ett tidigt stadium. Effektiviteten hos myndigheten bör på detta sätt kunna stärkas.

I samband med att personuppgifter granskas ska behandlingstiden bestämmas

Vi föreslår i avsnitt 8.18 att Säkerhetspolisen ska bestämma behandlingstid för uppgifter i samband med att uppgifterna genomgår inledande granskning. Detta är en viktig bedömning som utgör en integrerad del av den mer övergripande proportionalitetsprövningen.

Vi förutsätter att ett verksamhetsstöd utarbetas för bestämmande av behandlingstid, där riktlinjer för olika typfall kan underlätta bedömningen. Även denna prövning bör lämpligen kunna utföras av personal som arbetar operativt med inom de olika verksamhetsgrenarna och som bäst känner till behovet av uppgifterna över tid.

Det bör ställas krav på de personer som ska utföra inledande granskning

En av målsättningar med den föreslagna lagen är att den ska vara lättare att tillämpa för Säkerhetspolisen. Vår ambition har varit att skapa en lagstiftning som är anpassad för myndighetens verksamhet. Därmed inte sagt att lagen är enkel att tillämpa. Vi föreslår exempelvis att en proportionalitetsprövning ska vägleda tillämpningen

i högre grad än i dag. En bedömning som innehåller flera olika parametrar som kan vägas mot varandra.

Frågor som rör förutsättningar för personuppgiftsbehandling är generellt sett komplexa. Detta gäller särskilt när personuppgiftsbehandlingen utgör en myndighets kartläggning av enskildas personliga förhållanden som, per definition, utgör ett intrång i enskildas grundläggande fri- och rättigheter. Granskningen av personuppgifter för att bedöma förutsättningarna för fortsatt operativ behandling får därför inte ske slentrianmässigt.

I dag finns en hög kompentens hos Säkerhetspolisen avseende tillämpningen av den nuvarande lagstiftningen. De personer som i dag granskar om personuppgiftsbehandlingen är tillåten har särskilda kvalifikationer. Vår uppfattning är att det bör ställas krav på att alla som har behörighet att föra in uppgifter i Säkerhetspolisens operativa system även i fortsättningen måste vara särskilt lämpade att genomföra den inledande granskningen.

Några formella krav bör dock inte ställas upp i lagstiftningen. Hur tillräcklig kompetens kan tillförsäkras, exempelvis genom särskilda internutbildningar, bör vara ett ansvar för myndigheten. I lagen bör endast anges att granskningen ska utföras av särskilt angivna tjänstemän, vilket är samma begrepp som i dag används för att peka ut de som har åtkomst till uppgiftssamlingen för bearbetning och analys (3 kap. 4 § tredje stycket säpodatalagen). Begreppet innebär inte någon numerär och inget hindrar att all operativ personal vid en enhet har genomgått den utbildning och fått de behörigheter som krävs för att genomföra inledande granskning av personuppgifter. Genom att kravet på viss kompetens uppställs i säpodatalagen kommer frågan om medarbetarnas utbildning och kunskap också stå under tillsyn.

Vi föreslår en lagregel med denna innebörd.

Den inledande granskningen bör ske så snart det kan ske och vara tidsbegränsad

Att Säkerhetspolisen inledningsvis ska kunna behandla personuppgifter enligt andra och mer tillåtande regler kräver att behandlingen utgör ett tidsbegränsat undantag. Givetvis får inte personuppgifter behandlas med stöd av undantagsregeln som gäller inledande granskning under längre tid än vad som krävs för att genomföra gransk-

ningen. Det bör även uppställas ett skyndsamhetskrav för att granskningen som bör ske så snart det är möjligt.

Vid sidan om denna huvudregel finns det även skäl att begränsa den längsta tid Säkerhetspolisen får behandla personuppgifter för granskning. Vår uppfattning är att det är en förutsättning för ett undantag av detta slag i en verksamhet som är så känslig som Säkerhetspolisens. Lagen bör därför innehålla en fast tidsgräns inom vilken granskning måste ske.

Som tidigare nämnts har Norge en tidsgräns på fyra månader och Danmark fyra veckor. Det kan konstateras att den tidsgräns som gäller i Danmark är avsevärt kortare än vad som krävs för att PET ska kunna utföra initialgranskning. Den danska tillsynsmyndigheten har under flera år riktat kritik mot att behandling i granskningssystemen inte sker inom den reglerade tiden och nyligen har lämnats förslag om en översyn av systemet. Den norska fyramånadersfristen framstår mer anpassad till verksamheten och har vi har inte identifierat att denna tidsgräns lyfts som något problem. Samtidigt kan konstateras att mängden information som behandlas av Säkerhetspolisen har ökat mycket drastiskt de senaste åren. Den tekniska utvecklingen innebär att en mobiltelefon numera kan innehålla lika mycket information som ett medelstort datacenter gjorde för något decennium sedan. I händelse av exempelvis ett stort tillslag måste resurser prioriteras och mindre angelägna granskningar kan då bli liggande under viss tid. För att medge en ordnad och strukturerad informationshantering även under särskilda omständigheter, för vilka Säkerhetspolisen måste ha en god beredskap, bör tidsfristen inte sättas för snävt.

Den yttersta tidsgränsen föreslår vi av dessa skäl ska uppgå till sex månader.

Den inledande granskningen ska vara ett krav endast när det behövs en sådan granskning för att bedöma informationen

Inledande behandling omfattar även personuppgifter som upprättas eller på andra sätt skapas inom myndigheten. Det innefattar exempelvis att en medarbetare nedtecknar personuppgifter i promemoria eller i en tjänsteanteckning. I dessa fall kommer granskningen inte att vara separerad från den inledande behandlingen utan snarare vara en del av den. Det är medarbetarens ansvar att den behandling som

den faktiska åtgärden att skapa personuppgifter innebär sker författningsenligt.

Den inledande behandling som särskilt motiverar en särskild bestämmelse om granskning är sådan där informationsinnehållet är okänt. Om det är klart att den inledande behandlingen är förenlig med de krav som ställs även för efterföljande behandling, behöver inte uppgifterna granskas. Så kan vara fallet exempelvis då inhämtning sker från databaser där uppgiftsinnehållet till sin typ är känt. Om det exempelvis handlar om folkbokföringsuppgifter för registrerade personer ska givetvis inte adressuppgifter och liknande behöva granskas av dataskyddsskäl. Det står då klart att den inledande behandlingen behövs för ett särskilt ändamål och att uppgifterna är adekvata och relevanta att behandla. Vi föreslår därför att inledande behandling ska utföras när det behövs för att uppnå syftet, nämligen att säkerställa en författningsenlig behandling.

8.12.5 Ej granskad information bör kunna tillgängliggöras vid ett nödläge

Förslag: I nödsituationer bör en av regeringen särskilt utsedd befattningshavare vid Säkerhetspolisen få besluta om att information som inte granskats får behandlas även för operativa ändamål.

Principerna för ett undantag från kravet på inledande granskning

Säkerhetspolisens uppdrag innebär att det i vissa fall kan inkomma uppgifter som ställer mycket höga krav på myndighetens reaktionsförmåga. Exempelvis kan det inkomma ett tips från en samverkande tjänst om att en terroristcell aktiverats med uppdrag att inom 24 timmar detonera en bomb någonstans i Sverige. I det läget måste det finnas en ventil som innebär att det allmänna intresset nationell säkerhet väger tyngre än under normala förhållanden.

En viss händelse kan även föranleda en explosionsartad informationsutveckling, exempelvis terrorattentatet på Drottninggatan den 7 april 2017. Både riskanalysen för ytterligare terrordåd och jakten på gärningsmannen krävde en mycket omfattande analyskapacitet

av den stora mängd information som kontinuerligt inkom till Säkerhetspolisen.

Säkerhetspolisen bör i dessa, och andra liknande exceptionella fall kunna verka effektivt för att avvärja överhängande hot mot nationell säkerhet. Det bör därför finnas en särskild bestämmelse som kan tillämpas vid nationella nödlägen.

En nödbestämmelse som kan effektivisera informationshanteringen är att frångå den ändamålsbegränsning som innebär att insamlade eller inkomna uppgifter måste granskas innan de kan behandlas operativt. För att möjliggöra högsta möjliga förmåga i krissituationer bör ett sådant undantag införas i lagen.

Med hänsyn till det stora avsteget som en sådan bestämmelse innebär från lagens skyddsmekanismer bör ett undantag beslutas i särskild ordning. Närmare bestämmelsen om vem som är behörig att fatta beslut bör bestämmas i förordning.

Beslutet bör vara skriftligt och motiverat för att möjliggöra granskning i efterhand. För att möjliggöra sådan granskning bör Säkerhets- och integritetsskyddsnämnden få del av ett sådant beslut och kunna granska den behandling som sker med stöd av detta.

Hur bör undantaget vara utformat?

Det finns andra lagstiftningar som har olika slags ventiler som är tänkta att kunna hantera krissituationer. Det finns dock inte några motsvarande exempel i någon annan personuppgiftslagstiftning. I svensk konstitutionell rätt saknas allmänna formuleringar om nöd. I 5 kap. regeringsformen finns vissa bestämmelser avseende händelse av krig eller krigsfara, som kan innebära att rättighetsskyddet får stå tillbaka.

Vi ser inte något behov av att i säpodatalagen gå så långt som att speciallagstifta angående den exceptionella händelsen av krig eller krigsfara. Den situation vi anser behöva täckas är den då det föreligger ett allvarligt, verkligt och nära förestående hot mot nationell säkerhet. Det måste röra sig om situationer där det är absolut nödvändigt att behandla stora mängder information omedelbart. Hotet ska i princip avse statens väsentliga funktioner eller samhällets grundläggande intressen och vara så tidskritiskt att undantaget är absolut nödvändigt. En sådan situation kan exempelvis uppkomma om det

finns trovärdiga upplysningar om att ett allvarligt terrorattentat ska utföras på svensk mark eller mot svenska intressen i närtid. All tillgänglig information som Säkerhetspolisen kan samla och hämta in får då behandlas för att avvärja hotet.

Ett så långtgående undantag måste givetvis vara tidsbegränsat. Med hänsyn till att regeln syftar till att avvärja omedelbara eller nära förestående hot kan tidsbegränsningen vara relativt snäv. Vi anser att 30 dagar bör vara tillräckligt. Givetvis måste undantaget upphöra så snart det inte längre uppfyller kravet på att vara absolut nödvändigt. En ytterligare begränsning bör vara att den information som behandlas med stöd av undantaget endast får vara tillgänglig för dem som behöver behandla uppgifterna för det ändamål som föranlett undantaget. Denna begränsning syftar dels till att förhindra att uppgifterna behandlas för andra ändamål, som inte i sig hade kunnat motivera undantaget, dels till att minska risken för integritetskränkningar. Att Säkerhets- och integritetsskyddsnämnden ska underrättas så snart ett undantag införs innebär att nämnden får goda möjligheter att inleda granskning av den behandling som skett med stöd av ett undantagsbeslut.

8.12.6 Hur förhåller sig inledande granskning till särskilda uppgiftssamlingar?

Förslag: Inledande granskning kan ske i förhållande till kraven för registrering av uppgifter i en särskild uppgiftssamling (se kap. 9).

Framtagning från en särskild uppgiftssamling är inledande behandling och ska därför följas av inledande granskning.

Granskning innan beslut om registrering av uppgifter i en särskild uppgiftssamling

Vi föreslår i kapitel 9 att säpodatalagen ska kompletteras av ett särskilt regelverk som gäller behandling av personuppgifter i särskilda uppgiftssamlingar. Den lagstiftningen syftar bland annat till att möjliggöra behandling av informationsmängder av sådan omfattning att de inte är möjliga att granska enligt de krav som ställs efter inledande behandling. Vi föreslår dock att även sådana större dataset ska

genomgå en översiktlig granskning för att det ska vara möjligt att fatta ett formellt beslut om att registrera uppgifterna i en särskild uppgiftssamling.

Den inledande granskningen omfattar även uppgifter som hämtats in i syfte att registrera i en särskild uppgiftssamling. Granskningen ska i dessa fall ske mot de krav som uppställs för att registrera sådana uppgifter i särskilda uppgiftssamlingar.

Uppgifter som tagits fram från en särskild uppgiftssamling ska granskas

Enligt det särskilda regelverk vi föreslår om behandling av personuppgifter i särskilda uppgiftssamlingar kommer inledande behandling kunna ske av uppgifter som Säkerhetspolisen redan förfogar över. Detta sker enligt de särskilda reglerna om framtagning av uppgifter. Det är viktigt att sådana uppgifter granskas enligt säpodatalagens krav. Att tillstånd getts till framtagningen är nämligen inte en garanti för att uppgifterna får fortsätta att behandlas enligt säpodatalagen.

8.13 Särskilda upplysningar

8.13.1 Den nuvarande regleringen

Enligt den nuvarande lagstiftningen ska personuppgifter som görs gemensamt tillgängliga förses med vissa upplysningar. Om det ändamål som gemensamt tillgängliga personuppgifter behandlas för inte framgår av sammanhanget eller på något annat sätt, ska det enligt 3 kap. 3 § säpodatalagen tydliggöras genom en särskild upplysning. Enligt 4 § i samma kapitel ska det genom en särskild upplysning eller på något annat sätt framgå att en person som är registrerad inte är misstänkt för brott eller brottslig verksamhet. Enligt andra stycket i samma bestämmelse ska uppgifter om en person som kan antas ha direkt samband med brottslig verksamhet förses med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak, om det inte på grund av omständigheterna är onödigt.

De särskilda upplysningarna tillkom när 2010 års polisdatalag frångick registerbegreppet. Tidigare lagstiftningar på området angav

att personuppgifter skulle föras i särskilda register av vilka bland annat ändamål framgick. Registrens struktur innebar även att personer som förekommer i den brottsbekämpande verksamheten, som misstänkta, vittnen och målsägande tydligt särskildes vid registreringen. När uppgifter tilläts behandlas utanför särskilda register ansågs det nödvändigt att införa bestämmelser som säkerställer att den som söker information får motsvarande upplysningar om ändamålet för behandlingen, som han eller hon skulle ha fått om uppgifterna hade behandlats i ett register. Både verksamhetsskäl och integritetsskyddsskäl ansågs tala för att det vid informationssökning ska framgå varför en uppgift behandlas av polisen. Av samma skäl menade regeringen att det var viktigt att det skulle framgå att en uppgift rör en icke-misstänkt person när så är fallet samt hur tillförlitlig en underrättelseuppgift bedöms vara.[90]

8.13.2 Behövs särskilda upplysningar?

Bedömning: Varje bestämmelse som medför ett krav på att enskilda uppgifter ska genomgå manuell bedömning och handpåläggning är styrande för hur Säpo kan organisera sig och arbeta.

Krav på särskild upplysning ska prövas noga mot nyttan med kravet.

Vår utgångspunkt är att vi i så stor utsträckning som möjligt ska undvika att styra verksamheten genom personuppgiftslagstiftningen. Syftet med lagen är i första hand att värna enskildas personliga integritet. De regler i den nuvarande lagstiftningen som inte primärt uppfyller det syftet bör därför omprövas. Med hänsyn till den verksamhet som Säkerhetspolisen bedriver kan varje överreglering i personuppgiftslagen innebära en förmågesänkning. Ledtiderna i verksamheten behöver vara så korta som möjligt för att information som kommer till verksamheten så snabbt som möjligt ska kunna leda till åtgärder för att förebygga och avvärja hot.

De särskilda upplysningar som ska tillföras gemensamt tillgängliga uppgifter i den nuvarande lagstiftningen har pekats ut som en sådan reglering som i vissa fall kan medföra att ledtiderna i verksamheten

[90] Prop. 2009/10:85 s. 146–147.

blir onödigt, och ibland omotiverat, långa. Dagens regler om särskilda upplysningar innebär en manuell hantering av varje personuppgift. Det tål att upprepas att datatillväxten och informationsflödet i dagens samhälle utvecklas exponentiellt och det som för några decennier sedan utgjorde ett datacenter numera ryms i varje mobiltelefon.

Att manuellt granska enskildheter i stora informationsmängder är inte en realistisk arbetsmetod. Varje bestämmelse i en personuppgiftslag som medför ett krav på att varje enskild uppgift ska genomgå manuell granskning, bedömning och handpåläggning kommer med nödvändighet att bli kraftigt styrande för hur Säpo kan organisera sig och arbeta. Varje sådant krav måste därför prövas noga mot nyttan med kravet. Mängden personuppgifter som behövs för en kartläggning inom underrättelseverksamheten bör inte begränsas av de resurser som finns tillgängliga för att etikettera varje enskild personuppgift med en särskild upplysning. Personuppgiftsbehandling enligt denna lag vilar i stället på de grundläggande principerna att uppgifterna ska behövas för berättigade ändamål och inte innebära ett oproportionerligt intrång i de registrerades fri- och rättigheter.

8.13.3 Upplysning om ändamål med behandlingen

Förslag: Om det ändamål som personuppgifter behandlas för inte framgår av sammanhanget eller på något annat sätt, ska det tydliggöras genom en särskild upplysning.

Ändamålet med behandlingen måste framgå

Bestämmelsen om särskild upplysning om ändamål har sitt ursprung i det krav om att grunder för registrering som skulle anges för uppgifter som fördes in i det så kallade SÄPO-registret, som reglerades i den äldre polisdatalagen. Denna bestämmelse har levt kvar i 3 kap. 3 § säpodatalagen och innebär att en särskild upplysning om ändamål måste anges manuellt för alla de personuppgifter som Säkerhetspolisen behandlar. Då det rör sig om nya uppgifter som tillförs redan kända personer kan ändamålet i många fall framgå av sammanhanget. När det däremot handlar om ostrukturerad information som Säker-

hetspolisen kommer över genom exempelvis inhämtning på internet, beslag eller hemliga tvångsmedel handlar det om ett mycket omfattande arbete att särskilja det mer konkreta ändamålet för personuppgifter som hör till olika individer. Vissa uppgifter kan vara relevanta för ett visst ändamål, då de exempelvis har koppling till ett befarat terrordåd som planeras i någon viss miljö. Andra uppgifter kan i och för sig vara relevanta för underrättelseverksamheten, exempelvis angående den misstänktes kontakter inom en extremistisk miljö, men kan inte direkt kopplas till det ursprungliga ärendet. Sådana uppgifter, som kan vara relevanta för att kartlägga misstankar om annan brottslig verksamhet, behöver regelmässigt förses med en särskild upplysning. Personuppgifter förekommer i olika former av textmeddelanden och i ljud-, bild- eller videofiler. Sammantaget kan enskilda it-beslag ofta innehålla en mycket stor mängd uppgifter som tillsammans eller för sig går att koppla till en identifierad eller identifierbar fysisk person som är i livet. I ett it-beslag kan det i dag röra sig om tusentals personuppgifter som manuellt behöver förses med en sådan upplysning.

Redan av ändamåls- och finalitetsprincipen följer att ändamålet för personuppgiftsbehandling måste framgå vid en inledande behandling. Om ändamålet inte framgår, är det inte möjligt att göra prövningen om en viss behandling, är oförenlig med ändamålet för insamlingen. Det finns därför verksamhetsskäl som med styrka talar för att ändamålet måste anges genom en särskild upplysning, om det inte framgår av sammanhanget. Ändamålet med att en viss uppgift finns bevarad i Säkerhetspolisens it-miljö möjliggör även att åtkomsten till uppgiften, genom tekniska och organisatoriska åtgärder, begränsas endast till de medarbetare som har behov av uppgiften. Ur integritetssynpunkt är det viktigt att uppgifter endast behandlas av de som har ett konkret behov av uppgiften för att kunna utföra sina arbetsuppgifter på ett effektivt sätt. Att ändamålet med behandlingen framgår kan vidare vara en förutsättning för att en tillsynsmyndighet effektivt ska kunna kontrollera om viss behandling är berättigad och utförs i enlighet med lagens bestämmelser. Det förs inte längre särskilda register i specifika underrättelseprojekt där det utifrån registrets namn går att sluta sig till vad som är ändamålet med uppgifter i det. Det finns inte heller personakter där all information samlas om enskilda individer. Dagens system är och bör vara uppbyggda för att möjliggöra en snabbt och flexibelt informa-

tionsflöde för att verksamheten ska fungera så effektivt som möjligt. Vi anser sammantaget att det inte är möjligt att upprätthålla ändamålsprincipen om det inte på något sätt går att utläsa för vilket ändamål personuppgifter behandlas. Det finns därför fortfarande ett behov av särskilda upplysningar avseende ändamål.

Enligt gällande rätt har särskilda upplysningar endast varit ett krav för gemensamt tillgängliga uppgifter. Med hänsyn till att uppdelningen mellan gemensamt och icke-gemensamt tillgängliga uppgifter inte överförs till den nya lagen bör bestämmelsen gälla samtliga uppgifter som behandlas i den operativa it-miljön. Det är därmed senast i samband med att uppgifterna lämnar den inledande granskningen som upplysningen ska tillföras. På samma sätt som enligt nuvarande ordning bör kravet endast träffa uppgifter där det inte av sammanhanget går att utläsa det ändamål för vilket uppgifterna behandlats.

Hur detaljerad bör ändamålsupplysningen vara?

Vi har föreslagit att inledande behandling av uppgifter får ske enligt övergripande ändamål (se avsnitt 8.6.6). Denna princip bygger på att ändamålet ska preciseras efter den inledande granskningen. Det sker genom en särskild upplysning, om inte ändamålet framgår på annat sätt. Av underrättelseändamålet – kartlägga och klarlägga brottslig verksamhet – framgår att det kan vara relevant att inte endast behandla de uppgifter som rör kända hotaktörer eller konkreta hot. Även uppgifter som förekommer i sammanhang där hotaktörer befinner sig eller kan antas befinna sig kan vara relevanta att behandla för att kartlägga den brottsliga verksamheten. Ändamålsupplysningen bör därför omfatta en viss aktör eller ett visst hot, men tillämpas på alla uppgifter som behöver behandlas för kartläggningen. Om ett it-beslag skett från en misstänkt terrorist kan exempelvis ändamålet för att kartlägga terroristnätverket eller eventuella kopplingar till andra hotaktörer tillämpas på samtliga personuppgifter i it-beslaget. Det krävs inte att samtliga personuppgifter som förekommer i ett it-beslag prövas var för sig så länge de ingår i en relevant kontext som behövs för att kartlägga den brottsliga verksamheten.

8.13.4 I underrättelseverksamheten bör det inte längre uppställas krav på att personer som inte är misstänkta ska särskiljas genom en särskild upplysning

Bedömning: Det finns inte tillräckliga skäl för att behålla kravet på särskild upplysning avseende personer som inte är misstänkta för brott eller brottslig verksamhet.

Bakgrunden till den nuvarande bestämmelsen

Enligt 3 kap. 4 § säpodatalagen ska det genom en särskild upplysning anges om en person inte är misstänkt för brott eller för att ha utövat eller kan komma att utöva brottslig verksamhet som Säkerhetspolisen har till uppgift att bekämpa. I klartext innebär det att aktörer som inte är föremål för förundersökning eller är ”underrättelsemisstänkta” ska särskiljas från dem som är det. En underrättelsemisstanke består av att någon antas ha utövat eller kan komma att utöva brottslig verksamhet. Brottslig verksamhet är det begrepp som brukar användas för att fånga föremålet för brottsbekämpande underrättelseverksamheten. En misstanke om brottslig verksamhet förutsätter inte kännedom om konkreta gärningar. Det måste dock vara fråga om en viss typ av brottslighet, som däremot inte behöver vara närmare specificerad i fråga om omfattning eller detaljer (se avsnitt 3.5.6).

Bestämmelsen kan till exempel vara tillämplig då anhöriga till personer som antas utöva brottslig verksamhet inom viss våldsbejakande extremistmiljö finns registrerade. Då ska det anges att de inte är misstänkta. Ett annat fall kan vara att skyddspersoner inom personskyddsverksamheten ska särskiljas från de hotaktörer som denne ska beskyddas från.

Andelen misstänkta personer i underrättelseverksamheten är förhållandevis få och därför tillämpas bestämmelsen i praktiken motsatsvis genom att den särskilda uppgiften i stället anger om en person är misstänkt.

Bör det framgå att en person inte är underrättelsemisstänkt?

Bestämmelsen medför i dagsläget ett betydande manuellt merarbete för Säkerhetspolisen. Om den integritetsstärkande funktionen inte framgår tydligt, bör det övervägas om det alltjämt är relevant att reglera frågan i en personuppgiftslag.

Det kan till att börja med ifrågasättas hur betydelsefullt det ur integritetssynpunkt är att det framgår om en person antas ägna sig åt brottslig verksamhet vid registreringen, då den särskilda upplysningen tillförs. Ofta stärks eller avtar misstankar successivt i en utredning och detta framgår som regel av sammanhanget. För att den särskilda upplysningen ska fylla sin integritetsstärkande funktion bör den därför regelbundet uppdateras. Om en person är underrättelsemisstänkt eller inte, är en fråga som kräver en sammanvägd bedömning av all information som finns tillgänglig vid tidpunkten för bedömningen. Att kontinuerlig uppdatera misstankemarkeringar i hela Säkerhetspolisens underrättelsesystem skulle dock innebära ett orimligt omfattande merarbete.

Det är givetvis till fördel för tillsynen att kunna undersöka hur uppgifter om personer som inte kan misstänkas för brottslig verksamhet behandlas. Om det överhuvudtaget inte finns några misstankar om brottslig verksamhet, kan Säkerhetspolisen behöva förklara behovet av uppgifterna närmare. Den särskilda upplysningen om ändamålet med behandlingen bör dock kunna användas för att sluta sig till vilken brottslig verksamhet som föranlett registreringen. Genom innehållet i uppgifterna och sammanhanget de förekommer i bör Säkerhetspolisen kunna motivera behandlingen. Det gäller oavsett om personen är misstänkt eller inte.

Regeringen angav i förarbetena till de övriga brottsbekämpande myndigheters registerlagstiftning att det är särskilt viktigt att det i underrättelseverksamheten görs tydlig skillnad mellan personer som har ett direkt samband med den brottsliga verksamheten och andra personer.[91] Detta uttalande bygger dock på att bland annat Polismyndighetens underrättelseverksamhet bedrivs närmare det stadium då någon kan misstänkas för ett konkret brott. I tidigare förarbeten framkommer synsättet att det inom Säkerhetspolisens brottsförebyggande arbete normalt inte går att urskilja lika tydliga kopplingar till konkreta brott eller till brottslig verksamhet som

[91] Prop. 2017/18:269 s. 109.

inom den övriga polisen. Den underrättelseverksamhet som bedrivs inom Säkerhetspolisen är till sin natur ofta sådan att den ligger på ett tidigare stadium än den som bedrivs av polisen i övrigt men inriktad mot ett fåtal, väl avgränsade företeelser av särskilt samhällsfarlig karaktär.[92]

När underrättelseverksamhet sker på det sätt som krävs för Säkerhetspolisen brottsbekämpning kan det i det närmaste förutsättas att en stor majoritet av de registrerade inte är underrättelsemisstänkta. Integritetsintrånget av att överhuvudtaget vara registrerad bör därför inte vara särskilt mycket mindre genom att en särskild upplysning om att den registrerade inte är misstänkt finns. Om någon är av intresse som misstänkt framgår det ofta av sammanhanget eller går att sluta sig till av de övriga åtgärder Säkerhetspolisen vidtagit avseende personen.

Den nuvarande regleringen har ansetts vara särskilt relevant när uppgifter behandlas utanför sitt ursprungliga sammanhang.[93] Till att börja med ska konstateras att personuppgifter inom Säkerhetspolisens underrättelseverksamhet sällan behandlas utanför sitt sammanhang. Om en sökning görs mot en person, är det ofta relevant att ta del av hela sammanhanget som personen förekommer i. Om Säkerhetspolisen delar personuppgifter med en annan myndighet, exempelvis Polismyndigheten, är det inte i en form som innebär att det inte framgår av sammanhanget om personen i fråga är misstänkt eller inte. Detsamma gäller de tillfällen då Säkerhetspolisen delar uppgifter till samverkande tjänst i ett annat land.

Vi anser därmed att de argument som motiverar att avsaknad av underrättelsemisstanke ska anges som särskild upplysning i Säkerhetspolisens verksamhet inte har samma bärkraft som för Polismyndigheten och de övriga brottsbekämpande myndigheterna. Detta särskilt när bestämmelsen i praktiken tillämpas omvänt, dvs. det särskilt pekas ut underrättelsemisstänkta personer.

Behovet av upplysningen bör prövas utifrån Säkerhetspolisens särskilda verksamhet och de specifika integritetsintressen som gäller denna. Det integritetsintresse som värnas genom den särskilda upplysningen om underrättelsemisstanke är i första hand att det för Säkerhetspolisens personal som behandlar en viss persons personuppgifter direkt framgår om personen förekommer på grund av en

[92] Prop. 2009/10:85 s. 256.
[93] Prop. 2018/19:163 s. 89.

mer konkret misstanke om brottslig verksamhet eller av något annat skäl.

Säpodatalagen syftar i första hand till att värna den personliga integriteten för de registrerade. Vi bedömer inte att en markering av att personer som är registrerade inte misstänkta för brott eller brottslig verksamhet fyller någon reell integritetshöjande funktion. Om det finns en verksamhetsnytta med att behålla misstankemarkeringen utgör säpodatalagen inte något hinder mot det. Den nuvarande bestämmelsen framstår för oss som en reglering som ur integritetssynpunkt inte kan motivera det administrativa merarbete som den innebär. Det skulle medföra den typ av genomgång på uppgiftsnivå som blir påtagligt styrande för hur Säkerhetspolisen kan arbeta och organisera sig. Vi föreslår därför inte att bestämmelsen ska överföras till den nya lagen.

8.13.5 Upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak bör inte vara ett krav i lagen

Bedömning: Det finns inte tillräckliga skäl för att behålla kravet om särskild upplysning angående en uppgiftslämnares trovärdighet och uppgifternas riktighet i sak.

Den nuvarande bestämmelsens utformning

Av andra stycket i 3 kap. 4 § säpodatalagen följer att uppgifter om en person som kan antas ha direkt samband med brottslig verksamhet ska förses med en upplysning om uppgiftslämnarens trovärdighet eller uppgifternas riktighet i sak, om det inte på grund av omständigheterna är onödigt. Regleringen, som alltså riktar in sig på de som kan betecknas som underrättelsemisstänkta, motiverades av både integritets- och verksamhetsskäl.[94] Det är givetvis viktigt att det för någon som har tillgång till ett underrättelseregister inte ska framstå som om en person rör sig i kriminella kretsar eller ägnar sig åt brottslig verksamhet endast på grund av tips eller uppgifter med tvivelaktig tillförlitlighet. För verksamheten har bestämmelsen ansetts motiverad för att undvika att uppgifter som inte är tillförlit-

[94] Ibid. s. 90 och prop. 2017/18:269, s. 111.

liga ska läggas till grund för bedömningar och åtgärder som inte är sakligt motiverade. I Säkerhetspolisens underrättelsearbete är utgångspunkten att uppgifter som inte har bedömts i fråga om trovärdighet och sakriktighet inte läggs till grund för vare sig beslut, bedömningar eller åtgärder. Detta gäller oberoende av om det finns ett lagkrav om en sådan upplysning.

Bör det ställas upp ett krav på trovärdighets- och sakriktighetsbedömning i lagen?

Vi har bedömt att särskild upplysning om underrättelsemisstanke inte längre ska vara ett krav enligt lagen. Frågan är om det trots detta finns skäl att behålla kravet på en trovärdighets- och riktighetsbedömning för vissa uppgifter. Till att börja med kan påminnas om att syftet med en personuppgiftslag inte är att styra myndighetens verksamhet på andra sätt än de som är föranledda av i huvudsak integritetsskäl. Oavsett om Säkerhetspolisen behöver göra en trovärdighet- och sakriktighetsbedömning av information innan den kan läggas till grund för en åtgärd, bör det därför i personuppgiftslagstiftningen inte uppställas något sådant krav om det inte är motiverat utifrån lagens syften.

Det finns ett integritetsintresse av att en uppgift eller ett tips som är felaktigt inte ska föranleda en registrering hos Säkerhetspolisen och särskilt inte under längre tid än vad som är nödvändigt för att avfärda misstankarna. Det följer emellertid inte av den nuvarande regleringen i 3 kap. 4 § säpodatalagen att uppgifter med låg trovärdighet eller som är sakligt felaktiga ska raderas. Radering av irrelevanta och felaktiga uppgifter gäller oberoende av den här aktuella regleringen om särskild upplysning.

Det har beskrivits att upplysningen spelar en inte obetydlig funktion för tillsynsmyndigheten. Om uppgifter med låg trovärdighet ligger till grund för omfattande personuppgiftsbehandling, kan Säkerhetspolisen behöva förklara hur behandlingen förhåller sig till bland annat kraven på relevans och adekvans. Detta skulle kunna utgöra ett skäl att behålla den aktuella regleringen. Lagstiftaren har emellertid vid upprepade tillfällen påpekat att Säkerhetspolisens underrättelseverksamhet har en särställning i förhållande till övriga brottsbekämpande myndigheter. Myndigheten har till uppgift att kartlägga mycket tidiga skeenden av brottslig verksamhet innan

någon konkret misstanke har kunnat formeras och kan stundtals behöva hantera mycket stora informationsmängder.[95] Kravet på sakriktighets- och trovärdighetsbedömning förutsätter en granskning på detaljnivå. I likhet med flera andra bestämmelser är sådan detaljgranskning inte anpassad efter de stora och alltjämt växande informationsmängder som måste hanteras i verksamheten. Varje sådant granskningskrav riskerar att bli styrande för myndighetens verksamhet och hämma verksamhetsutveckling och införande av ny teknik eller nya metoder. Kravet på trovärdighet och sakriktighetsbedömning är en sådan bestämmelse som noga måste prövas mot nyttan.

Vi bedömer att det framstår som svårt att i ett inledande sked med tillräcklig precision kunna bedöma trovärdighet och sakriktighet på ett sätt som bidrar till skyddet av den personliga integriteten. Det ligger i verksamhets natur att Säkerhetspolisen måste undersöka förhållanden trots att det kan vara svårt att avgöra riktigheten av uppgifterna. Om det visar sig att uppgifter är felaktiga eller att en uppgiftslämnare saknar trovärdighet, finns inte heller skäl att behandla uppgifterna. Att uppgifter är mer eller mindre osäkra får däremot betecknas som ett normalläge inom underrättelseverksamhet. När uppgifter om brott, brottslig verksamhet eller personers koppling till sådan är säker medför det givetvis att åtgärder vidtas för att förebygga eller avvärja hot. I vissa fall medför det även att förundersökning ska inledas. De åtgärder som vidtas kan, på motsvarande sätt som en särskild upplysning, synliggöra hur Säkerhetspolisen bedömt sakriktighet och trovärdighet av exempelvis ett tips.

Det finns i nuvarande 3 kap. 4 § tredje stycket säpodatalagen ett undantag från kravet på särskild upplysning för uppgifter som behandlas i uppgiftssamlingen för bearbetning och analys. Regeringen ansåg i samband med att säpodatalagen beslutades att det var acceptabelt att uppgifter som ännu bearbetas inte försågs med en särskild upplysning om trovärdighet och sakriktighet. Det framhölls då att myndighetens personal är van vid att hantera svårbedömd information.[96] Skyddet för den enskildes integritet får sägas ha en undanskymd roll när det kommer till denna särskilda upplysning.

Vi har sammantaget inte funnit tillräckliga skäl till att behålla lagkravet på att det genom särskild upplysning måste framgå hur

[95] Jfr prop. 2018/19:163 s.93.
[96] Ibid. s. 93.

trovärdiga eller tillförlitliga uppgifter om en persons koppling till brottslig verksamhet är. Ur ett integritetsskyddsperspektiv uppfattar vi inte att upplysningen är av tillräcklig nytta. Upplysningen har inte heller några konsekvenser för hur personuppgifter får behandlas i övrigt.

8.13.6 Vid brottsutredning och lagföring bör det framgå om en person är misstänkt eller tillhör någon annan kategori

Förslag: I brottsutredningar ska så långt det är möjligt personuppgifter som rör olika kategorier av registrerade särskiljas så att det framgår om personen är misstänkt, dömd för brott, brottsoffer eller någon annan som berörs av ett brott.

Om det inte framgår av sammanhanget eller på annat sätt till vilken kategori personen hör, ska det tydliggöras genom en särskild upplysning.

Dataskyddskonventionens bestämmelser

Article 6 – Special categories of data

The processing of: […]

– personal data relating to offences, criminal proceedings and convictions, and related security measures; […]

shall only be allowed where appropriate safeguards are enshrined in law, complementing those of this Convention.

2. Such safeguards shall guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination.

Personuppgifter som rör brott, straffrättsliga förfaranden, fällande domar och relaterade säkerhetsåtgärder tillhör kategorin känsliga personuppgifter. Enligt dataskyddskonventionen ska behandling av sådana uppgifter vara omgärdad av tillräckliga säkerhetsåtgärder som särskilt ska beakta risken för rättighetsintrång och diskriminering.

Bakgrunden till dagens bestämmelse

Enligt nuvarande ordning ska det, enligt 3 kap. 4 § säpodatalagen, genom en särskild upplysning även anges om en person inte är misstänkt för brott som Säkerhetspolisen har till uppgift att bekämpa. För övriga brottsbekämpande myndigheter gäller att olika kategorier av registrerade ska särskiljas så att det framgår om personen är misstänkt, dömd för brott, brottsoffer eller någon annan som berörs av ett brott (2 kap. 9 § brottsdatalagen).

Att Säkerhetspolisen inte behöver särskilja andra kategorier av registrerade på samma sätt som övriga brottsbekämpande myndigheter är motiverat av att myndigheten ofta behandlar personuppgifter i ett tidigt skede i sin underrättelseverksamhet, då det normalt inte går att urskilja lika tydliga kopplingar till konkreta brott eller brottslig verksamhet. Regeringen ansåg att det därför inte var rimligt att särskilja fler kategorier än de som inte är misstänkta inom Säkerhetspolisens verksamhet.[97] Dagens reglering gör därmed inte skillnad på för vilket ändamål uppgifterna behandlas och lättnaden i förhållande till brottsdatalagen är motiverad utifrån Säkerhetspolisens omfattande underrättelseverksamhet.

Om personuppgifter behandlas för brottsutredning bör samma krav ställas som för Polismyndigheten

Säkerhetspolisen ägnar sig åt brottsutredning i en mindre skala jämfört med andra brottsbekämpande myndigheter. Säkerhetspolisens uppdrag som nationell säkerhetstjänst innebär att myndigheten i huvudsak bedriver underrättelseverksamhet inom sina olika verksamhetsgrenar. I praktiken är det mycket få av de som finns registrerade av Säkerhetspolisen i dess underrättelseverksamhet som når upp till en tillräcklig misstankegrad för att det ska kunna sägas att personen är misstänkt för brott. När en misstanke uppstår ska underrättelseverksamheten i princip övergå till förundersökning, enligt kravet som uppställs i 23 kap. 1 § rättegångsbalken. Det är tillräckligt att det finns anledning att anta att brott som hör under allmänt åtal har förövats för att en förundersökning ska inledas.

När väl Säkerhetspolisen kan konkretisera brottsliga gärningar och inleder förundersökning anser vi att det inte finns några bärande

[97] Ibid. s. 89.

skäl till att frångå den systematik som gäller för övriga brottsbekämpande myndigheter. Det finns ett integritetsintresse av att det i förundersökningar, eller med andra ord när personuppgifter behandlas för att utreda och lagföra brott, framgår om en person är exempelvis vittne eller misstänkt i den förundersökningen. Förundersökningskungörelsen (1947:948) utgår vidare från att målsägande, vittnen och misstänkta ska särskiljas i förundersökningsprotokollet (20–21 §§). De förundersökningar som Säkerhetspolisen bedriver lyder under samma regler som för Polismyndigheten. Ett förundersökningsprotokoll som upprättas av Säkerhetspolisen bör därför följa samma eller liknande struktur som för andra brottsbekämpande myndigheter.

Vi anser att de skäl som motiverar att Säkerhetspolisen inte ska särskilja olika kategorier av registrerade inte har samma bärkraft i de situationer då konkreta brottsmisstankar uppkommit. När brottsmisstankar uppkommit utgör uppgiften om dessa en känslig personuppgift enligt dataskyddskonventionen 108+. Vi anser att det mot denna bakgrund finns anledning att se strängare på personuppgifter som förekommer i en förundersökning än sådana som utgör underrättelseuppgifter. Det finns flera mekanismer som tillgodoser skyddet för dessa uppgifter, bland annat sekretessbestämmelser och regleringen av belastnings- och misstankeregister. En annan sådan mekanism är att de regler som följer av brottsdatalagen.

Vi anser att det finns övervägande skäl som talar för att Säkerhetspolisen, då personuppgifter behandlas för att utreda eller lagföra brott, så långt det är möjligt ska särskilja olika kategorier av registrerade så att det framgår om personen är misstänkt, dömd för brott, brottsoffer eller någon annan som berörs av ett brott. Bestämmelsen bör dock endast gälla de utredningar som Säkerhetspolisen ansvarar för. Om uppgifter från en förundersökning även behandlas för underrättelseändamål, gäller alltså kravet inte i den verksamheten.

Det finns inte skäl att det generellt ska vara Säkerhetspolisens ansvar att särskilja kategorier av registrerade exempelvis om uppgifterna behandlas för att utlämnas till annan svensk eller utländsk myndighet.

Bestämmelsen gäller så långt det är möjligt. Detta innebär att kraven kan vara beroende på vilket systemstöd som de aktuella personuppgifterna behandlas med och var de förekommer. När

personuppgifter behandlas i ett förundersökningsprotokoll är möjligheterna att särskilja roller goda och behovet stort. När personuppgifter från ett it-beslag inom en förundersökning analyseras med hjälp av ett analysprogram är möjligheterna att särskilja rollerna ofta begränsade. Det finns inte heller samma behov av att särskilja de olika rollerna i det systemet.

Bestämmelsen riktar således in sig främst på uppgifter som behandlas i förundersökningsprotokollet och som kan förväntas vara åtkomliga för många personer. Syftet med bestämmelsen är att förhindra att exempelvis en uppgiftslämnare missuppfattas som delaktig i brottslig verksamhet vilket skulle kunna få stora konsekvenser exempelvis om uppgiften delges någon som saknar insyn i förundersökningen.

8.14 Särskilda bestämmelser om känsliga personuppgifter

8.14.1 Dataskyddskonventionens bestämmelser

Article 6 – Special categories of data

1. The processing of:

– genetic data;

– personal data relating to offences, criminal proceedings and convictions, and related security measures;

– biometric data uniquely identifying a person;

– personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life,

shall only be allowed where appropriate safeguards are enshrined in law, complementing those of this Convention.

2. Such safeguards shall guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination.

I den ursprungliga dataskyddskonventionen från 1981 är vissa personuppgifter utpekade som särskilt skyddsvärda. Det gäller uppgifter som avslöjar ras, politiska åsikter eller religiös eller annan övertygelse, personuppgifter som rör hälsa eller sexualliv samt fällande domar i brottmål. Genom det tilläggsprotokoll som utgör dataskyddskon-

ventionen 108+ läggs till dessa även personuppgifter som avslöjar etniskt ursprung och fackföreningsmedlemskap. Utöver fällande domar i brottmål omfattas även andra liknande uppgifter som rör brott, straffrättsliga förfaranden och relaterade säkerhetsåtgärder i den uppdaterade konventionen. Därutöver har ytterligare två kategorier av särskilt skyddsvärda uppgifter lagts till: genetiska uppgifter och biometriska uppgifter som entydigt identifierar en person (artikel 6.1). Konventionens uppräkning av särskilt känsliga personuppgifter är i stort sett likalydande med vad som anges i det EU-rättsliga dataskyddsregelverket.[98]

Konventionen 108+ kräver att behandling av känsliga personuppgifter får ske endast när tillräckliga säkerhetsmekanismer är föreskrivna för att motverka de risker som behandlingen kan innebära för den registrerades enskilda intresse, rättigheter och grundläggande friheter. Särskilt ska risken för diskriminering motverkas (artikel 6.2). Konventionens generella utformning innebär att medlemsstaterna är fria att utforma sådana säkerhetsmekanismer på lämpligt sätt. Exempel som anges i kommentaren till konventionen är ett krav på uttryckligt samtycke för behandling, författningsreglering av de undantagsfall då behandling ska vara tillåten eller krav på föregående konsekvensanalys och särskilt utformade skyddsåtgärder. Noterbart är att varken dataskyddskonventionen 108 eller tilläggsprotokollet 108+ uttryckligen medger behandling av känsliga personuppgifter endast på grund av att de på ett tydligt sätt offentliggjorts av den registrerade.[99]

Skyddet för känsliga personuppgifter som föreskrivs i dataskyddskonventionen 108+ är absolut och det finns inga möjligheter att göra undantag från bestämmelsen, ens i verksamheter som rör nationell säkerhet eller försvar.

[98] I dataskyddsförordningen och brottsdatadirektivet är sexuell läggning särskilt uppräknat. I dataskyddskonventionen anses detta ingå i begreppet sexualliv. Uppgifter om fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder har ett dataskydd som är utformat på annat sätt än för övriga känsliga personuppgifter i dataskyddsförordningen (och regleras inte i direktivet). Skyddet för sådana uppgifter har getts ett relativt starkt skydd i EU-domstolens praxis, se mål C–439/19 och C–740/22.
[99] Jfr artikel 9.1.e i dataskyddsförordningen.

8.14.2 Europakonventionen och regeringsformen

Europadomstolen har i sin praxis, i första hand angående artikel 8 i Europakonventionen, tillerkänt vissa känsliga personuppgifter ett förhöjd skydd. I flera fall har domstolen haft anledning att påpeka att etnisk härkomst är en viktig beståndsdel av den enskildes privatliv som förtjänar ett starkt skydd. I exempelvis fallet *Ciubotaru mot Moldavien*[100] ansåg domstolen att en enskild måste ha särskilda möjligheter att ifrågasätta den etnicitet som registrerats av myndigheter. I fallet *Catt mot Förenade kungariket*[101] slog domstolen fast att uppgifter om en persons politiska uppfattning är så känslig att den endast får behandlas av brottsbekämpande myndigheter med förhöjt skydd. Uppgifter om en persons religiösa eller filosofiska övertygelse utgör både en del av privatlivet och av religionsfrihet vilket innebär att de måste behandlas med särskild aktsamhet. Domstolen har även, i fallet *Mockutė mot Litauen*[102] bland annat slagit fast att information om en persons sexualliv, moraliska integritet och psykiska hälsa utgör mycket känsliga uppgifter och som måste skyddas enligt artikel 8. Europakonventionen tillförsäkrar därför i sig ett förhöjt skydd för vissa känsliga personuppgifter.

I 2 kap. 6 § andra stycket regeringsformen skyddas var och en mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. I förarbetena till bestämmelsen har uttalats att det med *betydande intrång* ska läggas stor vikt vid uppgifternas karaktär. Ju känsligare uppgifterna är, desto mer ingripande måste det allmännas hantering av uppgifterna normalt anses vara. Även hantering av ett litet fåtal uppgifter kan med andra ord innebära ett betydande intrång i den personliga integriteten, om uppgifterna är av mycket känslig karaktär.[103] Av förarbetena framgår inte någon uppräkning av vilka uppgifter som är så känsliga att endast ett fåtal av dem skulle kunna innebära ett betydande intrång. Däremot anges att vad som utgör ett betydande integritetsintrång måste bedömas utifrån de samhällsvärderingar som råder vid varje givet tillfälle.[104] Det kan därför antas att de uppgifter som

[100] Europadomstolens dom den 27 april 2010 i mål nr 27138/04.
[101] Europadomstolens dom den 24 januari 2019 i mål nr 43514/18.
[102] Europadomstolens dom den 27 februari 2018 i mål nr 66490/09.
[103] Prop. 2009/10:80 s. 183.
[104] Ibid. s. 185.

ur kvalitativ bemärkelse får anses utgöra ett betydande intrång att registrera enligt regeringsformen i dag motsvarar de särskilda kategorier av personuppgifter som anges i dataskyddskonventionen och EU:s dataskyddsregelverk. Detta kan dock komma att förändras. Hur känslig en uppgift är kan skifta över tid och även vara beroende av kontext. En uppgift om sexuell läggning eller om en abort kan vara oerhört känslig för vissa personer eller i en viss kontext medan andra kan vara helt öppna även med sådana uppgifter.

Vid sidan av integritetsskyddet i regeringsformen föreskrivs i 2 kap. 3 § att ingen svensk medborgare utan samtycke får antecknas i ett allmänt register enbart på grund av sin politiska åskådning. Bestämmelsen innebär bland annat att en registrering som helt saknar samband med politisk åskådning inte får kompletteras med en sådan anteckning. En sådan anteckning får nämligen anses vara helt självständig och därmed grundad enbart på den registrerades åskådning. Bestämmelsen utgör däremot inte något hinder mot att exempelvis uppgift om partitillhörighet tillförs personer som på andra grunder än enbart sin politiska åskådning kan betraktas som säkerhetsrisker. Grunden för anteckningen är i detta fall att vederbörande anses utgöra en sådan risk.[105] Till skillnad mot integritetsskyddet i 2 kap. 6 § regeringsformen är förbudet mot åsiktsregistrering absolut.

8.14.3 Känsliga personuppgifter i EU-rätten

De flesta myndigheter behöver inte behandla uppgifter om exempelvis etnicitet, religiös övertygelse eller hälsa för att kunna utföra sina arbetsuppgifter på ett effektivt sätt. För sådana verksamheter är det följaktligen lämpligt med ett generellt förbud att behandla känsliga personuppgifter eller en instruktion om särskild prövning för att sådana uppgifter ska få behandlas. I andra verksamheter förekommer känsliga uppgifter hela tiden, som exempelvis inom sjukvården där känsliga hälsodata löpande behandlas. I dessa fall är det inte rimligt med en lagstiftning vars utgångspunkt är att uppgifter om hälsa inte får behandlas. I stället bör verksamheten vara uppbyggd på så sätt att uppgifterna behandlas med särskilt skydd, i form av bland annat tystnadsplikt.

[105] Prop. 1975/76:209 s. 118.

Dataskyddsförordningen bygger i stor utsträckning på denna princip: att verksamheter som inte behöver behandla känsliga personuppgifter normalt inte ska göra det och att verksamheter som behöver behandla sådana uppgifter ska göra det under särskilt skydd. För de brottsbekämpande myndigheterna anges i brottsdatadirektivet att känsliga personuppgifter endast får behandlas om

- det är absolut nödvändigt,
- det finns lämpliga skyddsåtgärder och
- behandlingen är tillåten enligt nationell rätt, sker för att skydda intressen av grundläggande betydelse för den registrerade eller annan, eller om den enskilde själv på ett tydligt sätt offentliggjort uppgiften.

Enligt EU-rätten har de brottsbekämpande myndigheterna därmed möjlighet att behandla alla slags känsliga personuppgifter, men endast om det är *absolut nödvändigt*.

8.14.4 Riskerna med att behandla känsliga personuppgifter

I dataskyddskonventionen motiveras det förstärkta skyddet för vissa uppgifter med att behandling av dessa kan leda till att enskildas fri- och rättigheter kränks på olika sätt.

Många av de särskilt skyddsvärda uppgifterna kan sägas utgöra kärnan av den personliga integriteten och privatlivets innersta sfär som så långt möjligt ska fredas från insyn. Det uppfattas i allmänhet som ett klart större intrång i den personliga integriteten att uppgifter som rör sexualliv, hälsa eller politiska åsikter finns registrerade än uppgifter om exempelvis namn, födelseort eller yrke. Detta oavsett om uppgifterna används i något otillbörligt syfte eller inte. Det finns ofta ett motstånd mot att frivilligt och utan skydd av anonymitet lämna ifrån sig uppgifter som är mycket privata.

Vidare pekas ofta på att många av de känsliga personuppgifterna är sådana som potentiellt riskerar att leda till diskriminering av olika slag. Uppräkningen av känsliga personuppgifter motsvarar därför i stor utsträckning olika diskrimineringsgrunder i annan lagstiftning och internationella instrument. Risken för diskriminering är sannolikt skälet till att det ska finnas särskilda skäl för

att exempelvis registrera en persons etniska ursprung. Även andra former av negativa konsekvenser för den enskilda har motiverat att exempelvis medlemskap i fackförening eller tidigare kriminalitet tillförts den kategori av personuppgifter som ska behandlas med större varsamhet än andra.

De uppgifter som inom den europeiska personuppgiftsrätten har pekats ut som särskilt skyddsvärda har det gemensamt att de är intimt kopplade till grundläggande fri- och rättigheter. Dessa rättigheter är sådana som avser förhållandet mellan medborgare och stat. Om en myndighet har tillgång till känsliga uppgifter om den registrerades mest intima sfär, såsom hans eller hennes sexualliv eller hälsa, kan de potentiellt komma att utnyttjas för att kränka personens värdighet eller integritet. På samma sätt kan en myndighets kartläggning av bland annat enskildas politiska åsikter eller trosuppfattning medföra en risk för demokratin.

Behandling av känsliga personuppgifter kan också i sig innebära eller vara en förutsättning för ett intrång eller en kränkning av andra rättigheter. Om staten behandlar uppgifter om enskildas religiösa eller filosofiska övertygelse kan det exempelvis utgöra ett intrång i Europakonventionens artikel 9, som skyddar tanke-, samvetes- och religionsfriheten. På samma sätt kan en registrering av en persons politiska åsikter innebära ett intrång i yttrandefriheten som garanteras av konventionens artikel 10. Behandling av uppgifter om fackföreningstillhörighet är en sådan uppgift som potentiellt kan leda till ett intrång i artikel 11, som skyddar föreningsfriheten.

8.14.5 Den nuvarande regleringen

Personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning får, enligt huvudregeln i 2 kap. 9 § säpodatalagen, inte behandlas. Enligt paragrafens andra stycket får sådana uppgifter dock komplettera andra uppgifter, om en person om det är absolut nödvändigt för ändamålet med behandlingen.

En biometrisk uppgift är en personuppgift som rör en persons fysiska, fysiologiska eller beteendemässiga kännetecken, som tagits fram genom särskild teknisk behandling och som möjliggör eller

bekräftar unik identifiering av personen. Sådana uppgifter, som exempelvis resultatet från en analys som skett med hjälp av ansiktsigenkänningsprogramvara, får behandlas om det är absolut nödvändigt för ändamålet med behandlingen (2 kap. 10 § säpodatalagen).

En genetisk uppgift är personuppgifter som rör en persons nedärvda eller förvärvade genetiska kännetecken och som härrör från analys av ett spår av eller ett prov från personen. Denna definition innebär att analyser som resulterar i så kallade dna-profiler, som syftar till att bekräfta en persons identitet, inte omfattas av begreppet.[106] Det som avses är i stället kromosom-, dna- och rna-analyser eller andra liknande analyser av prov eller spår, som gör det möjligt att inhämta unik information om bland annat en persons fysiologi, hälsa eller biogeografiska ursprung.[107] Genetiska uppgifter får i dagsläget inte behandlas hos Säkerhetspolisen (2 kap. 10 § säpodatalagen).

Vid sidan av de regler som gäller all behandling av känsliga personuppgifter finns även ett generellt sökförbud i syfte att få fram ett urval av personer grundat på känsliga personuppgifter. Sådana sökningar får dock göras avseende känsliga personuppgifter (med undantag för uppgifter om medlemskap i fackförening, ”ras” och biometriska uppgifter), om det är absolut nödvändigt för vissa ändamål.

8.14.6 Säkerhetspolisen bör kunna behandla känsliga personuppgifter i större utsträckning än i dag

Bedömning: Säkerhetspolisen bör kunna behandla känsliga personuppgifter i större utsträckning än i dag. Det bör därför inte föreskrivas ett generellt förbud mot att behandla känsliga personuppgifter.

[106] Jfr dock prop. 2017/18:232 s. 150. Där anges att ”genetiska uppgifter behandlas vid dna-analyser för att ta fram dna-profiler eller forensiska uppslag”. Varken den tekniska analysen av biologiskt material i syfte att få fram en dna-profil eller dna-profilen i sig bör dock anses utgöra behandling av genetiska uppgifter enligt definitionen eftersom ingen information om en persons nedärvda eller förvärvade genetiska kännetecken framgår av analysen.
[107] Prop. 2017/18:232 s. 86 f.

Förbudet mot att behandla känsliga personuppgifter är systematiskt felaktigt

Som framgått finns det i säpodatalagen ett generellt förbud mot att behandla känsliga personuppgifter. Från förbudet finns ett undantag för uppgifter som är absolut nödvändiga för Säkerhetspolisen att behandla. Från ett systemperspektiv kan det således sägas att lagstiftningens utgångspunkt är att Säkerhetspolisen normalt inte har behov av att behandla känsliga personuppgifter i sin verksamhet, men att det i undantagssituationer får ske på samma sätt som EU-rätten föreskriver för andra brottsbekämpande myndigheter.

Denna utgångspunkt stämmer uppenbarligen inte med Säkerhetspolisen verksamhet. Det finns ett tydligt och legitimt behov av att i relativt stor utsträckning behandla olika slags känsliga personuppgifter. I många fall är sådan behandling även helt avgörande för verksamheten. Exempelvis kräver Säkerhetspolisens kartläggning av religiöst eller politiskt motiverad terrorism att känsliga uppgifter om religiös åskådning eller politisk uppfattning behandlas. Det framstår därmed som felaktigt att föreskriva ett generellt förbud mot behandling av sådana personuppgifter som är en förutsättning för att Säkerhetspolisen ska kunna utföra sitt uppdrag.

På samma sätt som att hälsodata får behandlas inom sjukvården bör säpodatalagen bygga på att Säkerhetspolisen får behandla de uppgifter som behövs för att utföra myndighetens uppdrag. Den nya säpodatalagen bör därför föreskriva andra mekanismer för att förebygga missbruk av de känsliga uppgifter som måste behandlas.

Den högre behandlingströskeln för behandling av känsliga personuppgifter är inte motiverad

Förbudet för Säkerhetspolisen att behandla känsliga personuppgifter kompletteras av ett undantag då sådan behandling trots allt är tillåtet. Av säpodatalagen följer att personuppgifter som behandlas om en person får kompletteras med känsliga personuppgifter, om det är absolut nödvändigt. Kravet på absolut nödvändighet innebär enligt förarbetena att behandling av känsliga personuppgifter ska vara restriktiv och att behovet av att komplettera personuppgifts-

behandlingen med känsliga personuppgifter ska prövas noga i det enskilda ärendet.[108]

Prövningen av behovet av uppgiften mot den högre behandlingströskeln i varje enskilt ärende medför praktiska svårigheter för en myndighet som ägnar sig åt informationsinhämtning. Det är fullt rimligt att en myndighet avstår från att aktivt hämta in känsliga personuppgifter som inte är relevanta för verksamheten eller vidtar åtgärder för att sådana uppgifter inte ska lämnas till myndigheten. I en förhörssituation ska exempelvis inte frågor ställas om etnicitet eller sexuell läggning, om det inte är absolut nödvändigt för ändamålet.

Den högre behandlingströskeln innebär emellertid ett bekymmer i de fall då känsliga personuppgifter förekommer integrerade i annan relevant information. Att det är olika behandlingströsklar för olika uppgifter innebär att ett dokument, där både känsliga och andra personuppgifter förekommer, inte kan prövas i sin helhet. Principen om att behovet av varje känslig personuppgift ska prövas för sig innebär att det kan krävas att känsliga personuppgifter som inte är absolut nödvändiga för ändamålet kan behöva maskeras eller raderas ur sitt sammanhang. I inhämtade textdokument, e-post eller chattkonversationer kan därmed känsliga personuppgifter behöva maskeras i löpande text. I avlyssnade samtal kan på motsvarande sätt en känslig personuppgift som nämns, men som inte är absolut nödvändig för ändamålet, behöva ersättas med ett pip. Den arbetsinsats som krävs för att rensa information från känsliga personuppgifter som inte är absolut nödvändiga ska inte underskattas. Problemet är givetvis mest påtagligt inom underrättelseverksamheten där inflödet av information kan vara mycket stort (se avsnitt 6.1 och 6.2).

Det framstår som att den nuvarande regleringen i första hand är anpassad för personuppgifter som aktivt hämtas in eller som i stor utsträckning är avsedd att bearbetas manuellt, genom exempelvis upprättande av en promemoria eller införande av uppgifter i olika personregister. Som tidigare nämnts motsvarar detta sätt att se på informationshantering varken de mycket stora informationsflöden som generas i dagens samhälle eller det arbetssätt som krävs av Säkerhetspolisen för att myndighetens ska kunna utföra sitt nuvarande uppdrag på ett effektivt sätt.

[108] Se prop. 2018/19:163 s. 77 och prop. 2009/10:85 s. 325.

Vid sidan av att dagens reglering är systematiskt tveksamt är regleringen inte heller anpassad till verksamhetens behov. Till skillnad mot andra verksamheter där känsliga personuppgifter normalt sett måste hanteras för att utföra verksamheten utgår säpodatalagen från att samtliga känsliga personuppgifter ska utgöra ett särskilt motiverat undantag från annan personuppgiftsbehandling. Detta trots att uppgifterna endast mycket sällan kommer att behandlas av andra än Säkerhetspolisens personal, med sträng tystnadsplikt, under regelbunden tillsyn och omfattande intern kontroll.

Säkerhetspolisen bör få behandla känsliga personuppgifter

Som tidigare nämnts förekommer olika slags känsliga personuppgifter mycket ofta i utredningar som rör nationell säkerhet. Särskilt inom terrorismbekämpning men även avseende brott som rör nationell säkerhet med politiska förtecken är det närmast en huvudregel att känsliga personuppgifter behöver behandlas i någon utsträckning. Uppgifter som avslöjar politiska åsikter eller religiös övertygelse är givetvis fundamentala för att kartlägga exempelvis politiskt eller religiöst motiverade terrorister. I många fall kan även exempelvis psykisk hälsa vara en avgörande uppgift för att bedöma aktörers vilja att begå brott riktade mot en skyddsperson. I många fall utgörs ett signalement av känsliga personuppgifter där exempelvis etniskt ursprung eller fysiska kännetecken som rör personens hälsa anges.

Sverige har en förhållandevis sträng reglering avseende behandling av känsliga personuppgifter i jämförelse med de övriga länder vi har studerat. Detta kan till viss del förklaras med att säpodatalagen inte fullt ut är anpassad för Säkerhetspolisens verksamhet, utan i stora delar grundar sig på brottsdatadirektivet. Även i Norge har direktivet fått stort inflytande över den lagstiftning som gäller för säkerhetstjänsten PST. PST får följaktligen behandla känsliga personuppgifter endast om det absolut nödvändigt.[109] Nederländerna har en personuppgiftslag för underrättelsetjänsterna som är mer fristående från EU-rätten. I denna finns ett generellt förbud för underrättelsetjänsterna att *grunda* personuppgiftsbehandling på känsliga personuppgifter. Sådana uppgifter får behandlas om

[109] 7 § politiregisterloven (lov 28 maj 2010 nr 16).

det sker utöver behandlingen av andra personuppgifter och då med en högre behandlingströskel (som ungefär motsvarar absolut nödvändigt). Ett liknande förbud mot att *grunda* personuppgiftsbehandling på känsliga uppgifter återfinns även i den finska lagstiftningen. I Finland får emellertid underrättelsetjänsten Skypo behandla känsliga personuppgifter enligt samma behandlingströskel (nödvändigt) som andra uppgifter om bland annat en persons verksamhet och beteende. I Danmark, som har en skräddarsydd lag för säkerhetstjänsten PET:s verksamhet, finns däremot inte några särskilda regler för behandling av känsliga personuppgifter, annat än ett förbud mot åsiktsregistrering av ”lovlig politisk verksamhet”. Det uppställs dock krav på tekniska och organisatoriska åtgärder för att förhindra missbruk av känsliga personuppgifter som behandlas, som loggning och åtkomstbegränsning. Även underrättelsetjänsterna i Förenade kungariket får behandla känsliga personuppgifter i stort sett enligt samma regelverk som andra personuppgifter. Se även kapitel 4 om de refererade utländska rättssystemen.

Det finns skäl för mer tillåtande reglering för behandling av känsliga personuppgifter

I de länder vi jämfört finns därmed inte något exempel på lagstiftning som innehåller ett generellt förbud mot att behandla känsliga personuppgifter. Däremot förekommer i flera länder förbud mot att grunda behandling av på känsliga personuppgifter.

Vi anser inte heller att det är lämpligt att behålla den huvudregel som i dag förbjuder behandling av sådana uppgifter. Många av de uppgifter som ingår i kategorien känsliga personuppgifter utgör en naturlig och, i förhållande till andra brottsbekämpande myndigheter, särskiljande del av Säkerhetspolisens uppdrag. Att förse ett förbud med ett undantag som i praktiken tillämpas som en huvudregel är vidare systematiskt felaktigt och kan uppfattas som missvisande.

Den nuvarande regleringen påverkar Säkerhetspolisens verksamhet i betydande grad. Dagens krav på absolut nödvändighet för behandling av känsliga personuppgifter ska markera att sådana uppgifter ska användas restriktivt och behovet ska prövas noga i det enskilda ärendet. När information inkommer till myndigheten måste därför känsliga personuppgifter identifieras, granskas, bedömas

och om de vid tillfället inte kan anses vara absolut nödvändiga att behandla maskeras eller tas bort.

Till skillnad från andra delar av personuppgiftsgranskning är det svårt att effektivisera denna process. I vissa fall kan det konstateras att det finns ett behov av alla uppgifter för ett visst ändamål och att de är adekvata och relevanta. Däremot är det svårt att generellt bedöma om samtliga känsliga personuppgifter är absolut nödvändiga för ändamålet. Om informationen exempelvis har koppling till islamistisk terrorism kan det förvisso konstateras att alla uppgifter som rör religiös övertygelse är absolut nödvändiga. Däremot går det inte att säga att alla uppgifter som rör hälsa är det. Det innebär att all information måste granskas mycket noga för att bedöma om någon uppgift kan avslöja en persons hälsa, och om sådan information förekommer måste nödvändigheten av denna uppgift prövas mot ändamålet.

Denna prövning är inte anpassad till att det numera förväntas att Säkerhetspolisen ska kunna hantera mycket stora informationsmängder, som i princip undantagslöst innehåller känsliga personuppgifter av olika slag. Säpodatalagen bygger vidare på den 15 år gamla polisdatalagens regler i detta avseende. Då riksdagen tog ställning till säpodatalagen hade den första smarta telefonen, iPhone, nyligen lanserats. De få svenskar som hade möjlighet att komma över flaggskeppsmodellen kunde lagra 8 gigabyte data på sin enhet. Den senaste modellen av iPhone har 32 gånger så stor lagringskapacitet (och ofta väsentligt större kapacitet i olika integrerade molntjänster). Det är numera ovanligt att det överhuvudtaget raderas information från exempelvis e-post eller olika meddelandetjänster som därför kan innehålla uppgifter som ackumulerats under många år. Mängden information som ett normalt it-beslag i dag genererar kräver mångdubbelt med resurser att granska, än vad som förutsattes då reglerna infördes. En betydande del av dessa resurser går ut på att granska förekomsten av och pröva nödvändigheten av känsliga personuppgifter. Se avsnitt 6.1.3.

8.15 Hur bör behandling av känsliga personuppgifter regleras?

8.15.1 Bör samtliga känsliga personuppgifter regleras på samma sätt?

Bedömning: Biometriska uppgifter bör få behandlas som andra personuppgifter.

Det behövs inte några särskilda bestämmelser om behandling av uppgifter om straffrättsliga förfaranden och liknande.

Det bör inte införas några särskilda bestämmelser om uppgifter som offentliggjorts av den registrerade.

Förslag: Säkerhetspolisen ska inte få behandla genetiska uppgifter.

Bör behandling av vissa uppgifter som är tillåten i dag förbjudas?

Den brottskatalog som Säkerhetspolisen ansvarar för utmärks av att brottsligheten ofta är religiöst, politiskt eller på annat sätt ideologiskt motiverad och brott där uppgifter om etniskt ursprung kan vara relevanta. Den brottsbekämpande verksamheten som Säkerhetspolisen ansvarar för innebär däremot inte någon naturlig koppling till frågor som rör medlemskap i fackförening, hälsa, sexualliv eller sexuell läggning. Det skulle därmed kunna vara möjligt att särskilt reglera vissa av de känsliga personuppgifterna, som inte har någon koppling till Säkerhetspolisens kärnverksamhet.

Principiellt kan det vara korrekt att reglera frågor som ligger långt utanför kontexten nationell säkerhet på samma sätt som för andra brottsbekämpande myndigheter. Redan i dag har Säkerhetspolisen ett särskilt sökförbud avseende uppgifter som kan avslöja medlemskap i fackförening, vilket motiverats med att myndigheten inte har något behov av att göra sökningar på medlemskap i fackförening.[110] Det går att argumentera på samma sätt avseende behandling av personuppgifter som rör exempelvis sexualliv eller sexuell läggning och behålla dagens generella behandlingsförbud för sådana uppgifter.

[110] Prop. 2018/19:163 s. 80.

Samtliga uppgifter, som betecknas som känsliga personuppgifter kan dock i olika sammanhang vara relevanta att behandla inom Säkerhetspolisens verksamhet, även om behovet inte tydligt framgår i dagsläget. Grupper som utmärks genom känsliga personuppgifter kan utgöra måltavlor för bland annat terror, exempelvis på grund av sin religion eller sexuella läggning. Det är svårt att i dag förutse eller helt avfärda att även andra grupper, som exempelvis fackföreningar, skulle kunna bli måltavlor för sådan brottslig verksamhet som Säkerhetspolisen ska bekämpa. På samma sätt kan rörelser, som det i dag inte finns skäl för Säkerhetspolisen att bevaka, i framtiden radikaliseras. Det finns exempel från vår omvärld där medlemmar i den så kallade ”incel-rörelsen” radikaliserats i en våldsbejakande riktning. Samtliga av dessa exempel kräver en omfattande behandling av känsliga personuppgifter.

Ett ytterligare skäl som talar emot att ange en högre tröskel för behandling av vissa uppgifter är svårigheten att identifiera och pröva uppgifter var för sig. För Säkerhetspolisens del är det i dagsläget sällan är absolut nödvändigt att behandla uppgifter om enskildas sexualliv eller fackföreningstillhörighet. Om sådana uppgifter ska särbehandlas krävs emellertid en noggrann granskning för att identifiera just dessa uppgifter, eller andra uppgifter som kan vara avslöjande i detta avseende. En sådan ingående granskning och den noggranna prövningen som krävs för att bedöma om uppgiften är absolut nödvändig är ett stort verksamhetshinder för Säkerhetspolisen i dagsläget. Ett sådant krav redan för behandling i form av insamling och lagring måste motiveras av mycket tungt vägande integritetsskäl. Vi anser inte att skälen som talar för detta väger tillräckligt tungt för någon av de särskilda kategorierna uppgifter som betecknas som känsliga.

Vår slutsats är även att samtliga känsliga personuppgifter bör hanteras på samma sätt, trots att vissa kategorier kommer att behandlas mer frekvent än andra. Både nu gällande och den av oss föreslagna lagstiftning bygger på principer om ändamål, adekvans, relevans och uppgiftsminimering som begränsade faktorer för all personuppgiftsbehandling. Personuppgifter som inte behövs får inte behandlas, oavsett om de betecknas som känsliga eller inte.

Inga särskilda regler behövs för att skapa och bevara biometriska uppgifter

En särskild typ av känslig personuppgift är sådana som rör en persons fysiska, fysiologiska eller beteendemässiga kännetecken, som tagits fram genom särskild teknisk behandling och som möjliggör eller bekräftar unik identifiering av personen. Typiskt sett utgörs detta av DNA-profiler, fingeravtryck eller ansiktsigenkänning. Det finns dock flera tekniska metoder att utifrån till exempel bild, video, tal eller text hitta utmärkande kännetecken hos en individ och det sker en kontinuerlig teknisk utveckling inom detta område.

Behandling av biometriska uppgifter genom ansiktsigenkänning kan ske på exempelvis följande sätt. Olika datamodeller identifierar först alla ansikten i materialet. Därefter bearbetas dessa genom att olika programvaror bland annat rätar upp, kompenserar för bildvinkel och bedömer om det identifierade ansiktet är av tillräcklig kvalité för att kunna jämföras. Slutligen skapas en så kallad vektor av varje enskilt ansikte i bilden som uppfyller kraven för jämförelse. En ansiktsvektor är en generisk beskrivning av ansiktsdrag genom att olika parametrar, exempelvis avståndet mellan ögonen, ges numeriska värden. En ansiktsvektor är en datafil med hundratals parametrar som var och en getts ett numeriskt värde. Denna datafil är den biometriska uppgiften som möjliggör eller bekräftar unik identifiering av personen. Bildmaterialet, som vektorn är hämtad från, utgör däremot inte biometriska uppgifter.

Andra tekniska tillämpningar som finns för att på motsvarande sätt vektorisera fysiska, fysiologiska eller beteendemässiga kännetecken kan vara röstigenkänning från ljudinspelningar eller analys av rörelsemönster hos en individ från rörlig bild. Flera sådana biometriska analysmetoder kan även användas parallellt för att öka träffsäkerheten vid en jämförelse.

Behovet av att kunna behandla biometriska uppgifter inom Säkerhetspolisens verksamhet är stort. I praktiken finns behov av att en stor andel av det bildmaterial som Säkerhetspolisen behandlar ska genomgå den särskilda tekniska behandlingen som skapar en biometrisk uppgift i form av bland annat en ansiktsvektor. I annat fall finns det inget material att göra jämförelser mot om Säkerhetspolisen exempelvis skulle ha behov av att identifiera en viss person endast utifrån ett fotografi. Behovet av att behandla biometriska

uppgifter är därmed i praktiken lika stort som behovet av att överhuvudtaget behandla personuppgiften i form av exempelvis ett bildmaterial.

Det står klart att Säkerhetspolisen kommer att behöva utnyttja biometri i sitt brottsförebyggande och brottsbekämpande uppdrag. I dagsläget innebär kravet på absolut nödvändighet att exempelvis bilder av personer kan behandlas men inte nödvändigtvis den ansiktsvektor (i princip en numerisk lista) som kan användas för att automatiskt jämföra personen på bilden mot andra bilder. För att få skapa en ansiktsvektor eller någon annan biometrisk uppgift krävs att det är absolut nödvändigt för ändamålet.

Om ändamålet med att bevara exempelvis en övervakningsfilm är att kontrollera om en viss misstänkt person förekommer, krävs att biometriska uppgifter skapas för alla personer som syns i bildmaterialet för att kunna jämföras med den misstänktes biometri. Det kan röra sig om tusentals personer som passerar en övervakningskamera, där endast en är absolut nödvändigt att identifiera. Det kan ifrågasättas om det i dagsläget är absolut nödvändigt att behandla samtligas biometriska uppgifter för att göra jämförelsen. Efter att den biometriska jämförelsen är avslutad finns under alla omständigheter knappast något sådant absolut behov och samtliga uppgifter måste då raderas. Detta innebär att stora databehandlingar måste genomföras för att skapa nya biometriska uppgifter av ett biometriskt underlag inför varje enskild sökoperation. Det är både tidskrävande och ineffektivt.

Bevarandet av datafilen med den biometriska uppgiften, exempelvis det numeriska värdet för ansiktsparametrarna i en ansiktsvektor, är i sig inte särskilt integritetskänsligt. De flesta anser nog att bilden som den biometriska uppgiften är hämtad från är mer känslig. Däremot kan olika behandlingsåtgärder med de biometriska uppgifterna vara både integritetskänsliga och på andra sätt särskilt riskfyllda ur ett fri- och rättighetsperspektiv. Det finns därför skäl att begränsa hur biometriska uppgifter får användas.

Vi anser dock att skapande och bevarande av biometriska uppgifter i sig inte utgör en sådan särskilt känslig behandlingsåtgärd. Det är snarare en förutsättning för att det ska finnas skäl att behandla exempelvis rörlig bild. Enligt vår uppfattning bör behandling genom skapande och bevarande av biometriska uppgifter inte ske med större restriktivitet än insamling och bevarande av det

biometriska underlaget, i form av exempelvis film-, bild- eller ljudinspelningar.

Det finns inte skäl att tillåta Säkerhetspolisen att behandla genetiska uppgifter

I dagsläget finns ett absolut förbud för Säkerhetspolisen att behandla genetiska personuppgifter (2 kap. 10 § säpodatalagen). Under utredningen har frågan uppkommit om vad detta förbud innebär och om det bör kvarstå.

En genetisk uppgift utmärks av att den dels rör en persons nedärvda eller förvärvade genetiska kännetecken, dels härrör från analys av ett spår av eller ett prov från personen (se definitionen av i 1 kap. 5 § säpodatalagen). De genetiska kännetecken som avses ska alltså framkomma genom en analys av genetiskt material. Om exempelvis en persons hårfärg framkommer genom ett fotografi, är detta inte en genetisk uppgift, trots att detta kännetecken är nedärvt. I likhet med biometriska uppgifter är det inte källmaterialet som avses, som ett blod- eller vävnadsprov, utan vissa resultat från en analys av detta material. Den genetiska uppgiften är den information som så att säga lämnar laboratoriet i läsbar form.

Genetiska uppgifter är mycket strängt reglerat i Sverige. Till att börja med kan konstatera att definitionen av vad som utgör en genetisk uppgift är betydligt bredare i brottsdatalagen och säpodatalagen än i brottsdatadirektivet. I brottsdatadirektivet krävs dels att det genetiska kännetecknet ger ”unik information” dels att det ska avse en persons ”fysiologi eller hälsa”. En genetisk uppgift i de svenska lagstiftningarna omfattar å andra sidan alla genetiska kännetecken, det vill säga även de som inte ger unik information för varje person och även sådana som avser annat än fysiologi eller hälsa.

Skälet till detta är att regeringen ansåg att även andra uppgifter, som exempelvis en persons biogeografiska ursprung, som kan tas fram genom motsvarande analys förtjänade samma skydd som fysiologiska uppgifter om bland annat hud- eller hårfärg. Däremot finns inget motiv till att den svenska definitionen omfattar alla kännetecken, även sådana som inte är unika för en person.[111] Vidare finns i den svensk rätt omfattande förbud mot att behandla genetiska

[111] Se prop. 2017/18:232 s. 86–87. Det bör i sammanhanget noteras att endast 1 av 1 000 baspar i en mänsklig DNA-sträng är unik för en individ.

uppgifter. Av de brottsbekämpande myndigheterna är det endast Nationellt forensiskt centrum (NFC) vid Polismyndigheten som får behandla genetiska uppgifter och då endast om det är absolut nödvändigt (se 6 kap. 4 § polisens brottsdatalag). NFC får utföra forensiska analyser, undersökningar eller jämförelser åt bland annat Säkerhetspolisen. Regeringen uppfattade att genetiska uppgifter rent faktiskt behandlas enbart i den forensiska verksamheten vid NFC för att ta fram dna-profiler eller forensiska uppslag.[112] Regeringen ansåg därför inte att det fanns behov av att behandla genetiska uppgifter hos de myndigheter som kan lämna uppdrag åt NFC och till vilka resultaten av analysen skulle redovisas.[113]

Det omfattande förbudet mot att behandla genetiska uppgifter hos de brottsbekämpande myndigheterna har såvitt vi kunnat se inte någon motsvarighet i någon av de andra länder vi studerat. Däremot ställs ofta ett krav på absolut nödvändighet upp för sådan behandling. Därutöver är den svenska definitionen bredare än vad som följer av brottsdatadirektivet vilket innebär att fler uppgifter anses som genetiska i Sverige jämfört med andra EU-länder. Denna stränga reglering kan innebära ett problem för svenska myndigheter exempelvis i samarbetet och informationsdelningen med myndigheter i andra länder.

Genetiska uppgifter är inte någon central del av Säkerhetspolisens verksamhet och dagens reglering har därför inte beskrivits som något problem för myndigheten i dagsläget. Säkerhetspolisen har inte heller något behov av att behandla genetiska uppgifter som på något nämnvärt sätt skiljer sig från Polismyndigheten. Polismyndigheten har den 20 november 2024 skickat in en hemställan om en fullständig översyn av polisens brottsdatalag.[114] Där anges att översynen bör omfatta behoven för fler delar inom Polismyndigheten att behandla genetiska uppgifter varvid även innebörden av genetiska uppgifter kan behöva klargöras. Ärendet bereds i Regeringskansliet.

Frågan om behovet för Säkerhetspolisen att behandla genetiska uppgifter bör ses över tillsammans med andra myndigheter som har samma eller liknande reglering och som är beställare i förhållande

[112] Prop. 2017/18:232 s. 150.
[113] Prop. 2017/18:269 s. 154.
[114] *Hemställan om översyn av polisens brottsdatalag*, Polismyndighetens dnr A593.896/2024, Justitiedepartementets dnr Ju2024/02401.

till NFC. Den nuvarande regleringen bör överföras till den nya lagen i avvaktan på en sådan översyn.

Det behövs inga ytterligare regler avseende uppgifter om brott, straffrättsliga förfaranden och liknande

Av artikel 6.1 i dataskyddskonventionen 108+ följer att personuppgifter som rör brott, straffrättsliga förfaranden och fällande domar samt relaterade säkerhetsåtgärder är känsliga personuppgifter. I nuvarande säpodatalag regleras emellertid inte uppgifter av detta slag som känsliga personuppgifter. Det har sin bakgrund i att denna uppgiftskategori varken regleras särskilt i brottsdatadirektivet eller har ansetts utgöra känsliga personuppgifter i den tidigare polisdatalagen.

Visst skydd för dessa uppgifter finns i nuvarande säpodatalag. Personuppgifter som rör brottsmisstankar och liknande omfattas av särskilda regler avseende behandlingstid i 4 kap. 3 och 4 §§ (se avsnitt 8.18.9). I 4 kap. 5 § säpodatalagen finns även en begränsning avseende sökningar mot brottsmisstankar. Om en förundersökning eller ett åtal mot en person har lagts ner eller personen frikänts genom dom som fått laga kraft, får personen inte längre vara sökbar som misstänkt. Denna bestämmelse återfinns även i bland annat polisens brottsdatalag. I förarbetena förklaras att bestämmelsen inte ska tolkas så att uppgifter om att en viss person har pekats ut eller hörts som misstänkt inte längre får behandlas. Däremot ska det inte längre vara möjligt att vid sökning i elektroniskt lagrat material återfinna den utpekade personen genom en sökning efter misstänkta personer. Bestämmelsen utesluter således inte att personen anges som ”tidigare misstänkt”, förutsatt att det framgår att han eller hon inte längre är det.[115]

Det framstår som helt naturligt att en person som inte är misstänkt för brott hos Säkerhetspolisen inte heller ska vara sökbar som det. Det skulle kunna framstå som ett omotiverat intrång i enskilds rätt att en myndighet vid en sökning efter misstänkta personer inte skulle ta hänsyn till exempelvis frikännande domar. Den nuvarande sökbegränsningen bör därför kvarstå som en skyddsmekanism. Den gäller emellertid endast misstankar om fullbordade brott som

[115] Prop. 2009/10:85 s. 349.

utreds av Säkerhetspolisen och inte så kallade underrättelsemisstankar, som rör deltagande i brottslig verksamhet.

För en brottsbekämpande myndighet som Säkerhetspolisen bör dock behandling av känsliga personuppgifter i form av brott, straffrättsliga förfaranden och fällande domar samt relaterade säkerhetsåtgärder inte i övrigt särregleras. Det finns ett generellt och fullt legitimt behov av att behandla uppgifter om kriminell belastning hos personer som Säkerhetspolisen i övrigt har anledning att registrera. Till skillnad mot andra känsliga personuppgifter, om exempelvis politisk övertygelse eller trosuppfattning bör uppgifter som rör bland annat fällande domar kunna utgöra grunden för en registrering.

Det är rimligt att Säkerhetspolisen, om det finns behov av det, kan hålla register över exempelvis personer dömda för terrorbrott för att kartlägga brottslig verksamhet av detta slag. Exempelvis bör det vara möjligt att hålla sammanställningar av dömda terrorister, även om det endast är den fällande domen som utgör grund för registrering. Någon särreglering av hur sådana uppgifter generellt får behandlas bör därför inte införas.

Samma regler bör gälla för känsliga personuppgifter som offentliggjorts av den enskilde själv

Den tidigare personuppgiftslagen innehöll ett generellt förbud mot behandling av känsliga personuppgifter som kompletterades av olika undantag. Ett sådant undantag var om den enskilde samtyckt till behandling eller på ett tydligt sätt själv offentliggjort uppgiften. Denna bestämmelse gällde ursprungligen även för Polismyndigheten och därmed även för Säkerhetspolisen.[116] Då den äldre polisdatalagen år 2010 ersattes av en ny polisdatalag skulle personuppgiftslagens bestämmelse om offentliggjorda personuppgifter inte längre tillämpas. Denna förflyttning diskuterades dock inte i förarbetena. Frågan togs inte heller upp då polisdatalagen ersattes av säpodatalagen. Enligt brottsdatadirektivet är ett tydligt offentliggörande från den registrerade en grund som tillåter att känsliga uppgifter behandlas (artikel 10 c).

[116] Se bland annat 5 § polislagen (1998:622).

I de nya personuppgiftslagarna för Försvarsmakten och FRA finns ett generellt förbud mot att behandla känsliga personuppgifter vid sidan av sådana som kompletterar andra uppgifter och är absolut nödvändiga. Denna huvudregel kompletteras emellertid med ett undantag för uppgifter som den registrerade har lämnat sitt uttryckliga samtycke eller på ett tydligt sätt har offentliggjort uppgifterna. Paragrafen ger Försvarsmakten och FRA möjlighet att i dessa situationer behandla känsliga personuppgifter på samma sätt som andra personuppgifter.[117] Ett tänkbart exempel på offentliggörande kan enligt förarbetena vara att den registrerade har gjort personuppgifterna tillgängliga på internet.[118]

Säkerhetspolisen har framfört ett liknande behov av att kunna registrera känsliga personuppgifter som offentliggjorts av den registrerade själv, genom att undanta sådana uppgifter från de skyddsmekanismer som gäller i övrigt. De skäl som förts fram för att inte betrakta offentliggjorda uppgifter som lika känsliga är att den enskilde kan sägas ha eftergett sin integritet. Att skydda uppgifter som den enskilde inte själv värnar skulle kunna ses som motsägelsefullt.

Vår bedömning är dock att detta synsätt inte har fog för sig. Även om en enskild i någon mån gett upp sin integritet och uppgiften inte längre kan anses vara en del av privatlivet när den på ett tydligt sätt har offentliggjorts består dess skyddsvärde. En uppgift om en enskild kan även avslöja saker om andra personer, exempelvis familjemedlemmar, som inte samtyckt till en publicering. Det är inte heller möjligt för en enskild att ångra sig när en uppgift väl är offentliggjord. Skyddet för känsliga personuppgifter är inte heller avsett endast för att värna den enskildes privatliv. Opinionsfriheterna, särskilt yttrandefriheten, skulle kunna påverkas negativt om exempelvis politiska eller religiösa yttranden skulle kunna grunda registrering på grund av att de offentliggjorts.

Vi kan inte se något behov av ett undantag avseende känsliga personuppgifter som offentliggjorts som skulle överväga de potentiella eller faktiska riskerna för bland annat den personliga integriteten eller den fria åsiktsbildningen. Någon reglering, motsvarande Försvarsmaktens och FRA:s, som innebär att offentliggjorda käns-

[117] Se 2 kap. 19 § försvarsdatalagen respektive 2 kap. 17 § FRA-datalagen.
[118] Prop. 2020/21:224 s. 185. Förslaget var ursprungligen motiverat av det felaktiga antagandet att den då ännu inte beslutade säpodatalagen skulle innehålla motsvarande bestämmelser och att Försvarsmakten hade samma behov som Säkerhetspolisen i denna del, se SOU 2018:63 s. 192.

liga personuppgifter inte ska omfattas av samma skydd som andra känsliga personuppgifter bör därför inte införas.

8.15.2 Bör det vara en högre behandlingströskel för känsliga personuppgifter?

Bedömning: En högre behandlingströskel för vissa uppgifter är inte en lämplig skyddsmekanism för känsliga personuppgifter i Säkerhetspolisens verksamhet. Dessa uppgifter bör därför skyddas på annat sätt.

Av vad som angetts i föregående avsnitt har vi kommit till slutsatsen att förbudet mot att behandla känsliga personuppgifter är systematiskt felaktigt och att det ofta är nödvändigt för Säkerhetspolisen att behandla dessa. Vi har vidare beskrivit problemet som den nuvarande ordningen medför. Säpodatalagen bygger på äldre lagstiftning i denna del och innebär ett krav på att känsliga uppgifter ska användas restriktivt och prövas noga i det enskilda fallet. Detta krav är inte anpassat efter Säkerhetspolisens verksamhet och inte heller rimligt att upprätthålla i förhållande myndighetens behov och de förväntningar som ställs på underrättelseverksamheten.

Det finns även verksamhetsskäl som med styrka talar mot att uppställa olika behandlingströsklar för olika uppgifter som samlas in och bevaras. Med en differentierad behandlingströskel på uppgiftsnivå kommer allt material att behöva genomgå en omfattande granskning och individuell prövning på ett sätt som är oförenligt med en effektiv informationshantering inom underrättelseverksamhet. Det framstår som orimligt betungande att Säkerhetspolisen ska ägna sig åt maskering av enskilda personuppgifter som förekommer i den stora och alltjämt växande informationsmängd som myndigheten måste behandla för att kunna utföra sitt uppdrag. Utgångspunkten bör vara att information som existerar i ett naturligt sammanhang kan hanteras gemensamt och att enskilda uppgifter om exempelvis etnicitet inte ska maskeras i ett dokument som i övrigt är relevant att bevara.

Skyddet för den personliga integriteten och andra grundläggande fri- och rättigheter samt mekanismer för att förhindra missbruk av känsliga personuppgifter bör därför utformas på ett annat sätt än

i dag. Vi har därmed kommit till slutsatsen att det inte är lämpligt att underkasta behandling av känsliga personuppgifter en särskild prövning av absolut nödvändighet. Det förstärkta skyddet för känsliga personuppgifter bör därför uppnås på annat sätt. Det prövas i det följande.

8.15.3 Känsliga personuppgifter bör inte få vara skälet till att en persons personuppgifter registreras

Förslag: Uppgifter om en person ska inte få behandlas enbart utifrån sådant som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller uppgifter som rör hälsa, sexualliv eller sexuell läggning.

Vi anser att andra säkerhetsmekanismer än en generellt högre behandlingströskel är lämpligt för att säkerställa att känsliga personuppgifter behandlas med stor varsamhet.

Skälet till att en persons uppgifter överhuvudtaget behandlas inom Säkerhetspolisen är inte att denne exempelvis har en viss politisk eller religiös åskådning. Detta skulle stå i strid både med förbudet mot åsiktsregistrering i 2 kap. 3 § regeringsformen och vara oförenligt med förutsättningarna att begränsa enskildas rätt till privatliv enligt 21 § i samma kapitel. Det är också oförenligt med kravet i Europakonventionens artikel 8.2 att en viss etnicitet, medlemskap i en fackförening eller en omständighet hänförlig till sexualliv eller hälsa utgör grund för registrering. Dessa grundläggande skyddsregler gäller förstås oavsett utformningen av säpodatalagen.

Det särskilda skyddet för känsliga personuppgifter bör byggas upp utifrån principen att sådana uppgifter inte får vara enda skälet till personuppgiftsbehandlingen. Det innebär att Säkerhetspolisen exempelvis inte aktivt får inhämta uppgifter om personer på grund av att de har viss politisk uppfattning, filosofisk övertygelse eller sexuell läggning. Ett liknande skydd för alla känsliga uppgifter kommer då att gälla som för politisk åskådning enligt 2 kap. 3 § regeringsformen. Vår uppfattning är att denna reglering innebär ett gott skydd mot de risker som behandling av känsliga personuppgifter kan innebära för enskilda och allmänna intressen.

Den föreslagna regleringen innebär att Säkerhetspolisen inte som i dag behöver maskera och gallra bland personuppgifter när exempelvis en chattkonversation som inhämtats innehåller uppgifter om att någon har stukat foten (uppgift om hälsa) eller där hälsningsfraser med religiöst ursprung används (uppgift som avslöjar religiös övertygelse). Informationshanteringen kommer därmed att kunna effektiviseras väsentligt.

Att behandlingströskeln därmed blir densamma som för andra personuppgifter medför att känsliga personuppgifter kommer att behandlas i större utsträckning än i dag. För att balansera detta föreslår vi att bestämmelsen ska kompletteras med begränsningar för sökning och sammanställning, till vilket vi återkommer i avsnitt 8.15.5.

En liknande reglering som den vi föreslår finns i 13 § domstolsdatalagen (2015:728). Där anges att uppgifter om en person inte får behandlas enbart på grund av vad som är känt om personen utifrån känsliga personuppgifter. Vår uppfattning är även att den föreslagna begränsningen för behandling grundad på känsliga personuppgifter ligger i linje med regleringen i många andra länder vad gäller nationell säkerhetstjänst, se kapitel 4.

8.15.4 Känsliga personuppgifter påverkar proportionalitetsprövningen

Bedömning: All behandling av personuppgifter ska vara proportionerlig. Behandling av känsliga personuppgifter innebär normalt ett större intrång i enskilda eller allmänna intressen än annan personuppgiftsbehandling. Skälet för att utföra behandling måste därför väga tyngre än vid annan personuppgiftsbehandling.

Dataskyddskonventionen hindrar inte behandling av känsliga personuppgifter enligt samma grundläggande krav som andra uppgifter. Däremot förutsätter konventionen att behandling av sådana uppgifter enbart ska vara tillåten om lämpliga, i lag föreskrivna, säkerhetsåtgärder är på plats för att slå vakt om de risker sådan behandling kan medföra (se avsnitt 8.14.1). Medlemsstaterna är fria att anpassa sådana säkerhetsåtgärder efter ändamålet med att känsliga personuppgifter överhuvudtaget behandlas.

Vi föreslår en rad regler som förstärker skyddet för känsliga personuppgifter, bl.a. ska sådana uppgifter inte ensamt få ligga till grund för behandling och sökningar på känsliga personuppgifter ska omfattas av särskilda begränsningar. Därtill kommer även att förekomsten av känsliga personuppgifter påverkar proportionalitetsbedömningen som ska göras.

När en säkerhetstjänst behandlar känsliga personuppgifter ökar rent generellt risken för intrång i grundläggande fri- och rättigheter. Detta har inget att göra med att det skulle finnas något sådant uppsåt hos Säkerhetspolisen. Den ökade risken kommer av att själva kartläggningen utgör ett intrång i enskildas privatliv och att detta intrång är högre om känsliga personuppgifter behandlas.

Att känsliga personuppgifter behandlas i enskilda fall ingår i Säkerhetspolisens uppdrag. Som framgår av avsnitt 8.2.4 föreslår vi att all personuppgiftsbehandling som sker med stöd av säpodatalagen ska vara proportionerlig. I prövning kan förekomsten av känsliga personuppgifter i behandlingen vara en av flera aspekter som måste bedömas. Proportionalitetsprövningen utgör den mekanism som på ett övergripande plan ska tillgodose att tillämpningen inte innebär en kränkning av enskilds rätt eller på annat sätt är oförenlig med ett demokratiskt samhälle. Denna prövning ersätter i stor utsträckning behovet av att det i lag ska framgå att behovet ska vara särskilt tungt, det vill säga absolut nödvändigt.

Proportionalitetsprincipen innebär att det inte enbart är behovet som avgör om känsliga personuppgifter får behandlas, utan om behandlingen är proportionerlig i förhållande till andra skyddsvärda intressen. Det innebär att frågan om en känslig personuppgift får behandlas eller inte kan prövas mer flexibelt. Olika slags uppgifter innebär olika stor påverkan på enskilda eller allmänna intressen. På samma sätt kan olika behandlingsåtgärder innebära olika grader av intrång. Detta intrång ska sedan ställas mot en värdering av behovet av behandlingen i det enskilda fallet. Skyddet för känsliga personuppgifter har således delvis förflyttats från kravet på absolut nödvändighet till proportionalitetsprövningen.

Det sätt på vilket känsliga personuppgifter behandlas kan även medföra olika grader av intrång. Det är normalt sett ett större intrång om personal inom Säkerhetspolisen specifikt tar fram och delar känsliga uppgifter än att uppgifterna förekommer i sitt ursprungssammanhang. Med andra ord är det enligt vår uppfattning normalt

ett större intrång om Säkerhetspolisen upprättar en promemoria som sammanställer känslig information, exempelvis om en persons sexualliv, än att uppgifter som i och för sig kan vara avslöjande i detta avseende finns bevarade i ett it-beslag tillsammans med personens övriga kommunikation. Det krävs därmed ett ändamål av tillräcklig styrka för att exempelvis delge privata och särskilt känsliga uppgifter till en annan myndighet eller för att särskilt lyfta fram vissa känsliga uppgifter i en promemoria om en person.

Detta kan uttryckas som att det relevanta enskilda eller allmänna intresset påverkas mindre av att känsliga personuppgifter behandlas som en del av ett större sammanhang. Att det förekommer uppgifter om att en person har skadat sig på något sätt (hälsouppgift) eller besökt sin kyrka (religiös övertygelse) är i sitt sammanhang ofta proportionerliga att behandla. Att en sådan uppgift förkommer i ett dokument som ska behandlas behöver därför inte innebära några särskilda överväganden vid proportionalitetsbedömningen. Det kan dock påverka bedömning om det finns många känsliga uppgifter eller känsliga uppgifter som är särskilt integritetskänsliga. Som framgår av avsnitt 8.2.4 och 8.18.3 kan det innebära att särskilt känsliga uppgifter är proportionerliga att behandla endast under en kortare tid.

8.15.5 Sökning och sammanställning av känsliga personuppgifter

Förslag: Sökning och sammanställning av personer grundat på känsliga personuppgifter ska endast vara tillåtet om skälen för att utföra behandlingen uppenbart överväger intrånget i de enskilda eller allmänna intressen som kan påverkas av den.

Sökning och sammanställning grundat på känsliga personuppgifter kräver ett särskilt skydd

Genom vårt förslag om att Säkerhetspolisen ska få behandla de känsliga personuppgifter som behövs kan det förväntas att fler sådana personuppgifter också kommer att behandlas av Säkerhets-

polisen. Vi anser att det därför måste övervägas om detta förhållande bör balanseras med ytterligare skyddsmekanismer.

Inom Säkerhetspolisen finns hög informationssäkerhet och risken för att det ska spridas känsliga personuppgifter från verksamheten bedöms som mycket låg. Detsamma gäller obehörig tillgång till känsliga personuppgifter bland myndighetens egen personal. Det finns regler och system på plats för att hindra att medarbetare hanterar information som inte är relaterad till en arbetsuppgift. Vi anser att det finns ett tillräckligt skydd mot risken att enskildas rättigheter kränks genom att känsliga personuppgifter på ett otillbörligt sätt sprids inom eller utanför myndigheten.

En risk, som är mer systematisk, är att staten skulle använda känsliga personuppgifter för att sammanställa exempelvis vilka personer som tillhör ett visst trossamfund, är medlemmar i ett politiskt parti eller har en viss sexuell läggning. Förekomsten av sådana sammanställningar skulle utgöra en potentiell risk för diskriminering, eller andra åtgärder främmande för en demokrati. Redan oron bland medborgarna om att känsliga personuppgifter används på ett sådant otillbörligt sätt skulle utgöra ett demokratiskt problem. En sökning som avslöjar och sammanställer känsliga personuppgifter är en åtgärd som i sig innebär en integritetskränkning. Företeelsen ligger nära det som ursprungligen har motiverat förbudet mot behandling av känsliga personuppgifter, nämligen möjligheten att kartlägga personer på grundval av exempelvis etnicitet eller politiska åsikter.[119]

Samtidigt kan just dessa uppgifter i vissa fall vara helt nödvändiga för att skydda den nationella säkerheten eller värna enskildas grundläggande demokratiska fri- och rättigheter. Det står klart att Säkerhetspolisen måste kunna göra sammanställningar av medlemmar i bland annat våldsbejakande icke-demokratiska rörelser just utifrån uppgifter som avslöjar politisk övertygelse, eller få reda på vilka ur ett visst trossamfund som rest till ett annat land för att ansluta sig till en terrororganisation.

Vi anser av dessa skäl att det behövs särskilda regler för att utföra sökningar för att få fram ett urval av personer grundat på känsliga personuppgifter. Syftet är att uppnå ett skydd av just de intressen som bestämmelserna om känsliga personuppgifter ska värna.

[119] Se även prop. 2017/18:105 s. 90.

Hur bör sökning och sammanställning av känsliga personuppgifter regleras?

Den nuvarande säpodatalagen innehåller, i 2 kap. 12 §, ett förbud mot att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter. Förbudet i paragrafens första stycke kompletteras av ett undantag för sökningar i syfte att få fram ett urval av personer grundat på etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller uppgifter som rör hälsa, sexualliv eller sexuell läggning, om sökningen är absolut nödvändig för ett ändamål.

Trots att regeringen insåg att känsliga personuppgifter ofta behövde användas som sökbegrepp i verksamheten ansågs en reglering som bygger på ett generellt förbud med undantag ge en tydligare signal om att känsliga personuppgifter ska användas restriktivt.[120] Det undantag som medger sökningar innebär att det ska konstaterats att det finns ett påtagligt behov av sökningen i det enskilda fallet.[121]

På samma sätt som annan behandling av känsliga personuppgifter anser vi inte att skyddet endast ska utgå utifrån behovet av uppgiften, utan även beakta faktisk eller potentiell risk för intrång i enskilda eller allmänna intressen.

Vi anser att det finns skäl att införa en tydlig reglering för sökning och urval på grundval av känsliga personuppgifter. Eftersom den generella skyddsmekanismen för känsliga personuppgifter utgörs av proportionalitetsprövningen bör det förstärkta skyddet följa samma systematik.

Skälen för att göra ett urval grundat på känsliga personuppgifter bör uppenbart överväga andra skyddsvärda intressen

Det bör vara tillåtet att göra ett urval genom att söka på känsliga personuppgifter när ändamålet för denna behandling på ett tydligt sätt väger över de intressen som kan påverkas av behandlingen. Vilka intressen som riskeras, och hur, beror givetvis på vad urvalet i övrigt bygger på. Att söka på endast en känslig personuppgift, exempelvis sexuell läggning, skulle skapa en lista på alla registrerade personer

[120] Prop. 2018/19:163 s. 79.
[121] Prop. 2009/10:85 s. 266.

som uppfyller sökkriteriet. En sådan lista är givetvis mycket känslig och ändamålet som föranlett urvalet måste väga mycket tungt och vara välmotiverat. I andra fall kan en sökning innehålla en känslig personuppgift tillsammans med andra uppgifter, vilket innebär att urvalet inte endast sker utifrån den känsliga uppgiften. Ett sådant urval kan i många fall innebära en mindre risk för kränkning.

Vi anser att proportionalitetsprövningen som ska göras vid sökningar och urval grundat på känsliga personuppgifter inte bör utgå från att det är tillräckligt med en balans mellan intresset av att utföra sökningen och de enskilda och allmänna intressen som påverkas. Det bör i stället krävas att intresset som talar för behandlingen med marginal väger över vid prövningen. Detta bör uttryckas som ett högre krav än att skälet för att utföra behandlingen ska *överväga* intrånget i de enskilda eller allmänna intressen som kan påverkas av den. Inte heller att skälet *klart överväger* markerar tillräcklig restriktivitet för denna typ av behandling. Att skälet för åtgärden *uppenbart överväger* ger däremot tillräcklig ledning. Begreppet uppenbart innebär att det inte ska råda någon tvekan om att åtgärder inte innebär ett oproportionerligt intrång i grundläggande fri- och rättigheter.

Olika sökningar som innefattar känsliga personuppgifter förekommer i stor utsträckning. För att underlätta prövningen för enskilda medarbetare framstår det som rimligt att myndigheten upprättar interna riktlinjer och styrdokument som kan ge konkret vägledning för vanligt förekommande sökningar.

Det bör inte finnas någon begränsning av vilka uppgifter som får grunda ett urval

Enligt 2 kap. 12 § i säpodatalagen gäller ett generellt förbud mot att söka fram personurval baserat på känsliga personuppgifter. Vissa typer av känsliga personuppgifter omfattas dock av ett undantag i paragrafens tredje stycke, vilket innebär att sökning på dessa uppgifter är tillåten under vissa förutsättningar. Detta undantag gäller dock inte för alla känsliga personuppgifter. Uppgifter om ras, medlemskap i fackförening och biometriska uppgifter får inte användas som sökgrund. Genetiska uppgifter får inte heller användas för sökning, eftersom dessa överhuvudtaget inte får behandlas enligt nuvarande lagstiftning.

Den 1 juli 2025 tillförs paragrafen ett nytt fjärde stycke som medger sökningar i biometriregister som förs med stöd av polisens brottsdatalag, så länge sökningarna är absolut nödvändiga. Biometriska uppgifter får därför användas som sökbegrepp i de särskilda biometriregister över misstänkta, dömda och spår som förs med stöd av den lagen och till vilka Säkerhetspolisen får medges direktåtkomst. Biometriska uppgifter får dock inte användas för att få fram ett urval av personer i Säkerhetspolisens egna register.

När det gäller sökningar som grundas på den känsliga personuppgiften *ras* delar vi förstås den uppfattning som framförts i tidigare förarbeten om att begreppet inte har något vetenskapligt stöd. Det finns därför i och för sig inte någon anledning att särskilt reglera begreppet då det inte ska användas av svenska myndigheter. Den reglering vi föreslår avser emellertid endast i mycket begränsad utsträckning sådana personuppgifter där Säkerhetspolisen haft någon inflytande över utformningen. Om begreppet ras exempelvis förekommer i ett material som utformats i nazistiska eller andra högerextrema kretsar bör det inte finnas något förbud för Säkerhetspolisen att använda detta begrepp för att söka i och analysera materialet. Ett otillbörligt användande av sökbegrepp i andra sammanhang grundat i den ovetenskapliga uppfattningen om förekomsten av olika människoraser, är främmande för svensk förvaltningskultur och kan motverkas på andra sätt.

Skälen för att förbjuda sökningar på *fackföreningsmedlemskap* är att något sådant behov inte kunde förutses då säpodatalagen beslutades. Om det saknas behov, ska en sådan sökning förstås inte utföras. Om det däremot finns ett behov, exempelvis för att förhindra ett terroristbrott riktat mot delar av fackföreningsrörelsen, bör en sökning inte vara förbjuden. Vår uppfattning är att risken med ett förbud överväger riskerna som ett sådant urval kan innebära.

När det gäller *biometriska uppgifter* finns det ett stort och uttalat behov av att kunna använda sådana uppgifter för att göra ett personurval. Om en person ska identifieras är det ett ovärderligt verktyg att kunna bekräfta en unik identifiering av personen genom en teknisk process av en bild, video eller annat biometriskt underlag av personen. Det kan exempelvis handla om att Säkerhetspolisen har behov av att jämföra personer som förekommer på fotografier i en misstänkt terrorists mobilkamera med bilder av kända terrorister vars uppgifter redan behandlas. En sådan jämförelse innebär att bio-

metriska uppgifter tas fram och används som sökkriterier för att få fram ett urval av personer med överensstämmande biometri. Målet är givetvis att endast få fram en enda person och bekräfta en unik identifiering. Även en person utgör dock ett urval så länge det är flera personer som ingått i jämförelsen.

Vi anser att biometriska sökningar ska vara tillåta på samma sätt som för andra känsliga personuppgifter. Det innebär att sökningar får göras både i Säkerhetspolisen egna databaser och i de biometriregister som förs av Polismyndigheten. Sökningar i de särskilt reglerade biometriregistren bör kunna ske på samma sätt som för Polismyndigheten eftersom det i de allra flesta fall torde vara uppenbart att skälen för åtgärden överväger intrånget. Det har i detta fall gjorts en proportionalitetsavvägning på lagstiftningsnivå som innebär att de uppgifter som registrerats i sådana register omfattas av ett särskilt dataskydd.

När det gäller de egna biometriska uppgifter som Säkerhetspolisen kan behandla enligt vårt förslag kommer en noggrann proportionalitetsbedömningen behöva göras. Det innebär att det inte är tillräckligt att Säkerhetspolisen har behov av att utföra en sökning. Ändamålet för åtgärden måste också prövas och tydligt överväga intrånget i de registrerades fri- och rättigheter som sökningen innebär. Både mängden biometriska uppgifter som utgör underlag och hur de samlats in kommer påverka denna bedömning.

8.16 Meddelarfriheten och förtrolig kommunikation mellan misstänkt och försvarare (privilegierad kommunikation)

8.16.1 Behovet av ett förstärkt skydd för annat än känsliga personuppgifter

Bedömning: Det bör övervägas om ett förstärkt skydd ska införas för behandling av andra känsliga uppgifter än sådana som följer av dataskyddskonventionen.

De känsliga personuppgifterna som anges i artikel 6 dataskyddskonventionen har fått sin särställning genom att alla Europarådets medlemsstater kunnat enats om att behandling av dessa uppgifter

generellt bär med sig olika risker. Dessa risker kan uppkomma i alla slags verksamheter där uppgifter behandlas. Som framkommit i det föregående avsnittet finns det dock ofta goda skäl för en nationell säkerhetstjänst att behandla just sådana uppgifter.

Den lagstiftning vi föreslår har fördelen av att all personuppgiftsbehandling måste vara proportionerlig. Det innebär att åtgärder som är integritetskänslig eller i övrigt utgör ett intrång i en grundläggande fri- eller rättighet endast får ske för ändamål som är tillräckligt angelägna. Det är inte avgörande om en personuppgift omfattas av de särskilt uppräknade kategorierna eller om den är känsliga av någon annan anledning. Proportionalitetsprövningen har till syfte att ge en flexibel ram för behandling av uppgifter, där mycket känsliga uppgifter ska kunna behandlas men endast för mycket angelägna ändamål. Om behovet är mer diffust och inte lika angeläget, kan redan behandling av en mindre mängd integritetskänsliga uppgifter vara oproportionerlig.

En av utgångspunkterna för denna utredning har varit att ge Säkerhetspolisen en lagstiftning som är särskilt anpassad för en säkerhetstjänst. Det har motiverat en rad särskilda regleringar som ger Säkerhetspolisen möjlighet att behandla personuppgifter på ett sätt som inte skulle vara lämpliga i andra verksamheter; inte ens vid bekämpande av allvarliga brott. Frågan är mot denna bakgrund om det finns skäl att i denna mer tillåtande lagstiftning införa nya säkerhetsmekanismer i syfte att minska risken för påverkan på enskilda och allmänna intressen.

Det är framför allt två risker som vi särskilt har uppmärksammat: Den första risken rör den förtroliga kommunikation mellan en misstänkt och dennes försvarare och som utgör en viktig beståndsdel i en rättsstat. Den andra risken är att journalistiska källor obefogat ska vara föremål för säkerhetstjänstens intresse. Båda dessa risker aktualiseras när Säkerhetspolisen nu får förutsättningar till en mer effektiv underrättelseverksamhet. Om en säkerhetstjänst får en ökad förmåga i sin underrättelseverksamhet ökar också de potentiella konsekvenserna för den demokratiska rättsstaten vid missbruk av denna förmåga.

8.16.2 Kommunikation mellan den misstänkte och dennes försvarare

Förslag: Säkerhetspolisen ska förbjudas att behandla personuppgifter som utgör förtrolig kommunikation mellan en misstänkt och dennes försvarare.

Frågeförbud och tystnadsplikt för försvarare

I brottmålsprocessen är huvudregeln att det råder fri bevisföring och fri bevisprövning. Den fria bevisföringen är dock omskuren av en rad undantag för att utjämna förhållandena mellan åklagaren och den misstänkte och tillgodose kraven på en rättvis rättegång.

En sådan regel är 36 kap. 5 § rättegångsbalken som avser frågan om vilka skyldighet det finns för vissa offentliga funktionärer och vissa yrkeskategorier att vittna i brottmål. I detta avseende har försvararen en särställning. Av paragrafens tredje stycke framgår nämligen att försvarare får höras som vittnen om vad som anförtrotts dem för uppdragets fullgörande endast om parten medger det. Till skillnad mot andra yrkeskategorier omfattas inte de som har uppdrag som försvarare av något av de undantag som föreskrivs i fjärde stycket (genombrottsregeln).

Den inskränkta vittnesplikten har sin grund i att en misstänkt fritt måste kunna diskutera sin process med sin försvarare, utan risk för att uppgifterna därefter kommer att ligga honom eller henne till last. Detta har ansetts utgöra en viktig rättssäkerhetsmekanism. För advokater gäller, enligt 8 kap. 4 §, även en tystnadsplikt för sådant som han eller hon fått kännedom i sin yrkesutövning.

En försvarares rätt att inte behöva vittna om vad som förevarit i överläggningar har ansetts handla om att säkerställa ett förtroende för den viktig rättsstatlig principen att den som står anklagad för brott ska ha rätt till rättsligt biträde. Denna princip slås fast i artikel 6.3 c i Europakonventionen och det anses innebära ett krav på i princip full sekretess avseende sådan information som en advokat till följd av sitt uppdrag får tillgång till. Om inte den åtalade kan lita på sekretessen, kan han eller hon inte heller sägas ha fått tillgång till

rättsliga biträde.[122] Denna rätt är en central del av rätten till en rättvis rättegång.

Förbud att använda hemliga tvångsmedel i vissa fall

För att upprätthålla principen om att en misstänkt måste kunna ha förtroendefull kommunikation med sin försvarare är emellertid inte frågeförbudet för försvarare i 36 kap. 5 § rättegångsbalken tillräckligt. Ett sådant förbud kan nämligen kringgås genom att myndigheter på andra sätt får reda på vad som sagts under förtroliga överläggningar. Om exempelvis ett samtal mellan en försvarare och dennes klient avlyssnas, kan upptagningen användas som bevis i domstol enligt principen om fri bevisföring och fri bevisprövning. För att förhindra ett sådant kringgående har det ansetts nödvändigt att begränsningarna i vittnesplikten ska motsvaras av begränsningar i möjligheten att få fram motsvarande uppgifter genom tvångsmedelsanvändning.[123]

Det finns därför en rad särskilda regler som omgärdar bland annat denna kommunikation. I 27 kap. 2 § och 38 kap. 2 § rättegångsbalken finns bestämmelser som hindrar beslag och edition av handlingar som kan innehålla sådana uppgifter som försvararen inte kan tvingas vittna om. Enligt 27 kap. 22 § får hemlig avlyssning av elektronisk kommunikation inte avse telefonsamtal eller andra meddelanden som utgör sådan privilegierad kommunikation som avses i 36 kap. 5 §. Vidare framgår att hemlig rumsavlyssning ska upphöra så snart det framgår att en försvarare talar. Uppteckningar och upptagningar från hemliga tvångsmedel ska förstöras i de delar som avser sådan kommunikation. Liknande bestämmelser gäller enligt 27 § lagen (2020:62) om hemlig dataavläsning.

Personuppgifter som utgör kommunikation mellan en misstänkt och dennes försvarare ska inte få behandlas

Kommunikation mellan en misstänkt och dennes försvarare i de förundersökningar som Säkerhetspolisen själv bedriver kan endast i undantagsfall komma till Säkerhetspolisens kännedom. Däremot

[122] Se justitierådet Lindskog i NJA 2010 s. 122.
[123] Se prop. 1988/89:124 s. 46.

kan sådan kommunikation, i avslutade eller pågående processer, som rör annan brottslighet komma att omfattas av myndighetens underrättelseinhämtning. Det har exempelvis blivit allt vanligare att främmande makt använder lokala agenter som rekryteras bland livsstilskriminella. Om Säkerhetspolisen bedriver underrättelseverksamhet mot sådan brottslig verksamhet, kan det inte uteslutas att det bland andra personuppgifter som behandlas i vissa fall kan finnas förtrolig kommunikation mellan försvarare och misstänkt avseende helt annan brottslighet.

Det finns ett starkt skydd för den privilegierade kommunikationen mellan en försvarare och dennes klient; genom tystnadsplikt och undantag från vittnesplikt samt de särskilda reglerna för de hemliga tvångsmedlen. Det finns dock alltid en risk att uppgifter kan komma att behandlas utan att omfattas av några sådana skyddsregler. Eftersom uppgifter i sådan kommunikation sannolikt är av intresse för Säkerhetspolisens kartläggning av den brottsliga verksamheten finns också skäl att anta att det skulle finnas ett behov av att fortsätta att behandla uppgifterna. Proportionalitetsprövningen i den föreslagna lagen ger ett visst skydd mot fortsatt behandling av sådana uppgifter eftersom intrånget får betecknas som stort.

Det går dock att ifrågasätta om det överhuvudtaget bör finnas något ändamål som kan motivera att en så viktig rättsstatlig princip åsidosätts som skyddet av förtrolig kommunikation mellan klient och försvarare. Om det visar sig att Säkerhetspolisen haft tillgång till sådan privilegierad kommunikation, skulle spridningseffekterna kunna bli påtagliga och orsaka betydande misstro mot rättsstaten.

Intrånget av att personuppgifter som utgör förtrolig kommunikation mellan en misstänkt och dennes försvarare behandlas är generellt för stort för att kunna accepteras ens i förhållande till nationella säkerhetsintressen. Vi anser därför att säpodatalagen bör innehålla ett generellt förbud mot att behandla personuppgifter som avser det som en misstänkt, tilltalad eller dömd person anförtrott en försvarare inom ramen för dennes uppdrag. Säkerhetspolisen behöver inte aktivt eftersöka sådana uppgifter. Förbudet innebär att de ska tas bort när det framgått att myndigheten behandlar sådana uppgifter, se avsnitt 8.20.2.

Förbudet bör avse alla uppgifter som anförtrotts en försvarare i anledning av försvararuppdraget och inte endast de uppgifter som krävs för uppdragets fullgörande. Det innebär att även exempelvis

uppgifter som rör nedlagda misstankar omfattas. En direkt hänvisning till frågeförbudet i 36 kap. 5 § tredje stycket rättegångsbalken skulle kunna leda till vissa tillämpningssvårigheter. Behandlingsförbudet bör därför formuleras självständigt.

8.16.3 Meddelarfriheten

Förslag: Säkerhetspolisen ska förbjudas att behandla personuppgifter som innebär att en grundlagsskyddad meddelares anonymitet riskeras.

Meddelarskyddet i grundlag

Enligt 1 kap. 7 § tryckfrihetsförordningen och 1 kap. 10 § yttrandefrihetsgrundlagen står det var och en fritt att meddela uppgifter i vilket ämne som helst i syfte att de ska offentliggöras i ett sådan medium som skyddas av de båda grundlagarna.

Den svenska yttrandefriheten bygger bland annat på det så kallade ensamansvaret, vilket innebär att endast den ansvarige utgivaren står till svars för publiceringar. Andra, som på ett eller annat sätt bidrar till innehållet och dess offentliggörande, bär enligt huvudregeln inget rättsligt ansvar för sin medverkan. Det innebär att meddelarfrihet råder.

Meddelarfriheten är en självständig del av de båda grundlagarna och syftar till att uppmuntras människor att utnyttja sin yttrandefrihet. Detta sker i första hand genom att grundlagarna garanterar att var och en kan tillhandahålla uppgifter till exempelvis en nyhetsredaktion utan rädsla för straff eller andra repressalier från det allmänna. Ett tillhandahållande enligt lagen kan ske på många sätt bland annat genom att meddelaren lämnar information muntligen, överlämnar en skrivelse eller skickar in en handling elektroniskt. För att omfattas av meddelarfriheten ska syftet vara att uppgiften ska offentliggöras. Det finns dock inget krav på att meddelarens syfte ska uppnås. En redaktions val att inte publicera en uppgift innebär därmed inte att skyddet gått förlorat för meddelaren.

Ett meddelande som omfattas av yttrandefrihetsgrundlagen och tryckfrihetsförordningen kan enligt 1 kap. 14 § respektive 1 kap.

9 § inte föranleda straffansvar eller ersättningsskyldighet, om det inte särskilt anges i någon av dessa grundlagar. Detta brukar benämnas som exklusivitetsprincipen. Det råder vidare ett så kallat repressalieförbud där en myndighet eller annat allmänt organ förhindras att på annat sätt ingripa mot någon för att ha medverkat till en publicering. Repressalieförbudet ger skydd mot andra åtgärder som en myndighet vidtar i anledning av att någon utnyttjat sin meddelarfrihet, exempelvis ett arbetsledningsbeslut.

Meddelarfriheten är inte oinskränkt. De båda grundlagarna innehåller bestämmelser om så kallade meddelarbrott enligt 7 kap. 22 § tryckfrihetsförordningen och 5 kap. 4 § yttrandefrihetsgrundlagen. Det innebär att straffrihet inte råder för uppgifter som innebär att meddelaren gör sig skyldig till brott mot rikets säkerhet: Bland dem högförräderi, spionerі, utlandsspionerі och grov obehörig befattning med hemlig uppgift. Det är främst det sistnämnda brottet som utgör en praktiskt beaktansvärd begränsning av meddelarfriheten. De övriga brott som omnämns i de båda grundlagarna är svåra att leda i bevis med hänsyn till efterforskningsförbud och anonymitetsskydd (se nedan) samt kräver ett avsiktsuppsåt att gå främmande makt tillhanda.[124]

Vidare straffas även vissa brott mot tystnadsplikten som gäller uppgifter som omfattas av meddelarens tystnadsplikt, handlingar som lämnas i strid med en sekretessbestämmelse eller uppgifter som lämnas på annat sätt och som är kvalificerat hemliga.

Anonymitetsskydd genom tystnadsplikt och efterforskningsförbud

Enligt 3 kap. 1 § tryckfrihetsförordningen och 2 kap. 1 § yttrandefrihetsgrundlagen ger upphovsmän och meddelare rätt till anonymitet. Rätten till anonymitet konkretiseras i de för yttrandefriheten mycket centrala bestämmelserna om tystnadsplikt och efterforskningsförbud.

Tystnadsplikten följer av 3 kap. 3 § tryckfrihetsförordningen respektive 2 kap. 3 § yttrandefrihetsgrundlagen. Enligt dessa bestämmelser får den som tagit befattning med tillkomsten av en utgivning inte röja vad denne vet om vem som är upphovsperson eller

[124] Se Axberger m.fl., *Yttrandefrihetsgrundlagarna*, 2023, JUNO, avsnitt 7.2.2.

vem som är meddelare. Det innebär att inget som kan bidra till att göra bland annat ett meddelares identitet känd får röjas. Tystnadsplikten innefattar i princip allt som kan betecknas som personuppgifter, eftersom sådana uppgifter är de som ensamt eller tillsammans med annan information kan kopplas till en fysisk person (grundlagsskyddet gäller dock, till skillnad mot definitionen av en personuppgift, även personer som inte är i livet.) Den tystnadsplikt som gäller för publicister och andra som tagit befattning med sådana uppgifter är kvalificerad, och omfattas därmed inte i sig av meddelarfrihet.[125]

Tystnadsplikten för de som har information om en meddelares identitet kompletteras av efterforskningsförbudet. Efterforskningsförbudet regleras i 3 kap. 5 § tryckfrihetsförordningen respektive 2 kap. 5 § yttrandefrihetsgrundlagen. Innebörden är att en myndighet eller annat allmänt organ inte får efterforska en anonym upphovsman eller meddelare. Efterforskningsförbudet är centralt för att upprätthålla anonymitetsskyddet för de som väljer att lämna uppgifter till en publicist och förhindrar exempelvis utredningsåtgärder som går ut på att spåra läckor inom en myndighets organisation. I likhet med meddelarfriheten gäller inte heller anonymitetsskyddet för dem som meddelar uppgifter som utgör så kallade meddelarbrott, bland annat brott mot rikets säkerhet och åsidosättande av tystnadsplikten i vissa fall.

Reglerna om efterforskningsförbudet kompletteras av motsvarande regler avseende vittnesplikten som redogjorts för i det föregående avsnittet avseende försvarare. Enligt 36 kap. 5 § rättegångsbalken sjätte stycket får den som har tystnadsplikt enligt tryckfrihetsförordningen eller yttrandefrihetsgrundlagen inte höras som vittne om förhållanden där tystnadsplikt gäller.

De brottsbekämpande myndigheterna kan trots efterforskningsförbudet komma över information som omfattas av tystnadsplikt. Det kan exempelvis handla om att det vid ett beslag eller under avlyssning framkommer att en person som är misstänkt för brott även är en meddelare. Det finns därför kompletterande regler för olika straffprocessuella tvångsmedel. Förbud mot beslag av skriftlig handling, hemlig avlyssning av elektronisk kommunikation, hemlig rumsavlyssning och hemlig dataavläsning gäller även till förmån för meddelares anonymitet.

[125] Se 44 kap. 1 § 2–3 offentlighets- och sekretesslagen.

Personuppgifter som omfattas av grundlagsskyddad tystnadsplikt och efterforskningsförbud ska inte få behandlas

Anonymitet för meddelare utgör en mycket viktig beståndsdel i den demokratiska rättsstaten. Meddelarfriheten har ansetts central för det journalistiska uppdraget att granska stat och makthavare.

Säkerhetspolisens uppdrag och verksamhet avser bland annat att förebygga, förhindra och upptäcka brott mot rikets säkerhet och att utöva tillsyn över säkerhetsskyddslagens bestämmelser. Myndighetens uppdrag har på så sätt en naturlig koppling till meddelarfriheten. De så kallade meddelarbrotten utgörs i stor utsträckning av sådana brott som Säkerhetspolisen ansvarar för eller röjande av säkerhetsskyddsklassificerade uppgifter. Vid utredning av ett brott som rör nationell säkerhet eller i underrättelseverksamhet som bedrivs mot sådan brottslig verksamhet finns en möjlighet att Säkerhetspolisen kommer över uppgifter som omfattas grundlagsskydd. Om det rör sig om uppgifter som inhämtats med stöd av särskilda befogenheter finns regler som innebär att sådana uppgifter ska förstöras om de upptäcks.

Det kan dock, särskilt inom underrättelseverksamheten, förekomma situationer som innebär att Säkerhetspolisen kan komma att behandla grundlagsskyddade personuppgifter om en anonym meddelares eller upphovsmans identitet utan att behandlingen omfattas av något särskilt regelverk. Det kan exempelvis röra sig om uppgifter som Säkerhetspolisen fått från en samverkande tjänst eller som informations som inhämtats utan stöd av särskilda befogenheter. Säkerhetspolisen har tillgång till flera möjliga källor för information och en hög förmåga att lägga samman och koppla ihop olika delar för att kartlägga och klarlägga fenomen eller företeelser. Uppgifter som har ett grundlagsskydd kan beroende på sin natur vara av intresse för underrättelseverksamheten.

Vi anser att intresset av att värna det journalistiska källskyddet väger mycket tungt. Europadomstolen har även uttalat att skyddet för journalistiska källor utgör en väsentlig del av yttrandefriheten enligt artikel 10 i Europakonventionen. Domstolen har beskrivit skyddet av journalistiska källor som en av hörnstenarna i pressfriheten. Utan ett sådant skydd kan källor avstå att uppmärksamma pressen, och i förlängningen allmänheten, om frågor som är av stort allmänt intresse. Det journalistiska uppdraget att vara ”allmänhetens

vakthund” kan då komma att undergrävas. En sådan utveckling skulle sänka medias förmåga att tillhandahålla korrekt och tillförlitlig information. Europadomstolen har därför ansett att ett ingrepp endast kan vara förenligt med artikel 10 i konventionen, om det är motiverat av tvingande hänsyn till allmänintresset.[126]

Vi anser att det finns starkt vägande skäl för att dessa uppgifter ska behandlas med stor varsamhet oavsett hur de kommit Säkerhetspolisen tillhanda. Det finns, enligt vår bedömning, inte något tillräckligt tungt vägande skäl för att alls tillåta behandling av sådana uppgifter i den brottsbekämpande verksamheten. Skyddet för meddelare är inte oinskränkt och det har från lagstiftarens sida gjorts en avvägning av i vilka fall skyddet ska ge vika. Det finns enligt vår bedömning därför inte något skäl att tillåta behandling av grundlagsskyddade uppgifter vid sidan av de situationer som anges i yttrandefrihetsgrundlagen respektive tryckfrihetsförordningen.

Genom ett absolut behandlingsförbud kommer de ökade möjligheter för Säkerhetspolisen att behandla personuppgifter som vi föreslår inte medföra någon försvagning av meddelarfriheten. På så sätt värnas även yttrandefriheten i stort.

Behandlingsförbudet bör hänvisa direkt till tryckfrihetsförordningens och yttrandefrihetsgrundlagens bestämmelser. Behandlingen ska upphöra om det framgår att uppgifterna tillhör denna kategori. Det innebär inte att Säkerhetspolisen aktivt behöver försöka identifiera sådana uppgifter men de ska tas bort genast när det framgår att sådana uppgifter behandlas.

8.16.4 Det saknas tillräckliga skäl att ge förstärkt skydd för andra uppgifter som är undantagna vittnesplikt

Bedömning: Det finns inte tillräckligt skäl att föreskriva särskilda skyddsmekanismer för andra privilegierade uppgifter.

Vid sidan av den typen av kommunikation som vi redogjort för ovan finns andra uppgifter som har ett förstärkt skydd i lag. Av 36 kap. 5 § rättegångsbalken framgår att undantaget från vittnes-

[126] Europadomstolens dom den 25 februari 2003, *Roemen and Schmit mot Luxembourg*, mål nr 51772/99 och den 22 november 2012, *Telegraaf Media Nederland Landelijke Media B.V. m.fl. mot Nederländerna*, mål nr 39315/06.

plikten under vissa förutsättningar även gäller bland annat viss personal inom hälso- och sjukvården och andra juridiska biträden än försvarare. Vid sidan av försvarare och den som har kännedom om en meddelares identitet gäller det absoluta undantaget endast den som är präst inom ett trossamfund eller har motsvarande ställning. För en sådan person gäller undantaget från vittnesplikt det han eller hon har erfarit under bikt eller enskild själavård.

Även för dessa kategorier råder begränsningar med avseende på hemlig tvångsmedelsanvändning. Som regel får dock kopplingen mellan dessa yrkeskategoriers verksamhet och bekämpandet av brott som rör nationell säkerhet anses vara svag. De särskilda regler som gäller yrkeskategorierna i 36 kap. 5 § andra stycket rättegångsbalken avser att skydda förtroendet mellan dessa yrkesutövare och enskilda samt att värna den enskildes personliga integriteten. [127] Det rör sig, enligt vår mening, dock inte om några integritets- eller demokratirisker som behöver omhändertas vid sidan av de regler i rättegångsbalken som redan omfattar dessa uppgifter.

När det kommer till uppgifter som lämnats under bikt eller annan enskild själavård har regeringen i tidigare lagstiftningsärende övervägt behovet av ett förstärkt skydd.[128] De personuppgifter som utgör bikt eller enskild själavård omfattas i stor utsträckning av förstöringsskyldighet på grund av särskilda regler för respektive inhämtningsmetod.[129] Skyddet för sådana uppgifter är redan mycket starkt och det är svårt att se behovet av att ytterliga förstärka skyddet. Avvägningen sker inte heller mot brottslighet i allmänhet och intresset av att skydda integriteten i själavård och bikt. Avvägningen sker mot behovet av att skydda nationell säkerhet. Till det kommer den betydande svårigheten att avgöra vad som utgör bikt eller själavård i det enskilda fallet.

[127] Se prop. 2013/14:237 s. 131 ff.
[128] Prop. 2008/09:201 s. 81.
[129] Se dock 7 § 4 signalspaningslagen.

8.17 Längsta tid för behandling av personuppgifter

8.17.1 Dataskyddskonventionens bestämmelser om behandlingstid

Dataskyddskonventionen uppställer inga tidsfrister eller detaljerade regler angående behandlingstid.

> **Article 5 – Legitimacy of data processing and quality of data**
>
> 4. Personal data undergoing processing shall be
>
> e. preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed.

Kravet i artikel 5.4 e om tidsfrister för lagring av personuppgifter innebär att uppgifter bör raderas när det ändamål för vilket de behandlades har uppnåtts, eller att de då endast bevaras i en form som förhindrar direkt eller indirekt identifiering av den registrerade.

Det är upp till medlemsstaterna att vidta nödvändiga lagstiftningsåtgärder för att genomföra bestämmelserna i dataskyddskonventionen vilket ger en frihet i att reglera behandlingstid i nationell rätt. I likhet med många andra artiklar i konventionen är det möjligt att göra undantag från bestämmelsen om att behandlingen inte ska pågå längre än nödvändigt, om det krävs för att skydda nationell säkerhet.

8.17.2 Behandlingstider inom underrättelseverksamhet

Säpodatalagens bestämmelser

I avsnitt 3.5.7 redogör vi för säpodatalagens bestämmelser om behandlingstid. Inom underrättelseverksamhet gäller som huvudregel att personuppgifter inte får behandlas längre än tio år efter utgången av det kalenderår då den senaste registreringen gjordes avseende personen. För personuppgifter som behandlas inom kontraspionaget gäller dock att sådana uppgifter inte får behandlas längre än 40 år efter det kalenderår då den senaste registreringen gjordes avseende personens anknytning till brott eller brottslig verksamhet.

I avsnitt 6.1.5 redogör vi för Säkerhetspolisens behov av att kunna behandla personuppgifter längre än vad som följer av dagens regelverk.

Hur är andra säkerhets- och underrättelsetjänster reglerade?

I avsnitt 3.6.2 redogör vi översiktligt för Försvarsmaktens och FRA:s lagstiftning. För militära underrättelse- och säkerhetstjänsten och FRA gäller ingen längsta behandlingstid fastställd i lag. Där tillämpas i stället principen om att personuppgifter inte får behandlas längre än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Regeringen konstaterade i förarbetena att förståelse för ett skeende eller en aktörs agerande ofta kräver att det som observeras kan sättas in i ett kontextuellt och historiskt sammanhang. Först därefter kan bedömningar om underrättelserelevans göras. För vissa företeelser ansåg regeringen att det kan vara nödvändigt att kunna göra jämförelser med observationer som har gjorts långt tillbaka i tiden, inte sällan 10–20 år.[130]

Även vid en internationell jämförelse framstår den svenska behandlingstiden som relativt kort i förhållande till Säkerhetspolisens uppdrag. I Norge, Nederländerna och Förenade kungariket får underrättelsetjänsterna som huvudregel behandla personuppgifter så länge de är nödvändiga för ändamålet. I Finland tillämpar Skypo en generell behandlingstid om 25 år efter den sista registreringen om en person, med möjlighet till förlängning. Danska PET har en motsvarande bestämmelse om behandlingstid som dock högst får vara 15 år. I Danmark kompletteras dock lagens bestämmelse av en mer detaljerade reglering i förordning, om bestämmande av lagringstid i samband med registrering (se kapitel 4).

8.17.3 Problem med nuvarande reglering av behandlingstid

Bedömning: Tiden för personuppgiftsbehandling är en faktor som dag för dag ökar graden av intrång i den registrerades rättigheter. Det finns två huvudsakliga problem med dagens reglering:

1. Det finns en risk att personer som en gång registrerats fortsätter att behandlas under oproportionerligt lång tid, särskilt genom rutinmässig förlängning vid nya registreringar.

[130] SOU 2018:63 s. 163 och prop. 2020/21:224 s. 71.

2. Kravet på att varje personuppgift i gemensamt material ska bedömas separat skapar praktiska svårigheter som gör regleringen svårtillämpad.

En proportionerlig behandling blir med tiden oproportionerlig

Kartläggning av enskilda personers personliga förhållanden utgör ett intrång i skyddet för den personliga integriteten. På samma sätt kan en övervakning av åsiktsyttringar, deltagande på olika politiska manifestationer eller uttryck för religiös övertygelse utgöra ett intrång i grundläggande opinionsfriheter. Sådan kartläggning sker i alla demokratiska stater och är förenlig med de mänskliga rättigheterna så länge det är motiverat utifrån ett trängande allmänintresse. Däremot utgör tiden som en person finns i ett underrättelseregister en faktor som dag för dag ökar graden av intrång i den registrerades rättigheter. I många fall sammanfaller även det tilltagande intrånget med att de förhållanden som ursprungligen motiverade registreringen minskar i betydelse.

Tiden som en person finns registrerad kan därför ensamt utgöra en faktor som innebär att intrånget inte längre är motiverat och därför utgör en kränkning. Europadomstolen har vid upprepade tillfällen påtalat att personuppgifter, om än de var relevanta att samla in, inte får bevaras längre än vad som är nödvändigt för ändamålet.

I ett av domstolens vägledande avgöranden, *Segerstedt-Wiberg m.fl. mot Sverige*,[131] prövades Säkerhetspolisens behandling av personuppgifter om fem personer. Av dem ansågs Sverige ha kränkt fyras rätt till privatliv genom den tid som de varit registrerade hos Säkerhetspolisen. Behandlingen hade i de fallen skett med stöd av polisdatalagen. De personuppgifter som domstolen hade att bedöma var bland annat att en av klagandena, som var en välkänd journalist på Göteborgsposten, år 1967 ”antagligen” hade deltagit i en konferens i Warszawa.[132] För en av de andra klagandena prövades registreringar avseende bland annat en mängd tidningsartiklar från 1970-talet och framåt, huvudsakligen avseende dennes aktiviteter i idrotts-

[131] Europadomstolens dom den 6 juni 2006, i mål 62332/00.
[132] Se punkt 15 och 19.

föreningen Proletären FF som har kopplingar till kommunistpartiet KPML(r) samt uppgifter om hans medlemskap i partiet.[133]

Domstolen ansåg att dessa registreringar i och för sig var acceptabla under ändamålet att skydda nationell säkerhet, där staten har en bred bedömningsmarginal.[134] Att i över trettio år behandla uppgiften om att en person antagligen varit på ett politiskt möte i Warszawa var dock inte proportionerligt i förhållande till detta ändamål. Det ansågs inte heller nödvändigt att bevara uppgifter om idrottsledaren i Proletären FF under så lång tid, då hotet mot nationell säkerhet från KPML(r) numera varken kunde anses vara faktiskt eller ens potentiellt.[135]

Den personuppgiftsbehandling som prövades av domstolen, rörde uppgifter som lämnats ut till de klagande strax efter att den absoluta sekretessen för uppgifter hos Säkerhetspolisen upphävts år 1999. I huvudsak avsåg registreringarna öppet tillgänglig information som tillförts respektive personakt. Uppgifterna kan sedda var för sig inte anses ha varit av särskilt känslig natur och domstolen ansåg att det varit acceptabelt att ursprungligen samla in uppgifter om klagandena utifrån de misstankar som då funnits. Trots detta utföll avvägningen mellan klagandenas rätt till privatliv och statens intresse av att skydda nationell säkerhet till klagandenas fördel, på grund av en allt för lång behandlingstid.

En automatisk förlängning av behandlingstid vid nya registreringar innebär en risk för kränkning

Skälet till att de klagandes uppgifter i målet *Segerstedt-Wiberg m.fl. mot Sverige* behandlats under så lång tid var inte avsaknad av en behandlingsfrist i den dåvarande polisdatalagen. Även enligt den lagen skulle personuppgifter som huvudregel raderas senast tio år efter den senaste registreringen, om det inte fanns särskilda skäl.

Avseende de klagande i målet framstår det dock som att nya uppgifter registrerats kontinuerligt. För idrottsledaren i Proletären FF fanns exempelvis en registrering från 1990-talet som avsåg en namninsamling som han skrivit under för sänkta avgifter för idrottsanläggningar. Som det får förstås tillfördes denna uppgift mer eller

[133] Se punkt 30.
[134] Se punkt 87–88.
[135] Se punkt 90–91.

mindre rutinmässigt hans personakt, som ursprungligen öppnats genom en PM från 1973 som avsåg hans aktiva medlemskap i KPML(r). Trots att de ursprungliga misstankar om brottslig verksamhet inom KPML(r) får antas ha förlorat i betydelse under åren då de senaste registreringarna gjordes kvarstod de som grund för behandling. De nya registreringarna förlängde i sin tur behandlingstiden för de ursprungliga uppgifterna.

För journalisten vid Göteborgsposten saknades, såvitt framgår i målet, en personakt då han inte var föremål för någon egentlig brottsmisstanke då saken prövades i Europadomstolen. Hans personuppgifter återfanns i stället i en rapport från år 1967 angående en världskonferens i Warszawa. Rapporten fanns alltjämt registrerad hos Säkerhetspolisen, antagligen i syfte att kartlägga vilka personer som kan ha rekryterats som spion för främmande makt under kalla kriget. En datoriserad sökning på journalistens personuppgifter i Säkerhetspolisens dåvarande system gav inte någon träff.[136] Trots detta ansågs registreringen av hans personuppgifter i rapporten kränka hans rätt till privatliv.

Slutsatser om hur behandlingstid bör regleras

Rättsfallet *Segerstedt-Wiberg m.fl. mot Sverige* belyser två problem vid personuppgiftsbehandling inom underrättelseverksamhet. För det första finns det en risk att uppgifter om personer som en gång fångat säkerhetstjänstens uppmärksamhet kommer att fortsätta att behandlas under mycket lång tid. Det finns inom underrättelseverksamhet, till skillnad mot brottsutredning, inte något egentligt skäl för myndigheten att avfärda misstankar genom att avskriva ett ärende eller liknande. Ett överskott av information är sällan till nackdel för uppdraget att upptäcka brottslig verksamhet och olika lagtekniska lösningar som förlänger behandlingstid har därför en tendens att möjliggöra att existerande personakter växer och fortsätter att behandlas.

Det andra problemet är att personuppgifter som förekommer i ett material, låt vara att de endast rör sig om namn som nämns i ett avlyssnat samtal eller en personuppgift som ingår i ett dokument som är relevant att spara i sin helhet, alltjämt utgör en personuppgifts-

[136] Punkt 18–21.

behandling. Om varje enskild personuppgift i ett källmaterial ska bedömas för sig och endast behandlas så länge det är nödvändigt kommer den ursprungliga källan inte kunna behandlas längre än vad som är proportionerligt för den minst centrala uppgiften i den. För fortsatt behandling måste källmaterialet i annat fall genomgå en omfattande bearbetning där centrala partier isoleras från de mer perifera för att bedöma hur länge enskilda personuppgifter får behandlas. För en PM från en konferens i Warszawa är det kanske möjligt att göra en sådan separation. För mer ostrukturerade informationsmängder ställer det dock mycket höga krav på efterbehandling för att åstadkomma en funktionell isolering av olika personuppgifter. Det kan vara mycket svårt att separera bedömningar av personuppgifter som endast registreras för att de förekommer i ett sammanhang från de uppgifter som är skälet till att sammanhanget överhuvudtaget är relevant behandla.

Vi prövar frågan om hur behandlingstid bör regleras i den nya lagstiftningen med utgångspunkt i denna problemformulering.

8.17.4 Hur bör längsta behandlingstid bestämmas?

Bedömning: Om personuppgifter får behandlas så länge de behövs måste behovet omprövas med viss regelbundenhet för att undvika att den personliga integriteten kränks.

Det behövs ett alternativ till en reglering som förutsätter kontinuerlig omprövning av varje personuppgift.

Behovsstyrd behandlingstid

Vi delar tanken bakom den nuvarande lagstiftningens grundläggande princip om att personuppgifter inte ska få lagras längre än vad som behövs för det eller de ändamål de behandlas. Att denna princip ska tillämpas följer också av både av dataskyddskonventionen och av Europadomstolens praxis. För att en sådan reglering ska fylla någon integritetshöjande funktion krävs dock att det verkligen sker en kontinuerlig behovsprövning och att personuppgifter där behovet av fortsatt behandling inte är proportionerligt faktiskt raderas.

Särskilt inom underrättelseverksamhet är det ofta lätt att hitta argument för fortsatt behandling. Det finns därför goda skäl för att komplettera behovsprincipen för behandlingstid med bestämmelser om längsta tid för behandling.

Sådana regler får anses bygga på en presumtion för att behovet efter en viss tid inte längre motiverar intrånget som fortsatt registrering innebär.[137] Att tvinga fram en bedömning av behovet inom viss tid är ett effektivt sätt att förhindra orimligt långa behandlingstider.

Problemet är att en sådan tidsgräns som är avsedd att utgöra ett tak ofta blir ett golv. I avsnitt 3.5.7 redogör vi för Säkerhets- och integritetsskyddsnämndens uttalande om att det knappast kan anses förenligt med behovsprincipen att som huvudregel behandla alla personuppgifter under lagens längsta tid. Under behandlingstiden måste behovet av uppgifterna kontinuerligt omprövas.

Behovsstyrd behandlingstid, utan en lagstadgad yttersta tidsgräns, finns i Försvarsmaktens och FRA:s respektive personuppgiftslagar och i flera andra rättssystem som vi studerat, bland dem Norge och Förenade kungariket. Trots att lagen anger att personuppgifter får behandlas så länge som det behövs kompletteras den på olika sätt med mekanismer för regelbunden omprövning. Inom Försvarsmakten har vi fått uppgift om att det årligen sker en genomgång av uppgifter i underrättelsesystemen (”administrativa veckan”) för att vidta registervårdande insatser, bland annat genom att uppgifter som inte längre behövs ska raderas. I Norge finns i förordningen till polisregisterlagen en bestämmelse om att personuppgifter i underrättelseverksamheten ska granskas senast fem år efter den senaste registreringen och att fortsatt lagring ska motiveras därefter.

Denna metod, att föreskriva lämpliga tidsgränser för periodisk översyn av behovet av fortsatt behandling, följer av brottsdatadirektivet. Enligt artikel 5 i direktivet är periodisk översyn ett alternativ till tidsgränser för radering. I Förenade kungariket, som bygger sin lagstiftning för säkerhetstjänsten på dataskyddskonventionen 108, har tillsynsmyndigheten förklarat att det krävs interna riktlinjer som på ett objektivt sätt rättfärdigar en viss behandlingstid, trots att det inte finns någon yttre gräns i lagstiftningen (se om refererade utländska rättssystem i kapitel 4).

[137] Jfr prop. 2009/10:85 s. 210.

Lagtekniska utmaningar med behovsstyrd behandlingstid

Vi har konstaterat att Säkerhetspolisen generellt behöver behandla personuppgifter under längre tid än många andra myndigheter.

Säkerhetspolisen har förordat en längre generell behandlingstid som inte riskerar att uppgifter som senare kan visa sig nödvändiga raderas i förtid. Som framgått är även Sveriges tioårsgräns relativt kort vid en internationell jämförelse. Det finns många exempel på att det på förhand går att sluta sig till att uppgifter som registreras kommer behöva behandlas under längre tid än tio år. Att generellt utöka behandlingstiden, från tio till exempelvis 25 år, kan dock medföra att uppgifter om personer som inte längre har ett tillräckligt högt informationsvärde för Säkerhetspolisen ändå bevaras. Motsvarande behandlingstid ansågs i målet *Segerstedt-Wiberg m.fl. mot Sverige* vara oproportionerligt lång med hänsyn till att behovet av uppgifterna successivt avtagit i takt med att omvärlden förändrats.

En sådan generell höjning av behandlingstiden för alla uppgifter skulle därför behöva kompletteras med regler om kontinuerlig behovsprövning för att säkerställa att lagstiftningen lever upp till Sveriges internationella åtaganden. Ur integritetssynpunkt är regelbunden prövning av behovet av varje persons uppgifter att föredra.

Att reglera om periodvisa granskningar inom en längre tillåten behandlingstid innebär dock att stora resurser skulle behöva omfördelas från operativ verksamhet till registervård. För att en periodvis granskning ska fylla någon integritetshöjande funktion krävs nämligen mer än att uppgifterna granskas ytligt. Balansen mellan Säkerhetspolisens behov av en uppgift och den enskildes intressen av att inte vara registrerad är inte alltid lätt att utföra.

Att kontinuerligt och manuellt granska samtliga personuppgifter som Säkerhetspolisen behandlar är mycket resurskrävande och förutsätter en fördelning mellan operativ respektive registervårdande verksamhet som framstår som orimlig. För att förhindra att personuppgifter behandlas oproportionerligt länge samtidigt som myndighetens effektivitet, och i slutändan operativa förmåga, inte påverkas i allt för hög grad behövs ett alternativ till kontinuerlig och manuell behovsprövning.

Olika alternativ till kontinuerlig prövning

Kan vissa behandlingsåtgärder förlänga behandlingstiden?

Ett alternativ är att grunda den längsta behandlingstiden på vilka behandlingsåtgärder som vidtas om en person. Den nuvarande regleringen bygger på att nya uppgifter som registreras om en person förlänger behandlingstider för dennes samtliga personuppgifter. Som tidigare nämnts bär detta system på problemet att det sker en mer eller mindre automatisk förlängning av behandlingstiden för alla uppgifter. Detta trots att de uppgifter som tillförs kanske inte är av sådan tyngd att det framstår som motiverat att förlänga den ursprungliga registreringen med ett helt decennium. Det skulle vara möjligt att bygga ett system för förlängning på andra behandlingsåtgärder än registrering. Exempelvis skulle olika slags sökningar eller sammanställning kunna förlänga tidsfristen ett antal år för en person som ingår i en sådan sammanställning. Fördelen skulle vara att personuppgifter som inte aktivt används i den operativa verksamheten, vilket talar för att uppgiften inte längre uppfyller behovskriteriet, på så sätt gallras ur systemet efter hand samtidigt som uppgifter om mer centrala aktörer bevaras.

Ett problem är att Säkerhetspolisens fokusområden har en tendens att skifta över tid. Om stora resurser under en period har lagts på att kartlägga islamistisk terrorism kommer uppgifter inom detta område att förlängas. På grund av att myndigheten har begränsade resurser sker emellertid detta på bekostnad av andra verksamhetsgrenar trots att uppgifter där också kan vara väsentliga att kunna behandla över tid. Det finns även tekniska problem med att skapa ett effektivt och rättssäkert system runt olika behandlingsåtgärder. På något sätt måste endast vissa mer kvalificerade behandlingar påverka behandlingstiden. Detta för att undvika att allt för många personers uppgifter förlängs genom exempelvis kontinuerliga förekomstssökningar eller uppdateringar av uppgifter. Vi anser mot denna bakgrund att detta inte är en framkomlig väg.

Kan misstanke utgöra grund för behandlingstid?

Ett annat alternativ som vi övervägt är att koppla behandlingstiden för en viss persons personuppgifter till en misstanke avseende den brottsliga verksamhet som Säkerhetspolisen ansvarar för. En person som är underrättelsemisstänkt för allvarlig brottslig verksamhet skulle då kunna behandlas under längre tid än de perifera personer som ingår i en kartläggning, utan att själva vara misstänkta. Ett sådant system skulle ha fördelen att personer vars beteende kan föranleda att Säkerhetspolisen får vidta olika åtgärder skulle kunna bevaras så länge det behövs. Personuppgifter avseende andra, mer perifera, personer skulle kunna ges en kortare behandlingstid. Att på så sätt koppla det intrång som en längre behandlingstid innebär för den enskilda till konkreta omständigheter som rör brottslig verksamhet skulle ligga i linje med Europadomstolens praxis att varje intrång i den personliga integriteten måste vara nödvändigt i ett demokratiskt samhälle.

Vi har dock som framgått kommit till slutsatsen att misstankemarkering i underrättelseverksamheten inte är lämplig att överföra till den nya lagen, se avsnitt 8.13.4. Misstanke är ett begrepp som inte lämpligen bör användas i detta sammanhang, då misstankarna i underrättelseverksamhet per definition inte får vara av sådan tyngd att det finns anledning att anta brott har förövats. Att peka ut vissa aktörer som underrättelsemisstänkta på så vaga grunder som förutsätts för att informationen ska utgöra underrättelseverksamhet framstår inte som rättssäkert och behandlingstidens längd kan då få ett betydande inslag av godtycke.

När uppgifter behandlas om personer som kan antas ha begått ett konkret brott ska som regel en förundersökning inledas, vilket innebär att rättegångsbalkens regler blir tillämpliga. En del av Säkerhetspolisens uppdrag är att förhindra brott. Det innebär ofta att en krets kring de som är underrättelsemisstänkta måste kartläggas. Exempelvis innebär misstankar om att en person är en utländsk underrättelseofficer att kartläggning måste ske av de personer som denne har kontakt med, ibland i flera led. Avgränsningsproblem kan lätt uppkomma i ett sådant system som endast utgår från en misstanke.

Problemet med att personuppgifter som förekommer i ett källmaterial som i andra delar är relevant adresseras inte heller genom

något av dessa alternativ. Vi har därför övervägt ett ytterligare alternativ som kan tillgodose kravet på proportionalitet vid personuppgiftsbehandling och samtidigt vara förenligt med en effektiv verksamhet för Säkerhetspolisen.

8.18 Säkerhetspolisen bör bestämma behandlingstiden i samband med registrering av uppgifter

8.18.1 Behovet kan ofta bedömas vid registrering

Förslag: Behandlingstiden ska bestämmas vid inledande granskning då personuppgifter registreras eller då personuppgifter börjar behandlas för ett nytt ändamål.

Behovet kan ofta förutses

Huvudregeln i dataskyddskonventionen och i Europadomstolens praxis är att personuppgifter inte får behandlas under längre tid än vad som är behövs med hänsyn till ändamålet med behandlingen.

Vi anser att det är möjligt att göra en bedömning av hur länge en person behöver vara registrerad hos Säkerhetspolisen redan då uppgiften registreras. Det finns redan i dagens lagstiftning ett synsätt som innebär att behovet av att behandla vissa uppgifter är beroende av karaktären av den företeelse som föranlett registreringen. I säpodatalagen finns en möjlighet för Säkerhetspolisen att specifikt inom området säkerhetshotande verksamhet som avses i 18 och 19 kap. brottsbalken och som utövas av främmande makt bevara uppgifter i upp till 40 år. Den förlängda behandlingstiden inom kontraspionaget motiverades i förarbetena med att främmande makts informationsinhämtning regelmässigt bedrivs långsiktigt inom ambitiösa spionprogram. Säkerhetspolisen kan redan på förhand förutse att kartläggning av sådan verksamhet kommer att vara relevant under lång tid. Regeringen förklarade att det innan säpodatalagen infördes regelmässigt fattades förlängningsbeslut vid slutet av den tioåriga behandlingsfristen. Säkerhetspolisen uppskattade att personal inom kontraspionaget fattade flera tusen sådana beslut varje år. Reger-

ingen motiverade den förlängda behandlingstiden inom denna verksamhetsgren med att det inte är rimligt att lägga betydande resurser på att regelbundet fatta beslut om förlängning, trots att det ofta på förhand kan förutses att förlängning av fristen är nödvändig. Risken för att behandlingen av uppgifter upphör i förtid på grund av tidsbrist eller felaktiga beslut vägdes också in.[138]

Inom kontraspionaget finns därmed ett uttalat behov av långsiktig kartläggning, vilket motiverat en möjlighet till längre behandlingsfrist för vissa uppgifter. Vi anser att samma synsätt kan göras gällande även inom andra verksamhetsområden. Som framgår i avsnitt 6.1.5 finns även inom andra verksamhetsgrenar behovet av att lagra uppgifter under längre tid än vad som följer av den nuvarande tioårsfristen. Exempelvis bör uppgifter om att en person är verksam i en organisation som ägnat sig åt systematiska, omfattande och grova övergrepp kunna behandlas i minst 25 år. I annat fall finns bland annat en risk att den personen på felaktiga grunder beviljas svenskt medborgarskap eller att uppgifter som behövs för utredning av brott utan preskriptionstid raderas i förtid. På motsvarande sätt kan det ofta gå att förutse att det saknas skäl att lagra uppgifter under så lång tid som är maximalt tillåtet. En kortare behandlingstid bör förstås gälla i sådana fall. Det bör alltså övervägas regler som tar hänsyn till dessa varierande förhållanden.

Behandlingstiden kan bestämmas efter inledande granskning

Vi anser att det finns skäl att föreslå regler som låter Säkerhetspolisen att på förhand besluta om differentierade och proportionella behandlingstider. Vi har föreslagit att uppgifter som samlas in eller inhämtas ska genomgå en inledande granskning innan de görs operativt tillgängliga. I samband med denna granskning bör behovet av uppgifterna kunna bedömas. Vi utgår ifrån att operativ personal som arbetar i de verksamheter som uppgifterna är hänförliga till kommer att utföra stora delar av denna inledande granskning. De kommer då att ha genomgått de utbildningarna m.m. som krävs för att granska att uppgifterna behandlas författningsenligt. När denna granskning utförs bör det framtida behovet av uppgifterna i verksamheten kunna bedömas.

[138] Se prop. 2018/18:162 s. 124 ff.

Genom att beslutet om behandlingstid tar sikte det konkreta behovet i det enskilda fallet kommer dataskyddskonventionens krav att kunna uppfyllas. Risken att uppgifter behandlas under orimligt lång tid på grund av att de inte hunnit eller kunnat omprövas minskar också då behandlingstiden är individuellt anpassad.

Om Säkerhetspolisen, då personuppgifter registreras, bestämmer en behandlingstid kan både verksamhetens behov och integritetsintresset värnas. Detta system har delvis sin förebild i Danmark och de regler som gäller för den danska säkerhetstjänsten PET, se avsnitt 4.2.2.

Ny behandlingstid för nya ändamål

En personuppgift som inledningsvis behandlats för ett visst ändamål kan komma att återaktualiseras för ett annat. Exempelvis kan uppgifter som inledningsvis behandlats för att kartlägga terroristnätverk visa sig leda till främmande makts säkerhetshotande verksamhet. Uppgifter som behandlas för underrättelseändamål kan ge upphov till att en förundersökning inleds. Uppgifter från en förundersökning kan behöva fortsätta att behandlas i underrättelseverksamhet. Ett annat exempel är att personuppgifter kan behöva behandlas för utvecklingsändamål (se avsnitt 8.4.6).

Behovet av att behandla uppgifter i den nya verksamheten, för andra ändamål, är inte alltid detsamma som behovet av uppgifterna i den verksamhet där de ursprungligen behandlats. När uppgifter börjar behandlas för ett nytt ändamål måste behandlingstiden därmed bestämmas efter behovet i förhållande till det nya ändamålet.

8.18.2 Längsta behandlingstid i lag

Förslag: Behandlingstiden får inte bestämmas till längre än vad som behövs för ändamålet och får inte överskrida

- 60 år om ändamålet för behandlingen hänför sig till säkerhetshotande verksamhet från främmande makt,
- 5 år om uppgifterna behandlas endast för utvecklingsändamål, och
- 25 år om uppgifterna behandlas för något annat ändamål.

Det finns skäl att föreskriva en längsta behandlingstid i lag

I och med att en behandlingstid bestäms redan vid registreringen av en uppgift kommer det att finnas en yttre gräns för varje personuppgift som behandlas. Det bör dock även finnas en dataskyddsmekanism som förhindrar registreringar som i praktiken är obegränsade i tid. Inom denna yttre tidsram bör Säkerhetspolisen kunna besluta om en behandlingstid anpassad efter ändamålet med behandling, uppgiftens karaktär och övriga omständigheter.

En längsta behandlingstid som regleras i lag är normerande för vilka tider som Säkerhetspolisen bestämmer, där den yttersta tiden i spannet måste vara förbehållet de mest angelägna fallen. Vidare ger det ett mått av transparens som annars inte är möjlig att uppnå.

En längsta behandlingstid som är angiven i lag bör kunna vara betydligt längre än den nuvarande tioårsfristen, eftersom den inte är avsedd att utgöra den generella behandlingstiden för samtliga uppgifter. Dagens tioårsfrist utgör en balans mellan intresset av att inte vara registrerad och Säkerhetspolisens behov av kartläggning av brottslig verksamhet. Det innebär att behov kopplade till skyddet av nationell säkerhet har fått stå tillbaka för att balansera intrånget i enskildas fri- och rättigheter. Vi föreslår att denna bedömning inte på samma sätt ska göras på lagstiftningsnivån utan i stället i tillämpningen av differentierade behandlingsfrister i det enskilda fallet. Lagstiftningen bör därför medge en behandlingstid som på ett bättre sätt motsvarar det faktiska behovet av att i vissa särskilt angelägna fall kunna behandla uppgifter under lång tid.

En rimlig behandlingstid för underrättelseverksamheten

En generell behandlingstid som medger kartläggning över tid

Den längsta behandlingstiden bör vara tillräckligt för att kunna kartlägga centrala individer inom alla verksamhetsgrenarna så länge dessa personer kan anses utgöra ett hot mot nationell säkerhet. Den brottskatalog som Säkerhetspolisen i dag ansvarar för innehåller en rad mycket allvarliga brott där det i vissa fall saknas preskriptionstid. Det finns erfarenheter av att personer som begått allvarliga brott upptäcks och lagförs efter mycket lång tid. I dessa fall kan underrättelseuppgifter spela en avgörande roll i brottsutred-

ningen. Samtidigt bör det finnas en rimlig gräns för hur länge en person kan kvarstå utan att behovet omprövas. Så som illustreras i fallet *Segerstedt-Wiberg m.fl. mot Sverige* finns alltid en risk (eller möjlighet) att omvärlden förändras på så sätt att misstankar efter ett antal decennier kan framstå som främmande, om än de framstod som relevanta i sin ursprungliga omvärldskontext.

Vi anser att den längsta behandlingstid som bör kunna beslutas då personuppgifter registreras ska vara 25 år. Efter 25 år bör den brottsliga verksamheten antingen ha konkretiserats genom nya uppgifter eller kunnat avfärdas. Denna längsta tid är förstås avsedd att tillämpas endast i de mest angelägna fallen.

Främmande makts säkerhetshotande verksamhet

Alltjämt kvarstår behovet av att kunna kartlägga företeelser som statliga aktörer ligger bakom. Inom främmande makts spionprogram som riktas mot Sverige och vårt närområde utgör enskilda personer endast kuggar i en betydligt större maskin. På motsvarande sätt som i den nuvarande lagstiftningen finns därför skäl att se annorlunda på personuppgifter som behandlas för ändamålet kontraspionage. Säkerhetspolisen bör ha möjlighet att teckna en bild av hela spionprogrammet och hur det utvecklas över tid.

Den nuvarande behandlingsfristen är 40 år för sådana uppgifter. Säkerhetspolisen har pekat på flera förhållanden som talar för att denna tidsfrist inte är tillräckligt lång. Utländska underrättelseofficerare behöver exempelvis regelmässigt kartläggas under hela den tid då de kan förväntas arbeta på främmande makts uppdrag. Denna tid överensstämmer inte alltid med en tjänstetid. En underrättelseofficer som bosätter sig i Sverige efter pension kan alltjämt förväntas vara av intresse för Säkerhetspolisen. För att kunna kartlägga utländsk underrättelseverksamhet bör personuppgifter därför få behandlas under mycket lång tid. I likhet med vad som framförts angående den militära underrättelse- och säkerhetstjänstens kartläggning av utländska militära befattningshavare bör behandlingstiden motsvara en persons hela aktiva karriär.

Vi anser därför att en yttre behandlingsfrist bör vara 60 år i dessa fall. Integritetsintresset hos personal som är verksamma vid ambassader eller andra beskickningar med uppdrag för främmande makt

väger ofta inte heller lika tungt som i många andra fall. En person som är utsänd att för sin stats räkning inhämta information, eller den som har samröre med en sådan person, räknar sannolikt med att i någon mån vara kartlagd av värdlandets säkerhetstjänst. Att uppgifter om denna behandlas under lång tid kan därför ofta vara proportionellt.

Utvecklingsändamål

Vi har föreslagit en lagregel som uttryckligen medger att Säkerhetspolisen ska få behandla personuppgifter för att fortlöpande utveckla den teknik och metodik som behövs för brottsbekämpningen. För sådana utvecklingsändamål kan finnas integritetsrisker som inte motsvaras av ett motsvarande allmänintresse.

När personuppgifter behandlas för andra operativa ändamål bör det inte finnas något hinder mot att dessa uppgifter även används för exempelvis maskininlärning. Denna behandling får då prövas utifrån de grundläggande kraven på bland annat proportionalitet.

När uppgifter däremot samlats in enbart för utvecklingsändamål, eller på annat sätt endast behandlas i detta syfte, finns det dock skäl att begränsa behandlingstiden. Uppgifter som behandlas enbart för utvecklingsändamål kan röra personer som inte på något sätt genom sitt eget beteende kan förvänta sig att finnas registrerade hos Säkerhetspolisen. Det kan exempelvis röra sig om personuppgifter som används för att förbättra språkmodeller, översättningstjänster eller ansiktsigenkänningsprogramvara.

Sådana uppgifter bör endast få behandlas under kortare tid och som längst i fem år.

8.18.3 Proportionell behandlingstid

Förslag: Behandlingstiden ska bestämmas så att en proportionerlig behandling av personuppgifter uppnås. Det innebär att tiden inte endast ska bestämmas efter verksamhetens behov utan även beakta intrånget i de enskilda eller allmänna intressena som behandlingen innebär över tid.

Den längsta tiden för behandling av personuppgifter bör som sagt inte vara densamma som den tid som alla personuppgifter i praktiken behandlas. I likhet med annan personuppgiftsbehandling enligt lagen ska bestämmande av behandlingstid vara förenlig med de grundläggande principerna för ett fri- och rättighetsintrång. Det innebär att behandlingstiden inte ska vara längre än vad som behövs för ändamålet med behandlingen och inte heller utgöra ett oproportionerligt intrång i den registrerades fri- och rättigheter.

Den första delen av denna prövning, hur länge uppgifterna behövs är givetvis beroende av vilket ändamål och vilken slags uppgifter det är fråga om. Som nämnt kan det vid kartläggning av främmande makts underrättelseverksamhet i Sverige ofta finnas behov av en långsiktig kartläggning. När det å andra sidan gäller personuppgifter som ska behandlas för att utforma hot- och riskanalyser inom personskyddsverksamhet kan uppgifter ofta vara mer av en färskvara.

När behovet klarlagts krävs att behovet och ändamålet prövas mot andra skyddsvärda intressen; i första hand den registrerades intresse av att inte förekomma i Säkerhetspolisens register längre än nödvändigt. Även andra allmänna intressen som risken för att opinionsfriheterna påverkas negativt ska vägas in. Det kan exempelvis finnas en avkylande effekt för den fria åsiktsbildningen om uttalanden och uttryck för politisk övertygelse bevaras mycket länge. Om intrånget i fri- och rättigheter är så stort att behandlingen sammantaget framstår som oproportionerlig, måste behandlingstiden förkortas för att nå en jämnvikt mellan behovet av att skydda nationell säkerhet och enskildas grundläggande fri- och rättigheter.

Eftersom den längsta behandlingstiden ska anses vara reserverad för det fall då ändamålen med styrka talar för att den ska bestämmas till 25 år kommer normaltiden behöva vara kortare. Vid en bred underrättelseinhämtning, då misstankar om brottslig verksamhet är vaga, får behovet av uppgifterna anses relativt sett lägre än vad som är fallet exempelvis om en person rest för att ansluta sig till Islamiska staten. Att behandla personuppgifter i 25 år vid en sådan bredare kartläggning, av exempelvis en viss miljö där radikalisering kan misstänkas, skulle vara ett oproportionerligt intrång i de registrerades personliga integritet och medföra risker för opinionsfriheterna.

I de fall, då ändamålet med att behandla de enskilda personuppgifterna saknar närmare konkretion kan inte proportionalitetsröv-

ningen medge en allt för lång behandlingstid. Ett bredare underrättelseändamål tillåter behandling av många personuppgifter. Detta måste kompenseras genom en betydligt kortare behandlingstid för detta ändamål, för att behandlingen ska anses proportionerlig och uppfylla kravet på att vara nödvändigt i ett demokratiskt samhälle.

Det finns flera faktorer som kommer att behöva beaktas vid avvägningen. I svensk lagstiftningstradition anges sällan de ingående parametrarna i en proportionalitetsprövning. Hur bedömningen ska gå till följer bland annat av praxis från Europadomstolen och svenska domstolar. Vi uppfattar att det inte heller är lämpligt att låsa fast prövningen kring vissa bestämda rekvisit. Innehållet i olika begrepp skiftar över tid och är beroende av bland annat utvecklingen i samhället och ny teknik. Någon närmare instruktion i lagstiftningen för hur behandlingstiden generellt ska bestämmas behövs därmed inte. Det är tillräckligt att hänvisa till att behandlingstiden är en del av den proportionalitetsprövning som ska gälla all personuppgiftsbehandling.

I denna bedömning ingår att pröva behovet av att behandla uppgifterna mot det intrång som registreringen innebär för den enskilde. Behovet av fortsatt behandling avtar ofta över tid. Intrånget däremot får anses vara relativt sett högre ju längre en uppgift finns bevarad hos en säkerhetstjänst, särskilt om uppgifterna är av känslig eller privat natur. Intrångsbedömningen bygger på den grundläggande tanken att varje år en uppgift behandlas minskar normalt behovet samtidigt som intrånget ökar. När intrånget överstiger behovet föreligger inte längre proportionalitet och behandlingen ska därmed avslutas.

Självklart måste bedömningen i verksamheten ofta vara schabloniserad och det kommer finnas ett stort behov av metodstöd för de medarbetare som fastställer behandlingstid. Denna modell förutsätter även att verksamhetsstöden anpassas till det förändrade regelverket så att det ger stöd för dessa bedömningar.

8.18.4 Behandlingstid för uppgifter om barn

Förslag: Det ska framgå att Säkerhetspolisen ska ta hänsyn till att barns personuppgifter ska omfattas av ett särskilt starkt personuppgiftsskydd.

När det gäller barn som registreras hos Säkerhetspolisen finns i 4 kap. 7 § andra stycket säpodatalagen särskilda bestämmelser om behandlingstid. För gemensamt tillgängliga uppgifter är behandlingstiden hälften så lång för barn som för vuxna. Denna ordning var ursprungligen intern myndighetspraxis som kodifierades i samband med säpodatalagens tillkomst. De integritetsskyddande reglerna ansågs göra sig gällande i särskilt hög grad vid behandling av uppgifter om barn.[139] Motsvarande argumentation ligger även bakom bland annat de förkortade gallringstiderna ur belastningsregistret. Vissa påföljder gallras ur belastningsregistret efter fem år om uppgiften avser en person som var under 18 år vid tidpunkten för brottet. För vuxna är motsvarande gallringsfrist tio år.[140]

Vi anser att det finns goda skäl för att uppgifter om barn inte ska registreras enligt samma principer som för vuxna. En belastande registrering som avser en ung person får anses utgöra ett större integritetsintrång än en motsvarande registrering för en vuxen. Intrånget över tid får även anses öka i högre takt när det gäller registreringar som avser barn. Det finns skäl för att misstag som beror på bristande utveckling och dåligt omdöme i barndomen inte ska påverka individens framtida livsval i högre grad än nödvändigt.

Uppgifter om barn som inte innebär något påtagligt intrång i barnets rätt bör dock inte omfattas av särskilda regler. Om det finns uppgifter om ett barn som exempelvis omnämns i ett samtal eller förekommer på ett fotografi behöver inte några särskilda hänsyn tas. Barnets rätt kan inte anses ha påverkats genom att förekomma i ett sådant sammanhang. Att barns personuppgifter är mer skyddsvärda avser belastande registreringar.

Vi anser att det vid bestämmande av behandlingstid särskilt ska beaktas att uppgifter som rör barn ska omfattas av ett särskilt starkt personuppgiftsskydd. Detta bör komma till uttryck i lag och innebär att detta förhållande särskilt ska beaktas. Det finns dock inte skäl att föreskriva någon bestämd kortare behandlingstid i dessa fall. Behandlingstiderna är som sagt avsedda att utgöra ett tak, och inte att den normala behandlingstiden. Att barns uppgifter ska omfattas av ett särskilt starkt personuppgiftsskydd medför att de längsta behandlingstiderna bör tillämpas endast i undantagsfall.

[139] Prop. 2018/19:163 s. 121.
[140] Se 17 § lagen (1998:620) om belastningsregisterlag och prop. 2009/10:191 s. 10 ff.

8.18.5 Behandlingen ska upphöra om det framgår att uppgifterna inte behövs

Förslag: Personuppgifter får inte behandlas om det framgår att uppgifterna inte längre behövs för ändamålet med behandlingen.

Av behovsprincipen följer att personuppgifter endast får behandlas om de behövs för ett ändamål. Den nuvarande ordningen bygger på tanken om att behovet av en uppgift kontinuerligt ska omprövas. Det system vi föreslår innebär att prövningen görs på förhand, då behandlingen av uppgiften påbörjas.

Även om det följer av den allmänna principen om att uppgifter som inte behövs inte ska behandlas kan det finnas anledning att särskilt ange att detta gäller även inom behandlingsfristen. Om Säkerhetspolisen upptäcker att personuppgifter inte längre behövs ska det finnas en skyldighet att omedelbart avsluta behandlingen.

Vi kommer i avsnitt 8.20.2 närmare redogöra för vår syn på kontinuerlig personuppgiftsgranskning.

8.18.6 Det bör vara möjligt att förlänga behandlingstiden

Förslag: Säkerhetspolisen ska få besluta att förlänga behandlingstiden för personuppgifter som fortfarande behövs för det ändamål som de behandlas för.

Säkerhets- och integritetsskyddsnämnden ska underrättas om behandlingstiden överstiger de längsta tider som anges i lag.

Enligt 4 kap. 10 § säpodatalagen får Säkerhetspolisen, om det finns särskilda skäl, besluta att personuppgifter får behandlas under längre tid än vad som följer av de olika fristerna i lagen. Ett särskilt skäl kan vara att ärendet rör en företeelse eller en person som har förlorat aktualitet men som goda grunder kan antas få ny betydelse i framtiden. Av förarbetena framgår att ett förlängningsbeslut ska dokumenteras särskilt och behovet av längre behandlingstid motiveras.[141]

[141] Se prop. 2018/19:163 s. 127 och 238 samt prop. 2009/10:85 s. 269.

Även om behandlingstiden differentieras på ett annat sätt genom vårt förslag kan behovet av uppgifter förändras då de behandlats en tid. Nya uppgifter om personen eller en bättre förståelse för den företeelse som uppgifterna har anknytning till kan förändra tidigare bedömningar. Det finns därför alltjämt goda skäl till att den tid som ska bestämmas i samband med registrering ska kunna förlängas om behovet av uppgiften kvarstår eller om det är möjligt att förutse att den är längre än vad som antogs då uppgiften registrerades.

Att det ska finnas möjlighet att förlänga och ompröva behandlingstid kan också bidra till att tiderna inte sätts längre än vad som är nödvändigt ”för säkerhets skull”. Det är Säkerhetspolisens ansvar att bestämma behandlingstiden med tillämpning av proportionalitetsprincipen inom de gränser som anges i lagen. Om det finns behov av att förlänga behandlingstiden, antingen för att den löpt ut eller för att det går att förutse att behovet är längre, bör Säkerhetspolisen kunna göra det på samma sätt som då behandlingstiden bestäms. Så länge förlängningen inte innebär att uppgiften behandlas längre än vad som hade kunnat bestämmas redan första gången finns inte någon anledning att ställa några krav på särskilda skäl eller liknande.

Om behandlingstiden däremot förlängs över de frister som anges i lagen, 25 år eller 60 år, bör det ställas krav på att det ska göras genom ett motiverat beslut. Om det är proportionerligt att förlänga tiden längre än 25 år, får det antas att skälet som talar för åtgärden är av väsentlig betydelse för nationell säkerhet. I dessa fall bör även Säkerhets- och integritetsskyddsnämnden underrättas om beslutet, i syfte att effektivisera tillsynen över denna prövning.

8.18.7 Behandlingstiden för uppgifter som är förenade av ett sammanhang bör kunna bedömas gemensamt

Förslag: Det ska vara möjligt att bestämma en proportionerlig behandlingstid för alla personuppgifter som är förenade av ett sammanhang.

Underrättelseverksamhet kräver sammanhang

Säkerhetspolisens behov skiljer sig mycket från den personuppgiftsbehandling som utförs av många andra myndigheter. En myndighet som exempelvis Försäkringskassan eller Centrala Studiestödsnämnden behandlar i huvudsak uppgifter som den enskilde lämnat in och som är relevanta för att pröva ett visst ärende. Detsamma gäller personuppgiftsbehandling som sker inom näringslivet, där den enskilde lämnar ifrån sig personuppgifter genom att exempelvis använda sig av vissa tjänster. Den största delen av personuppgifter från sådan insamling rör den enskilde själv. Systematiken inom personuppgiftsrätten utgår ofta denna typ av personuppgiftsbehandling där de registrerade kan särskiljas och bedömas för sig.

I dag är utgångspunkten även för Säkerhetspolisens personuppgiftsbehandling att olika personers uppgifter behandlas var för sig i olika personakter. Denna struktur är dock inte anpassad för myndighetens uppdrag som bland annat innebär aktiv informationsinhämtning i syfte att upptäcka brottslig verksamhet. Vi har i avsnitt 8.6.3 redogjort för vår bedömning av att det för den nationella säkerhetstjänsten inte kan ställas krav på att behovet av varje enskild personuppgift alltid ska kunna motiveras, utan att ändamålen för personuppgiftsbehandling ska kunna avse sammanhang. Detta har vi formulerat som att samtliga uppgifter i ett relevant sammanhang kan behövas för kartläggning av brottslig verksamhet. Frågan är hur behandlingstiden ska bestämmas för dessa uppgifter.

Om Säkerhetspolisen exempelvis behandlar en avlyssnad konversation mellan två personer kommer det där förekomma personuppgifter av olika slag. I konversationen kommer det givetvis finnas uppgifter om de personer som talar med varandra, men ofta också en mängd direkta eller indirekta personuppgifter som rör andra, som endast omnämns. Även om det skulle vara önskvärt att de individer som inte har något att göra med den brottsliga verksamhet som kartläggs skulle maskeras eller registreras endast under en kortare tid är detta i praktiken inte möjligt.

För det första är det inom underrättelseverksamheten svårt att på ett tidigt stadium ha den överblick som krävs för att kunna avfärda uppgifter om individer som omnämns på detta sätt som obehövliga. Det följer av underrättelseverksamhetens natur att det behövs

en bredare kartläggning för att slutligen kunna klarlägga vilka personuppgifter som hör till relevanta aktörer och vilka som inte gör det.

För det andra skulle en radering av vissa personuppgifter i den exemplifierade konversationen kunna förta sammanhanget av andra uppgifter. Om ett avlyssnat samtal skulle vara fullt av raderade partier eller plötsliga luckor, där en person som är perifer i sammanhanget omnämns, skulle källvärdet av samtalet som helhet riskera att bli påtagligt lägre.

För det tredje innebär den manuella bedömningen och gallringen bland alla de personuppgifter som kan förekomma i en informationsmängd en påtaglig och i praktiken svårhanterad administrativ börda.

Det finns exempel på hur frågan om personuppgifter i ett sammanhållet källmaterial kan hanteras. I den danska lagstiftningen finns exempelvis en bestämmelse som innebär att PET inte är skyldig att radera personuppgifter som ingår i handlingar eller liknande om handlingen i övrigt uppfyller behovskriteriet för att bevaras. Regeln innebär alltså att behovet av att bevara handlingen även omfattar de uppgifter i den som i och för sig inte behövs eller är relevanta för ändamålet med insamlingen. I Danmark finns därmed en skillnad i regleringen av skyldigheten att radera personuppgifter som förekommer på uppgiftsnivå i förhållande till det som kan betecknas som dokumentnivå.

Behandlingstiden bör kunna bestämmas för ett källmaterial i sin helhet med beaktande av proportionalitetsprincipen

Som tidigare nämnts utgör bestämmande av behandlingstid en central del av proportionalitetsprövningen i Säkerhetspolisens personuppgiftsbehandling. En längre behandlingstid utgör ett större intrång som måste vara motiverat av starkare skäl än en kortade behandlingstid. Vi har anammat synsättet att Säkerhetspolisens personuppgiftslagstiftning måste vara anpassat efter myndighetens särskilda verksamhet, där en av förutsättningarna är att fler personuppgifter behöver behandlas än för många andra myndigheter.

Det finns ett behov att i större utsträckning än tidigare kunna bedöma material i ett sammanhang. Det kan exempelvis röra sig om ett it-beslag i form av en mobiltelefon. I stället för att gå igenom varje enskild personuppgift i beslaget bör behovet av att bevara de uppgifter som finns i telefonen kunna bedömas samlat. Ett sådant

källmaterial innehåller ofta betydligt fler personuppgifter än vad som är direkt relevant för ändamålet med behandlingen. För att sådan information ska kunna behandlas krävs ett regelverk som erkänner och klargör att det är relevant och adekvat att behandla även mer perifera personers uppgifter över tid. Det kan exempelvis vara anhöriga eller bekanta till den som beslaget riktades mot men som inte genom eget beteende gjort skäl för att finnas registrerade hos Säkerhetspolisen. Dessa personers personuppgifter behandlas inte för att upptäcka eller förebygga brottslig verksamhet där de själva ingår. Uppgifterna behandlas i stället för att kartlägga den aktör som ingår i en viss brottslig verksamhet och därmed för att kartlägga och klarlägga den brottsliga verksamheten i stort. Detta får betydelse även för frågan om hur behandlingstiden ska bestämmas.

För att det ska vara möjligt för Säkerhetspolisen att på ett effektivt sätt bedriva sin verksamhet bör behandlingstid för uppgifter som förekommer i större, integrerade sammanhang kunna bestämmas gemensamt. Behandlingstiden bestäms då inte för varje persons uppgifter, utan för en viss handling eller ett visst sammanhang.

När behandlingstiden ska bestämmas kommer frågan om proportionalitet att vara avgörande. I många fall kan det vara möjligt för Säkerhetspolisen att avgränsa ett material på så sätt att det mest centrala personuppgifterna kan behandlas under den tid som behövs. Om det emellertid förekommer en större mängd mer perifera personuppgifter i ett informationsunderlag, är det vår uppfattning att det bör påverka behandlingstiden för materialet som helhet. Det samlade integritetsintrånget för materialet blir högre ju fler personers uppgifter som behandlas. Eftersom behovet av att bevara de mer perifera uppgifterna inte är av samma styrka som behovet avseende de centrala aktörerna, kan behandlingstiden för materialet i sin helhet behöva justeras nedåt för att uppnå proportionalitet.

En omfattande behandling kan normalt inte ske lika länge som en mer koncentrerad, eftersom intrånget blir större ju fler uppgifter det rör sig om. Samtidigt kan ett mycket tungt vägande ändamål motivera en lång behandlingstid för de uppgifter som ingår i kartläggningen. Det krävs dock ett konkret och specifikt ändamål av tillräcklig tyngd för att väga upp intrånget för de personer som inte är föremål för några omedelbara misstankar. Det kan vara till fördel om Säkerhetspolisen utformar metodstöd som medför viss schablonisering av bedömningen.

8.18.8 Från vilken tid ska behandlingsfristen räknas?

Förslag: Behandlingstiden ska antingen räknas från den senaste registreringen avseende personens anknytning till ändamålet för behandlingen eller avse viss tid.

Den nuvarande ordningen

Den nuvarande säpodatalagen innehåller flera olika bestämmelser om den tidpunkt från vilken de olika behandlingstiderna ska räknas.

För uppgifter som inte är gemensamt tillgängliga räknas tiden från att det ärendet avslutats eller, om de inte kan hänföras till ett ärende, från att uppgifterna behandlades första gången. För uppgifter som förekommer i brottsanmälningar är gränsen densamma som åtalspreskription. I avslutade förundersökningar räknas behandlingstiden från besluts- eller domsdatum. För övriga uppgifter som gjorts gemensamt tillgängliga räknas tiden från utgången av det kalenderår då den senaste registreringen gjordes avseende personen. För sådana personuppgifter som behandlas inom kontraspionaget krävs dock att registreringen ska avse personens anknytning till brott eller brottslig verksamhet.

De olika tidsfristerna bygger på en systematik från brottsdatalagen och tidigare polisdatalagar. Polisens underrättelseverksamhet sker i stor utsträckning i särskilda underrättelseärenden, där tanken är att uppgifterna endast behandlas av ett fåtal personer. I sådana underrättelseprojekt får uppgifter behandlas till dess att ärendet avslutades och ett år därefter. För Säkerhetspolisens finns inga egentliga skäl att inleda motsvarande underrättelseärenden. Vi anser att den nya lagen behöver ha en annan utgångspunkt när det gäller hur behandlingsfristen ska konstrueras.

Det behövs en möjlighet att räkna behandlingsfristen för varje person från den senaste registreringen

Det finns ett behov av att behandla uppgifter i personakter

Det nuvarande systemet är komplext på ett sätt som inte framstår som motiverat av integritetshänsyn. Den behandlingsfrist som i dagsläget främst tillämpas är att tiden förlängs vid varje ny registrering. Denna bestämmelse är lätt att tillämpa om det förekommer personakter i verksamheten. Varje uppgift som tillförs en personakt förlänger då tiden som hela akten får behandlas. Bestämmelsen är dock inte lätt att tillämpa för uppgifter som förekommer i integrerade sammanhang. Det är svårt att hantera ett dokument som innehåller uppgifter om flera olika personer.

Det finns alltjämt ett stort behov av att behandla uppgifter på ett sätt som påminner om personakter. Personer som är centrala i underrättelseverksamheten utgör aktörer i system vilket gör det möjligt att exempelvis koppla samman dem i olika nätverk eller länka en person till en företeelse. Att skapa en aktör i systemet innebär att information och uppgifter bearbetas och sammanförs på ett sådant sätt att alla uppgifter kan behandlas fristående från sina olika källor. För de existerande och framtida personuppgifter som behandlas på detta sätt utgör tiden från den senaste registreringen ett lämpligt sätt att bestämma behandlingstid. Denna möjlighet bör därför i och för sig behållas.

Vilken slags uppgift ska kunna förlänga behandlingstiden?

När behandlingstiden bestäms för en persons personuppgifter är det alltså lämpligt att fristen räknas från den senaste registreringen. Frågan är om alla uppgifter ska kunna förlänga en behandlingsfrist eller endast uppgifter av mer kvalificerat slag.

För Polismyndighetens kriminalunderrättelseverksamhet är det nya registreringar beträffande personens anknytning till brottslig verksamhet som förlänger behandlingsfristen.[142] Frågan om motsvarande krav skulle ställas på uppgifter i Säkerhetspolisens underrättelseverksamhet togs upp i förarbetena till säpodatalagen. Utredningen föreslog en motsvarande bestämmelse som för Polismyndigheten

[142] Se 4 kap. 7 § polisens brottsdatalag.

även för Säkerhetspolisens del. Regeringen delade bedömningen att tiden för hur länge personuppgifter får behandlas hos Säkerhetspolisen naturligtvis inte ska kunna påverkas av att vilka uppgifter som helst registreras. När det gäller Säkerhetspolisens underrättelseverksamhet menade emellertid regeringen att det ofta är svårt att veta vilken brottslig verksamhet en viss uppgift kan hänföras till, eftersom myndigheten agerar i ett så tidigt skede. Om möjligheterna att fortsätta behandla personuppgifter knyts till omständigheter som har betydelse för personens anknytning till brottslig verksamhet, skulle det enligt regeringen kunna vara negativt för Säkerhetspolisens underrättelseverksamhet. Regeringen stannade därför vid den reglering som tidigare gällt. Regeringen framhöll dock att det självfallet är viktigt att inte vilka uppgifter som helst ska kunna påverka behandlingstiden och att det hade varit önskvärt med ett sådant förtydligande.[143]

För registreringar inom kontraspionaget räknas i stället den 40-åriga behandlingstiden från den sista registreringen som rör personens koppling till brottslig verksamhet, vilket hör samman med att det endast är för detta ändamål som denna behandlingsfrist gäller.

När Säkerhetspolisen efter den inledande granskningen registrerar nya personuppgifter för fortsatt behandling ska det ske för ett särskilt, uttryckligt angivet och berättigat ändamål, se avsnitt 8.7. Vid en sådan granskning borde det stå klart om den nya uppgiften är av betydelse för det specifika ändamål som personuppgifterna ursprungligen behandlas för. Om ändamålet med behandling är att kartlägga viss brottslig verksamhet, är uppgifter som inhämtats om personer i denna miljö normalt sett av betydelse för ändamålet. Om det däremot kontinuerligt inhämtas adressuppgifter för dessa personer, bör registreringarna inte i sig anses vara av tillräcklig betydelse för ändamålet att kartlägga den brottsliga verksamheten. Registreringen får inte vara rutinmässig eller för att hålla uppgifter uppdaterade. Det måste krävas att registreringen sker för att berika underrättelsematerialet, inte endast hålla det uppdaterat.

Vi anser mot denna bakgrund att behandlingstiden ska kunna räknas från den sista registreringen som är av betydelse för ändamålet med behandlingen.

[143] Prop. 2018/19:163 s. 121 f.

Det behövs en möjlighet att bestämma en fast behandlingstid

I säpodatalagen finns inte några särskilda regler om behandlingstiden för annat än enskilda personuppgifter. Det finns exempelvis inte några regler om hur länge ett dokument, innehållandes personuppgifter angående många olika personer, ska behandlas. Även om alla personuppgifter behövs och dokumentet i och för sig får behandlas, kommer en ny registrering avseende en av personerna som förekommer där att medföra att behandlingsfristen blir olika för olika delar av dokumentet. Den nya registreringen förlänger nämligen behandlingstiden för samtliga uppgifter om den personen, men inte för de andra.

Information från ett dokument måste därför brytas ut och behandlas för sig. Dokumentet i sin helhet kan endast bevaras i tre år enligt reglerna om uppgiftssamlingar för bearbetning och analys, i 4 kap. 8 § säpodatalagen. Att bryta ut varje enskild persons uppgifter för att behandla i varje persons personakt är inte en effektiv informationshantering.

Vi har i avsnitt 8.18.7 föreslagit att det ska vara möjligt för Säkerhetspolisen att bedöma uppgifter som är förenade av sitt sammanhang gemensamt. Hur länge ett sådant sammanhang, som ett dokument eller en datafil, får behandlas ska bestämmas då uppgifterna registreras. Eftersom det inte är möjligt med en löpande behandlingstid som utgår från den sista registreringen måste behandlingstiden vara fast och utgå från datumet för registreringen.

Den behandlingstiden avser då samtliga personuppgifter som är förenade av sammanhanget. Det innebär att enskilda uppgifter som behöver bevaras längre än vad som är proportionerligt för hela detta sammanhang kan behöva brytas ut och behandlas för sig.

Att kunna bestämma en fast behandlingstid är en möjlighet, men inget krav. Om det genom nya tekniska landvinningar exempelvis är möjligt att automatiskt maskera personuppgifter ur ett dokument efter att behandlingstiden löpt ut kan den löpande behandlingstiden även användas för uppgifter som finns i ett gemensamt sammanhang.

8.18.9 Uppgifter i ärenden om utredning eller lagföring av brott

Bedömning: Det behövs inte några särskilda bestämmelser för uppgifter i ärenden om utredning eller lagföring av brott.

Den nuvarande regleringen

Att Säkerhetspolisen har brottsutredande och lagförande uppgifter innebär att det finns ett relativt omfattande regelverk kring hur misstänktas personuppgifter får behandlas. Bestämmelserna är direkt överförda från 2010 års polisdatalag och identiska bestämmelser återfinns i polisens brottsdatalag.

Reglerna, som återfinns i 4 kap. 3–5 §§ säpodatalagen kan sammanfattas enligt följande. Personuppgifter som finns i en brottsanmälan får inte behandlas om anmälan avskrivs för att den påstådda gärningen inte utgör brott eller efter att det anmälda brottet preskriberats. Personuppgifter som finns i en förundersökning får inte behandlas längre än fem år efter att förundersökningen lagts ned eller en dom vunnit laga kraft. Vidare får inte personer som frikänts för brott eller där förundersökning eller åtal mot personen lagts ner vara sökbara som misstänkta för det aktuella brottet.

Ursprungligen är de särskilda reglerna för uppgifter i avslutade förundersökningar motiverade av att Polismyndigheten har ett behov av att behandla uppgifter som förekommit i brottsanmälningar och förundersökningar under längre tid än andra uppgifter. Efter en tid kan nya uppgifter framkomma som kan göra att en nedlagd förundersökning behöver tas upp på nytt. Det ansågs även viktigt att kunna jämföra uppgifter ur äldre förundersökningar med nya omständigheter vid seriebrottslighet eller för att belysa förhållande mellan en misstänkt gärningsman och ett brottsoffer. Den femårsgräns som angetts ansåg regeringen vara en rimlig avvägning mellan verksamhetens behov och de registrerades integritet.[144]

För Säkerhetspolisens del utgör reglerna emellertid inte en verksamhetsanpassad förlängning av behandlingstiden i vissa fall. Tvärtom utgör reglerna en begränsning, eftersom den generella behandlingstiden för de flesta uppgifter som Säkerhetspolisen behandlar är tio år

[144] Prop. 2009/10:85 s. 225 ff.

från den senaste registreringen. Det innebär att uppgifter som stärker misstankarna mot en person, exempelvis genom att en brottslig verksamhet kan konkretiseras till en brottslig gärning, i praktiken behandlas kortare tid än uppgifter som behandlas för andra ändamål än brottsutredning. Om uppgiften innebär att det finns anledning att anta att ett brott som hör under allmänt åtal har förövats, ska en förundersökning inledas. På grund av att de brott som Säkerhetspolisen ansvarar för är särskilt svårutredda leder dock sällan förundersökning till åtal. Det är därför vanligt att förundersökningar behöver läggas ner. Enligt 4 kap. 4 § säpodatalagen får personuppgifter som finns i en förundersökning inte behandlas längre än fem år efter nedläggningsbeslutet. Hade uppgiften inte räckt till för att inleda förundersökning, hade behandlingstiden i stället varit tio år.

Inga särskilda regler om behandlingstid för personuppgifter som behandlas för utredning och lagföring av brott

Förundersökningar och andra brottsutredningar utgör endast en mindre del av Säkerhetspolisens verksamhet. De förundersökningar som bedrivs leder mer sällan till åtal jämfört med annan polisverksamhet. Det beror delvis på de särskilda bevissvårigheter som är förknippade med Säkerhetspolisens brottskatalog, men även på Säkerhetspolisens fokus att i ett tidigt skede förhindra brott. De förundersökningar som inleds är ofta resultatet av ett aktivt underrättelsearbete och mer sällan initierade på grund av en brottsanmälan.

Säkerhetspolisen hanterar sällan ärenden av enkel beskaffenhet. De allra flesta förundersökningar inleds efter beslut av åklagare vid Riksenheten för säkerhetsmål. Åklagare leder också regelmässigt förundersökningarna och fattar därmed beslut om att gå vidare eller lägga ner undersökningen. I många fall läggs förundersökningar ner på grund av att misstankar kunnat avfärdas eller att misstankarna i och för sig kvarstår men utredningsmöjligheterna har tömts ut.

Även om en förundersökning lagts ner kan det dock i många fall finnas ett mycket stort behov av att bevara uppgifterna för underrättelseändamål. Att bevisningen inte är tillräcklig för att gå vidare med förundersökningen eller att en misstänkt omfattas av diplomatisk immunitet innebär inte att underrättelseinhämtning i ärendet bör upphöra.

Vi anser att Säkerhetspolisens bedömning av hur länge personuppgifter behöver behandlas i underrättelseverksamheten inte bör påverkas av åklagarens beslut angående förundersökningen. Åklagarens bedömning i frågan om en förundersökning ska läggas ner bör inte, som nu, påverka hur länge personuppgifter får behandlas för andra ändamål än brottsutredning.

Detsamma gäller frågan om uppgifter som lett till åtal och dom. En dom påverkar givetvis ändamålet brottsutredning och lagföring, eftersom ändamålet för denna personuppgiftsbehandling i princip är uppnått. Det finns flera exempel på att åtal väckts för förberedelse till brott vilket resulterat i en frikännande dom främst för att Säkerhetspolisen agerat i ett så tidigt skede att vissa gärningsmoment varit svåra att bevisa. I dessa fall har ofta uppgifter som förekommit i förundersökningen en mycket stor betydelse för fortsatt underrättelsearbete avseende den brottsliga verksamhet som omgärdat den konkreta gärningen. Vi anser inte heller att en frikännande dom bör påverka hur länge uppgifter som behandlats för brottsutredning ska få behandlas för andra ändamål.

Säkerhetspolisen har särskilda it-system för att ta upp och upprätta anmälningar om brott. Vidare har myndigheten system där brottsanmälan registreras efter det att ett beslut om att inleda förundersökning fattats. I systemen upprättas förundersökningsprotokoll elektroniskt. Uppgifter som hanteras i systemen är uppgifter om det aktuella brottet men även uppgifter om eventuella målsägande, vittnen, skäligen misstänkta personer och andra personer som är relevanta inom ramen för en brottsutredning. Det faller sig naturligt att de personuppgifter som behandlas i dessa system behandlas för brottsutredande ändamål. Personuppgifter som registreras i dessa system får givetvis behandlas så länge förundersökning eller annan brottsutredning pågår. När ärendet avslutas får Säkerhetspolisen i enlighet med de regler som gäller i övrigt besluta om hur länge personuppgifterna får fortsätta att behandlas för det brottsutredande ändamålet. Det finns likt i dag skäl att fortsätta att behandla uppgifter i nedlagda förundersökningar under en tid. Hur länge avslutade utredningar ska behandlas bör beslutas av Säkerhetspolisen med beaktande av bland annat behovs- och proportionali-

tetsprincipen. Vägledning finns i detta avseende i Europarådets rekommendation för personuppgiftsbehandling inom polissektorn.[145]

Att uppgifter raderas ur de system som används för brottsutredning bör inte påverka behandlingstiden för uppgifterna i andra system, exempelvis system för underrättelseverksamhet. Vi föreslår därför att denna särreglering tas bort.

8.19 Enskildas rättigheter

8.19.1 Det bör vara förbjudet med automatiserat beslutsfattande som påtagligt påverkar den enskilde

Förslag: Personuppgifter ska inte få användas för att fatta automatiserade beslut med betydande påverkan för en person.

Dataskyddskonventionens bestämmelser

Article 9 – Rights of the data subject

1 Every individual shall have a right:

a. not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration;

2. Paragraph 1.a shall not apply if the decision is authorised by a law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests.

Dataskyddskonventionens bestämmelse om automatiserat beslutsfattande innebär en rätt för enskilda att på ett meningsfullt sätt påverka och ifrågasätta automatiserade beslut. Denna rätt avser i första hand en möjlighet att visa på felaktigheter avseende de personuppgifter som använts som underlag för beslutet eller på omständigheter som gör att den profil som tillämpats inte är relevant i det enskilda fallet.

I kommentaren framhålls att rätten att kunna påverka automatiserade beslut är särskilt viktigt då enskilda kan stigmatiseras, exem-

[145] Se principle 7 i, *Recommendation no. R (87) 15 of the committee of ministers to member states regulating the use of personal data in the police sector*.

pelvis genom tillämpning av algoritmiska resonemang som leder till att en rättighet begränsas eller att en social förmån nekas.[146] Ett automatiserat beslutsfattande som inte tar hänsyn till den enskildas rätt i detta avseende är endast tillåtet om det föreskrivs i lag, som måste innehålla tillräckliga skyddsmekanismer för den registrerades frioch rättigheter.

Vilket slags automatiserat beslutsfattande omfattas av artikeln?

Liknande regler om automatiserat beslutsfattande finns även i brottsdatadirektivet. Av artikel 11 i direktivet följer bland annat att det utan stöd i författning är förbjudet att fatta beslut som enbart grundas på automatiserad behandling om de har negativa rättsverkningar eller i betydande grad påverkar den registrerade. I förarbetena till brottsdatalagen förklaras att automatiserade beslut är sådana beslut som inte fattas av någon tjänsteman, utan som blir den automatiska följden av till exempel att en viss handling ges in eller inte inkommer inom viss tid.[147]

Av konventionstexten framgår att de särskilda bestämmelserna endast avser beslut som har *betydande påverkan* (”significantly affecting”) för honom eller henne. Med betydande påverkan avses, enligt kommentarens exemplifiering, beslut från myndigheter som har en rättsverkan.

Det bör vara förbjudet med automatiserat beslutsfattande som påverkar den enskilde på ett betydande sätt

Automatiserade beslut förekommer i viss utsträckning inom den svenska förvaltningen, men det rör sig främst om beslut i skattefrågor och i frågor som regleras i socialförsäkringsbalken. Regeringen förklarade i samband med att brottsdatalagen beslutades att det inte kunde uteslutas att automatiserat beslutsfattande även skulle kunna börja tillämpas inom brottsdatalagens tillämpningsområde och såg därför skäl att införa en sådan möjlighet enligt de regler som direktivet ställer upp.[148]

[146] *Explanatory Report – CETS 223 – Automatic Processing of Personal Data (Amending Protocol)*, p. 75.
[147] Prop. 2017/18:232 s. 168.
[148] Ibid. s. 168.

Möjligheterna till automatiserat beslutsfattande får anses vara på väg att förändras i samband med utvecklingen av AI. Det finns också höga ambitioner om att införa denna teknik i olika delar av den offentliga förvaltningen.[149]

Det fattas en rad beslut inom Säkerhetspolisens verksamhet med betydande påverkan för den enskilde, både grundade på polisiära befogenheter och på särskild lagstiftning. En betydande påverkan kan uppkomma exempelvis genom beslut om ett hemligt tvångsmedel, ett beslut om att inleda eller lägga ned en förundersökning, ett beslut om att vidta en åtgärd enligt lag om särskild utlänningskontroll eller ett tillsynsbeslut inom ramen för Säkerhetspolisens uppdrag enligt säkerhetsskyddslagen.

Säkerhetspolisen kan ha möjlighet att effektivisera sin verksamhet genom att införa olika former av automatiserat beslutsfattande. Myndigheten har dock förklarat att den inte ser något behov av detta i dagsläget. Det är också en väsentlig skillnad mellan automatiserat beslutsfattande som rör frågor som är mycket välreglerade och frågor som i stor utsträckning rör bedömningar och värderingar. Inom Säkerhetspolisens brottsbekämpande verksamhet framstår det därför som relativt avlägset med helt automatiserat beslutsfattande.

Vår uppfattning är att frågan om vilken roll automatiserat beslutsfattande ska spela inom Säkerhetspolisens verksamhet är svår att besvara i dagsläget och inte heller bör besvaras av denna utredning. Dataskyddskonventionens krav för att tillåta automatiserat beslutsfattande är knappast möjliga att upprätthålla inom Säkerhetspolisens brottsbekämpande verksamhet, där det framstår som främmande att ge den enskilde en möjlighet att påverka beslutet. Att undanta konventionens skyddsbestämmelse är svårmotiverat då det inte framförts något konkret verksamhetsbehov i dagsläget. Eftersom konventionen ställer upp vissa krav, går det inte heller att lämna frågan helt oreglerad.

Vår uppfattning är att införandet av automatiserat beslutsfattande som direkt kan påverka enskilda, inom en så känslig verksamhet som Säkerhetspolisen, måste föregås av noggranna överväganden och vara motiverat av konkreta behov. Vi föreslår därför på nuvarande underlag att Säkerhetspolisen ska förbjudas att fatta

[149] Se exempelvis AI-kommissionens, *Färdplan för Sverige*, s. 15 och Myndigheten för digital förvaltning, *AI för offentlig förvaltning*, www.digg.se/ai.

helt automatiska beslut inom lagens tillämpningsområde. Ett förbud mot automatiskt beslutsfattande bör även vara begränsat på det sätt som följer av konventionen, vilket innebär att det endast är beslut med betydande påverkan som bör omfattas.

Av konventionens bestämmelse följer dock att det endast är själva beslutsfattandet som avses, inte olika handläggningsåtgärder eller beredning av ett ärende. Det innebär att artikeln inte sätter upp hinder mot helt *automatiserade beslutsstöd*. Vi ser inte heller någon anledning till att införa några särskilda begränsningar för de automatiserade processer som sker inför ett beslut eller som ingår som ett led i handläggningen. Avgörande är att sådana automatiska processer inte ensamt är utslagsgivande för ett beslut. Det måste finnas ett reellt utrymme för den mänskliga beslutsfattaren att göra egna bedömningar och avvägningar utifrån ett samlat material.

8.19.2 Rätten till allmän information bör inte följa av lag

Bedömning: Det finns inte skäl att i lag föreskriva om att Säkerhetspolisen ska offentliggöra viss allmänna information om personuppgiftsbehandling.

Dataskyddskonventionens bestämmelser

Article 8 – Transparency of processing.

1 Each Party shall provide that the controller informs the data subjects of:

a. his or her identity and habitual residence or establishment;

b. the legal basis and the purposes of the intended processing;

c. the categories of personal data processed;

d. the recipients or categories of recipients of the personal data, if any; and

e. the means of exercising the rights set out in Article 9,

as well as any necessary additional information in order to ensure fair and transparent processing of the personal data.

2. Paragraph 1 shall not apply where the data subject already has the relevant information.

> 3. Where the personal data are not collected from the data subjects, the controller shall not be required to provide such information where the processing is expressly prescribed by law or this proves to be impossible or involves disproportionate efforts.

Artikel 8 i dataskyddskonventionen innehåller bestämmelser som syftar till att uppnå transparens för personuppgiftsbehandling. Transparensen syftar till att göra det möjligt för de registrerade att förstå och därmed utöva sina rättigheter i samband med personuppgiftsbehandling. Den information som ska lämnas enligt artikel 8.1 ska vara lättförståelig och lämnas antingen direkt till de som registreras eller vara allmänt tillgänglig via en webbsida eller liknande.

Av artikel 8.3 framgår att skyldigheten inte är tillämplig vid indirekt insamling av uppgifter, under förutsättning att insamlingen sker med stöd av lag, om det inte är möjligt eller skulle vara oproportionerligt betungande. Av kommentaren till artikeln framgår att undantaget bland annat åsyftar behandling i samband med brottsutredningar.[150]

Skyldigheten att lämna viss allmän information bör inte vara lagreglerad

Den nuvarande allmänna informationsplikten följer av 6 kap. 1 § säpodatalagen. Där framgår att Säkerhetspolisen bland annat ska lämna information om myndighetens identitet, dataskyddsombudets kontaktuppgifter och för vilka kategorier av ändamål personuppgiftsbehandling får ske. Vidare ska myndigheten lämna uppgifter om enskildas rätt till information, rättelse, och radering (eller begränsning). Det gjordes i samband med säpodatalagen inga närmare överväganden om skälet bakom att införa den allmänna informationsskyldigheten i lag. Det hänvisades i stället till att motsvarande informationsplikt gäller enligt brottsdatalagen. Regeringen konstaterade att det av brottsdatadirektivet även följer en skyldighet att lämna information om möjligheten att lämna in klagomål till tillsynsmyndigheten men att detta inte behövs för Säkerhetspolisens del.[151] Varken i förarbetena till säpodatalagen eller till brottsdata-

[150] *Explanatory Report – CETS 223 – Automatic Processing of Personal Data (Amending Protocol)*, p. 67–70.
[151] Prop. 2018/19:163 s. 154 f.

lagen görs några överväganden om huruvida skyldigheten att lämna information bör följa av lag.[152]

Vi anser att den nuvarande regleringen kan ifrågasättas av flera skäl. För det första får transparenskravet för personuppgiftsbehandling anses uppfyllt genom lagstiftningen. Av lagen ska det vara möjligt att utläsa den rättsliga grunden, för vilka ändamål personuppgifter får behandlas (8.1 b), vilka kategorier av personuppgifter som får behandlas (8.1 c), vilka överföringar som får ske (8.1 d) och hur enskilda kan utöva sina rättigheter (8.1 e). Att myndigheten ska göra sin identitet och säte känt för allmänheten följer av andra bestämmelser (8.1 a).

Konventionsbestämmelsen om transparens kan antas ha till huvudsakligt ändamål att reglera privata subjekt. För myndigheter framgår motsvarande information ofta direkt av författning. Särskilt för Säkerhetspolisens verksamhet, som till stora delar omfattas av sekretess, är det svårt att på något meningsfullt sätt närmare förklara lagstiftningens praktiska tillämpning. Däremot kan det fylla en funktion att myndigheten är skyldig att hänvisa till de bestämmelser som reglerar personuppgiftsbehandlingen och då särskilt till de bestämmelser som avser enskildas rättigheter.

För det andra framstår skyldigheten att informera om vissa aspekter av verksamheten inte lämpad för lagreglering. Reglering av en myndighets skyldighet att informera om sin verksamhet utgör ett område som faller inom regeringens så kallade restkompetens enligt 8 kap. 7 § regeringsformen. Av säpodatalagens förarbeten framgår även att den närmare utformningen av informationen kan regleras i förordning. Av 5 kap. 1 § säpodataförordningen följer att informationen ska vara lättillgänglig, lättbegriplig och lämnas i lämplig form. För oss framstår det som att informationsskyldigheten lämpligen bör kunna regleras genom bestämmelser i förordning i sin helhet och inte tynga ned lagstiftningen.

8.19.3 Rätten till registerutdrag bör finnas kvar

Bedömning: Enskildas möjlighet till insyn i Säkerhetspolisens personuppgiftsbehandling bör vara mer begränsad än vad som är motiverat för andra myndigheter.

[152] Jfr prop. 2017/18:232 s. 223 ff.

Förslag: På begäran av en enskild ska Säkerhetspolisen lämna skriftligt besked om personuppgifter som rör honom eller henne behandlas. Om sådana uppgifter behandlas, ska sökanden få följande skriftliga information:

1. vilka personuppgifter om sökanden som behandlas,
2. varifrån personuppgifterna kommer,
3. den rättsliga grunden och ändamålen med behandlingen,
4. mottagare eller kategorier av mottagare av personuppgifterna och
5. hur länge personuppgifterna får behandlas.

Uppgifter som den sökanden inte redan tagit del av ska lämnas utan kostnad en gång per år.

Dataskyddskonventionens bestämmelser

> 9.1 Every individual shall have a right:
>
> b. to obtain, on request, at reasonable intervals and without excessive delay or expense, confirmation of the processing of personal data relating to him or her, the communication in an intelligible form of the data processed, all available information on their origin, on the preservation period as well as any other information that the controller is required to provide in order to ensure the transparency of processing in accordance with Article 8, paragraph 1;
>
> c. to obtain, on request, knowledge of the reasoning underlying data processing where the results of such processing are applied to him or her;

Artikel 9.1 b innehåller de rättigheter som enskilda har att begära information om hur de egna personuppgifterna behandlas. Av artikel 9.1 c följer att enskilda även ska ha rätt att få information om varför en viss behandling gett ett visst resultat. Med det avses enligt kommentaren till konventionen kunskaper som rör profilering genom användande av algoritmer och logiken bakom automatiserat beslutsfattande.[153]

[153] *Explanatory Report – CETS 223 – Automatic Processing of Personal Data (Amending Protocol)*, p. 76–77.

Rätten till registerutdrag bör finnas kvar

Rätten till personrelaterad information om personuppgiftsbehandling regleras i nuvarande 6 kap. 2 § säpodatalagen. Bestämmelsen är utformad med brottsdatalagen som förebild. Reglerna innebär att enskilda har en rätt att vända sig till myndigheten med en fråga om personuppgifter behandlas och om så är fallet få ta del av dem genom ett så kallat registerutdrag. Av nuvarande bestämmelse följer att Säkerhetspolisen ska lämna information om vilka personuppgifter som behandlas, varifrån personuppgifterna kommer, den rättsliga grunden för behandlingen, ändamålen med behandlingen, mottagare eller kategorier av mottagare av personuppgifterna, hur länge personuppgifterna får behandlas och rätten att begära rättelse och radering.

I förarbetena till säpodatalagen framhöll regeringen att en del i personuppgiftsskyddet utgörs av enskildas rätt att få veta hur deras personuppgifter behandlas. Information om den personuppgiftsbehandling som pågår är en förutsättning för att enskilda ska kunna kontrollera om behandlingen är författningsenlig och i övrigt kunna bevaka sina intressen. Regeringen ansåg att det i princip kunde ställas samma krav på Säkerhetspolisen som på andra myndigheter när det gäller enskildas rättigheter. Skälet var att det på så sätt ansågs bli lättare för den enskilde att ta tillvara sina rättigheter. Mot den bakgrunden överfördes huvuddelen av bestämmelserna i brottsdatalagen som reglerar enskildas rättigheter till säpodatalagen.[154]

Rätten till information om personuppgiftsbehandling utgör inte en rätt att ta del av de handlingar där uppgifterna förekommer. Reglerna om personuppgiftsbehandling, och den rätt till information som skapas genom dem, utgör bara en mindre del av den samlade rätten till information. Rätten att ta del av allmänna handlingar med stöd av 2 kap. 1 § tryckfrihetsförordningen utgör den huvudsakliga möjligheten till insyn i myndigheters verksamhet. Till skillnad mot rätten till registerutdrag kan var och en utnyttja rätten att ta del av en allmän handling, det vill säga även den som inte är berörd, som en journalist.

Rätten till registerutdrag får sägas ha en betydligt mindre roll för enskilda i Säkerhetspolisens verksamhet än för många andra myndigheter eller privata subjekt som omfattas av en motsvarande

[154] Prop. 2018/19:163 s. 153 f.

eller liknande reglering. Det är nämligen möjligt att begränsa denna rätt med hänsyn till sekretess. Eftersom det i princip råder sekretess för frågan om en persons personuppgifter förekommer eller inte hos Säkerhetspolisen, finns det i praktiken mycket begränsade möjligheter till direkt insyn, i vart fall inom underrättelseverksamheten.[155]

Det finns emellertid andra uppgifter än sådana som rör underrättelseverksamhet där det kan vara meningsfullt att begära ett registerutdrag. Det kan exempelvis gälla uppgifter om personer som är föremål för registerkontroller enligt säkerhetsskyddslagstiftningen. Det framstår därför inte som nödvändigt och proportionerligt att helt frånta enskilda rätten till registerutdrag.

Vi anser att den principiella rätten till registerutdrag i huvudsak kan överföras till den nya lagstiftningen. Enligt 6 kap. 9 § säpodatalagen, som är förenlig med dataskyddskonventionens bestämmelser i detta avseende, ska registerutdrag lämnas kostnadsfritt en gång per år. Det bör framgå av förordning hur avgiften ska bestämmas.

Någon rätt för enskilda att ta del av underlaget bakom automatiska processer bör inte införas

Dataskyddskonventionens bestämmelse avseende rätten till information om varför en viss behandling gett ett visst resultat har till syfte för enskilda att kunna ifrågasätta bland annat profilering och automatiserat beslutsfattande. I avsnitt 8.19.1 har vi kommit fram till att automatiserat beslutsfattande som medför en betydande påverkan för enskilda inte ska tillåtas.

Andra automatiska behandlingsprocesser bör inte omfattas av någon rätt till enskild insyn. Om Säkerhetspolisens skulle använda sig av profilering med stöd av olika algoritmer eller andra automatiska processer, skulle det röra sig om tekniska förmågor som inte bör vara möjliga för enskilda att kartlägga. Det gäller oavsett om det rör sig om sådana processer i underrättelseverksamhet eller i andra delar av verksamheten, eftersom myndighetens allmänna tekniska förmåga då kan bedömas.

Konventionens bestämmelse får förmodas ha som främsta ändamål att ge enskilda en rätt till insyn i automatiserat beslutsfattande

[155] Jfr RÅ 2000 ref. 15.

av olika slag, exempelvis genom kreditvärdighetskontroller och liknande. Automatiskt beslutsfattande är enligt vårt förslag inte tillåtet för Säkerhetspolisen. När det gäller Säkerhetspolisens verksamhet som omfattas av den föreslagna lagen finns starka skäl som talar för en begränsning av rättigheten. Det står för oss klart att det är nödvändigt och proportionerligt i ett demokratiskt samhälle att helt begränsa enskildas rätt till insyn i Säkerhetspolisens tekniska system. Vi föreslår därför att dataskyddskonventionens rättighet i detta avseende inte ska gälla för den verksamhet som omfattas av den föreslagna lagen.

8.19.4 Regleringen av Säkerhetspolisens möjlighet att begränsa enskildas rätt till information ska förenklas

Bedömning: Den nuvarande regleringen av Säkerhetspolisens möjlighet att begränsa rätten till information är onödigt komplex. Det är tillräckligt att ge myndigheten rätt att begränsa information på grund av sekretess eller annan omständighet som följer av lag.

Förslag: Rätten till information gäller inte i den utsträckning det är särskilt föreskrivet i lag eller annan författning eller annars framgår av beslut som har meddelats med stöd av författning att uppgifter inte får lämnas ut till den registrerade. Säkerhetspolisen ska inte vara skyldig att lämna ut skälen för ett beslut att avslå en ansökan om information.

Enligt nuvarande regelverk får Säkerhetspolisen, enligt 6 kap. 3 § säpodatalagen, avslå begäran om att ta del av registerutdrag om det är särskilt föreskrivet eller annars följer av beslut som meddelats med stöd av författning. Med det avses i första hand sekretess enligt 18 kap. offentlighets- och sekretesslagen eller ett förbehåll som utländsk myndighet uppställt i samband med att information överförts till Säkerhetspolisen.

Vidare får en ansökan, enligt 6 kap. 5 §, avslås om den är uppenbart ogrundad. Av 6 kap. 4 § framgår vidare att rätten till registerutdrag inte omfattar personuppgifter i löptext som inte färdigställts eller som förekommer i minnesanteckningar. Det sistnämnda undan-

taget gäller dock inte om uppgifterna lämnats ut till annan, behandlas enbart för vetenskapliga, statistiska eller historiska ändamål eller har behandlats längre tid än ett år.

Med hänsyn till att rätten till registerutdrag i praktiken främst begränsas av underrättelsesekretess framstår regleringen i nuvarande lagstiftning som onödigt tung. Undantaget för konceptanteckningar och liknande är tillkomna efter modell från 2 kap. 12 § tryckfrihetsförordningen men har knappast någon praktisk betydelse inom Säkerhetspolisens verksamhet.

Av 6 kap. 3 § andra stycket säpodatalagen framgår att Säkerhetspolisen inte är skyldig att lämna ut skälen för beslut om att begränsa rätten till ett registerutdrag. Ett avslag på en förfrågan om information från en person vars uppgifter behandlas i Säkerhetspolisens underrättelseverksamhet, men där sekretess hindrar att information lämnas, förses regelmässigt med samma motivering som om personen inte alls hade förekommit. Personuppgiftslagstiftningen ska givetvis inte möjliggöra för en person att få reda på om den står under Säkerhetspolisens uppsikt genom att det i beslutsmotiveringen skulle framgå om personen är registrerad eller inte. Detta är sedan länge fastslaget genom praxis men det finns skäl att det, i likhet med den nuvarande ordningen, även ska framgå direkt av lagen.

Vi anser att det nuvarande regelverket bör renodlas på så sätt att rätten att neka enskild information ska begränsas till de fall då uppgifterna omfattas av sekretess eller av annan anledning inte får lämnas ut. I övrigt fyller de nuvarande reglerna inte någon funktion som motiverar att de överförs till den nya lagstiftningen.

Enskildas rätt till insyn i Säkerhetspolisen är på grund av sekretess kraftigt beskuren i jämförelse till många andra verksamheter. Det är en naturlig följd av myndighetens uppdrag och utgör ett undantag från datakonventionens bestämmelser. För oss råder det ingen tvekan om att undantagen är välmotiverade och proportionerliga. Undantagen kompenseras även av rätten till indirekt insyn, genom Säkerhets- och integritetsskyddsnämndens kontrollåtgärder på begäran av enskild. Om Säkerhetspolisen inte kan lämna ut ett begärt registerutdrag, bör myndigheten därför upplysa sökanden om den rätt till kontroll som följer av 3 § lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet.

8.19.5 Det bör inte finnas en särskild möjlighet att motsätta sig personuppgiftsbehandling eller begära rättelse eller radering

Bedömning: Enskilda bör inte ha rätt att motsätta sig personuppgiftsbehandling eller begära rättelse eller radering av uppgifter som behandlas av Säkerhetspolisen.

Dataskyddskonventionens bestämmelser

Article 9 – Rights of the data subject

1 Every individual shall have a right:

d. to object at any time, on grounds relating to his or her situation, to the processing of personal data concerning him or her unless the controller demonstrates legitimate grounds for the processing which override his or her interests or rights and fundamental freedoms;

e. to obtain, on request, free of charge and without excessive delay, rectification or erasure, as the case may be, of such data if these are being, or have been, processed contrary to the provisions of this Convention;

Av artikel 9.1 d framgår dels en rätt att motsätta sig personuppgiftsbehandling, dels de undantag från denna rätt som kan följa av en rättslig grund som väger tyngre.

Enligt kommentaren till konventionen kan personuppgiftsbehandling som rör allmän säkerhet vara motiverad även när den enskilde motsätter sig detta. Behandling som följer av lag och som syftar till att bekämpa brott kan ifrågasättas inom ramen för brottmålsprocessen. I dessa fall är det inte nödvändigt att ge en självständig möjlighet till rättelse eller radering av personuppgifter grundad endast på personuppgiftsbehandlingen.[156]

Av artikel 9.1 e framgår att enskilda kan begära rättelse eller radering av personuppgifter som behandlats i strid med någon av konventionens bestämmelser.

[156] *Explanatory Report – CETS 223 – Automatic Processing of Personal Data (Amending Protocol)*, p. 78 och 80.

Det finns inte skäl att ge enskilda en självständig rätt till rättelse eller radering

Nuvarande lagstiftning innehåller en rad bestämmelser som rör enskildas rätt till att få till stånd rättelse, komplettering och radering av personuppgifter. Av 6 kap. 7 § säpodatalagen framgår att Säkerhetspolisen på begäran av den registrerade utan onödigt dröjsmål ska rätta eller komplettera personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålet med behandlingen. Av nästföljande paragraf följer en skyldighet att på begäran av den registrerade utan onödigt dröjsmål radera personuppgifter som behandlats i strid med vissa uppräknade, grundläggande bestämmelser i lagen. Säpodatalagens bestämmelser i dessa avseenden följer motsvarande reglering i brottsdatalagen.

Det relativt omfattande regelkomplexet som på ett ingående sätt beskriver enskildas rättigheter har, såvitt känt, aldrig tillämpats. För att en enskild på ett meningsfullt sätt ska kunna utnyttja sin rätt till rättelse av en felaktig uppgift eller radering av en uppgift som behandlats felaktigt krävs en ingående kunskap om vilka personuppgifter som behandlats och på vilket sätt. Som framgått av föregående avsnitt 8.19.4 råder det i normalfallet en sträng sekretess i förhållande till den registrerade om just sådana förhållanden.

Reglerna om enskildas rätt till rättelse, komplettering och radering återger alltså inte en reell rättighet. Vi anser att den faktiska tillämpningen som är avsedd också bör återspeglas i lagstiftningen, för att undvika att ge medborgarna en felaktig uppfattning om sina rättigheter i förhållande till myndigheten. För det fall personuppgifter behandlas för ett ändamål som inte innebär att de omfattas av sekretess i förhållande till den registrerade och den enskilde påtalar ett förhållande som medför att personuppgifter bör rättas m.m. följer denna skyldighet redan av lagens allmänna bestämmelser. Dataskyddskonventionens krav på att det ska finnas en rätt att motsätta sig personuppgiftsbehandling och till rättelse och radering kan vara viktiga i förhållande till exempelvis privata bolag. Säkerhetspolisens personuppgiftsbehandling står dock under tillsyn av fyra, av varandra oberoende, organ till vilka enskilda kan rikta sina klagomål.

Vid sidan av att det inte framstår som helt transparent att lagfästa en rättighet som är mycket svår att utnyttja innebär den nuva-

rande möjligheten en administrativ börda för myndigheten. Eftersom den nuvarande bestämmelsen inte endast utgör en rätt utan även innehåller ett skyndsamhetskrav, kan ett fåtal individer genom upprepade och omfattande ansökningar orsaka betydande merarbete för myndigheten.

Ett undantag från en rättighet, vars huvudsakliga syfte inte är att reglera behandling inom brottsbekämpande verksamhet, framstår som ett välmotiverat undantag från dataskyddskonventionen. Att begränsa enskildas rätt att med egna rättsmedel påverka hur Säkerhetspolisen behandlar personuppgifter, framstår som både nödvändigt och proportionerligt i ett demokratiskt samhälle eftersom det handlar om brottsbekämpande verksamhet som avser nationell säkerhet.

Denna begränsning kompenseras genom rätten till indirekt insyn. Att en enskild har möjlighet att vända sig till Säkerhets- och integritetsskyddsnämnden för att begära kontroll av hur Säkerhetspolisen behandlar dennes personuppgifter är motiverat bland annat av att enskilda har små faktiska möjligheter att själv ifrågasätta behandlingen.

8.19.6 Det ska finnas möjlighet till skadestånd

Förslag: Det finns inte skäl att ändra den nuvarande bestämmelsen om rätt till ersättning för den skada och kränkning av den personliga integriteten som orsakats av att personuppgifter behandlas i strid med lagen. Motsvarande regler ska därför föras över till den nya lagen.

Dataskyddskonventionens bestämmelser

Article 9 – Rights of the data subject

1 Every individual shall have a right:

f. to have a remedy under Article 12 where his or her rights under this Convention have been violated;

g. to benefit, whatever his or her nationality or residence, from the assistance of a supervisory authority within the meaning of Article 15, in exercising his or her rights under this Convention.

> 12 Each Party undertakes to establish appropriate judicial and non-judicial sanctions and remedies for violations of the provisions of this Convention.

Av artikel 9.1 f och 12 framgår att enskilda ska ha tillgång till rättsmedel då deras rättigheter enligt konventionen kränkts. Vilken form av rättsmedel som ska finnas är upp till konventionsstaten men det ska ge enskilda möjlighet att rättslig ifrågasätta beslut eller praxis som rör personuppgiftsbehandling. En sådan möjlighet är rätten till ekonomisk kompensation för materiella och ideella skador som orsakats av behandlingen.[157]

Av artikel 9.1 g följer att enskilda ska ha rätt till bistånd från en tillsynsmyndighet. I kommentaren till artikeln framgår att hjälpen med att få sina rättigheter tillgodosedda ska ske genom en anmälan som innehåller tillräcklig information för att identifiera den ifrågasatta personuppgiftsbehandlingen. När detta inte är möjligt, exempelvis på grund av en begränsad rätt till insyn, kan det behöva göras anpassningar för att tillgodose enskildas rätt till bistånd.[158]

Det finns inte några skäl att ändra de nuvarande reglerna om skadestånd

Enligt nuvarande lagstiftning ska den personuppgiftsansvarige ersätta den registrerade för den skada och den kränkning av den personliga integriteten som orsakats av personuppgiftsbehandling som skett i strid med säpodatalagen eller föreskrifter som meddelats i anslutning till den. Bestämmelsen är utförligt motiverad i förarbetena både till den likalydande bestämmelsen i brottsdatalagen och till säpodatalagen.[159]

Rätten till skadestånd utgör ett viktigt rättsmedel för enskilda och fyller både ett kompensatoriskt och ett preventivt syfte. Ideellt skadestånd är en sedan länge etablerad princip för att kompensera kränkningar av fri- och rättigheter enligt Europakonventionen och utgör ett sådant rättsmedel för enskild som avses i dataskyddskonventionens artikel 9.1 f. Det framstår därför som både lämpligt och

[157] *Explanatory Report – CETS 223 – Automatic Processing of Personal Data (Amending Protocol)*, p. 100.
[158] Ibid. p. 57.
[159] Prop. 2017/18:232 s. 339–344 och prop. 2018/19:163 s. 184–187.

nödvändigt att det finns en rätt som motsvarar dagens bestämmelse. Vi ser inga skäl att ändra gällande rätt i detta avseende.

Under remissbehandlingen av säpodatalagen framfördes att de praktiska möjligheterna till skadestånd var små. Av artikel 9.1 g i dataskyddskonventionen 108+ framgår att tillsynsmyndigheten ska bistå enskilda med att utöva sina rättigheter enligt konventionen. I detta sammanhang kan det finnas anledning att lyfta fram Säkerhets- och integritetsskyddsnämndens skyldighet att, enligt 20 § i förordningen (2007:1141) med instruktion för Säkerhets- och integritetsskyddsnämnden, anmäla vissa förhållanden till andra myndigheter. Om nämnden vid tillsyn över Säkerhetspolisens personuppgiftsbehandling uppmärksammar felaktigheter som kan medföra skadeståndsansvar för staten, får nämnden anmäla det till Justitiekanslern. Om motsvarande felaktighet uppmärksammas vid en kontroll som görs på begäran av enskild är nämnden skyldig att göra en sådan anmälan. Enligt 11 § förordning (1975:1345) med instruktion för Justitiekanslern ska Justitiekanslern pröva anmälningar från Säkerhets- och integritetsskyddsnämnden om felaktigheter som kan medföra skadeståndsansvar för staten. Om Justitiekanslern finner att det som har förekommit kan föranleda skadeståndsansvar för staten, ska Justitiekanslern bereda den som berörs tillfälle att framställa sådant anspråk.

Det strikta skadeståndsansvaret som följer av nuvarande lagstiftning innebär att enskilda kan kompenseras vid felaktig personuppgiftsbehandling så snart en skada eller kränkning kan påvisas. Rättsmedlet får därför anses vara tillgängligt, och genom de möjligheter som finns till indirekt insyn, också effektivt.

8.19.7 Överklagande av information om personuppgiftsbehandling och avgift bör prövas i samma ordning som utlämnande av allmän handling

Förslag: Säkerhetspolisens beslut att inte lämna ut information om personuppgiftsbehandling eller om att ta ut avgift för sådan information ska överklagas till kammarrätt. Övriga beslut av Säkerhetspolisen ska inte kunna överklagas.

Den nuvarande ordningen

Enligt 8 kap. 2 § säpodatalagen får Säkerhetspolisens beslut i fråga om rättelse, komplettering, radering eller begränsning av personuppgifter på enskilds begäran överklagas till allmän förvaltningsdomstol, det vill säga förvaltningsrätt. Detsamma gäller beslut att inte lämna information om personuppgiftsbehandling (registerutdrag) eller att ta ut avgift för sådan information. Enligt 6 kap. 8 § offentlighets- och sekretesslagen överklagas Säkerhetspolisens beslut om att inte lämna ut en allmän handling till kammarrätt.

I förarbetena till brottsdatalagen, vars bestämmelser överförts till säpodatalagen, förs ett relativt ingående resonemang angående skillnaden mellan att lämna ut ett registerutdrag och en allmän handling. Regeringen konstaterar att de i sig mycket komplexa regelverken om tillgång till handlingar och begränsningen av rätten att ta del av dem har ett annat fokus än lagstiftningen om personuppgiftsbehandling. Rätten till personrelaterad information ger enligt regeringen inte den registrerade någon rätt att få del av annat än information om just behandlingen av personuppgifterna. Det innebär att det inte ska prövas om den registrerades personuppgifter finns i en allmän handling och i så fall i vilken omfattning handlingen kan lämnas ut. I stället ska det prövas om det förhållandet att personuppgifter behandlas i ett visst sammanhang, exempelvis i underrättelseverksamhet, kan avslöjas för den registrerade. Regeringen konstaterade att det förhållandet att det avslöjas att personuppgifterna behandlas i ett enskilt fall kan riskera att hindra underrättelseverksamheten och att informationen då bör kunna begränsas. Regeringens uppfattning var att en sådan prövning inte kräver lika ingående överväganden som en prövning enligt offentlighets- och sekretesslagen. Om det ändå görs en formell sekretessprövning och myndigheten beslutar att inte lämna information, ska beslutet dock överklagas enligt de särskilda reglerna i offentlighets- och sekretesslagen, det vill säga till kammarrätten.[160]

[160] Se prop. 2017/18 :232 s. 238 f. med hänvisning till HFD 2014 ref. 55.

Överklaganden av beslut om att inte lämna ut information och beslut om att inte lämna ut allmän handling bör överklagas i samma ordning

Som tidigare nämnts omfattas uppgiften om en persons personuppgifter behandlas av Säkerhetspolisen i normalfallet av underrättelsesekretess enligt 18 kap. 2 § offentlighets- och sekretesslagen.[161] En ansökan om ett så kallat registerutdrag, innefattande uppgifter som behandlas i underrättelseverksamheten, besvaras därför i de allra flesta fall genom en sekretessprövning. Det innebär att sakfrågan i normalfallet överklagas till Kammarrätten i Stockholm precis på samma sätt som ett beslut som avser utlämnande av allmän handling.[162] I undantagsfall kan ett ärende komma under förvaltningsrättens prövning, om avslag sker på någon formell grund, om begäran är orimlig eller uppenbart ogrundad eller om det skulle avse en avgift.

I många fall ansöker enskilda om flera olika rättsföljder i samma ärende, exempelvis om att både få del av alla handlingar som rör honom eller henne och att få del av ett registerutdrag. I dessa fall framstår det som mindre lämpligt att beslut fullföljs till olika instanser.

Det som prövas genom ett överklagande av beslut som rör både rätten till information och rätten att ta del av allmän handling är normalt känsliga uppgifter. Den instans som prövar frågan kommer exempelvis att kunna få tillgång till den sekretessbelagda uppgiften om personens uppgifter behandlas, vilket kan avslöja Säkerhetspolisens underrättelseförmåga. Uppgifterna i sig omfattas i normalfallet av sekretess. På en aggregerad nivå, då flera uppgifter kan läggas samman, kan det dock även handla om säkerhetsskyddsklassificerad information i säkerhetsskyddsklass hemligt, eller till och med kvalificerat hemlig.

Det innebär att den domstol som ska hantera uppgifterna behöver ha ett väl utvecklat säkerhetsskydd. Ur informationssäkerhetsperspektiv finns alltid ett mervärde i att sprida uppgifterna till så få aktörer som möjligt. Säkerhetspolisen behöver också ta fram rutiner för överlämningen av uppgifterna med flera olika aktörer utifrån deras respektive förutsättningar att ta emot och skydda uppgifterna.

[161] RÅ 2000 ref. 19.
[162] För exempel på sådan prövning, se Kammarrätten i Stockholms dom den 24 maj 2024 i mål nr 2438–24.

Det framstår som mest lämpligt att minska sårbarheten i verksamheten genom att Säkerhetspolisens beslut som rör information om personuppgiftsbehandling ska överklagas i samma ordning som utlämnande av allmän handling. Säkerhetsskyddsaspekter talar starkt för att hålla nere antalet instanser. Det talar för att överklaganden som rör personuppgiftsbehandling ska prövas i den ordning som gäller för beslut enligt offentlighet- och sekretesslagen. Det innebär att kammarrätten bör vara första instans vid prövningen av Säkerhetspolisens beslut även enligt säpodatalagen.

Övriga beslut som Säkerhetspolisen fattar med stöd av lagen bör inte kunna överklagas

I förarbetena till säpodatalagen anförs att enskildas rätt att överklaga beslut enbart bör ta sikte på sådana beslut av myndigheten som den fattat i egenskap av personuppgiftsansvarig och som direkt berör den enskilde och som gått honom eller henne emot. Andra beslut som Säkerhetspolisen fattar i egenskap av personuppgiftsansvarig, som administrativa beslut i fråga om tillgången till personuppgifter, bör däremot inte få överklagas.[163]

Vi föreslår i föregående avsnitt 8.19.5 att Säkerhetspolisen inte längre ska fatta beslut om rättelse, komplettering, radering eller begränsning på enskilds begäran. Sådana beslut ska i stället enbart fattas med stöd av Säkerhetspolisens allmänna skyldigheter att vidta åtgärder för en författningsenlig behandling. En skyldighet för Säkerhetspolisen att rätta och uppdatera uppgifter eller att avsluta behandling som inte är författningsenlig föreligger enligt denna bestämmelse oavsett hur saken kommit till myndighetens kännedom. Sådana beslut bör därför, i likhet med gällande rätt, inte få överklagas.

Det bör i sammanhanget erinras om att de registrerades rättigheter i stor utsträckning tillgodoses genom det särskilda systemet för indirekt insyn och tillsyn som sker av Säkerhets- och integritetsskyddsnämndens på begäran av enskild.

[163] Prop. 2018/19:163 s. 188.

8.20 Säkerhetspolisens skyldigheter

8.20.1 Dataskyddskonventionens krav

Article 10 – Additional obligations

1. Each Party shall provide that controllers and, where applicable, processors, take all appropriate measures to comply with the obligations of this Convention and be able to demonstrate, subject to the domestic legislation adopted in accordance with Article 11, paragraph 3, in particular to the competent supervisory authority provided for in Article 15, that the data processing under their control is in compliance with the provisions of this Convention.

2. Each Party shall provide that controllers and, where applicable, processors, examine the likely impact of intended data processing on the rights and fundamental freedoms of data subjects prior to the commencement of such processing, and shall design the data processing in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms.

3. Each Party shall provide that controllers, and, where applicable, processors, implement technical and organisational measures which take into account the implications of the right to the protection of personal data at all stages of the data processing.

4. Each Party may, having regard to the risks arising for the interests, rights and fundamental freedoms of the data subjects, adapt the application of the provisions of paragraphs 1, 2 and 3 in the law giving effect to the provisions of this Convention, according to the nature and volume of the data, the nature, scope and purpose of the processing and, where appropriate, the size of the controller or processor.

Punkten 1 i artikel 10 innebär att de skyldigheter som följer av konventionen även ska medföra ett ansvar för personuppgiftsansvariga att kunna bekräfta och visa regelefterlevnad. Den personuppgiftsansvarige ska därför kunna visa att personalen har den utbildning som krävs eller att det finns interna riktlinjer och rutiner för att exempelvis radera uppgifter från system i rätt tid.[164]

Av punkten 2 följer en skyldighet att utföra en konsekvensbedömning innan en behandling påbörjas. Konventionen ställer inte upp några formkrav för en sådan bedömning. I kommentaren framhålls att en konsekvensbedömning ska innefatta en heltäckande proportionalitetsprövning av den planerade åtgärden.[165]

[164] *Explanatory Report – CETS 223 – Automatic Processing of Personal Data (Amending Protocol)*, p. 85.
[165] Ibid. p. 88.

Punkten 3 innehåller ett krav på att de tekniska och organisatoriska åtgärder som krävs ska genomföras med hänsyn till skyddet för personuppgifter under alla steg av behandlingen. Det innebär, enligt kommentaren, bland annat att personuppgiftsskyddet ska beaktas redan då system utvecklas genom inbyggt dataskydd. Vidare framgår att principen om dataskydd som standard bör gälla.[166]

Av punkten 4 framgår att konventionsstaterna kan anpassa kraven på de personuppgiftsansvariga efter bland annat arten och volymen av de personuppgifter som behandlas, ändamålen med behandlingen och de risker som behandlingen kan medföra för de registrerades intressen och grundläggande fri- och rättigheter. Enligt kommentaren är syftet bland annat att möjliggöra undantag från vissa bestämmelser för exempelvis småföretag som inte ska behöva införa onödigt kostsamma åtgärder för harmlösa behandlingar.[167]

8.20.2 Skyldighet att vidta åtgärder för författningsenlig behandling av personuppgifter

Förslag: Säkerhetspolisen ska vidta de åtgärder som krävs för författningsenlig behandling, om det framgår att personuppgifter behandlas i strid med lag. Detsamma ska gälla om det krävs för att utföra en rättslig förpliktelse.

Nuvarande reglering

I nuvarande säpodatalag finns en generell skyldighet, enligt 2 kap. 13 och 14 §§ att rätta, uppdatera och radera personuppgifter som inte behandlas författningsenligt. Enligt 2 kap. 13 § ska alla rimliga åtgärder vidtas för att personuppgifter som med hänsyn till ändamålet med behandlingen är felaktiga eller ofullständiga utan onödigt dröjsmål rättas. Åtgärderna ska också syfta till att förhindra att sådana uppgifter lämnas ut eller görs tillgängliga. Personuppgifter som är inaktuella ska uppdateras, om det är nödvändigt. Enligt 2 kap. 14 § ska alla rimliga åtgärder vidtas för att personuppgifter

[166] Ibid. p. 89.
[167] Ibid. p. 90.

som behandlas i strid med vissa lagkrav utan onödigt dröjsmål raderas och för att förhindra att de lämnas ut eller görs tillgängliga. Detsamma gäller om radering krävs för att utföra en rättslig förpliktelse.

De båda paragraferna har sina motsvarigheter i brottsdatalagen (2 kap. 15 och 16 §§) och hade liknande, om än mindre detaljerade, motsvarigheter även i den tidigare lagstiftning som gällde för Säkerhetspolisen. Bestämmelserna är utformade efter de principer som framgår i brottsdatadirektivet men har en mer långtgående implementering i svensk rätt.

Säkerhetspolisens skyldigheter att vidta åtgärder på eget initiativ motsvaras i huvudsak av enskildas rättigheter att begära rättelse, komplettering och radering, se avsnitt 8.19.5.

Det bör finnas en skyldighet att vidta åtgärder för författningsenlig behandling

Den lag vi föreslår innehåller en mängd krav för behandlingen av personuppgifter. Det är självklart att den personuppgiftsansvarige har en skyldighet att vidta de åtgärder som krävs för att uppfylla lagens krav, då uppgifter behandlas för första gången men även under den fortsatta behandlingen.

Av artikel 10.1 i dataskyddskonventionen 108+ följer att den personuppgiftsansvarige ska vidta ändamålsenliga åtgärder för att uppfylla konventionens krav. Konventionen innehåller däremot inte någon uttömmande uppräkning av hur långt denna skyldighet sträcker sig eller med vilka medel den personuppgiftsansvarige ska uppnå detta mål.

Bestämmelsen bör införas som en självständig skyldighet för Säkerhetspolisen. Vi anser inte att det finns något skäl att, som dagens reglering är utformad, särskilt räkna upp vilka åtgärder som ska vidtas. Av bestämmelserna om personuppgifters kvalitet framgår vad som krävs i detta avseende. Om det exempelvis saknas en särskild upplysning om ändamål och ändamålet inte framgår på annat sätt, ska en sådan upplysning tillföras. Om en grundläggande förutsättning för att behandla personuppgifter saknas, måste behandlingen upphöra. Det sker normalt genom att uppgiften raderas. Både arkivrättsliga skäl och att uppgiften kan behöva finnas kvar som bevis för felaktigheten talar för att det inte ska föreskrivas något absolut raderingskrav.

Dagens regler innefattar skyldigheter enligt lag, förordning eller rättslig förpliktelse. En rättslig förpliktelse kan exempelvis utgöras av ett föreläggande eller beslut från tillsynsmyndigheten. Detta bör gälla även i den nya lagen.

Inget krav på kontinuerlig granskning av alla personuppgifter

Av många myndigheter är det rimligt att begära registervård i form av att akter och ärenden med viss regelbundenhet granskas och att felaktiga personuppgifter rättas och inaktuella uppgifter uppdateras. Frågan är om det är lämpligt att i lag föreskriva en skyldighet för Säkerhetspolisen att gå igenom de personuppgifter som behandlas för att upptäcka fel eller om det är tillräckligt att rätta felaktigheter när de framkommer.

Skyldigheten att granska uppgifter genom kontinuerlig registervård är förstås att föredra ur ett integritetsperspektiv, eftersom det säkerhetsställer en hög kvalitet på personuppgifterna och förhindrar att uppgifter behandlas felaktigt under en längre tid. Att kontinuerligt och manuellt granska samtliga personuppgifter som Säkerhetspolisen behandlar är dock mycket resurskrävande och förutsätter i praktiken en fördelning mellan operativ respektive registervårdande verksamhet som inte framstår som rimlig. Det bör därför inte ställas ett krav på att Säkerhetspolisen ska garantera att alla uppgifter uppfyller lagens alla krav vid alla tillfällen. Eftersom bland annat behov, proportionalitet och relevans kan variera över tid skulle ett sådant krav kräva att samtliga uppgifter granskades med viss regelbundenhet. Att Säkerhetspolisen är skyldig att vårda sina register genom exempelvis stickprovskontroller eller andra rutiner för registervård är en annan sak. En sådan egenkontroll omfattar verksamheten i stort och inte varje enskild uppgift.

Skyldigheten att vidta åtgärd bör i stället uppkomma då en felaktighet konstaterats. Om det t.ex. i det operativa arbetet kan konstateras att uppgifter behandlas trots att de inte längre behövs, på grund av ändrade förhållanden eller ny kunskap, ska de inte längre behandlas. Säkerhets- och integritetsskyddsnämnden kan också konstatera brister vid sin tillsyn. Även myndighetens dataskyddsombud kan upptäcka felaktigheter som behöver rättas till. Om en

enskild påtalar en felaktighet uppkommer genom bestämmelsen en skyldighet att vidta åtgärd om det finns fog för det.

Ansvaret för att personuppgifter behandlas författningsenligt är givetvis i första hand Säkerhetspolisens. Det är därför myndighetens ansvar att tillse att det finns rutiner på plats både för att förhindra och upptäcka felaktigheter. Oavsett hur felaktigheter upptäcks innebär den föreslagna bestämmelsen att de ska åtgärdas.

Av lagtexten bör det av dessa skäl framgå att Säkerhetspolisens skyldighet att agera i form av radering m.m. gäller först när det framgår att en åtgärd krävs. Det hänvisas vidare till författningskommentaren till 5 kap. 1 §.

8.20.3 Tekniska och organisatoriska åtgärder

Förslag: De nuvarande reglerna om Säkerhetspolisens skyldigheter att vidta tekniska och organisatoriska åtgärder och att begränsa tillgång till personuppgifter ska överföras oförändrade till den nya lagen.

Nuvarande reglering

Enligt 5 kap. 1 § säpodatalagen ska Säkerhetspolisen, genom lämpliga tekniska och organisatoriska åtgärder, säkerställa och kunna visa att behandlingen av personuppgifter är författningsenlig och att registrerades rättigheter skyddas. Bestämmelsen om tekniska och organisatoriska åtgärder följer av brottsdatadirektivet. Regeringen ansåg att det i detta avseende kunde ställas samma krav på Säkerhetspolisen som på övriga brottsbekämpande myndigheter, vilket motiverade en bestämmelse med samma innehåll som 3 kap. 2 § brottsdatalagen.

Det finns vidare, i 5 kap. 2 § säpodatalagen, ett krav på så kallat inbyggt dataskydd, vilket innebär att nödvändiga skyddsåtgärder ska integreras både vid behandlingen och när medlen för behandlingen bestäms. Regeringen ansåg att brottsdatadirektivets krav på att integritetsfrågor ska beaktas, från förstudie och kravställning via design och utveckling till användning och avveckling, innebär både att säkerheten i systemen kan höjas och författningsenlig och kor-

rekt behandling underlättas. En bestämmelse som var likalydande med brottsdatalagens regel togs därför in säpodatalagen.

Av 5 kap. 3 § följer att det i Säkerhetspolisens behandlingsystem som regel inte ska vara möjligt att behandla andra personuppgifter än de som är nödvändiga för varje särskilt angivet ändamål (dataskydd som standard). Dataskydd som standard innebär att arbetsflödena i ett system automatiskt ska styra användaren mot ett integritetssäkert arbetssätt och att grundinställningarna ska vara satta så att inte mer information än nödvändigt samlas in eller visas. Den personuppgiftsansvarige ska vidta lämpliga åtgärder för att i standardfallet säkerställa att så sker. Regeringen ansåg att de krav som följer av brottsdatadirektivet bör ställas även på Säkerhetspolisen i detta avseende. Regeringen påpekade dock att det inte alltid är möjligt att ange ändamålen lika tydligt och detaljerat inom underrättelseverksamheten som i annan brottsbekämpande verksamhet, vilket kan påverka hur dataskyddet som standard implementeras i Säkerhetspolisens verksamhet.[168]

I 5 kap. 4 § anges att personuppgiftsbehandling ska loggas i den utsträckning det är särskilt föreskrivet. Loggning är en säkerhetsåtgärd som innebär att behandlingshistorik sparas under en viss tid. Det är en teknisk funktion i systemet som fungerar automatiskt och som inte går att ändra eller påverka på annat sätt. Loggningen ger Säkerhetspolisen information om åtkomst och användning av system. Loggning kan därmed ge information om bland annat obehörig åtkomst eller angrepp mot systemen och är därför en mycket viktig del av myndighetens informationssäkerhetsarbete. Den ger också tillsynsmyndigheten nödvändig information för granskning i efterhand av hur personuppgifter har behandlats.

Kravet på dataskydd som standard och på loggning gäller endast det som i säpodatalagen kallas för *automatiserade behandlingssystem*. Med automatiserade behandlingssystem avses behandlingssystem som är särskilt utformade eller anpassade för verksamheten där personuppgifter behandlas mer eller mindre strukturerat. Det kan till exempel handla om verksamhetsstöd i form av dokument- och ärendehanteringssystem och olika typer av register och databaser. För att dataskydd som standard ska kunna införas i automatiserade behandlingssystem krävs det att Säkerhetspolisen har tekniska möjligheter och rätt att vidta sådana åtgärder i systemet. Standardprogram som Word,

[168] Prop. 2018/19:163 s. 135.

Outlook och Excel är inte att anse som automatiserade behandlingssystem i paragrafens mening och omfattas därför inte av kraven.[169]

De nuvarande reglerna om tekniska och organisatoriska åtgärder är välavvägda och kan överföras till den nya lagen

Säpodatalagens bestämmelser om tekniska och organisatoriska åtgärder följer i stora delar brottsdatadirektivet och är mer detaljerade och långtgående än de krav som uppställs i dataskyddskonventionen. För FRA och Försvarsmakten, vars personuppgiftslagar likt Säkerhetspolisens är fristående EU-rätten, saknas exempelvis särskilda bestämmelser om inbyggt dataskydd och dataskydd som standard.

Syftet med den lagstiftning vi föreslår är att upprätthålla ett högt skydd för personuppgifter. De nuvarande bestämmelserna fyller en viktig funktion och är redan integrerade i Säkerhetspolisens organisation. Det har inte heller framgått att dessa bestämmelser hindrar en ändamålsenlig personuppgiftsbehandling.

Det finns goda skäl för att under sådana omständigheter inte förändra en etablerad ordning. Det finns också uppenbara fördelar med att eventuella system som Säkerhetspolisen utvecklar följer en brett tillämpad dataskyddsstandard.

Vi har sammantaget inte funnit skäl att göra några ändringar avseende de nuvarande bestämmelserna i 5 kap. 1–4 §§ säpodatalagen. De bör således föras över till den nya lagen.

8.20.4 Dataskyddsombud

Förslag: De nuvarande reglerna om dataskyddsombud bör i huvudsak överföras till den nya lagen. Skyldigheten att anmäla att ett dataskyddsombud utses eller entledigas bör dock gälla i förhållande till både Integritetsskyddsmyndigheten och Säkerhets- och integritetsskyddsnämnden.

Det finns inga bestämmelser i dataskyddskonventionen som innebär en skyldighet att utse ett dataskyddsombud inom en organisation som behandlar personuppgifter. Enligt kommentaren till artikel 10.1

[169] Ibid. s. 136 f.

kan ett av flera sätt för en personuppgiftsansvarig att visa att organisationen uppfyller konventionens krav vara att utse ett eller flera personuppgiftsombud. Sådana ombud ska ha tillräckliga befogenheter att agera för att åstadkomma regelefterlevnad inom organisationen.[170]

I Sverige finns en lång historia av en ombudsfunktion i personuppgiftslagstiftningen. Genom 1998 års personuppgiftslag infördes en roll som liknar dagens dataskyddsombud, under beteckningen personuppgiftsombud. En liknande funktion (kontaktperson) återfanns emellertid redan i 1973 års datalag genom ett tillägg som trädde i kraft år 1988.[171] Kravet på att utse ett dataskyddsombud och de uppgifter som ska åligga denne följer av brottsdatadirektivet och dataskyddsförordningen. När säpodatalagen beslutades ansågs det lämpligt att ett dataskyddsombud fick samma roll och samma uppgifter som det tidigare personuppgiftsombudet.[172]

Det finns inte heller nu några skäl som talar mot att Säkerhetspolisen ska vara skyldig att inom myndigheten utse ett eller flera dataskyddsombud. Reglerna bör därför i huvudsak överföras.

Enligt nuvarande säpodatalag ska en anmälan om att ett dataskyddsombud utsetts eller entledigats göras till tillsynsmyndigheten, det vill säga Integritetsskyddsmyndigheten. Det framgår inte av förarbetena varför det endast är Integritetsskyddsmyndigheten som ska underrättas om ändrade förhållanden och därmed inte Säkerhets- och integritetsskyddsnämnden. Däremot framgår att denna anmälan är viktig, eftersom ombudet ska ha till uppgift att samarbeta med tillsynsmyndigheten och fungera som kontaktpunkt för den i vissa fall.[173] Ombudet har, enligt 5 kap. 10 § 5 säpodatalagen, särskilt ansvar att samarbeta med tillsynsmyndigheten vid förhand-samråd, men även i andra frågor som rör behandling av personuppgifter.

Eftersom Säkerhetspolisens tillämpning av säpodatalagen står under tillsyn av två, i förhållande till varandra oberoende, myndigheter framstår det som lämpligt att ändrade förhållanden ska anmälas till dem båda. Vi föreslår därför en sådan bestämmelse.

[170] *Explanatory Report – CETS 223 – Automatic Processing of Personal Data (Amending Protocol)*, p. 87.
[171] Se de ändringar i 8 § datalagen (1973:289) som beslutades genom prop. 1986/87:116.
[172] Prop. 2018/19:163 s. 146.
[173] Ibid. s. 145.

8.21 Säkerhetsåtgärder och tillgång till personuppgifter

8.21.1 Dataskyddskonventionens krav

Article 7 – Data security

1. Each Party shall provide that the controller, and, where applicable the processor, takes appropriate security measures against risks such as accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data.

2. Each Party shall provide that the controller notifies, without delay, at least the competent supervisory authority within the meaning of Article 15 of this Convention, of those data breaches which may seriously interfere with the rights and fundamental freedoms of data subjects.

Artikel 7.1 innebär att den personuppgiftsansvarige ska införa säkerhetsåtgärder för att förebygga risker som oavsiktlig eller otillåten åtkomst till eller förstöring, förlust, användning, förändring eller röjande av personuppgifter. Sådana säkerhetsåtgärder kan vara av både av teknisk och organisatorisk art. Skyddet ska anpassas efter bland annat uppgifternas art och mängd, de potentiella konsekvenserna för enskilda vid otillåten behandling och graden av sårbarhet i den tekniska struktur som används för behandlingen. Kostnaden för säkerhet bör stå i proportion till hur allvarliga och sannolika de potentiella riskerna är.[174]

Av artikel 7.2 framgår att en personuppgiftsansvarig ska vara skyldig att utan dröjsmål underrätta tillsynsmyndigheten om personuppgiftsincidenter som kan medföra betydande intrång i de registrerades fri- och rättigheter.

Skyldigheterna som följer av artikel 7.1 är absoluta, men underrättelseskyldigheten i artikel 7.2 omfattas av medlemsstaternas möjlighet att göra nödvändiga och proportionerliga undantag motiverade av bland annat nationell säkerhet och brottsbekämpning.

[174] *Explanatory Report – CETS 223 – Automatic Processing of Personal Data (Amending Protocol)*, p. 62.

8.21.2 Tillgång till personuppgifter

Förslag: De nuvarande bestämmelserna om tillgång till personuppgifter ska överföras till den nya lagen.

Bedömning: Det finns inte tillräckligt starka skäl för att ändra den nuvarande regleringen om den interna tillgången till personuppgifter.

Den nuvarande regleringen

Enligt 5 kap. 5 § säpodatalagen ska Säkerhetspolisen se till att tillgången till personuppgifter begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter. Motsvarande bestämmelse återfinns även i brottsdatalagen (3 kap. 6 §) och en rad andra personuppgiftslagar. Bestämmelsen är inte ny för säpodatalagen, utan är överförd från den tidigare polisdatalagen. Syftet är att förhindra intrång i enskildas personliga integritet genom att skydda uppgifterna från att behandlas för andra syften än att utföra en tjänsteuppgift.

När stora informationsmängder är samlade på ett sådant sätt att integritetskänsliga personuppgifter är enkelt sökbara på elektronisk väg, finns enligt regeringen uppenbara risker för intrång i den personliga integriteten. I förarbetena förklaras därför att det är en hörnsten i skyddet av enskildas integritet att åtkomst endast medges till de personuppgifter som den enskilde tjänstemannen behöver för att kunna utföra sina arbetsuppgifter. Vidare konstateras att det inte endast ska vara en fråga om vilka uppgifter en medarbetare *får* behandla, utan även vilka uppgifter som denne *kan* behandla. Ju fler personer i en myndighet som har tillgång till personuppgifter, desto större är risken för obehörig åtkomst eller spridning av uppgifterna. Det innebär att den faktiska åtkomsten ska vara begränsad till vad som krävs.[175]

[175] Prop. 2018/19:163 s. 139 och prop. 2017/18:232 s. 180 f.

Finns det skäl att ändra den nuvarande ordningen?

Bestämmelsen i nuvarande 5 kap. 5 § säpodatalagen innebär en skyldighet för myndigheten att bland annat besluta om behörighetssystem som begränsar tillgången till personuppgifter. Säkerhetspolisen har implementerat en omfattande sektionering av information där tillgång begränsas till uppgifter som behövs för specifika verksamheter eller arbetsuppgifter.

Det framgår av interna styrdokument vem som har mandat att besluta om behörigheter till myndighetens informationssystem. För att få behörighet ska medarbetaren ha ett behov av uppgifterna samt ha tillräcklig kunskap om informationssystemet, informationssäkerhet och personuppgiftsskydd. Tillgångsfrågan bedöms utifrån uppgifternas skyddsvärde från både verksamhets- och integritetssynpunkt.

Säkerhetspolisen tillämpar olika behörighetsnivåer i sina informationssystem – från behörigheter som endast tillåter läsning till sådana som medger redigering. Loggning och logguppföljning används för att kontrollera efterlevnaden av reglerna.

Att begränsa sökningar och registerslagningar till sådana som är motiverade av arbetsuppgifter är en central säkerhetsmekanism för att skydda de registrerades personliga integritet. Säkerhetspolisens befintliga system och rutiner för tilldelning av behörigheter framstår som välfungerande och välavvägda.

Bestämmelserna kompletteras även av särskild lagstiftning. Enligt lag (2019:547) om förbud mot användning av vissa uppgifter för att utreda brott ska Säkerhetspolisen begränsa tillgången till uppgifter från FRA på ett sätt som särskilt beaktar att dessa inte får användas för att utreda brott.

Den nuvarande regleringen bör överföras till den nya lagen

Begränsning av tillgång till personuppgifter är en grundläggande komponent i skyddet av den personliga integriteten. Den nuvarande bestämmelsen har visat sig vara ett effektivt verktyg för att säkerställa detta skydd inom Säkerhetspolisens verksamhet.

Bestämmelsen ger Säkerhetspolisen ett tydligt ansvar samtidigt som den tillåter en flexibel tillämpning anpassad efter verksam-

hetens särskilda behov. Den har fungerat väl i praktiken och är väl integrerad i myndighetens interna processer och styrdokument.

Vi anser att den nuvarande regeln, som även har motsvarigheter i många andra personuppgiftslagar, bör överföras till den nya lagen utan ändringar.

8.21.3 Säkerhetsåtgärder

Förslag: De nuvarande bestämmelserna om säkerhetsåtgärder för skydd mot otillåten behandling, förlust, förstöring och annan oavsiktlig skada ska överföras till den nya lagen.

Den nuvarande regleringen

Enligt 5 kap. 7 § säpodatalagen ska Säkerhetspolisen vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas, särskilt mot obehörig eller otillåten behandling och mot förlust, förstöring eller annan oavsiktlig skada.

Även denna bestämmelse har sin motsvarighet i brottsdatalagen och gällde redan innan säpodatalagen genom en liknande bestämmelse i personuppgiftslagen. Enligt förarbetena ska frågan om vilka åtgärder som är lämpliga bestämmas utifrån de tekniska möjligheter som finns, vad det skulle kosta att genomföra åtgärderna och de särskilda risker som finns med behandlingen. Vidare ska behandlingens art, omfattning, sammanhang och ändamål beaktas. Särskild hänsyn bör även tas till i vilken utsträckning känsliga personuppgifter behandlas och hur integritetskänsliga övriga personuppgifter som behandlas är.[176]

I säkerhetsskyddslagen (2018:585) och säkerhetsskyddsförordningen (2021:955) finns bestämmelser, som har företräde framför säpodatalagen i fråga om informationssäkerhet för bland annat informationssystem som har betydelse för säkerhetskänslig verksamhet. Enligt 2 kap. 2 § säkerhetsskyddslagen ska den som till någon del bedriver säkerhetskänslig verksamhet förebygga att säkerhetsskyddsklassificerade uppgifter obehörigen röjs, ändras, görs otillgängliga

[176] Prop. 2018/19:163 s. 143.

eller förstörs och förebygga skadlig inverkan i övrigt på uppgifter och informationssystem som gäller säkerhetskänslig verksamhet.

Den nuvarande regleringen bör överföras till den nya lagen

Det kan ifrågasättas om det fyller någon funktion att vid sidan av det regelverk som gäller säkerhetsskyddsklassificerade uppgifter även ställa upp informationssäkerhetskrav i säpodatalagen. Säkerhetspolisens operativa it-infrastruktur omfattas i sin helhet av säkerhetsskyddslagens regler.

Syftet är dock olika för de båda lagarna. Säkerhetsskyddslagen reglerar skyddet för säkerhetskänslig verksamhet mot spioneri, sabotage, terroristbrott och andra brott som kan hota verksamheten samt skydd i andra fall av säkerhetsskyddsklassificerade uppgifter. Säpodatalagens bestämmelser om informationssäkerhet avser att skydda de registrerades uppgifter från att spridas eller förstöras. Syftet är att förhindra integritetsintrång eller rättsförlust. Det kan ställas olika krav på informationssäkerhet när det gäller å ena sidan verksamhetens behov och å andra sidan skydd för enskildas rättigheter.

Ytterligare ett skäl till att behålla bestämmelsen om informationssäkerhet i säpodatalagen är att det innebär att informationssäkerheten till skydd för enskilda står under tillsyn. Säkerhetspolisen är tillsynsmyndighet enligt säkerhetsskyddslagen och står inte själv under någon tillsyn i det avseendet.[177] Övervägande skäl talar för att behålla den nuvarande bestämmelsen om säkerhetsåtgärder i den nya lagen.

8.21.4 Det finns inte skäl att införa någon rapporteringsskyldighet vid personuppgiftsincidenter

Bedömning: Det finns inte skäl att införa en skyldighet att anmäla personuppgiftsincidenter till tillsynsmyndigheten.

[177] Se 8 kap. 1 § säkerhetsskyddsförordning.

Skälen för bedömningen

Skyldigheten att rapportera personuppgiftsincidenter, enligt artikel 7.2 i dataskyddskonventionen, har sin motsvarighet i brottsdatadirektivet och regleras för de brottsbekämpande myndigheternas del genom 3 kap. 9–11 §§ brottsdatalagen. Skyldigheterna enligt brottsdatalagen gäller emellertid inte för it-incidenter i informationssystem som har betydelse för säkerhetskänslig verksamhet eller om det annars finns skäl att anta att en säkerhetsskyddsklassificerad uppgift otillåtet har röjts. Sådana incidenter ska, enligt 2 kap. 4 § säkerhetsskyddsförordningen, i stället rapporteras till Säkerhetspolisen, eller i vissa fall till Försvarsmakten.

Behovet av att skydda information om incidenter som kan innebära att uppgifter med betydelse för Sveriges säkerhet kan ha läckt har ansetts vara så stort att endast den myndighet som utövar tillsyn över säkerhetsskyddet ska få ta del av den. En personuppgiftsincident i Säkerhetspolisens informationssystem som drabbar personuppgifter som behandlas med stöd av säpodatalagen kommer alltid att ha betydelse för Sveriges säkerhet. Det finns därför goda skäl för att personuppgiftsincidenter angående uppgifter som behandlas enligt säpodatalagen ska undantas från konventionens krav om anmälan till tillsynsmyndigheten. Undantaget, motiverat av skyddet för nationell säkerhet, är nödvändigt och proportionerligt.

8.22 Personuppgiftsbiträden

Förslag: Nuvarande regler för anlitande av personuppgiftsbiträden, skyldigheten för biträdet att följa instruktioner och förbud mot att utan tillstånd anlita underbiträden ska överföras till den nya lagen.

Personuppgiftsbiträdets skyldigheter ska omfatta samma tekniska och organisatoriska åtgärder som gäller för Säkerhetspolisen. Vidare ska biträdet vara skyldig att samarbeta med tillsynsmyndigheten och utföra konsekvensbedömningar.

8.22.1 Dataskyddskonventionens krav

Article 2 – Definitions

For the purposes of this Convention:

d. ”controller” means the natural or legal person, public authority, service, agency or any other body which, alone or jointly with others, has decision-making power with respect to data processing;

f. ”processor” means a natural or legal person, public authority, service, agency or any other body which processes personal data on behalf of the controller.

Dataskyddskonventionen 108+ innehåller, till skillnad mot sin föregångare, regler om personuppgiftsbiträden. För personuppgiftsbiträden gäller artiklarna 7 och 10 i konventionen på samma sätt som för den personuppgiftsansvarige. Det finns däremot inte några särskilda regler för hur ett biträde ska utses, vilken behörighet som denne har eller om biträdet i sin tur kan anlita ett underbiträde (jämför artikel 22 i brottsdatadirektivet).

Artikel 7 i konventionen reglerar säkerhetsåtgärder och tillgång till personuppgifter (se avsnitt 8.20). Artikel 10 reglerar den personuppgiftsansvariges skyldigheter i olika avseenden: skyldigheten att säkerställa och kunna visa att personuppgifter behandlas konventionsenlig, skyldigheten att bedöma konsekvenserna och anpassa behandlingen för att minska risken för intrång i de intressen som påverkas samt att införa de tekniska och organisatoriska åtgärder som krävs med hänsyn till skyddet för personuppgifter (se avsnitt 8.20.3).

8.22.2 Den nuvarande regleringen

Personuppgiftsbiträden regleras i 5 kap. 11–14 §§ säpodatalagen. I 5 kap. 11 § framgår att Säkerhetspolisen får anlita personuppgiftsbiträden. Innan ett personuppgiftsbiträde anlitas ska Säkerhetspolisen försäkra sig om att biträdet kommer att vidta de lämpliga tekniska och organisatoriska åtgärder som krävs för att behandlingen av personuppgifter ska vara författningsenlig och för att skydda registrerades rättigheter. Vidare framgår att personuppgiftsbiträdets behandling av personuppgifter ska regleras i ett skriftligt avtal eller annan skriftlig överenskommelse. Av 5 kap. 12 § följer att det krävs

skriftligt tillstånd från Säkerhetspolisen innan ett personuppgiftsbiträde får anlita ett eget personuppgiftsbiträde (underbiträde).

Av 5 kap. 13 § framgår den självklara förutsättningen att personuppgiftsbiträdet ska behandla personuppgifter i enlighet med instruktioner från Säkerhetspolisen. Om ett personuppgiftsbiträde går utanför sina instruktioner och själv bestämmer ändamålen med och medlen för behandlingen, ska biträdet anses vara personuppgiftsansvarig för den behandlingen, vilket bland annat kan medföra skadeståndsansvar mot de registrerade.

5 kap. 14 § hänvisar till att en del av de skyldigheter som gäller för Säkerhetspolisen som personuppgiftsansvarig även gäller för biträden. Det är skyldigheten att föra loggar och att begränsa medarbetares tillgång till personuppgifter till det som krävs för att fullgöra sina respektive arbetsuppgifter. Vidare gäller skyldigheten att vidta lämpliga säkerhetsåtgärder även för personuppgiftsbiträden. Att dessa skyldigheter gäller även för biträden innebär inte att ansvaret delegerats. Säkerhetspolisen är, enligt 1 kap. 6 § säpodatalagen, ansvarig även för den behandling som utförs av biträden på uppdrag av myndigheten.

8.22.3 Det bör ställas högre krav på personuppgiftsbiträden för att säkerställa att dataskyddskonventionen efterlevs

Det behövs regler om personuppgiftsbiträden

Säkerhetspolisen utnyttjar inte möjligheten till personuppgiftsbiträden i någon större omfattning. Bestämmelserna är dock viktiga för att kunna säkerställa tekniska lösningar och resiliens i myndigheten. Det måste också vara möjligt för Säkerhetspolisen att exempelvis uppdra åt Polismyndigheten att behandla personuppgifter i samband med gemensamma insatser. Ett annat fall kan vara att Försvarsmakten lämnar stöd enligt lagen (2006:343) om Försvarsmaktens stöd till polisen vid terrorismbekämpning, med exempelvis övervakningsåtgärder.

Säkerhetspolisen är givetvis noga med att utforma ett eventuellt personuppgiftsbiträdesavtal av bland annat informationssäkerhetsskäl. Säpodatalagens regler är avsedda att skydda den personliga integriteten genom tvingande minimiregler vid sidan av sådana biträdesavtal och

att ålägga biträden ett självständigt ansvar. Det finns därför goda skäl att behålla regler om personuppgiftsbiträden.

De nuvarande reglerna om anlitande av personuppgiftsbiträden och behandling enligt instruktioner bör överföras till den nya lagen

De nuvarande bestämmelserna om anlitande av personuppgiftsbiträden och behandling enligt den personuppgiftsansvariges instruktioner i 5 kap. 11–13 §§ framstår som välavvägda.[178] Inte minst av tillsynsskäl är det avgörande att ett avtal eller annan överenskommelse med personuppgiftsbiträdet är skriftligt och att inte biträdet kan anlita underbiträden utan Säkerhetspolisens uttryckliga godkännande. Det framstår även som naturligt att Säkerhetspolisen, innan ett avtal ingås, måste säkerställa att biträdet har förmåga att uppfylla kraven för att skydda personuppgifter. Dessa regler bör således föras över till den nya lagen.

Personuppgiftsbiträdets skyldigheter måste anpassas till dataskyddskonventionen

I 5 kap. 14 § säpodatalagen hänvisas till att personuppgiftsbiträdet har vissa specifika skyldigheter, vilka framgår av 5 kap. 4, 5, 7 och 8 §§ i samma lag. Dessa nuvarande bestämmelser motsvarar dock inte fullt ut de skyldigheter som anges i dataskyddskonventionen 108+. Enligt konventionens artikel 10 ska ett biträde följa samma krav som den personuppgiftsansvarige avseende tekniska och organisatoriska åtgärder för att säkerställa dataskyddet. Det finns därför skäl att utvidga biträdets skyldigheter så att samtliga relevanta krav blir tillämpliga även för personuppgiftsbiträden.

Det innebär att de nuvarande bestämmelserna i 5 kap. 1–8 §§ säpodatalagen även bör gälla för ett biträde. Det är regler om tekniska och organisatoriska åtgärder, tillgång till personuppgifter, säkerhetsåtgärder och konsekvensbedömning. Det bör dock inte finnas något krav på förhandssamråd med tillsynsmyndigheten. Om en konsekvensbedömning visar på en särskild risk för intrång i den registre-

[178] Se prop. 2018/19:163 s. 148–151.

rades personliga integritet bör förhandssamrådet ske mellan tillsynsmyndighet och Säkerhetspolisen, och inte med biträdet.

8.23 Informationsutbyte

8.23.1 Behandling för ändamål i annan verksamhet

Förslag: Personuppgifter får behandlas för att tillhandahålla information till andra om det sker i enlighet med lag eller förordning.

Det ska inte längre krävas särskilda skäl för att tillhandahålla information till Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst eller i Försvarets radioanstalts försvarsunderrättelseverksamhet.

Personuppgifter ska även få tillhandahållas om de behövs i verksamhet som rör underrättelse- och säkerhetsfrågor hos en internationell organisation som Sverige är medlem.

Den nuvarande regleringen

De så kallade sekundära ändamålen, i 2 kap. 4 § säpodatalagen, syftar till att ge Säkerhetspolisen en möjlighet att dela personuppgifter för ändamål som endast är relevanta för mottagande myndighet. Paragrafen innehåller en uppräkning av de verksamheter där informationsdelning har ansetts nödvändig och särskilt motiverad.[179] För att tillhandahålla personuppgifter till dessa verksamheter behövs inte någon prövning mot finalitetsprincipen. I huvudsak gäller de sekundära ändamålen brottsbekämpning hos andra myndigheter i Sverige eller utomlands. Vidare anges att uppgifter får behandlas för att delges andra underrättelse- och säkerhetstjänster. Både svenska partners, i första hand den militära underrättelse- och säkerhetstjänsten, men även samverkande utländska tjänster.

Säkerhetspolisen får även behandla personuppgifter för att tillhandahålla information till riksdagen och regeringen. Om det finns en skyldighet att lämna uppgifter till följd av lag eller förordning, får uppgifter även behandlas för detta ändamål.

[179] Se prop. 2009/10:85 s. 260 ff.

I övrigt får personuppgifter behandlas för sekundära ändamål endast i enskilda fall och efter en prövning av utlämnandets förenlighet med finalitetsprincipen.

Informationsdelning i överenstämmelse med lag eller förordning

Sekretess och sekundära ändamål

Uppräkningen i nuvarande 2 kap. 4 § är inte uttömmande. Av andra stycket framgår att personuppgifter som behandlas enligt säpodatalagen även får tillhandahållas annan i den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning. Det innebär att någon ytterligare prövning enligt finalitetsprincipen inte behöver göras, om det finns en sekretessbrytande uppgiftsskyldighet.

I många andra lagar anges att detta även ska gälla i de fall då det inte föreligger en skyldighet att lämna uppgift, men då det finns en möjlighet till det. Det rör sig med andra ord om de fall där det finns en sekretessbestämmelse som medger utlämnande. Dessa bestämmelser är motiverade av att det får förutsättas att det gjorts en avvägning mellan intresset av att uppgiften lämnas ut och intresset av att skydda enskilda personers integritet i samband med införandet av den bestämmelsen som medger utlämnande. Om det föreskrivs att personuppgifter även får lämnas ut om det sker i ”överensstämmelse med lag eller förordning”, avses de tillfällen då lagstiftaren redan genom en sekretessbestämmelse tagit ställning till att uppgiften i sig får lämnas ut. Att utlämnandet sker genom automatiserad behandling, så att en personuppgiftslag är tillämplig, hindrar då inte utlämnandet.[180]

Det framstår som rimligt att frågan om en personuppgift får behandlas genom utlämnande endast ska prövas med tillämpning av ett regelverk. I princip all Säkerhetspolisens personuppgiftsbehandling sker numera datoriserat och med stöd av antingen dataskyddsförordningen eller säpodatalagen. Det finns inte något skäl till att utlämnanden av uppgifter som är helt eller delvis automatiserat ska omfattas av ett ytterligare regelverk i förhållande till utlämnande av uppgifter som behandlas helt manuellt och endast prövas enligt offentlighets- och sekretesslagen.

[180] Se t.ex. prop. 2007/08:126 s. 59.

Frågan om förhållandet mellan sekretess och så kallad sekundär personuppgiftsbehandling utreds för närvarande av *Utredningen om förbättrade möjligheter till informationsutbyte mellan myndigheter* (Ju 2023:22).

De sekundära ändamålen bör kompletteras med en bestämmelse om utlämnande som sker i överenstämmelse med lag eller förordning

Uppräkningen av de sekundära ändamålen i säpodatalagen avser de typfall då uppgiftslämnande sker inom ramen för lagens tillämpningsområde och då utlämnande kan ske oavsett för vilket ändamål uppgiften ursprungligen behandlats. Uppräkningen bidrar till transparens i fråga om hur Säkerhetspolisen kan behandla uppgifter, trots att listan inte är uttömmande. Vid sidan av uppräkningen ska myndigheten i dag tillhandahålla information till följd av sekretessbrytande bestämmelser.

Det finns skäl att överväga om säpodatalagen ska få samma reglering som många andra myndigheter som innebär att uppgifter även får lämnas ut om det sker i överensstämmelse med lag eller förordning. Att en sekretessbestämmelse som medger uppgiftslämnande har företräde framför nuvarande 2 kap. 4 § säpodatalagen utgör sannolikt gällande rätt.[181] Vi anser dock att det finns goda skäl att förtydliga att avvägningen mellan enskilda och allmänna intressen gjorts i den sekretessbestämmelse som medger uppgiftslämnande mellan myndigheter. Om lagstiftaren kommit fram till att uppgifter som behandlas inom Säkerhetspolisens verksamhet får lämnas ut utan hinder av sekretess, bör någon ytterligare prövning enligt finalitetsprincipen inte behöva göras.

Den nuvarande uppräkningen av sekundära ändamål i 2 kap. 4 § säpodatalagen kan anses fylla en funktion avseende uppgifter som inte omfattas av någon sekretessbestämmelse. Att lämna ut personuppgifter utgör en integritetsrisk för enskilda. Det finns därför goda skäl till att räkna upp de typfall då en sådan behandling kan ske för att göra tillämpningen mer transparent.

Utöver den uppräkning av verksamheter med vilka Säkerhetspolisen typiskt sett delar information föreslår vi att det ska framgå att uppgifter även får behandlas för uppgiftslämnande i överens-

[181] Jfr HFD 2021 ref. 10.

stämmelse med lag eller förordning. Det omfattar förvisso även de uppräknade myndigheterna.

Informationsdelning med den militära underrättelse- och säkerhetstjänsten och FRA

I likhet med de andra så kallade sekundära ändamålen har bestämmelserna om informationsdelning mellan Säkerhetspolisen och de den militära underrättelse- och säkerhetstjänsten följt med från tidigare reglering. I förarbetena till 2010 års polisdatalag, där möjligheten att tillhandahålla information till Försvarsmaktens underrättelseverksamhet och säkerhetstjänst först infördes, angavs att underrättelseverksamhet som rör rikets säkerhet är en gemensam angelägenhet för Säkerhetspolisen och Försvarsmakten. För att personuppgifter skulle få lämnas ut för denna verksamhet förklarades dock att det dels skulle vara fråga om en uppgift som Säkerhetspolisen bedömer behövs i Försvarsmaktens verksamhet, dels att det fanns särskilda skäl för att tillhandahålla uppgiften. Vilken slags skäl som ska anses vara särskilda anges inte förarbetena men exemplifieras med att det under en förundersökning som Säkerhetspolisen bedriver kommer fram information som kan vara mycket viktig för Försvarsmakten i dess underrättelseverksamhet. Det kan till exempel röra sig viktiga uppgifter om en försvarsanställd eller någon i dennes närmaste krets och som är viktiga för Sveriges säkerhet. Ett annat exempel som anges är att Säkerhetspolisen i sin brottsbekämpning noterar svagheter eller brister i skyddet för Försvarsmaktens anläggningar som skulle kunna få allvarliga konsekvenser.[182]

Genom säpodatalagen tillfördes utlämnande till FRA vid sidan av Försvarsmakten. I lagförarbetena angavs att Säkerhetspolisen, Försvarsmakten och FRA har angränsande uppdrag beträffande Sveriges säkerhet som förutsätter nära samarbete och kontinuerligt informationsutbyte. Regeringen ansåg att på samma sätt som brottsbekämpning i vissa avseenden är en för flera myndigheter gemensam angelägenhet är också underrättelseverksamhet som rör Sveriges säkerhet en för Säkerhetspolisen, Försvarsmakten och FRA gemensam angelägenhet, även om myndigheterna har olika uppdrag i förhållande till Sveriges säkerhet. Regeringen ansåg att det därför

[182] Prop. 2009/10:85 s. 262 och 365 f.

måste finnas ett utrymme för att utbyta information mellan myndigheterna. Kravet på särskilda skäl för utlämnande kvarstod emellertid, i syfte att markera att bestämmelsen ska tillämpas restriktivt.[183]

Vår uppfattning är att hotbilden mot Sverige och säkerhetsläget i vårt närområde ställer krav på ett nära samarbete mellan våra säkerhet- och underrättelsetjänster. Den hotbild som finns mot Sverige har alltmer fått internationella dimensioner. En antagonistisk statlig aktör kan exempelvis verka för att destabilisera Sverige på flera fronter och med olika metoder. Hybridhoten har blivit allt vanligare och ofta kan det vara svårt att på förhand avgöra om ett angrepp, exempelvis ett sabotage mot kritisk infrastruktur, rör Sveriges försvar och säkerhet eller om det är en fråga för Säkerhetspolisen.

Med hänsyn till det försämrade säkerhetsläget finns det att ta bort hinder för att förebygga och förhindra hot mot nationell säkerhet. Skälen som talar för ett restriktivt informationsutbyte mellan den nationella säkerhetstjänsten och försvarsunderrättelsemyndigheterna får anses vara överskuggade av de skäl som talar för ett mer integrerat samarbete. Säkerhetspolisen ingår även i det nationella underrättelserådet tillsammans med chefen för den militära underrättelse- och säkerhetstjänsten och generaldirektören för FRA. Vår bedömning är därför att kravet på särskilda skäl ska utgå ur den nuvarande bestämmelsen.

Informationsdelning inom Nato

Sveriges Nato-medlemskap har inneburit att Säkerhetspolisen ingår i nya strukturer för underrättelsesamverkan. Som nationell säkerhetstjänst representerar Säkerhetspolisen tillsammans med Försvarsmakten Sverige i *Natos civila underrättelsekommitté* (Civilian Intelligence Committee). Civila underrättelsekommittén rapporterar direkt till Nordatlantiska rådet och ger råd i frågor som rör spionerі, terrorism och relaterade hot.

Säkerhetspolisen hade redan tidigare ett integrerat samarbete med vissa betrodda partners i andra länder. De nuvarande bestämmelserna om informationsdelning tar också sikte på enskilda säkerhets- och underrättelsetjänster. Samarbete med mellanfolkliga organisationer

[183] Prop. 2018/19:163 s. 70.

förutsätter att dessa bedriver brottsbekämpande verksamhet, som Europol.

Den information som behöver kunna delas inom ramen för Natos underrättelsesamarbete bör kunna ske utan en prövning mot finalitetsprincipen. Den underrättelsesamverkan som bedrivs inom Natos civila underrättelsekommitté kan i princip anses vara brottsbekämpande. För att undvika eventuella otydligheter bör det dock klargöras att personuppgifter får behandlas för att tillhandahålla information som behövs för underrättelse- och säkerhetsverksamhet i en mellanfolklig organisation där Sverige är medlem. Vi föreslår en lagreglering med denna innebörd.

8.23.2 Direktåtkomst och sekretessbrytande bestämmelser

Förslag: Säkerhetspolisen ska ha samma möjlighet att medge direktåtkomst som enligt nuvarande lag.

De nuvarande bestämmelserna om direktåtkomst och sekretessbrytande bestämmelser ska därför överföras till den nya lagen, med de justeringar som är föranledda av andra ändringar.

Den nuvarande regleringen

Direktåtkomst

Genom säpodatalagen utökades möjligheterna för Säkerhetspolisen att medge direktåtkomst till svenska och utländska myndigheter. Dessa regler är motiverade av att brottsbekämpning bedrivs dygnet runt och vissa uppgifter måste vara tillgängliga omedelbart även utanför kontorstid. Genom direktåtkomst behöver den mottagande myndigheten inte vända sig till den utlämnande myndigheten med en särskild begäran. Tjänstemännen kan i stället eftersöka och hämta den information som direktåtkomsten ger tillgång till.

Det ansågs vidare ligga i Sveriges intresse, och följa av våra internationella åtaganden, att Säkerhetspolisen på ett effektivt sätt kan bidra till att förhindra terrorism utomlands. Ett väl fungerande samarbete med andra underrättelse- och säkerhetstjänster inom kontraterrorverksamheten ansågs underlättas av möjligheten till direktåtkomst även för utländska säkerhets- och underrättelse-

tjänster inom EU- och EES-samarbetet. År 2023 utökades möjligheterna till direktåtkomst till att avse även underrättelse- och säkerhetstjänster i Schweiz och Förenade kungariket. Skälet var att dessa länder varken är medlemmar i EES eller EU men ingår i det europeiska forumet för att bekämpa terroristbrott, *Counter Terrorism Group*.

För att kunna medge direktåtkomst krävs som regel sekretessbrytande bestämmelser. I annat fall krävs att varje uppgift som görs tillgänglig genom direktåtkomst måste sekretessprövas. I nuvarande lagstiftning finns därför sekretessbrytande bestämmelser. Vidare får endast gemensamt tillgängliga uppgifter göras tillgängliga genom direktåtkomst

Sekretessbrytande bestämmelser

De personuppgifter som Säkerhetspolisen behandlar omfattas som regel av sekretess enligt 15 kap. 1 och 2 §§ och 18 kap. 1 och 2 §§ offentlighets- och sekretesslagen. Där regleras utrikes- och försvarssekretessen samt sekretessen till skydd för brottsbekämpningen. Bestämmelserna är tillämpliga på uppgifter som hänför sig till eller rör viss verksamhet. Det innebär att de gäller i all verksamhet där sådana uppgifter förekommer.

Uppgifter om enskilda i Säkerhetspolisens verksamhet omfattas även av sekretess enligt 35 kap. 1 § offentlighets- och sekretesslagen. Enligt paragrafen gäller sekretess för uppgifter som rör enskildas personliga och ekonomiska förhållanden och som förekommer i brottsbekämpande verksamhet. Uppgifter om enskilda kan även omfattas av sekretess enligt 37 kap. 1 § och 21 kap. 3 och 5 §§. Enligt 37 kap. 1 § gäller sekretess i verksamhet för kontroll över utlänningar och i ärenden om svenskt medborgarskap. Enligt 21 kap. 3 § gäller sekretess för enskildas kontaktuppgifter i vissa situationer och enligt 5 § gäller sekretess till skydd för utlännings säkerhet i vissa fall.

I 10 kap. offentlighets- och sekretesslagen anges under vilka förhållanden myndigheter kan lämna ut uppgifter trots att sekretess gäller. I kapitlet finns flera bestämmelser som medger att Säkerhetspolisen tar del av uppgifter. Uppgifter som rör terroristbrott eller andra allvarliga brott bryter i vissa fall genom sekretessskyddet till förmån för enskild. När det gäller möjligheten för

Säkerhetspolisen att lämna ut uppgifter så är det i huvudsak 10 kap. 28 § offentlighets- och sekretesslagen som är av intressen. Enligt denna bestämmelse hindrar inte sekretess för en uppgift att den lämnas till en annan myndighet, om uppgiftsskyldighet följer av lag eller förordning.

Sådan uppgiftsskyldighet som krävs för att sekretessen ska brytas finns i dag i bland annat säpodatalagen. I 2 kap. 15 § anges att personuppgifter ska lämnas ut för att framställa rättsstatistik, vilket i praktiken innebär en uppgiftsskyldighet i förhållande till Brottsförebyggande rådet.

I 2 kap. 17 och 18 §§ säpodatalagen framgår att Polismyndigheten, Försvarsmakten och FRA under vissa förhållanden har rätt att ta del av uppgifter utan hinder av den sekretess som kan föreligga till förmån för enskildas personliga förhållanden. Utlämnande får ske utan hinder av den sekretess som gäller för kontaktuppgifter enligt 21 kap. 3 §, för uppgift i bland annat förundersökning och eller underrättelseverksamhet enligt 35 kap. 1 § eller i ärenden om utlänningskontroll och medborgarskap enligt 37 kap. 1 § offentlighets- och sekretesslagen. En förutsättning för utlämnande är att den mottagande myndigheten behöver uppgiften i sin verksamhet. Eftersom dessa bestämmelser innebär en rätt för de mottagande myndigheterna att ta del av uppgifterna behöver ingen sekretessprövning ske för utlämnande till de myndigheterna som anges och som behöver uppgifterna för de angivna ändamålen.

I 2 kap. 16 § säpodatalagen regleras under vilka förhållanden personuppgifter får lämnas ut till Interpol eller Europol, eller till en polismyndighet eller åklagarmyndighet i en stat som är ansluten till Interpol samt till en utländsk underrättelse- eller säkerhetstjänst.

Denna bestämmelse är motiverad av 8 kap. 3 § offentlighets- och sekretesslagen. Där anges att uppgifter som omfattas av sekretess som huvudregel inte får röjas för en utländsk myndighet eller en mellanfolklig organisation. Detta förbud är förenat med två undantag, dels om utlämnande sker i enlighet med särskild föreskrift i lag eller förordning, dels om uppgiften i motsvarande fall skulle få lämnas ut till en svensk myndighet och det står klart att det är förenligt med svenska intressen att uppgiften lämnas till den utländska myndigheten eller den mellanfolkliga organisationen.

2 kap. 16 § säpodatalagen är en sådan särskild föreskrift i lag som medger utlämnande av sekretessbelagda uppgifter till utländska myndigheter och mellanfolkliga organisationer.

Säkerhetspolisen bör ha samma möjligheter att medge direktåtkomst som i dag

Det finns inga skäl att ändra på möjligheterna till direktåtkomst

Då säpodatalagen beslutades gjordes grundliga överväganden avseende både direktåtkomst och vilka sekretessbrytande bestämmelser som var nödvändiga och proportionerliga.[184]

Det har inte uppmärksammats något problem med de nuvarande bestämmelser om direktåtkomst och inte heller något behov av att förändra dem. De skäl som föranlett att de infördes gör sig minst lika starkt gällande i dag. Myndighetssamverkan i Sverige är nödvändig för att bekämpa brott och samarbetet inom det europeiska samarbetet för kontraterrorism underlättas av att myndigheten både kan ta emot och lämna ut uppgifter genom direktåtkomst. Vår avsikt är därför att föreslå en lagreglering som inte ändrar de materiella förutsättningarna för direktåtkomst, om det inte är nödvändigt.

Utlämnande genom direktåtkomst måste vara proportionerligt

De förutsättningar som gällde då reglerna om direktåtkomst och sekretessgenombrott infördes i säpodatalagen var något annorlunda än de förutsättningar som gäller enligt vårt förslag. Reglerna om gemensamt tillgängliga uppgifter är slopade till förmån för en särskild reglering av inledande granskning. Säkerhetspolisen får möjlighet att behandla känsliga personuppgifter i större utsträckning än i dag och att behandla uppgifter för de mer verksamhetsanpassade ändamålet att kartlägga och klarlägga brottslig verksamhet. Dessutom tas kravet på vissa särskilda upplysningar bort, vilket innebär att det bland annat inte längre behövs någon upplysning om trovärdighet eller sakriktighet (se avsnitt 8.13.4 och 8.13.5). Det kan mot denna bakgrund finnas betänkligheter mot att tillåta att alla uppgifter som

[184] Se prop. 2018/19:163 s. 98–115.

behandlas för brottsbekämpande ändamål hos Säkerhetspolisen även lämnas ut genom direktåtkomst.

Att lämna ut en personuppgift, oavsett om det sker elektroniskt genom direktåtkomst eller på annat sätt, är en personuppgiftsbehandling. Enligt vårt förslag ska alla behandlingsåtgärder vara proportionerliga. Skälet för att utföra behandlingen ska överväga intrånget i de enskilda eller allmänna intressen som kan påverkas av den. Denna bestämmelse kan få inverkan på vilka uppgifter som kan delas genom direktåtkomst med annan myndighet. En del av proportionalitetsprövningen utgörs av risken för att personuppgifter missbrukas eller sprids på ett otillbörligt sätt. Detta gäller särskilt känsliga personuppgifter eller uppgifter som på annat sätt är integritetskänsliga. Det finns därför anledning att noga överväga vilka uppgifter som görs tillgängliga för andra myndigheter.

Att medge direktåtkomst kräver en prövning, både av de mottagande myndigheternas behov, proportionaliteten i förhållande till enskildas intressen och av skyddet för den egna verksamheten. Det bör även beaktas att den mottagande myndigheten måste kunna behandla uppgiften författningsenligt enligt de bestämmelser som gäller i den verksamheten. Detta gäller särskilt då Säkerhetspolisens förutsättningar att behandla personuppgifter enligt den föreslagna lagen kommer skilja sig alltmer från Polismyndigheten och andra mottagare.

Vår bedömning är att de uppgifter som i dag utlämnas med direktåtkomst även fortsättningsvis kan göra det. Denna behandling är proportionerlig. I takt med att Säkerhetspolisen förändrar sin informationshantering med stöd av den föreslagna lagen kan dock frågan om vilka uppgifter som delas genom direktåtkomst behöva ses över i särskild ordning. Frågan kan komma att uppmärksammas vid tillsyn.

Sekretessbrytande bestämmelser krävs för direktåtkomst

För att direktåtkomst ska vara funktionell krävs en bestämmelse som bryter sekretessen mellan myndigheterna. I annat fall kommer utlämnandet behöva prövas i varje enskilt fall. De nuvarande reglerna i 2 kap. 16–18 §§ anger de särskilda fall då sekretess inte ska gälla

mellan myndigheterna och tillkom för att möjliggöra direktåtkomst, men de är inte begränsade till sådant utlämnande.[185]

Det har uttryckligen enligt våra direktiv inte varit denna utrednings uppdrag att se över sekretess mellan myndigheterna. Om det finns skäl att ändra reglerna måste frågan beredas med de myndigheter som omfattas av dem, vilket i så fall får ske i särskild ordning. De nuvarande bestämmelserna bör därför överföras till den nya lagen.

8.23.3 Överföring av personuppgifter till mottagare utomlands

Bedömning: Det ska inte göras någon åtskillnad i lagen mellan tredje land och medlemsstater i EU och EES. Sekretessbrytande bestämmelser i förhållande till utländska myndigheter bör tydliggöras.

Förslag: Om mottagaren kan garantera tillräckligt skydd för personuppgifter och om det är förenligt med svenska intressen, ska Säkerhetspolisen få föra över personuppgifter till brottsbekämpande myndigheter, säkerhets- och underrättelsetjänster och vissa mellanfolkliga organisationer, utan hinder av sekretess.

I enskilda fall och efter en sekretessprövning ska överföring av personuppgifter även få ske till en andra mottagare och till mottagare som inte kan garantera tillräckligt skydd för personuppgifter. I dessa fall ska skälet för att lämna ut personuppgifter uppenbart överväga intrånget i de enskilda eller allmänna intressen som kan påverkas av överföringen.

Dataskyddskonventionens krav

Artikel 14 i dataskyddskonventionen 108+ behandlar frågan om det fria flödet av personuppgifter mellan konventionens medlemsstater.

> **Article 14 – Transborder flows of personal data**
>
> 1. A Party shall not, for the sole purpose of the protection of personal data, prohibit or subject to special authorisation the transfer of such data to a recipient who is subject to the jurisdiction of another Party

[185] Ibid. s. 111 f.

to the Convention. Such a Party may, however, do so if there is a real and serious risk that the transfer to another Party, or from that other Party to a non-Party, would lead to circumventing the provisions of the Convention. A Party may also do so, if bound by harmonised rules of protection shared by States belonging to a regional international organisation.

2. When the recipient is subject to the jurisdiction of a State or international organisation which is not Party to this Convention, the transfer of personal data may only take place where an appropriate level of protection based on the provisions of this Convention is secured.

3. An appropriate level of protection can be secured by:

a. the law of that State or international organisation, including the applicable international treaties or agreements; or

b. ad hoc or approved standardised safeguards provided by legally-binding and enforceable instruments adopted and implemented by the persons involved in the transfer and further processing.

4. Notwithstanding the provisions of the previous paragraphs, each Party may provide that the transfer of personal data may take place if:

a. the data subject has given explicit, specific and free consent, after being informed of risks arising in the absence of appropriate safeguards; or

b. the specific interests of the data subject require it in the particular case; or

c. prevailing legitimate interests, in particular important public interests, are provided for by law and such transfer constitutes a necessary and proportionate measure in a democratic society; or

d. it constitutes a necessary and proportionate measure in a democratic society for freedom of expression.

5. Each Party shall provide that the competent supervisory authority within the meaning of Article 15 of this Convention is provided with all relevant information concerning the transfers of data referred to in paragraph 3.b and, upon request, paragraphs 4.b and 4.c.

6. Each Party shall also provide that the supervisory authority is entitled to request that the person who transfers data demonstrates the effectiveness of the safeguards or the existence of prevailing legitimate interests and that the supervisory authority may, in order to protect the rights and fundamental freedoms of data subjects, prohibit such transfers, suspend them or subject them to condition.

Dataskyddskonventionens syfte är bland annat att markera att respekten för privatlivet och skyddet av personuppgifter är grundläggande värden och därigenom bidra till det fria informationsflödet. Artikel 14 reglerar överföring av personuppgifter till ett annat land eller en mellanfolklig organisation. Av punkten 1 följer att skyddet för personuppgifter inte får hindra en överföring till en annan stat som också är ansluten till konventionen. Konventionen ska utgöra en garanti för att dess grundläggande dataskyddsprinciper följer med personuppgifter som rör sig över en landsgräns. Undantag från principen om att personuppgifter ska kunna flöda fritt mellan medlemsstaterna ska endast göras i undantagsfall och om det finns en konkret risk för att mottagarlandet inte uppfyller konventionens alla krav. Bestämmelsen hindrar emellertid inte att det fria flödet av uppgifter regleras till förmån för allmänna intressen, som allmän ordning eller nationell säkerhet.

Punkten 2 innebär att överföring av personuppgifter till ett land som inte medlem av konventionen endast får ske om en tillräcklig skyddsnivå kan garanteras. I punkten 3 anges att bland annat nationell lag och bindande överenskommelser kan garantera en tillräcklig skyddsnivå i mottagarlandet. Punkten 4 anger när kravet på tillräcklig skyddsnivå kan efterges: bland annat om det föreligger ett berättigat och angeläget allmänintresse med överföringen som följer av lag och utgör en nödvändig och proportionerlig åtgärd i ett demokratiskt samhälle. Den femte punkten föreskriver att en tillsynsmyndighet ska underrättas om alla överföringar som sker med stöd av bindande överenskommelser, och på förfrågan ska ha möjlighet att granska även överföringar som sker med stöd av den enskildes intresse eller ett legitimt intresse. Den sjätte och sista punkten i artikeln innebär att den personuppgiftsansvariga ska kunna visa effektiviteten av dataskyddet hos mottagaren eller att det föreligger ett legitimt intresse med överföringen. Tillsynsmyndigheten ska även ha befogenhet att förbjuda, upphäva eller föreskriva villkor för överföringar i syfte att skydda de registrerades grundläggande fri- och rättigheter.

Konventionen medger endast att undantag görs från punkterna 5 och 6 i artikeln och endast sådana undantag som gäller behandling som sker för nationell säkerhet eller försvar.

Även den nu gällande dataskyddskonventionen 108 innehåller i artikel 12 regler som delvis motsvarar de som ska gälla enligt tilläggsprotokollet.

Nuvarande reglering

Säpodatalagen har, som nämnt i bland annat avsnitt 3.5.1, en nära koppling till brottsdatadirektivet och EU-rätten. Det innebär att överföringar inom EU regleras i enlighet i brottsdatadirektivets intentioner om en harmoniserad lagstiftning med en adekvat skyddsnivå inom hela unionen. Vid sidan av de sekretessbrytande bestämmelserna i 2 kap. 16 § säpodatalagen saknas därför närmare bestämmelser som rör överföring av uppgifter till myndigheter inom EU. Säkerhetspolisen får överföra personuppgifter till Europol, polismyndigheter och underrättelse- eller säkerhetstjänster inom EU utan hinder av vare sig sekretess eller några särskilda krav för personuppgiftsskydd.

Enligt regeringen var en reglering som innebär högre krav för överföringar till stater som inte är medlemmar i EU eller anslutna till EES-samarbetet viktig ur integritetssynpunkt, eftersom samma skydd inte kan garanteras för personuppgifterna i sådana stater. Regeringen ansåg att brottsdatalagens bestämmelser kunde tas som utgångspunkt. Regleringen blev därmed betydligt utförligare än tidigare men medgav, enligt regeringen, större möjligheter att överföra personuppgifter än enligt den tidigare lagstiftningen.[186]

Reglerna om överföringar av personuppgifter till tredje land och till internationella organisationer återfinns i 9 kap. säpodatalagen och är delvis likalydande med brottsdatalagens motsvarande bestämmelser. Av 9 kap. 1 § följer förutsättningarna för att Säkerhetspolisen ska få överföra personuppgifter till mottagare i tredjeland eller en internationell organisation. Mottagaren ska vara antingen en brottsbekämpande myndighet, en underrättelse- eller säkerhetstjänst eller en internationell organisation med brottsbekämpande uppdrag. Vidare ska mottagaren omfattas av ett beslut från EU-kommissionen om adekvat skyddsnivå (9 kap. 2 §) alternativt ska mottagaren genom ett avtal eller på annat sätt kunna garantera att

[186] Ibid. s. 192 f.

personuppgifterna kommer att omfattas av tillräckliga skyddsåtgärder hos den som mottar dem (9 kap. 3 §).

Det finns även, i 9 kap. 4 § säpodatalagen, ett undantag från kraven om att uppgifter som överförs till tredjeland ska ha tillräckligt dataskydd hos mottagaren. Kravet är då att det ska vara fråga om de i paragrafen uppräknade situationerna. De särskilda situationerna avser bland annat en möjlighet att överföra uppgifter för att avvärja en omedelbar och allvarlig fara för allmän säkerhet i Sverige eller i det tredje landet.

I enskilda fall kan överföringar även göras, om det behövs för brottsbekämpande syften eller för att fastställa, göra gällande eller försvara ett rättsligt anspråk. Sådana överföringar får dock endast ske efter en intresseavvägning. Om den registrerades intresse av skydd mot kränkning av rättigheter och friheter väger tyngre än det allmännas, får personuppgifterna inte överföras. Ett exempel där den registrerades intresse förstås väger tyngre är om han eller hon riskerar dödsstraff, kroppsstraff eller tortyr om hans eller hennes personuppgifter överförs till ett tredjeland.

I 9 kap. 1–4 §§ säpodatalagen regleras överföringar till brottsbekämpande myndigheter och vissa andra offentliga eller mellanstatliga organ. I enskilda fall får Säkerhetspolisen även överföra personuppgifter till andra. Sådana överföringar regleras i 9 kap. 5 §. Det kan röra sig om att Säkerhetspolisen behöver uppgifter från ett privat företag som exempelvis en social mediaplattform, en meddelandetjänst eller ett flygbolag. Det kan även finnas behov av att överföra uppgifter till andra myndigheter än de brottsbekämpande, som exempelvis en utländsk folkbokföringsmyndighet. Det tål att påminna sig om att en förfrågan om en person som syftar till att få uppgifter samtidigt innebär att dennes personuppgifter, exempelvis namn eller annan identitetsuppgift, överförs. En överföring till annan mottagare än de typiska är dock omgärdad av flera skyddsmekanismer. Till att börja med ska överföringen vara absolut nödvändig för att Säkerhetspolisen ska kunna utföra en uppgift. Vidare ska det vara ineffektivt eller olämpligt att överföra uppgifterna till en av de ordinarie mottagarna, som en brottsbekämpande myndighet eller en säkerhetstjänst. Det innebär att överföringen i princip inte ska kunna underlåtas och syftet med överföringen kan komma att förfelas om Säkerhetspolisen väljer den normala informationsvägen. Ett exempel är att det finns ett tidskritiskt behov av en viss

uppgift eller åtgärd och det kan förutses att det inte kommer kunna ske tillräckligt snabbt om den kontaktvägen väljs.

I likhet med vissa överföringar till länder utan tillräckligt personuppgiftsskydd får även överföringar till andra mottagare endast ske efter en intresseavvägning mellan den registrerades intresse av skydd mot fri- och rättighetskränkningar och det allmänna intresset av överföringen.

Försvarsmaktens och FRA:s regelverk

Försvarsmaktens och FRA:s respektive personuppgiftslagstiftning tar inte hänsyn till om en personuppgiftsöverföring sker inom eller utom EU. I avsnitt 7.1.1 har vi redogjort för att det finns skäl att frångå det EU-rättsliga regelverket och i högre grad än tidigare harmonisera Säkerhetspolisens lagstiftning i materiellt avseende med i första hand det som gäller för den militära underrättelse- och säkerhetstjänsten. Det finns därför skäl att redogöra särskilt för hur frågan om överföring till mottagare utomlands har reglerats i försvarsdatalagen respektive FRA-datalagen.

Försvarsmakten får, enligt 2 kap. 22 § försvarsdatalagen, föra över personuppgifter till ett annat land eller en internationell organisation endast om sekretess inte hindrar det och det är nödvändigt för att Försvarsmakten ska kunna fullgöra sina uppgifter inom ramen för det internationella försvars- och säkerhetssamarbetet. Regeringen kan i förordning även föreskriva om att överföring får ske även i andra fall, om det är nödvändigt för verksamheten vid Försvarsmakten. Inom begreppet försvars- och säkerhetssamarbete ingår bland annat Försvarsmaktens försvarsunderrättelsesamarbete med andra länder.

I förarbetena förklaras att huruvida en överföring av personuppgifter ska ske eller inte i sin helhet måste avgöras efter en sekretessprövning och försvars- och säkerhetspolitiska överväganden.[187] Något uttryckligt krav på mottagarens skydd för personuppgifter finns därmed inte.

För FRA finns mer detaljerade krav för överföringar av personuppgifter. Enligt 2 kap. 20 § FRA-datalagen får personuppgifter föras över till ett annat land eller en internationell organisation, om

[187] Prop. 2020/21:224 s. 187.

det är nödvändigt för att Försvarets radioanstalt ska kunna fullgöra sina uppgifter inom ramen för det internationella försvarsunderrättelse- och säkerhetssamarbetet. Överföringen ska riktas till en utländsk underrättelse- eller säkerhetstjänst eller till ett underrättelse- eller säkerhetsorgan i en internationell organisation. Vidare får inte sekretess hindra överföringen och mottagaren måste garantera ett tillräckligt skydd för personuppgifterna. Slutligen får överföringen inte innebär ett oproportionerligt intrång i den registrerades personliga integritet. Det sistnämnda kravet trädde i kraft den 1 juli 2024 och är föranlett av den kritik som riktats mot Sverige av Europadomstolen i målet *Centrum för rättvis mot Sverige*.[188]

EU-samarbetet och EU-rätten bör inte påverka överföringar utomlands

EU garanterar inte grundläggande fri- och rättigheter för personuppgifter som behandlas för nationell säkerhet

Nuvarande reglering av överföringar av uppgifter utomlands innebär att högre krav för överföringar till stater som inte är medlemmar i EU eller anslutna till EES-samarbetet. Det ansågs viktig ur integritetssynpunkt, eftersom det inte kan garanteras samma skydd för personuppgifterna i sådana stater. Vi har i avsnitt 7.1.1 behandlat frågan om hur Säkerhetspolisens verksamhet förhåller sig till EU-samarbetet och EU-rätten. Utgångspunkten är att i synnerhet den nationella säkerheten ska vara varje medlemsstats eget ansvar och att Sverige därför bör reglera Säkerhetspolisen behandling av personuppgifter utifrån nationella överväganden och med beaktande av Europakonventionen och dataskyddskonventionen.

Eftersom EU-rätten har ett begränsat inflytande över frågor som rör nationell säkerhet, kan det även ifrågasättas om EU-samarbetet utgör en relevant grund för att bedöma integritetsskyddet för personuppgifter som behandlas i sådan verksamhet. Flera av EU:s medlemsstater reglerar personuppgiftsbehandling för nationell säkerhet enligt regelverk som är helt skilda från EU-rätten. Någon gemensam skyddsnivå finns alltså inte på området nationell säkerhet. Det finns därför ingen anledning att dela upp länder på sätt som gjort i säpodatalagen. Begreppet tredje land bör därför inte an-

[188] Prop. 2023/24:136.

vändas och regler om överföring bör tillämpas även för medlemsstater i EU och EES. Däremot är det förstås sannolikt så att EU-länder och andra demokratiska rättsstater kan garantera tillräckligt skydd för personuppgifter.

EU-kommissionens beslut om adekvat skyddsnivå avser inte behandling för nationell säkerhet

Som en följd av att nuvarande lagstiftning överfört vissa av brottsdatalagens bestämmelser om överföring av personuppgifter har EU-kommissionens beslut om adekvat skyddsnivå fått betydelse även inom området nationell säkerhet (9 kap. 2 § säpodatalagen).

Det kan konstateras att EU inte är behöriga att besluta om frågor som rör nationell säkerhet och att det därför kan finnas principiella betänkligheter mot att låta EU-kommissionens bedömning av adekvat skyddsnivå vara bindande i detta avseende. Skyddsnivån i ett beslut från kommissionen bygger också på den generella dataskyddsförordningen tillämpningsområde och tar inte hänsyn till de särskilda ändamål som kan föranleda en överföring för nationell säkerhet. Det framstår inte som lämpligt att behålla reglerna om att EU-kommissionens beslut om adekvat skyddsnivå ska få påverkan på Säkerhetspolisens möjlighet att överföra personuppgifter. EU-kommissionens rättsliga ställningstagande i detta avseende kan dock sannolikt tjäna som en del av utredningen om en mottagare kan garantera tillräcklig skyddsnivå för personuppgifter som överförs.

Mellanfolklig, mellanstatlig eller internationell organisation?

I det regelkomplex som Säkerhetspolisen i dag har att förhålla sig till när det gäller internationellt samarbete förekommer olika begrepp. I säpodatalagen 1 kap. 5 § definieras *internationell organisation* som en organisation och dess underställda organ som lyder under folkrätten eller ett annat organ som inrättats genom eller på grundval av en överenskommelse mellan två eller flera stater. Begreppet används huvudsakligen i 9 kap. som rör överföring av personuppgifter till tredje land och internationella organisationer.

I 2 kap. 4 § regleras sekundära ändamålsbestämmelser och i 16 § de sekretessbrytande bestämmelserna. I dessa paragrafer, som gäller

bland annat Interpol, Europol, används begreppet mellanfolklig organisation. Vad som avses med en mellanfolklig organisation eller om en sådan skiljer sig från en internationell organisation anges inte i lag eller förarbeten. 2 kap. 16 § avser att bryta den sekretess som följer av 8 kap. 3 § offentlighets- och sekretesslagen, där begreppet mellanfolklig organisation används. Begreppet används även i 16 § i Säkerhetspolisen instruktion angående internationellt samarbete Mellanfolklig organisation används även i bland annat 10 kap. 1 § regeringsformen. Där anges att överenskommelser med andra stater eller med mellanfolkliga organisationer ingås av regeringen. Enligt förarbetena avses med mellanfolkliga organisationer endast sådana organisationer som är rättssubjekt enligt folkrätten.[189]

I exempelvis terroristbrottslagen förekommer även begreppet *mellanstatlig organisation*. Lagen bygger på EU:s rambeslutet om bekämpande av terrorism, som i sin svenska översättning emellertid använder begreppet internationell organisation. Regeringen ansåg att begreppet mellanstatlig organisation bättre beskrev sådana internationella organisationer som är rättssubjekt enligt folkrätten och som förtjänar samma skydd som enskilda stater, som FN, EU eller Europarådet.[190]

Det saknas såvitt känt någon betydelseskillnad mellan begreppet internationell organisation, enligt definitionen i säpodatalagen och begreppet mellanfolklig organisation. Eftersom mellanfolklig organisation är det begrepp som används i regeringsformen och i offentlighets- och sekretesslagen bör det genomgående användas i säpodatalagen. Det finns ingen anledning att definiera begreppet i den lagen eftersom det måste förutsättas ha samma betydelse som i bland annat regeringsformen.

Alla överföringar ska vara proportionerliga

Till skillnad mot den nuvarande lagstiftningen bygger vårt förslag på att all personuppgiftsbehandling ska vara proportionerlig. Den särskilda proportionalitetsprövningen som enligt den nuvarande lagen ska göras inför vissa överföringar, där mottagaren inte är en

[189] Prop. 1973:90 s. 357.
[190] Prop. 2002/03:38 s. 34 och 83.

utpekad myndighet eller då tillräckligt skydd för personuppgifter saknas, gäller enligt vårt förslag alla överföringar.

Det kan många gånger vara särskilt angeläget med en sådan prövning just när personuppgifter ska föras över till en mottagare i annat land. Kontrollen över hur personuppgifterna kommer att behandlas blir mindre och i många fall är det svårt att följa upp. Det rättighetsintrång och andra enskilda intressen som en gång bedömts avseende Säkerhetspolisens behandling av personuppgifterna i fråga är inte nödvändigtvis desamma som då uppgifterna behandlas av mottagare utomlands. Hur känsliga personuppgifter är varierar mycket beroende på i vilken kontext uppgifterna behandlas. En uppgift som avslöjar sexuell läggning kan exempelvis vara avsevärt mycket mer känslig i länder där homosexualitet är kriminaliserat eller där straffrihet råder för förföljelse än vad uppgiften är i Sverige. Detsamma gäller de flesta andra känsliga personuppgifterna som religiös eller filosofisk övertygelse eller politiska åsikter.

Redan spridning av en uppgift till en myndighet eller annan mottagare i ett annat land får också anses utgöra ett intrång i rätten till privatliv. Det finns därför en högre tröskel för att överföra uppgifter till andra länder än att behandla dem i Sverige. Skälen som talar för en överföring behöver därför ofta vara starka. Det finns givetvis andra skäl till att informationsöverföringar inte görs lättvindigt som grundas på bland annat säkerhetspolitiskas överväganden och frågor som rör säkerhetsskydd avseende den egna myndigheten och dess förmågor. Det är dock angeläget att poängtera att en proportionalitetsprövning av en personuppgiftsöverföring måste utgå från integritetsintrånget, som ska tillmätas självständig betydelse.

Givetvis kommer ändamålet med en överföring av personuppgifter att påverka prövningen. En överföring kan vara nödvändig för att lösa uppgifter i Sverige, exempelvis genom att en förfrågan om en person ställs till en samverkande tjänst eller genom att Säkerhetspolisen ber att få uppgifter om en person från sociala mediaplattformer. Ändamålet kan då vägas mot intrånget på samma sätt som vid annan behandling. När överföring av personuppgifter sker för att mottagaren ska kunna lösa en uppgift i sin verksamhet, blir prövningen ofta svårare. En motsvarande prövning kan ske om Säkerhetspolisen har tillräcklig kännedom om för vilket ändamål mottagaren ska behandla uppgifterna och övriga omständigheter. I andra fall, då ändamålet och syftet är mer vagt formulerat kan prövningen vara

svårare att genomföra, eftersom vagt och brett formulerade ändamål inte kan motivera ett lika stort intrång i den registrerades intressen (se avsnitt 8.2.4).

Mottagare i andra länder

Systematiskt utbyte med myndigheter och mellanfolkliga organisationer bör förtydligas

Enligt 8 kap. 3 § 1 offentlighets- och sekretesslagen bryts sekretessen i förhållande till utländska myndigheter och mellanfolkliga organisationer om utlämnade sker i enlighet med särskild föreskrift i lag eller förordning.

I dag anges, i 2 kap. 16 § säpodatalagen, att Säkerhetspolisen får lämna ut personuppgifter till Interpol eller Europol, eller till en polismyndighet eller åklagarmyndighet i en stat som är ansluten till Interpol, om det behövs för brottsbekämpande verksamhet hos mottagaren. Vidare anges att uppgifter får lämnas till en utländsk underrättelse- eller säkerhetstjänst. Det finns inte något krav på att den mottagande tjänsten, i likhet med Säkerhetspolisen, ska ha ett uttryckligt brottsbekämpande uppdrag. Slutligen anges att personuppgifter får lämnas ut till en utländsk myndighet eller mellanfolklig organisation, om utlämnandet följer av en internationell överenskommelse som Sverige har tillträtt efter riksdagens godkännande. Syftet med bestämmelsen är att bryta sekretessen på sätt som anges i 8 kap. 3 § 1 offentlighets- och sekretesslagen. Dessa regler har överförts från tidigare polisdatalag.

I 9 kap. 1 § säpodatalagen finns dock ytterligare en särskild föreskrift som anger att Säkerhetspolisen under vissa förutsättningar får överföra personuppgifter till vissa mottagare i ett tredjeland eller till en internationell organisation. Dessa regler följer av brottsdatadirektivet och liknar de som finns i brottsdatalagen. Även bestämmelserna i nuvarande 9 kap., som omfattar alla internationella organisationer med brottsbekämpande uppdrag (inte endast Europol, Interpol) och alla brottsbekämpande myndigheter (inte endast polismyndigheter och åklagarmyndigheter i en stat ansluten till Interpol), är formulerade så att de också bryter sekretessen enligt 8 kap. 3 § 1 offentlighets- och sekretesslagen. Överföringar enligt 9 kap. kräver dock att mottagaren ska kunna garantera tillräckligt skydd för personuppgifter.

Något sådant krav följer inte av 2 kap. 16 § säpodatalagen. Bestämmelserna överlappar emellertid varandra och en sådan utländsk myndighet som anges i 2 kap. 16 § kan också omfattas av 9 kap. 1 §, om den mottagande staten är ett tredjeland. Det är därför mycket svårt att se vilken självständig funktion den nuvarande 2 kap. 16 § säpodatalagen spelar. I sammanhanget kan nämnas att Interpol har 196 medlemsländer, vilket innebär att skillnaden mellan de myndigheter som utlämnande kan ske till enligt 2 kap. 16 § och 9 kap. 1 § är försumbar.

Det finns inte något skäl att inom ramen för denna utredning göra andra allmänna överväganden än vad som tidigare gjorts avseende till vilka mottagare som en överföring får ske utan hinder av sekretess. Däremot finns skäl att förtydliga vilka möjligheter som finns för Säkerhetspolisen att överföra personuppgifter till andra länder och förenkla regelverket. Eftersom vi anser att Säkerhetspolisens informationsutbyte med medlemsstater i EU och EES inte ska regleras på annat sätt än för tredjeländer bör reglerna kunna sammanföras.

Under vår utredningstid har Sverige har blivit medlem av Nato. Inom den organisationen finns ett underrättelse- och säkerhetssamarbete där Säkerhetspolisen numera ingår. Det bör därför förtydligas att ett systematiskt informationsutbyte ska få ske även inom ramen för detta samarbete. Det bör formuleras på liknande sätt som i 2 kap. 20 § FRA-datalagen där det anges att en överföring får ske till underrättelse- eller säkerhetsorgan i en internationell organisation.

Av säpodatalagen följer att Säkerhetspolisen får *behandla* personuppgifter för brottsbekämpande verksamhet hos en utländsk myndighet eller mellanfolklig organisation, eller i verksamhet hos utländsk underrättelse- eller säkerhetstjänst (se avsnitt 8.23.1 ovan). De uppgifter som får behandlas får i dag också som huvudregel *utlämnas* till alla brottsbekämpande myndigheter och underrättelse- och säkerhetstjänster i länder som antingen genom EU- eller EES-medlemskap presumeras ha tillräckligt dataskydd, eller till tredjeländer som på annat sätt kan garantera detta. Dessutom får personuppgifter delas med mellanfolkliga organisationer som har ett brottsbekämpande uppdrag eller om utlämnandet följer av en internationell överenskommelse som Sverige har tillträtt efter riksdagens godkännande.

Sammanfattningsvis kan konstateras att den nuvarande huvudregeln inte sätter upp några sekretesshinder för uppgiftsutlämnande till de mottagare som Säkerhetspolisen kan förväntas ha ett infor-

mationsutbyte. Däremot framstår det som något inkonsekvent att sekretessen brutits i förhållande till myndigheter som inte har ett brottsbekämpande uppdrag och som Säkerhetspolisen i enskilda fall får överföra uppgifter till. Uppgifter får lämnas till sådana myndigheter i enskilda fall enligt nuvarande 9 kap. 5 §. Om förutsättningarna i övrigt är uppfyllda krävs ingen sekretessprövning. Det framstår också som inkonsekvent att ställa upp ett krav på att utlämnade ska vara förenligt med svenska intressen enbart för de mottagare anges i 2 kap. 16 § men inte de som anges i 9 kap. 1 och 5 § säpodatalagen.

Vad som avses med begreppet *svenska intressen* är inte heller klart. Begreppet kommer från 8 kap. 3 § 2, som reglerar utlämnanden som inte sker med stöd av en (sekretessbrytande) särskild föreskrift. Enligt denna bestämmelse får uppgifter lämnas ut om den i motsvarande fall skulle få lämnas ut till en svensk myndighet och det enligt den utlämnande myndighetens prövning står klart att utlämnandet är förenligt med svenska intressen. Eftersom svenska intressen ska beaktas enligt just en sådan sekretessbrytande särskild föreskrift som anges i 8 kap. 3 § 1, får det antas att kravet ansetts nödvändigt att behålla, men att det inte ska motsvara en sekretessprövning. I begreppet svenska intressen ingår dock, enligt ett uttalande från Säkerhets- och integritetsskyddsnämnden, en avvägning mellan Säkerhetspolisens behov av att lämna uppgifter och sekretessintresset, exempelvis det integritetsintrång och de konsekvenser som detta kan innebära för den enskilde.[191]

Den brottslighet som Säkerhetspolisen har till uppgift att förebygga och avslöja är i många fall gränsöverskridande till sin natur och utlämnade av information för att förebygga brott mot nationell säkerhet eller terrorbrott med andra länder lär sällan vara oförenligt med svenska intressen. Sekretessintresset för enskilda kommer enligt vårt förslag i stor utsträckning beaktas genom den proportionalitetsprövning som har en motsvarande funktion. Begreppet svenska intressen antyder dock även att en säkerhetspolitisk avvägning ska göras, exempelvis genom hänsyn till reciprocitet i underrättelsesamarbetet som sker mellan allierade. Det kan därför finnas skäl att begreppet ska kvarstå, för en bestämmelse som avser att bryta sekretessen i förhållande till utländska myndigheter enligt 8 kap. 3 § offentlighets- och sekretesslagen.

[191] Se Säkerhets- och integritetsskyddsnämndens uttalande den 22 maj 2013 i ärende dnr 2005-2012, s. 3 med hänvisning till prop. 1981/82:186 s. 59.

Skyddsnivån för personuppgifter måste garanteras för systematiskt informationsutbyte

För en stor del av de utlämnanden som sker i dag krävs inte någon sekretessprövning men däremot krävs att mottagaren garanterar ett tillräckligt dataskydd. Säpodatalagen har utgångspunkten att alla EU:s och EES:s medlemsstater har en tillräckligt hög skyddsnivå och att någon individuell prövning inte behöver göras. Att ta bort hinder för utbyte av personuppgifter mellan medlemsstater är ett av brottsdatadirektivets syften. Av brottsdatalagen följer därför att någon prövning om skydd för personuppgifter inte får göras om överföring sker till en annan medlemsstat (se 2 kap. 20 § brottsdatalagen). Det finns dock ingen nu gällande rättsakt inom EU eller EES som på samma sätt garanterar att medlemsstater upprätthåller en tillräcklig skyddsnivå för personuppgifter som behandlas för nationell säkerhet. Trots detta finns det endast krav angående så kallade tredje länders skyddsnivå i säpodatalagen. För tredjeländer krävs ett beslut om adekvat skyddsnivå, tillräckliga skyddsåtgärder eller ett undantag för särskilda situationer (9 kap. 2 och 3 §§ säpodatalagen).

Som framgått ovan är vår bedömning att tillräckliga skyddsåtgärder för personuppgifter ska bedömas i en nationell säkerhetskontext och inte av EU-kommissionen. Det bör därför vara Säkerhetspolisen som ska bedöma om mottagare kan garantera tillräcklig skyddsnivå. Sverige är, i likhet med alla EU:s och EES:s medlemsstater, i dag bundet av dataskyddskonventionen 108, som i de flesta fall utgör en garanti för tillräckligt skydd. Konventionen anger, i artikel 12.2, att de stater som är ansluta till konventionen inte ska uppställa hinder för överföringar endast motiverade av skyddet för personuppgifter. Enligt sin artikel 3.2 a kan vissa kategorier av personuppgifter undantas från konventionens tillämpningsområde, exempelvis de som rör brottsbekämpning. Det kan därför finnas anledning att studera huruvida en medlemsstat gjort undantag från konventionens bestämmelser avseende uppgifter som behandlas hos mottagaren. Om några undantag inte gjorts bör en tillräcklig skyddsnivå anses föreligga. Den moderniserade dataskyddskonventionen 108+ innehåller grundläggande principer för dataskydd som inte är möjliga att undanta behandling som sker för nationell säkerhet. Den moderniserade konventionen innebär därför att även nationella säkerhets-

tjänster eller brottsbekämpande myndigheters personuppgiftsbehandling bland annat måste vara rättsligt grundad och proportionerlig.

För länder som inte tillträtt dataskyddskonventionen får en tillräckligt skydd för personuppgifter antingen bedömas utifrån nationell lagsstiftning (eller regler för den mellanfolkliga organisationen) eller genom avtal eller andra bindande rättsliga instrument för mottagaren. Ett avtal kan vara en del av ett villkor vid överföring av personuppgifter i det enskilda fallet eller utgöra en del av standardiserat avtal.

Skyddet för personuppgifter måste vara effektivt och bindande för mottagaren. Se artikel 14.3 i dataskyddskonventionen 108+ och det tilläggsprotokoll till dataskyddskonventionen 108 (ETS 181), som Sverige har tillträtt. Säkerhetspolisen bör i samma utsträckning som i dag även kunna beakta att den som ska behandla personuppgifterna kommer att ha tystnadsplikt som omfattar de överförda uppgifterna eller att det garanteras att personuppgifterna inte kommer att behandlas för något annat ändamål än det för vilket de överförs. Även bindande åtaganden om att inte föra personuppgifterna vidare eller att inte använda personuppgifterna efter en viss tidpunkt bör kunna beaktas. Det innebär att uppställande av den så kallade tredjepartsregeln bör kunna ge ett tillräckligt skydd för personuppgifterna.

Informationsutbyte mellan underrättelse- och säkerhetstjänster bygger i stor utsträckning på förtroende. Om en underrättelse- eller säkerhetstjänst missbrukar förtroendet, blir konsekvensen att den inte längre kommer att få del av relevant information i samma utsträckning som andra. Det har en självreglerande effekt genom att den mottagande myndigheten måste garantera tillräckligt skydd för uppgifterna för att kunna få del av dem.[192]

Mer ändamålsenliga regler för internationellt informationsutbyte

Mot bakgrund av det ovanstående lämnar vi förslag om att Säkerhetspolisen ska kunna dela personuppgifter i huvudsak med samma mottagare som i dag. Därutöver ska det av lagen framgå att Säkerhetspolisen kan dela information inom Natos underrättelse- och säkerhetssamarbete. Eftersom vi har uppfattningen att Säkerhetspolisens personuppgiftsbehandling som avser informationsdelning är en del av Sveriges exklusiva nationella lagstiftningskompetens ska inte

[192] Prop. 2018/19:163 s. 197.

någon åtskillnad göras mellan medlemsstater i EU eller EES och tredjeländer.

För ett systematiskt informationsutbyte krävs att mottagaren ska kunna garantera tillräckligt skydd för personuppgifter. Det kan ske bland annat genom att dataskyddskonventionen 108+ trätt i kraft i förhållande till mottagarlandet eller på annat sätt. Sekretess hindrar inte systematisk överföring men likt i dag ska en prövning göras om överföringen är förenligt med svenska intressen.

I enskilda fall bör överföringar få ske även utan att skyddsnivån kan garanteras men proportionalitetskravet bör då skärpas

Nuvarande 9 kap. 4 § säpodatalagen innebär att personuppgifter i särskilda fall får överföras utomlands även om det saknas tillräckliga garantier för mottagarens skydd av personuppgifter. De särskilda fall som räknas upp avser den registrerades eller annan persons vitala eller berättigade intressen (1) och för att avvärja en omedelbar och allvarlig fara för allmän säkerhet (4). I enskilda fall får överföringar göras för att bekämpa brott (2) eller för ett fastställa, göra gällande eller försvara ett rättsligt anspråk (3). I dessa fall ska en prövning göras om den registrerades intresse av skydd mot kränkning av rättigheter och friheter väger tyngre än det allmännas intresse av en sådan överföring. Bestämmelsen har en EU-rättslig förebild och motsvaras av 8 kap. 5 § brottsdatalagen.

Dataskyddskonventionen 108+ tillåter under vissa villkor även överföringar till mottagare som inte kan garantera tillräckligt skydd för personuppgifter. Enligt artikel 14.4 finns möjlighet till sådana överföringar om den registrerade har lämnat informerat samtycke (a), om det krävs för att tillgodose den enskildas konkreta behov i ett enskilt fall (b) eller om det utgör en nödvändig och proportionerlig åtgärd för yttrandefriheten i ett demokratiskt samhälle (d). I punkten 4 c anges det för Säkerhetspolisen mest relevanta skälet för en sådan överföring: om det föreligger ett angeläget och befogat allmänt intresse och en sådan överföring utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle.

De nuvarande undantagen i säpodatalagen är förenliga med konventionsbestämmelserna, men är inte utformade specifikt efter Säkerhetspolisens verksamhet. Tillsammans med den proportiona-

litetsprövning som ska ske för alla behandlingar bör undantagen kunna utformas mer generellt.

För att kompensera risken för brist på skydd för personuppgifter hos mottagaren bör en prövning göras där skälen för att överföra uppgifterna med råge måste överväga integritetsintrånget och risken för kränkningar hos mottagaren. Vi föreslår att det ska krävas att skälet för att lämna ut uppgifterna *uppenbart* överväger intrånget i de enskilda eller allmänna intressen som kan påverkas av den. Sådana överföringar bör dock endast ske i enstaka fall, och inte avse systematisk informationsdelning. Det finns aldrig någon skyldighet för Säkerhetspolisen att lämna ut uppgifter till andra länder. Det faller sig därför naturligt, med hänsyn till att ändamålet uppenbart måste väga över intrånget, att sådana överföringar främst kommer ske för Säkerhetspolisens intressen eller i särskilt angelägna fall.

Den nuvarande lagen lämnar inte någon anvisning om huruvida avsikten varit att bestämmelserna i 9 kap. 4 § skulle vara sekretessbrytande avseende utländska myndigheter. Eftersom det rör sig om ett utlämnande i enlighet med särskild föreskrift bryter dock bestämmelsen formellt sekretessen enligt 8 kap. 3 § 1 offentlighets- och sekretesslagen.

Det går att ifrågasätta om det är lämpligt att ett utlämnande, som inte skulle fått ske till en svensk myndighet, får ske till en myndighet som inte kan garantera bland annat konfidentialitet för uppgifterna. Det framstår som rimligt och förväntat att kraven ska vara högre för ett sådant utlämnade än för motsvarande utlämnade inom landets gränser. Vi anser därför att det uttryckligen ska anges att bestämmelsen om utlämnanden i enskilda fall inte ska bryta sekretessen. Därmed får uppgiften lämnas ut till utländska myndigheter och mellanfolkliga organisationer enligt kraven i 8 kap. 3 § 2 offentlighets- och sekretesslagen. Enligt denna bestämmelse får en uppgift lämnas ut om den i motsvarande fall skulle få lämnas ut till en svensk myndighet och det enligt den utlämnande myndighetens prövning står klart att det är förenligt med svenska intressen att uppgiften lämnas till den utländska myndigheten eller den mellanfolkliga organisationen.

Vi föreslår en lagreglering med denna innebörd.

I enskilda fall får överföringar ske även till andra mottagare än myndigheter och mellanfolkliga organisationer

Behovet av att direkt överföra personuppgifter till mottagare i andra länder som inte är brottsbekämpande myndigheter eller en underrättelse- eller säkerhetstjänst har ökat som en följd av globaliseringen. Det kan vara nödvändigt att gör förfrågningar om personer till olika sociala mediaplattformar eller andra tjänsteleverantörer som befinner sig i andra länder. Vi anser att dagens möjligheter bör finnas kvar.

Den nuvarande regleringen anger att en överföring till en annan mottagare än en brottsbekämpande myndighet eller en underrättelse- eller säkerhetstjänst i det tredjelandet ska vara absolut nödvändigt för att Säkerhetspolisen ska kunna utföra en uppgift. Vidare krävs att det skulle vara ineffektivt eller olämpligt att i stället överföra uppgiften till en brottsbekämpande myndighet eller en underrättelse- eller säkerhetstjänst i tredjelandet. Slutligen krävs att den registrerades intresse av skydd mot kränkning av rättigheter och friheter inte väger tyngre än det allmännas intresse av att överföringen görs.

I likhet med vad vi föreslår om överföringar till mottagare som inte kan garantera tillräckligt skydd för personuppgifter anser vi att det endast bör få ske i enskilda fall. Det skärpta proportionalitetskravet bör också gälla. Det ska måste alltså vara uppenbart att det allmänna intresset av överföringen väger tyngre de andra intressen som kan påverkas.

Riskerna med överföringar till andra mottagare är svårbedömda och det framstår som uteslutet att det skulle ske överföringar i annat intresse än Säkerhetspolisens. Intresset av att överföra personuppgifter måste vara särskilt angeläget om det rör sig både om en mottagare som inte kan garantera tillräckligt personuppgiftsskydd och om är ett privat subjekt eller annan myndighet som inte kan garantera krav på informationssäkerhet.

Enligt 8 kap. 1 § offentlighets- och sekretesslagen får en uppgift för vilken sekretess gäller inte röjas för enskilda. Enskilda utgörs av fysiska eller juridiska personer utanför den offentliga sektorn, oavsett om de befinner sig inom eller utom landet. Eftersom bestämmelsen endast ger en möjlighet men inte en skyldighet att lämna ut uppgifter bryter den inte sekretess i förhållande till privata subjekt. Bestämmelsen bör formuleras på så sätt att den inte bryter sekretessen i för-

hållande till utländska myndigheter enligt 8 kap. 3 § 1 offentlighets- och sekretesslagen. En myndighet som inte har ett brottsbekämpande uppdrag bör inte behandlas på annat sätt än en motsvarande svensk myndighet.

Direktåtkomst för utländska underrättelse- och säkerhetstjänster

Enligt 3 kap. 7 § säpodatalagen får vissa europeiska underrättelse- eller säkerhetstjänst medges direktåtkomst för de personuppgifter som behövs för att bekämpa terroristbrott. Denna utredning har inte haft till uppdrag att göra några närmare överväganden i denna fråga som var föremål för översyn så sent som år 2023.[193]

Motsvarande möjlighet till direktåtkomst bör införas i den föreslagna lagen. Direktåtkomsten anger endast sättet för utlämnade. Övriga bestämmelser ska vara uppfyllda för att direktåtkomst ska medges. Det innebär bland annat att samtliga underrättelse- eller säkerhetstjänster som medges sådan åtkomst måste kunna garantera tillräckligt skydd för personuppgifter.

Givetvis påverkas proportionalitetsprövningen av att personuppgifter görs tillgängliga på detta sätt. Integritetsrisken är påtaglig för uppgifter som andra länders säkerhetstjänster har tillgång till. Ändamålet är, enligt nuvarande bestämmelse, samarbetet mot terrorism som är ett tungt vägande allmänintresse. Vår uppfattning är att den nuvarande omfattningen av direktåtkomsten är proportionerlig.

[193] Prop. 2022/23:116.

9 En ny lag för Säkerhetspolisens behandling av stora informationsmängder

9.1 Principerna bakom förslaget

9.1.1 En särskild lag

Vi har i avsnitt 7.2 redogjort för bakgrunden till att vi föreslår att Säkerhetspolisen ska få en ny förmåga att behandla stora informationsmängder. Denna förmåga utgörs av en särskild form av personuppgiftsbehandling. För att uppnå lagens syften krävs nämligen undantag från flera av de principer som gäller för annan behandling enligt dataskyddskonventionen 108+. Sådana undantag är möjliga att göra i Säkerhetspolisens verksamhet som rör det mycket angelägna allmänna intresset nationell säkerhet. Vi har i avsnitt 7.2.2 redogjort för varför vi tycker att sådana undantag också är nödvändiga och proportionerliga i ett demokratiskt samhälle.

Vi anser att dessa undantag bör regleras i en egen lag som kompletterar, och i delar ersätter, säpodatalagens generella regler. Vi uppfattar också att en egen lag ger en bättre överblick och underlättar hänvisningar eller framtida ändringar än om motsvarande reglering skulle föras in i ett eget kapitel i säpodatalagen.

9.1.2 En europarättslig utgångspunkt

Europadomstolens praxis angående signalspaning kan ge vägledning

Vi har inte kunnat hitta någon auktoritativ vägledning när det gäller hur behandling av stora mängder personuppgifter i syfte att skydda nationell säkerhet bör regleras för att vara förenlig med Europakonventionen och dataskyddskonventionen 108+. Det finns dock andra, mer eller mindre likartade situationer, som bedömts av Europadomstolen. Vi anser att viss vägledning kan hämtas från sådana avgöranden.

Det finns enligt vår bedömning en stor skillnad mellan att personuppgifter förekommer i ett material som en säkerhetstjänst har tillgång till jämfört med att myndigheten behandlar personuppgifter genom att samla in och sammanställa dem på individnivå. I det senare fallet kan förekomsten av det som kan betecknas som en personakt utgöra ett intrång i rätten till privatliv, vilket inte alls är lika framträdande för uppgifter som endast förekommer, bland många andra, i ett större material. I de fall där Europadomstolen konstaterat att artikel 8 har kränkts har det rört sig om registreringar i strukturerade databaser eller att uppgifter förekommer i en personakt. Denna skillnad i intrång beroende på hur personuppgifter behandlas har manifesterats i främst de domar som rör signalspaning och hemliga tvångsmedel. Europadomstolen har i sådana fall, under vissa villkor, accepterat att en mycket stor mängd personuppgifter behandlas som till övervägande del rör personer utan anknytning till insamlingsändamålet.

Europadomstolens stora kammare har i målet *Centrum för Rättvisa mot Sverige* prövat den svenska lagstiftningen som rör signalspaning. I avgörandet beskriver Europadomstolen signalspaning som en flerstegsprocess. Det första steget utgörs av datainsamling, där även uppgifter som är ointressanta för ändamålet med insamlingen ingår. I ett andra steg filtreras informationen genom tillämpning av särskilda urvalskriterier, vilka antingen kan vara inriktade på individer (”strong selectors”) eller utgöra mera komplexa sökningar. Den information som på så sätt utvunnits ur den större datamängden analyseras till sitt innehåll för första gången av en analytiker i det tredje steget. Det fjärde steget innebär att myndigheten lagrar de relevanta uppgifterna för att användas i verksamheten genom

exempelvis upprättande av underrättelserapporter. I vissa fall delas dessa uppgifter även till andra underrättelsetjänster, inom eller utom det egna landet.[1]

Enligt domstolen ökar intrånget i enskildas rättigheter enligt artikel 8 allteftersom denna process fortskrider. Kommunikation som inhämtas genom signalspaning i det första steget, för att raderas som irrelevant i nästa steg, innebär enligt domstolen förvisso alltjämt ett intrång i den enskildes rätt till privatliv, men inte ett särskilt påtagligt intrång. Domstolen påpekade även att det är tillräckligt att information om en individs privatliv lagras för att det ska anses utgöra ett intrång enligt artikel 8. Att personuppgifter behandlas automatiserat och inte direkt av människor är inte förmildrande, utan medför tvärtom än högre krav på säkerhetsåtgärder för att förhindra att personuppgifter hanteras i strid med konventionen. Störst krav på säkerhetsåtgärder för att garantera en konventionsenlig hantering av personuppgifterna ställs i slutet av processen då uppgifter om individer analyseras, bearbetas och eventuellt delas.

I målet *Big Brother Watch mot Förenade kungariket* utvecklade domstolen sin syn på stora datamängder som inte inhämtats genom signalspaning av den egna myndigheten. Domstolen ansåg att en underrättelsemyndighet som tar emot uppgifter som efterfrågats från en utländsk partner måste behandla dessa uppgifter som om de vore inhämtade genom signalspaning av den egna myndigheten. Detta ska gälla alla uppgifter som kan vara resultatet av signalspaning, även om det inte står klart att så är fallet.[2] I målet begränsade domstolen sin prövning till signalspaningsinformation från myndigheter i tredjeland som efterfrågats av den egna underrättelsetjänsten. Det finns emellertid anledning att anta att behandling av stora mängder uppgifter även i andra sammanhang förr eller senare kommer att prövas av Europadomstolen.[3]

År 2015 publicerade den så kallade Venedigkommissionen en rapport angående signalspaning. Kommissionen är ett rådgivande

[1] Europadomstolens (stora avdelningen) dom 25 maj 2021, *Centrum för Rättvisa m.fl. mot Sverige*, mål nr 35252/08, p. 239–243.
[2] Europadomstolens dom 25 maj 2021, *Big Brother Watch m.fl. mot Förenade kungariket*, mål nr 58170/13 m.fl., p. 498.
[3] Jfr klagomålet till Europadomstolen i mål, A.L m.fl. mot Frankrike nr 44715/20 och 47930/21, vilka handlar om överföring av uppgifter från EncroChat, där domstolen under beredningen bett svaranden (Frankrike) att argumentera för om det finns skäl att tillämpa motsvarande kriterier som ställts upp för signalspaning vid prövningen. Målet avskrevs i oktober 2024 med hänvisning till att klagandena inte uttömt de nationella rättsmedlen.

organ till bland annat Europarådet och består av oberoende experter på det konstitutionella området. I rapporten sägs bland annat att frågan om huruvida en lagstiftning som tillåter signalspaning passerar gränsen till massövervakning till stor del beror på om tröskeln för att behandla de genom signalspaning insamlade personuppgifterna sätts lågt, vilket ger myndigheten tillgång till informationen.[4] Vi har uppfattningen att detta uttalande har bäring även avseende andra insamlingsmetoder som innebär ett intrång i grundläggande fri- och rättigheter.

Olika grader av intrång för olika behandlingsåtgärder

Vi ser likheter mellan den principskiss som Europadomstolen dragit upp avseende signalspaning, i målet *Centrum för Rättvisa mot Sverige*, och den process som kan förväntas vid behandling av stora informationsmängder. även vid sådan behandling kan man se en flerstegsprocess med ett gradvis ökat intrång i fri- och rättigheter.

Den typ av informationshantering som vi avser att reglera kan exempelvis inledas genom insamling av en större mängd uppgifter (bland annat personuppgifter). Uppgiftsmängden är sådan att den inte är möjlig att granska manuellt. Efter insamlingen sker automatiserad behandling genom att olika urvalskriterier och sökbegrepp tillämpas på uppgiftsmängden. Det leder fram till att en mer begränsad mängd uppgifter, som är relevanta för verksamheten, filtreras fram för fortsatt bearbetning och analys. I praktiken är en sådan behandling indelad i samma fyra steg som signalspaning: 1) insamling, 2) filtrering, 3) bearbetning och analys samt 4) delgivning eller annan åtgärd.

Den största skillnaden från signalspaning är att det första steget i processen inte avser en viss, mycket integritetskänslig, inhämtningsmetod. Signalspaning fångar uppgifter under överföring medan den behandling av stora uppgiftsmängder vi avser att reglera i stället kommer att ske i ett mer statiskt material, som behandlas över tid. En annan skillnad mot signalspaning är att den, särskilt när den är trådbunden, sker i mycket stora och huvudsakligen odifferentierade informationsströmmar. Säkerhetspolisens behov avser möjligheten

[4] European Commission for Democracy Through Law, *Report on The Democratic Oversight of Signals Intelligence Agencies, nr 719/2013*, antagen den 20–21 mars 2015.

att hantera större informationsmängder, men endast sådana informationsmängder som samlats in för att de med viss sannolikhet är relevanta för ett uttalat ändamål. Vi föreslår inte att Säkerhetspolisen ska få någon ytterligare metod för insamling av information. Den insamling som i praktiken sker i dag men som vi förtydligat i vårt förslag till ny säpodatalag och benämnt inledande behandling, är den generella metoden för insamling av personuppgifter, se avsnitt 8.6. För sådan insamling föreslår vi ett krav på att personuppgifterna ska vara befogade att behandla för ett ändamål. Vid sidan av den möjlighet till insamling som säpodatalagen medger finns olika särskilt reglerade inhämtningsmetoder, som hemlig dataavläsning eller hemlig avlyssning av elektronisk kommunikation. Sådana inhämtningsmetoder kan ur integritetshänseende vara lika känsliga som signalspaning, men får endast ske för vissa specifika ändamål och under strikt kontroll.

Behandling av öppet tillgänglig information, med stöd av reglerna om inledande behandling, är inte lika integritetskänslig som den information som signalspaningsmyndigheten hanterar. Däremot kan lagring av öppet tillgänglig information över tid, i kombination med uppgifter som inhämtas i hemlighet genom olika tvångsmedel, sammantaget innebära ett stort intrång i enskilda och allmänna intressen, till exempel opinionsfriheterna. Vi har utformat vårt förslag med dessa utgångspunkter.

Principskiss för reglering av stora datamängder

För signalspaning är det självklart att kraven på personuppgifter som får inhämtas inte kan vara desamma som för uppgifter som exempelvis ska delas med andra myndigheter. Som Europadomstolen har konstaterat bygger signalspaning på att stora uppgiftsmängder hanteras, men att fri- och rättighetsintrånget i första hand påverkas av hur kvalificerad behandlingsåtgärden är. Att samla in och lagra personuppgifter utgör inte samma intrång som att läsa, analysera och dela dem. Den lag vi föreslår måste ta hänsyn till denna skillnad i intrång och reglera olika behandlingsåtgärder för sig.

Vi anser att de principer som Europadomstolen har fastställt är välavvägda och lämpliga att överföra till en lagstiftning med generell tillämplighet för behandling av stora uppgiftsmängder. I ett sådant

system måste det finnas en acceptans för att stora mängder personuppgifter samlas in och lagras över tid. Detta för att möjliggöra olika behandlingsåtgärder, så länge denna behandling behövs för skyddet av nationell säkerhet.

Nya tekniska behandlingsmetoder kan innebära en högre grad av intrång än om uppgifter bearbetas och analyseras manuellt. En automatiserad profilering utifrån en persons levnadsvanor, kommunikation eller andra yttre faktorer kan utgöra ett betydande integritetsintrång. Att däremot gallra bort uppenbart irrelevanta personuppgifter på automatiserad väg innan dessa når ett mänskligt öga kan innebära ett lägre intrång än motsvarande manuell behandling. Ett exempel är om en person manuellt behöver gå igenom alla bilder i en mobiltelefon för att hitta de få som är av intresse. Detta jämfört med om ett automatiskt program för bildigenkänning redan har gallrat fram endast de bilder som matchar vissa kriterier, exempelvis där skjutvapen förekommer.

Med utgångspunkt i vad Europadomstolen har slagit fast är vi av uppfattningen att stora datamängder inte kan hanteras enligt samma behandlingsneutrala principer som i det övriga dataskyddsregelverket. Det kan med andra ord inte ställas upp ett enda allmänt krav för all personuppgiftsbehandling, med innebörden att uppgifterna när detta krav är uppfyllt får samlas in, lagras, läsas, analyseras, raderas eller delges. Eftersom vi anser att olika behandlingsåtgärder innebär olika grader av intrång, måste de omgärdas av olika regler, som syftar till att minimera intrånget och förhindra att systemet missbrukas.

Vårt synsätt bygger därför på en intrångstrappa som börjar med *insamling* och *registrering* av uppgifter för att sedan övergå till olika *automatiserade behandlingsåtgärder* och slutar vid *framtagning* av informationen. Vi anser att de olika stegen på denna intrångstrappa motiverar olika dataskyddsmekanismer.

Insamling och registrering

Det första steget i den skisserade flerstegsprocessen utgörs av insamling och lagring av personuppgifter. Säkerhetspolisen har flera källor för informationsinhämtning, exempelvis hemliga tvångsmedel. Inom myndighetens nuvarande regelverk finns även vissa möjligheter att ta del av information från öppna källor (öppen information). Den

rättsliga grunden för *insamling* av personuppgifter finns redan i dag. Vi föreslår inte någon saklig ändring i denna del. Däremot föreslår vi en särskild reglering i säpodatalagen av det vi benämner *inledande behandling* av personuppgifter. Genom denna reglering tydliggörs kraven för att få samla in personuppgifter när detta är befogat för ett ändamål.

Riktad insamling som sker mot en viss individ, organisation eller gruppering kommer i princip att kunna hanteras inom ramen för vårt förslag till ny säpodatalag. I dessa fall är det möjligt att rikta insamling mot de uppgifter som behövs för ett särskilt ändamål. Under den inledande granskningen kan sedan de uppgifter som visar sig vara onödiga raderas. Säpodatalagen är lämplig för att bygga underrättelser kring kända företeelser och kända aktörer. Det kan exempelvis handla om att gå vidare med misstankar som uppkommit genom tips eller spaning.

För att Säkerhetspolisen ska kunna upptäcka hotaktörer som inte är kända på förhand och vara proaktiv i stället för reaktiv krävs andra metoder. Det är nämligen mycket svårt att i dessa syften rikta in underrättelseverksamheten på det sätt som förutsätts för behandling enligt säpodatalagen. Vårt förslag till ny lag innehåller flera lättnader i förhållande till det nuvarande regelverket. Det finns däremot inte någon möjlighet att med stöd av den lagen behandla personuppgifter som vare sig behövs eller är relevanta och adekvata för ett särskilt, uttryckligt angivet och berättigat ändamål. För att Säkerhetspolisen ska kunna behandla stora informationsmängder behövs en annan rättslig systematik än vad som är fallet i en generell personuppgiftslagstiftning.

För att upptäcka ett okänt hot måste information kunna behandlas utifrån prognoser och bedömningar av kontext snarare än de enskilda uppgifter som ingår i informationen. Vi föreslår därför att Säkerhetspolisen ska kunna lagra även stora informationsmängder. När Säkerhetspolisen beslutar att lagra sådana uppgiftsmängder sker, enligt den begreppsapparat vi föreslår för den nya lagen, en *registrering*.

Framtagning

I slutet av intrångstrappan återfinns den behandling som gör information tillgänglig för en människa. Att en människa kan ta del av innehållet i registrerade uppgifter är det intrång i rätten till privatliv

som artikel 8 i Europakonventionen i första hand är avsedd att motverka. Skyddet av privatliv utgör ett skydd mot att andra människor på något sätt får tillgång till eller kännedom om uppgifter som den enskilde har rätt att hålla för sig själv. Att lagring av personuppgifter i sig utgör ett intrång i privatlivet har, enligt vår uppfattning, en koppling till att rätten till privatliv därigenom kan kränkas genom att en annan människa tar del av de lagrade uppgifterna.

Ett motsvarande intrång kan uppkomma om en automatiserad process leder fram till en åtgärd från en myndighet som kan påverka den enskilde. Vi har i avsnitt 8.20.1 bedömt att automatiskt beslutsfattande inom säpodatalagens tillämpningsområde inte bör tillåtas. Att en människa får del av personuppgifter utgör därför den gemensamma nämnaren för behandling som utgör den största risken för betydande intrång genom att stora informationsmängder behandlas. Vi har valt att benämna denna personuppgiftsbehandling *framtagning*. Framtagning är den personuppgiftsbehandling som innebär att de registrerade uppgifterna tillgängliggörs. Det är i sin tur en förutsättning för att myndigheten ska kunna utföra olika åtgärder som påtagligt påverkar den registrerade.

Övriga automatiserade behandlingsåtgärder

Mellan registrering och framtagning av personuppgifter finns lagring och andra behandlingsåtgärder som inte utgör en framtagning.

Den information som lagrats i ett it-system måste på något sätt kunna struktureras, sammanföras, gallras och göras sökbar. Sådana databastekniska åtgärder omfattas av begreppet personuppgiftsbehandling men behöver enligt vår bedömning inte innebära något tillkommande intrång i den registrerades rättigheter. Registervård i form av exempelvis radering av uppgifter efter en viss tid sker i den registrerades intresse och är en förutsättning för att behandling ska vara tillåten.

Det finns andra, mer kvalificerade behandlingsåtgärder, som inte heller innebär att intrånget blir större än att personuppgifter överhuvudtaget finns registrerade. Det kan exempelvis handla om automatiserad översättning från främmande språk eller att bildigenkänningsprogramvara automatiskt tillför metadata om vad bilder föreställer. Det är viktigt att lagen inte ställer upp onödiga hinder för teknikutveckling inom Säkerhetspolisen. Lagen bör därför inte

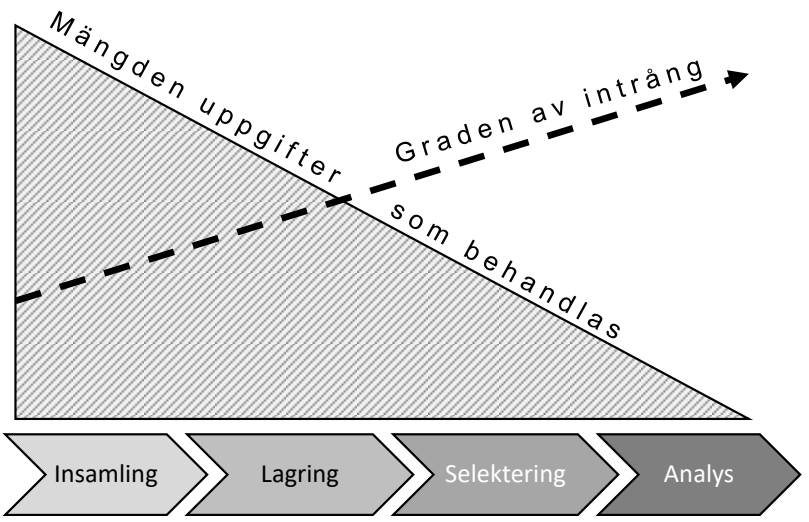
hindra behandlingsåtgärder i syfte att underlätta informationshantering, som inte i sig utgör något tillkommande intrång i de registrerades rättigheter.

Viss automatiserad personuppgiftsbehandling kan dock utgöra ett tillkommande fri- och rättighetsintrång. Det mest närliggande exemplet är så kallad profilering. Det bör ställas krav på att sådana åtgärder bara sker, om det behövs för ett visst ändamål. Vår uppfattning är dock att intrånget i enskildas personliga integritet, även av sådana åtgärder främst uppkommer när det är möjligt att ta del av och kunna vidta en åtgärd utifrån resultatet.

En principiell skiss

Det nu sagda går att sammanfatta grafiskt. Skissen nedan utgår från Europadomstolens ställningstaganden i fråga om behandling av information från signalspaning. Av skissen kan slutsatsen dras att det i första hand inte är mängden uppgifter som styr graden av intrång, utan typen av behandling. I takt med att mer avancerad behandling görs, stiger graden av intrång trots att mängden behandlade uppgifter sjunker. En slutsats av detta är att det krävs successivt ökade kompensatoriska åtgärder i takt med att behandlingen går från insamling och lagring till selektering och analys.

Figur 9.1 Principer bakom förslaget



9.1.3 Stora risker kräver kraftiga skyddsmekanismer

Riskerna med att behandla stora informationsmängder

En förutsättning för att signalspaning ska kunna godtas som metod, är att det finns robusta skyddsmekanismer. Europadomstolen har uttalat att tillräckliga skyddsmekanismer är en förutsättning, eftersom underrättelseverksamhetens natur är sådan att enskilda inte kan bevaka sin egen rätt, samtidigt som det potentiellt går att missbruka systemet.

Mängden personuppgifter utgör i sig en faktor som måste vägas in när det kommer till att bedöma intrånget i den personliga integriteten och andra grundläggande fri- och rättigheter. Om en stor mängd uppgifter om en enskild individ samlats in från många olika källor, går det att kartlägga dennes privat- och familjeliv, trosuppfattning, politiska åsikter eller religiösa övertygelse. Inlägg på sociala medier tillsammans med uppgifter om en persons bosättning, arbete eller sociala nätverk kan teckna en bild som är mer detaljerad än vad som går att få genom att exempelvis avlyssna dennes telefon. Intrånget blir särskilt tydligt om det handlar om källor som inte endast är öppet tillgängliga utan där även uppgifter som den enskilde inte själv har möjlighet att kontrollera kan ingå.

Till integritetsrisken för den enskilde ska läggas risken för avhållande inverkan på det demokratiska, offentliga samtalet. Risken att tilldra sig intresse genom offentlig debatt i ämnen som är godtagbara i ett demokratiskt samhälle, även om de kan anses vara anstötliga eller extrema i något avseende, kan leda till just sådana effekter. Om dessa effekter uppkommer, har lagstiftningen som är till för att skydda demokratin fått motsatt effekt. Den fria åsiktsbildningen är en av hörnpelarna som bär upp vårt demokratiska statsskick och även teoretiska risker för att en lag leder till avhållande inverkan på det fria och öppna samtalet måste tas på stort allvar, se vidare avsnitt 7.2.3.

Vår uppfattning är att den lagstiftning om stora informationsmängder vi nu föreslår bär med sig sådana risker att det rättsstatliga skyddet måste vara mycket starkt för att kompensera för dessa.

Generellt förbud mot framtagning hanterar riskerna

Vi har kommit till slutsatsen att den relativt låga tröskeln för Säkerhetspolisen att inleda personuppgiftsbehandling, genom insamling eller inhämtning, behövs för att myndigheten ska kunna utföra sitt uppdrag. I avsnitt 8.6 redogör vi för att inledande behandling ska få ske av personuppgifter som är befogade för ett brett formulerat ändamål. Dessa krav är lägre än vad som gäller för att personuppgifter ska få fortsätta att behandlas för operativa ändamål, se avsnitt 8.7. Vi har därför reglerat hur granskning av personuppgifter ska ske.

En förmåga som innebär att stora informationsmängder får behandlas innebär att uppgifter som samlas in också får bevaras över tid, trots att de inte når upp till kraven för fortsatt behandling enligt säpodatalagen. Sådan informationshantering innebär ett intrång i grundläggande fri- och rättigheter. När det kommer till de personuppgifter som Säkerhetspolisen registrerat med stöd av denna särskilda lag föreslår vi därför ett generellt förbud mot det vi benämner *framtagning.* Det innebär att myndigheten inte ska kunna läsa eller på annat sätt ta del av uppgifterna. På så sätt skapas ett grundläggande skydd för de personuppgifter som behandlas. Den lag vi föreslår ska därför innehålla dels ett förbud mot framtagning, dels reglerade undantag från detta förbud.

Tillsynsmyndigheterna ska ha goda möjligheter att granska både vilka bedömningar som ligger bakom Säkerhetspolisens registreringar enligt denna lag respektive vilka framtagningar som görs och ha korrigerande befogenheter när det samlade intrånget anses för stort. På så vis anser vi att riskerna minimeras och legitimiteten för systemet upprätthålls.

Vi har inte kunnat hitta något annat sätt att ge Säkerhetspolisen en helt nödvändig ny förmåga att hantera stora informationsmängder och samtidigt minimera de risker som denna förmåga kan medföra. Den prövning vi föreslår är i princip unik i Sverige och bygger på en svensk förvaltningstradition. I andra undersökta länder är det dock vanligt att behandling av stora datamängder underkastas någon form av judiciell prövning, ofta närliggande den som gäller för tillstånd för signalspaning.

9.2 Lagens tillämpningsområde

Förslag: Lagen ska tillämpas för behandling av personuppgifter från och med tidpunkten för deras registrering.

Lagen ska omfatta vissa behandlingsåtgärder. Den första och mest grundläggande behandlingsåtgärden är att i sökbara system digitalt bevara uppgifter som samlats in. Vi har valt att ge begreppet registrering en för denna lag självständig betydelse.

Det är genom registreringen som avsteg från personuppgiftsrättens grundläggande principer sker. För att kunna behandla stora och osorterade uppgiftsmängder räcker det inte att behandla endast de personuppgifter som behövs för ett visst, på förhand specificerat och konkretiserat ändamål. För att lagen ska ha någon funktion måste den också ge möjlighet att över tid bevara sådana personuppgifter som med säkerhet inte behövs för något ändamål, på grund av att de förekommer i en uppgiftsmängd, som är befogad att behandla i sin helhet. Personuppgifterna i en sådan uppgiftsmängd kan därmed inte sägas uppfylla kravet på att vara adekvata, relevanta eller inte för omfattande för ändamålet.

Det är naturligt att registrering utgör tröskeln för lagens tillämpning – lagen ska reglera både själva registreringsförfarandet av personuppgifter och all efterföljande behandling av dessa registrerade uppgifter.

Lagen bör endast vara tillämplig på automatiserad behandling av personuppgifter. Det finns varken något behov eller någon praktisk möjlighet att tillämpa principerna i den föreslagna lagen för uppgifter som behandlas i pappersform eller liknande.

9.3 Insamling och registrering

9.3.1 Inledande behandling av vissa datamängder enligt lagen ska inte regleras särskilt

Bedömning: Säkerhetspolisen har tillräckliga möjligheter till inledande behandling enligt andra regelverk. Enligt säpodatalagen får inledande behandling ske om det är befogat för ett ändamål. Någon särskild reglering för insamlingen eller annan inledande

behandling av personuppgifter som ska registreras behövs därför inte.

Inledande behandling regleras i säpodatalagen

Säkerhetspolisen har behov av att samla in eller på annat sätt initialbehandla stora informationsmängder inom alla sina verksamhetsgrenar och för en rad olika ändamål. Att de datamängder som behöver behandlas blir allt större speglar den mycket stora ökningen av data som genereras i samhället. I avsnitt 6.2 redogör vi för denna utveckling. I avsnitt 7.2 redogör vi för vår uppfattning att Säkerhetspolisen har ett behov och ett legitimt intresse av att kunna samla in stora mängder personuppgifter.

Säkerhetspolisen har i dag möjlighet att samla in och ta emot material från en rad källor. I princip alla dessa källor kan generera informationsmängder som inte medger den granskning som förutsätts för att säpodatalagens regler ska kunna tillämpas. Det kan exempelvis vara samverkande tjänster som delar innehåll från avkrypterade meddelandetjänster, inhämtning från sociala medier för att analysera hotbilden för en skyddsperson över tid, överskottsinformation från ett hemligt tvångsmedel eller ett it-beslag.

Det är endast några av dessa informationskällor, som till exempel it-beslag och hemliga tvångsmedel, som är specialreglerade. Den initialbehandling av personuppgifter som inte är reglerad genom särskild lagstiftning kommer att omfattas av säpodatalagens bestämmelser. De bestämmelser i säpodatalagen som vi föreslår innebär att inledande behandling kan ske av personuppgifter som är befogade för ett övergripande ändamål, så länge denna behandling är proportionerlig. Vi anser att dessa kriterier på ett bra sätt avgränsar exempelvis insamling av uppgifter från internet eller vilka dataset som kan inhämtas. Det finns därför inte något skäl att föreskriva om några andra regler för inledande behandling av personuppgifter, även om syftet är att uppgifterna ska behandlas enligt den lag vi här föreslår.

Inledande granskning enligt säpodatalagen kan leda till att uppgifter registreras enligt denna lag

En nyhet i vårt förslag till ny säpodatalag är att den reglerar inledande granskning av personuppgifter som samlats in. Granskningens syfte är att säkerställa att personuppgifter behandlas författningsenligt. Innan sådan granskning skett får personuppgifterna inte behandlas för något operativt ändamål. Regleringen syftar till att ge Säkerhetspolisen författningsstöd för att hantera information trots att det inte är känt vilka personuppgifter informationen innehåller, se avsnitt 8.12 och 8.13.

I vårt förslag till säpodatalag är tröskeln för inledande behandling lägre än för fortsatt operativ behandling. Uppgifter får samlas in om de är befogade för ett övergripande ändamål men endast de uppgifter som behövs för ett mer konkretiserat ändamål får vidarebehandlas för operativa syften. Inledande behandling av information sker därför av betydligt större informationsmängder än vad som slutligen förs över till operativa system. De olika kraven för insamling och fortsatt operativ behandling innebär att information filtreras, ofta i flera steg, under granskningen. Uppgifter som inte får fortsätta att behandlas enligt säpodatalagen ska enligt huvudregeln raderas under granskningsskedet.

Genom den kompletterande lagstiftningen som vi här föreslår tillkommer emellertid möjligheten att i stället registrera sådana uppgifter, som inte uppfyller säpodatalagens krav för fortsatt behandling, enligt denna lag. Även uppgifter som samlats in i syfte att registreras som en särskild informationsmängd kommer att träffas av den nyssnämnda bestämmelsen om inledande granskning. Granskningen kommer då att syfta till att säkerställa att uppgifterna kan behandlas författningsenligt enligt den lag vi här föreslår.

Registrering kan vara ett alternativ till radering vid behandlingstidens utgång

Vi har i anslutning till säpodatalagens bestämmelser återkommande refererat till att mängden perifera uppgifter i en källa kan få betydelse vid proportionalitetsprövningen. Ett dataset där det kan antas att det finns större mängder personuppgifter vars behov inte går att konkretisera i förhållande till ett uttryckligt angivet ändamål, inne-

bär att intrånget blir större och svårare att motivera. För att behandling ska vara proportionerlig kan behandlingstiden då behöva vara mycket kort.

Detta kan illustreras med exempelvis hot- och riskanalys inför Almedalsveckan eller ett statsbesök. För att kunna göra en hotbedömning kan Säkerhetspolisen ha ett behov av en bred inhämtning för att analysera exempelvis debattartiklar och uttalanden som gjorts på sociala medier en viss tid innan ett offentligt framträdande ska ske. Intrånget är givetvis mycket stort då det kan röra sig om en bred insamling av politiska uttryck och grundlagsskyddade yttranden. Inhämtning och analys kan alltjämt vara proportionerligt, under förutsättning att ändamålet är tillräckligt tungt och om intrånget sker endast under en mycket begränsad tid. Enligt säpodatalagens grundläggande principer om minsta möjliga intrång ska personuppgifter inte behandlas längre än vad som behövs för ändamålet. Det innebär att behandling som regel inte kan motiveras efter att bedömning och analys utförts.

Det finns emellertid ett stort behov av kunskapsuppbyggnad avseende orsaker till hotdrivande kommunikation, trender, mönster och avvikelser för att kunna bedöma och reducera framtida hot. I stället för att radera uppgifterna efter att de inte längre får behandlas enligt säpodatalagen, kan de registreras enligt den här föreslagna lagen. Fri- och rättighetsintrånget av en sådan registrering är, på grund av förbudet mot framtagning, betydligt mindre än om de behandlas enligt säpodatalagen. Därför kan det vara proportionerligt att behandla personuppgifter under längre tid om de genom att registreras förs över till den föreslagna nya lagens tillämpningsområde.

9.3.2 Uppgifter som är befogade för ett övergripande ändamål ska få registreras om det är proportionerligt

Förslag: Säkerhetspolisen ska kunna besluta att personuppgifter ska registreras i en särskild uppgiftssamling, om det är befogat för vissa ändamål.

Ändamål

Vi har i avsnitt 8.6.6 redogjort för bakgrunden till vårt ställningstagande för att ändamålen för inledande behandling ska vara mer övergripande än ändamålen för fortsatt behandling. Där uttrycks det så att inledande behandling får ske, om det är befogat för ett ändamål inom de verksamheter som beskriver Säkerhetspolisens brottsbekämpande uppdrag eller någon annan rättslig grund. Uppgifter som inledningsvis behandlats för ett sådant brett ändamål får dock endast fortsätta att behandlas, om de behövs för ett särskilt, uttryckligt angivet och berättigat ändamål. Detta mer konkretiserade ändamål ska, om det inte framgår av sammanhanget, även anges genom en särskild upplysning.

Ändamålen fyller på så sätt olika funktioner. Inledande behandling får ske för övergripande ändamål. Fortsatt behandling av insamlade uppgifter får däremot endast ske för särskilda, uttryckligt angivna ändamål. Det innebär att det måste finnas ett mer konkretiserat behov för att få behandla uppgifter över tid. Det är en följd av att personuppgiftsbehandling över tid utgör ett sådant intrång i enskildas fri- och rättigheter som måste kunna viktas mot ett konkret ändamål vid en proportionalitetsprövning. Ett alltför brett formulerat ändamål, som exempelvis ”kontraterror”, tillåter inte en sådan prövning.

Den lag vi föreslår bygger på ett generellt förbud mot att ta fram registrerade uppgifter. Det intrång som sker av att uppgifter lagras över tid är i dessa fall inte alls lika stort som för uppgifter som är fritt tillgängliga för sökning och framtagning inom den operativa verksamheten. Syftet med den särskilda lag vi föreslår är att ge Säkerhetspolisen en delvis ny förmåga. Det handlar om möjligheten att behandla information i den breda underrättelseverksamheten, som syftar till att bland annat upptäcka okända hot. Hot som är okända är definitionsmässigt svåra att konkretisera. Det innebär att det ofta inte heller är möjligt att ange ett ändamål för personuppgiftsbehandling som är tillräckligt konkret för att kunna konstatera att en viss mängd personuppgifter behövs och är relevanta och adekvata för detta ändamål.

För att förbättra Säkerhetspolisens förmåga att upptäcka okända hot bör sådana uppgifter i stället kunna registreras som en uppgiftsmängd för breda underrättelseändamål. Kraven på ändamål för personuppgiftsbehandling bör därför vara samma för registrering som

för inledande behandling. Det innebär att uppgifter bör kunna registreras för ändamål inom någon av Säkerhetspolisens verksamhetsområden. Vi återkommer, i avsnitt 9.10.2, om vår syn på behandling för brottsutredande ändamål inom denna lags tillämpningsområde.

Behov

För insamling och annan inledande behandling enligt vårt förslag till ny säpodatalag ställs krav på att uppgifterna är *befogade* för ändamålet, se avsnitt 8.6.7. För att uppgifterna ska få fortsätta att behandlas efter den inledande granskningen krävs däremot att de *behövs*. Med begreppet ”behövs” avses att uppgiften krävs för att Säkerhetspolisen ska kunna utföra sitt uppdrag. På samma sätt som för den inledande behandlingen bör behandlingströskeln för registrering av uppgiftsmängder enligt den nya lagen vara lägre än för de mer kvalificerade behandlingsåtgärderna.

Syftet med att behandla stora informationsmängder är bland annat att upptäcka ett okänt hot eller kartlägga trender och mönster över tid. Då är det inte möjligt att endast behandla de uppgifter som behövs vid tidpunkten för registrering. Detta behov går nämligen inte att fastställa förrän uppgifterna har kunnat behandlas under en tid. Endast om uppgifter tillåts att registreras för att de på aggregerad nivå antas vara relevanta, är det möjligt att pröva om de faktiskt är det. Det kan exempelvis komma fram uppgifter över tid som sammantagna tecknar en bild som inte varit möjlig att se om varje informationsled endast kunnat bedömas för sig.

Vi anser därför att det finns goda skäl till att ha samma låga behovskriterium för registrering som för inledande behandling. Det ska därför krävas att uppgifterna är befogade för ett ändamål för att de ska få registreras. Betydelsen av *befogat* bör vara densamma som vad gäller insamling.

När det gäller personuppgifter som redan behandlas enligt säpodatalagen, för att det står klart att de behövs under en viss tid, kan det alltjämt vara befogat att behandla uppgifterna därefter. Då kan det bli aktuellt att registrera uppgifterna enligt den här föreslagna lagen i stället för att radera dem.

Den grundläggande skillnaden i denna lagstiftning jämfört med andra personuppgiftslagstiftningar är att de flesta bestämmelser

inte avser att reglera *behandling av personuppgifter*. I stället är det vissa av de behandlingsåtgärder som ingår i behandlingsbegreppet som regleras på skilda sätt. För att lagen på ett tydligt sätt ska kunna ge särskilda rättsliga förutsättningar för olika behandlingsåtgärder finns det ett behov av att definiera vissa av de komponenter som ingår i behandlingsbegreppet.

Vi föreslår mot denna bakgrund att det införs vissa särskilda definitioner i den nya lagen. De begrepp som i första hand kräver definitioner är *registrering* och *framtagning*. Vidare bör den lagtekniska termen *särskild uppgiftssamling* definieras.

9.3.3 Principen om uppgiftsminimering kan inte tillämpas på stora informationsmängder

Bedömning: Det krävs undantag från dataskyddskonventionen 108+, artikel 5.4 c, om att personuppgifter ska vara adekvata, relevanta och inte för omfattande i förhållande till ändamålet med behandlingen.

Skälen för bedömningen

Dataskyddskonventionen 108+ innehåller grundläggande bestämmelser om adekvans, relevans och uppgiftsminimering. Dessa principer är i praktiken oförenliga med behandling av stora informationsmängder där innehållet till största delen är okänt.

Kravet i artikel 5.4 c i dataskyddskonventionen 108+ om att uppgifter inte får vara för omfattande har både en kvantitativ och en kvalitativ aspekt, se avsnitt 8.10.2. I kvantitativt avseende ska behandlingen av uppgifter begränsas till den mängd som behövs för ändamålet med behandlingen. Vid en kvalitativ bedömning kan personuppgifter som i och för sig är adekvata och relevanta, men där en behandling skulle innebära ett oproportionerligt intrång betraktas som alltför omfattande.

Både prövningen av adekvans, relevans och om behandlingen är alltför omfattande kräver en kännedom om innehållet i det som registrerats. Det går att bilda sig en översiktlig uppfattning om innehållet i stora informationsmängder, vilket även förutsetts i den här

föreslagna lagstiftningen. Någon egentlig prövning avseende adekvans, relevans och om behandlingen är för omfattande kan däremot inte komma i fråga. Det kräver en granskning som är så ingående att syftet med lagen skulle förfelas.

Vi föreslår därmed att den här föreslagna lagen, till skillnad från vårt förslag till säpodatalag, ska innehålla ett undantag från dataskyddskonventionen 108+ avseende principen om uppgiftsminimering. Sådana undantag är möjliga att göra i Säkerhetspolisens verksamhet som rör nationell säkerhet. Undantaget gäller inom lagens tillämpningsområde, vilket innebär att undantaget främst får betydelse vid registrering av uppgifter. Undantaget är en förutsättning för att kunna hantera stora informationsmängder i syfte att förebygga, förhindra och upptäcka brottslig verksamhet som innefattar brott mot Sveriges säkerhet eller terroristbrott. Undantaget är därför nödvändigt för att effektivt kunna förebygga, förhindra och upptäcka hot mot nationell säkerhet.

Framtagna uppgifter ska behandlas enligt säpodatalagen, se avsnitt 8.12.6 och 9.10.1.

Det innebär att uppgifter som inte är relevanta eller adekvata och sådana som är för omfattande för ändamålet ska raderas innan de kan behandlas för något operativt ändamål. Undantaget avseende uppgiftsminimering som gäller för registrering kommer därmed inte att medföra att irrelevanta eller onödigt omfattande uppgifter behandlas i den operativa verksamheten. Undantaget från dataskyddskonventionen går därför inte längre än vad som är nödvändigt i ett demokratiskt samhälle.

9.3.4 Ska det finnas andra begränsande faktorer för insamling och registrering av stora informationsmängder?

Bedömning: Säkerhetspolisen bör bestämma vilka personuppgifter som är befogade för ett ändamål och pröva proportionaliteten av registreringen.

Ska endast vissa typer av information få registreras?

Det är möjligt att i lag begränsa vilka informationsmängder som får registreras med stöd av den nya lagen. Vi har bland annat övervägt att likt Norge endast göra lagen tillämplig på öppet tillgänglig information, se avsnitt 4.4.3. En annan legalbegränsning skulle kunna innebära att vissa källor undantas från lagens tillämpningsområde eller att innehållet i informationen skulle kunna begränsa möjligheten till registrering. Exempelvis skulle kommunikationsuppgifter kunna undantas eller begränsas på något sätt, exempelvis till metadata och inte kommunikationsinnehåll.

Ett annat exempel skulle kunna vara att information som tillhör en del av privatlivets kärna eller liknande inte får förekomma. En sådan, närmast filosofisk, begränsning finns bland annat inom tysk konstitutionell rätt (”Kernbereich persönlicher Lebensgestaltung”) som skyddas av den tyska författningsdomstolen genom särskilt skydd i olika lagstiftningar som rör statlig övervakning). Ett annat alternativ är att insamling av stora datamängder ska underkastas en förhandsprövning eller underställas något annat organ som är fristående från myndigheten. Liknande mekanismer förekommer både i Nederländerna och Förenade kungariket. I dessa länder tar speciallagstiftningen för behandling av stora informationsmängder främst sikte på förvärv av stora dataset från internet och regleras på liknande sätt som signalspaning, se avsnitt 4.5.3 och 4.6.3.

Det är mycket svårt att i lag peka ut vilken typ av information som bör få registreras i en särskild uppgiftssamling. Hoten mot Sveriges säkerhet varierar över tid och de miljöer där hoten förekommer är rörliga. Dessutom kan en lagstiftning som inte är teknikneutral snabbt bli obsolet. Vi anser att det endast är Säkerhetspolisen som kan ha den överblick som krävs för att kunna avgöra vilken slags information och från vilka källor som det är relevant för myndigheten att ha tillgång till över tid. Förändringar av hot och behovet av att kartlägga dessa sker snabbare än processen att genom författning peka ut vissa källor eller viss typ av information.

De gränsdragningsfrågor och den osäkerhet som skulle uppkomma i samband med att ny teknik introduceras skulle med all säkerhet påverka möjligheten att utnyttja lagstiftningen för sina syften. Samtidigt kan det med fog ifrågasättas om det är möjligt att på förhand peka ut vissa källor som mer känsliga än andra. I Norge,

där lagstiftningen begränsats till behandling av öppet tillgänglig information, har det påpekats att det finns mycket stora integritetsrisker även i denna informationsmiljö. Den begränsningen träffar exempelvis inte endast information som den enskilde valt att publicera eller på ett eller annat sätt har kontroll över. Även information som olovligen publicerats, exempelvis efter ett dataintrång eller förtal och lögner om en person som publicerats av annan, kommer kunna behandlas enligt lagen, se vidare i avsnitt 4.4.3.

Olika innehållsbegränsningar, som exempelvis kommunikationsinnehåll, kan många gånger ge en falsk bild av att integriteten skyddas. Det har ansetts att behandling av annan kommunikationsdata, exempelvis vilka som kommunicerat, hur länge och var, kan vara tillräcklig för att teckna en intim bild av en person; en bild lika skyddsvärd som innehållet i kommunikationen.[5] Detta särskilt om uppgifter från olika källor kan kombineras med varandra för att komplettera bilden.[6] Integritetsskyddet bör av dessa skäl byggas på annan grund än att i lagen peka ut viss typ av information som godtagbar. Vi återkommer till sådana skyddsmekanismer.

Ska det krävas förhandstillstånd för registrering?

Vi har även övervägt förhandstillstånd för registrering från en självständig funktion inom Säkerhetspolisen, från en självständig myndighet eller från en domstol. Ett system med förhandsprövning innebär samtidigt en stor förskjutning i förhållande till behandling av personuppgifter enligt säpodatalagen. Utgångspunkten för lagen är att intrånget i enskildas fri- och rättigheter är som störst när uppgifter tas fram och inte när de registreras. De känsligaste inhämtningsmetoderna är dessutom särskilt reglerade och underkastade förhandsprövning från en självständig aktör i form av till exempel domstolsprövning.

Det framstår sammantaget som att effektiviteten i systemet skulle riskeras om registrering skulle vara föremål för förhandsprövning av exempelvis åklagare eller domstol. Det bör därför vara Säkerhetspolisen som ansvarar för att registrering av uppgifter med stöd av lagen är proportionerlig och i övrigt författningsenlig. Registreringarna kommer vara föremål för tillsyn.

[5] Se bland annat EU-domstolens dom den 6 oktober 2020 i mål C 511/18 m.fl., *La Quadrature du Net*, p. 117.
[6] Se Europadomstolens avgörande i målet *Centrum för Rättvisa mot Sverige*, p. 256.

Säpodatalagens bestämmelse om proportionalitet är tillräcklig

Vi har i vårt förslag till säpodatalag föreslagit en generell proportionalitetsprincip som ska gälla för all personuppgiftsbehandling. Den gäller för insamling av uppgifter och bör gälla även för registrering.

Registrering ska få ske av uppgifter som inte kunnat granskas i detalj. Sådana registreringar sker för att möjliggöra framtida sökningar i materialet. Det är svårt att avgränsa storleken av en sådan uppgiftsmängd endast med tillämpning av ändamåls- och behovsprincipen. Bedömningen måste kunna göras mot uppgiftsmängder och inte uppgifter. Det kan vara svårt att avgöra hur stor uppgiftsmängd som behövs för att uppnå ändamålet med registreringen.

Uppgiftsmängden som får registreras kommer därför främst begränsas av kravet på proportionalitet. Den föreslagna lagstiftningen är avsedd att täcka alla typer av behov att behandla stora informationsmängder. Det är inte endast fråga om att reglera öppet tillgänglig information. En informationsmängd som inte är känslig ur integritetshänseende kan vara proportionerlig att behandla, även om den innehåller stora mängder personuppgifter. Det kan röra sig om en heltäckande lista av vilka ip-nummer som varje land förfogar över. Intrånget i andra intressen är i detta fall i det närmaste obefintligt. När det kommer till mer känslig information, som inhämtning från sociala medier, finns det skäl som talar i motsatt riktning. I dessa fall växer intrånget med antalet personuppgifter som behandlas.

En personuppgiftsbehandling är proportionerlig, om skälet för att utföra behandlingen överväger intrånget i de enskilda eller allmänna intressen som kan påverkas av den. Tanken är dock inte att varje personuppgift ska granskas. Till skillnad från inledande behandling sker dock registrering av uppgifter som, i vart fall översiktligt, går att granska innan behandlingsåtgärden vidtas. Det innebär att det under den inledande granskningen är möjligt att rensa insamlade uppgifter från onödiga, irrelevanta eller oproportionerligt känsliga uppgifter innan informationen registreras. Beroende på vilken data det rör sig om kan det ske på olika sätt.

Ett onödigt intrång i en fri- och rättighet kan aldrig vara proportionerligt. Det finns därför krav på att Säkerhetspolisen, i rimlig utsträckning, ska filtrera de informationsmängder som samlats in för att en registrering inte ska utgöra ett större intrång i fri- och rättigheter än vad som är befogat.

9.3.5 Motiverade beslut om registrering

Förslag: Varje uppgift som registreras med stöd av lagen ska kunna spåras till ett skriftligt beslut. Av beslutet ska framgå

1. vad de registrerade uppgifterna i huvudsak avser och från vilken källa eller vilka källor de härrör,
2. vilket intrång i enskilda och allmänna intressen som behandling av uppgifterna kan antas medföra,
3. för vilket eller vilka ändamål uppgifterna registreras,
4. hur länge uppgifterna som längst får behandlas, och
5. de skäl och omständigheter i övrigt som föranlett registreringen.

Krav på ett motiverat beslut om registrering

Vår utgångspunkt är att Säkerhetspolisen bör ha handlingsutrymmet att registrera de uppgifter som bedöms vara befogade för ett övergripande ändamål. Det ligger därmed ett mycket stort ansvar på Säkerhetspolisen att iaktta den proportionalitetsprincip som utgör grunden för dataskyddet vid behandling även av stora informationsmängder.

Proportionalitetsprövningen är av sådan vikt att vi anser att det finns starka skäl för att i lagen ange närmare bestämmelser om hur denna prövning ska formaliseras. Att det finns formkrav för prövningen bidrar till att den struktureras och tydliggörs. Detta är viktigt både för Säkerhetspolisens egen uppföljning men framför allt för tillsynsmyndighetens möjlighet att granska hur lagen tillämpas.

Ett skriftligt beslut manar också till reflektion och eftertanke. En strukturerad prövning har därför förutsättningar att bli bättre och mer rättssäker.

Vi anser av dessa skäl att det bör finnas ett krav på att Säkerhetspolisen ska fatta ett motiverat beslut i varje enskilt fall när uppgifter registreras i en särskild uppgiftssamling.

Vad bör ett registreringsbeslut innehålla?

Endast den formalia som är nödvändig för tillämpning och tillsyn bör anges i lag

Det är svårt att prognostisera i vilken omfattning Säkerhetspolisen kommer att registrera stora informationsmängder med stöd av lagen. Det är dock viktigt att processen inte är onödigt formalistisk. Varje krav som ställs för en registrering bör motiveras av ett berättigat intresse. Lagen hindrar givetvis inte att Säkerhetspolisen av verksamhetsskäl utvecklar registreringsprocessen med angivande av ytterligare information som kan behövas för att underlätta förståelsen eller nyttan av uppgifterna. De uppgifter som av dataskyddsskäl måste framgå av ett registreringsbeslut är de som behövs för en effektiv tillsyn och för tillståndsprövning vid framtagning. Det innebär att uppgifter som behövs vid proportionalitetsprövningen måste framgå.

Källa och informationsmängdens huvudsakliga innehåll

Redan vid inledande behandling krävs en proportionalitetsprövning. behovet av åtgärden måste väga tyngre än risken för intrång i den personliga integriteten eller andra enskilda och allmänna intressen. Efter inledande behandling ska uppgifter initialgranskas för att bedöma bland annat behov och proportionalitet av fortsatt behandling. I detta skede finns möjlighet att vidta olika behandlingsåtgärder för granskningsändamål.

Eftersom ett registreringsbeslut innebär att den information som registreras inte längre är tillgänglig, varken för Säkerhetspolisen eller tillsynsmyndigheten, är det viktigt att uppgiftsmängden som ska registreras beskrivs i tillräcklig utsträckning för att det ska vara möjligt att bedöma att registreringen skett på ett korrekt sätt. Granskningen av större uppgiftsmängder kan givetvis inte ske i detalj. Däremot måste uppgifter som samlats in genom inledande behandling översiktligt kunna beskrivas för att uppgifterna ska kunna registreras i en särskild uppgiftssamling.

Som ett grundkrav bör källan tydligt anges. Exempelvis kan det anges att beslutet omfattar överskottsinformation från användandet av ett tvångsmedel eller att det rör sig om information som in-

hämtats från öppna källor, som till exempel ett forum i en viss extremistmiljö.

Vid sidan av källa bör även informationsinnehållet övergripande beskrivas. I vissa fall följer innehållet redan av källan. Det är kan exempelvis vara uppenbart att om en referensdatabas avseende ip-nummer registrerats, innehåller den just ip-nummer. I andra fall måste Säkerhetspolisen ange om informationsmängden består av exempelvis kommunikationsinnehåll, metadata eller öppen information från sociala medier. Om det rör sig om exempelvis videomaterial, kan det vara nödvändigt att ange om det rör sig om en rekryteringsvideo från en terroristorganisation eller material från en övervakningskamera.

I den övergripande beskrivningen måste även den kvantitativa omfattningen av de registrerade uppgifterna anges. Utifrån denna beskrivning måste det gå att sluta sig till den ungefärliga mängden personuppgifter och antalet registrerade som förekommer i informationsmängden. Det är väsentligt för tillsynen över registreringsbeslutet att det går att sluta sig till om en registrering avser personuppgifter från en väl avgränsad eller en bredare grupp. Ju känsligare uppgifter som registreringen avser, desto viktigare är det med uppgifter om hur många individer som kan påverkas av intrånget.

Intrångsbedömning

Vid en proportionalitetsbedömning ska en avvägning göras mellan intresset av att utföra en åtgärd mot de andra skyddsvärda intressena som kan komma att påverkas av åtgärden. När det kommer till behandling av stora informationsmängder, där detaljkunskaper om innehållet saknas, kan en sådan bedömning vara mycket svår att göra eftersom de intressen som påverkas av behandlingen bygger på antaganden eller prognoser.

För att förenkla tillsynen över registreringen och ge förutsättningar för att pröva proportionaliteten vid en framtagning bör en registrering kategoriseras i intrångshänseende. Lämpligen kan en intrångskategorisering innebära att en informationsmängd som rör den privata sfären, som åtkommits genom avlyssning eller annan jämförbar åtgärd placeras i en hög kategori. Om känsliga personuppgifter kan antas förekomma i högre utsträckning än normalt,

bör detta vara en annan riskfaktor som motiverar en hög intrångskategori. Det kan handla om uppgifter som rör uttryck för politisk uppfattning eller religiös övertygelse. En proportionalitetsavvägning ska göras mot både enskilda och allmänna intressen. Bland de allmänna intressena märks bland annat de positiva opinionsfriheterna.

Intrångskategorier behöver anges med tillräcklig differentiering för att ge en verklig vägledning för tillämpningen samtidigt som det ska vara hanterbart i verksamheten. Det kan i viss mån krävas en schablonisering vid bedömningen. Syftet med en intrångsbedömning av de uppgifter som registreras är bland annat att det ska vara möjligt att inrikta tillsynen mot de känsligaste uppgifterna eller att ge domstolen en möjlighet att begränsa de kategorier av uppgifter som får tas fram för ett visst ändamål.

Det är därför lämpligt att skapa ett system för kategorisering som medger att uppgifter jämförs med varandra. Med hänsyn till att innehållet inte kan granskas i sin helhet eller i detalj under den inledande granskningen måste det accepteras att bedömningen bygger på rimliga antaganden. Hur detta system ska utformas är alltför komplext för att det ska vara lämpligt att göra i lag. Det bör därför i stället regleras i förordning eller genom myndighetens egna föreskrifter och interna riktlinjer.

Ändamålet

Att ändamålet med registreringen anges är helt avgörande för att de grundläggande principerna bakom dataskyddet ska kunna upprätthållas. Uppgifter får registreras för samma övergripande ändamål som för inledande behandling. För inledande behandling beskrivs detta som att ändamålet anges inom en verksamhet, men att en rättslig grund eller ett visst verksamhetsområde inte är tillräckligt specifikt. Det innebär att det exempelvis behöver anges vilken typ av brottslighet som ska kartläggas genom registreringen. De breda ändamålen bör kunna tillämpas på samma sätt som vid inledande behandling, se avsnitt 8.6.6.

Skälen i övrigt

Vid sidan av de mer beskrivande delarna av ett registreringsbeslut bör även skälen anges. Beslutet att registrera uppgifter innebär att en proportionalitetsbedömning har gjorts och skälen för registreringen bör spegla denna avvägning. Skälen måste därför beskriva vilka fri- och rättigheter som påverkas av en registrering och skälen för att intrånget är nödvändigt i ett demokratiskt samhälle. I praktiken bör det av skälen för beslutet framgå på vilket sätt uppgifterna är befogade att registrera för ändamålet. Det kan exempelvis handla om att beskriva de indikatorer som talar för att det i en viss uppgiftsmängd kan vara befogat att söka efter uppgifter som har att göra med terrorrekrytering.

Skälen för en registrering är en viktig del av att göra det möjligt att utöva tillsyn över registreringen av personuppgifter. Det får därför inte vara en alltför schabloniserad motivering, särskilt inte om det gäller registreringar av mer känslig art. Det kan däremot antas att många registreringar kommer ha likartade bedömningar, eftersom de avser liknande uppgifter som registreras för samma ändamål. Det kan exempelvis gälla vid registrering av vissa referensdatabaser.

Spårbarhet

Lagen är endast tillämplig för behandling av personuppgifter som registrerats i en särskild uppgiftssamling. Inga personuppgifter ska alltså få förekomma i en särskild uppgiftssamling, om de inte registrerats med stöd av ett beslut.

Omvänt kan sägas att alla uppgifter som behandlas i en särskild uppgiftssamling måste kunna spåras tillbaka till ett registreringsbeslut. Detta förhållande bör följa av lag. Det bör därför krävas att alla personuppgifter som behandlas även rent tekniskt måste kunna härledas till det beslut som föranlett lagringen. Det innebär att om ett beslut förfaller eller upphävs måste alla uppgifter som lagrats med stöd av beslutet ofelbart och omedelbart kunna raderas.

9.3.6 Vem ska vara behörig att fatta registreringsbeslut?

Förslag: Ett beslut om att registrera personuppgifter ska få fattas endast av medarbetare som har de särskilda kunskaper och den erfarenhet som krävs för att göra bedömningen.

Skälen för förslaget

I det föregående har vi beskrivit vad som krävs för att en uppgiftsmängd ska få registreras och hur ett beslut ska utformas. De bedömningarna kommer att förutsätta särskild kunskap och erfarenhet. Det krävs en viss kompetens för att kunna bedöma om både de materiella och de formella förutsättningarna för att fatta ett registreringsbeslut är uppfyllda. Vi har i avsnitt 8.12.4 beskrivit att det bör ställas vissa kompetenskrav på de personer som utför inledande granskning, vilket även föregår registrering i särskilda uppgiftssamlingar.

Frågan är om det bör ställas än högre krav på de medarbetare vid myndigheten som ska ha behörighet att besluta om registrering i en särskild uppgiftssamling. Den prövning som ska föregå en registrering är på många sätt en svårare prövning än den som gäller frågan om fortsatt behandling enligt säpodatalagen. Det framstår som naturligt att ett beslut om att exempelvis registrera en databas innehållandes hundratusentals personuppgifter ska vara förbehållet vissa utvalda medarbetare. Proportionalitetsprövningen kan i många fall vara svår och kräva kunskaper inom flera rättsområden.

Även om det är självklart att myndigheten måste begränsa behörigheten att registrera uppgifter till vissa medarbetare föreslår vi att det därutöver ska finnas ett uttryckligt krav i lagen avseende kompetens och allmän lämplighet för att få utföra prövningen. Det ska krävas att en beslutsfattare har de särskilda kunskaper och erfarenhet som krävs för att kunna göra de bedömningar som ska föregå en registrering.

9.3.7 Referensdatabaser

En särskild typ av informationsmängder utgörs av det som kan betecknas som referensdatabaser. En referensdatabas utgörs av personuppgifter som sammanställts för ett visst syfte. Ett exempel är en

elektronisk telefonkatalog. Många myndigheter använder sig av olika referensdatabaser i sitt dagliga arbete. Det kan handla om databaser som tillhandahålls av kommersiella aktörer och som finns öppet tillgängliga, eller om stängda databaser som den egna myndigheten eller andra myndigheter ansvarar för.

Säkerhetspolisens verksamhet kräver emellertid en mycket stor försiktighet när det kommer till att exponera sitt intresse för vissa personer eller företeelser utåt. Det går inte att utesluta att andra aktörer, som Säkerhetspolisen är beroende av, brister i informationssäkerheten. En annan aspekt är att Säkerhetspolisen inte ska behöva vara beroende av en annan aktör för uppgifter som är viktiga för verksamheten. Öppet tillgängliga databaser kan exempelvis överbelastas eller på andra sätt saboteras. Det finns därför behov för Säkerhetspolisen att förvärva och lagra vissa referensdatabaser i sin helhet för att kunna genomföra sökningar i en säker miljö.

Både Försvarsmakten och FRA har liknande behov att inom myndighetens väggar behandla uppgifter som finns allmänt tillgängliga. I 2 kap. 10 § i Försvarsmaktens personuppgiftslag respektive 2 kap. 9 § FRA:s personuppgiftslag anges att myndigheterna får behandla personuppgifter som utgör allmänt tillgänglig information, om det är nödvändigt för något av respektive lags uppräknade ändamål. Den särskilda regleringen för allmänt tillgänglig information tar i första hand sikte på att upprätta interna referensdatabaser. Det kan röra sig om uppgifter som finns med i elektroniska telefonkataloger eller förteckningar över ip-adresser i olika länder som FRA behöver kunna behandla i sin verksamhet. Se vidare om FRA:s och Försvarsmaktens möjlighet att behandla bland annat allmänt tillgänglig information i referensdatabaser i avsnitt 3.6.2

Säkerhetspolisen behov av referensdatabaser bör hanteras inom denna lagstiftning

Säkerhetspolisens behov av att kunna behandla personuppgifter i referensdatabaser bör kunna tillgodoses genom den nya lagen. En referensdatabas är ofta mycket omfattande. en katalog över världens ip-adresser omfattar i dagsläget över fyra miljarder personuppgifter, om än av mycket lågt integritetsvärde. En helt komplett telefonkatalog för Sverige skulle omfatta nästan 30 miljoner nummer. Sett endast till mängden personuppgifter är sådana referensdatabaser

lämpliga att hantera inom den särskilda lagens tillämpningsområde. Det kan dock ifrågasättas om det strikta dataskydd som omgärdar denna lag är anpassat efter sådana referensdatabaser, som främst behandlas av informationssäkerhetsskäl. Det kan, särskilt i förhållande till FRA och Försvarsmaktens lagstiftning, framstå som ett alltför omfattande dataskydd.

Det skulle dock vara svårt att särreglera mer harmlösa referensdatabaser inom säpodatalagens tillämpningsområde så att de omfattas av ett mindre krävande regelverk men samtidigt behålla den strikta regleringen av sådana databaser som kan vara mer känsliga. För att undvika att begrepp som exempelvis ”allmänt tillgänglig information” får en alltför vid tillämpning, vid sidan av det avsedda området, krävs en legaldefinition av vilka uppgifter som får behandlas. Den teknikneutralitet vi eftersträvar skulle då gå förlorad. Risken är att definitionen är alltför snäv för att kunna följa teknikutvecklingen eller alltför vid för att utgöra ett adekvat dataskydd för uppgifterna. Dessutom bör även referensdatabaser som inte är allmänt tillgängliga kunna behandlas.

Vår slutsats är därför att denna lag bör användas för att ge Säkerhetspolisen större möjligheter att lokalt lagra olika referensdatabaser. Registrering av dessa ska ske enligt samma principer som gäller för andra uppgifter. Av detta följer bland annat att även referensdatabaser ska vara befogade att behandla för ett ändamål och beskrivas till sitt innehåll och karaktär.

Någon särskild reglering av referensdatabaser krävs därmed inte i förhållande till andra slags informationsmängder.

Referensdatabaser bör kunna uppdateras kontinuerligt

I normalfallet ska varje registrering vara föranledd av ett separat beslut. När det gäller referensdatabaser som avser exempelvis telefonnummer, adresser eller ip-nummer, är de endast relevanta om de hålls uppdaterade.

Det är då möjligt att göra en prövning av referensdatabasen som sådan, innefattande kontinuerliga uppdateringar. Kontinuerlig inhämtning och uppdatering av uppgifter bör då kunna ske med stöd av ett och samma registreringsbeslut. Frågan om ändamål, behov

och proportionalitet görs för databasen som ska inhämtas och inte för databasens exakta innehåll vid tidpunkten för beslutet.

Lagen bör utformas så att den tillåter ett beslut som innebär både att en viss databas ska registreras i en särskild uppgiftssamling och att databasen sedan dagligen ska uppdateras med förändringar i databasen.

9.4 Särskilda uppgiftssamlingar

9.4.1 Hur ska registrerade personuppgifter benämnas?

Förslag: Personuppgifter som registreras ska fortsätta att behandlas i särskilda uppgiftssamlingar.

Uppgifter ska behandlas i särskilda uppgiftssamlingar

Efter att uppgifter har registrerats ska de bevaras i någon form av it-miljö. Som framgår av avsnitt 9.2 är lagen endast tillämplig vid automatiserad behandling av personuppgifter. Uppgifter som registrerats kommer underkastas ett särskilt dataskydd. Det dataskydd som omfattar registrerade ska vara att uppgifterna, som huvudregel, inte ska få tas fram, se avsnitt 9.3.1 ovan. Vi har valt att använda begreppet *särskild uppgiftssamling* för att benämna de uppgifter som behandlas efter att ha registrerats med stöd av den föreslagna lagen. Begreppet uppgiftssamlingar förekommer i flera andra personuppgiftslagar. I den nuvarande säpodatalagen finns exempelvis särskilda regler som gäller uppgiftssamlingen för bearbetning och analys.

Till skillnad mot hur begreppet tidigare använts och används i annan lagstiftning är en särskild uppgiftssamling enligt denna nya lag omgärdad av mycket omfattande restriktioner i fråga om tillgång. Informationen som lagras i en särskild uppgiftssamling är därför inte att jämställas med till exempel ”gemensamt tillgängliga uppgifter”. De särskilda uppgiftssamlingarna kan snarare sägas vara motsatsen till gemensamt tillgängliga uppgifter.

Informationen i en särskild uppgiftssamling kännetecknas även av att den kan vara ostrukturerad och det ställs lägre krav för att uppgifterna ska få behandlas, så länge de inte tas fram. Ändamålet med att uppgifterna förekommer i samlingen är att de på en mer aggregerad nivå är befogade för Säkerhetspolisens verksamhet. Det

kan med säkerhet sägas att inte alla personuppgifter i den särskilda uppgiftssamlingen behövs för verksamheten.

I Förenade kungariket finns ett rättsligt ramverk för att hantera stora informationsmängder. Där definieras det som där benämns ”bulk personal dataset” bland annat av att informationsmängdens karaktär är sådan att majoriteten av individerna som förekommer i den inte är, och sannolikt inte kommer att bli, av intresse för underrättelsetjänsten. Se avsnitt 4.5.3. Vi anser inte att vår definition bör innehålla ett krav på att en särskild uppgiftssamling ska innehålla uppgifter som *inte* berör brottslig verksamhet eller liknande. Redan av kraven för registrering följer att det inte krävs att varje uppgift ska behövas för ett särskilt ändamål.

9.4.2 Vad är en särskild uppgiftssamling?

Förslag: En särskild uppgiftssamling ska utgöras av uppgifter som registrerats med stöd av lagen.

En särskild uppgiftssamling är ett juridiskt begrepp

Begreppet särskild uppgiftssamling är ett juridiskt begrepp, inte ett tekniskt. Det finns inte skäl att uppställa några krav på hur uppgifterna rent tekniskt ska bevaras, så länge lagens krav om åtkomstbegränsning upprätthålls.

Det bör därmed vara möjligt att hålla uppgifterna logiskt åtskilda genom åtkomstbegränsningar i ett system som används för andra ändamål likväl som att behandla dem i ett eller flera särskilda, tekniskt åtskilda system. Det krävs dock att säkerheten i åtkomstbegränsningen är tillräckligt stark för att säpodatalagens krav på tekniska och organisatoriska åtgärder ska vara uppfyllda. Säkerhetspolisen ansvarar för att det inte ska vara möjligt att ta fram de personuppgifter som finns registrerade i en särskild uppgiftssamling.

Trots att begreppet uppgiftssamling används i singularis finns det inte något krav på att det ska röra sig om ett sammanhållet system. Det juridiska begreppet bör kunna omfatta flera olika register, databaser, dataset eller andra slags samlingar av personuppgifter.

Endast personuppgifter omfattas av begreppet

Lagen reglerar endast personuppgiftsbehandling, vilket innebär uppgifter om fysiska personer som är i livet. Åtkomstbegränsningen avser därför endast de *personuppgifter* som registrerats. Större datamängder utgörs ofta av både personuppgifter och annan slags information. Även det senare slaget av uppgifter bör utan hinder av lagen kunna registreras, trots att det inte uppställs något krav på särskilda åtkomstbegränsningar för dem. Det krävs med andra ord inte att andra uppgifter än sådana som utgör personuppgifter tas bort för att ett visst material i sin helhet ska få registreras i en särskild uppgiftssamling.

9.4.3 Hur ska uppgifterna skyddas?

Förslag: Tillgången till personuppgifter som registrerats i en särskild uppgiftssamling ska vara begränsade genom tekniska eller organisatoriska åtgärder.

Effektiv åtkomstbegränsning är en förutsättning

De särskilda uppgiftssamlingarna kan potentiellt komma att innehålla en stor mängd personuppgifter om personer som aldrig annars skulle ha fångat Säkerhetspolisens intresse och som utan den nu föreslagna lagstiftningen inte heller skulle förekomma bland de uppgifter myndigheten behandlar. För att ett sådant system ska vara förenligt med skyddet för grundläggande fri- och rättigheter krävs ett mycket starkt dataskydd för de uppgifter som registrerats.

Ett sådant krav som vi föreslår är att de uppgifter som registrerats i en särskild uppgiftssamling ska vara förbjudna att ta fram. Undantag från detta förbud ska regleras särskilt och innebär ett krav på förhandstillstånd. Förbudet mot framtagning utgör en förutsättning för de relativt låga krav som ställs för registrering. Det innebär att förbudet måste efterlevas på ett sätt så att det är effektivt i praktiken.

Tekniska eller organisatoriska åtgärder

Vi har i avsnitt 8.20.3 förklarat att de nuvarande kraven på tekniska och organisatoriska åtgärder bör gälla även enligt vårt förslag till säpodatalag. Det innebär bland annat att det i Säkerhetspolisens behandlingssystem som regel inte ska vara möjligt att behandla andra personuppgifter än de som är nödvändiga för varje särskilt angivet ändamål. Vidare har vi ansett att de nuvarande reglerna om tillgång till personuppgifter ska fortsätta att gälla, se avsnitt 8.21.2. Det medför bland annat att tillgången till personuppgifter ska begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter. Även regleringen om säkerhetsåtgärder i nuvarande lag kommer att föras över till den nya lagen, se avsnitt 8.21.3. Detta krav innebär att Säkerhetspolisens ansvarar för att skydda de personuppgifter som behandlas mot bland annat obehörig eller otillåten behandling.

Det finns därmed redan regler som ska tillförsäkra att det inte ska vara möjligt att behandla personuppgifter på ett otillåtet sätt. Det behövs inte någon särskild regel om hur framtagningsförbudet ska upprätthållas. Det bör däremot framgå av definitionen att Säkerhetspolisen ansvarar för att möta de tekniska och organisatoriska krav som ställs upp i lagen.

Att Säkerhetspolisen upprätthåller kraven på tekniska och organisatoriska åtgärder genom datatekniska åtgärder och intern kontroll står under tillsyn. Tillsynsmyndigheternas uppdrag innefattar att kontrollera och kontinuerligt följa upp hur Säkerhetspolisen skyddar uppgifterna i särskilda uppgiftssamlingar.

9.4.4 Absolut sekretess bör gälla alla uppgifter i en särskild uppgiftssamling

Förslag: Uppgifter som är registrerade i en särskild uppgiftssamling ska omfattas av sekretess. För uppgift i en särskild uppgiftssamling ska sekretess gälla till förmån för enskilds personliga och ekonomiska förhållanden samt för Säkerhetspolisens underrättelseverksamhet.

Sekretessen ska vara absolut och gälla i högst 70 år.

Enskildas personliga förhållanden måste skyddas

Den här föreslagna lagen innebär att det finns ett dataskyddsrättsligt hinder mot att behandla personuppgifter genom att ta fram dem. Detta särskilda behandlingsförbud är riktat mot Säkerhetspolisen som personuppgiftsansvarig men ska gälla all behandling. Syftet med behandlingsförbudet är att de registrerade inte ska få sin personliga integritet kränkt genom att andra ska kunna läsa eller på annat sätt ta del av de registrerade uppgifterna. Vi anser inte att syftet med att någon tar del av de registrerade uppgifterna är avgörande för frågan om det utgör ett intrång i den personliga integriteten. Det generella förbudet mot att ta fram personuppgifter är i de registrerades intresse och utgör enligt oss en förutsättning för att behandlingen som helhet ska kunna tillåtas.

Registrerade uppgifter är allmänna handlingar

Uppgifter som registreras i särskilda uppgiftssamlingar utgör allmänna handlingar enligt 2 kap. 3 § tryckfrihetsförordningen. Eftersom lagen endast är tillämplig för automatiserad behandling kommer de registrerade uppgifterna att utgöra upptagningar. En upptagning är en handling som endast med tekniska hjälpmedel kan läsas eller avlyssnas eller uppfattas på annat sätt. Denna särskilda kategori av handlingar utgörs inte av dokument i traditionell mening utan av sakligt och logiskt sammanhängande uppgifter. Ett exempel på detta är de uppgifter som finns samlade i en digital akt.

Upptagningar regleras särskilt i 2 kap. 6 § tryckfrihetsförordningen. Där anges att en upptagning anses förvarad hos en myndighet, om upptagningen är tillgänglig för myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas eller avlyssnas eller uppfattas på annat sätt. Säkerhetspolisen kommer sannolikt endast att behandla personuppgifter som är läsbara eller på annat sätt kan göras tillgängliga för myndigheten, även om uppgifterna inte får tas fram utan tillstånd. Att myndigheten saknar tillstånd till framtagning innebär sannolikt att upptagningen ändå ska anses tillgänglig enligt bestämmelsen.

Så länge det rör sig om upptagningar bestående av sakligt och logiskt sammanhängande uppgifter utgör de handlingar enligt tryckfrihetsförordningen. När det gäller att sammanställa uppgifter ur en

upptagning för automatiserad behandling, som exempelvis resultaten av en sökning, finns särskilda regler. En sammanställning av uppgifter ur en upptagning för automatiserad behandling ska anses förvarad hos myndigheten endast om myndigheten kan göra sammanställningen tillgänglig med rutinbetonade åtgärder. Det får förutsättas att Säkerhetspolisen kommer ha tämligen avancerade möjligheter att utföra sökningar och sammanställningar i särskilda uppgiftssamlingar.

Däremot har den så kallade begränsningsregeln i 2 kap. 7 § tryckfrihetsförordningen betydelse i detta sammanhang. Den anger att en sammanställning inte ska anses vara förvarad hos myndigheten, om sammanställningen innehåller personuppgifter och myndigheten enligt lag eller förordning saknar befogenhet att göra sammanställningen tillgänglig.

Begränsningsregeln träffar begäran om utlämnande av allmän handling som innebär att en myndighet måste bryta mot ett sökförbud i sin personuppgiftslag. Den av oss föreslagna lagen innebär att Säkerhetspolisen kommer att sakna befogenhet att göra sammanställningar tillgängliga. Sammanställningar som omfattas av det generella förbudet mot framtagning kommer därför inte att utgöra allmänna handlingar. Däremot kommer begränsningsregeln inte att träffa färdiga elektroniska handlingar, som exempelvis meddelanden eller fotografier som finns registrerade i särskilda uppgiftssamlingar. Trots att sådana uppgifter inte får behandlas utgör de sannolikt allmänna handlingar som anses förvarade hos Säkerhetspolisen.

Sekretess för uppgifter i särskilda uppgiftssamlingar

Eftersom de särskilda uppgiftssamlingarna består av allmänna handlingar har som huvudregel, enligt 2 kap. 1 § tryckfrihetsförordningen, var och en rätt att ta del av dem. Som nämnts är sådan tillgång motsatsen till vad vi vill åstadkomma.

Enligt 2 kap. 2 § tryckfrihetsförordningen får rätten att ta del av allmänna handlingar begränsas för vissa syften. En begränsning av rätten att ta del av allmänna handlingar ska anges noga i offentlighets- och sekretesslagen. Frågan är om det finns sådana bestämmelser och om de är tillräckliga för att tillgodose integritetsskyddsaspekten av den föreslagna ordningen.

Sekretess till förmån för enskilds personliga förhållanden

Enskildas personliga integritet skyddas i förhållande till andra än den myndighet som behandlar uppgiften genom sekretess. Enligt 35 kap. 1 § offentlighets- och sekretesslagen gäller sekretess för enskilds personliga och ekonomiska förhållanden, om uppgiften förekommer bland annat i förundersökning i brottmål, angelägenhet som avser användning av tvångsmedel i brottmål eller i annan verksamhet för att förebygga brott. Paragrafen skyddar även uppgifter som rör säkerhetsprövning enligt säkerhetsskyddslagen (2018:585).

I Säkerhetspolisens verksamhet enligt utlännings och medborgarskapslagstiftningen kan även sekretess enligt 37 kap. 1 § offentlighets- och sekretesslagen aktualiseras. Den gäller för uppgift om en enskilds personliga förhållanden i verksamhet för kontroll över utlänningar och i ärende om svenskt medborgarskap.

Sekretess gäller om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider skada eller men.

Sekretess till förmån för Säkerhetspolisens verksamhet

Vi har uppfattningen att många uppgifter i en särskild uppgiftssamling kommer att omfattas av den nuvarande sekretessbestämmelsen i 18 kap. 2 § offentlighets- och sekretesslagen. Den så kallade underrättelsesekretessen gäller uppgift som hänför sig till bland annat Säkerhetspolisens verksamhet att förebygga, förhindra eller upptäcka brottslig verksamhet.

Sekretessen gäller med ett omvänt skaderekvisit vilket innebär att sekretess gäller, om det inte står klart att uppgiften kan röjas utan att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas. Hänvisningen till säpodatalagens underrättelseändamål innebär att även behandling enligt den särskilda regleringen i den här föreslagna lagen kommer att omfattas. Det är nämligen verksamheten som skyddas, oavsett om den regleras av säpodatalagen eller annan lagstiftning.

Att underrättelsesekretessen skyddar ”den framtida verksamheten” innebär att uppgiften i sig inte behöver vara känslig. Om uppgiften avslöjar vilka källor Säkerhetspolisen förfogar över, kan uppgiften skada den framtida verksamheten. Uppgiften om en person före-

kommer eller inte förekommer i Säkerhetspolisens register omfattas normalt av sekretess, eftersom denna fråga kan avslöja myndighetens underrättelseförmåga.

Sekretess till skydd för rikets säkerhet eller dess förhållande till andra stater eller mellanfolkliga organisationer

Frågor som rör Säkerhetspolisens förmåga kan även omfattas av försvarssekretess enligt 15 kap. 2 § offentlighets- och sekretesslagen. Vissa uppgifter som skulle störa Sveriges mellanfolkliga förbindelser, eller på annat sätt skadar landet om de röjs, omfattas även av utrikessekretess enligt 15 kap. 1 §.

Enligt båda dessa bestämmelser gäller ett rakt skaderekvisit.

Det behövs absolut sekretess för uppgifter i särskilda uppgiftssamlingar

Många av de uppgifter som kan förväntas finnas i en särskild uppgiftssamling kommer vara sekretessreglerade enligt en eller flera av de ovan nämnda sekretessbestämmelserna. Dessa regler innebär dock inte att sekretess råder för uppgiften. För att bedöma det ska utlämnandet prövas mot de olika skaderekvisiten.

Det bör inte vara möjligt att på andra sätt, med stöd av annan lag, få åtkomst till personuppgifter från en särskild uppgiftssamling. Syftet med den här föreslagna lagen är att uttryckligen förbjuda att uppgifter ens görs tillgängliga. Det bör exempelvis inte vara möjligt för en enskild att med stöd av tryckfrihetsförordningen ta del av en registrerad uppgift som allmän handling. Det ska inte heller vara möjligt för Säkerhetspolisen att ta del av de registrerade uppgifterna för att pröva ett utlämnande.

Eftersom de registrerade personuppgifterna utgör upptagningar och därmed allmänna handlingar, måste möjligheten att inskränka rätten att ta del av dem ske genom en bestämmelse om sekretess.

Det är inte lämpligt med olika slags sekretess för olika uppgifter. Om vissa uppgifter skulle omfattas av överförd sekretess och andra av primär sekretess, går systemet inte att upprätthålla enligt våra intentioner. Det krävs därför en särskild sekretessbestämmelse för alla uppgifter i en särskild uppgiftssamling. Integritetsintrånget

är mycket högt, både med hänsyn till mängden uppgifter som kan komma att behandlas och på grund av syftet med behandlingen. Vi anser att det bästa sättet att tillförsäkra uppgifterna ett tillräckligt skydd är att införa en absolut sekretessbestämmelse för uppgifter som är registrerade i en särskild uppgiftssamling. Samma skäl motiverade bland annat absolut sekretess för Skatteverkets urvals- och analysdatabas.[7]

Genom absolut sekretess finns inte skäl att göra en sekretessprövning, vilket skulle förutsätta tillgång till det material som ska sekretessprövas. Att Säkerhetspolisen får tillgång till handlingar, för att pröva om de ska lämnas ut, strider mot intentionerna i den lag vi föreslår, som innebär att personuppgifterna ska skyddas av ett framtagningsförbud.

Två nya sekretessbestämmelser

Sekretess för enskildas personliga förhållanden

Rätten att ta del av allmänna handlingar får enligt 2 kap. 2 § första stycket tryckfrihetsförordningen begränsas endast om det krävs med hänsyn till vissa intressen, bland annat skyddet för enskildas personliga eller ekonomiska förhållanden eller intresset av att förebygga eller beivra brott.

Den sekretess vi föreslår är i första hand motiverad av samma skäl som skyddet av personuppgifter. Det innebär att bestämmelsen är motiverad av skyddet för enskild. Avdelning fem i offentlighets- och sekretesslagen samlar de kapitel som avser skyddet för enskildas personliga eller ekonomiska förhållanden. I kapitel 35 finns de bestämmelser som gäller i verksamhet som syftar till att förebygga brott. En sekretessbestämmelse bör därför lämpligen införas i detta kapitel. Bestämmelsen bör införas som en ny paragraf i anslutning till 1 § där sekretess i samband med förundersökning och annan brottsförebyggande verksamhet regleras.

[7] Se prop. 2022/23:41 s. 47 f.

Sekretess för att skydda Säkerhetspolisens verksamhet

Utöver det primära intresset med sekretessbestämmelsen, som är att värna enskilds personliga integritet finns ytterligare ett skyddsintresse: Säkerhetspolisens underrättelseverksamhet. En uppgift som är registrerad i en särskild uppgiftssamling och som inte rör enskilds personliga förhållanden behöver också ett skydd. I princip bör alla uppgifter i särskilda uppgiftssamlingar som kan avslöja Säkerhetspolisens underrättelseförmåga bör vara sekretessbelagda. Uppgifter om vilken tillgång till information Säkerhetspolisen har kan vara avslöjande för bland annat verksamhetens inriktning, samarbetspartners och tekniska förmåga.

Den bestämmelse som gäller underrättelsesekretess enligt 18 kap. 2 § offentlighets- och sekretesslagen är också tillämplig på dessa förhållanden. Denna bestämmelse har ett omvänt skaderekvisit som förutsätter att sekretessen prövas i varje enskilt fall. Tidigare rådde absolut sekretess för sådana uppgifter. De skäl som anfördes mot den absoluta sekretessen har inte samma bärkraft för uppgifter i särskilda uppgiftssamlingar. Den absoluta sekretessen avskaffades för att den inneburit att intresset av insyn och kontroll åsidosatts, vilket ansågs förtroendeskadligt.[8] Vi lämnar förslag som innebär goda möjligheter för en effektiv tillsyn. Dessutom kommer varken registreringsbeslut, tillstånd eller framtagna uppgifter att omfattas av absolut sekretess. För sådana uppgifter gäller andra sekretessbestämmelser, som 15 kap. 2 § eller 18 kap. 2 § offentlighets- och sekretesslagen.

Vi anser att en absolut sekretessbestämmelse till skydd för Säkerhetspolisens verksamhet ska införas. Bestämmelsen bör införas i anslutning till underrättelsesekretessen i 18 kap. 2 § offentlighets- och sekretesslagen. Bestämmelsen bör vara utformad så att den inte endast gäller uppgifter som direkt avslöjar en förmåga utan även uppgifter som, tillsammans med andra uppgifter, kan bidra till att kartlägga underrättelseverksamheten.

[8] Prop. 1997/98:97 s. 64.

Hur länge ska sekretessen gälla?

Sekretess för uppgifter i en särskild uppgiftssamling måste gälla under hela den tid de får behandlas operativt där. När en uppgift inte längre är del av en särskild uppgiftssamling kommer den här föreslagna sekretessbestämmelsen inte längre att gälla. Det innebär att när behandlingstiden löpt ut för behandling i en särskild uppgiftssamling kommer uppgiften omfattas av annan reglering. Därmed kan tiden bestämmas så att den omfattar den tid en uppgift som längst kan behandlas. Sekretessen bör gälla högst sjuttio år, vilket är detsamma som för underrättelsesekretess enligt 18 kap. 2 § offentlighets- och sekretesslagen. Eftersom uppgifter i princip inte kommer kunna behandlas så länge i särskilda uppgiftssamlingar, kommer den faktiska sekretesstiden att vara kortare.

När upphör sekretessen?

Den absoluta sekretessen vi föreslår kommer gälla vid sidan av behandlingsförbudet som innebär att uppgifter inte får tas fram från särskilda uppgiftssamlingar.

Som vi redogör i det följande kommer sekretessen därmed att gälla endast så länge uppgifterna inte har tagits fram med stöd av ett tillstånd. När en uppgift är framtagen kommer den inte längre att omfattas av den föreslagna lagens tillämpningsområde, se avsnitt 9.2. Det innebär att en sekretessbestämmelse som hänvisar till uppgifter som behandlas med stöd av den här föreslagna lagen endast gäller för uppgifter som Säkerhetspolisen inte har tagit fram. Framtagna uppgifter kommer i stället att omfattas av de sekretessbestämmelser som i övrigt gäller i Säkerhetspolisens verksamhet.

9.5 Framtagning och annan behandling av personuppgifter

9.5.1 Vilka behandlingsåtgärder bör begränsas?

Förslag: Framtagning av personuppgifter ska inte vara tillåtet. Att en uppgift tas fram innebär att uppgifter tillgängliggörs på ett sätt som innebär att innehållet i eller innebörden av personuppgifter avslöjas.

Framtagning av uppgifter bör begränsas

Enligt vår tolkning av Europadomstolens praxis sker det största intrånget i grundläggande fri- och rättigheter när personuppgifter behandlas på så sätt att de finns tillgängliga för mänskliga ögon. Först då kan behandlingen föranleda åtgärder från myndigheten eller delas till andra. Vår uppfattning är därför att det är *framtagningen* av de personuppgifter som har registrerats som utgör den mest kritiska behandlingsåtgärden.

En framtagning kan bestå av en eller flera behandlingsåtgärder som innebär att olika urvalskriterier tillämpas på en större mängd uppgifter. Därefter tillgängliggörs de personuppgifter som träffas av dessa selektorer.

Den behandlingsåtgärd som lagstiftningen ska reglera är att personuppgifter från en särskild uppgiftssamling sammanställs enligt särskilda kriterier och visas. Ett exempel är att en selektor i form av ett personnamn används för att söka i en särskild uppgiftssamling. Om personnamnet förekommer där, kommer de uppgifter som finns registrerade om denne att tas fram och vara tillgängliga för den tjänsteman som utfört sökningen. Mer komplexa kriterier kan bestå av alla personuppgifter som relaterar till inlägg på sociala medier som uppfyller vissa selektorer kännetecknande för terrorisminnehåll. Att resultatet från en sådan sökning eller sammanställning presenteras på något sätt, utgör en framtagning.

Det finns givetvis mycket mer avancerade urvalskriterier och selektorer som kan tillämpas för att ta fram personuppgifter och denna teknik utvecklas ständigt. Algoritmiska sökningar och mjukvara som bygger på maskininlärning kan möjliggöra att personupp-

gifter tas fram efter en avancerad analys av ett stort material. Sådan automatiserad behandling av personuppgifter innebär stora möjligheter för en säkerhetstjänst men också stora risker.

För att kunna tillåta en omfattande inledande behandling och lagring av personuppgifter krävs enligt vår uppfattning att särskilda skyddsåtgärder omgärdar framtagning av dessa. Registrerade uppgifter kan därför inte vara åtkomliga på samma sätt som andra uppgifter som Säkerhetspolisen har tillgång till. De begränsningar vi anser vara nödvändiga att införa rör framtagning av personuppgifter.

I de jämförda länder som har reglerat behandling av stora informationsmängder finns exempel på strikta begränsningar för att få utföra sökningar i materialet och ta fram information. I Förenade kungariket krävs ministertillstånd som underställs ett oberoende domstolsliknande organ innan sökningar får göras och information tas fram, se avsnitt 4.5.3. I Nederländerna kan tjänstemän inom underrättelsetjänsterna göra binära sökningar, som endast ger resultatet träff eller inte träff, i stora uppgiftssamlingar. För att få ta del av informationsinnehållet från en sökning krävs att en motiverad ansökan beviljas av högre tjänstemän, se avsnitt 4.6.3. I Norge finns däremot inte några särskilda förfaranden för att säkerhetstjänsten ska kunna söka i stora informationsmängder annat än särskilda ändamålsbestämmelser. Detta fanns bland de skäl som de norska tillsynsmyndigheterna framförde i frågan om den lagstiftning är förenlig med Europakonventionen, se avsnitt 4.4.3.

En framtagning innebär att uppgiftens innehåll avslöjas

Genom att uppgifterna tas fram möjliggörs underrättelseanalys och andra åtgärder. Vi bedömer att det är i detta skede som det mest betydande intrånget sker i privatlivet för de personer vars uppgifter presenteras. Enligt de principer som vi anammat för denna lagstiftning utgör behandling i form av att uppgifter selekteras och tas fram det tredje steget i intrångstrappan, se avsnitt 9.1. Det fjärde steget innebär att uppgifter används operativt, exempelvis genom att behandlas i en underrättelseanalys.

Att uppgifter tas fram behöver emellertid inte nödvändigtvis vara detsamma som att uppgiften skrivs ut i klartext. Ett binärt svar på en ställd fråga kan enligt vår mening avslöja lika mycket som att upp-

giften finns läsbar. Exempelvis kan en selektor vara frågan om ett personnamn förekommer i en viss informationsmängd. Beroende på vilken informationsmängd det handlar om kan svaret ja eller nej vara mycket betydelsefullt, trots att det inte avslöjas var eller på vilket sätt namnet förekommer. Det ligger även nära till hands att den tekniska utvecklingen inom informationshantering redan nu eller inom kort kommer resultera i att den manuella granskningen av en analytiker får stå tillbaka till förmån för automatiserad analys.

En automatisk analys kan kringgå behovet av att behöva ta del av informationen som finns lagrad. Om lagen endast begränsade visning av uppgifter, skulle förbudet kunna kringgås på olika sätt. Med användning av AI-teknik kan det potentiellt vara möjligt att få svar om innehållet i en särskild uppgiftssamling utan att någon del av det presenteras.

De skyddsåtgärder som ska gälla framtagning måste därför omfatta alla tänkbara sätt att få information om vilka personuppgifter som finns i en särskild uppgiftssamling. Vi anser att det bör innefatta att innehållet i en registrerad personuppgift likväl som innebörden av den presenteras eller på annat sätt avslöjas. Det innebär att det inte på något sätt ska gå att sluta sig till vilka personuppgifter som finns i uppgiftssamlingen och inte heller uppgifternas innebörd eller innehåll.

9.5.2 Behandlingsåtgärder som inte innebär en framtagning bör vara tillåtna

Förslag: Annan personuppgiftsbehandling än registrering och framtagning ska kunna ske för databastekniska ändamål, för registervårdande ändamål eller för ett särskilt, uttryckligt angivet och berättigat ändamål.

Olika skydd för olika åtgärder

Moderna personuppgiftslagstiftningar är teknikneutrala på så sätt att begreppet personuppgiftsbehandling omfattar både existerande och framtida sätt att hantera information med hjälp av tekniska hjälpmedel. Det innebär att kraven för behandling enligt exempel-

vis säpodatalagen gäller både insamling och bevarande av uppgifter. Kraven träffar även sökningar i och sammanställningar av informationen liksom åtgärder som att radera eller sortera personuppgifter.

I det system vi här föreslår krävs att det dras en gräns mellan sådan personuppgiftsbehandling som ska begränsas (framtagning) och andra behandlingsåtgärder. Vår uppfattning är nämligen att det inte är nödvändigt att underkasta alla tänkbara behandlingsåtgärder lika starka dataskyddsmekanismer. Det bör exempelvis vara möjligt för Säkerhetspolisen att ägna sig åt mer eller mindre automatisk registervård även i särskilda uppgiftssamlingar. Det finns inga dataskyddsskäl som talar för att radering av en persons personuppgifter efter en viss tid eller enligt vissa villkor skulle innebära ett intrång som motiverar några särskilda skyddsåtgärder.

Behandlingsåtgärder som inte innebär en framtagning

Att behandla *andra uppgifter* än personuppgifter bör inte vara begränsat. Det gäller även uppgifter som förekommer i anslutning till personuppgifter utan att träffas av definitionen. Det kan exempelvis handla om filformat eller storlek på lagrade filer, källkod eller andra liknande uppgifter som det kan finnas behov av att bevara tillsammans med personuppgifter. Så länge den information som avslöjas varken direkt eller indirekt utgör personuppgifter bör det inte finnas några särskilda begränsningar när det gäller att läsa eller ta del av sådana uppgifter. Sådana uppgifter omfattas inte av något dataskyddsregelverk. Att dessa uppgifter däremot kan omfattas av absolut sekretess och därmed inte får lämnas ut är en annan sak. Definitionen av vad som utgör en personuppgift bör givetvis vara detsamma som i övrig lagstiftning.

För att kunna behandla stora mängder uppgifter krävs att vissa *databastekniska åtgärder* kan vidtas. Det kan bland annat röra sig om indexering eller optimering av uppgifter för att göra dem sökbara eller på annat sätt kompatibla med viss programvara. Ett annat exempel är att strukturera eller jämföra data för att undvika att flera kopior av samma information finns registrerade. Det kan även röra sig om andra tekniska åtgärder som kan underlätta fortsatt behandling av uppgifter utan att det för den delen utgör en framtagning. Att personuppgifter säkerhetskopieras, indexeras, tillförs metadata

eller struktureras på olika sätt omfattas visserligen av det behandlingsbegrepp som alla moderna personuppgiftslagar delar, men inte av de skyddsintressen som dessa lagar värnar. De exemplifierade behandlingsåtgärderna syftar till att förbereda data på olika sätt.

Vidare innebär exempelvis att personuppgifter raderas efter att behandlingstiden löpt ut en behandlingsåtgärd. Sådan *registervårdande behandling* måste givetvis vara tillåten att vidta även i särskilda uppgiftssamlingar.

Personuppgifter behandlas i olika databastekniska och registervårdande syften i alla verksamheter. Det innebär inte att uppgifter fritt får behandlas för databastekniska eller registervårdande *ändamål.* Det innebär endast att vissa tekniska eller registervårdande behandlingsåtgärder, som inte utgör en framtagning, får vidtas med personuppgifterna utan ytterligare krav. Det är inte möjligt att hantera information i en databas utan att alls ha möjlighet att ta del av informationen i syfte att göra exempelvis felsökningar. Genom att informationen tillgängliggörs blir behandlingen dock att bedöma som en framtagning som kräver ett tillstånd. Vi ser inte något skäl till att undanta sådana åtgärder från tillståndsplikt.

Bör någon annan behandlingsåtgärd omfattas av särskilda skyddsåtgärder?

De ställningstaganden som vi gjort i det föregående avser registervård och andra åtgärder som avser att säkerställa och optimera funktionen i olika datasystem. Det kan även finnas behov av att utföra olika slags automatiserade analyser.

Vissa sådana behandlingsåtgärder innebär att information på olika sätt förändras, exempelvis genom översättning eller transkribering. Andra behandlingar tillför information till personuppgifter exempelvis genom att biometriska uppgifter eller taggar för bildigenkänning skapas. Vi anser inte heller att sådana åtgärder i sig utgör ett större intrång än att behandla uppgifterna i sin ursprungsform. Däremot kan sådana åtgärder vara en förutsättning för att kunna utföra en önskad selektering; finns inte biometriska uppgifter i en bildsamling går det inte heller att utföra sökningar mot sådan data. En framtagning som bygger på biometriska uppgifter eller en automatisk översättning skulle kunna anses mer känslig eftersom data förändrats, med ökad risk för felkällor och att uppgifter tillförs som

den enskilde inte på något sätt kan kontrollera. En person kan exempelvis ha kontroll över vad denne skriver eller säger, men inte över hur detta kan komma att översättas. Vi anser ändå inte att det finns skäl att särskilt reglera sådana rutinmässiga åtgärder som förbereder data för att kunna användas på ett meningsfullt sätt genom en framtagning. Det ökade intrång i de registrerades grundläggande fri- och rättigheter som sådan bearbetning av personuppgifter medför uppstår inte förrän uppgifterna tas fram.

Vid sidan av sådana behandlingsåtgärder, vars huvudsakliga syfte är att möjliggöra, effektivisera eller förenkla framtagningar, finns emellertid behandlingar som innebär en mer kvalificerad analys av personuppgifter. Sådana behandlingsåtgärder kan bland annat innebära att personuppgifter används för att försöka förutse en händelseutveckling eller för att kartlägga nätverk. Att möjliggöra sådan automatisk analys är ett av skälen till att det överhuvudtaget finns ett behov av att behandla stora informationsmängder.

Till skillnad mot klassisk underrättelseanalys som sker av uppgifter som förfinats till underrättelser blir automatisk analys ofta bättre ju större uppgiftsmängden är. Att en persons personuppgifter ingår i en automatisk analys får anses utgöra ett större fri- och rättighetsintrång än att uppgifterna endast finns registrerade. Den granskning av en persons personuppgifter som en sådan analys innebär kan i någon mån anses utgöra övervakning och kartläggning av enskildas personliga förhållanden. Så länge resultatet av analysen inte är tillgänglig eller behandlingen avslöjar innehållet i några registrerade personuppgifter anser vi dock inte att åtgärderna är av sådant slag att de utgör ett betydande intrång i den personliga integriteten enligt 2 kap. 6 § andra stycket regeringsformen.

Givetvis gäller förbudet mot automatiskt beslutsfattande, se avsnitt 8.19.1, även uppgifter i särskilda uppgiftssamlingar. På så sätt förhindras att automatisk analys ensamt leder till ett beslut som påtagligt påverkar en enskild persons ställning. Däremot kan automatiserad analys, som med hjälp av maskininlärningsprogramvara kan detektera mönster och skeenden, i framtiden vara ett hjälpmedel vid aggregerad terrorhotsbedömning, för att bedöma påverkanskampanjer eller liknande. Sådana behandlingar kan utföras utan att uppgifter tas fram. Mot bakgrund av att sådan behandling i någon mån kan sägas utgöra en kartläggning, bör dock den behandlingen vara underkastad vissa dataskyddsprinciper. Den slags behandling

som det här är fråga om bör endast få ske om det behövs för ett konkret ändamål. Tröskeln för åtgärden är därmed densamma som för personuppgiftbehandling enligt säpodatalagen och innebär att ändamål och behov måste prövas tillsammans med proportionalitet, innan en sådan behandling utförs. Kravet på konsekvensanalys, förhandssamråd och tekniska och organisatoriska åtgärder gäller även behandling av uppgifter i särskilda uppgiftssamlingar.

De överväganden vi gjort bör komma till uttryck genom att det i lagen anges att annan behandling än framtagning får ske för att tekniskt möjliggöra, effektivisera och förenkla en framtagning (databastekniska skäl), för att upprätthålla författningsenlighet exempelvis genom att radera uppgifter i rätt tid (registervård) eller om det behövs för ett särskilt, uttryckligt angivet och berättigat ändamål. De förra fallen avser rudimentära eller rutinbetonade bearbetningar och registervård. Det senare avser andra behandlingsåtgärder, som bland annat kan innebära automatisk analys. All behandling med stöd av dessa regler förutsätter att behandlingen kan ske utan att personuppgifter i någon form tillgängliggörs. För framtagning uppställs krav på tillstånd.

9.5.3 Olika alternativ för att begränsa framtagning

Det finns flera metoder att begränsa vilka personuppgifter som får tas fram. Ett sätt är att ge anvisningar i lag avseende vilken information som får behandlas, vilka behandlingsåtgärder som får utföras och för vilket ändamål. Det skulle kunna föreskrivas att sökning i de särskilda uppgiftssamlingarna får ske endast på visst sätt, baserad på vissa data och för vissa uttryckliga ändamål. Exempelvis skulle det kunna anges att uppgifter från hemliga tvångsmedel endast får behandlas genom översättning, transkribering och sökning för ändamål som är förenliga med det ursprungliga insamlingsändamålet. En annan metod är att, i likhet med vad som gäller vid signalspaning, begränsa de sökbegrepp som får användas i en särskild uppgiftssamling som är direkt hänförliga till en viss fysisk person till fall av synnerlig vikt. Ett annat sätt kan vara att, som i Norge, begränsa registrering till ”allmänt tillgänglig information” och behandlingen till ”automatisk analys” i syfte att bidra till en viss slags underrättelser, se avsnitt 4.4.3. I Förenade kungariket finns ett relativt komplext

regelverk för stora informationsmängder. Där gäller olika regler för var och en av de metoder som får användas för att samla in uppgifterna, se avsnitt 4.5.3.

Fördelar med att direkt i lag ange hur insamlad information får vidarebehandlas är att systemet är transparent och ger medborgare en möjlighet att förutse hur insamlade personuppgifter kan komma att användas. Att bedömningen av vilka ändamål som är godtagbara och på vilket sätt uppgifter får användas sker i parlamentarisk ordning ger systemet legitimitet och möjliggör även ett demokratiskt ansvarsutkrävande.

Ett sådant lagbundet system riskerar emellertid att bli stelbent och med tiden teknikberoende. Särskilt i kontexten nationell säkerhet kan nya företeelser och hot uppkomma utan förvarning. Om nya situationer inte täcks av lagens förutsättningar, kan Säkerhetspolisens möjlighet att reagera vara begränsad. Det kan exempelvis komma att ske en teknisk utveckling som innebär att vissa källor eller visst slags information inte längre med säkerhet kan anses omfattas av ett rekvisit. Även om tillämpningen inom lagens kärnområde kan ske effektivt riskerar den att förlora i flexibilitet och teknikneutralitet.

Avgränsningsfrågor om vad som avses med ett visst snävare ändamål, en källa eller en behandlingsåtgärd kan medföra att tillämpningen med tiden försvåras av osäkerhet om en behandlingsåtgärd är laglig eller inte. För att särskilda legala begränsningar ska fylla någon integritetsstärkande funktion måste de även begränsas till de situationer där det i lagstiftningsögonblicket står klart att behovet av åtgärden överväger de andra intressena. Lämnas för stort handlingsutrymme åt den verkställande myndigheten riskerar systemet enligt vår bedömning att stå i strid med Europakonventionen. Den tekniska utvecklingen kan leda till att vissa behandlingsmetoder helt enkelt inte bör få användas.

Ett annat sätt, som är mer flexibelt, är att ställa upp mer generella begränsningar i lag. Lämpligen i form av en proportionalitetsprövning inför varje behandlingsåtgärd. Ett sådant system skulle motsvara FRA:s och Försvarsmaktens behandling av allmänt tillgänglig information. FRA och Försvarsmakten har i praktiken mycket stora möjligheter att behandla allmänt tillgänglig information, som exempelvis inhämtats från internet. Dessa myndigheter har emellertid ett betydligt mer avgränsat uppdrag och för försvarsunderrättelse-

verksamheten, en begränsande lagstiftning och en specifik inriktning beslutad av regeringen. En motsvarande reglering för Säkerhetspolisen skulle sakna dessa komponenter. Det skulle kunna anses oförenligt med Sveriges internationella åtaganden enligt Europakonventionen att begränsa behandlingen endast genom hänvisning till det breda uppdraget som följer av polislagen och Säkerhetspolisens myndighetsinstruktion. Det krävs sannolikt en mer funktionell och tydligare begränsning av myndighetens handlingsutrymme.

En annan metod är att reglera framtagning genom interna föreskrifter eller krav på ett beslut av vissa befattningshavare. För att upprätthålla ett sådant system som vilar på interna förhandsprövningar och samtidigt göra det förenligt med Europakonventionens krav på ”end-to-end safeguards” skulle det behöva kompletteras med en förstärkt tillsyn. Det skulle kunna ske genom att tillsynsmyndigheten ges ett motsvarande uppdrag som de *Judicial Commissioners* som i Förenade kungariket utövar tillsyn över varje enskilt beslut som rör särskilt integritetskänslig personuppgiftsbehandling. Ett sådant system skulle exempelvis kunna regleras genom obligatoriskt förhandssamråd med en tillsynsmyndighet.

Det finns flera fördelar med att förankra personuppgiftsbehandling med en oberoende tillsynsmyndighet. Tillsynsmyndigheten kan i dessa fall bevaka att tillämpningen inte står i strid med lagstiftarens intentioner och en intensiv tillsyn skulle kunna medföra att frågor om personlig integritet och andra fri- och rättigheter får ännu högre prioritet i verksamheten. Det finns givetvis både praktiska och juridiska komplikationer med att involvera tillsynsmyndigheten på detta sätt i det dagliga arbetet. Bland annat skulle tillsynsmyndigheten behöva ha tillräckliga befogenheter för att ett sådant system skulle utgöra en tillräckligt stark kontrollmekanism. Om ett samråd därför i praktiken skulle behöva avslutas med ett godkännande eller ett förbudsbeslut, är det snarast att likna vid ett tillståndsförfarande. Det är något som vi, av skäl som utvecklas nedan, anser lämpligen bör anförtros ett annat organ än tillsynsmyndigheten.

9.5.4 Ett tillståndsförfarande för personuppgiftsbehandling bör införas

Förslag: De personuppgifter som finns registrerade i en särskild uppgiftssamling ska endast kunna tas fram efter tillstånd.

En europarättslig utgångspunkt

Den europarättsliga utgångspunkten som vi anammat innebär att vi anser att behandling av stora informationsmängder över tid ur rättighetsintrångshänseende har likheter med hemlig avlyssning eller signalspaning. Det är därför naturligt att vända sig till Europadomstolens praxis för vägledning angående skyddsmekanismer även när det kommer till att avgöra vilket skydd som ska gälla framtagning av uppgifter. Europadomstolen återkommer med ett skäl som gäller både signalspaning[9] och hemliga tvångsmedel:[10]

> Review and supervision of secret surveillance measures may come into play at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated. As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his rights. In addition, the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning of Article 8 § 2, are not to be exceeded. In a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure.

Ett tillståndsförfarande inför en opartisk och oberoende domstol är därmed den modell som Europadomstolen i första hand förespråkar för att upprätthålla ett system med ”end-to-end safeguards” när det gäller hemlig övervakning. Enligt vår uppfattning är den prövning

[9] Se *Centrum för Rättvisa mot Sverige* p. 250, *Big Brother Watch m.fl. mot Förenade kungariket* p. 336
[10] Se *Klass m.fl. mot Tyskland* p. 55–56 och *Roman Zakharov mot Ryssland* p. 233.

som ska göras inför en framtagning ur en särskild uppgiftssamling likartad med den prövning som föregår hemliga tvångsmedel eller signalspaning, se avsnitt 7.2.3 och 9.1.3.

Tillstånd är den mest effektiva skyddsmekanismen för framtagning

Den särskilda lagstiftning vi här föreslår för att hantera stora informationsmängder är avsett att utgöra ett verktyg för underrättelseverksamhet. Som vi tidigare konstaterat, i bland annat avsnitt 3.3.2, är Säkerhetspolisens underrättelseverksamhet särpräglad i förhållande till övriga brottsbekämpande myndigheter. Den sker med en större bredd än vad som normalt gäller för kriminalunderrättelseverksamhet, men är inriktad mot ett fåtal mycket samhällsfarliga brott. För att skydda de registrerades personuppgifter är förhandstillstånd enligt oss den mest effektiva skyddsmekanismen.

Enskilda kommer inte kunna bevaka sin egen rätt. Det är givetvis uteslutet att Säkerhetspolisen skulle informera personer som är av intresse för underrättelseverksamheten om att deras personuppgifter behandlas. Avsaknaden av rättsmedel för enskilda måste därför kompenseras genom ett motsvarande rättssäkerhetsskydd. Det bästa sättet att få till stånd ett sådant skydd är att underkasta varje framtagning en tillståndsprövning.

Det finns flera andra fördelar med ett tillståndsförfarande. Till skillnad mot andra sätt att reglera tillgången till de uppgifter som registrerats enligt lagen ger förhandstillstånd inför en framtagning fördelen av teknikneutralitet och flexibilitet samtidigt som ett starkt, rättsstatligt integritetsskydd kan upprätthållas. Om exempelvis en ny kraftfull teknik utvecklas för att analysera data kan tekniken användas så länge den anses proportionerlig i förhållande till det ändamål som den ska användas för. Riskerna med en teknikneutral lagstiftning minskar om ny teknik genomgår en oberoende prövning innan den sjösätts. Samtidigt krävs inte ny eller ändrad lagstiftning för att använda nya behandlingsmetoder. Det går inte heller att utesluta att vissa framtida tekniker kommer att prövas av Europadomstolen eller omfattas av något för Sverige bindande internationellt instrument. En teknikneutral lagstiftning med förhandsprövning är i dessa fall mer flexibel än en lag som särskilt anger vissa behandlingsmetoder.

Krav på tillstånd kompenserar för undantag

Genom att tillåta behandling av stora datamängder på det sätt vi föreslår görs flera avsteg från dataskyddskonventionens bestämmelser. Det är bestämmelser som huvudsakligen syftar till att skydda den enskildes personliga integritet och andra angelägna allmänna intressen. Sådana undantag är tillåtna bland annat för att upprätthålla nationell säkerhet, så länge lagstiftningen respekterar kärnan av de grundläggande fri- och rättigheterna och utgör en nödvändig och proportionerlig åtgärd i ett demokratiskt samhälle (se artikel 11 i dataskyddskonventionen 108+).

Att tillföra en förhandsprövning av en oberoende domstol som bland annat ska pröva om en viss slags personuppgiftsbehandling är förenlig med grundläggande fri- och rättigheter är en mycket stark rättssäkerhetsmekanism. Vår uppfattning är att en sådan prövning är ett lämpligt sätt att hantera de många och komplexa frågor som kan uppkomma vid tillämpningen av den föreslagna lagstiftningen. Genom att vi ersätter vissa principer som gäller annan behandling av personuppgifter med ett oberoende och självständigt tillståndsförfarande anser vi att de grundläggande fri- och rättigheter som dataskyddet avser att upprätthålla inte urholkas. Kärnan i rättigheterna består.

9.6 Vilket prövningsorgan bör lämna tillstånd till framtagning?

9.6.1 En domstol ska lämna tillstånd

Bedömning: Förhandstillstånd till framtagning ska lämnas av en domstol.

Vi föreslår ett system med förhandskontroll innan uppgifter från en särskild uppgiftssamling får tas fram. Europadomstolen har vid upprepade tillfällen påtalat att åtgärder som kan innebära ett substantiellt intrång i de fri- och rättigheter som skyddas av Europakonventionen med fördel ska prövas av en oberoende och opartisk domstol. En sådan rättslig kontroll innebär enligt Europadomstolen den bästa garantin för oberoende, opartiskhet och ett korrekt

förfarande. Som ett alternativ kan även tillstånd lämnas av ett annat organ än domstol, så länge detta organ är oberoende och självständigt i förhållande till den exekutiva myndigheten.

Vid val av prövningsorgan har flera alternativ övervägts. En domstolsprövning är att föredra framför ett domstolsliknande organ av flera vägande skäl. För det första har Europadomstolen i sin praxis tydligt angett att domstolsprövning utgör det starkaste skyddet för den enskildes rättigheter vid hemliga tvångsmedel och signalspaning. I målet *Centrum för rättvisa mot Sverige* framhöll domstolen att ”judicial control offers the best guarantees of independence, impartiality and a proper procedure”. Även om Europadomstolen accepterar alternativa mekanismer, betraktas dessa som sekundära alternativ med ännu högre krav på oberoende och självständighet.

För det andra finns ingen befintlig nämnd eller annat domstolsliknande organ i Sverige som har den expertis som krävs för uppgiften. En nyinrättad nämnd skulle ställas inför samma utmaningar som en ny domstol vad gäller rekrytering av kvalificerad personal, säkerhetsklassning och uppbyggnad av rutiner, men utan de konstitutionella garantier för oberoende som omgärdar domares ställning.

För det tredje ger regeringsformen särskilda konstitutionella garantier för domstolars och domares oberoende som saknar motsvarighet för nämnder och andra förvaltningsmyndigheter. Domare utnämns med fullmakt och åtnjuter ett särskilt skydd mot avsättning, vilket stärker deras oberoende ställning. Detta är särskilt värdefullt när det gäller avvägningar mellan olika skyddsvärda intressen.

Sammanfattningsvis finns det starka systematiska, konstitutionella och praktiska skäl för att välja en domstolsprövning framför alternativa modeller.

9.6.2 Vilken domstol ska väljas?

Bedömning: Det finns tre huvudalternativ för hur den obligatoriska domstolsprövningen kan organiseras: inrättande av en ny specialdomstol, att ge Försvarsunderrättelsedomstolen ytterligare en uppgift eller en särskild domstol som, likt mark- och miljödomstolarna, integreras i en befintlig domstolsstruktur.

Tre huvudsakliga alternativ

Den första frågan är om prövningen kan och bör inordnas i den befintliga domstolsstrukturen med allmänna domstolar och allmänna förvaltningsdomstolar. Uppgiften att pröva om framtagning ska ske är en mycket särpräglad domstolsuppgift som inte följer av något annat dataskyddsregelverk än det föreslagna. Det ställer höga krav på säkerhet när det gäller alltifrån personal till lokaler och verksamhetsstöd. Vår bedömning är redan av det skälet att det inte är möjligt att inordna prövningen i det ordinarie domstolsväsendet.

Vi har identifierat tre huvudsakliga alternativ för domstolsprövningen:

1. *Underrättelsedomstolen*: En helt ny domstol, Underrättelsedomstolen, skulle kunna inrättas enbart för uppgiften att pröva framtagning av uppgifter från särskilda uppgiftssamlingar. En sådan domstol skulle från grunden kunna utformas specifikt för denna uppgift.
2. *Försvarsunderrättelsedomstolen*: Uppgiften att pröva framtagning av uppgifter skulle kunna läggas direkt på den redan existerande Försvarsunderrättelsedomstolen, som i dag prövar tillstånd till signalspaning enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.
3. *Särskild domstol som inrättas i annan domstol*: En tredje möjlighet är att skapa en lösning liknande den som gäller för mark- och miljödomstolarna, där en särskild domstol skapas och inordnas i en befintlig domstol (till exempel Försvarsunderrättelsedomstolen). Det skulle innebära att en domstol med särskild sammansättning utses för prövningen, men utan att formellt vara en separat specialdomstol.

Valet mellan dessa alternativ behöver göras med hänsyn till flera faktorer, såsom kostnadseffektivitet, säkerhet, kompetens och långsiktig hållbarhet för prövningssystemet.

Ny specialdomstol kräver starka skäl

Att inrätta en helt ny specialdomstol för prövningen skulle innebära att det går att utforma domstolens organisation och arbetssätt helt efter de aktuella behoven. En sådan domstol skulle från grunden kunna anpassas för mål om framtagning från särskilda uppgiftssamlingar.

Nackdelarna med detta alternativ överväger dock tydligt fördelarna. Det har sedan lång tid funnits en strävan i Sverige att undvika att inrätta specialdomstolar om det inte finns ytterst tungt vägande skäl. Flera specialdomstolar har avskaffats. För att motivera att införa en ny specialdomstol ska behovet i princip inte kunna tillgodoses på annat sätt. I detta fall finns det som framgått alternativ. Om behoven kan tillgodoses på annat sätt, talar det starkt emot att inrätta en ny specialdomstol.

Det vore vidare mycket resurskrävande att bygga upp en ny domstol. Det skulle behöva rekryteras nya domare och ledamöter med särskild kompetens, utforma lokaler med högt säkerhetsskydd samt utveckla nya rutiner för hantering av sekretessbelagda respektive säkerhetsskyddsklassificerade uppgifter. Alla dessa uppbyggnadsåtgärder skulle ta tid och resurser i anspråk. Dessutom förväntas måltillströmningen vara förhållandevis begränsad, vilket gör en helt ny domstolsorganisation ineffektiv att upprätthålla. Detta talar med styrka emot alternativet att inrätta en ny, liten domstol.

Frågan är därmed närmast om något av de andra alternativen är tillräckligt goda för att undvika att tillskapa en ny domstol.

9.6.3 Försvarsunderrättelsedomstolen bör väljas

Förslag: Försvarsunderrättelsedomstolen är den mest lämpliga instansen för att pröva frågor om tillstånd till framtagning från särskilda uppgiftssamlingar. Domstolen har nödvändig kompetens och erfarenhet. Domstolen har vidare redan etablerade säkerhetsrutiner kring bland annat medarbetare, lokaler och arbetssätt.

Försvarsunderrättelsedomstolen är mest lämpad för tillståndsgivningen

Försvarets radioanstalt ska enligt 4 a § signalspaningslagen ansöka om tillstånd för signalspaning hos Försvarsunderrättelsedomstolen. Tillstånd får enligt 5 § signalspaningslagen endast lämnas om uppdraget är förenligt med lagen (2000:130) om försvarsunderrättelseverksamhet och signalspaningslagen, syftet med inhämtningen inte kan tillgodoses på ett mindre ingripande sätt, uppdraget beräknas ge information vars värde är klart större än det integritetsintrång som inhämtning i enlighet med ansökan kan innebära, de sökbegrepp eller kategorier av sökbegrepp som är avsedda att användas är förenliga med 3 § signalspaningslagen samt ansökan inte avser endast en viss fysisk person, se avsnitt 3.6.2.

Försvarsunderrättelsedomstolen gör alltså i andra sammanhang en prövning som har likheter med den som blir aktuell vid en prövning av en ansökan om tillstånd att ta fram uppgifter från särskilda uppgiftssamlingar.

Tanken på att utvidga Försvarsunderrättelsedomstolens uppdrag är inte heller ny. I samband med remitteringen av betänkandet *Datalagring och åtkomst till elektronisk information* (SOU 2023:22) uppkom frågan om vilken instans som skulle ansvara för överprövning av Säkerhetspolisens beslut om så kallad nationell säkerhetsdatalagring. I betänkandet föreslogs att en särskilt inrättad nämnd skulle stå för överprövningen. Försvarsunderrättelsedomstolen påtalade i sitt remissvar att sambandet mellan inre och yttre säkerhet är mer direkt än tidigare till följd av globaliseringen. Även inre hot mot den nationella säkerheten har således ofta en internationell dimension. Försvarsunderrättelsedomstolen ansåg sig därför ha kompetens att bedöma hot mot den nationella säkerheten och att pröva integritetsskyddsaspekter, även vad gäller den nationella säkerhetslagringen. Åklagarmyndigheten framhöll i samma ärende att Försvarsunderrättelsedomstolen har betydande kunskaper när det gäller de aktuella frågorna om hot mot Sveriges säkerhet. Regeringskansliet har mot denna bakgrund remitterat ett utkast till lagrådsremiss med förslag att Försvarsunderrättelsedomstolen får uppdraget att överpröva Säkerhetspolisens beslut om nationell säkerhetsdatalagring.[11]

[11] Utkast till lagrådsremiss och remissvar finns i Regeringskansliets dnr Ju2024/02286.

Historiskt har det funnits en tveksamhet kring att blanda försvarsunderrättelseverksamhet (militär underrättelse, till exempel signalspaning) med den nationella säkerhetstjänsten (Säkerhetspolisens verksamhet). Ambitionen har varit hålla isär försvarsmyndigheternas underrättelsearbete och säkerhetspolisens uppdrag. Mandatet för försvarsunderrättelseverksamheten har emellertid över tid anpassats från kartläggning av ”yttre militära hot” till ”yttre hot”, vilket bland annat innebär att även internationell terrorism och grov gränsöverskridande brottslighet med säkerhetspolitiska konsekvenser kan omfattas av försvarsunderrättelseverksamheten.

Försvarsunderrättelsedomstolen har sedan lång tid byggt upp gedigen kompetens och erfarenhet av att bedöma hot mot nationell säkerhet. Dess huvuduppgift sedan tidigare är att hantera tillstånd till signalspaning enligt signalspaningslagen, vilket innebär att domstolen är väl förtrogen med att pröva ärenden som rör nationens säkerhet och integritetsskyddsfrågor.

Domstolens ledamöter – både juristdomare och särskilda ledamöter – har kunskap inom relevanta områden som underrättelseverksamhet, säkerhetsfrågor och tekniska aspekter av informationsinhämtning. Denna breda kompetens är direkt överförbar till de uppgifter som skulle bli aktuella enligt den nya lagen. Därmed finns en upparbetad förståelse för de svåra avvägningar som måste göras mellan effektivitet i underrättelsearbete och skyddet för individers rättigheter.

De likheter som finns mellan signalspaning och framtagning av uppgifter från särskilda uppgiftssamlingar understryker att en gemensam prövningsordning är naturlig:

1. Båda verksamheterna avser inhämtning och bearbetning av stora informationsmängder.
2. Båda prövningarna balanserar nationella säkerhetsintressen mot skyddet för enskildas integritet och övriga allmänna intressen.
3. Båda verksamheterna kräver en teknisk förståelse för att kunna göra korrekta rättsliga bedömningar.

Av detta framgår att det finns mycket starka skäl att låta Försvarsunderrättelsedomstolen pröva frågor enligt den nya lagen. Vi lämnar därför ett sådant förslag. Nästa fråga är emellertid vilken lagteknisk lösning som bör väljas.

9.6.4 Försvarsunderrättelsedomstolen pekas ut i den nya lagen

Förslag: Försvarsunderrättelsedomstolen ska pröva frågor om tillstånd till framtagning av personuppgifter från särskilda uppgiftssamlingar. Detta ska framgå av den nya lagen om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar. I den lagen ska även de särskilda processreglerna för prövningen finnas.

Det bästa alternativet vore en förändring av lagen om försvarsunderrättelsedomstol

Vårt förslag innebär att Försvarsunderrättelsedomstolens verksamhet kommer att stå på flera ben. Det kommer att vara en domstol med bredare inriktning mot underrättelseverksamhet. Domstolen borde därmed rätteligen benämnas Underrättelsedomstolen. Det naturliga vore i detta läge att ersätta lagen (2009:966) om Försvarsunderrättelsedomstol med en ny lag om Underrättelsedomstol. I den lagen skulle en gemensam del kunna behandla frågor som domstolens uppdrag, sammansättning, domförhetsregler, sekretess, förhandlingsoffentlighet med mera. Det kunde sedan följa separata kapitel för den prövning som ska ske inom de olika områden som domstolen har att hantera (till exempel signalspaning, nationell säkerhetsdatalagring och framtagning från särskilda uppgiftssamlingar). En sådan lösning skulle även vara flexibel för eventuella framtida uppdrag för domstolen.

Vi har emellertid inte ansett att det ligger inom vårt mandat att föreslå så stora förändringar i lagen om Försvarsunderrättelsedomstol. Förändringar i den lagen skulle komma att antingen påverka även signalspaningsmål eller kräva större strukturella förändringar av lagen. Om regeringen anser att uppdraget, som vi föreslår, ska läggas på Försvarsunderrättelsedomstolen bör det dock övervägas att i särskild ordning ta fram beredningsunderlag för en samordning av de processuella reglerna i en gemensam lag.

Försvarsunderrättelsedomstolen bör pekas ut direkt i den nya lagen

Våra slutsatser hittills gör att det återstår två lagtekniska alternativ. En möjlighet är att föreslå en lag om underrättelsedomstol, som blir en särskild domstol, och sedan i författning peka ut att Försvarsunderrättelsedomstolen ska vara underrättelsedomstol. Det andra alternativet är att direkt i den föreslagna lagen om behandling av personuppgifter i särskilda uppgiftssamlingar peka ut Försvarsunderrättelsedomstolen. De processuella reglerna skulle då finnas i den materiella lagen.

Ett av alternativen är som framgått att inrätta en särskild domstol som sedan inordnas i en befintlig domstol. Detta är en känd konstruktion på vissa områden. Som exempel kan nämnas mark- och miljödomstolarna och patent- och marknadsdomstolen. Ofta drivs denna konstruktion fram av en vilja att skapa särskilda sammansättningsregler och ofta med särskilda personalkategorier som inte finns i domstolen i övrigt, till exempel tekniska råd och patentråd.

Det är en tämligen komplicerad konstruktion och skapar vissa inlåsande effekter. Som framgått anser vi att ett bättre alternativ i detta fall vore att mer genomgripande förändra lagen om Försvarsunderrättelsedomstol. Det saknas även för de fall som nu är aktuella behov av andra sammansättningsregler än de som redan gäller för prövning i Försvarsunderrättelsedomstolen. Skulle lagstiftaren i framtiden vilja justera regelverket i linje med vad vi skisserat tidigare, blir det svårare om en konstruktion med särskild domstol har valts.

En fristående lösning är enklare att anpassa vid framtida lagändringar, medan en mark- och miljödomstols-liknande modell kan medföra att förändringar kräver mer omfattande omstrukturering. Vi lämnar därför inte något sådant förslag.

Efter att ha vägt alternativen framstår det således som att det bästa alternativet är att Försvarsunderrättelsedomstolen pekas ut direkt i lagen. Det innebär att de processuella reglerna också bör framgå av lagen. Att Försvarsunderrättelsedomstolen därmed kommer att ha att tillämpa processregler dels i lagen om Försvarsunderrättelsedomstol och i signalspaningslagen, dels i den lag vi här föreslår är inte något unikt. Motsvarande situation förekommer relativt frekvent i förvaltningsprocessen.

9.6.5 Anpassning av lagen om Försvarsunderrättelsedomstol

Förslag: Försvarsunderrättelsedomstolens uppdrag justeras till att omfatta tillstånd till framtagning från särskilda uppgiftssamlingar.

Sammansättningsreglerna ändras så att domstolen kan bestå av högst två ordförande, högst två vice ordförande samt minst två och högst tio särskilda ledamöter.

Det föreslås även vissa följdändringar för att anpassa lagstiftningen till att det kan finnas flera ordföranden i domstolen och att en av dem ska vara chef för domstolen.

Skälen för förslaget

Eftersom valet faller på Försvarsunderrättelsedomstolen behöver lagstiftningen justeras för att ge domstolen det nya ansvaret. Vi har strävat efter att göra detta på ett sätt som minimerar komplexiteten och undviker onödigt omfattande lagändringar.

Den huvudsakliga ändringen är en utvidgning av domstolens uppgifter. I lagens inledande paragraf bör en ny punkt läggas till, som anger att domstolen ska pröva frågor om tillstånd till framtagning enligt den nya lagen. Detta är den enklaste lösningen för att ge domstolen ytterligare en uppgift. Det motsvarar även den metod som används i utkastet till lagrådsremiss angående nationell säkerhetsdatalagring. Domstolen kan alltså potentiellt ha tre uppgifter när alla nu aktuella lagförslag är hanterade.

Försvarsunderrättelsedomstolen kommer att behöva vissa resursförstärkningar för att klara av den ökade arbetsbördan som tillståndsprövningen av framtagning från särskilda uppgiftssamlingar medför. Detta behandlas närmare i avsnitt 12.5.4. Det är förstås svårbedömt vad den nya uppgiften kommer att kräva i form av dömande och administrativ personal. Det är dock uppenbart att det efter en tid kan visa sig för lite med endast en ordinarie domare i domstolen och maximalt sex särskilda ledamöter. Lagstiftningen bör därför medge en utökning av antalet möjliga ledamöter i domstolen.

Samtidigt finns det goda konstitutionella skäl att inte medge ett alltför högt antal möjliga domare i domstolen.

Vi föreslår därför att Försvarsunderrättelsedomstolen ska kunna ha upp till två ordförande (varav en är chef för domstolen), upp till två vice ordförande samt mellan två och tio särskilda ledamöter. Detta ska jämföras med nuvarande ordning där domstolen har en ordförande, högst två vice ordförande och två till sex särskilda ledamöter.

9.7 Tillståndet

9.7.1 Förutsättningar för att lämna tillstånd

Förslag: Tillstånd till framtagning får endast lämnas om

1. åtgärden står i överensstämmelse med lag och Sveriges internationella åtaganden,
2. åtgärden kan antas vara nödvändig för ändamålet, och
3. det står klart att intresset av åtgärden överväger andra enskilda och allmänna intressen.

Vi har ansett att framtagning ska vara den behandlingsåtgärd som ska vara tillståndspliktig. Prövningen ska avse frågan om det ska göras ett undantag från förbudet att ta fram uppgifter som registrerats. Det generella förbudet utgör en stark dataskyddsmekanism. Att det är en domstol som ska besluta om undantag från detta förbud har vi motiverat bland annat av att det utgör det starkaste skyddet för personuppgifter, samtidigt som Säkerhetspolisen kan behandla stora informationsmängder.

Domstolen bör pröva om en framtagning utgör ett berättigat undantag från skyddet av den personliga integriteten, rätten till privatliv och de allmänna intressen som aktualiseras. Det innebär att domstolen ska pröva om ett tillstånd kan lämnas utifrån kraven på legalitet, nödvändighet och proportionalitet. Dessa krav är förutsättningar för att begränsa grundläggande fri- och rättigheter enligt både regeringsformen och Europakonventionen. Enligt dataskyddskonventionen 108+ är en förutsättning för undantag, enligt artikel 11 att de sker med respekt för grundläggande fri- och rättigheter och utgör en nödvändig och proportionerlig åtgärd i ett demokratiskt samhälle, bland annat för att skydda nationell säkerhet.

Tillståndsprövningen bör omfatta alla de krav som ställs på att begränsa en fri- och rättighet.

För det första krävs att åtgärdens laglighet prövas. Det innebär ett krav på rättslig grund för behandlingen samt författningsenlighet i övrigt. En framtagning måste vara förenlig med en rättslig grund för personuppgiftsbehandling, det vill säga ett av myndighetens författningsreglerade uppdrag. Kravet på laglighet bör även innefatta en prövning av att framtagningen står i överenstämmelse med Sveriges internationella åtaganden. För det andra måste åtgärdens nödvändighet prövas. Det innebär att behandlingen ska behövas för ändamålet och detta behov ska inte vara möjligt att uppnå med mindre ingripande medel. Slutligen ska proportionaliteten prövas, genom att skälen för åtgärden vägs mot de andra intressen som kan påverkas.

Kraven är därmed i praktiken desamma som gäller för annan personuppgiftsbehandling, med den skillnad att den görs efter en ansökan från Säkerhetspolisen i det enskilda fallet.

9.7.2 Varje enskild framtagning eller framtagningar av ett visst slag?

Det finns i praktiken två sätt att se på tillståndsplikten. Antingen ska varje enskild framtagning tillståndsprövas eller också vissa typer av framtagningar. Det förra synsättet innebär att Säkerhetspolisen ska söka om tillstånd för vissa, uttryckliga sökkriterier och domstolen ger tillstånd för att dessa och inga andra får användas vid ett eller flera behandlingstillfällen. En sådan process skulle innebära att domstolen får en stor insyn i de behandlingar som utförs och ett starkt inflytande över underrättelseverksamheten. Det är emellertid ett mycket tungt prövningsförfarande som inte heller respekterar ansvarsfördelningen mellan myndighetsutövning och rättsskipning. Det kan förväntas att Säkerhetspolisen kommer behöva använda ett stort antal sökkriterier vid många tillfällen varje dag. En tillståndsprocess för varje enskild framtagning skulle därför inte heller vara möjlig att administrera på ett rimligt sätt.

Utgångspunkten måste därför vara att tillstånd ska kunna gälla en viss typ av framtagningar som får utföras under en viss begränsad tid. Sökkriterierna måste därför kunna anges med ett visst mått av abstraktion. Det innebär att det ska vara möjligt att exempelvis göra

sökningar efter aktörer där det finns kända underrättelsemisstankar eller framtagningar som sker efter att en viss, närmare angiven, automatisk analysmetod har tillämpats.

Tillståndsprövningen bör vara likartad den som gäller för signalspaningsmyndigheten enligt signalspaningslagen. Enligt denna lagstiftning ges tillstånd för ett visst tidsbegränsat inhämtningsuppdrag, där de sökbegrepp eller kategorier av sökbegrepp som får användas vid inhämtningen anges.

För trådbunden signalspaning omfattar ett inhämtningsuppdrag vissa signalbärare. För den tillståndsprocess vi här föreslår bör tillstånd till framtagning avse vissa källor eller vissa kategorier av uppgifter. Rättighetsintrånget beror i stor utsträckning på vilken typ av information som framtagning sker från. Det är givetvis stor skillnad om en sökning görs mot en elektronisk telefonkatalog, från sociala medier, från överskottsinformation från hemlig avlyssning eller från dekrypterade kommunikationstjänster. Det kan därför finnas skäl att formulera tillstånden till framtagning olika beroende på vilken slags uppgifter som ska behandlas.

Om tillståndet avser framtagningar av visst slag, kommer även frågan om tillståndet ska avse endast de personuppgifter som finns registrerade vid tillfället för ansökan eller om även framtida registreringar ska omfattas. Det finns både praktiska och systematiska skäl som talar för att det senare ska vara fallet. Många av de källor som kommer att finnas registrerade avser uppgifter som behöver hållas uppdaterade. Sökningar och framtagning ur sådana källor måste kunna ske löpande och inte kräva nya tillstånd dagligen. Vidare avser prövningen en riskbedömning. Det är inte känt för vare sig domstolen eller Säkerhetspolisen exakt vilka uppgifter som registrerats.

Säkerhetspolisen bör därför ha möjlighet att inom tillståndets ramar göra de sökningar, sammanställa och framtagningar från det innehåll som uppgiftssamlingarna har vid varje given tidpunkt. Om de särskilda uppgiftssamlingar som omfattas av tillståndet ändras påtagligt efter det att tillståndet har meddelats, bör saken uppmärksammas av Säkerhetspolisen eller tillsynsmyndigheten i samband med en eventuell ansökan om förlängning av tillståndet.

9.7.3 Tidsbegränsning

Förslag: Ett tillstånd till framtagning ska gälla i viss tid.

För tillstånd till signalspaning har sedan länge gällt en tidsgräns om sex månader. Detta trots att de företeelser som gäller exempelvis militära förhållanden i vårt närområde kan vara av intresse under mycket lång tid. Tidsbegränsningen är därför inte avsedd att markera hur länge verksamheten får bedrivas utan säkerställer att behovet omprövas med tillräcklig regelbundenhet.

Vi anser att det är självklart att beslut om framtagning måste vara tidsbegränsade. Den största integritetsvinsten med tillståndsförfarandet kommer av att domstolen har möjlighet att regelbundet följa upp hur ett meddelat tillstånd har tillämpats. Vi anser däremot inte att det finns skäl att föreskriva en yttersta tidsgräns. Det finns inte skäl att ompröva ett tillstånd som endast avser exempelvis framtagning ur en elektronisk telefonkatalog eller liknande lika ofta som mer känsliga tillstånd, exempelvis sådana som sker med ny teknik. Det är därför tillräckligt att föreskriva att tillstånd ska vara tidsbegränsade.

9.7.4 Uppgiftsminimering

Förslag: En framtagning får inte förväntas leda till att fler personuppgifter än vad som är nödvändigt för ändamålet behandlas.

Vi har i avsnitt 9.3.3 kommit till slutsatsen att principen om uppgiftsminimering står i motsats till syftet med att kunna behandla personuppgifter i särskilda uppgiftssamlingar.

Det finns däremot möjlighet att tillämpa principen vid framtagning. Vid en proportionalitetsprövning ingår frågan om att intrånget inte ska vara större än vad som behövs för ändamålet. Det bör även komma till uttryck genom att inte fler uppgifter än vad som behövs ska kunna tas fram med stöd av ett tillstånd. Ett sådant krav markerar att den viktiga dataskyddsprincipen om uppgiftsminimering ska inverka på prövningen.

9.8 Tillståndsprocessen

9.8.1 Processregler i den nya lagen

Bedömning: De närmare processreglerna för prövning av framtagning av uppgifter från särskilda uppgiftssamlingar bör införas den nya lagen. De nya reglerna ska så långt möjligt ansluta till motsvarande regler vid prövning av mål om signalspaning.

Förslag: Lagen om Försvarsunderrättelsedomstol ska hänvisa till den lagen om särskilda uppgiftssamlingar.

Skälen för bedömningen och förslaget

De processuella bestämmelserna som gäller för tillståndsprövning av frågor som rör signalspaning är utformade för att möjliggöra ett effektivt och rättssäkert förfarande. Det finns, som nämnts, skäl att göra så små förändringar som möjligt i den nuvarande ordningen. De processuella bestämmelserna för tillstånd till framtagning bör därför ansluta till det existerade regelverket där det är lämpligt.

De processregler som ska gälla endast för mål om tillstånd till framtagning ska införas i den föreslagna lagen om särskilda uppgiftssamlingar. De flesta reglerna i lagen om Försvarsunderrättelsedomstol kommer således endast att gälla i mål om signalspaning. I lagen om Försvarsunderrättelsedomstol bör det införas en upplysningsbestämmelse som klargör att det i den föreslagna lagen finns särskilda processregler för en prövning av en ansökan om framtagning.

9.8.2 Hur bör ansökan vara utformad?

Förslag: Säkerhetspolisen ska i ansökan om tillstånd till framtagning av information i särskilda uppgiftssamlingar ange

1. vilka kategorier av uppgifter framtagningen ska avse och från vilka typer av källor framtagning ska ske,
2. det särskilda ändamålet med och behovet av framtagningen,

3. vilka sökbegrepp, kategorier av sökbegrepp eller andra urvalskriterier som är avsedda att användas vid framtagningen och, om det finns skäl, med vilken teknik urvalet ska ske,
4. vilken tid tillståndet ska gälla, och
5. de skäl och omständigheter i övrigt som myndigheten vill åberopa till stöd för sin ansökan.

Vad syftar ansökan till?

En ansökan avser att ge förutsättningar för en rättssäker framtagning som respekterar kärnan i de grundläggande fri- och rättigheterna som påverkas av den personuppgiftsbehandling som sker med stöd av den föreslagna lagen. Som framgår av avsnitt 7.1.3 är vår uppfattning att lagregleringen ska vara begränsad till vad som är nödvändigt för lagens syften. Endast de uppgifter som är nödvändiga för prövningen bör därför formaliseras i lag.

Det krävs därmed att Säkerhetspolisen bidrar med den information som behövs för att pröva legalitet, nödvändighet och proportionalitet. Att en ansökan är formaliserad och att det i lagen anges hur den ska vara utformad skapar en ram för denna prövning. I det följande utvecklas kraven som vi anser bör ställas på innehållet i en ansökan.

Kategorier av uppgifter och källor för framtagningen

För att kunna göra en proportionalitetsprövning kan det finnas ett behov att bedöma omfattningen av de uppgifter som kommer att behandlas genom en framtagning. En framtagning innebär att uppgifter prövas mot olika urvalskriterier eller selektorer. Vilket underlag som dessa selektorer kommer att appliceras på kan påverka hur stort intrång som sökningen och framtagningen innebär.

Som en del av principen om uppgiftsminimering ska ansökan inte omfatta fler uppgifter än nödvändigt. Eftersom det redan av ett registreringsbeslut ska anges vilken slags uppgifter som registreras, kan det vara möjligt att göra ett urval av kategorier eller källor som är relevanta genom att hänvisa till denna beskrivning. Ett annat sätt

kan vara att peka ut vissa källor eller att begränsa ansökan till uppgifter som registrerats under en viss tidsperiod.

I mål enligt signalspaningslagen prövar domstolen vilka så kallade signalbärare som ska omfattas av signalspaningen. Enligt den prövningen ska beskrivningen av signalbärarna göras på ett sådant sätt att domstolen kan bedöma omfattningen av det integritetsintrång som kan bli följden av att tillgång ges till signalbärarna.[12] Det finns anledning att se på kategorier och källor för framtagning på ett liknande sätt. Det bör dock som framgått inte finnas något hinder mot att en ansökan omfattar källor som inte ännu har registrerats.

Ändamål och behov

Ändamålet med framtagningen är helt centralt för proportionalitetsprövningen. Ändamålet måste givetvis vara särskilt, i den mening som avses i säpodatalagen, vilket innebär att det inte är tillräckligt med det breda ändamål som kan föranleda inledande behandling eller registrering. Att ändamålet anges i en ansökan innebär att det är uttryckligt angivet. Domstolen prövar om ändamålet är berättigat.

Att behovet ska anges är på samma sätt centralt för prövningen. Det krävs för att det ska stå klart att undantaget från skyddet av personuppgifter, som en framtagning innebär, är nödvändigt i ett demokratiskt samhälle.

Sökbegrepp och teknik

Sökbegrepp är en central del av Försvarsunderrättelsedomstolens prövning enligt signalspaningslagen. Den erfarenhet och kompetens som domstolen förvärvat inom ramen för den verksamheten kommer kunna utnyttjas för att bedöma sökbegrepp även för framtagning.

Sökbegrepp, selektorer och andra urvalskriterier har en nära anknytning till ändamålet med framtagningen. Genom sökbegreppen kan domstolen bilda sig en uppfattning om ändamålet kommer att kunna uppnås och om urvalskriterierna riskerar att medge framtagning av uppgifter som inte behövs för ändamålet.

[12] Prop. 2008/09:201 s. 52.

Att vi anser det nödvändigt att i vissa fall redogöra för och tillståndspröva den teknik som ska användas utgör en skyddsmekanism mot att lagen utnyttjas på ett sätt som inte varit förutsett. Det är mycket svårt att förutse vilka möjligheter som kommer finnas att göra en selektion av personuppgifter om, eller när, nya AI-förmågor kan tillämpas. Vissa nya tekniker kommer att föra med sig olika risker. Vi anser därför att det är viktigt att domstolen kan begränsa teknik som utgör en risk som inte står i proportion med nyttan.

Skäl och övriga omständigheter

Det kan krävas både en bakgrund och en redogörelse för den bredare underrättelsebilden för att domstolen ska ha en möjlighet att bedöma en åtgärds proportionalitet. Det kan handla om generella hotbilder, förändringar i olika miljöer eller framväxten av nya företeelser.

Den proportionalitetsbedömning som Säkerhetspolisen har gjort kan behöva motiveras både rättsligt och sakligt. Genom att uppställa ett krav på skäl och övriga omständigheter ges också en möjlighet för domstolen att begära komplettering i de avseenden som domstolen finner nödvändigt.

9.8.3 Rent ansökningsförfarande eller en kontradiktorisk process?

Bedömning: Ansökningsprocessen bör ha kontradiktoriska inslag. Det finns skäl att uppgifter som framkommit vid tillsynen även ska kunna utgöra underlag vid tillståndsprövning.

Olika alternativ för förfarandet

En tillståndsprocess kan utgöra ett ansökningsförfarande som endast innefattar Säkerhetspolisen och domstolen. Det är även möjligt att involvera någon ytterligare aktör vars syfte är att bistå med viss kompetens eller belysa frågan från ett annat perspektiv. Slutligen kan en process, som då innebär faktisk kontradiktorisk rättsskipning, innefatta två eller fler parter som är fria att vidta rättshandlingar och dispositioner i processen. Det går även att utforma ett kvasikontradik-

toriskt system där exempelvis en ytterligare aktör har rätt att klaga på ett beslut och vara part i överrätt eller där en aktör har yttranderätt, utan att vara part.

Vi har i avsnitt 9.6.3 lämnat förslag om att det är Försvarsunderrättelsedomstolen som ska vara prövningsorgan. Det mest naturliga är därför att ta inspiration från den ansökningsprocess som gäller för signalspaning.

Ett rent ansökningsförfarande?

Ett rent ansökningsförfarande innebär att Säkerhetspolisen ansöker hos domstolen om en åtgärd. Ett sådant enpartsförfarande har inte de drag som är utmärkande för den domstolsprocess som enligt Europadomstolen utgör den bästa garanten för ett självständigt, opartiskt och korrekt förfarande. Däremot kan ett rent ansökningsförfarande hos ett domstolsliknande organ ge tillräckliga konstitutionella rättssäkerhetsgarantier. Då Försvarsunderrättelsedomstolen utreddes ansågs domstolens sammansättning kunna kompensera för att endast en part deltog som sökande i mål rörande signalspaning. Bland domstolens ledamöter skulle nämligen finnas personer med erfarenhet och kunskap om underrättelseverksamhet jämte ledamöter med särskild förmåga att belysa integritetsskyddsintresset. I stället för att bevakningen av integritetsskyddsintresset skulle läggas utanför rätten ansågs detta ansvar integrerat i domstolens uppgift genom att de ledamöter som utses har förmåga att ta nödvändiga integritetshänsyn.[13]

Regeringen beaktade dock den remisskritik mot förslaget som bland annat innebar att prövningen inte i tillräcklig grad motsvarar den som i övrigt förekommer vid domstolar, framför allt med avseende på partsställningen.[14]

Vi delar bedömningen att de aktörer som förekommer i en domstolsprocess har betydelse för hur rättssäker prövningen blir. En domstol utmärks av att processen tillåter att olika perspektiv bryts mot varandra och att en parts uppfattning inte står oemotsagd. Det är svårt att upprätthålla den dynamiken i ett rent ansökningsförfa-

[13] Ds 2009:1 s. 78–79.
[14] Prop. 2008/09:201 s. 70.

rande. Även om det är tillåtet med en sådan process, är en reell domstolsprövning att föredra.

En kontradiktorisk process?

Det svårt att hitta någon naturlig motpart till Säkerhetspolisen i en kontradiktorisk process. Vid en framtagning har varje individ som kan tänkas vara registrerad och omfattas av framtagningskriterierna potentiellt andra intressen än Säkerhetspolisen. Dessa personer kan emellertid inte företräda sina intressen i processen, naturligtvis inte direkt, men inte heller indirekt. Det är nämligen inte möjligt att alla gånger veta vilka som kan omfattas av en framtagning.

En framtagning är inte begränsad till sökningar på kända personuppgifter utan kan lika gärna ske efter kriterier som syftar till att hitta tidigare okända aktörer. Det kan därför aldrig bli fråga om en äkta kontradiktorisk process.

De personer som potentiellt kan omfattas av framtagningskriterierna kan visserligen antas bestrida ansökan, men kan varken själva eller genom ombud ges talerätt.

Offentliga ombud eller integritetsombud?

Bakgrunden till ombudssystemet

Inom annan övervakningslagstiftning, som hanteras av de allmänna domstolarna, finns offentliga ombud. Offentliga ombud ska bevaka enskildas integritetsintressen i ärenden hos domstol om bland annat hemlig avlyssning av elektronisk kommunikation och hemlig kameraövervakning. Ett offentligt ombud har rätt att ta del av det som förekommer i ärendet, yttra sig i ärendet och överklaga rättens beslut. I mål hos Försvarsunderrättelsedomstolen som rör tillstånd till signalspaning förekommer i dag så kallade integritetsskyddsombud som ska bevaka enskildas integritetsintresse i mål vid domstolen. Ombudet har rätt att ta del av det som förekommer i målet och att yttra sig. Till skillnad mot vad som gäller för hemliga tvångsmedel finns ingen möjlighet att överklaga Försvarsunderrättelsedomstolens domar och integritetsskyddsombudens roll är därmed mer begränsad. Det förslag om ett prövningsförfarande för nationell säkerhets-

datalagring, som föreslås träda i kraft den 1 mars 2026, innebär att ett särskilt offentligt ombud för nationell säkerhetslagring ska bevaka enskildas intressen.

Gemensamt för dessa ombud är att de ska ha hög juridisk kompetens och att de utses av regeringen för en viss tid på förslag från Domarnämnden och Sveriges advokatsamfund. Dessa ombud har inte tillgång till annat material än domstolen och deras roll är därmed begränsad till att argumentera för de intressen som de är satta att ta tillvara och, för de offentliga ombuden vid de allmänna domstolarna, att överklaga tveksamma fall.

Synen på dessa ombud har skiftat över tid. Lagstiftaren var tidigare mycket skeptisk till om ombuden fyllde någon reell funktion då denna var hänvisad till samma utredning som sökanden åberopade till stöd för ansökan.[15] SÄPO-kommittén gick så långt att beskriva ett system med allmänt ombud i det närmaste som en skenprocess.[16] Under 2000-talet omprövades dock den tidigare uppfattningen och flera fördelar med en oberoende ombudsroll som har till särskild uppgift att bevaka enskildas intressen lyftes fram. Offentliga ombud infördes därför i tillståndsprocessen för de hemliga tvångsmedlen. Genom införandet av ett system med offentliga ombud skapas enligt regeringen ett slags kontradiktorisk process som ger bättre förutsättningar för en allsidig belysning av saken.[17] Då signalspaningslagen reformerades under slutet av 2000-talet fick integritetsfrågorna ett stort utrymme. Domstolsprövning med endast en sökande som part ansågs inte i tillräcklig grad motsvara den prövning som i övrigt förekommer vid domstolar. Systemet med integritetsskyddsombud infördes för att ge prövningen en tydligare kontradiktorisk karaktär med ett ombud som representerade det intresse som står i motsatsförhållande till den ansökande myndighetens.[18] Det offentliga ombud för nationell säkerhetslagring föreslås att, vid sidan av enskildas integritetsintresse, även ha till uppdrag att bevaka det ekonomiska intresset hos de företag som ska tillhandahålla datalagring.[19]

[15] Prop. 1988/89:124 s. 53 f.
[16] SOU 1990:51 s. 176 f.
[17] Prop. 2002/03:74 s. 22–24.
[18] Prop. 2008/09:201 s. 70–71.
[19] Utkast till lagrådsremiss, *Datalagring och tillgång till elektronisk information*, s. 52.

Vilken roll har ombuden i tillsynssystemet?

Det finns ett europarättsligt krav på effektiva skyddsmekanismer genom hela processen, inbegripet tillstånd och tillsyn. De offentliga ombudens roll är att förstärka tillståndsprocessen. Varken i tvångsmedelslagstiftningen eller signalspaningslagen har de offentliga ombuden någon roll att spela i den efterföljande tillsynen av hur tillstånden följs.

Ombudens roll sträcker sig inte längre än processen för att pröva tillståndet. Ombudet kan därmed inte få reda på vilka konsekvenser eller vilken effekt tillståndet haft för de intressen som ombudet ska värna. Den efterföljande tillsynen sköts av myndigheter som i sin tur inte har någon del i tillståndsprocessen. Det råder även en mycket sträng sekretess för alla uppgifter som förekommer, både vid tillstånd och tillsyn. Det är därför knappast möjligt för tillsynsmyndigheten att vända sig till ett offentligt ombud eller ett integritetsskyddsombud för att framföra synpunkter på hur tillståndet tillämpas i verksamheten.

På så sätt får inte heller domstolen med säkerhet reda på om tillstånden är välavvägda eller tillräckligt avgränsade i förhållande till andra intressen än sökandens. Det är nämligen endast sökanden som känner till både vad som förekommit vid tillståndsförfarandet och vilka eventuella synpunkter tillsynsmyndigheten haft på hur tillståndet utnyttjats.

Ett sätt att berika processen med erfarenheter från tillsynen skulle kunna vara att föreskriva att ett eventuellt offentligt ombud eller liknande deltar i processen och ska samråda med tillsynsmyndigheten eller på annat sätt inhämta underlag i samband med processen. Det skulle då kunna vara en tillkommande roll för ombudet, vid sidan av att självständigt representera de intressen som står i motsats till sökandens.

En annan lösning skulle vara att ersätta ombudets roll i processen med tillsynsmyndigheten, företrädesvis i form av Säkerhets- och integritetsskyddsnämnden. Denna lösning framstår som mer effektiv.

9.8.4 Säkerhets- och integritetsskyddsnämnden ska yttra sig i samband med ett tillståndsförfarande

Förslag: Den särskilda tillsynsmyndigheten ska ges tillfälle att yttra sig över ansökan.

Integritetsskyddsombud ska endast användas i mål om signalspaning och inte när det gäller andra måltyper i Försvarsunderrättelsedomstolen.

Kan Säkerhets- och integritetsskyddsnämnden få en roll i tillståndsprocessen?

Den process som ska tillgodose kraven på ett rättssäkert förfarande för framtagning bör vara så robust som möjligt. De två viktigaste länkarna i den kedjan är domstolen och tillsynsmyndigheten. Vi anser att betydande rättsäkerhetsvinster skulle kunna uppnås om tillsynsmyndigheten, som har förutsättningar att få kännedom om hur besluten verkställs även har en möjlighet att förmedla detta till domstolen. Detta får sägas vara ett särskilt uttalat behov för en så pass teknikneutral och flexibel lagstiftning som vi här föreslår.

Det kan i många fall vara svårt att förutse hur omfattande integritetsintrång en viss framtagning faktiskt kan resultera i. Givetvis kan den verkställande myndigheten välja att redovisa detta till domstolen om ett tillstånd söks på nytt, men det kontradiktoriska momentet som tillsynsmyndigheten kan bidra med får anses medföra ett betydligt större rättighetsskydd. Viljan att belysa brister i tillståndet till men för andra intressen än verksamhetens får antas vara lägre hos den verkställande myndigheten än hos tillsynsmyndigheten. I vissa fall kan det visa sig att ett tillstånd inte är proportionerligt först efter att det börjat tillämpas. Så kan exempelvis vara fallet då det rör sig om att tillämpa ny teknik eller nya metoder.

Generellt har en kontradiktorisk process stora fördelar i förhållande till ett rent ansökningsförfarande. En motpart som företräder andra intressen än sökanden berikar både det material som domstolen ska ta ställning till och den rättsliga diskussionen. Det finns goda skäl ge även en röst till samhällsintressen som indirekt eller direkt står i motsatsförhållande till de intressen som föranleder ansökningen. Ett offentligt ombud kan ges ett tydligt intresse att bevaka

i processen, vilket inte på samma sätt låter sig göras för en annan myndighet under regeringen. Det går dock inte att bortse från skillnaden i styrkeförhållanden mellan den ansökande myndigheten och en representant för allmänheten, som ofta utgörs av en pensionerad domare eller advokat. För att bedöma en ansökan om framtagning och på ett relevant sätt lämna synpunkter på den kommer det ofta att krävas ett inte obetydligt mått av tekniskt kunnande.

Tillståndsförfarandet syftar bland annat till att möjliggöra och samtidigt kontrollera införandet av ny teknik som skulle kunna utgöra en fri- och rättighetsrisk. Det pågår en mycket snabb och svårbedömd teknisk utveckling inom detta område. Det finns en risk att en allmän juridisk skicklighet inte längre är tillräcklig för att kunna göra välavvägda bedömningar i de frågor som avhandlas i en ansökan om tillstånd. Den specialistkunskap som kommer krävas inom detta specifika område är ovanlig och svårrekryterad.

Vår bedömning är att de farhågor som tidigare angetts angående offentliga ombud kan sägas vara särskilt framträdande i den process vi nu reglerar. Ombudet riskerar att vara i händerna på sökanden och kan få allt svårare att överblicka de komplexa juridiska och tekniska aspekterna som ansökan avser. Ett ombud bör också komplettera domstolens kompetens på något sätt, vilket i dagsläget kan vara svårt att se.

Alternativet med att låta den särskilda tillsynsmyndigheten, Säkerhets- och integritetsskyddsnämnden, ha en del i tillståndsprocessen är enligt oss att föredra. Även Integritetsskyddsmyndigheten skulle kunna ha denna roll. Av de båda tillsynsmyndigheterna är det dock nämnden som har mest erfarenhet och kunskap inom Säkerhetspolisens verksamhetsområde.

Att föra in en annan myndighet i processen har som nämnts inte den fördelen att processen får det kontradiktoriska momentet att parterna kan sägas representera motsatta intressen. Däremot kan den särskilda tillsynsmyndigheten bevaka att lagens syften upprätthålls. Säpodatalagen syftar, vilket vi redogör för i avsnitt 8.1.1, till att skydda fysiska personers grundläggande rättigheter och friheter i samband med behandling av personuppgifter och att säkerställa att Säkerhetspolisen kan behandla personuppgifter på ett ändamålsenligt sätt. Tillsynsmyndigheten kommer av naturliga skäl i första hand att ha anledning att bevaka det förstnämnda syftet.

Säkerhets- och integritetsskyddsnämnden har bland annat i uppgift att ur ett rättssäkerhets- och integritetsskyddsperspektiv utöva tillsyn över viss brottsbekämpande verksamhet. Det är en myndighet under regeringen men med en särskild parlamentarisk anknytning. Nämndens ledamöter utses av regeringen efter nominering från riksdagens partigrupper. Att det är nämnden som agerar i processen kan, enligt vårt tycke, utgöra en lämplig ersättare för den roll som ett offentligt ombud spelar. Säkerhets- och integritetsskyddsnämndens ledamöter utgörs till största del av representanter för allmänheten.

Säkerhets- och integritetsskyddsnämnden ska yttra sig i processen

Det framstår inte som lämpligt att Säkerhets- och integritetsskyddsnämnden ska vara motpart i processen. Nämnden har inte något eget intresse i saken och kommer därför inte kunna vidta några rättshandlingar för egen del. Detsamma gäller för integritetsskyddsombuden. Ett integritetsskyddsombud har, enligt 5 § lag om Försvarsunderrättelsedomstol rätt att ta del av det som förekommer i målet och att yttra sig.

Det är lämpligt att Säkerhets- och integritetsskyddsnämnden ska ha motsvarande ställning i processen.

Bestämmelserna om integritetsskyddsombud ska endast gälla mål om signalspaning.

Eftersom den särskilda tillsynsmyndigheten ska yttra sig i processen finns inte tillräckliga skäl att även använda ett integritetsskyddsombud. Det ska därför anges i lagen om Försvarsunderrättelsedomstol att integritetsskyddsombud endast ska användas i mål som rör signalspaning. Detta förslag till lagändring har även lämnats i det tidigare nämnda utkastet till lagrådsremiss, Datalagring och tillgång till elektronisk information.

9.8.5 Sekretessfrågor i samband med att nämnden uppträder i domstol

Förslag: Det ska införas bestämmelser om överföring av sekretess i samband med att nämnden uppträder i domstol.

En sekretessbrytande bestämmelse för uppgifter som behövs för domstolens prövning av en tillståndsfråga ska införas i offentlighets- och sekretesslagen.

Sekretess hos Säkerhets- och integritetsskyddsnämnden

Sekretess hos Säkerhets- och integritetsskyddsnämnden regleras särskilt i 42 kap. 5–8 §§ offentlighets- och sekretesslagen. Sekretessbestämmelserna där avser nämndens tillsynsverksamhet enligt lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet.

När nämnden får en sekretessreglerad uppgift från en myndighet i sin tillsynsverksamhet gäller, enligt 42 kap. 8 § offentlighets- och sekretesslagen, att sekretessbestämmelsen blir tillämplig på uppgiften även hos nämnden. I 42 kap. 6 och 7 §§ finns bestämmelser om vad som gäller för uppgifter som nämnden fått från en enskild respektive uppgift som lämnats till nämnden från en utländsk myndighet eller en mellanfolklig organisation.

Beträffande uppgifter som nämnden fått del av och som inte kan hänföras till tillsynsverksamheten kan emellertid andra bestämmelser om sekretess vara tillämpliga. Den så kallade underrättelsesekretessen i 18 kap. 2 § offentlighets- och sekretesslagen gäller för uppgift som hänför sig till vissa utpekade verksamheter, vilket innebär att sekretessen följer med uppgiften när den överlämnas till en annan myndighet.[20] Utrikessekretessen och försvarssekretessen enligt 15 kap. 1–2 §§ offentlighets- och sekretesslagen gäller generellt hos alla myndigheter där uppgiften förekommer.

[20] Se prop. 2023/24:117 s. 158–159.

Sekretess för uppgifter som nämnden tar del av i domstol

I tillståndsprocessen kommer i många uppgifter att omfattas av underrättelsesekretess enligt 18 kap. 2 § offentlighets- och sekretesslagen, som gäller för uppgiften även hos nämnden. Det kan dock inte uteslutas att även uppgifter som omfattas av någon annan sekretessbestämmelse kan förekomma vid sammanträde eller i ansökan.

Eftersom det kan vara otydligt vad som gäller för sekretessbelagda uppgifter som förekommer i mål om framtagning bör detta särskilt regleras. I likhet med vad som gäller sekretessreglerade uppgifter i tillsynsverksamheten bör sekundär sekretess gälla för alla sekretessreglerade uppgifter som förekommit i mål om framtagning. Detta bör regleras särskilt i 42 kap. offentlighets- och sekretesslagen.

Sekretessbrytande bestämmelse för yttrande till domstolen

Ett av skälen till att den särskilda tillsynsmyndigheten ska få en ställning i processen är att myndigheten har kunskap om förhållanden och som domstolen kan behöva för sin prövning. Särskilt om sådant som har framkommit vid nämndens tillsyn, men som inte annars skulle utgöra en del av utredningen i målet. Det kan exempelvis handla om frågor som rör granskning av tidigare tillstånd där samma teknik för framtagning använts, eller myndighetens bedömning av hur känsliga de uppgifter som tagits fram har varit.

Får nämnden i sin tillsynsverksamhet en sekretessreglerad uppgift från en myndighet, blir sekretessbestämmelsen tillämplig på uppgiften även hos nämnden. Får nämnden en uppgift från en enskild och skulle en sekretessbestämmelse till skydd för enskilds personliga förhållanden ha varit tillämplig på uppgiften hos den myndighet som ärendet får anses avse, blir den sekretessbestämmelsen tillämplig på uppgiften även hos nämnden. Detsamma gäller, för alla sekretessbelagda uppgifter, som nämnden får från en utländsk myndighet eller mellanfolklig organisation.

Sekretessen som gäller för uppgift hos nämnden gäller även i förhållande till domstolen.

Ett skäl för att Säkerhets- och integritetsskyddsnämnden föreslås yttra sig under tillståndsprocessen i domstolen är att nämnden ska kunna berika processen med andra uppgifter än sådant som sökan-

den åberopar och som nämnden tagit del av genom sin tillsynsverksamhet eller på annat sätt. Eftersom domstolen och nämnden utgör två delar av samma tillsynssystem bör inte sekretess hindra att de uppgifter som behövs ska kunna lämnas till domstolen. Ett skaderekvisit i en sekretessbestämmelse kan i vissa fall hindra att nämnden lämnar uppgifter till domstolen.

Vi föreslår därför att det ska införas en sekretessbrytande bestämmelse mellan den särskilda tillsynsmyndigheten och Försvarsunderrättelsedomstolen för uppgifter som lämnas till domstolen under processen. Bestämmelsen bör gälla generellt, det vill säga att sekretess som gäller för en uppgift hos nämnden inte ska hindra att den lämnas till domstolen i ett mål om framtagning. Det bör varken ställas krav på att uppgiften ska vara nödvändig för domstolens prövning av målet eller att utlämnandet ska vara nödvändig för att nämnden ska kunna utföra sina uppgifter. Sådana hinder skulle annars kunna innebära att uppgifter som är viktiga för domstolens förståelse för verksamheten, som tillstånden reglerar inte fritt skulle kunna lämnas.

Då måste sekretessgenombrottet regleras i offentlighets- och sekretesslagen och inte som en uppgiftsskyldighet i processbestämmelserna. Bestämmelsen bör införas i anslutning till den ovan föreslagna bestämmelsen om överförd sekretess för uppgifter som lämnas i mål om framtagning.

Vi anser inte att det finns några principiella skäl för att uppgifter som nämnden har tillgång till och som omfattas av sekretess till skydd för allmänna intressen inte ska kunna lämnas till domstolen. Däremot bör den sekretessbrytande bestämmelsen inte omfatta uppgifter till skydd för enskildas personliga eller ekonomiska förhållanden.

9.8.6 Sammanträde

Förslag: Ansökningar ska prövas efter sammanträde dit Säkerhetspolisen och Säkerhets- och integritetsskyddsnämnden ska kallas.

Som huvudregel ska sammanträdet inte vara offentligt.

Sammanträde ger det bästa och säkraste underlaget inför en prövning

De principer om muntlighet, omedelbarhet och koncentration som ligger till grund för rättegångsbalkens regler om huvudförhandling gäller inte förvaltningsprocessen där ett skriftligt förfarande utgör huvudregeln. När lagen om Försvarsunderrättelsedomstol infördes gjordes bedömningen att ett sammanträde skulle gynna en effektiv handläggning och ge en förutsättning för ett meningsfullt yttrande från integritetsskyddsombudet. Det infördes därför särskilda regler för sammanträden avseende mål som rör tillstånd till signalspaning. I 12 § lagen om Försvarsunderrättelsedomstol anges bland annat att domstolen ska hålla sammanträde.

Vi anser att motsvarande regler som gäller för tillstånd till signalspaning bör införas för tillstånd till framtagning. Domstolen bör därför hålla sammanträde dit Säkerhetspolisen och den särskilda tillsynsmyndigheten ska kallas.

Huvudregeln om förhandlingsoffentligheten ska inte gälla

I 2 kap. 11 § andra stycket regeringsformen anges att förhandling vid domstol ska vara offentlig. Denna grundprincip kommer till uttryck i 5 kap. 1 § första stycket rättegångsbalken, som även enligt 16 § förvaltningsprocesslagen (1971:291) gäller för mål som handläggs enligt den lagen. Från grundprincipen kan göras undantag om det kan antas att det vid förhandlingen kommer att förebringas uppgift som omfattas av sekretess.

Rättegångsbalkens bestämmelser om offentlighet är inte direkt tillämpliga på specialdomstolarna. Då Försvarsunderrättelsedomstolen inrättades framfördes att det vid sammanträde regelmässigt kommer att läggas fram uppgifter som omfattas av sekretess enligt 15 kap. 1 och 2 §§ offentlighets- och sekretesslagen. Dessutom ansåg regeringen att det kunde finnas behov av att låta sekretessen omfatta också uppgifter om vilka företrädare för signalspaningsmyndigheten och biträden från inriktande myndigheter som är närvarande vid sammanträdet. Sådan information kan i annat fall användas för att kartlägga nyckelpersoner inom svensk underrättelseverksamhet.[21]

[21] Prop. 2008/09:201 s. 76.

Regeringen ansåg trots detta att den grundläggande principen om förhandlingsoffentlighet skulle gälla, men med utökade möjligheter till undantag. För att kunna säkerställa skyddet för sekretessbelagda uppgifter infördes därför en möjlighet för rättens ordförande att besluta att en förhandling ska hållas inom stängda dörrar, om det kan antas att det vid förhandlingen kommer att läggas fram en uppgift, för vilken det hos domstolen gäller sekretess. Regeringen framhöll att när det vid Försvarsunderrättelsedomstolen framläggs uppgifter som omfattas av sekretess är det sällan möjligt att hålla någon del av förhandlingen offentlig.

Den information vi fått till oss är att det aldrig hållits en förhandling vid Försvarsunderrättelsedomstolen där huvudregeln om förhandlingsoffentlighet har tillämpats. De skäl som talar för att tillämpa undantagsregeln om stängda dörrar framstår som lika starka i de mål som kommer röra Säkerhetspolisens ansökningar om framtagning. Det framstår därför som missvisande att föreskriva att förhandlingar ska vara offentliga när de i praktiken inte är det. Huvudregeln om förhandlingsoffentlighet bör därför inte gälla mål som rör framtagning. Däremot bör domstolen ha möjlighet att förordna om att förhandlingen, helt eller delvis ska vara offentlig, om det står klart att det inte kommer läggas fram några uppgifter som omfattas av sekretess.

9.8.7 Tillståndets innehåll

Förslag: Domstolens avgörande i sak ska ske genom dom där det ska anges

1. från vilka kategorier av uppgifter och från vilken typ av källor som framtagning får ske,
2. de sökbegrepp, kategorier av sökbegrepp eller andra urvalskriterier som får användas vid framtagning samt, om det finns skäl, med vilken teknik urvalet får ske,
3. vilken tid tillståndet gäller,
4. de villkor i övrigt som behövs för att begränsa intrånget i enskilda eller allmänna intressen samt för att möjliggöra en effektiv tillsyn, och
5. de skäl som bestämt utgången.

Tillstånd genom dom

En domstol bör avgöra saken som är föremål för prövning genom dom. En bestämmelse med det innehållet bör därför införas. Det motsvarar den praxis som gäller vid Försvarsunderrättelsedomstolen i mål som rör signalspaning.

Utformningen av tillståndet syftar till att klargöra hur och vilka personuppgifter Säkerhetspolisen får ta fram ur en särskild uppgiftssamling. Tillståndet ska även möjliggöra tillsyn över lagen.

Den formalia som ska anges för ett tillstånd ska motsvara det som krävs för att uppnå dessa syften. Vi har i avsnitt 9.8.2 redogjort för vad som ska framgå av en ansökan. Motsvarande uppgifter ska framgå av en dom.

Uppgiftsminimering

När det gäller kategorier och källor som en framtagning ska ske från är det skillnad på vilket material som ska genomsökas och på det material som ska få tas fram. Begränsningen av vilka personuppgifter som ska tas fram har att göra med hur sökresultatet ska kontextualiseras. Om exempelvis sökning görs med en viss selektor i en källa som innehåller textmeddelanden från ett it-beslag, är det sällan tillräckligt att få fram att just denna selektor förekommer. Träffen i sig är inte det mest intressanta, utan det sammanhang som den förekommer i. Samtidigt kan inte en sökträff medge framtagning av en alltför stor informationsmängd.

De kategorier och de sökbegrepp som ska tillåtas måste sträva efter en framtagning som är adekvat, relevant och inte för omfattande i förhållande till ändamålet. Hur ett tillstånd ska utformas för att uppnå detta är en fråga för rättstillämpningen.

Särskilda villkor

Det bör anges att domstolen även kan föreskriva särskilda villkor. Det kan handla om villkor som behövs för att begränsa intrånget i fri- och rättigheter exempelvis genom att inskränka de uppgifter som får tas fram på olika sätt. Att det i tillstånd är möjligt att föreskriva särskilda villkor är en allmän förvaltningsrättslig princip och

kräver inte lagstöd så länge villkoren ligger inom ramen för de syften som ska tillgodoses genom tillståndsgivningen.[22]

Det finns dock skäl att särskilt upplysa om att villkor utgör en del av tillståndsgivningen för framtagning. Villkor kan användas för att begränsa intrånget i de registrerades fri- och rättigheter men även föreskrivas i tillsynsmyndighetens intresse.

Villkor ska därför kunna begränsa exempelvis hur ett tillstånd får användas och förhindra ändamålsglidning. Det ska också kunna röra sig om ett villkor som behövs för att efterlevnaden av tillståndet ska kunna granskas i efterhand, exempelvis krav på särskild loggning av sökningar eller bevarande av uppgifter under tid för att tillsynsmyndigheten ska kunna ta del av utfallet av en framtagning.

Tidsgräns

Vi har i avsnitt 9.7.1 redogjort för skälen till att ett tillstånd ska vara tidsbegränsat. Det finns skäl att särskilt beakta att nya tillstånd kan behöva omprövas efter kortare tid än sådana framtagningar som sker för rutinmässiga ändamål.

9.8.8 Ändring av tillstånd

Förslag: Domstolen ska kunna ändra vad som föreskrivits i tillstånd.

Skälen för förslaget

Ett tillstånd till framtagning kan behöva omprövas under tiden tillståndet löper. Det kan exempelvis handla om att något sökbegrepp måste justeras eller att det uppmärksammats något fel i samband med att en ansökan prövas som även har bäring på andra tillstånd. För att förhindra att ett tillstånd endast kan ändras genom en helt ny ansökan, bör domstolen kunna besluta om ändring.

I enklare fall bör rätten kunna bestå av en ordförande ensam.

[22] HFD 2020 ref. 18 p. 26 och 30.

9.9 Interimistiskt beslut om framtagning

9.9.1 Behovet av att kunna agera i kris

I 5 b § signalspaningslagen finns bestämmelser om brådskande förfarande. Om det kan befaras att inhämtande av Försvarsunderrättelsedomstolens tillstånd skulle medföra fördröjning eller annan olägenhet av väsentlig betydelse får tillstånd till signalspaningen ges av den befattningshavare vid signalspaningsmyndigheten som regeringen föreskriver.

Om tillstånd har lämnats ska åtgärden genast anmälas skriftligen till Försvarsunderrättelsedomstolen. I anmälan ska skälen för åtgärden anges. Försvarsunderrättelsedomstolen ska skyndsamt pröva ärendet och, om den finner att det inte finns skäl för åtgärden, upphäva eller ändra beslutet. Om Försvarsunderrättelsedomstolen ändrar ett brådskande beslut ska även sådan upptagning eller uppteckning av uppgifter som kan hänföras till ändringen omgående förstöras i den utsträckning upptagningen eller uppteckningen kan hänföras till ändringen.

Den särskilda bestämmelsen om brådskande fall av signalspaning avser att möjliggöra inhämtning om det föreligger plötsliga hot mot rikets säkerhet som en från utlandet härrörande omedelbart förestående terroristattack i Sverige eller ett akut hot mot svensk trupp utomlands.[23]

Nyligen har Utredningen om översyn av lagen om signalspaning i försvarsunderrättelseverksamhet överlämnat sitt slutbetänkande till regeringen, *Signalspaning i försvarsunderrättelseverksamhet – en modern och ändamålsenlig lagstiftning* (SOU 2024:59). Där föreslås att förbudet mot signalspaning av signaler där både mottagare och avsändare befinner sig i landet ska förses med ett undantag. Enligt förslaget ska förbudet mot inhämtning av inhemsk trafik inte tillämpas i sådana brådskande situationer som innebär fara för människors liv eller hälsa eller för omfattande förstörelse av egendom. Den situation som avses med undantaget ska gälla försvarsunderrättelseverksamhet, innefattande kartläggning av strategiska förhållanden avseende bland annat internationell terrorism och annan grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen.

[23] Prop. 2006/07:63 s. 101.

Undantaget är motiverat utifrån behovet av en ventil som kan användas vid nödliknande situationer. Utredningen ansåg att det handlar om en sådan situation där tjänstemän vid signalspaningsmyndigheten antingen måste följa signalspaningslagstiftningen och då riskera människors liv eller att agera i strid med lagen. En annan aspekt som lyftes av utredningen är att allmänhetens förtroende för statens förmåga att skydda befolkningen skulle kunna påverkas negativt om det skulle bli känt att till exempel ett terroristattentat hade kunnat förhindras och människoliv räddas.[24] Undantaget från inhemsk signalspaning kräver tillstånd från Försvarsunderrättelsedomstolen. Med hänsyn till rekvisiten för att undantaget ska vara tillämpligt får det dock förutsättas att det interimistiska tillstånd som beskrivits ovan kommer att tillämpas parallellt med undantaget i de flesta fall.

I Sverige saknas generella bestämmelser om konstitutionell nöd. Det är därför nödvändigt att överväga om det finns behov av att, likt det nuvarande regelverket för signalspaning, införa särskilda regler för nödliknande situationer. Vi anser att det finns goda skäl att i Säkerhetspolisen verksamhet möjliggöra en effektiv informationshantering i krissituationer. När vi nu inför ett tillståndsförfarande, som med nödvändighet kräver viss tidsutdräkt, finns skäl att införa en möjlighet att i brådskande fall kunna göra framtagningar utan domstolens tillstånd.

9.9.2 Framtagning ska få ske utan domstolens tillstånd i vissa fall

Förslag: Om det kan befaras att ett inhämtande av domstolens tillstånd skulle medföra en fördröjning eller annan olägenhet som är av väsentlig betydelse för att avvärja en omedelbart förestående fara för människors liv eller hälsa eller omfattande förstörelse av egendom, bör framtagning kunna ske utan domstolens tillstånd.

[24] SOU 2024:59 s. 167.

Skälen för förslaget

Vi anser att det finns behov av att kunna använda den förmåga som vårt förslag innebär i kris, exempelvis om det krävs för att avvärja en överhängande risk för ett terroristattentat. Det finns anledning att formulera bestämmelsen efter förlaga från det som gäller för signalspaning i brådskande situationer och det som föreslås avseende undantag för inhemsk inhämtning.

Vi anser att det inte finns anledning att ge en möjlighet till interimistiska tillstånd i andra fall än då människoliv är i fara eller det finns risk för omfattande förstörelse av egendom. Givetvis måste situationen även vara så tidskritisk att ett tillstånd inte kan avvaktas.

Vi anser därför att reglerna ska utgå från att inhämtande av domstolens tillstånd skulle medföra en fördröjning eller annan olägenhet som är av väsentlig betydelse för ändamålet med framtagningen. Det motsvarar rekvisiten för interimistiskt beslut enligt 5 b § signalspaningslagen. Ändamålet för framtagningen anser vi ska vara begränsat till de fall som avser en omedelbart förestående fara för människors liv eller hälsa eller omfattande förstörelse av egendom. Detta krav motsvaras av det förslag om en ny 2 b § signalspaningslagen som lämnats i SOU 2024:59.

9.9.3 Tillstånd i brådskande fall

Förslag: Av regeringen utpekade befattningshavare vid Säkerhetspolisen ska kunna lämna tillstånd i brådskande fall.

Särskilt utpekade befattningshavare vid Säkerhetspolisen ska kunna lämna tillstånd till framtagning i vissa fall

I likhet med vad som gäller i fråga om signalspaning enligt signalspaningslagen bör ett undantag från den generella tillståndsplikten inte beslutas av de tjänstemän som arbetar direkt i den verksamhet där behovet uppmärksammats. Det bör endast komma i fråga att undantaget från domstolsprövning beslutas av högre tjänstemän i myndighetsledningen. Beslutet fattas under enskilt tjänsteansvar.

Regeringen bör föreskriva om de befattningshavare vid myndigheten som är behöriga att fatta beslut.

Ett interimistiskt beslut bör utformas med samma krav som gäller för tillstånd meddelat av domstol

För signalspaning gäller att ett beslut i brådskande fall (enligt 5 b § signalspaningslagen) ska utformas med samma krav som gäller för ett tillstånd som meddelats av domstol. Detsamma bör gälla för beslut om interimistisk framtagning.

Det innebär att ett beslut om tillstånd ska uppfylla samma krav som vid redogjort för i avsnitt 9.7 och utformas som en tillståndsdom, se avsnitt 9.8.6.

9.9.4 Ett beslut om tillstånd till framtagning ska anmälas till domstolen

Förslag: Ett beslut om framtagning ska anmälas till domstolen och anses vara en ansökan om framtagning med samma innehåll.

Domstolen ska ha möjlighet att inhibera beslutet och besluta att framtagna personuppgifter inte längre får behandlas.

Den särskilda tillsynsmyndigheten ska underrättas om ett beslut om framtagning.

Ett beslut ska prövas av domstol

Då ett beslut om brådskande signalspaning fattas enligt 5 b § signalspaningslagen ska åtgärden genast anmälas skriftligen till Försvarsunderrättelsedomstolen. Domstolen ska skyndsamt pröva ärendet och, om den finner att det inte finns skäl för åtgärden, upphäva eller ändra beslutet. Om domstolen anser att beslutet varit felaktigt, ska de uppgifter som inhämtats omgående förstöras.

Det finns behov av liknande regler i den lag vi föreslår. Beslutet om framtagning bör därför anmälas till domstolen. En anmälan ska utgöra en ansökan om framtagning, med samma innehåll som det interimistiska beslutet. Samma processregler ska gälla för att pröva denna ansökan, vilket bland annat innebär att det som huvudregel ska hållas ett sammanträde.

En sådan prövning bör ske skyndsamt. Eftersom det inte alltid är möjligt att sammankalla en fullsutten rätt tillräckligt snabbt bör särskilda regler införas för att det även i en brådskande situation

ska finnas möjlighet att upprätthålla skyddet av grundläggande fri- och rättigheter i lagen. Domstolen bör därför ges befogenheter att inhibera beslutet. För att en sådan inhibition ska vara verksam bör det även omfatta ett förbud mot att fortsätta att behandla de uppgifter som tagits fram med stöd av beslutet. Sådana beslut bör kunna fattas av en ordförande ensam.

När ett anmält beslut ska avgöras slutligt bör frågan handläggas på samma sätt som ett tillstånd, särskilt avseende den särskilda tillsynsmyndighetens yttrande. Om domstolen, efter den slutliga prövningen, anser att beslutet varit felaktigt bör det finnas en möjlighet att besluta om att alla de personuppgifter som tagits fram omedelbart ska raderas.

Följden av att ett beslut inte underställs i rätt tid

Om ett beslut om interimistisk framtagning inte anmälts i rätt tid, kan det få konsekvenser för de befattningshavare eller tjänstemän vid myndigheten som är ansvariga för åtgärden. Det bör dock även finnas en regel som tydligt anger vad den formella bristen att inte anmäla ett beslut i tid får för konsekvenser för de registrerade.

Framtagningar som sker utan tillstånd har vi bedömt vara oförenliga med det grundläggande skyddet för personuppgifter. Därför bör ett beslut som inte anmälts i tid inte få ligga till grund för framtagningar och de uppgifter som tagits fram med stöd av ett sådant beslut ska inte få behandlas.

Den särskilda tillsynsmyndigheten ska underrättas om beslutet

För att den särskilda tillsynsmyndigheten ska ha möjlighet att i efterhand granska förfarandet kring ett interimistiskt beslut måste den ha kännedom om det. En underrättelseskyldighet underlättar sannolikt även myndighetens inställelse och yttrande under prövningen i domstolen. Det bör därför införas en underrättelseskyldighet i förhållande till den särskilda tillsynsmyndigheten i anslutning till att ett interimistiskt beslut har fattats.

9.10 Hur ska framtagna uppgifter få användas?

9.10.1 Framtagna uppgifter ska uppfylla kraven i säpodatalagen för att få användas

Bedömning: Tillståndsgiven framtagning ska betraktas som inledande behandling enligt säpodatalagen.

Fortsatt behandling sker med stöd av säpodatalagen vilket innebär att framtagna uppgifter ska undergå inledande granskning innan de får behandlas för andra ändamål.

När ska behandling av personuppgifter övergå till att behandlas med stöd säpodatalagen?

På det sätt som *särskilda uppgiftssamlingar* är definierade kommer en framtagen uppgift inte längre omfattas av det begreppet. En särskild uppgiftssamling innebär att åtkomsten till uppgifterna är begränsad genom tekniska eller organisatoriska åtgärder och inte får tas fram utan tillstånd.

Efter att tillstånd medgetts och en uppgift tagits fram är uppgiften följaktligen inte längre en del av en särskild uppgiftssamling. Eftersom vi föreslår att lagens tillämpningsområde ska begränsas till uppgifter som är registrerade i särskilda uppgiftssamlingar, kommer framtagna uppgifter inte längre att omfattas av lagen om särskilda uppgiftssamlingar som vi här föreslår.

En framtagning som medges för brottsbekämpande ändamål kommer innebära att fortsatt behandling för det ändamålet ska ske enligt säpodatalagen. Detta är den avsedda effekten och kräver alltså ingen lagreglering.

Framtagning är inledande behandling enligt säpodatalagen

Vi har i avsnitt 8.6 föreslagit att säpodatalagen ska innehålla särskilda regler för inledande behandling. Trots att inledande behandling även föregått uppgifternas registrering i en särskild uppgiftssamling anser vi att framtagning ska utgöra sådan inledande behandling, se avsnitt 8.12.6.

Eftersom denna lag innehåller kompletterande bestämmelser till säpodatalagen ersätter tillståndet de förutsättningar som annars gäller för inledande behandling. Om framtagningen behövs för det ändamål som angetts i tillståndet krävs inte någon särskild prövning av om en framtagning även uppfyller kraven på att vara befogade för ett ändamål enligt säpodatalagen.

Ett interimistiskt beslut om framtagning kan kombineras med ett undantag från inledande granskning

I avsnitt 9.9 har vi föreslagit regler för interimistiska beslut om framtagning. I avsnitt 8.12.5 har vi därutöver föreslagit möjligheten att fatta beslut om undantag från kravet på inledande granskning.

Kraven är inte likalydande, en interimistisk framtagning får endast ske om det är av väsentlig betydelse för att avvärja en omedelbart förestående fara för människors liv eller hälsa eller omfattande förstörelse av egendom. Undantaget från granskningskravet får ske när det är absolut nödvändigt för att fullgöra en uppgift av synnerlig vikt. Granskningsundantaget är inte begränsat till fall som avser att avvärja allvarliga våldsbrott och liknande.

Det bör påpekas att undantagen är omgärdade av krav på omedelbar anmälan till den särskilda tillsynsmyndigheten och att de är tidsbegränsade. För framtagning enligt den här föreslagna lagen krävs också att beslutet anmäls till domstolen. Undantagssituationerna i de båda lagarna innebär inte heller tillsammans att kravet på exempelvis ändamål och proportionalitet efterges.

Vi bedömer att Säkerhetspolisen ska ha förmåga att agera effektivt i kris och att det ska finnas reglering som medger ett sådant agerande. De undantagsregler som vi föreslagit i de båda lagstiftningarna är både nödvändiga för att i ett demokratiskt samhälle skydda nationell säkerhet och proportionerliga i förhållande till detta syfte.

9.10.2 Framtagna uppgifter ska inte få användas i en förundersökning

Förslag: Uppgifter som tagits fram från en särskild uppgiftssamling ska inte få användas för att utreda brott.

Ett tillägg med den betydelsen ska göras i lagen (2019:547) om förbud mot användning av vissa uppgifter för att utreda brott.

Avvägning mellan rättssäkerhet och effektiv brottsbekämpning

Genom den här föreslagna lagstiftningen görs omfattande undantag från de principer som det europarättsliga dataskyddet vilar på. Många av de personer som registreras och vars uppgifter behandlas enligt denna lag kommer inte ha någon koppling till brottslig verksamhet eller till någon annan grund som Säkerhetspolisen normalt får åberopa för personuppgiftsbehandling. Vi har intagit ställningen att stora informationsmängder, oavsett om de handlar om öppen information som kan hämtas exempelvis från sociala medier eller om det rör sig om förtrolig kommunikation som avlyssnats i hemlighet, i dessa fall bör hanteras enligt samma grundläggande principer. Avgörande för intrånget är inte källan till informationen utan den sammanlagda mängden av information som behandlas och kan kombineras.

I Sverige har Säkerhetspolisen ett dubbelt uppdrag. Säkerhetspolisen är en säkerhetstjänst som bedriver polisverksamhet, vilket i västvärlden är relativt ovanligt. Denna dubbla roll medför att uppgifter som behandlas inom myndighetens underrättelseverksamhet normalt sett kan leda till att en förundersökning inleds, med straffprocessuella befogenheter.

I andra länder finns en rättstradition som tar avstånd från att ge myndigheter med polisiära befogenheter tillgång även till omfattande befogenheter i underrättelseverksamheten. Skälet är bland annat att undvika att en alltför omfattande maktkoncentration inom en och samma organisation. Vid sidan av denna aspekt, som inte har samma stöd i den nordiska rättstraditionen, finns betänkligheter angående den grundläggande rättsstatliga principen om rätten till en rättvis rättegång för de som blir föremål för en förundersökning där till-

ståndspliktig personuppgiftsbehandling utgör avgörande bevisning mot honom eller henne.

Mot dessa förbehåll av mer principiell natur står behovet av effektiva verktyg för att skydda nationell säkerhet och de grundläggande fri och rättigheterna i Sverige. Om det exempelvis finns information om ett nära förestående brott kan en användningsbegränsning innebära att myndigheter inte får förhindra brottet, trots att det funnits möjlighet till det. Det finns en stark förväntan om att Säkerhetspolisen effektivt ska kunna utreda och lagföra personer som begår allvarliga brott riktade mot Sveriges säkerhet eller terroristbrott. Europadomstolen har också slagit fast att medlemsstaterna har positiva skyldigheter att utreda brott. Bland annat innebär det att materiella och processuella bestämmelser ska möjliggöra en effektiv brottsbekämpning genom utredning och lagföring av personer. Enligt Europadomstolen ska en avvägning göras mellan de olika intressena och rättigheterna som ska skyddas. Integritetsintresset ska inte självklart ska ha företräde gentemot intresset av att utreda brott.[25]

Underrättelser från FRA får inte användas i förundersökning

Det har tidigare gjorts överväganden om information från signalspaning ska få användas vid brottsutredningar. Som en följd av dessa överväganden gäller numera ett förbud mot att använda sådan information för att utreda brott. Som en bakgrund till våra överväganden finns skäl att något redogöra för dessa regler.

Säkerhetspolisen och Nationella operativa avdelningen i Polismyndigheten har möjlighet att inrikta signalspaning i försvarsunderrättelseverksamhet.

Försvarsunderrättelseverksamhet ska, enligt lagen (2000:130) om försvarsunderrättelseverksamhet, bedrivas till stöd för svensk utrikes-, säkerhets- och försvarspolitik samt i övrigt för kartläggning av yttre hot mot landet. I denna verksamhet får det inte vidtas åtgärder som syftar till att lösa uppgifter som enligt lagar eller andra föreskrifter ligger inom ramen för Polismyndighetens, Säkerhets-

[25] Se Europadomstolens domar, i mål 23452/94 den 28 oktober 1998, *Osman mot Förenade kungariket*, p. 115–116, i mål 39272/98, den 4 mars 2004, *M.C. mot Bulgarien*, p. 151, i mål 59320/00, den 24 juni 2004, *Von Hannover mot Tyskland*, p. 57–58 samt i mål 2872/02, den 2 december 2008, *K.U. mot Finland*, p. 46.

polisens och andra myndigheters brottsbekämpande och brottsförebyggande verksamhet.

Signalspaning får ske endast i försvarsunderrättelseverksamhet. Enligt 1 § signalspaningslagen, begränsas även möjligheten till signalspaning till kartläggning av vissa uppräknade företeelser, bland dem strategiska förhållanden avseende internationell terrorism och annan grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen, utveckling och spridning av massförstörelsevapen och främmande underrättelseverksamhet mot svenska intressen.

Eftersom signalspaning endast får ske för försvarsunderrättelseändamål, och inte för att bekämpa brott, måste inriktningen ske för utrikes- eller säkerhetspolitiska behov. Försvarsunderrättelseverksamheten får dessutom inte utövas på ett sådant sätt att den inrymmer polisiära befogenheter såsom förundersökningsåtgärder. Skälet till det är att det inte ska vara möjligt att kringgå de regler som omgärdar straffprocessuella tvångsmedel genom att inhämta samma information i försvarsunderrättelseverksamheten. Säkerhetspolisen inriktar signalspaning för strategisk underrättelseinhämtning i syfte att bland annat förebygga och förhindra bland annat terrorism och brott mot rikets säkerhet, som utgör direkta hot mot Sverige och det svenska samhället samt för att kunna motverka spridning av massförstörelsevapen.

När FRA rapporterar underrättelser till Säkerhetspolisen och Polismyndigheten kan dessa innehålla information som innebär konkreta brottsmisstankar. I dessa fall är myndigheterna enligt huvudregeln skyldiga att inleda förundersökning. Förbudet mot att använda försvarsunderrättelser inom brottsbekämpningen innebar att FRA tidigare inte kunde fortsätta rapportera när en förundersökning inletts. För att motverka att uppgifter som är av relevans för Polismyndigheten och Säkerhetspolisens underrättelseverksamhet inte kunde rapporteras infördes den särskilda lagen (2019:547) om förbud mot användning av vissa uppgifter för att utreda brott. Av den framgår att uppgifter i underrättelser som Försvarets radioanstalt rapporterat till en annan myndighet i enlighet med lagen (2000:130) om försvarsunderrättelseverksamhet inte får användas för att utreda brott.

Att personuppgifter behandlas för brottsutredande ändamål har i vissa sammanhang ansett utgöra ett större intrång i den personliga

integriteten än behandling för andra ändamål.[26] Det är ett skäl till att signalspaning även i de flesta andra europeiska länder förbehålls underrättelseverksamhet. Integritetsintrånget anses i de flesta fall för stort om sådana metoder även kan användas polisiärt. Det journalistiska källskyddet och andra viktiga yttrandefrihetsprinciper kan komma att påverkas i högre grad om sådana uppgifter tillåts leda till åtal.

Allmänt om behovet av att använda uppgifter som tagits fram i en förundersökning.

Som tidigare nämnts avvärjer Säkerhetspolisen ofta brottslig verksamhet innan några åtalbara gärningar hunnit begås (se avsnitt 3.3.2). Detta innebär att Säkerhetspolisen brottsutredande verksamhet är förhållandevis liten. När Säkerhetspolisen väl bedriver förundersökning som leder till åtal rör det sig å andra sidan ofta om fall som är av stor betydelse för nationell säkerhet, som spionage eller terroristbrott. Det är ofta mycket angeläget att personer som exempelvis olovligen delgett säkerhetsklassificerade uppgifter till främmande makt eller att terrorister lagförs och frihetsberövas under överskådlig tid. Detta för att förhindra dem att orsaka ytterligare skada mot samhället.

Med undantag för Finland har även de övriga nordiska länderna en polisär funktion inom säkerhetstjänsterna. I Norge har PST möjlighet att samla in öppet tillgänglig information. Uppgifter som samlats in för detta ändamål är spärrad för all användning annan än sådan som är särskilt föreskriven. Bland de särskilt föreskrivna ändamålen finns utredning av de brott som PST ansvarar för. Det ska därmed, när lagen träder i kraft, vara möjligt för PST att vid sidan av sitt underrättelsearbete även göra sökningar i brottsutredande syfte i de förmodat mycket stora informationsmängder som kommer att ackumuleras. Dessa möjligheter att använda inhämtat och lagrad information motiveras i förarbetena med att det rör sig om öppet tillgängligt material som likväl hade kunnat återfinnas genom sedvanlig informationsinhämtning på internet. Då personuppgiftsskyddet är lika starkt för sökningar i det lagrade materialet som i PST:s verksamhet i stort har det ansetts motiverat att PST får möj-

[26] *S. och Marper mot Förenade kungariket*, p. 103.

lighet att utnyttja den lagrade informationsmängden även i sin övriga verksamhet. Flera remissinstanser har förhållit sig kritiska till detta uttalande eftersom personuppgiftsbehandling får ske i upp till femton år, vilket ofta är längre än vad personuppgifter finns allmänt tillgängliga.

Danmark har i likhet med Sverige och Norge en säkerhetstjänst som även har ett brottsutredande uppdrag. Där finns i dagsläget inte någon lagstiftning som tillåter behandling av stora informationsmängder men den, i förhållande till övriga polisen, mer tillåtande personuppgiftslagstiftningen i PET-loven gäller både PET:s underrättelse- och brottsutredande verksamhet som rör nationell säkerhet. PET har stora möjligheter att samköra uppgiftssamlingar, både från olika myndigheter och offentligt tillgängliga uppgifter.

Rätten till en rättvis rättegång

Enligt artikel 6 i Europakonventionen gäller att var och en vid prövningen av en anklagelse för brott ska vara berättigad till en rättvis rättegång vilket innefattar vissa minimirättigheter. Bedömningen enligt artikel 6 i Europakonventionen ska, enligt Europadomstolens praxis, omfatta förfarandet som helhet snarare än enskilda inslag. Vad som utgör en rättvis rättegång kan emellertid inte fastslås genom en viss regel utan beror på domstolens utvärdering av omständigheterna i det enskilda fallet. I varje enskilt fall bedömer domstolen om det straffrättsliga förfarandet som helhet varit rättvist. Det kan emellertid inte uteslutas att en viss omständighet kan vara så avgörande att det är möjligt för domstolen att bedöma om en kränkning skett utifrån denna enda omständighet. Exempelvis kan en åtgärd som vidtagits under det inledande förfarandet försvagat den misstänktes ställning i sådan utsträckning att alla efterföljande steg i förfarandet var orättvisa. Den kumulativa effekten av olika förfarandefel kan även leda till en överträdelse av artikel 6 även om varje fel i sig inte skulle ha övertygat domstolen om att förfarandet var orättvist.

Vid bedömningen av om förfarandet i sin helhet har varit rättvist kan dock hänsyn tas till allmänintresset av att det aktuella brottet utreds och bestraffas. Artikel 6 ska inte tillämpas på ett sådant sätt att det medför oproportionerliga svårigheter för polismyndigheterna att vidta effektiva åtgärder för att bekämpa terrorism eller andra

grova brott vid fullgörandet av sina skyldigheter enligt konventionen. En konventionsstat har en skyldighet även att skydda var och ens rätt till liv, skyddet mot omänsklig eller förnedrande behandling och rätt till frihet och personlig säkerhet. Sådana hänsyn kan dock aldrig motivera åtgärder som utsläcker själva kärnan i rätten till ett rättvist försvar.

Equality of arms och rätten till en kontradiktorisk process

Parternas likställdhet i processen utgör enligt Europadomstolen en fundamental beståndsdel av en rättvis rättegång. Den kräver att varje part ges en rimlig möjlighet att lägga fram sin sak under förhållanden som inte missgynnar honom eller henne i förhållande till motparten. Parternas likställdhet i processen kräver en rättvis balans mellan dem. En grundläggande del av denna princip är rätten att granska bevisning.

Vid sidan av att kunna granska och utvärdera den bevisning som åberopas till stöd för ett åtal har den tilltalade en rätt att själv, på samma villkor som åklagaren, föra egen bevisning i målet. För att kunna utnyttja denna rättighet krävs i regel att åklagaren lämnar ut all bevisning som denne förfogar över som är relevant både till förmån och till nackdel för den misstänkte. Det kan röra sig om bevisning som används för att styrka den tilltalades skuld likväl som uppgifter som kan göra det möjligt för den tilltalade att rentvå sig själv eller för att framföra förmildrande omständigheter. Den bevisning som är relevant i detta sammanhang är inte bara bevisning som direkt åberopas till styrkande av faktiska omständigheter, utan även annan utredning som kan avse tillförlitligheten och fullständigheten av sådan bevisning. Enligt praxis anses det inte tillräckligt att åklagarmyndigheterna enligt lag är skyldiga att ta hänsyn till fakta som talar både för och emot den misstänkte.

Rätten att få tillgång till relevant bevisning är dock inte en absolut rättighet. I brottmål kan det finnas motstridiga intressen, som till exempel rör nationell säkerhet eller polisiära metoder, vilket måste vägas mot den tilltalades rättigheter. Endast sådana inskränkningar som är strängt nödvändiga är emellertid tillåtna enligt artikel 6. För att säkerställa att den tilltalade får en rättvis rättegång måste dessutom de eventuella svårigheter som försvaret drabbas av genom en sådan begränsning vägas upp under processen.

Stora informationsmängder i förundersökning

Stora informationsmängder som analyseras med tekniska hjälpmedel i ett brottmålsförfarande har prövats av Europadomstolen i målet *Sigurður Einarsson m.fl. mot Island*.[27] Målet handlade om eftermälet av finanskrisen som drabbade den isländska storbanken Kaupþing. Efter att banken tagits över av staten åtalades flera i den tidigare bolagsledningen för oegentligheter. Som ett led i utredningen beslagtog åklagaren enorma mängder data från bankens it-system. Den information som ingick i beslaget omfattade hundratusentals dokument.

För att kunna hantera informationsmängden och sortera i materialet använde sig de brottsutredande myndigheterna av sök- och analysverktyget Clearwell. Materialet kunde delas upp i tre kategorier, där den första utgjordes av hela den osorterade informationsmängden som genomsökts med programvaran, den andra av *utredningshandlingar* som åklagaren ansåg hade koppling till anklagelserna på något sätt och den tredje av *bevis* som åberopades i domstolen. Försvaret delgavs bevisen och hade möjlighet att få tillgång till utredningshandlingarna men gavs i den isländska processen ingen möjlighet att ta del av det som låg utanför någon av dessa båda kategorier: den osorterade informationsmängden.

Frågan i Europadomstolen var bland annat huruvida försvaret med stöd av principen om ”equality of arms” antingen hade rätt att göra sökningar i den osorterade informationsmängden med hjälp av samma analysverktyg som åklagaren använt, eller att ta del av de dokument som analysverktyget initialt pekat ut (taggat) som intressanta. Det fanns en stor mängd handlingar i den osorterade informationsmängden som taggats av Clearwell, men som efter manuell granskning inte överförts till någon av kategorierna utredningshandlingar eller bevis.

Europadomstolen konstaterade, angående den första frågan, att det inte finns någon rättighet för försvaret att få tillgång till hela den osorterade datamängden, vars innehåll inte heller åklagaren hade någon kännedom om. Däremot ansåg domstolen att det är en viktig rättsäkerhetsmekanism att försvaret ges möjlighet att påverka urvalskriterierna för när handlingar skulle taggas som intressanta för fortsatt manuell granskning.[28]

[27] Europadomstolens dom den 4 juni 2019 i mål 39757/15, *Sigurður Einarsson m.fl. mot Island*.
[28] Se punkten 90.

Den andra frågan handlade om försvarets tillgång till den data som analysverktyget Clearwell initialt flaggat upp som relevant, men som inte överförts till kategorin utredningshandlingar. Denna information hade genomgått ytterligare automatiserad och manuell analys och åklagarsidan hade därmed faktiskt kännedom om innehållet och hade gjort bedömningen att det inte rörde åtalet. Europadomstolen godtog inte att denna bedömning gjorts utan inblandning av försvaret. Försvarets tillgång till handlingar borde därför inte varit begränsad till kategorin utredningshandlingar. Domstolen ansåg att försvaret även borde ha fått tillgång till i vart fall en lista av de dokument som programvaran Clearwell initialt bedömt som relevant och en möjlighet att genomföra sökningar till vederläggande av åtalet i denna uppgiftsmängd.[29]

Det går att dra flera slutsatser av Europadomstolens argumentation i detta mål. En av dessa är att försvaret bör få möjlighet att inverka på analysen av stora informationsmängder, genom att exempelvis kunna påverka vilka sökkriterier som ska tillämpas. En annan slutsats som kan dras är att information som tagits fram från en automatiserad analys av ett stort material som regel ingår i de handlingar som försvaret ska ha rätt att ta del av, även om de från förundersökningens sida har bedömts som irrelevanta. Hur parternas likställdhet skulle bedömas i mål där vikten av att hemlighålla underrättelseinformation är betydligt högre än i mål som rör ekonomisk brottslighet är svårt att säga. Domstolen pekar under alla omständigheter ut vikten av att åklagarsidan inte får ha ett informationsövertag på bekostnad av den tilltalades rätt till försvar. Det får betraktas som en möjlighet att försvaret även i mål som rör exempelvis terrorbrottslighet måste få en möjlighet att själv utföra vissa sökningar och ta del av överskottsinformation.

Uppgifter som tagits fram från en särskild uppgiftssamling bör inte få användas för att utreda brott

Vi anser att det finns likheter, både i materiellt och principiellt hänseende, mellan underrättelser från signalspaningsmyndigheten FRA och framtagningar från en särskild uppgiftssamling. Behandling av

[29] Se punkten 91.

stora datamängder framstår som ett utpräglat underrättelseverktyg, på samma sätt som signalspaning.[30]

Bland de skäl som motiverat att underrättelser från FRA inte får användas i förundersökning finns den misstänktes insynsrätt. FRA:s signalspaningsförmåga riskerar att avslöjas i en rättegång. Samma problematik finns för behandling av stora informationsmängder i särskilda uppgiftssamlingar. Europadomstolen har påtalat att när stora uppgiftsmängder varit en del i en brottmålsprocess, bör försvaret ha inflytande över urvalskriterier och selektering. Vidare kan det inte uteslutas att försvaret har rätt att ta del av de uppgifter som tagits fram som Säkerhetspolisen, även om de inte inkluderas i den aktuella förundersökningen. Denna rätt skulle kunna möjliggöra en kartläggning av vilka uppgifter som Säkerhetspolisen har tillgång till. Vår uppfattning är att behandling av personuppgifter i särskilda uppgiftssamlingar kommer vara en underrättelseförmåga av väsentlig betydelse för Säkerhetspolisen. Vilka uppgifter som ingår i denna förmåga bör inte riskeras att avslöjas genom den misstänktes insynsrätt.

Det finns en rad andra komplexa rättsliga frågor att ta ställning till om uppgifter som tagits fram från en särskild uppgiftssamling ska få användas i en rättegång. En försvarare har exempelvis ett berättigat intresse att kunna söka efter friande bevisning eller åtminstone att begära kompletterande utredningsåtgärder enligt principen om ”equality of arms”. Detta kan vara praktiskt svårt att genomföra i en så säkerhetskänslig verksamhet och inom ramen för ett noga reglerat tillståndsförfarande.

Vid sidan av de frågor om rättssäkerhet och rätten till en rättvis rättegång som kan uppkomma när särskilda uppgiftssamlingar används för att ta fram bevisning går det inte att bortse från att integritetsintrånget kan vara högre när det gäller uppgifter som används för att utreda brott jämfört med uppgifter som används i underrättelseverksamhet. FRA:s signalspaningsförmåga utgör ett påtagligt integritetsintrång. Det har motiverat att metoden är strängt reglerad, bland annat genom att signalspaning endast får ske i försvarsunderrättelseverksamheten och endast för vissa, i lag utpekade, ändamål av mycket stor vikt. Vi har inte ansett att det finns skäl att begränsa Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar

[30] I tysk konstitutionell rätt finns exempelvis ett uttryckligt förbud mot sådan maktkoncentration enligt doktrinen ”den som kan känna till (nästan) allt bör inte ha möjlighet att göra (nästan) allt; och den som kan göra (nästan) allt får inte ha möjlighet att veta (nästan) allt”, se Christoph Gusy, *Grundrechte Und Verfassungsschutzrecht*, 2011.

till ändamål som är av motsvarande karaktär. Även om integritetsintrånget av att uppgifter behandlas i särskilda uppgiftssamlingar inte är lika stort som det intrång som sker genom signalspaning, haltar jämförelsen mellan de två underrättelseförmågorna i detta avseende. Uppgifter som registrerats i särskilda uppgiftssamlingar får avse inrikes förhållanden och är inte begränsade till strategiska underrättelser avseende exempelvis spridning av massförstörelsevapen eller internationell terrorism. Att dessutom tillåta att sådana uppgifter används för att utreda brott är, enligt vår uppfattning, ett stort kliv.

Det finns emellertid även starka skäl som talar i motsatt riktning: framför allt att lagstiftningen är motiverad av skyddet för nationell säkerhet. Landets inre säkerhet skyddas främst genom att säkerhetshotande verksamhet är kriminaliserad och att de individer som utgör hot mot nationell säkerhet lagförs. Även om det finns många sätt att avvärja brottslig verksamhet, genom att exempelvis förhindra personer att resa in i landet eller genom att Säkerhetspolisen ger sig till känna och underrättar de misstänkta om att planerna är avslöjade, finns inget annat sätt att i en rättsstat frihetsberöva sådana personer än genom lagföring. Vissa verktyg är beroende av att en förundersökning inleds. Det finns därför i och för sig starka skäl som talar för att Säkerhetspolisen inte ska begränsas i sin uppgift att utreda brott. Om personuppgifter som tas fram ur en särskild uppgiftssamling inte får användas för att utreda brott, kan Säkerhetspolisen inte heller använda straffprocessuella tvångsmedel för att stärka misstankarna. I slutändan kan det uppkomma en situation som innebär att Säkerhetspolisen har kännedom om planer på ett brott, men saknar rättsliga förutsättningar att förhindra det.

Det finns således skäl som talar både för och emot att tillåta information från särskilda uppgiftssamlingar att användas för att utreda brott. Vid den slutliga avvägningen fäster vi avgörande vikt vid att det är fråga om en helt ny förmåga och att det är osäkert hur frågan skulle bedömas från ett konventionsrättsligt perspektiv. Vi har därför sammantaget stannat för att det i dagsläget finns övervägande skäl som talar för att personuppgifter som tagits fram från särskilda uppgiftssamlingar ska omfattas av samma förbud mot att användas för att utreda brott som underrättelser som FRA delger Säkerhetspolisen.

Ett förbud mot att använda personuppgifter som tagits fram med stöd av den föreslagna lagen för att utreda brott bör tillföras

lagen (2019:547) om förbud mot användning av vissa uppgifter för att utreda brott. Dessutom bör ändamålet att utreda och lagföra brott inte tillåtas för vare sig registrering eller framtagning.

9.11 Längsta behandlingstid

9.11.1 Samma princip för behandlingstid som i säpodatalagen

Förslag: När Säkerhetspolisen registrerar personuppgifter, ska en proportionerlig behandlingstid för de registrerade uppgifterna bestämmas.

Skälen för förslaget

Vi har i avsnitt 8.18 lämnat förslag om att en behandlingstid ska bestämmas vid registrering av uppgifter enligt säpodatalagen. Samma skäl som där förs fram kan göras gällande för uppgifter som registreras i särskilda uppgiftssamlingar. Det bör vara möjligt att bestämma en proportionerlig behandlingstid redan då uppgifter registreras. Det är dessutom i princip inte möjligt att omvärdera uppgifternas relevans kontinuerligt, eftersom det exakta innehållet i särskilda uppgiftssamlingar förväntas vara okänt. Vi anser därmed att behandlingstiden ska anges redan i ett registreringsbeslut. Behandlingstiden ska följa principerna i den här föreslagna lagen, det vill säga. att uppgifterna ska vara befogade för ett ändamål under hela behandlingstiden. Därutöver ska behandlingstiden återspegla en proportionerlig personuppgiftsbehandling.

Det kommer inte vara praktiskt möjligt att separera personuppgifter på ett sätt som medger att tiden bestäms från exempelvis den sista registreringen. Därför bör behandlingstiden alltid bestämmas från registreringsdatumet för uppgiften och sedan en viss bestämd tid därefter.

9.11.2 Yttersta tidsgränser

Förslag: Behandlingstiden får inte bestämmas till längre än tio år. Om behandlingstiden bestäms till längre än fem år, ska detta motiveras och den särskilda tillsynsmyndigheten underrättas.

Skälen för förslaget

Vi föreslår vissa lagstadgade tidsfrister i säpodatalagen som innebär att uppgifter som regel inte får behandlas längre än 25 år, med undantag för uppgifter inom kontraspionaget eller utvecklingsverksamheten.

Det bör på motsvarande sätt införas en längsta behandlingstid för uppgifter som registrerats i särskilda uppgiftssamlingar. När det kommer till hur en sådan behandlingstid ska bestämmas anser vi att det ska beaktas att registrering enligt de lägre kraven vi föreslår i denna lag utgör ett undantag från flera av de sedvanliga dataskyddsmekanismerna. Ändamålet för att en persons personuppgifter förekommer i en särskild uppgiftssamling kommer exempelvis inte ha den precision som kan förväntas i andra sammanhang och de flesta individer som är registrerade kommer sannolikt inte kunna relateras till detta ändamål. Det finns därför en betydande skillnad mot att en person är registrerad med stöd av säpodatalagens bestämmelser. Vi anser att detta motiverar en avsevärt kortare behandlingstid.

Samtidigt måste det finnas utrymme för flexibilitet i systemet där det kommer finnas en mycket stor skillnad i integritetsintrång mellan olika registreringar. Registreringar som avser exempelvis en katalog av ip-nummer eller offentliga adressuppgifter utgör ett lågt intrång på individnivå i jämförelse med exempelvis inhämtning från sociala medier. Det bör därför vara möjligt att bestämma behandlingstiden inom ett visst spann.

I det norska lagförslaget om behandling av öppen tillgänglig information finns en tidsgräns om fem år som kan förlängas med fem år i taget till maximalt femton år, se avsnitt 4.4.3. I den lagstiftning som gäller för ”bulk personal data” i Förenade kungariket finns ett tillståndskrav även för bevarande av stora uppgiftssamlingar. Sådana tillstånd löper på sex månader. Det innebär att de datamängder som behandlas måste omprövas var sjätte månad genom att nytt tillstånd söks, för fortsatt bevarande, se avsnitt 4.5.3.

I båda dessa system får det antas att den längsta behandlingstiden är den tid som uppgifter i praktiken också behandlas. Vi har i vårt förslag till säpodatalag försökt undvika en sådan systematik. I stället ska Säkerhetspolisen kunna bestämma en proportionerlig behandlingstid inom en yttre ram. Denna yttre ram ska representera det som kan tillåtas i de mest angelägna fallen, och inte den normala behandlingstiden. Vi anser att det samlade fri- och rättighetsintrånget av att behandla personuppgifter i särskilda uppgiftssamlingar kan bli mycket stort, beroende på den samlade informationsmängdens omfattning. Det finns därför goda skäl till att hålla nere behandlingstiden. Bedömningen av om behandling är proportionerlig kommer behöva utgå från de personuppgifter som inte får behandlas enligt säpodatalagen. Det vill säga uppgifter om personer som inte kan förvänta sig att var kartlagda av Säkerhetspolisen och där behandlingen, på individnivå, innebär ett undantag från behovs- och ändamålsprincipen.

Vår uppfattning är att det i många fall kan accepteras att personuppgifter behandlas för underrättelseändamål i fem år. Denna tid kan dock vara för kort för att kunna teckna långsiktiga trender och kartlägga skeenden över tid. Det bör vara möjligt att redan vid registrering ange att uppgifter får behandlas i tio år. För att säkerställa att uppgifter inte behandlas under så lång tid om inte behovet starkt talar för det, bör den särskilda tillsynsmyndigheten underrättas om behandlingstiden överskrider fem år. Då kan tillsynsmyndigheten kontinuerligt få en uppfattning om i vilken omfattning behandlingstiden bestäms i det övre spannet, och inleda tillsyn över dessa beslut om det anses påkallat.

9.11.3 Möjlighet till förlängning genom nytt registreringsbeslut

Förslag: Behandlingstiden för registrerade uppgifter ska kunna förlängas. Den sammanlagda behandlingstiden får överstiga 25 år endast om det finns synnerliga skäl.

Skälen för förslaget

I avsnitt 8.18.6 har vi redogjort för att det för behandling som sker med stöd av säpodatalagen bör finnas en möjlighet att förlänga den tid som angetts vid en registrering, om det alltjämt finns ett behov av uppgifterna därefter. Samma skäl talar för att det ska vara möjligt att förlänga tiden även för uppgifter som registrerats i en särskild uppgiftssamling.

En proportionell behandlingstid innebär att behovet av att behandla uppgifterna måste ställas mot det intrång som registreringen innebär för enskilda och allmänna intressen. Behovet av fortsatt behandling avtar ofta över tid. Intrånget däremot får anses vara relativt sett högre ju längre en uppgift finns bevarad hos en säkerhetstjänst, särskilt om uppgifterna är av känslig eller privat natur eller om de rör opinionsfriheterna. Då proportionalitet ska bedömas bör utgångspunkten vara att för varje år en uppgift behandlas minskar behovet samtidigt som intrånget ökar. Vid den tidpunkt då axlarna skär varandra och intrånget överstiger behovet föreligger inte längre proportionalitet.

Om en tidigare bestämd behandlingstid förlängs är det viktigt att det görs genom en konkret omprövning och inte av slentrian. Vi anser därför att en omprövning som innebär att behandlingstiden förlängs ska göras genom att ett nytt registreringsbeslut fattas. Det innebär att behovet av den fortsatta behandlingen motiveras skriftligt.

Vi anser att det även om proportionalitet ska prövas krävs en tröskel för att förhindra att uppgifter behandlas för länge. I säpodatalagen har vi föreslagit en yttersta tidsgräns på 25 år för de flesta uppgifter. Det avser uppgifter vars innehåll är känt och bedömt som adekvat och relevant för ett ändamål.

En längre behandlingstid i särskilda uppgiftssamlingar bör inte vara längre än den längsta tiden som anges i säpodatalagen annat än i mycket särpräglade fall. För att markera detta bör det i lagen framgå att det krävs synnerliga skäl för att den samlade behandlingstiden ska få tillåtas överstiga 25 år. Det innebär att en behandling som pågått längre än 25 år endast får ske för mycket angelägna ändamål. Det kan exempelvis handla om uppgiftssamlingar som har direkt relevans för kartläggning av främmande makts säkerhetshotande verksamhet, där de framtagna uppgifterna får behandlas i upp till 60 år.

10 Tillsyn

10.1 Inledning

Effektiv tillsyn är en central skyddsmekanism i ett demokratiskt samhälle, särskilt när det gäller myndigheter som har omfattande befogenheter att behandla personuppgifter. Tillsynen över Säkerhetspolisens personuppgiftsbehandling fyller en viktig rättssäkerhetsfunktion och syftar till att säkerställa att enskildas grundläggande fri- och rättigheter respekteras.

Personuppgiftslagstiftningen utgör ett skyddsnät för många grundläggande fri- och rättigheter. I frånvaro av andra skyddsmekanismer, till exempel för nya informationskällor eller insamlingsmetoder som ännu inte reglerats specifikt, kan en personuppgiftslag säkerställa ett grundläggande skydd mot otillåtna eller oproportionerliga intrång i enskildas integritet. Det är därför av stor rättsstatlig vikt att Säkerhetspolisens personuppgiftsbehandling står under en effektiv, robust och ändamålsenlig tillsyn.

De två lagstiftningar som vårt förslag innehåller ger Säkerhetspolisen utökade möjligheter att behandla personuppgifter för att utföra sitt uppdrag. Lagarna bygger på principen att detaljreglering i viss mån får stå tillbaka till förmån för kravet på proportionalitet. Det innebär att frågan om proportionalitet delvis förflyttas från lagstiftningsnivå till tillämpningen.

Europadomstolen har vid upprepade tillfällen konstaterat att personuppgiftsbehandling som utförs av en nationell säkerhetstjänst nästan undantagslöst innebär ett intrång i enskildas rättigheter. Även om intrånget kan vara mindre omfattande än vid exempelvis hemlig avlyssning, är det viktigt att uppmärksamma de risker som insamling, sammanställning och analys av uppgifter kan medföra.

Europadomstolen har återkommande använt sig av följande skäl för att beskriva riskerna med att ge en nationell säkerhetstjänst ett

omfattande mandat och vad som krävs för att statlig övervakning av medborgare i syfte att värna nationell säkerhet ska vara förenlig med Europakonventionens krav:

> In view of the risk that a system of secret surveillance set up to protect national security (and other essential national interests) may undermine or even destroy the proper functioning of democratic processes under the cloak of defending them, the Court must be satisfied that there are adequate and effective guarantees against abuse.[1]

Vi har ett stort förtroende för Säkerhetspolisens nuvarande verksamhet och organisation. Vi har under utredningen återkommande uppmärksammat att myndigheten är noggrann med att följa gällande rätt och hellre avstår från en åtgärd än att riskera att kränka enskildas fri- och rättigheter. Vi anser emellertid inte att detta kan vara ett skäl att avstå från att upprätthålla stränga krav på rättssäkerhets- och tillsynsmekanismer. Sådana mekanismer är avsedda att få till en ordning som är hållbar över tid och som tillser att intrånget i den personliga integriteten minimeras.

Det finns mot denna bakgrund skäl att överväga om det nuvarande systemet är tillräckligt eller om det finns anledning att bygga ut och förstärka tillsynen.

10.2 Den parallella tillsynen bör kvarstå

Bedömning: Det finns inte skäl att ändra den nuvarande ordningen där tillsynen över Säkerhetspolisens personuppgiftsbehandling sker av både Integritetsskyddsmyndigheten och Säkerhets- och integritetsskyddsnämnden. Det bör dock förtydligas att det finns två tillsynsmyndigheter med olika uppgifter och befogenheter.

10.2.1 Skälen bakom den nuvarande ordningen

Som framgår av avsnitt 3.5.9 utövas tillsyn över Säkerhetspolisens personuppgiftsbehandling av två olika myndigheter. Integritetsskyddsmyndigheten är den generella tillsynsmyndighet vars upp-

[1] Se bland annat *Big Brother Watch m.fl. mot Förenade kungariket*, mål 58170/13, 62322/14 och 24960/15, p. 339.

gifter och befogenheter framgår direkt av säpodatalagen. Enligt lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet ska Säkerhets- och integritetsskyddsnämnden utöva särskild tillsyn över Säkerhetspolisens behandling av personuppgifter, i enlighet med de tillsynsbefogenheter som framgår av den lagen.

De befogenheter att granska och kontrollera behandlingen av personuppgifter som de båda lagstiftningarna var för sig medger är snarlika. Frågan är om det alltjämt bör vara två tillsynsmyndigheter som utövar parallell tillsyn eller om det finns anledning att koncentrera resurserna till en av dem. I den nuvarande säpodatalagens förarbeten övervägdes alternativen tämligen ingående.[2] Regeringens slutsats var att myndigheterna kompletterar varandra och att skälen för att låta den parallella tillsynen bestå övervägde skälen för att anförtro tillsynen åt antingen Säkerhets- och integritetsskyddsnämnden eller Integritetsskyddsmyndigheten.

10.2.2 Det finns inte skäl att frångå parallell tillsyn

Sedan säpodatalagen beslutades år 2019 har det inte skett någon större förändring som talar mot regeringens tidigare ställningstagande i frågan. Enligt vår uppfattning talar utvecklingen snarare för att skälen för den parallella tillsynen har blivit starkare. Integritetsskyddsmyndigheten kommer sannolikt att få nya uppdrag med anledning av EU:s så kallade AI-förordning. Integritetsskyddsmyndigheten kommer under alla omständigheter att behöva skaffa sig kompetens inom nya teknikområden som rör personuppgiftsbehandling. Det bör vara möjligt att utnyttja denna kompetens även vid tillsyn över Säkerhetspolisen.

Även om Säkerhetspolisens verksamhet är särpräglad i förhållande till många andra myndigheters, finns det anledning att tro att vissa tekniska lösningar eller system kommer att vara desamma som hos andra myndigheter. Att Integritetsskyddsmyndigheten kan jämföra tillämpning och förmedla hur likartade situationer har bedömts tidigare kan vara värdefullt även vid tillsynen över Säkerhetspolisen.

Säkerhetspolisen samverkar med bland annat Polismyndigheten, den militära underrättelse- och säkerhetstjänsten och FRA. Polis-

[2] Se prop. 2018/19:163 s. 168–171.

myndigheten står på samma sätt som Säkerhetspolisen under särskild tillsyn av Säkerhets- och integritetsskyddsnämnden. Den försvarsunderrättelseverksamhet som bedrivs av bland annat Försvarsmakten och FRA står under särskild tillsyn av Statens inspektion för försvarsunderrättelseverksamheten. Utöver de särskilda tillsynsmyndigheterna för respektive verksamhet utövar Integritetsskyddsmyndigheten en generell tillsyn över samtliga dessa myndigheters personuppgiftsbehandling.

Integritetsskyddsmyndigheten har därmed möjlighet att få en inblick i hur personuppgifter behandlas inom ramen för både den öppna polisens brottsbekämpning, Säkerhetspolisens verksamhet som rör nationell säkerhet och Försvarsmaktens uppgifter som rör försvar och säkerhet. Detta för Integritetsskyddsmyndigheten unika tillsynsmandat ger bland annat möjlighet att utöva tillsyn över samverkansprojekt som bedrivs eller kan komma att bedrivas myndigheterna emellan. Det skulle exempelvis kunna röra sig om ett utökat informationsutbyte eller gemensamma tekniska plattformar. Integritetsskyddsmyndigheten är det enda organ som skulle vara behörig att utöva tillsyn över personuppgiftsbehandlingen hos alla inblandade myndigheter. De särskilda tillsynsmyndigheterna måste däremot stanna inom respektive tillsynsområde och lagstiftning, vilket kan orsaka svårigheter vid tillsyn av behandling av uppgifter som innebär att de överförs eller delas mellan olika rättsliga och tekniska system.

Säkerhets- och integritetsskyddsnämnden har å andra sidan – genom kontinuerlig och verksamhetsnära tillsyn över Säkerhetspolisens personuppgiftsbehandling – fått särskild insikt i och erfarenhet av den verksamhet som Säkerhetspolisen bedriver. Den lagstiftning som vi föreslår bygger i betydligt högre utsträckning än tidigare på att Säkerhetspolisens särskilda behov ska kunna tillgodoses inom proportionella ramar. Bedömningen av vad som utgör en proportionerlig personuppgiftsbehandling och vad som faller utanför denna ram kräver just sådana insikter som Säkerhets- och integritetsskyddsnämnden besitter. En sådan, i många avseenden delikat, proportionalitetsbedömning anser vi med fördel kan anförtros en nämnd med stark parlamentarisk anknytning. Nämndens särskilda sammansättning har ansetts utgöra dess styrka och vara särskilt viktig för att tillgodose allmänhetens insyn i verksamhet som omfattas av stark sekretess.

Till detta kommer de argument som framförts för att behålla den parallella tillsynen i förarbetena till den nuvarande ordningen.[3] Sammantaget har vi därmed inte funnit några skäl som rubbar tidigare ställningstaganden om att Säkerhetspolisens personuppgiftsbehandling bör stå under tillsyn av både Integritetsskyddsmyndigheten och Säkerhets- och integritetsskyddsnämnden.

10.3 Det bör framgå att Säkerhets- och integritetsskyddsnämnden utövar särskild tillsyn över personuppgiftsbehandlingen

Förslag: Det ska av den nya lagen framgå att det finns två myndigheter som utövar tillsyn.

Den *särskilda tillsynsmyndigheten* införs som begrepp vid sidan av tillsynsmyndigheten.

Nuvarande säpodatalag innehåller en upplysning om att bestämmelser om tillsyn även finns i lagen om tillsyn över viss brottsbekämpande verksamhet (7 kap. 2 §). Av den sistnämnda lagen framgår Säkerhets- och integritetsskyddsnämndens uppdrag och befogenheter.

En utgångspunkt för vårt förslag är att det ska vara möjligt att ge tillsynsmyndigheterna de verktyg som behövs för en effektiv tillsyn. Säkerhets- och integritetsskyddsnämnden utövar tillsyn även över andra lagstiftningar och andra brottsbekämpande myndigheters verksamhet. Lagen om tillsyn över viss brottsbekämpande verksamhet är generellt utformad och lämnar samma tillsynsbefogenheter i förhållande till alla myndigheter som omfattas av tillsynen. Vi föreslår förändringar i regleringen av Säkerhetspolisens personuppgiftsbehandling som på ett tydligt sätt separerar denna lagstiftning från de lagar som har sitt ursprung i brottsdatadirektivet.

Vi anser att denna förändring motiverar att ge nämnden särskilda befogenheter, som inte är nödvändiga i förhållande till de andra brottsbekämpande myndigheterna. Dessa befogenheter bör därför lämpligen införas i den materiella lagstiftningen och inte

[3] Se prop. 2018/19:163 s. 168–171. Se även bland annat SOU 2016:65 s. 181–185.

som en särskild reglering i lagen om tillsyn över viss brottsbekämpande verksamhet.

För att kunna hänvisa till Säkerhets- och integritetsskyddsnämnden på ett konsekvent sätt i lagstiftningen bör den särskilda tillsyn som nämnden utför ges en beteckning i säpodatalagen. I nuvarande 7 kap. används begreppet tillsynsmyndigheten. Med detta avses Integritetsskyddsmyndigheten (se 2 a § andra stycket förordning, 2007:975, med instruktion för Integritetsskyddsmyndigheten). Det finns inte skäl att ändra vilken myndighet som utpekas som tillsynsmyndigheten i den nya säpodatalagen.

För att särskilja Säkerhets- och integritetsskyddsnämnden från Integritetsskyddsmyndigheten bör i stället benämningen *särskilda tillsynsmyndigheten* införas i säpodatalagen. Denna beteckning anser vi motsvara Säkerhets- och integritetsskyddsnämndens tillsynsuppdrag enligt både lagen om tillsyn över viss brottsbekämpande verksamhet och säpodatalagen. Genom denna beteckning finns inte heller någon risk för sammanblandning avseende vilka uppgifter och vilka befogenheter som tillfaller respektive myndighet enligt säpodatalagen och lagen om behandling av uppgifter i särskilda uppgiftssamlingar.

10.4 Undersökningsbefogenheter

Bedömning: Det finns inte skäl att ändra Integritetsskyddsmyndighetens nuvarande undersökningsbefogenheter. Det bör förtydligas att Säkerhets- och integritetsskyddsnämndens undersökningsbefogenheter motsvarar Integritetsskyddsmyndighetens.

Personuppgiftsbehandling blir alltmer komplex genom införande av ny teknik. För att säkerställa att den tekniska utvecklingen inte hindrar, utan i stället gynnar, en effektiv tillsyn bör Säkerhetspolisen ha en skyldighet att i rimlig utsträckning anpassa tekniska system efter den särskilda tillsynsmyndighetens behov och skapa förutsättningar för att utnyttja dessa system för en effektiv och ändamålsenlig tillsyn.

10.4.1 Vad krävs för en effektiv tillsyn?

Dataskyddskonventionen 108+ uppställer en rad krav som måste uppfyllas genom medlemsländernas lagstiftningar. Även om artikel 11 i konventionen medger vissa undantag från grundläggande principer för skyddet av nationell säkerhet, är det viktigt att notera att dessa undantag inte påverkar det grundläggande kravet på oberoende och effektiv granskning.

Konventionen fastslår tydligt att personuppgifter som behandlas för ändamål som rör nationell säkerhet och försvar alltjämt ska vara föremål för oberoende och effektiv granskning enligt nationell lagstiftning (artikel 11.3 andra stycket). Detta utgör en betydelsefull skillnad mellan den ursprungliga dataskyddskonventionen 108 och den uppdaterade konventionen 108+.

Tillsynsmyndighetens roll har förändrats i takt med att möjligheterna till automatiserad personuppgiftsbehandling har ökat genom alltmer sofistikerad informationsteknik. Vi befinner oss i början av ett skifte där tillsynen över formell regelefterlevnad behöver kompletteras med en djupare prövning av:

- Hur personuppgiftsbehandlingen faktiskt genomförs tekniskt.
- Vilka konsekvenser behandlingen får eller kan riskera att få.
- Behandlingens faktiska eller potentiella negativa effekter på grundläggande fri- och rättigheter.

Detta kräver en bredare och djupare tillsyn som omfattar både de formella förutsättningarna för personuppgiftsbehandling och de tekniska metoderna genom vilka behandlingen sker.

EU:s byrå för grundläggande rättigheter ger faktabaserade råd till EU och dess medlemsländers beslutsfattare i syfte att bland annat bidra till mer välgrundade lagar om grundläggande rättigheter. Ett sådant råd berör medlemsstaternas nationella underrättelsetjänster och de säkerhetsmekanismer som omgärdar statlig övervakning.[4] Byrån lämnar ett antal rekommendationer till lagstiftare i syfte att värna grundläggande rättigheter. Flera av dessa rekommendationer avser de resurser som krävs för en effektiv

[4] Europeiska unionens byrå för grundläggande rättigheter (FRA), *Underrättelsetjänsters övervakning: skyddsåtgärder för grundläggande rättigheter och rättsmedel i Europeiska unionen – Volym II – Sammanfattning*, 2018.

tillsyn. Byrån har bland annat framhållit att tillsynsramverket ska vara kraftfullt och adekvat i förhållande till underrättelsetjänstens befogenhet och kapacitet. Tillsynsorganen bör ha tillräckliga resurser, vilket innefattar tekniskt kvalificerad personal inom olika fackområden. Byrån har gjort undersökningar på plats i flera av EU:s medlemsstater. Vid dessa har man kunnat konstatera att det finns brister i tillgång till it-expertis och i teknisk förmåga bland tillsynsmyndigheterna, vilket identifierats som en stor utmaning. En av rekommendationerna är att EU:s medlemsstater genom lagstiftning bör ”säkerställa att tillsynsorganen har den tekniska expertis som krävs för att göra en oberoende bedömning av underrättelsetjänsternas ofta synnerligen tekniska arbete”.[5]

Sverige har i dag ett robust ramverk för tillsyn över Säkerhetspolisens personuppgiftsbehandling. Integritetsskyddsmyndighetens korrigerande befogenheter kompletteras av Säkerhets- och integritetsskyddsnämndens kontinuerliga och verksamhetsnära tillsyn.

De föreslagna lagändringarna och den tekniska utveckling som kan förutses ger dock anledning att överväga om vissa aspekter av tillsynen behöver förstärkas för att säkerställa att den förblir effektiv även i framtiden. Särskilt viktigt är att tillsynsmyndigheterna har tillräckliga befogenheter och resurser för att kunna granska alltmer avancerade tekniska lösningar för personuppgiftsbehandling.

10.4.2 Utökade skyldigheter för Säkerhetspolisen att bistå den särskilda tillsynsmyndigheten

Förslag: Säkerhetspolisen ska i skälig omfattning vidta de tekniska åtgärder som är nödvändiga för att den särskilda tillsynsmyndigheten ska kunna utföra sina arbetsuppgifter på ett ändamålsenligt sätt.

[5] Ibid, s. 10, *FRA:s yttrande 4*.

Teknikutvecklingen kan försvåra en effektiv tillsyn

Vårt förslag till säpodatalag och lag om behandling av personuppgifter i särskilda uppgiftssamlingar ger Säkerhetspolisen stora möjligheter att utnyttja ny teknik för en effektiv informationshantering. Vi har avstått från att försöka detaljreglera hur ny teknik ska få användas i verksamheten och i stället gett teknikneutrala förutsättningar att behandla personuppgifter, så länge behandlingen är proportionerlig.

Det är svårt att förutse på vilket sätt ny teknik kan komma att påverka Säkerhetspolisens verksamhet. Det är däremot inte svårt att förutse att den kommer att göra det. Det finns en risk att teknikutveckling som sker för ett starkt verksamhetsintresse samtidigt försvårar för tillsynen. Alltmer komplexa behandlingsåtgärder kan bli svårare och svårare att undersöka och bedöma vid tillsyn. Algoritmiska sökningar, profilering och andra förutsägelser genom maskininlärning är exempel på förmågor som kan komma att bli viktiga för Säkerhetspolisen. En förutsättning för att använda tekniker och metoder som kan påverka grundläggande fri- och rättigheter är att de behövs och är proportionerliga. Särskilt frågan om proportionalitet kan vara svår att bedöma när behandlingen nått en sådan teknisk komplexitet att det börjar bli svårt att redogöra för processen som leder fram till ett visst resultat (black box-teknik).

Det är uteslutet att bakbinda Säkerhetspolisens möjligheter att utnyttja den tekniska utvecklingen i större utsträckning än vad som är nödvändigt. Samtidigt är det också uteslutet att tillåta att Säkerhetspolisens förmågor utvecklas utan möjligheter till en oberoende kontroll. I det teknikskifte som kan förutses i närtid är det därför viktigt att tillsynsmyndigheterna har goda förutsättningar att utvecklas i takt med att tillsynsuppdragets komplexitet ökar.

Tillsynsbefogenheter i en era av snabb teknisk utveckling

En grundförutsättning för att tillsynen ska kunna utvecklas och förstärkas är att det tillförs tillräckligt med resurser. Vi lämnar i avsnitt 12.5.3 förslag om sådana resursförstärkningar. En minst lika viktig del av tillsynen är emellertid att tillsynen utvecklas i takt den snabba tekniska utvecklingen. Lagens syfte, som närmare redogörs för i avsnitt 8.1.1, är dubbelt: att skydda fysiska personers grund-

läggande rättigheter och friheter och att säkerställa att Säkerhetspolisen kan behandla personuppgifter på ett ändamålsenligt sätt. Tekniska system och förmågor som byggs upp med stöd av denna lag ska återspegla detta dubbla syfte, bland annat genom krav på inbyggt dataskydd och dataskydd som standard. Sådana åtgärder sker inom ramen för den personuppgiftsansvariges skyldigheter.

De befogenheter som Säkerhets- och integritetsskyddsnämnden i dagsläget har tillgång till har tillkommit i en tid då förutsättningarna att behandla personuppgifter såg väsentligt annorlunda ut. Nämndens utredningsbefogenheter är visserligen omfattande och innefattar rätt att få uppgifter, upplysningar och biträde. Regleringen omfattar alla uppgifter och handlingar som nämnden bedömer behövs för tillsynen, och biträde kan bestå i att tillsynsobjekten gör lokaler och system tillgängliga.

I takt med den tekniska utvecklingen uppstår dock nya utmaningar. Komplexa system, automatiserade processer och AI-baserade analyser kräver nya tillvägagångssätt vid tillsyn. Det räcker enligt vår bedömning inte längre att få tillgång till lokaler och handlingar när personuppgiftsbehandling i allt större utsträckning sker i avancerade tekniska miljöer som kräver särskild kompetens och särskilda verktyg för att kunna granskas effektivt.

Lagens syfte är att både skydda grundläggande rättigheter och säkerställa att Säkerhetspolisen kan behandla personuppgifter ändamålsenligt. För att upprätthålla denna balans krävs en tillsyn som kan hålla jämna steg med den tekniska utvecklingen. Dagens reglering är inte utformad för att möta de utmaningar som modern teknik medför för en effektiv tillsyn. Det krävs därför att nämndens befogenheter stärks i detta avseende.

Skyldighet att vidta tekniska åtgärder för effektiv tillsyn

Det är en central del av vårt förslag att Säkerhets- och integritetsskyddsnämnden ska kunna utföra en effektiv och kvalificerad tillsyn över Säkerhetspolisens personuppgiftsbehandling. För detta krävs att Säkerhetspolisen samarbetar och biträder vid tillsynen. Dessutom anser vi att Säkerhetspolisen ska vara skyldig att vidta de tekniska åtgärder som är nödvändiga för att tillsynen ska kunna ske på ett ändamålsenligt sätt. Detta kan exempelvis innebära att:

- Särskilda informationsmängder tillgängliggörs för tillsynsmyndigheten under en avgränsad tid
- Tillsynsmyndigheten ges möjlighet att analysera tvärsnitt av information i stället för att Säkerhetspolisen utför specifika sökningar
- Komplexa urvalsverktyg utvecklas för att hitta eller sålla bort information vid tillsyn
- Tillsynsmyndigheten får möjlighet att utnyttja AI och andra avancerade analysverktyg i sin granskande verksamhet

Avgörande är att de tekniska framsteg som möjliggör effektivare personuppgiftsbehandling i den operativa verksamheten även ska kunna utnyttjas för tillsyn.

Säkerhetspolisen måste givetvis själv ha full kontroll över sina egna tekniska system. Den möjlighet som vi nu föreslår måste därför formuleras som en skyldighet för Säkerhetspolisen. Det är Säkerhetspolisen som ska vara skyldig att vidta de tekniska åtgärder som behövs för att tillsynen ska kunna utföras på ett ändamålsenligt sätt.

De tekniska funktioner och de syften som ska uppfyllas med dem måste formuleras av tillsynsmyndigheten. Det är endast tillsynsmyndigheten som utifrån de rättsliga förutsättningarna ska ha befogenhet att bestämma behoven och inriktningen för tillsynen. Om det finns flera sätt att uppnå ett syfte, har Säkerhetspolisen möjlighet att vidta åtgärderna på ett så effektivt sätt som möjligt och på det sätt som är lämpligast. De praktiska formerna för samarbetet som krävs för att verkställa och utforma tekniska åtgärder får utarbetas myndigheterna emellan. Denna i vårt tycke viktiga, och förmodligen allt viktigare tillsynsmekanism, bör emellertid formaliseras som en skyldighet i lag.

Av de båda tillsynsmyndigheterna är det Säkerhets- och integritetsskyddsnämnden som utför den kontinuerliga och verksamhetsnära tillsynen. Det är därför naturligt att det är nämnden och inte Integritetsskyddsmyndigheten som ska ha den utökade undersökningsbefogenheten att begära biträde i form av tekniska åtgärder. Integritetsskyddsmyndigheten har förstås ändå inom ramen för sina undersökningsbefogenheter möjlighet att för sin tillsynsverksamhet nyttja de anpassningar av system som görs.

Säkerhetspolisens skyldigheter att vidta tekniska åtgärder kan inte vara obegränsad. Det får betecknas som särpräglat att en myndighet på detta sätt åläggs att vidta resurskrävande åtgärder i en annan myndighets intresse. Hur långt skyldigheten ska utsträckas kan dock vara svårt att lämna ett generellt svar på.

Samtidigt är det viktigt att ha i åtanke att en effektiv tillsyn, enligt vår bedömning, är en faktisk förutsättning för Säkerhetspolisens verksamhet. Utan en tillräckligt robust tillsyn är den personuppgiftsbehandling vi föreslår inte förenlig med Sveriges internationella åtaganden. Genom en tidig samverkan mellan Säkerhets- och integritetsskyddsnämnden och Säkerhetspolisen i frågor som rör tekniska system bör nämndens behov kunna klarläggas. Säkerhetspolisen kan då ta med sig tillsynsperspektivet exempelvis inom ramen för en upphandling eller utveckling (se vidare avsnitt 10.9).

Säkerhetspolisens skyldigheter i nyssnämnda avseende bör begränsas till det som är skäligt. Säkerhets- och integritetsskyddsnämndens behov måste beaktas men får inte på ett påtagligt sätt påverka Säkerhetspolisens förmåga att lösa sitt uppdrag. Skyldigheten innebär dock att det i vissa fall krävs att resurser läggs på funktioner som endast gagnar tillsynen. I system som är helt centrala kan det därför krävas att exempelvis utvecklingsresurser läggs på funktionalitet som ska användas för tillsynsändamål, förutsatt att det kan ske utan att gå ut över Säkerhetspolisens operativa förmåga.

10.4.3 Undersökningsbefogenheter enligt säpodatalagen

Förslag: Tillsynsmyndighetens nuvarande undersökningsbefogenheter bör överföras till den nya lagen.

Bedömning: I befogenheten för tillsynsmyndigheten att få den hjälp och den information som behövs för tillsynen ingår i skälig omfattning den tekniska fortbildning som krävs för att granska automatiserade behandlingsmedel som programvara och system.

De nuvarande undersökningsbefogenheterna

Integritetsskyddsmyndigheten har omfattande befogenheter att granska och utöva tillsyn över i princip alla myndigheter. Detta inkluderar den allra mest känsliga verksamheten som bedrivs i Sverige genom Försvarsmaktens, FRA:s och Säkerhetspolisens försorg. Integritetsskyddsmyndighetens tillsynsuppdrag och de befogenheter som följer av detta uppdrag är, ur ett internationellt perspektiv, mycket långtgående avseende dessa typer av verksamheter.

Integritetsskyddsmyndigheten har under en längre tid, på grund av andra prioriteringar, inte utövat tillsyn över Säkerhetspolisens behandling av personuppgifter. Myndigheten har alltså inte bedrivit någon kontinuerlig tillsyn över Säkerhetspolisens personuppgiftsbehandling. Inget har dock framkommit som ger oss skäl att ifrågasätta att Integritetsskyddsmyndigheten har både den kompetens och organisation som behövs för att utföra sitt tillsynsuppdrag på ett bra sätt.

De undersökningsbefogenheter som framgår av 7 kap. 3 § säpodatalagen ger Integritetsskyddsmyndigheten rätt att på begäran få

1. tillgång till alla personuppgifter som behandlas,
2. upplysningar om och dokumentation av behandlingen av personuppgifter och säkerhets- och skyddsåtgärder,
3. tillträde till lokaler som Säkerhetspolisen eller personuppgiftsbiträdet disponerar samt tillgång till utrustning och andra medel för behandling av personuppgifter, och
4. den hjälp och den information som behövs för tillsynen.

Dessa befogenheter kompletteras av en skyldighet för Säkerhetspolisen att, enligt 5 kap. 8 § säpodatalagen, samarbeta med tillsynsmyndigheten. Samarbetsskyldigheten innebär att Säkerhetspolisen inom rimlig tid och på lämpligt sätt ska ge Integritetsskyddsmyndigheten tillgång till det material och de resurser som behövs för tillsynen. Säkerhetspolisen måste även ställa personal till förfogande för att exempelvis utföra sökningar.[6]

[6] Prop. 2018/19:163 s. 254.

Vår uppfattning är att Integritetsskyddsmyndigheten har en långtgående möjlighet att granska Säkerhetspolisens personuppgiftsbehandling. Det har inte framförts några behov som inte tillmötesgås genom den nuvarande regleringen. Denna bör därför överföras till den nya lagen.

Tillgång till och utbildning i tekniska system

En effektiv tillsyn måste ha förmåga att granska den personuppgiftsbehandling som sker i en teknisk process. För en sådan granskning kan krävas relativt ingående tekniska kunskaper. Den juridiska kompetens som finns inom tillsynsmyndigheten behöver därför kompletteras med personal som har förståelse för den bakomliggande tekniska strukturen. Vi är övertygade om att tillsynsmyndigheterna kommer behöva förstärka sina respektive organisationer med någon form av teknisk kompetens.

Det kan knappast krävas en fullständig teknisk förståelse för varje enskilt system för att utföra en granskning eller utöva tillsyn. För att kunna ställa relevanta frågor och uppmärksamma brister eller risker krävs däremot många gånger en teknisk utbildning. Därutöver krävs att varje enskilt system på något sätt görs tillgängligt för tillsyn.

De nuvarande undersökningsbefogenheterna omfattar *tillgång till utrustning och andra medel för behandling av personuppgifter*. Det innebär inte någon rätt för tillsynsmyndigheten att fritt använda Säkerhetspolisens utrustning och datasystem. Däremot innefattas en rätt för tillsynsmyndigheten att, med hjälp av Säkerhetspolisens personal, ta del även av den bakomliggande tekniken.

Säkerhetspolisen måste, inom rimliga ramar, kunna förklara och visa hur ett visst resultat uppnåtts då personuppgifter behandlas i olika datasystem eller mjukvaror. Säkerhetspolisen måste kunna redogöra för sina personuppgiftsbehandlingar på ett sätt som möjliggör en meningsfull tillsyn, även när avancerade tekniska system används. När det gäller AI-system och maskininlärning finns en inneboende utmaning i att exakt förklara hur enskilda resultat uppnås, eftersom dessa modeller ofta fungerar som en ”black box” där sambanden mellan indata och utdata inte är fullt transparenta.

Denna begränsning undantar dock inte Säkerhetspolisen från tillsyn. Myndigheten ska kunna:

1. Ge en ingående förklaring av systemets övergripande funktion, arkitektur och syfte
2. Redovisa vilka data som använts för träning av AI-modeller
3. Beskriva vilka testmetoder som använts för att validera systemets tillförlitlighet
4. Förklara vilka begränsningar systemet har och hur dessa hanteras
5. Redogöra för de processer och rutiner som finns för att bedöma och värdera de resultat som systemet levererar

Särskilt viktig är tillsynen över hur Säkerhetspolisen värderar, tolkar och använder de resultat som AI-systemen levererar i sin verksamhet. Detta omfattar även dokumentation av processen för hur beslut fattas baserat på systemets resultat, samt vilka kompletterande bedömningar som görs.

Tillsynsmyndigheten ska ha rätt att granska samtliga dessa aspekter för att säkerställa att personuppgiftsbehandlingen förblir proportionerlig, rättssäker och förenlig med grundläggande fri- och rättigheter, även när tekniskt komplexa system används.

Tillsynen bör med stöd av de nuvarande undersökningsbefogenheterna kunna ske av tillsynsmyndighetens IT-specialister, med stöd av motsvarande personalgrupp vid Säkerhetspolisen.

Den nuvarande undersökningsbefogenheten som anger att tillsynsmyndigheten har rätt till *den hjälp och den information som behövs för tillsynen* innefattar, enligt de nuvarande förarbetena, även information som inte har direkt anknytning till behandlingen av personuppgifter. Det är tillräckligt att tillsynsmyndigheten behöver informationen för tillsynen. Det kan exempelvis handla om verksamhetsplaner som beskriver den verksamhet där behandlingen utförs.[7]

Vår uppfattning är att denna rätt rimligen även innefattar en allmän beskrivning av och utbildning i de tekniska system som används för personuppgiftsbehandling. Syftet är att tillsynsmyndigheten ska ges förutsättningar till en effektiv tillsyn. Det kan innebära att Säkerhetspolisen måste bidra till kompetensutvecklingen

[7] Ibid. s. 254 f.

för de personer som ska utöva tillsyn över de specifika system som finns inom myndigheten. Säkerhetspolisen kan ha tekniska system skräddarsydda för verksamheten, som därmed inte är möjliga att lära sig utanför organisationen. Av informationssäkerhetsskäl kan det även vara en fördel om Säkerhetspolisen kan bidra till och vara ansvarig för den kompetensutveckling som krävs för att granska de system som används inom verksamheten.

Eftersom de nu diskuterade skyldigheterna för Säkerhetspolisen följer redan av gällande rätt, föreslår vi inte någon lagändring.

10.4.4 Kompletterande undersökningsbefogenheter för Säkerhets- och integritetsskyddsnämnden

Förslag: Rätten till uppgifter, upplysningar, information och biträde som följer av lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet ska kompletteras genom hänvisning till de undersökningsbefogenheter som tillsynsmyndigheten (Integritetsskyddsmyndigheten) har enligt säpodatalagen.

Enligt 4 § lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet har nämnden rätt att av Säkerhetspolisen få de uppgifter och upplysningar, den information och det biträde som nämnden begär. Även domstolar och de förvaltningsmyndigheter som inte omfattas av tillsynen är skyldiga att lämna nämnden de uppgifter som den begär. Denna uppgifts- och biträdesskyldighet är inte formulerad på samma sätt som Integritetsskyddsmyndighetens undersökningsbefogenheter enligt säpodatalagen, men har till sitt innehåll getts en i huvudsak motsvarande innebörd hos myndigheterna.

Det är viktigt att den reglering vi föreslår fungerar i alla situationer. Vår uppfattning är att tillsynsmyndigheterna kan ha sin viktigaste uppgift under tider då samarbetet med tillsynsobjektet inte fungerar som önskvärt. För att undvika oklarheter i frågan om undersökningsbefogenheterna i något avseende skiljer sig åt mellan de båda tillsynsorganen bör den likformighet som redan anses föreligga även komma till formellt uttryck. Vi föreslår därför att nämndens undersökningsbefogenheter enligt 4 § lagen om tillsyn över viss brottsbekämpande verksamhet ska kompletteras genom att det

i säpodatalagen framgår att nämnden även har de undersökningsbefogenheter som gäller för tillsynsmyndigheten.

10.4.5 Samarbetsskyldigheten ska gälla även i förhållande till den särskilda tillsynsmyndigheten

Förslag: Säkerhetspolisen ska vara skyldig att samarbeta med alla myndigheter som utövar tillsyn över personuppgiftsbehandlingen enligt säpodatalagen och anslutande förordning.

Samarbetsskyldighet är en förutsättning för effektiv tillsyn

Genom den nuvarande säpodatalagen infördes, i 5 kap. 8 §, en uttrycklig samarbetsskyldighet med tillsynsmyndigheten. Syftet var att den personuppgiftsansvarige skulle underlätta för tillsynsmyndigheten att utöva sina tillsynsbefogenheter på ett effektivt sätt. I princip måste samtliga undersökningsbefogenheter utnyttjas genom att Säkerhetspolisen är behjälplig på olika sätt. Samarbetsskyldigheten ger därmed förutsättningarna för att tillsynsmyndigheten på ett effektivt sätt ska kunna utöva sina rättigheter i samband med tillsynen.

Samarbetsskyldigheten aktualiseras endast när tillsynsmyndigheten utför sina uppgifter enligt lagen eller förskrifter som meddelats i anslutning till den. Det har inte ansetts möjligt för tillsynsmyndigheten att med tvång utnyttja sina undersökningsbefogenheter vilket ytterligare motiverat att samarbetet ska formuleras som en skyldighet för den personuppgiftsansvarige.[8]

Den rätt till tillgång till uppgifter som finns för Integritetsskyddsmyndigheten, genom undersökningsbefogenheterna i säpodatalagens nuvarande 7 kap. 3 §, kräver att myndigheten begär vissa uppgifter. Samarbetsskyldigheten uppfattar vi ger en bredare skyldighet för Säkerhetspolisen att vara behjälplig när tillsynsmyndigheten utövar tillsyn, exempelvis genom att visa vilka möjligheter som finns att utföra sökningar eller hur system används i den operativa verksamheten.

[8] Ibid. s. 142 och prop. 2017/18:232 s. 292.

Samarbetsskyldigheten bör även omfatta Säkerhets- och integritetsskyddsnämnden

I gällande rätt finns endast en skyldighet för Säkerhetspolisen att samarbeta med Integritetsskyddsmyndigheten. Skälet till att bestämmelsen i säpodatalagen formulerats så förefaller i första hand ha att göra med att det endast är tillsynsmyndigheten som utpekas i brottsdatadirektivet (artikel 26).

Vi har inte kunnat hitta något bärande skäl till att samarbetsskyldigheten begränsats till Integritetsskyddsmyndigheten. Ett aktivt och väl utfört samarbete innebär att Säkerhetspolisen ska underlätta för tillsynsmyndigheten exempelvis genom att berätta hur system fungerar och hjälpa till i utförandet av tillsynsuppgifter. Utan ett sådant aktivt samarbete kan det vara i princip omöjligt att ta fram personuppgifter och granska behandlingen av dem.

Säkerhets- och integritetsskyddsnämnden har rätt att få de uppgifter och upplysningar, den information och det biträde som nämnden begär. Dessa befogenheter har en likartad utformning som de undersökningsbefogenheter som tillkommer Integritetsskyddsmyndigheten. Det innebär att Säkerhetspolisen är skyldig att lämna nämnden de uppgifter som den begär, även om det förutsätter viss efterforskning från myndigheternas sida. Rent utredningsarbete omfattas inte av skyldigheten.

Säkerhetspolisen är även skyldig att biträda nämnden. Sådant biträde kan bestå i att myndigheterna gör lokaler, databaser, register och andra handlingar som omfattas av ett tillsynsärende tillgängliga för nämnden och lämnar de uppgifter som nämnden behöver för att klarlägga de förhållanden som tillsynen avser.[9]

De motiv som föranledde att Integritetsskyddsmyndighetens undersökningsbefogenheter kompletterades av en samarbetsskyldighet för Säkerhetspolisen gör sig i minst lika stor utsträckning gällande i förhållande till Säkerhets- och integritetsskyddsnämnden. Dessa skäl blir särskilt tydliga när vi föreslår att det uttryckligen ska anges att tillsynsmyndighetens undersökningsbefogenheter även gäller den särskilda tillsynsmyndigheten (se avsnitt 10.4.4 ovan)

Även om samarbetet fungerar tillfredsställande i dagsläget anser vi att det finns skäl att införa en uttrycklig samarbetsskyldighet i förhållande till nämnden. Risken är annars att skillnaden i regler-

[9] Prop. 2017/18:269 s. 280 f. och prop. 2006/07:133 s. 81 f.

ingen kan motivera att myndigheterna bemöts på olika sätt vid tillsynen. Även om denna risk framstår som avlägsen i dagsläget finns inga skäl att särskilja regleringen i detta avseende. Om något så är det särskilt angeläget att skyldigheten att samarbeta är reglerad i förhållande till den myndighet som regelbundet utövar tillsyn, nämligen Säkerhets- och integritetsskyddsnämnden.

Vi anser därför att en uttrycklig samarbetsskyldighet för Säkerhetspolisen ska införas i den nya lagen och omfatta även den särskilda tillsynsmyndigheten. Det förtydligar att den särskilda tillsynsmyndigheten kan begära exempelvis att Säkerhetspolisen i skälig utsträckning bidrar med de resurser som krävs för att utöva en effektiv tillsyn, liksom att kontaktpersoner utses inom olika verksamhetsgrenar eller att tillsynsmyndigheten får egen tillgång till datorer eller annan utrustning.[10]

10.4.6 Det krävs särskilda undersökningsbefogenheter för tillsyn över behandling i särskilda uppgiftssamlingar

Bedömning: Tillsynsmyndigheterna bör inte ha rätt att utan tillstånd ta del av personuppgifter som behandlas i särskilda uppgiftssamlingar.

Förslag: Säkerhets- och integritetsskyddsnämnden ska ha möjlighet att för tillsynsändamål ansöka om framtagning från en särskild uppgiftssamling.

Inom ramen för ett enskilt fall bör även Integritetsskyddsmyndigheten ha denna möjlighet.

Det krävs tillstånd för att ta fram personuppgifter för tillsynsändamål

Tillsyn över behandlingen enligt den föreslagna lagen om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar kan exempelvis komma att bestå av att nämnden granskar de registreringsbeslut som fattats av ett visst slag eller under en viss

[10] En sådan möjlighet behöver utformas med beaktande av synen på när tillgången kan betraktas som direktåtkomst (jfr prop. 2017/18:232 s. 291).

tid. Nämnden kan ställa uppföljande frågor om det i något avseende framstår som otydligt varför en viss registrering gjorts eller vilka uppgifter registreringen omfattar. Sådan tillsyn kan ske med stöd av de nuvarande undersökningsbefogenheterna.

Lagen om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar bygger på principen om att uppgifterna som är registrerade inte ska vara åtkomliga utan särskilt tillstånd. Denna princip är en viktig förutsättning för att den föreslagna lagen ska vara förenlig med skyddet för personlig integritet och andra grundläggande fri- och rättigheter. Att Säkerhetspolisen inte utan tillstånd får göra sökningar och framtagningar är motiverat bland annat av att en myndighet inte kan ges för stora befogenheter utan att det motsvaras av en tillräckligt effektiv skyddsmekanism. Frågan är om samma synsätt kan göras gällande för tillsynsmyndigheters tillgång till personuppgifter som registrerats i en särskild uppgiftssamling.

Å ena sidan kan det finnas skäl att se annorlunda på det intrång som en framtagning ska anses innebära när ändamålet är att kontrollera att de registrerades rättigheter inte kränks. Det får anses vara mindre integritetskänsligt att ta fram personuppgifter i det syftet än att göra det för exempelvis brottsbekämpande ändamål. Det har exempelvis inte ansetts vara oförenligt med ett sökförbud om en sökning görs för tillsynsmyndighetens räkning. Å andra sidan är en viktig aspekt av det personuppgiftsskydd vi föreslagit att intrånget av att vara registrerad ska anses vara avsevärt högre när någon har möjlighet att ta fram uppgifter utan tillstånd. Risken att uppgifter sprids eller missbrukas är generell och gäller tillsynsmyndigheternas personuppgiftsbehandling likväl som andras. Även framtagningar för att exempelvis kontrollera systemens funktionalitet eller för registervård där personuppgifter tas fram som utförs av tekniker vid Säkerhetspolisen har vi ansett kräva tillstånd. Vi anser att tillståndskravet för framtagning måste gälla generellt och därför omfatta även tillsynsmyndigheterna.

Tillsynsmyndigheternas befogenheter att få tillgång till alla de personuppgifter som behandlas kommer därmed inte att gälla dem som behandlas i särskilda uppgiftssamlingar. För att förtydliga detta bör ett uttryckligt undantag från dessa befogenheter införas i lagen om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar.

Det innebär att Säkerhets- och integritetsskyddsnämnden eller Integritetsskyddsmyndigheten inte kan begära att Säkerhetspolisen ska ta fram personuppgifter från en särskild uppgiftssamling, om det saknas tillstånd till detta. Ett sådant tillstånd får endast medges för vissa ändamål. Ett tillstånd till framtagning för ett brottsbekämpande ändamål omfattar inte framtagningar för tillsynsändamål. Det går därför inte att med stöd av ett sådant tillstånd, på tillsynsmyndighetens begäran, kontrollera om andra uppgifter än vad som kan anses vara befogade för ett registreringsändamål förekommer i en särskild uppgiftssamling eller om beskrivningen av ett registreringsbeslut överensstämmer med de uppgifter som det omfattar. Däremot hindrar den föreslagna ordningen inte att nämnden kontrollerar en framtagning som redan skett på Säkerhetspolisens begäran. Tvärtom kommer det att vara en viktig del av tillsynen att Säkerhetspolisen håller sig inom domstolens tillstånd och de villkor som är förenat med tillståndet, vilket vi återkommer till nedan.

En effektiv tillsyn över särskilda uppgiftssamlingar måste dock på något sätt kunna inbegripa en tillsyn över de enskilda personuppgifter som behandlas i en sådan. En möjlighet är att Säkerhetspolisen ska vara skyldig att ansöka om tillstånd för att tillgodose tillsynsbehov. Det skulle innebära att tillsynsmyndigheten först hemställer hos Säkerhetspolisen om att myndigheten ska ansöka om ett tillstånd hos domstolen men till förmån för tillsynsmyndigheten. Vid sidan av att effektiviteten av ett sådant förfarande framstår som tveksam kan det ifrågasättas om ordningen fullt ut tillgodoser kravet på oberoende tillsyn. Förutsättningarna för tillsynen bör inte utgå från en sådan aktiv åtgärd från Säkerhetspolisen.

Tillsynsmyndigheterna ska ha möjlighet att ansöka om tillstånd till framtagning

Vi anser att det enklaste och mest effektiva är att ge möjlighet för tillsynsmyndigheten att själv, för tillsynsändamål, ansöka om tillstånd till framtagning. Domstolen får då pröva omfattningen av och syftet med åtgärden utifrån samma grundläggande krav som gäller då Säkerhetspolisen ansöker om tillstånd.

Tillsynen ska vara oberoende och det är självklart att det är den särskilda tillsynsmyndigheten som själv väljer inriktningen på tillsynen. Integritetsriskerna är normalt mindre då en framtagning

sker för en tillsynsmyndighets räkning. Det avgörande för tillståndsprövningen är att framtagningen bidrar till en ändamålsenlig tillsyn enligt nämndens valda inriktning samtidigt som den inte omfattar fler uppgifter än vad som behövs. De närmare förutsättningarna och vilka villkor som ska gälla vid ett sådant tillstånd bör vara en fråga för rättstillämpningen. Även i detta fall gäller det grundläggande kravet på proportionalitet mellan behovet och de andra intressen som kan påverkas.

Av de båda tillsynsmyndigheterna är det Säkerhets- och integritetsskyddsnämnden som utför den kontinuerliga och verksamhetsnära tillsynen. Nämnden uppträder i domstolen i samband med yttranden över Säkerhetspolisens ansökningar och har en organisation som känner till verksamheten. Vi har i avsnitt 9.7.2 redogjort för att det kan finnas skäl att låta vissa tillstånd löpa under en längre tid och avse olika slags framtagningar som sker för samma ändamål. Det bör vara en möjlighet för nämnden att ansöka om tillstånd för att ta fram de personuppgifter som krävs för en kontinuerlig och verksamhetsnära tillsyn över tillämpningen av den föreslagna lagen.

Integritetsskyddsmyndigheten kan inte på samma sätt förväntas ha en kontinuerlig tillsyn över Säkerhetspolisens tillämpning av den föreslagna lagen. Integritetsskyddsmyndigheten förfogar dock över korrigerande tillsynsbefogenheter som även bör kunna tillämpas för behandling som sker enligt denna lag.

Integritetsskyddsmyndigheten kan starta tillsyn på eget initiativ eller efter en anmälan från Säkerhets- och integritetsskyddsnämnden. I båda dessa fall kan det finnas behov för myndigheten att ta del av registrerade personuppgifter genom framtagning. Myndigheten måste givetvis ha en fullgod utredning innan den beslutar om en korrigerande befogenhet som kan få betydelse för Säkerhetspolisen operativa förmåga.

Vi anser att det därför, i enskilda fall, bör finnas möjlighet även för Integritetsskyddsmyndigheten att ansöka om tillstånd till framtagning.

Övriga undersökningsbefogenheter avseende särskilda uppgiftssamlingar

Att tillsynsmyndigheterna inte utan tillstånd kan få del av de personuppgifter som behandlas innebär inte att det saknas undersökningsbefogenheter i övrigt. Utan tillstånd kan tillsyn ske bland annat av de tekniska hjälpmedel som används för att utföra framtagning enligt tillstånd. Det innefattar exempelvis hur olika urvalskriterier som tillåts enligt ett tillstånd tillämpas eller tolkas.

Tillsynsmyndigheterna har också rätt att ta del av alla registreringsbeslut med stöd av lagen och exempelvis granska hur behandlingstid bestäms eller hur besluten motiverats.

En av de viktigaste uppgifterna är att granska att tillståndet efterlevs och att inga andra personuppgifter tas fram än vad som följer av ett tillstånd. Eftersom det får förutsättas att det kontinuerligt kommer att tas fram uppgifter med stöd av tillstånd är utgångspunkten att det i första hand kommer vara en tillsyn som utförs av Säkerhets- och integritetsskyddsnämnden. Inom ramen för tillståndsprövningen i domstol kommer nämnden kunna yttra sig om vad som framkommit vid tillsynen och bland annat föreslå vilka särskilda villkor som kan behövas för effektiv tillsyn och kontroll, se avsnitt 9.8.4.

10.5 Samverkan och samråd

10.5.1 Samverkan mellan tillsynsmyndighet och verksamhetsutövare

Förslag: Säkerhetspolisen och den särskilda tillsynsmyndigheten ska löpande samverka i frågor som rör Säkerhetspolisens skyldigheter enligt lag eller annan författning.

Tillsynsmyndighetens uppdrag att lämna råd och stöd samt dess förebyggande befogenheter ska överföras till den nya lagen.

Samverkan i dag

Integritetsskyddsmyndigheten

En stor del av Integritetsskyddsmyndighetens verksamhet går ut på att förebygga att fel begås, bland annat genom att lämna råd och anvisningar till den personuppgiftsansvariga myndigheten. I säpodatalagen ges tydliga instruktioner till Integritetsskyddsmyndigheten att hjälpa den personuppgiftsansvarige att göra rätt och förebygga att denne behandlar personuppgifter i strid med lag. I 7 kap. 1 § säpodatalagen, där tillsynsmyndighetens uppgifter beskrivs, anges bland annat att tillsynsmyndigheten, när det är påkallat, ska ge råd och stöd beträffande Säkerhetspolisens skyldigheter enligt lag. Enligt 4 § i samma kapitel ska tillsynsmyndigheten agera med råd, rekommendationer eller påpekanden om den bedömer att det finns risk för att Säkerhetspolisen kan komma att behandla personuppgifter i strid med lag. Tillsynsmyndigheten kan lämna rådgivning när den identifierar risker i pågående behandling eller om Säkerhetspolisen påkallar det. Rådgivning kan avse såväl formella som informella samråd men Integritetsskyddsmyndigheten har inte någon skyldighet att lämna råd, vid sidan av den särskilt reglerade situationen då Säkerhetspolisen påkallar förhandssamråd enligt 5 kap. 6 § andra stycket säpodatalagen. Som nämnts utövar Integritetsskyddsmyndigheten i dagsläget inte någon regelbunden tillsyn över Säkerhetspolisen, som inte heller har påkallat formella förhandssamråd i någon nämnvärd utsträckning. Det finns inte någon etablerad samverkan mellan Säkerhetspolisen och Integritetsskyddsmyndigheten vid sidan av eventuella förhandssamråd.

Säkerhets- och integritetsskyddsnämnden

Den regelbundna och särskilda tillsynen över säpodatalagen utövas av Säkerhets- och integritetsskyddsnämnden, som genom sin tillsyn får både en inblick i och en överblick över Säkerhetspolisens behandling av personuppgifter. Tillsynen ska ske genom inspektioner och andra undersökningar. Nämnden får uttala sig om konstaterade förhållanden och sin uppfattning om behov av förändringar i verksamheten och ska verka för att brister i lag eller annan

författning avhjälps (2 § lagen om tillsyn över viss brottsbekämpande verksamhet).

Det finns därmed inte något liknande uppdrag för nämnden, som innebär en skyldighet att ge råd och stöd till Säkerhetspolisen, som för Integritetsskyddsmyndigheten. I samband med att nämnden ska utöva sin tillsyn sker viss samverkan mellan myndigheterna. Det kan röra praktiska frågor, som när inspektioner ska genomföras eller att vissa frågor anmäls och förbereds på förhand. Det förekommer däremot i dagsläget inte någon regelbunden och återkommande samverkan på högre myndighetsnivå eller i mer övergripande frågor.

Tillsynsmyndighetens samverkansskyldighet ska kvarstå

Den nuvarande ordningen innebär en relativt omfattande reglering av Integritetsskyddsmyndighetens skyldigheter att ge råd och stöd avseende Säkerhetspolisens skyldigheter som personuppgiftsansvarig. Samtidigt är det inte Integritetsskyddmyndigheten som är den av de båda tillsynsmyndigheterna som har bäst möjlighet att lämna råd i frågor som rör de lagar vi föreslår. Vårt förslag till ny säpodatalag avviker i många avseenden från de regelverk över vilka Integritetsskyddsmyndigheten i övrigt utövar tillsyn. Generella råd om personuppgiftsbehandling kommer därför endast i undantagsfall gälla Säkerhetspolisens, eftersom sådana råd utgår från den EU-rätt som reglerar stora delar av samhällets personuppgiftsbehandling i övrigt. Det finns en annan inre logik i ett system som i sig utgör ett långsträckt undantag från skyddet av grundläggande fri- och rättigheter, i syfte att värna demokratin och den nationella säkerheten. Det är därför inte möjligt att dra självklara analogislut mellan närliggande lagstiftningar som bygger på andra grundläggande avvägningar och den säpodatalag vi föreslår. Vi anser dock att det i dagsläget inte finns några skäl att ta bort eller ändra på Integritetsskyddsmyndighetens uppdrag eller befogenheter som följer av nuvarande 7 kap. 1 och 4 §§. Myndigheten har en viktig roll att spela, både vad gäller tillsynen över Säkerhetspolisens specifika lagstiftning och i vissa generella frågor där myndigheten besitter särskild kompentens, se avsnitt 10.2.2. Det kan dock finnas skäl att överväga om rådgivning, stöd eller annan samverkan i frågor som rör Säkerhetspolisens skyl-

digheter som personuppgiftsansvarig ska regleras även avseende Säkerhets- och integritetsskyddsnämnden.

Samverkan bör regleras även avseende den särskilda tillsynsmyndigheten

Säkerhets- och integritetsskyddsnämnden har utifrån sin särskilda kompetens inom den sektorsspecifika lagstiftning som Säkerhetspolisen tillämpar goda möjligheter att diskutera specifika tillämpningsfrågor eller påpeka risker som identifieras under tillsynen. De lagar vi föreslår bygger på en relativt intrikat bedömning av behov, intrång och proportionalitet. Sådana proportionalitetsbedömningar har vi ansett vara frågor som med fördel kan prövas och bedömas av en nämnd med stark parlamentarisk anknytning. Eftersom Säkerhets- och integritetsskyddsnämnden utövar särskild tillsyn över lagen anser vi att det finns skäl att nämnden ska få en rådgivande roll som komplement till uppdraget att uttala sig i efterhand, om konstaterade förhållanden.

Hur bör samverkan regleras?

Det är inte lämpligt med samma regler som för Integritetsskyddsmyndigheten

Det finns flera sätt att ge den särskilda tillsynsmyndigheten i uppdrag att lämna råd eller anvisningar och på andra sätt samverka kring Säkerhetspolisens skyldigheter som personuppgiftsansvarig enligt de nya lagar vi föreslår.

Det är exempelvis möjligt att lämna ett motsvarande uppdrag till Säkerhets- och Integritetsskyddsnämnden som gäller för tillsynsmyndigheten. Det skulle då kunna formuleras som att den särskilda tillsynsmyndigheten ska ge råd och stöd till Säkerhetspolisen och personuppgiftsbiträden om deras skyldigheter enligt lag eller annan författning. En sådan skyldighet kan innebära en abstrakt rådgivning, om exempelvis innehållet i gällande rätt och olika rättsliga ställningstaganden. Med tanke på den höga kompetens som finns inom Säkerhetspolisen i frågor som rör personuppgiftsbehandling i allmänhet finns dock knappast något behov för sådan rådgivning.

Ett annat (eller kompletterande) sätt att få till stånd ett informationsutbyte mellan myndigheterna är att ge Säkerhets- och integritetsskyddsnämnden motsvarande förebyggande befogenheter som tillsynsmyndigheten har i nuvarande 7 kap. 4 § säpodatalagen. Det skulle innebära att den särskilda tillsynsmyndigheten genom råd, rekommendationer eller påpekanden ska försöka förmå Säkerhetspolisen att vidta åtgärder för att motverka risken att personuppgifter inte kommer att behandlas författningsenligt. I tidigare förarbeten har det emellertid ansetts angeläget att det inte ska uppfattas som att nämnden kan godkänna ett förfarande på förhand.

Om nämnden på samma sätt som Integritetsskyddsmyndigheten skulle ges befogenhet att lämna de råd med mera som behövs för att motverka risker vid behandling av personuppgifter, skulle det innebära ett slags förhandsbesked. Eftersom nämndens tillsyn bygger på uttalanden om konstaterade förhållanden skulle det kunna bli otydligt när nämnden uttalar sig (enligt 2 § lagen om tillsyn över viss brottsbekämpande verksamhet) eller lämnar ett ”förebyggande råd”. De råd eller rekommendationer som kan lämnas av Integritetsskyddsmyndigheten kan följas upp med ett överklagbart beslut, om den personuppgiftsansvarige inte rättar sig. Säkerhets- och Integritetsskyddsnämnden kan endast följa upp ett förebyggande råd med ett uttalande om de förhållanden som därefter kan konstateras. Att ge nämnden en motsvarighet till Integritetsskyddsmyndighetens förebyggande befogenheter enligt nuvarande 7 kap. 4 § bedömer vi sammantaget inte vara lämpligt.

Samverkan bör ske i frågor som rör den personuppgiftsansvariges skyldigheter

För oss framstår det som lämpligast att införa ett författningsreglerat krav på samverkan mellan Säkerhetspolisen och Säkerhets- och integritetsskyddsnämnden.

I 8 § första stycket förvaltningslagen (2017:900) finns det en generell skyldighet för myndigheter att samverka med varandra. En myndighet avgör alltid själv i vilken utsträckning som resurser ska avsätts för att bistå den myndighet som begär assistans. Samverkan enligt bestämmelsen kan ske genom att myndigheter samråder och lämnar varandra upplysningar eller bistår med särskild sakkunskap

genom informella kontakter per telefon eller vid möten.[11] Enligt 6 § andra stycket myndighetsförordningen (2007:515) ska myndigheter under regeringen verka för att genom samarbete med varandra och andra ta till vara de fördelar som kan vinnas för enskilda samt för staten som helhet.

Den generella samverkansskyldigheten mellan olika statliga myndigheter ger förutsättningar för samverkan men lämnar frågan om med vem samverkan ska ske, vad den ska avse och hur omfattande den ska vara till regeringen eller till myndighetens ledning. För att få till stånd den samverkan som vi anser vara nödvändig i de frågor som rör personuppgiftbehandling på detta område krävs att ändamålet anges särskilt.

Vi anser att samverkan ska avse frågor som rör Säkerhetspolisens skyldigheter enligt lag eller annan författning. Det innebär givetvis endast lagar som den särskilda tillsynsmyndigheten utövar tillsyn över. Samverkan avser därmed Säkerhetspolisens skyldigheter som personuppgiftsansvarig. Vidare anser vi att bestämmelsen bör formuleras som en skyldighet och inte en möjlighet. Det finns redan möjligheter till myndighetssamverkan utan särskilt författningsstöd. Eftersom vi uppfattar att samverkan är en viktig del i en effektiv tillsyn anser vi att den bör formuleras som ett krav som riktar sig både till Säkerhetspolisen och den särskilda tillsynsmyndigheten. Slutligen anser vi att det finns skäl att markera att samverkansskyldigheten inte ska avse ett enskilt fall utan ska vara en integrerad del i båda myndigheternas verksamheter. Det bör därför anges att skyldigheten ska avse en löpande samverkan.

En samverkan mellan två utpekade myndigheter under regeringen kan med fördel regleras i respektive myndighetsinstruktion. Säkerhets- och integritetsskyddsnämnden är inrättad genom lag som också anger vilka uppgifter som ingår i nämndens tillsynsuppdrag. Det framstår därför som lämpligt att samverkansskyldigheten också har lagform. Vi bedömer även att samverkan mellan den särskilda tillsynsmyndigheten och Säkerhetspolisen är av sådan vikt att det bör vara ett lagkrav.

[11] Prop. 2016/17:180 s. 293.

Vad innebär samverkan i frågor som rör Säkerhetspolisens skyldigheter?

Det finns risker med att lagstifta om obligatorisk samverkan mellan myndigheter. Samverkan kan komma att bli formalistisk och innehållslös, om en sådan skyldighet anses uppfylld endast genom något som bara i formell mening kan betecknas som samverkan.

Den samverkan som bör ske mellan verksamhetsutövare och tillsynsmyndighet måste sträva efter att lagens syften, i bred mening, ska uppnås. Det innebär att samverkan ska syfta till att skydda enskildas grundläggande fri- och rättigheter genom att säkerställa att Säkerhetspolisen behandlar personuppgifter på ett ändamålsenligt sätt. Lagens dubbla syfte har förstärkts med de förändringar som vi föreslår. Det är möjligt att vidta åtgärder som innebär ett större intrång än tidigare, men endast om det är motiverat av ett tillräckligt starkt verksamhetsskäl. Samverkan ska ske i frågor som handlar om att Säkerhetspolisen uppfyller sina skyldigheter att behandla personuppgifter författningsenligt.

De frågor som ska diskuteras bör vara framåtblickande och inte avse konstaterade förhållanden. Samverkan kan inte ersätta den granskning av regelefterlevnad som nämnden utför. Det är därför viktigt att poängtera att samverkan sker i syfte att de båda myndigheterna ska kunna föra en dialog om övergripande frågor till skillnad från den kommunikation som sker inom ramen för ett tillsynsärende.

Samverkan måste kunna ske på tjänstemannanivå för att vara effektiv. Det innebär att myndigheterna inte avger bindande eller slutliga uppfattningar i frågor. Tanken är snarare att ge möjlighet till perspektivförskjutningar och utbyta erfarenheter och uppfattningar mellan medarbetare vid respektive myndighet. Någon gång kan medarbetare vid myndigheterna tolka nämndens position i en viss fråga på olika sätt och det bör finnas ett forum för att uppmärksamma detta. Vår uppfattning är att det kan gynna en effektiv tillsyn samtidigt som det kan skapa större förutsebarhet för Säkerhetspolisen.

Det är samtidigt viktigt att respektive myndighet bibehåller sin integritet och att samverkan inte kommer i konflikt med en oberoende och opartisk tillsyn. Vi bedömer emellertid inte att riskerna i detta avseende ska överdrivas. Vid domstolar förekommer en relativt omfattande samverkan i förhållande till bland annat parter och

partsombud. Erfarenheterna från sådan samverkan är att de resulterar i att prövningen ofta sker mer effektivt och med en högre kvalitet. Det kan exempelvis handla om att aktörer kommer överens om åtgärder som gynnar en mer koncentrerad process eller att en part förklarar och ger sin syn på en fråga av mer övergripande art. Det förekommer dock, enligt vår erfarenhet, sällan att någon av parterna som ofta företräder helt motsatta intressen uppfattar att deras inbördes förhållande eller professionella distans rubbats genom sådan samverkan.

Vad kan samverkan utmynna i?

Integritetsskyddsmyndigheten har stora möjligheter att agera genom olika tillsynsbefogenheter. Myndigheten kan exempelvis lämna ett råd eller anvisning. Därefter kan myndigheten utfärda en varning och slutligen ett föreläggande att inom viss tid åtgärda en brist. Om detta inte hjälper, kan tillsynsmyndigheten besluta om ett förbud mot fortsatt behandling. Samverkan eller samråd med Integritetsskyddsmyndigheten kan därför avslutas genom ett beslut. För nämnden finns endast möjlighet att uttala sig om konstaterade förhållanden. Det innebär att samverkan med nämnden kan komma att bli mer informell än med tillsynsmyndigheten. Det finns inte förutsättningar att vare sig rättsligt eller slutligt avgöra frågor där samverkan skett. Däremot kommer det finnas goda möjligheter att i dialog mellan myndigheterna komma fram till rimliga slutsatser om vilka skyldigheter som åvilar Säkerhetspolisen i olika avseenden.

Under utredningen har frågan lyfts om det borde vara möjligt att eskalera frågor från samverkan på tjänstemannanivå, till ett formellt förhandsavgörande av nämnden. Detta trots att frågan inte rör konstaterade förhållanden, utan en abstrakt och hypotetisk fråga. Det skulle antingen kunna handla om att en viss oenighet kunnat konstateras under samverkan eller att en fråga inte har något klart svar eller är öppen för tolkning. Vi har därför övervägt om det bör införas en möjlighet för Säkerhetspolisen att lyfta en fråga till nämnden för ett formellt förhandsbesked.

Vi har sett tydliga fördelar med en sådan ordning. Det skulle sannolikt kunna leda till ett effektivare genomslag av lagstiftningen och underlätta en omprövning av tidigare ställningstaganden vid

förändrade förhållanden (till exempel ny teknisk utveckling). Men det finns också nackdelar med att införa en sådan prövning. Det finns farhågor kring bland annat vilket värde ett sådant förhandsbesked skulle ha i praktiken och hur det skulle påverka nämndens roll i tillsynsprocessen. Vi har dragit slutsatsen att nackdelarna i dagsläget överväger fördelarna. Om en sådan möjlighet ska införas, bör frågan i stället utredas i särskild ordning. I så fall lämpligen när lagstiftningen varit i kraft en tid.

Sekretess hindrar inte samverkan

Samverkan utgör en del av Säkerhets- och integritetsskyddsnämndens tillsyn över säpodatalagen. I 42 kap. 5–8 §§ offentlighets- och sekretesslagen regleras den sekretess som gäller nämndens tillsynsverksamhet. Om nämnden i sint tillsynsverksamhet får en sekretessreglerad uppgift från en myndighet, blir sekretessbestämmelsen tillämplig på uppgiften även hos nämnden. Uppgifter som nämnden får del av inom ramen för samverkan kommer därför att omfattas av samma sekretess hos nämnden som hos Säkerhetspolisen.

10.6 Förebyggande befogenheter och förhandssamråd

Förslag: De nuvarande bestämmelserna om tillsynsmyndighetens förebyggande befogenheter ska överföras till den nya lagen.

Den nuvarande ordningen med konsekvensbedömning och förhandsamråd mellan Säkerhetspolisen och tillsynsmyndigheten bör överföras till den nya lagen.

10.6.1 Integritetsskyddsmyndigheten bör ha samma förebyggande befogenheter som i dag

Om tillsynsmyndigheten bedömer att det finns risk för att personuppgifter kan komma att behandlas i strid med författning, ska myndigheten genom råd, rekommendationer eller påpekanden försöka förmå Säkerhetspolisen eller personuppgiftsbiträdet att vidta åtgärder för att motverka risken Detta följer av de förebyggande befogenheterna i 7 kap. 4 § första stycket säpodatalagen.

Bestämmelsen innebär en skyldighet för tillsynsmyndigheten att agera förebyggande då en risk upptäckts. Medlen för det är i första hand muntliga eller skriftliga råd, rekommendationer och påpekanden som inte är tvingande. Det kan vara tillräckligt att tillsynsmyndigheten upplyser om på vilket sätt personuppgiftsbehandling riskerar att strida mot regelverket. På vilket sätt en förändring ska åstadkommas är en fråga för den personuppgiftsansvarige. Tillsynsmyndigheten är skyldig att lämna skriftliga råd vid förhandssamråd. De förebyggande befogenheterna ska som regel prövas före tillsynsmyndigheten tillämpar kraftfullare påtryckningsmedel.

Tillsynsmyndigheten ges i 7 kap. 4 § andra stycket, en möjlighet att utfärda en skriftlig varning om en planerad behandling riskerar att stå i strid med lag eller annan författning. En varning är avsedd att i ett enskilt fall markera allvaret i en situation och försöka förmå den personuppgiftsansvarige att ändra sig i fråga om planerad behandling. En varning som utfärdas inför en planerad behandling kan ses som ett förhandsbesked i hur behandlingen kan komma att bedömas när den genomförs. När en varning utfärdas angående en pågående behandling innebär det närmast ett besked om att myndigheten kommer att utfärda ett föreläggande eller förbud om det inte sker en frivillig rättelse. En varning kan aktualiseras om rådgivning eller påpekanden inte ger resultat men den behöver inte ha föregåtts av sådana mjukare styrmedel. En varning får dock anses vara en mer kvalificerad åtgärd än de som omnämns i paragrafens första stycke och kan ses som ett steg på vägen mot tillämpning av korrigerande befogenheter. En varning är inte möjlig att överklaga.[12]

Nuvarande 7 kap. 4 § säpodatalagen ger viktiga verktyg för tillsynsmyndigheten när den ska utföra sitt uppdrag enligt 7 kap. 1 §. Det är viktigt att förtydliga att tillsynsmyndighetens roll i att förebygga att fel begås ska ha företräde framför rollen att besluta om bindande åtgärder. Att tillsynsmyndigheten tillämpar korrigerande befogenheter ska vara förbehållet de fall då Säkerhetspolisen inte frivilligt rättar sig efter råd, anvisningar eller uttalanden. Det behövs därför en särskild bestämmelse om att tillsynsmyndigheten ska vara skyldig att använda sig av förebyggande tillsynsbefogenheter, om det finns en risk för att personuppgifter kan komma att behandlas lagstridigt.

[12] Prop. 2018/19:163 s. 255 och prop. 2017/18:232 s. 294 f.

Det har inte framkommit några skäl till att ändra den nuvarande bestämmelsen, som därför bör överföras till den nya lagen.

10.6.2 Fortsatt konsekvensbedömning och förhandssamråd

Finns det skäl att ändra nuvarande ordning?

I nuvarande säpodatalag finns, i 5 kap. 6 §, en skyldighet för Säkerhetspolisen att göra en bedömning av de risker som är förenade med att en ny typ av behandling, eller betydande förändringar av redan pågående behandling, genomförs. En sådan konsekvensbedömning ska ske innan behandlingen utförs eller förändringar genomförs. Skyldigheten att genomföra en sådan konsekvensbedömning fanns inte tidigare utan infördes i och med brottsdatalagen och är gemensam för alla brottsbekämpande myndigheter. Regeringen ansåg då att konsekvensbedömning fyller en viktig funktion ur ett integritetsperspektiv.[13]

Enligt 5 kap. 6 § andra stycket säpodatalagen ska Säkerhetspolisen samråda med Integritetsskyddsmyndigheten, om konsekvensbedömningen visar att det finns särskild risk för intrång i registrerades personliga integritet eller om typen av behandling innebär särskild risk för intrång (förhandssamråd). Enligt 4 kap. 8 § säpodataförordningen ska riskerna med införande av ny teknik, nya rutiner eller nya förfaranden särskilt beaktas.

Regler om förhandssamråd fanns redan under polisdatalagens tid men gällde då främst utveckling eller inköp av nya it-system.[14] Då skulle samråd ofta ske parallellt med tillsynsmyndigheten och med Säkerhets- och integritetsskyddsnämnden. När säpodatalagen beslutades ifrågasattes denna ordning, eftersom det dubbla samrådsförfarandet riskerade resultera i motstridiga uppfattningar mellan de båda tillsynsmyndigheterna.[15] Därför ersattes det parallella samrådet med att Säkerhets- och integritetsskyddsnämnden ska ges tillfälle att yttra sig om det är lämpligt (6 kap. 2 § säpodataförordningen).

I avsnitt 10.2 har vi redogjort för vår uppfattning om att den parallella tillsynen, både genom Integritetsskyddsmyndigheten och

[13] Prop. 2018/19:163 s. 141.
[14] Se 2 § polisdataförordningen (2010:1155).
[15] Prop. 2018/19:163 s. 173.

Säkerhets- och integritetsskyddsnämnden, bör kvarstå. Där framgår att vår uppfattning är att det finns flera skäl som talar för att behålla Integritetsskyddsmyndighetens tillsyn; bland annat att myndigheten har en nationell och internationell överblick och är av en sådan storlek att flera kompetenser kan samlas där. Förhandssamrådet är främst avsett att ge tillsynsmyndigheten en möjlighet att lämna råd innan nya tekniska system köps in eller utvecklas. Många gånger används samma tekniska system inom flera myndigheter eller av andra, motsvarande, myndigheter inom EU. I dessa fall kan Integritetsskyddsmyndighetens överblick och möjlighet att dra lärdom av andra tillsynsmyndigheters arbete vara mycket värdefullt.

Vår uppfattning är att Säkerhetspolisen befinner sig mitt i ett tekniksprång när det gäller att hantera information. Helt ny teknik innebär ofta en osäkerhet i förhållande till existerande regelverk och begreppsapparater. Exempelvis kan de behandlingsåtgärder som är möjliga att vidta med hjälp av maskininlärning och artificiell intelligens vara svåra att jämföra med regler anpassade efter existerande teknik. Just sådan osäkerhet kan förhindra, försvåra eller fördröja nödvändiga investeringar i ny teknik och utveckling eller implementering av nya metoder att hantera information. Det är därför viktigt att det ska vara möjligt att få författningsenligheten prövad genom förhandssamråd innan behandling påbörjas eller betydande förändringar genomförs.

Vi anser sammanfattningsvis att de nuvarande reglerna om en skyldighet att genomföra en konsekvensbedömning och samråda med tillsynsmyndigheten bör kvarstå. Reglerna har inte framhållits som problematiska av någon av myndigheterna. Säkerhetspolisen har sällan tillämpat reglerna om förhandssamråd. Det kan dock sannolikt komma att ändras eftersom vi uppfattar att samhället och med det även Säkerhetspolisen står inför ett potentiellt mycket stort teknikskifte. Maskininlärningstekniker har nått ett stadium då de kan appliceras operativt i större omfattning än förut. Det framstår därför som naturligt att samordna prövningen av nya typer av behandlingar eller betydande förändringar av redan pågående behandlingar, under samma myndighet som prövar motsvarande frågor enligt dataskyddsförordningen och brottsdatadirektivet. En sådan samordning innebär förstås inte att utfallet måste bli detsamma för Säkerhetspolisen som för andra myndigheter som omfattas av EU-rätten.

Likt i dag bör Säkerhets- och integritetsskyddsnämnden informeras om och ha möjlighet att yttra sig under samrådet om det behövs. Rätten att få tillgång till underlaget för förhandssamrådet och tillsynsmyndighetens yttrande bör också vara oförändrad.

Våra ställningstaganden innebär att nuvarande regler bör föras över till den nya lagen.

Relation mellan förhandssamråd och samverkansskyldighet

Vi har i föregående avsnitt lämnat förslag om att Säkerhetspolisen och Säkerhets- och integritetsskyddsnämnden ska samverka i frågor som rör Säkerhetspolisens skyldigheter som personuppgiftsansvarig. Det innebär att frågor som rör exempelvis nya behandlingsåtgärder kan vara föremål för både samverkan med nämnden och samråd med tillsynsmyndigheten. Det som i tidigare förarbeten lyfts angående risken för olika budskap från de båda tillsynsmyndigheterna kan därför komma att återaktualiseras trots att förhandssamråd endast ska ske med Integritetsskyddsmyndigheten.

Denna risk ska emellertid inte överdrivas. Vi anser snarare att den löpande samverkan som vi föreslår mellan Säkerhetspolisen och Säkerhets- och integritetsskyddsnämnden kan vara till fördel i detta sammanhang. Exempelvis kan samverkan ske redan i frågan om samrådsskyldighet med Integritetsskyddsmyndigheten föreligger. Om förhandssamrådet föregåtts av löpande samverkan mellan Säkerhets- och integritetsskyddsnämnden och Säkerhetspolisen, bör förutsättningarna vara goda för att eventuella oklarheter redan klarats ut. Under ett förhandssamråd förväntas exempelvis Säkerhetspolisen kunna presentera en teknisk lösning för Integritetsskyddsmyndigheten att ta ställning till.[16] Om Säkerhets- och integritetsskyddsnämnden genom mer informell samverkan kan ge sitt perspektiv på valet av teknisk lösning, bör integritets- och tillsynsfrågor kunna lyftas redan innan ett förslag presenteras för Integritetsskyddsmyndigheten. Det förhållandet att ett förhandssamråd föregåtts av viss samverkan mellan Säkerhetspolisen och Säkerhets- och integritetsskyddsnämnden kan sannolikt också bidra till att ett eventuellt yttrande från nämnden kan ske snabbare.

[16] Ibid. s. 141.

10.7 Korrigerande befogenheter

10.7.1 Integritetsskyddsmyndighetens befogenheter bör kvarstå

Förslag: Det finns inte skäl att göra någon ändring i vilka korrigerande befogenheter som tillsynsmyndigheten har enligt nuvarande lagstiftning. Tillsynsmyndighetens befogenheter att besluta om förelägganden eller förbud ska därför överföras till den nya lagen.

Säkerhetspolisens personuppgiftsbehandling har sedan 1970-talet stått under tillsyn av Datainspektionen, som numera heter Integritetsskyddsmyndigheten. Tillsynsmyndigheten har samma korrigerande befogenheter i förhållande till Säkerhetspolisen som till andra brottsbekämpande myndigheter, frånsett möjligheten att ge sanktionsavgift. Att den generella tillsynsmyndigheten har sådana befogenheter även avseende personuppgiftsbehandling som rör nationell säkerhet är ovanligt. Inom EU är det endast Finland, Österrike, Slovenien, Cypern och Sverige som har denna ordning.[17]

Om tillsynsmyndigheten konstaterar att Säkerhetspolisen eller ett personuppgiftsbiträde behandlar personuppgifter i strid med lag eller annan författning, får den utfärda föreläggande om att vidta åtgärder eller förbjuda fortsatt behandling om bristen är allvarlig (7 kap. 5 § säpodatalagen).

Förelägganden kan avse exempelvis rättelse, radering och begränsning av behandlingen. Tillsynsmyndigheten får även utfärda bindande förelägganden som tar sikte på att Säkerhetspolisen ska uppfylla andra skyldigheter, som att införa bättre säkerhetslösningar, fullgöra dokumentationsskyldighet eller att överlämna viss dokumentation. Motsvarande möjlighet för tillsynsmyndigheten finns även i brottsdatalagen.

Med förbud mot fortsatt behandling avses att någon behandling inte längre får förekomma. Förbud mot fortsatt behandling aktualiseras om Säkerhetspolisen på ett allvarligt sätt har åsidosatt sina skyldigheter och bristerna är sådana att de inte kan åtgärdas på annat sätt än att behandlingen upphör. Personuppgifter får dock

[17] EU:s människorättsbyrå (FRA), *Surveillance by intelligence Services: Fundamental rights safeguards and remedies in the EU – 2023 update*, s. 24 ff.

alltid behandlas för arkivändamål, om ett förbud annars skulle stå i strid med 2 kap. tryckfrihetsförordningen.[18]

Tillsynsmyndigheten har därmed stora möjligheter att få till stånd en korrekt och författningsenlig behandling genom bindande förelägganden eller förbud. Integritetsskyddsmyndigheten har, såvitt känt, inte tillämpat sina befogenheter i förhållande till Säkerhetspolisen.

Säkerhets- och integritetsskyddsnämnden har inte några korrigerande befogenheter att tillgå när det gäller säpodatalagen. Nämnden har i förhållande till Säkerhetspolisen endast möjlighet att uttala sig om konstaterade förhållanden. Nämnden har dock även, enligt 20 § förordning (2007:1141) med instruktion för Säkerhets- och integritetsskyddsnämnden, en skyldighet att i vissa fall föra vidare sina iakttagelser till tillsynsmyndigheten. I paragrafen anges bland annat att om nämnden bedömer att Säkerhetspolisen brister i sina skyldigheter vid behandling av personuppgifter på ett sådant sätt att korrigerande befogenheter kan aktualiseras, ska nämnden anmäla det till Integritetsskyddsmyndigheten. När anmälan har gjorts ska nämnden ge myndigheten det biträde som behövs. Integritetsskyddsmyndigheten har även rätt att ta del av nämndens underlag i den utsträckning som det behövs.

Vi bedömer att nuvarande ordning är tillfredsställande och föreslår att den överförs till den nya lagen.

10.7.2 Beslut om förelägganden eller förbud ska överklagas till Försvarsunderrättelsedomstolen

Förslag: Tillsynsmyndighetens beslut om föreläggande eller förbud mot fortsatt behandling ska kunna överklagas till Försvarsunderrättelsedomstolen. Domstolens avgörande ska inte få överklagas.

[18] Prop. 2018/19:163 s. 177 f.

Beslut som rör kvalificerat hemliga uppgifter kan komma att prövas av fem olika instanser

Enligt 8 kap. 3 § säpodatalagen får tillsynsmyndighetens tillsynsbeslut överklagas till allmän förvaltningsdomstol. Det är Säkerhets- och integritetsskyddsnämnden som utför den specialiserade och löpande tillsynen över Säkerhetspolisens personuppgiftsbehandling. Ett tillsynsbeslut från Integritetsskyddsmyndigheten får därför antas i de allra flesta fall ske efter en anmälan från Säkerhets- och integritetsskyddsnämnden. Redan innan ett beslut överklagas har därmed två, av varandra oberoende, förvaltningsmyndigheter uttalat sig i frågan. Därefter finns möjligheter till en, i praktiken, treinstansprövning i allmän förvaltningsdomstol med Förvaltningsrätten i Stockholm som första domstolsinstans.

Frågan har väckts om den nuvarande ordningen är den mest lämpliga. Även om det historiskt varit mycket ovanligt att tillsynsbeslut aktualiserats, och än mindre att ett sådant beslut överklagas, finns det risker med det nuvarande systemet. Om en situation uppkommer där Integritetsskyddsmyndigheten fattar ett tillsynsbeslut som därefter överklagas av Säkerhetspolisen får det antas röra en fråga av särskild vikt. Tillsynsmyndigheten ska endast fatta korrigerande beslut efter att andra möjligheter uttömts. Säkerhetspolisen måste också göra flera svåra överväganden innan ett beslut överklagas, exempelvis om det som finns att vinna med att överklaga ett beslut överväger riskerna att myndighetens förmåga avslöjas. Det skulle exempelvis kunna röra information som är mycket angelägen för Säkerhetspolisen att få behandla och där myndigheten inte delar tillsynsmyndighetens slutsatser om författningsenlighet. Ett annat exempel är ett föreläggande som kan leda till en betydande förmågesänkning. De uppgifter som behöver presenteras för att överpröva ett sådant tillsynsbeslut kommer på en aggregerad nivå sannolikt att nå upp till nivån *hemlig* eller *kvalificerat hemlig* enligt säkerhetsskyddslagen (2018:585).

Säkerhetsskyddslagstiftningen kommer därmed att aktualiseras på ett sätt som kan vara krävande för en vanlig domstol. Med hänsyn till den förmodat höga tröskeln för att Säkerhetspolisen över huvud taget skulle föra en fråga till domstol, är det sannolikt att beslutet kan komma under prövning i vart fall i ytterligare en instans. De domstolar som potentiellt ska hantera uppgifter av det

aktuella slaget behöver ha ett väl utvecklat säkerhetsskydd. Oavsett hur väl tilltaget säkerhetsskyddet är, finns det dock alltid ett mervärde ur ett säkerhetsperspektiv i att begränsa antalet personer som får tillgång till uppgifter om Säkerhetspolisens verksamhet.

Mot bakgrund av känsligheten i de uppgifter som kan tänkas behöva avhandlas vid ett överklagande kan den nuvarande ordningen väcka vissa betänkligheter.

Prövningen av tillsynsbeslut bör begränsas till färre insatser

Det är något motsägelsefullt att uppgifter som kan vara mycket känsliga och som exempelvis kan utnyttjas för att kartlägga Säkerhetspolisens förmågor inom underrättelseverksamheten, kan komma att prövas i den nuvarande omfattningen med hänsyn till de tillkommande risker som detta innebär.

Som nämnts är det över huvud taget ovanligt att en generell tillsynsmyndighet som Integritetsskyddsmyndigheten har så vittgående befogenheter att begränsa hur personuppgifter får behandlas för ändamål som rör nationell säkerhet. Redan på grund av att konsekvenserna av ett felaktigt tillsynsbeslut kan påverka den nationella säkerheten, finns starka skäl för att, som i dag, tillåta en rättslig överprövning och förhindra omedelbar verkställighet.

Vi anser att antalet instanser bör begränsas av informationssäkerhetsskäl. Till att börja med kan konstateras att enskilda inte kan klaga på Integritetsskyddsmyndighetens beslut, som endast riktar sig mot Säkerhetspolisen. Rättssäkerhetskraven på beslut som rör myndigheters mellanhavanden bör inte anses vara lika uttalade som när en enskild överklagar.

Integritetsskyddsmyndigheten fattar beslut efter att ha inhämtat yttrande från Säkerhetspolisen. Underlaget kan också vara en motiverad anmälan från Säkerhets- och integritetsskyddsnämnden. En sådan anmälan bygger i sin tur på nämndens ställningstagande om att viss behandling inte är författningsenlig; ett uttalande som givetvis föregåtts av kommunikation med Säkerhetspolisen. Eftersom ärendet redan är kommunicerat och i sak utrett, ofta av två myndigheter, framstår det inte som nödvändigt att beslutet ska överprövas av en underrätt. Vår uppfattning är att ett beslut om

föreläggande eller förbud bör överprövas direkt av överrätt eller en specialdomstol.

Försvarsunderrättelsedomstolen bör vara exklusivt behörig att pröva överklagade tillsynsbeslut

Tillsynsbeslut bör överklagas till Försvarsunderrättelsedomstolen

Om ett överklagat tillsynsbeslut ska överprövas av allmän förvaltningsdomstol, ligger det närmast till hands att utse Kammarrätten i Stockholm till exklusivt forum. Kammarrätten har beredskap för att hantera säkerhetsskyddsklassificerad information och har förutsättningar att uppfylla säkerhetsskyddslagstiftningens krav. Genom rättens sammansättning finns förutsättningar till att överklagade frågor får en allsidig belysning och ge rättslig vägledning. Frågan är om det finns något alternativ till en prövning i kammarrätten.

Vi föreslår i detta betänkande att Försvarsunderrättelsedomstolen ska pröva vissa andra frågor som berör Säkerhetspolisens personuppgiftsbehandling. Försvarsunderrättelsedomstolen utgör en specialdomstol inom underrättelseområdet som prövar förvaltningsrättsliga frågor. Försvarsunderrättelsedomstolen kommer därför att ha särskilda insikter inom Säkerhetspolisens verksamhetsområde och vara välorienterad i de olika avvägningar som måste göras där.

Ingen allmän domstol kommer att kunna mäta sig med det fysiska säkerhetsskydd som Försvarsunderrättelsedomstolen redan har. Den instans som ska pröva dessa frågor måste av nödvändighet omgärdas av ett sådant skydd. Försvarsunderrättelsedomstolen förfogar exempelvis över en helt avlyssningssäker förhandlingssal och har även på andra sätt det säkerhetsskydd som krävs för att hantera kvalificerat hemlig information. Vi anser att informationssäkerhetsriskerna i samband med att en tillsynsfråga överklagas minskar betydligt genom att saken prövas av domare som uteslutande handlägger frågor som rör säkerhetsskyddsklassificerade uppgifter, där kompetensen inom informationssäkerhet är på högsta nivå. Försvarsunderrättelsedomstolens särskilda sammansättningsregler och de kvalifikationskrav som gäller för ledamöterna borgar också för att frågor kan få en allsidig belysning. Det möjliggör en

långsiktig praxisbildning som tar hänsyn till de intressen som vårt förslag till säpodatalag avser att tillgodose.

Vi anser sammantaget som att det framstår som lämpligt ur flera avseenden att Försvarsunderrättelsedomstolen tillförs även denna uppgift. Med hänsyn till hur ovanligt det kan förmodas vara att Integritetsskyddsmyndigheten fattar ett tillsynsbeslut tillgodoses möjligheten till en säker överprövning dessutom utan nämnvärda tillkommande kostnader.

Försvarsunderrättelsedomstolens avgörande av tillsynsfrågor bör inte få överklagas

Som tidigare nämnts kommer den första domstol som överprövar Integritetsskyddsmyndighetens föreläggande eller beslut om förbud ofta ha en utredning där både Integritetsskyddsmyndigheten och Säkerhets- och integritetsskyddsnämnden tagit ställning i sak. Vi uppfattar att det ur ett rättssäkerhetsperspektiv då är tillräckligt med en överprövning i en instans. Det kan övervägas om Försvarsunderrättelsedomstolens avgöranden bör kunna överklagas till kammarrätten eller Högsta förvaltningsdomstolen. Vår uppfattning är att en sådan möjlighet inte är nödvändig. Övriga frågor som prövas av Försvarsunderrättelsedomstolen får inte överklagas. Det saknas bärande skäl för att undanta de nu aktuella besluten från denna princip. Vårt förslag innebär att Försvarsunderrättelsedomstolen endast kan överpröva två former av beslut meddelade av Integritetsskyddsmyndigheten med stöd av säpodatalagen: förelägganden och förbud. Den praxis som en överinstans skulle bidra med skulle därför endast träffa ett mycket smalt rättsområde. De fördelar som kan vinnas med en möjlighet till överklagande, som en förhöjd rättssäkerhet och mer kvalitativ rättsbildning, anser vi inte uppväga de olägenheter ur informationssäkerhetssynpunkt som är förenade med en sådan möjlighet.

10.7.3 Säkerhets- och integritetsskyddsnämnden ska ges korrigerande befogenhet avseende personuppgifter som tagits fram ur en särskild uppgiftssamling

Förslag: Den särskilda tillsynsmyndigheten Säkerhets- och integritetsskyddsnämnden ska kunna besluta om radering av uppgifter som tagits fram från en särskild uppgiftssamling utan att framtagningen är förenligt med ett tillstånd.

Bedömning: Integritetsskyddsmyndigheten ska ha samma förebyggande och korrigerande befogenheter för behandling av personuppgifter i särskilda uppgiftssamlingar som enligt säpodatalagen.

Vilka befogenheter bör Integritetsskyddsmyndigheten ha vid tillsyn över behandling i särskilda uppgiftssamlingar?

I avsnitt 9.8 beskrivs det tillståndsförfarande som omgärdar framtagning av uppgifter ur särskilda uppgiftssamlingar. Det kommer av naturliga skäl att främst vara Säkerhets- och integritetsskyddsnämnden som ansvarar för tillsynen över personuppgiftsbehandling i de särskilda uppgiftssamlingarna. Vi har, i avsnitt 10.4.6, föreslagit att tillsynsmyndigheterna ska få nya undersökningsbefogenheter genom en möjlighet att ansöka om tillstånd till framtagning för tillsynsändamål. Nämnden kommer även att yttra sig i tillståndsprocessen. Tillstånd till framtagning kan innehålla särskilda villkor för att underlätta tillsyn. Genom att vara delaktig i tillståndsprocessen kommer nämnden löpande hållas underrättad om de tillstånd som är aktuella och kunna påverka deras innehåll.

Integritetsskyddsmyndigheten får förutsättas utöva en mindre verksamhetsnära tillsyn över den behandling som sker i särskilda uppgiftssamlingar. Frågan är om det finns skäl att frånta tillsynsmyndigheten några befogenheter då den utövar tillsyn över behandling i särskilda uppgiftssamlingar?

Säpodatalagen och lagen om särskilda uppgiftssamlingar är nära sammanflätade. Uppgifter som tagits fram med stöd av tillstånd ska behandlas enligt säpodatalagen. Uppgifter som behandlas enligt säpodatalagen kommer att kunna överföras till behandling i särskilda

uppgiftssamlingar. Att Integritetsskyddsmyndigheten har generella tillsynsbefogenheter över all personuppgiftsbehandling, oavsett vilken lagstiftning som den grundas på, har vi tidigare framhållit som en styrka och ett av skälen till att den parallella tillsynen bör bestå. Vi anser därför att det är viktigt att det inte riskerar att uppstå några glapp i fråga om tillsynsmyndighetens befogenheter. Integritetsskyddsmyndigheten bör därför så långt det är möjligt ha samma tillsynsbefogenheter för behandling som sker enligt den föreslagna lagen om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar.

Vi anser därför att det inte finns några skäl att frånta Integritetsskyddsmyndigheten de förebyggande eller korrigerande befogenheter som följer av säpodatalagen avseende behandling som sker med stöd av lagen om särskilda uppgiftssamlingar. På motsvarande sätt som tillsynen över säpodatalagen kommer Säkerhets- och integritetsskyddsnämnden att ansvara för den löpande tillsynen. Korrigerande befogenheter kommer därför ofta att aktualiseras först efter en anmälan från nämnden.

Vi föreslår således att de tillsynsbefogenheter som tillsynsmyndigheterna har ska gälla även enligt lagen om särskilda uppgiftssamlingar (som framgått med undantag för rätten att utan domstolstillstånd ta del av uppgifterna i samlingarna).

Säkerhets- och integritetsskyddsnämnden bör ges korrigerande befogenhet avseende uppgifter som tagits fram utan tillstånd

Vi har återkommande gjort jämförelsen mellan den behandling av personuppgifter som kan ske i särskilda uppgiftssamlingar med FRA:s behandling av personuppgifter genom signalspaning. Bedömningen är att intrånget är likartat och att motsvarande rättssäkerhetsmekanismer därför krävs för att uppnå ett fullgott skydd mot kränkning av enskildas fri- och rättigheter genom behandlingen. Det främsta medlet för att uppnå detta skydd är, som framgår av avsnitt 9.5.4, det nya tillståndsförfarande som vi föreslår.

Tillstånd är en förutsättning för FRA:s signalspaning. Därutöver utövar Statens inspektion för försvarsunderrättelseverksamheten särskild tillsyn över verksamheten. I likhet med vad som gäller för Säkerhetspolisen utövar Integritetsskyddsmyndigheten generellt tillsyn över personuppgiftsbehandlingen vid sidan av den särskilda

tillsynsmyndigheten. Integritetsskyddsmyndigheten kan förelägga FRA eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller för att fullgöra andra skyldigheter.[19] Ett sådant föreläggande kan innebära att uppgifter begränsas eller förstörs.

Vid sidan av Integritetsskyddsmyndighetens befogenheter har Statens inspektion för försvarsunderrättelseverksamheten en möjlighet till korrigerande beslut. Myndigheten får nämligen besluta att viss inhämtning ska upphöra eller att upptagning eller uppteckning av inhämtade uppgifter ska förstöras, om det vid kontroll framkommer att inhämtningen inte är förenlig med tillstånd.[20] Det innebär att kontrollmyndigheten omedelbart kan föranstalta om radering av personuppgifter som inhämtats genom signalspaning, men som antingen saknar tillstånd eller där inhämtningen inte varit förenlig med det tillstånd som meddelats. Ett sådant beslut är inte överklagbart och ska därför verkställas när Statens inspektion för försvarsunderrättelseverksamheten så bestämmer.

Skälen bakom denna starka sanktionsmöjlighet var att regeringen ansåg att möjligheten skulle innebära ett förstärkt skydd för enskilda. Detta trots att regeringen ansåg det självklart att signalspaningsmyndigheten ska rätta sig efter de anvisningar som Statens inspektion för försvarsunderrättelseverksamheten kan besluta om, som inte är bindande i formell mening.[21]

Det finns inte några utförliga motiv till den särskilda tillsynsmyndighetens befogenheter att besluta om upphörande och radering. Konsekvensen av denna befogenhet får dock förmodas vara att den i någon mån utjämnar styrkeförhållandena mellan tillsynen och Försvarets radioanstalt. Befogenheten anvisar också vilken av de två myndigheterna som har tolkningsföreträde i den särskilda fråga som kan föranleda åtgärden. Försvarets radioanstalt ska givetvis ges möjlighet att ge sin syn på om inhämtning varit förenligt med tillstånd, vilket kan tänkas vara en tolkningsfråga. Ett beslut förutsätter att myndigheten inte självmant vidtagit rättelse.

Mot bakgrund av vår bedömning avseende likheterna mellan Försvarets radioanstalts signalspaning och behandlingen av personuppgifter i särskilda uppgiftssamlingar finns det anledning att över-

[19] 6 kap. 5 § FRA-datalagen.
[20] 10 § andra stycket lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.
[21] Prop. 2006/07:63 s. 117 f.

väga om motsvarande korrigerande befogenhet ska införas för den särskilda tillsynsmyndigheten.

Vår uppfattning är att Säkerhets- och integritetsskyddsnämnden kommer ha ett större inflytande över de tillstånd som meddelas och en större insikt i domstolens skäl, genom att myndigheten normalt ska yttra sig och närvara vid förhandlingen. Det talar för att de eventuella brister i tillämpningen som nämnden uppmärksammat kan komma till domstolens kännedom och föranleda justering i de tillstånd som meddelas. Möjligheten att föreskriva särskilda villkor för att underlätta tillsyn kan även komma att underlätta nämndens tillsyn på olika sätt. Detta talar mot att nämnden behöver ytterligare befogenheter.

Samtidigt finns det ett krav på omfattande säkerhetsåtgärder när det gäller behandling som sker som ett undantag i förhållande till de principer som i övrigt gäller. Redan av det skälet finns anledning att förstärka tillsynen över personuppgiftsbehandlingen i särskilda uppgiftssamlingar. Frågan om en framtagning varit förenlig med ett meddelat tillstånd är typiskt sett svår för Integritetsskyddsmyndigheten att ta ställning till. Myndigheten har inte närvarat vid förhandlingen och är inte heller insatt i domstolens praxis på samma sätt som Säkerhetspolisen och Säkerhets- och integritetsskyddsnämnden. En anmälan till Integritetsskyddsmyndigheten om behov av korrigerande befogenheter är vidare en process som får antas ske med viss tidsutdräkt. Om en framtagning skett i strid med meddelat tillstånd, kan uppgifterna innan Integritetsskyddsmyndigheten utfärdat ett föreläggande eller förbud hunnit föranleda åtgärder eller spridas utanför Säkerhetspolisen.

Vi anser därför att det finns skäl att förstärka Säkerhets- och integritetsskyddsnämndens tillsyn genom motsvarande befogenhet som Statens inspektion för försvarsunderrättelseverksamheten har enligt 10 § andra stycket lagen (2008:717) om signalspaning i underrättelseverksamhet.

Den korrigerande befogenheten bör formuleras som en möjlighet för nämnden att besluta att framtagna uppgifter ska förstöras, om det framgår att framtagningen inte varit förenlig med tillstånd. Det omfattar även uppgifter som tagits fram från en särskild uppgiftssamling helt utan tillstånd. Säkerhets- och integritetsskyddsnämndens bedömning bör endast avse om Säkerhetspolisens framtagning varit förenlig med det tillstånd som meddelats. Riktigheten

av domstolens avgörande som sådant ligger således utanför tillsynen.

Statens inspektion för försvarsunderrättelseverksamhetens motsvarande beslut kan inte överklagas. Det finns goda skäl för att även ett raderingsbeslut fattat av Säkerhets- och integritetsskyddsnämnden ska gälla omedelbart. Besluten är av sådan karaktär att omedelbar verkställighet är önskvärd, eftersom det avser en kränkning av enskildas rättigheter. Nämnden har en domstolsliknande sammansättning med en stark parlamentarisk koppling och det är inte heller uppenbart vart ett beslut fattat i sådan ordning skulle överklagas. Nämndens beslut kan inte heller i andra fall överklagas. Om Säkerhetspolisen inte håller med om nämndens bedömning, finns vidare goda möjligheter att föra frågan till domstolen genom en ny ansökan.

10.7.4 Kontroll på begäran av enskild

Förslag: Säkerhets- och integritetsskyddsnämnden ska inte vara skyldig att på begäran av en enskild kontrollera om han eller hon varit föremål för personuppgiftsbehandling i en särskild uppgiftssamling.

Av 3 § lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet följer en skyldighet för Säkerhets- och integritetsskyddsnämnden att på begäran av enskild bland annat kontrollera om han eller hon varit föremål för personuppgiftsbehandling enligt säpodatalagen och om denna behandling i så fall varit författningsenlig. Denna kontrollmöjlighet för enskilda brukar betecknas som indirekt insyn, eftersom den enskilda i normalfallet inte får reda på annat än att kontrollen utförts. Redan informationen om huruvida en persons personuppgifter förekommer eller inte omfattas regelmässigt av sekretess.

Det har inte varit en del av denna utrednings uppdrag att göra någon särskild översyn över lagen om tillsyn över viss brottsbekämpande verksamhet. Vi har därför inte funnit skäl att närmare utreda utformningen av det nuvarande regelverket. Vi kan däremot konstatera att en stor mängd kontroller utförs och att rätten till indirekt insyn är väsentlig för att uppnå en tillräcklig skyddsnivå

enligt Europadomstolens praxis. Frågan är om denna rätt ska utsträckas även till vårt förslag om behandling av personuppgifter i särskilda uppgiftssamlingar.

Det är inte möjligt att i dagsläget bedöma hur vår föreslagna lagstiftning kommer att tillämpas och hur många personuppgifter som kommer förekomma i särskilda uppgiftssamlingar. Det är dock högst troligt att antalet personuppgifter som förekommer i särskilda uppgiftssamlingar, inom en snar framtid, kommer att vara större än de personuppgifter som behandlas med stöd av säpodatalagen. Vi har ansett detta acceptabelt eftersom tillgången till uppgifterna är strikt begränsad. Fri- och rättighetsintrånget av att vara registrerad i en särskild uppgiftssamling har vi mot denna bakgrund bedömt som relativt lågt. Redan av dessa skäl kan ifrågasättas om det finns ett behov av indirekt insyn avseende de särskilda uppgiftssamlingarna.

Att de uppgifter som endast behandlas i en särskild uppgiftssamling inte är tillgängliga, vare sig för Säkerhetspolisen eller för Säkerhets- och integritetsskyddsnämnden, innebär även att en kontroll är mycket svår att utföra. En kontroll skulle kräva att nämnden ansökte om tillstånd och att Säkerhetspolisen utförde framtagningen. Det skulle därmed vara först då en kontroll utförs som uppgifterna tillgängliggörs. Det skulle, något ironiskt, innebära att det fri- och rättighetsintrång som behandling av uppgifterna innebär blir större när en kontroll utförs, och både Säkerhetspolisen och nämnden får reda på vilka uppgifter som behandlas om den enskilde.

Vidare kan konstateras att den lag som vi föreslår ska reglera de särskilda uppgiftssamlingarna medger behandling av många uppgifter även om de inte, var för sig, behövs för ett ändamål. Att en enskilds personuppgifter förekommer i en särskild uppgiftssamling är därför i de flesta fall författningsenligt. Huruvida registreringsbeslutet är författningsenligt bör vara föremål för en mer systematisk tillsyn än vad som är möjligt genom de enskilda kontrollärendena.

Uppgifter som tas fram med stöd av tillstånd och är tillgängliga för Säkerhetspolisen behandlas därefter med stöd av säpodatalagen. Framtagna uppgifter kommer därför att omfattas av rätten till indirekt insyn så länge de behandlas med stöd av säpodatalagen.

Vi har sammantaget funnit att nackdelarna med att låta den indirekta insynen omfatta de personuppgifter som behandlas i särskilda uppgiftssamlingar är betydligt större än fördelarna. Det finns enligt vår bedömning inte heller något sådant krav enligt Europakonventionen, då de rättssäkerhetsmekanismer som omgärdar dessa uppgifter utgör tillräckligt dataskydd.

10.8 Säkerhets- och integritetsskyddsnämndens uppdrag

10.8.1 Säkerhets- och integritetsskyddsnämndens särskilda tillsynsfokus

Lagen om tillsyn över viss brottsbekämpande verksamhet anger över vilka verksamheter som Säkerhets- och integritetsskyddsnämnden ska utöva tillsyn. Av 1 § följer bland annat att nämnden ska utöva tillsyn över användandet av hemliga tvångsmedel och över den behandling av personuppgifter som utförs av Polismyndigheten, Säkerhetspolisen och Ekobrottsmyndigheten i brottsbekämpande syfte. I sista meningen i andra stycket framgår att tillsynen *särskilt ska avse* behandling enligt bland annat 2 kap. 9 § säpodatalagen. Bestämmelsen innehåller förbudet mot att behandla känsliga personuppgifter och undantag därifrån.

Att behandling av känsliga personuppgifter ska vara särskilt tillsynsfokus har gällt allt sedan år 1996 då Säkerhets- och integritetsskyddsnämndens föregångare Registernämnden inrättades för att utöva tillsyn över Säkerhetspolisens behandling i det dåvarande SÄPO-registret. Det finns säkert flera anledningar till att det har uppfattats som särskilt angeläget att granska hur Säkerhetspolisen behandlar uppgifter om bland annat politiska sympatier. Vid sidan av de historiska skäl som var särskilt framträdande under 1990-talet, ställer även dataskyddskonventionen 108 krav på tillräckliga skyddsåtgärder för känsliga personuppgifter (artikel 6).

10.8.2 Finns det skäl att ange särskilt tillsynsfokus i lag?

Förslag: Det bör inte längre anges i lag att Säkerhets- och integritetsskyddsnämndens tillsyn särskilt ska avse Säkerhetspolisens behandling av känsliga personuppgifter.

Då den nuvarande säpodatalagen beslutades framhöll regeringen att tydliga regler för tillsynsverksamheten är en fördel för tillsynsmyndigheten och tillsynsobjekten samt för enskilda som befarar att deras personuppgifter kan ha behandlats på ett otillåtet sätt. Det innebär att de får klarhet om vilka skyldigheter respektive rättigheter de har och vilka resultat som kan förväntas av tillsynen. Samtidigt ansåg regeringen att det var lika viktigt att inte skapa detaljregler som riskerar att begränsa tillsynsmyndighetens möjligheter att arbeta oberoende och att prioritera bland sina arbetsuppgifter på det sätt som den anser bäst gagnar tillsynsverksamheten som helhet. I avvägningen mellan att skapa tydliga regler och att inte åstadkomma ett regelsystem som riskerar att hämma tillsynsmyndighetens oberoende var regeringens utgångspunkt att en effektiv tillsyn bäst gagnas av att tillsynsmyndigheten får så stor frihet som möjligt att välja sina arbetsformer.

Den nuvarande regleringen innebär att Säkerhets- och integritetsskyddsnämnden måste utöva tillsyn över hur Säkerhetspolisen behandlar känsliga personuppgifter men i övrigt saknas regler om inriktningen. Det har medfört att cirka en tredjedel av de publicerade uttalandena som rör Säkerhetspolisen avser frågan hur känsliga personuppgifter behandlas i myndighetens olika system. Frågan om hur sådana uppgifter behandlas berörs dock i princip i alla uttalanden från nämnden.

I den lagstiftning vi föreslår ingår frågan om förekomsten av känsliga personuppgifter i den proportionalitetsprövning som ska göras innan en behandling sker. Det är ett annat sätt att se på känsliga personuppgifter, där frågan inte längre endast avser om behovet är tillräckligt starkt, utan även om skälet för behandling överväger intrånget i motstående intressen. Denna prövning sker emellertid inte endast för uppgifter som tillhör den katalog som benämns som känsliga personuppgifter. Det finns förstås andra uppgifter som kan uppfattas som känsliga, till exempel att en myndighet har tillgång till privata meddelanden eller semesterfoton. Vi har föreslagit

att behandlingströskeln för känsliga personuppgifter ska vara densamma som för andra uppgifter. Tillsynen av hur känsliga personuppgifter generellt behandlas sammanfaller därför till stor del med frågan om behandlingen sammantaget är proportionerlig. Det finns enligt vår mening inte längre någon anledning att särskilt fokusera tillsynen på hur de känsliga personuppgifterna behandlas.

Det stärkta skydd för känsliga personuppgifter som vi föreslår handlar i större utsträckning om hur sådana uppgifter kan användas för att göra sökningar och urval bland personer. Sådan behandling av känsliga personuppgifter finns det särskild anledning att utöva tillsyn över. Det följer emellertid redan av förslaget till säpodatalag, genom de särskilda krav som uppställs för denna typ av behandling.

Vi delar den uppfattning som regeringen framförde vid införandet av nuvarande säpodatalag. Varje särskilt uppdrag som åläggs tillsynsmyndigheten innebär att myndigheten beskärs från att fördela sina resurser på det sätt som den själv anser bäst. Exempelvis kan det tänkas att Säkerhets- och integritetsskyddsnämndens tillsyn över känsliga personuppgifter under det senaste decenniet medfört att Säkerhetspolisens behandling av sådana uppgifter ofta är författningsenlig. Även om Säkerhets- och integritetsskyddsnämnden skulle anse att riskerna i verksamheten kan identifieras främst inom andra områden innebär 1 § andra stycket sista meningen i lagen om tillsyn över viss brottsbekämpande verksamhet att nämnden, trots det, måste lägga resurser på fortsatta kontroller av behandlingen av känsliga personuppgifter.

Givet våra övriga förslag anser vi att det saknas skäl att i lag styra tillsynens inriktning. Vi anser att den personliga integriteten inte värnas i större utsträckning genom att lagstiftaren låst fast denna särskilda prioritering för tillsynen. Om det finns anledning till myndighetsstyrning, bör detta lämpligen göras genom att regeringen anger det i myndighetsinstruktion i stället för att det anges i lag. Vi har dock inte uppfattat att det finns något skäl att ifrågasätta att nämnden själv har bäst inblick i vilka frågor eller teman som bör granskas och undersökas. Följaktligen föreslår vi att det tillsynsfokus som anges i Säkerhets- och integritetsskyddsnämndens särskilda lagstiftning bör utgå.

11 Ikraftträdande och övergångsbestämmelser

11.1 Ikraftträdande

Förslag: De nya författningarna – lagen om Säkerhetspolisens behandling av personuppgifter och lagen om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar – ska träda i kraft den 1 januari 2027. Samma ikraftträdande ska gälla även för övriga författningsändringar.

11.1.1 Skälen för förslaget

Både lagen om Säkerhetspolisens behandling av personuppgifter och lagen om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar innebär omfattande förändringar av det regelverk som styr Säkerhetspolisens personuppgiftsbehandling. Den nuvarande lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter upphävs och ersätts av två nya lagar med delvis andra utgångspunkter och krav.

Det krävs både organisatoriska och tekniska åtgärder för att Säkerhetspolisen ska kunna tillämpa de nya regelverken på ett ändamålsenligt sätt. Myndigheten behöver göra anpassningar i sina tekniska system, ta fram nya rutiner och arbetsmetoder samt utbilda personalen. De nya lagarna ställer andra krav på granskning och dokumentation av de uppgifter som behandlas. Det ställs bland annat krav på att behandling ska vara proportionell och behandling enligt den nya lagen om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar ska prövas och dokumenteras på ett helt nytt sätt.

I samråd med Säkerhetspolisen har vi bedömt att det är rimligt att de nya lagarna träder i kraft den 1 januari 2027. Denna tidpunkt ger Säkerhetspolisen tillräckligt med tid för att genomföra nödvändiga anpassningar och förbereda sig för tillämpningen av de nya lagarna.

För den särskilda tillsynsmyndigheten och tillsynsmyndigheten medför de nya lagarna också nya uppgifter. Även dessa myndigheter behöver tid för att anpassa sin verksamhet och utarbeta nya rutiner för tillsynen.

Alla övriga författningsförslag är en konsekvens av de två föreslagna nya lagarna och bör därför ha samma datum för ikraftträdande.

11.2 Övergångsbestämmelser

11.2.1 Lag om Säkerhetspolisens behandling av personuppgifter

Förslag: Personuppgifter som behandlas av Säkerhetspolisen vid ikraftträdandet får fortsätta att behandlas enligt äldre föreskrifter till och med den 31 december 2029. Efter denna tidpunkt ska all personuppgiftsbehandling ske i enlighet med de nya lagarna.

Äldre föreskrifter ska fortsätta att gälla för överklagande av beslut som meddelats före den nya lagens ikraftträdande.

Det finns förvisso starka skäl att den nya säpodatalagen tillämpas fullt redan när den träder i kraft. Att tillämpa äldre regler parallellt med nya innebär nämligen att både Säkerhetspolisen och tillsynsmyndigheterna måste förhålla sig till dubbla regelverk. Med hänsyn till att Säkerhetspolisen ofta har behov av att fortsätta behandla även äldre information är en sådan dubbel ordning på sikt inte möjlig att upprätthålla. Säkerhetspolisens datavolymer är emellertid omfattande och innefattar personuppgifter som behandlas i myndighetens olika it-system. För att kunna behandla personuppgifter enligt den nya lagstiftningen måste Säkerhetspolisen bland annat göra proportionalitetsbedömningar och fastställa behandlingstiden för alla uppgifter som behandlas. Det är ett omfattande arbete (se även avsnitt 12.5.2). Vi har därför funnit att det är nödvändigt att införa en övergångsperiod.

Den föreslagna övergångsbestämmelsen innebär att personuppgifter som behandlas av Säkerhetspolisen vid ikraftträdandet får fortsätta att behandlas enligt äldre föreskrifter till och med den 31 december 2029, dvs. i tre år efter ikraftträdandet. Under denna tid måste Säkerhetspolisen successivt granska befintliga uppgifter och anpassa behandlingen till de nya reglerna. Detta innefattar bland annat proportionalitetsbedömningar enligt den nya lagen och bedömningar av om behandlingen ska fortsätta enligt den ordinarie lagen eller om uppgifterna ska överföras till behandling enligt lagen om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar.

Övergångsbestämmelsen ger Säkerhetspolisen möjlighet att stegvis anpassa sin personuppgiftsbehandling till de nya reglerna utan att myndighetens förmåga att utföra sitt uppdrag äventyras. Efter den 31 december 2029 ska dock all behandling ske i enlighet med de nya reglerna, vilket innebär att Säkerhetspolisen senast vid denna tidpunkt måste ha genomfört alla nödvändiga anpassningar.

Eftersom den nuvarande lagen innehåller regler om överklagande som nu ändras måste det föreskrivas en övergångsbestämmelse även i denna del. Vi föreslår bland annat en ändrad instansordning för överklagande av vissa beslut. Den nuvarande lagen bör fortfarande tillämpas för överklagande av beslut som har meddelats före ikraftträdandet av den nya lagen.

11.2.2 Följdändringar

Förslag: Vissa följdändringar i andra lagar kräver att äldre föreskrifter fortsätter att tillämpas under en övergångsperiod.

I de lagar som hänvisar till den nuvarande säpodatalagen krävs övergångsbestämmelser avseende den behandling som kan ske under övergångsperioden. Det gäller exempelvis lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet, där det måste framgå att nämnden ska utöva tillsyn även över behandling som sker med stöd av övergångsbestämmelserna.

12 Konsekvenser

12.1 Inledning

Enligt kommittéförordningen (1998:1474) ska en utredning redovisa vilka konsekvenser som förslagen i ett betänkande kan få i olika avseenden. Nya bestämmelser trädde i kraft den 6 maj 2024, men eftersom denna utredning tillsattes före nämnda datum gäller – enligt övergångsregleringen – i stället motsvarande bestämmelser i dess äldre lydelse.

Av dessa framgår bland annat att om förslagen påverkar kostnaderna eller intäkterna för staten, kommuner, regioner, företag eller andra enskilda, ska en beräkning av dessa konsekvenser redovisas. Och om förslagen innebär samhällsekonomiska konsekvenser i övrigt, ska dessa redovisas. När det gäller kostnadsökningar och intäktsminskningar för staten, kommuner eller regioner, ska utredningen föreslå en finansiering. Vidare ska eventuella konsekvenser för den kommunala självstyrelsen anges. Detsamma gäller eventuella konsekvenser för brottsligheten och det brottsförebyggande arbetet, för sysselsättning och offentlig service i olika delar av landet, för små företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt i förhållande till större företags, för jämställdheten mellan kvinnor och män eller för möjligheterna att nå de integrationspolitiska målen. Om ett betänkande innehåller förslag till nya eller ändrade regler, ska förslagens kostnadsmässiga och andra konsekvenser anges. Detta ska ske på ett sätt som motsvarar de krav som finns i 6 och 7 §§ förordningen (2007:1244) om konsekvensutredning vid regelgivning.

Enligt 6 § i denna förordning ska en konsekvensutredning innehålla

- en beskrivning av problemet och vad man vill uppnå,
- en beskrivning av vilka alternativa lösningar som finns för det man vill uppnå och vilka effekterna blir om någon reglering inte kommer till stånd,
- uppgifter om vilka som berörs av regleringen,
- uppgifter om vilka kostnadsmässiga och andra konsekvenser regleringen medför och en jämförelse av konsekvenserna för de övervägda regleringsalternativen,
- en bedömning av om regleringen överensstämmer med eller går utöver de skyldigheter som följer av Sveriges anslutning till Europeiska unionen, och
- en bedömning av om särskilda hänsyn behöver tas när det gäller tidpunkten för ikraftträdande och om det finns behov av speciella informationsinsatser.

Enligt utredningsdirektivet ska utredaren, utöver vad som följer av kommittéförordningen, noga analysera vilka konsekvenser de förslag som lämnas har för den personliga integriteten. Utredaren ska också bedöma hur förslagen förhåller sig till Sveriges internationella åtaganden om mänskliga rättigheter.

12.2 Problembeskrivning och syfte

Säkerhetspolisen står i dag inför en komplex och breddad hotbild mot Sveriges säkerhet. Auktoritära stater som Ryssland, Kina och Iran bedriver omfattande säkerhetshotande verksamhet mot Sverige genom underrättelseinhämtning, påverkansoperationer, cyberangrepp och olovlig teknik- och kunskapsanskaffning. Samtidigt har hotet från våldsbejakande extremism förändrats, där extremistiska budskap får större spridning via digitala plattformar. Detta beskrivs i kapitel 5.

Den nuvarande säpodatalagen är inte anpassad efter dessa förhållanden och begränsar Säkerhetspolisens förmåga att effektivt hantera omfattande informationsmängder. Lagen innehåller be-

stämmelser som i stort överförts utan ändringar från tidigare lagstiftning och härstammar från en tid då hoten mot Sveriges säkerhet, den tekniska utvecklingen och informationsmängderna såg annorlunda ut. Detta beskrivs i kapitel 6.

Syftet med våra förslag är att ge Säkerhetspolisen mer ändamålsenliga verktyg för att möta dagens hotbild, samtidigt som grundläggande fri- och rättigheter skyddas genom lämpliga skyddsmekanismer.

12.3 Förslag och alternativa lösningar

Våra förslag

Vi föreslår en genomgripande reform av regelverket för Säkerhetspolisens personuppgiftsbehandling genom:

- En helt ny säpodatalag som utgår från dataskyddskonventionen 108+ och Europakonventionen i stället för EU-rätten, se kapitel 8.
- En särskild lag om behandling av personuppgifter i särskilda uppgiftssamlingar, se kapitel 9.
- Förstärkt och förändrad tillsyn, se kapitel 10.

Den nya lagstiftningen bygger på:

- Proportionalitetsprincipen som grundläggande krav.
- Ändamålsenliga behandlingstider anpassade för underrättelseverksamhetens långsiktiga behov.
- Teknikneutral utformning som möjliggör användning av moderna tekniker.
- Systeminriktad kontroll snarare än kontroll av enskilda personuppgifter.

Nollalternativet

Om ingen förändring genomförs kvarstår de nuvarande begränsningarna:

- En administrativt tung granskningsfunktion som skapar flaskhalsar i informationsflödet, se avsnitt 6.1.1–2.
- Krav på konkret behov och ändamål för varje enskild personuppgift, se avsnitt 6.1.3–4.
- För korta längsta tider för behandling givet inriktningen på Säkerhetspolisens verksamhet, se avsnitt 6.1.5.
- Begränsad möjlighet att behandla referensdatabaser eller att utveckla moderna tekniska verktyg, se avsnitt 6.1.6 och 6.2.6.

Nollalternativet skulle innebära att nuvarande lagstiftning fortsätter att tillämpas. Det skulle leda till fortsatta svårigheter för Säkerhetspolisen att effektivt förebygga, förhindra och upptäcka säkerhetshot mot Sverige. Som framgår i kapitel 6 och 7 ser vi stora problem med den nuvarande ordningen.

Nollalternativet innebär att Säkerhetspolisens förmåga även fortsatt hindras av en personuppgiftslagstiftning som inte är anpassad till dagens förhållanden (se till exempel Riksrevisionens granskningsrapport Säkerhetspolisens verksamhet, RiR 2024:24). Detta sker i en tid då hotbilden blir alltmer komplex och informationsmängderna ökar exponentiellt, se kapitel 5 och 6. Vi har bedömt att detta inte är ett godtagbart alternativ.

12.4 Konsekvenser för den personliga integriteten

Bedömning: Förslagen medför ett ökat intrång i den personliga integriteten. Intrånget balanseras genom införandet av robusta skyddsmekanismer med tydliga proportionalitetskrav och förstärkta rättssäkerhetsgarantier i form av förhandskontroll i domstol och förstärkt tillsyn.

Skälen för bedömningen

Den personliga integriteten kan påverkas

Skälen till våra förslag är grundligt motiverade i de tidigare kapitlen. Där har vi genomgående analyserat vilka konsekvenser förslagen får för de grundläggande fri- och rättigheterna i Sverige.

I avsnitt 6.3 bedömer vi att Säkerhetspolisens behov av att behandla personuppgifter är så stort att de åtgärder som krävs för att möta det kan medföra en risk för betydande intrång eller kränkning av mänskliga rättigheter. Rätten till privatliv och skyddet för den personliga integriteten påverkas av att personuppgifter samlas in och bevaras hos en säkerhetstjänst. Om enskilda uppfattar att olika former av opinionsyttringar kan medföra att Säkerhetspolisen registrerar dessa och behandlar dem över tid, kan det få en avhållande effekt på viljan att yttra sig offentligt.

I kapitel 7 redogör vi för inriktningen för våra förslag och hur riskerna ska mötas. De förslag vi lämnar i kapitel 8 och 9 möter i stora delar Säkerhetspolisens behov att kunna behandla personuppgifter. Det samlade intrånget i den personliga integriteten kommer att bli större än tidigare, då fler personuppgifter kommer att registreras och behandlas under längre tid. Även andra grundläggande fri- och rättigheter, främst opinionsfriheten, skulle kunna påverkas.

Skyddsmekanismer för att motverka intrång i grundläggande fri- och rättigheter

För att balansera de utökade möjligheterna för Säkerhetspolisen att behandla personuppgifter innehåller våra förslag flera skyddsmekanismer:

- **Grundläggande proportionalitetsprincip** som kräver att varje behandlingsåtgärd ska vara proportionerlig i förhållande till ändamålet. Detta ger ett starkare skydd än nuvarande lagstiftning, som främst utgår från Säkerhetspolisens behov och en prövning av om varje enskild uppgift behandlas korrekt utan att fullt ut beakta vilket faktiskt intrång behandlingen innebär.

- **Skydd för privilegierad information** som innebär att Säkerhetspolisen inte får behandla meddelanden mellan en försvarare och en misstänkt eller uppgifter som skyddas av meddelarfriheten.
- **Domstolskontroll** för framtagning av uppgifter från särskilda uppgiftssamlingar, vilket ger en oberoende förhandsprövning.
- **Användningsbegränsning:** Uppgifter som tagits fram från en särskild uppgiftssamling får inte användas för att utreda brott, exempelvis i en förundersökning.
- **Förstärkt tillsyn** genom tydligare roller och utökade befogenheter för tillsynsmyndigheterna, särskilt för Säkerhets- och integritetsskyddsnämnden, som också tillförs betydande resurser.
- **Samverkan** mellan Säkerhetspolisen och tillsynsmyndigheterna i frågor som rör personuppgiftsbehandling.
- **Tillsynsperspektiv vid teknikutveckling** som innebär att Säkerhetspolisen åläggs att i skälig utsträckning vidta nödvändiga tekniska åtgärder för att möjliggöra effektiv tillsyn.

Samlad bedömning av integritetsintrånget

Vår bedömning är att risken för kränkning av grundläggande fri- och rättigheter inte har ökat genom förslagen, trots att fler personuppgifter kommer att behandlas. De nya skyddsmekanismerna skapar en bättre balans mellan säkerhetsbehov och integritetsskydd än dagens lagstiftning.

Det finns inte skäl att återupprepa alla de överväganden som gjorts i dessa avseenden. I respektive avsnitt i betänkandet har vi gjort bedömningar om potentiella intrång i grundläggande fri- och rättigheter och hur dessa ska motverkas, kompenseras eller accepteras. I kapitel 8 har vi återkommande redogjort för de avvägningar vi gjort mellan den personliga integriteten och det allmänna intresset av att skydda nationell säkerhet i samband med att Säkerhetspolisen behandlar personuppgifter för brottsbekämpande ändamål. I kapitel 9 har vi lämnat förslag på undantag från dataskyddsrättsliga grundprinciper. Dessa undantag har kompenserats med kraftfulla alternativa skyddsmekanismer. Vi har föreslagit ett krav på skriftligt motiverade beslut för registrering av personuppgifter,

krav på förhandstillstånd från en oberoende domstol för framtagning av personuppgifter, förbud mot att använda uppgifterna i förundersökningar och effektiva möjligheter för Säkerhets- och integritetsskyddsnämnden att utöva tillsyn.

Vår samlade bedömning är sammanfattningsvis att Sverige med god marginal kommer att hålla sig innanför de skyldigheter som följer av våra internationella åtaganden genom de förslag vi lämnar. Även denna bedömning görs genomgående i betänkandet i anslutning till respektive förslag.

12.5 Konsekvenser för brottsligheten och det brottsförebyggande arbetet

Bedömning: Den nya säpodatalagen och lagen om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar stärker tydligt Säkerhetspolisens förmåga att förebygga, förhindra och upptäcka brottslig verksamhet mot rikets säkerhet eller terrorbrott. Förslaget till ny säpodatalag stärker även Säkerhetspolisens förmåga att utreda sådana brott.

12.5.1 Skälen för bedömningen

Stärkt operativ förmåga

Genom att Säkerhetspolisen ges ökade möjligheter att behandla personuppgifter kommer myndighetens samlade operativa förmåga att öka. Våra förslag utökar inte möjligheterna till informationsinhämtning, men ger bättre möjligheter att bearbeta och analysera information över tid. Detta skapar synergieffekter med existerande förmågor. Dessa positiva effekter gäller för både underrättelseverksamheten och den brottsutredande verksamheten.

Möjligheten att behandla stora informationsmängder i särskilda uppgiftssamlingar ger Säkerhetspolisen bättre förutsättningar att upptäcka mönster och sammanhang som annars skulle vara svåra att identifiera. Detta är särskilt värdefullt i komplexa underrättelseärenden där information som initialt verkar perifer senare kan visa sig ha avgörande betydelse.

Effektivare resursanvändning

Den nya lagstiftningen minskar den administrativa bördan kring granskning av personuppgifter, vilket frigör resurser till operativt arbete. Efter en inledande implementeringsperiod kommer Säkerhetspolisen kunna arbeta mer effektivt genom bland annat minskad administrativ hantering kring varje enskild personuppgift och ändamålsenliga behandlingstider som inte innebär kontinuerlig behovsprövning.

Den samlade effekten bedöms bli mycket positiv för Säkerhetspolisens möjlighet att utföra sitt uppdrag. Effekten kan dock inte kvantifieras.

12.6 Ekonomiska konsekvenser för staten

12.6.1 Bakgrund

Vi föreslår att de båda lagstiftningarna ska träda i kraft i sin helhet från den 1 januari 2027. Vi har därutöver föreslagit övergångsbestämmelser som ska gälla under tre år.

Förslagen innebär i sig inte några ökade kostnader för de myndigheter som påverkas. I huvudsak kommer de direkta konsekvenserna bestå i att Säkerhetspolisen ska tillse att de delvis nya kraven som lagarna uppställer, bland annat vad gäller proportionalitet och individuellt bestämd behandlingstid, tillämpas korrekt efter att tiden för övergångsbestämmelserna löpt ut. Detsamma gäller de båda tillsynsmyndigheterna som måste förhålla sig till helt ny lagstiftning.

Lagstiftningarna kommer att möjliggöra en ökad förmåga för Säkerhetspolisen, exempelvis genom att personuppgifter kan behandlas för teknikutveckling och att stora informationsmängder kan behandlas i särskilda uppgiftssamlingar. Kostnader till följd av sådan behandling är emellertid inte en direkt konsekvens av denna lagstiftning, utan en fråga om prioriteringar inom existerande eller förhöjd anslagsram. Det kommer däremot att uppstå kostnader för tillsyn av sådana nya system och domstolen måste rustas för att kunna hantera ansökningar.

12.6.2 Sammanlagda ekonomiska konsekvenser

Vi har bedömt att de sammanlagda ekonomiska konsekvenserna för staten uppgår till cirka:

- 45 miljoner kronor år 2027,
- 36,3 miljoner kronor år 2028,
- 28,5 miljoner kronor år 2029 och
- 18,5 miljoner kronor per år från 2030.

De kostnader som uppstår i andra myndigheter än Säkerhetspolisen föreslås finansieras genom omfördelningar från Säkerhetspolisens ramanslag. De ekonomiska konsekvenserna ryms därmed inom befintliga ekonomiska ramar för statsbudgeten som helhet. I det följande beskrivs dessa kostnader för respektive myndighet.

12.6.3 Säkerhetspolisen

Bedömning: Förslagen innebär att Säkerhetspolisen måste omfördela resurser under en genomförandefas men att personuppgifter därefter kan behandlas mer effektivt.

Omfördelningen kan hanteras inom Säkerhetspolisens ramanslag och det finns inte skäl att här lämna förslag om särskild finansiering. Om inte resurser tillförs engångsvis, kan det dock kortsiktigt påverka Säkerhetspolisens operativa förmåga.

Skälen för bedömningen

Nuvarande anslag

Säkerhetspolisen har i budgetpropositionen för år 2025 tilldelats 2,75 miljarder kronor. För 2026 beräknas anslaget öka med 233 miljoner kronor och från och med 2027 med 300 miljoner kronor.

Mellan åren 2023 och 2027 beräknas myndighetens anslag ha ökat med cirka 1 miljard kronor, vilket motsvarar cirka 50 procent.

En ny säpodatalag

Förslaget kommer att förändra Säkerhetspolisens informationshantering och, enligt myndighetens egna beräkningar, bidra till en ökad effektivitet i det operativa arbetet på tre års sikt. Under en övergångsperiod på tre år kommer Säkerhetspolisen att behöva granska nuvarande information i enlighet med den föreslagna lagstiftningen. Granskning och omprövning av informationen som behandlas enligt den nuvarande lagen kommer att behöva göras parallellt med att den nya lagen ska börja tillämpas för nya personuppgifter som behandlas.

För att hantera övergången och för att dra nytta av den nya lagstiftningens möjligheter att behandla personuppgifter, bedömer Säkerhetspolisen att en resursförstärkning krävs. En resursförstärkning krävs även för att omhänderta de stora utbildningsinsatserna för Säkerhetspolisens operativa personal i att kunna granska information enligt förslaget samt för att upprätta metodstöd och handböcker. Den nya lagstiftningen innebär ett större ansvar hos fler medarbetare än tidigare att säkerställa författningsenlig personuppgiftsbehandling. Denna förflyttning från högt specialiserade personuppgiftsexperter till ett större ansvar hos fler medarbetare kommer att ge ökad effektivitet på sikt men innebär en kostnad under övergångsperioden.

Kostnaden för att förhindra en operativ förmågesänkning under övergångsperioden mellan den nuvarande och föreslagna säpodatalagen bedöms vara 30 miljoner kronor år 2027 och därefter falla till 20 miljoner kronor 2028 och 10 miljoner kronor år 2029. Därefter bedömer Säkerhetspolisen att effektiviseringen av informationshanteringen bidrar till en omfördelning av resurser som innebär att en ökad operativ förmåga inom befintlig budgetram.

Vår bedömning är att dessa kostnader kan hanteras inom Säkerhetspolisens anslag men noterar att detta oundvikligen kommer att medföra en viss operativ förmågesänkning under en period. Det är ytterst en politisk fråga om en sådan sänkning är acceptabel.

Särskilda uppgiftssamlingar

Genom förslaget om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar tillkommer nya administrativa krav för bland annat registrering och ansökningar hos domstolen. Det kommer att kräva att Säkerhetspolisen under en genomförandefas utvecklar nya rutiner och genomför en organisationsförändring för de särskilda krav som ställs enligt den föreslagna lagen. Vidare tillkommer kostnad för utbildning, upprättande av interna riktlinjer, manualer och vägledningar.

De direkta kostnaderna som uppkommer för Säkerhetspolisen genom förslaget bedöms till 10 miljoner kronor, under en genomförandeperiod om ett år. Under genomförandeperioden kommer analytisk teknikkompetens behöva utökas och ytterligare resurser kan behöva tillföras, bland annat för att hantera den nya domstolsprocessen.

Säkerhetspolisen har själv bedömt att det efter genomförandefasen inte uppkommer några direkta kostnader till följd av lagförslagen, som då kan hanteras inom befintlig budgetram.

För att fullt ut utnyttja den nya förmågan krävs investeringar i teknik. Vid användning av tekniken uppstår vidare löpande kostnader. Detta är dock inte direkta konsekvenser av lagförslagen och bör därför hanteras som prioriteringar inom den befintliga anslagsramen eller genom tillskjutande resurser. Det kan emellertid konstateras att om lagstiftningens intentioner ska få fullt genomslag, torde det krävas resurssatsningar.

12.6.4 Säkerhets- och integritetsskyddsnämnden

Förslag: Säkerhets- och integritetsskyddsnämnden kommer behöva förstärka sin tillsynsverksamhet till följd av förslagen. Nämnden ska därför tilldelas ökat ramanslag med

– 11 666 000 kronor år 2027,

– 12 953 000 kronor år 2028, och

– 15 194 000 kronor från år 2029 och framåt.

Anslagsökningen finansieras genom att motsvarande summa förs över från Säkerhetspolisens ramanslag.

Skälen för förslagen

Nuvarande anslag

Säkerhets- och integritetsskyddsnämnden har enligt budgetpropositionen för år 2025 ett anslag om cirka 42,7 miljoner kronor som beräknas öka till drygt 45 miljoner år 2026 och knappt 46 miljoner år 2027.

Regeringen har under år 2024 remitterat ett utkast till lagrådsremiss *Datalagring och tillgång till elektronisk information* (Ju2024/02286). I utkastet föreslås att Försvarsunderrättelsedomstolen övertar uppgiften som kontrollorgan från Säkerhets- och integritetsskyddsnämnden. Nämndens kostnader för kontrollorgansfunktionen beräknades öka med 3 miljoner kronor från år 2026 (se prop. 2023/24:1, Utgiftsområde 4, s. 73). Om uppgiften överförs enligt förslaget, kommer motsvarande medel att överföras från nämnden till Försvarsunderrättelsedomstolen.

Ny säpodatalag

Den nya säpodatalagen ger Säkerhetspolisen större möjligheter att behandla personuppgifter än idag, vilket påverkar tillsynsverksamheten väsentligt. Bedömning av laglighet ska i större utsträckning göras med utgångspunkt i en proportionalitetsbedömning i stället för från precisa lagregler. Detta ställer högre krav på analys och bedömning i varje tillsynsärende. Att avgöra vad som utgör proportionerlig personuppgiftsbehandling kräver särskilda insikter och mer verksamhetsnära tillsyn. Att tillsynen kan stärkas är en viktig del för att säkerställa att den nya lagstiftningen även i praktiken uppfyller våra internationella åtaganden.

Kontroller på begäran av enskilda förväntas också bli mer komplexa. De synergieffekter som finns av att nämnden utövar tillsyn över likartade personuppgiftslagar minskar genom förslaget till ny säpodatalag.

För att möta dessa utmaningar behövs fler kvalificerade föredragande. Nämnden bedömer behovet till tre nya föredragande, till en kostnad av 1 050 000 kronor per person och år (inklusive anslutning till Försäkringskassans it-lösning). Total årlig kostnad blir därmed 3 150 000 kronor. Därtill kommer engångskostnader för

inventarier, säkerhetsskåp och särskilt anpassad utrustning på totalt 477 000 kronor.

Den nya lagen ger Säkerhetspolisen möjlighet att utnyttja ny teknik för effektiv informationshantering. Personuppgiftsbehandlingen kommer därmed att bli alltmer avancerad och komplex. För att kunna utöva tillsyn över nya komplexa behandlingsåtgärder krävs kvalificerad teknisk kompetens med fördjupade kunskaper för att förstå de bakomliggande strukturerna. För att möta de nya utmaningar som Säkerhetspolisens mer utvecklade tekniska lösningar medför, behöver nämnden därför rekrytera kvalificerad kompetens på området. Denna utmaning hänger samman även med tillsynen över särskilda uppgiftssamlingar. Konsekvenserna av detta bedöms samlat nedan

Särskilda uppgiftssamlingar

Nämnden har bedömt att tillsynen över lagen om särskilda uppgiftssamlingar kommer att kräva föredragande med lång erfarenhet av kvalificerat juridiskt arbete. Särskilt viktigt är detta för personal som ska ta fram underlag för, avge yttranden till eller företräda nämnden i domstol. Nämnden behöver också bygga upp beredskap för att med kort varsel kunna uppträda i domstol och själv ansöka om framtagning av uppgifter.

Initialt bedöms behovet uppgå till tre ytterligare föredragande. Nämnden har uppskattat den årliga kostnaden till 1 650 000 kronor per person och år, totalt 4 950 000 kronor årligen. Därtill kommer engångskostnader för inventarier och särskilt anpassad utrustning på sammanlagt 477 000 kronor.

Behovet av teknisk kompetens

Förslagen i utredningen möjliggör för Säkerhetspolisen att använda mer avancerad teknik för informationshantering. För en effektiv tillsyn måste teknisk kompetens finnas även hos tillsynsmyndigheten. Nämnden behöver därför successivt bygga upp en teknisk kompetens, vid sidan av den juridiska.

Nämnden har bedömt att det finns behov av att rekrytera en person vid lagens ikraftträdande och ytterligare två till tre personer

under de följande två åren. För detta ändamål beräknas kostnaden till 2 500 000 kronor år 1, ytterligare 2 300 000 kronor år 2 och ytterligare 2 300 000 kronor år 3. I dessa belopp ingår kostnader för specialanpassad hård- och mjukvara samt engångskostnader för inventarier.

Att denna tekniska kompetensuppbyggnad kan ske ser vi som en central del i tillsynen av den nya lagen.

Övriga faktorer

Nämndens nuvarande lokaler kan inte rymma den planerade personalökningen utan ombyggnad för att skapa ytterligare fyra tjänsterum. En överenskommelse om sådan utvidgning finns sedan tidigare med hyresvärden.

Förslagen kräver även att nämnden övergår till delvis nya arbetssätt. Den mer omfattande proportionalitetsprövningen innebär att större informationsmängder kan behöva granskas, tillsammans med tekniska aspekter av behandlingen. Detta leder till mer omfattande föredragningar vid nämndens sammanträden, vilket sannolikt kräver fler möten. Kostnaden för extra möten beräknas till 28 000 kronor per tillfälle, främst för ledamöternas resor. Med fyra extra möten per år blir merkostnaden 112 000 kronor årligen.

Övriga delar av förslagen bedöms kunna hanteras inom ramen för befintliga budgetmedel.

Finansiering

De sammanlagda kostnader som redovisats ovan innebär att Säkerhets- och integritetsskyddsnämndens ramanslag behöver höjas med cirka 11 miljoner kronor från år 2027, 13 miljoner kronor från år 2028 och 15 miljoner kronor från år 2029. Till det kommer engångskostnader framför allt år 2027 med cirka 1 miljon kronor.

Det är Säkerhetspolisen som får en verksamhetsnytta av att förslagen genomförs. Det är därför naturligt att de ökade kostnaderna för tillsynen belastar Säkerhetspolisens anslag. Finansiering bör således ske genom att motsvarande summa överförs från anslagspost 1:2 Säkerhetspolisen till nämndens anlagspost. Med detta sagt bör betonas att lagförslagen inte leder till någon motsvarande kost-

nadsbesparing för Säkerhetspolisen. Det innebär att förslaget kommer att leda till motsvarande operativ förmågesänkning. Det är ytterst en politisk fråga om en sådan sänkning är acceptabel.

Tabell 12.1 Säkerhets- och integritetsskyddsnämndens kostnader

Utgiftsområde 4 anslag 1:15

	År 1	År 2	År 3
Personalkostnader			
– Föredragande säpodatalagen	3 150	3 150	3 150
– Föredragande särskilda uppgiftssamlingar	4 950	4 950	4 950
– Teknisk kompetens	2 441	4 682	6 923
Tillkommande nämndsammanträden	112	112	112
Engångskostnad (utrustning m.m.)	1 013	59	59
	11 666	**12 953**	**15 194**

12.6.5 Försvarsunderrättelsedomstolen

Förslag: Försvarsunderrättelsedomstolen behöver öka antalet särskilda ledamöter till följd av förslagen. Det medför en årlig kostnadsökning med 250 000 kronor.

Därutöver krävs en förstärkning av domstolens kansli med två tjänster, till en kostnad av 3 100 000 kronor per år och en engångskostnad om 400 000 kronor. Detta under förutsättning att domstolens kansli inte förstärks i motsvarande mån genom att domstolen tilldelas rollen som kontrollorgan, enligt lagen om lagring av och tillgång till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet.

Kostnadsökningen ska finansieras genom att motsvarande summa överförs från Säkerhetspolisens ramanslag i utgiftsområde 4 till utgiftsområde 6.

Skälen för förslaget

Nuvarande anslag

Försvarsunderrättelsedomstolen har enligt budgetpropositionen för år 2025 ett ramanslag om cirka 12 miljoner kronor.

Regeringen har under år 2024 remitterat ett utkast till lagrådsremiss *Datalagring och tillgång till elektronisk information* (Ju2024/02286). I utkastet föreslås att Försvarsunderrättelsedomstolen ska överta uppgiften som kontrollorgan. Om uppgiften som kontrollorgan överförs till Försvarsunderrättelsedomstolen enligt förslaget, kommer Försvarsunderrättelsedomstolen tilldelas ytterligare 3 miljoner kronor från år 2026.

Nya uppgifter

Försvarsunderrättelsedomstolen föreslås få nya uppgifter till följd av våra förslag. Domstolen föreslås vara prövningsinstans för tillstånd som söks för framtagning från särskilda uppgiftssamlingar. Vidare föreslår vi att tillsynsmyndighetens beslut som fattas med stöd av säpodatalagen ska överklagas till Försvarsunderrättelsedomstolen. Den senare uppgiften, som torde vara sällsynt förekommande, bedömer vi kunna inrymmas inom befintligt anslag.

Som prövningsorgan enligt förslag till lag om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar behövs däremot en ökad resurstilldelning. Enligt domstolens egen bedömning torde domarkapaciteten, i vart fall i ett inledningsskede, kunna upprätthållas med en ordförande, två vice ordföranden och tio särskilda ledamöter. Det innebär en ökning med fyra särskilda ledamöter jämfört med i dag. Tillkommande kostnader för de särskilda ledamöterna bedöms öka med 250 000 kronor per år. I beloppet ingår även kostnader för utbildning.

När det gäller domstolens kansli, bedömer domstolen att de tillkommande uppgifterna kräver två heltidsanställningar på kansliet. Personalkostnaden för dessa beräknas till cirka 3 000 000 kronor per år. Därutöver tillkommer cirka 100 000 kronor per år i löpande kostnader för bland annat telefoni, licenser samt kostnader hänförliga till personal- och ekonomiadministration. Engångskostna-

der i form av bland annat kontorsinredning, IT och säkerhetsskyddsåtgärder uppskattas till cirka 400 000 kronor.

Med en sådan bemanning kan verksamheten, genom en omdisponering, bedrivas i nuvarande lokaler och några ytterligare lokalkostnader är då inte nödvändiga.

Om domarkapaciteten visar sig otillräcklig och en ytterligare domare behöver anställas, bedöms den årliga kostnaden uppgå till ytterligare 2 000 000 kronor per år. I sådant fall finns även ett behov av utökning av nuvarande lokaler. Om sådana lokaler kan tillhandahållas av FOI i anslutning till nuvarande lokaler bedöms lokalkostnaden öka med cirka 200 000 kronor per år. Om domstolen skulle behöva flytta till andra lokaler inom FOI, tillkommer höga kostnader för ett nytt sammanträdesrum. Därtill kommer engångskostnader för ombyggnation och andra anpassningar av lokalerna bedömt till cirka 1 000 000 kronor samt för återställandet av nuvarande lokaler till cirka 800 000 kronor.

Finansiering

De sammanlagda kostnaderna för domstolen innebär ett behov av att öka ramanslaget från och med år 2027 med cirka 3 350 000 kronor per år. Därutöver tillkommer en engångskostnad om 400 000 kronor.

Som framgår ovan finns det förslag om att domstolen ska tilldelas uppgifter även som kontrollorgan för datalagringsskyldigheten i syfte att skydda nationell säkerhet, enligt tidigare nämnda utkast till lagrådsremiss. Om båda förslagen genomförs, kommer domstolens resursbehov dock inte att fördubblas. De handläggare som krävs för att utföra arbetsuppgifter enligt utkastets förslag kan sannolikt utföra uppgifter även till följd av våra förslag. Uppgifternas karaktär och den kompetens som krävs vid handläggningen torde i stora delar vara överlappande.

Om utkastet till lagrådsremissen genomförs, bör kostnadsökningen till följd av våra förslag inledningsvis kunna stanna vid förstärkningen av antalet särskilda ledamöter och vissa engångskostnader (250 000 kronor årligen plus 400 000 kronor engångsvis). Det måste dock finns beredskap att tillskjuta ytterligare resurser till domstolen, om behovet av domarkapacitet visar sig större än beräknat.

Den ökade kostnaden för domstolen är en följd av att Säkerhetspolisen får förmågan att behandla stora informationsmängder i särskilda uppgiftssamlingar. Därför bör domstolens kostnader finansieras genom en överföring från Säkerhetspolisens anslag (utgiftsområde 4 anslagspost 1:2) till Försvarsunderrättelsedomstolens anslag (utgiftsområde 6 anslagspost 1:12).

Med detta sagt bör betonas att lagförslagen inte leder till någon motsvarande kostnadsbesparing för Säkerhetspolisen. Det innebär att förslaget kommer att leda till motsvarande operativ förmågesänkning. Det är ytterst en politisk fråga om en sådan sänkning är acceptabel.

12.6.6 Övriga myndigheter

Bedömning: *Integritetsskyddsmyndigheten* kommer att påverkas av förslagen men bedöms kunna hantera konsekvenserna inom befintligt anslag. *Polismyndigheten* kommer att tillämpa säpodatalagen endast i undantagsfall, vilket inte bedöms medföra några ekonomiska konsekvenser. *Sveriges domstolar* påverkas i marginell utsträckning, vilket inte medför några konsekvenser som inte inryms inom domstolarnas ordinarie ramanslag.

Skälen för bedömningen

Konsekvenser för Integritetsskyddsmyndigheten

Integritetsskyddsmyndigheten kommer att ha i stort sett samma uppdrag i förhållande till Säkerhetspolisen som i dag. Tillsynen kommer dock inte att kunna ske på samma sätt som den som utövas i förhållande till andra brottsbekämpande myndigheter. Det kommer därför att behövas särskilda utbildningsinsatser för tillsyn över säpodatalagen. Att vårt förslag till säpodatalag avviker från den tidigare lagen kan inte anses utgöra en särskild konsekvens för Integritetsskyddsmyndigheten. Myndigheten utövar tillsyn över flera olika lagstiftningar, bland annat försvarsdatalagen och FRA-datalagen som i likhet med vårt förslag saknar EU-rättslig koppling. Tillsynen över den nya säpodatalagen är en uppgift som vi bedömer ryms inom myndighetens nuvarande anslag.

Integritetsskyddsmyndigheten kommer att ges möjlighet att ansöka om tillstånd till framtagning. Det kan dock inte förväntas ske i sådan omfattning att det medför några särskilda ekonomiska konsekvenser.

Konsekvenser för Polismyndigheten

Polismyndigheten kommer att tillämpa den nya lagen i de fall myndigheten har övertagit en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen. Detta kommer dock att ske i ett mycket begränsat antal fall och bedöms inte påverka Polismyndighetens verksamhet i någon större omfattning. De kostnadsökningar som förslaget i denna del kan medföra för myndigheten bedöms marginella och kan hanteras inom myndighetens befintliga ram.

Konsekvenser för allmänna förvaltningsdomstolar

De förslag vi lämnar om att begränsa de rättsmedel som enskilda har att begära rättelse, komplettering eller radering, innebär att färre överklagbara beslut kommer att fattas. Tillsynsmyndighetens beslut om föreläggande eller förbud ska enligt vårt förslag inte längre överklagas till allmän förvaltningsrätt. Dessutom föreslår vi att beslut om att inte lämna ut registerutdrag eller att ta ut avgift ska överklagas till kammarrätt som första instans.

Våra förslag innebär att Förvaltningsrätten i Stockholm inte längre kommer att pröva några beslut enligt säpodatalagen. Det innebär dock inte annat än en mycket marginell förändring i domstolens sammanlagda målstock. Även för Kammarrätten i Stockholm innebär förändringen en mycket marginell justering i verksamheten. Vi bedömer sammantaget att förslagen är kostnadsneutrala för Sveriges domstolar.

12.7 Övriga konsekvenser

Nationell säkerhet undantagen från EU:s dataskyddsreglering

Vårt förslag utgår från att skyddet av nationell säkerhet är en nationell angelägenhet som faller utanför EU:s kompetensområde. Lagstiftningen baseras därför på dataskyddskonventionen och Europakonventionen i stället för på EU-rätten. Detta är förenligt med artikel 4.2 i fördraget om Europeiska unionen, som fastslår att nationell säkerhet förblir varje medlemsstats eget ansvar. Förslaget innebär därmed inget åsidosättande av Sveriges åtaganden enligt EU-rätten.

Kommunala självstyret

Förslagen påverkar inte det kommunala självstyret, då de enbart berör statliga myndigheter och deras verksamhet.

Jämställdhet mellan könen

Förslagen förväntas inte få några konsekvenser för jämställdheten mellan kvinnor och män. Lagstiftningen är könsneutral och tillämpas lika oavsett kön.

Barnkonventionen

Säkerhetspolisens verksamhet är av naturliga skäl främst inriktade mot vuxna. I den mån personuppgifter om barn behandlas, föreslår vi att behandlingstiden ska anpassas för att särskilt beakta att barns personuppgifter ska omfattas av ett särskilt starkt dataskydd. Detta ger ett förstärkt skydd för barns integritet i förhållande till vuxnas och är i linje med principen om barnets bästa i barnkonventionen. Vårt förslag tillgodoser kraven i barnkonventionen.

Ikraftträdande och informationsinsatser

Vi föreslår att lagstiftningen träder i kraft den 1 januari 2027, med en övergångsperiod på tre år där personuppgifter som redan behandlas vid ikraftträdandet får fortsätta att behandlas enligt den äldre lagen fram till och med den 31 december 2029.

Detta ger Säkerhetspolisen och tillsynsmyndigheterna tillräcklig tid att anpassa sina system, rutiner och arbetssätt. Det kommer att krävas omfattande utbildningsinsatser för berörd personal, särskilt inom Säkerhetspolisen och tillsynsmyndigheterna.

Det stegvisa införandet balanserar behovet av att snabbt införa ett modernare regelverk mot myndigheternas förmåga att upprätthålla sin verksamhet under övergångsperioden.

13 Författningskommentar

13.1 Förslaget till lag om Säkerhetspolisens behandling av personuppgifter

1 kap. Allmänna bestämmelser

Lagens syfte

1 § Syftet med lagen är att skydda fysiska personers grundläggande rättigheter och friheter i samband med behandling av personuppgifter och att säkerställa att Säkerhetspolisen kan behandla personuppgifter på ett ändamålsenligt sätt.

Av bestämmelsen, som motiveras i avsnitt 8.1.1, framgår lagens syften. Paragrafen motsvarar delvis 1 kap. 1 § i nuvarande lag.

Lagen syftar både till att skydda fysiska personers grundläggande fri- och rättigheter vid personuppgiftsbehandling och till att möjliggöra för Säkerhetspolisen att inom lagens tillämpningsområde behandla personuppgifter på ett ändamålsenligt sätt.

Lagens tillämpningsområde

2 § Denna lag gäller vid behandling av personuppgifter som rör nationell säkerhet i Säkerhetspolisens brottsbekämpande verksamhet.

Lagen gäller även vid Polismyndighetens behandling av personuppgifter, när myndigheten har övertagit en uppgift från Säkerhetspolisen inom denna lags tillämpningsområde.

När Polismyndigheten har övertagit en uppgift enligt andra stycket, ska vad som i denna lag sägs om Säkerhetspolisen i stället gälla Polismyndigheten.

Paragrafen anger, tillsammans med 3 och 4 §§, lagens tillämpningsområde och innebär endast förtydliganden och redaktionella änd-

ringar i förhållande till nuvarande 1 kap. 2 § (jfr prop. 2018/19:163 s. 211). Överväganden finns i avsnitt 8.1.2.

Av *första stycket* framgår lagens tillämpningsområde. Lagen reglerar behandling av personuppgifter som rör nationell säkerhet i Säkerhetspolisens brottsbekämpande verksamhet. I princip all verksamhet vid Säkerhetspolisen är i någon mån brottsbekämpande. Brottsbekämpning har samma betydelse som motsvarande begrepp i nuvarande lagstiftning.

Vad som utgör nationell säkerhet går inte att fullt ut bestämma på nationell nivå. Nationell säkerhet utmärks bland annat av att den syftar till att skydda statens grundfunktioner och samhällets grundläggande intressen. Det krävs inte att ändamålet för varje enskild behandling går att koppla till skyddet av nationell säkerhet. Det är tillräckligt att behandlingen ingår som ett led i en verksamhet med det syftet. Av 1 kap. 1 § första stycket 3 lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område följer att Säkerhetspolisen i stället ska tillämpa den lagen, om behandling sker för brottsbekämpande syften som inte rör nationell säkerhet.

Av *andra stycket* framgår att lagen gäller vid Polismyndighetens behandling av personuppgifter när myndigheten har övertagit en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen. Lagen ska tillämpas när Säkerhetspolisen har lämnat över en arbetsuppgift som rör nationell säkerhet till Polismyndigheten enligt 15 § förordningen med instruktion för Säkerhetspolisen eller när Säkerhetspolisen begärt bistånd av Polismyndigheten med stöd av 25 § förordningen (2022:1718) med instruktion för Polismyndigheten. Av *tredje stycket* följer att det som sägs i lagen om Säkerhetspolisen då i stället gäller Polismyndigheten.

3 § Lagen gäller vid sådan behandling av personuppgifter som är helt eller delvis automatiserad och för annan behandling av personuppgifter som ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Paragrafen, som motsvarar nuvarande 1 kap. 3 § (jfr prop. 2018/19:163 s. 212) begränsar lagens tillämpningsområde till helt eller delvis automatiserad behandling av personuppgifter och personuppgifter som är strukturerade på ett sätt som gör att det är möjligt att söka eller

sammanställa uppgifterna enligt särskilda kriterier. Lagen reglerar därmed sådan personuppgiftsbehandling som omfattas av dataskyddskonventionen 108+ (CETS 223). Av 1 kap. 5 § framgår vad som utgör en personuppgift och vad som utgör behandling av personuppgifter. Lagen är endast tillämplig för sådan informationshantering som utgör behandling av personuppgifter. Det innebär bland annat att behandling av uppgifter om juridiska personer eller avlidna inte omfattas av lagens tillämpningsområde.

4 § Om en annan lag innehåller någon bestämmelse som avviker från denna lag, tillämpas den bestämmelsen.

I lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar finns bestämmelser om Säkerhetspolisens behandling av personuppgifter i vissa fall.

Paragrafen reglerar hur lagen förhåller sig till annan författning och motsvarar delvis nuvarande 1 kap. 4 §. De allmänna övervägandena görs i avsnitt 8.1.3.

Av *första stycket* framgår att lagen är subsidiär till avvikande bestämmelser i andra lagar men, till skillnad mot nuvarande lag inte till förordning. Exempel på sådana avvikande regler finns i lagen (2017:496) om internationellt polisiärt samarbete.

I *andra stycket* upplyses om att personuppgifter som ska eller har registrerats i en särskild uppgiftssamling ska behandlas enligt särskilda regler i den lagen.

Definitioner

5 § I denna lag används följande uttryck med nedan angiven betydelse.

Uttryck	Betydelse
Behandling av personuppgifter	En åtgärd eller kombination av åtgärder som vidtas i fråga om personuppgifter eller uppsättningar av personuppgifter, oavsett om det görs automatiserat eller inte, t.ex. insamling, granskning, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämnande, spridning eller tillhanda-

	hållande på annat sätt, justering, sammanföring, begränsning, radering eller förstöring.
Biometriska uppgifter	Personuppgifter som rör en persons fysiska, fysiologiska eller beteendemässiga kännetecken, som tagits fram genom särskild teknisk behandling och som möjliggör eller bekräftar unik identifiering av personen.
Genetiska uppgifter	Personuppgifter som rör en persons nedärvda eller förvärvade genetiska kännetecken och som härrör från analys av ett spår av eller ett prov från personen.
Inledande behandling	Behandling av personuppgifter som innebär att personuppgifter samlas in, hämtas in, tas emot eller på något annat sätt kommer Säkerhetspolisen till handa eller att personuppgifter nedtecknas, upprättas eller på något annat sätt skapas inom myndigheten, eller att personuppgifter tas fram från en särskild uppgiftssamling enligt lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftsinsamlingar.
Känsliga personuppgifter	Biometriska uppgifter, genetiska uppgifter och uppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning.
Personuppgift	Varje upplysning om en identifierad eller identifierbar fysisk person som är i livet.
Personuppgiftsansvarig	Den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter.

Personuppgiftsbiträde	Den som behandlar personuppgifter för den personuppgiftsansvariges räkning.
Registrerad	Den fysiska person som personuppgiften gäller.

I paragrafen definieras olika uttryck som används i lagen. Vissa uttryck överförs från 1 kap. 5 § i nuvarande lag.

Behandling av personuppgifter

Uttrycket motsvarar nuvarande definition (jfr prop. 2018/19:163 s. 212).

Biometriska uppgifter

Biometriska uppgifter, som är känsliga personuppgifter, har samma betydelse som i nuvarande lag (jfr prop. 2018/19:163 s. 213). Allmänna överväganden om begreppet görs i avsnitt 8.15.1.

Genetiska uppgifter

Uttrycket motsvarar nuvarande definition (jfr prop. 2018/19:163 s. 215).

Inledande behandling

Uttrycket, som är nytt, omfattar all sådan behandling som innebär att personuppgifter kommer till Säkerhetspolisen eller skapas inom myndigheten. Allmänna överväganden finns i avsnitt 8.6.5. Uppräkningen av de åtgärder som ingår i begreppet är inte uttömmande. De behandlingsåtgärder som ingår i inledande behandling utgör även behandling av personuppgifter. Begreppet framtagning definieras i 1 kap. 2 § lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar.

Känsliga personuppgifter

Känsliga personuppgifter definieras inte i nuvarande 1 kap. 5 § men används, med samma betydelse i 2 kap. 11 §.

Känsliga personuppgifter är personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning. Därutöver omfattas genetiska och biometriska uppgifter, som också har egna definitioner.

Uppgift om hälsa har samma innebörd som i nuvarande lag (jfr prop. 2018/19:163 s. 216).

Personuppgift

Uttrycket personuppgift definieras på samma sätt som i nuvarande lag (jfr prop. 2018/19:163 s. 214). Begreppet har samma betydelse som i annan personuppgiftslagstiftning och motsvarande uttryck i artikel 2 a i dataskyddskonventionen 108+.

Personuppgiftsansvarig

Uttrycket återfinns i nuvarande lagstiftning (jfr prop. 2018/19:163 s. 215).

Personuppgiftsbiträde

Uttrycket återfinns i nuvarande lagstiftning (jfr prop. 2018/19:163 s. 215).

Registrerad

Uttrycket återfinns i nuvarande lag (jfr prop. 2018/19:163 s. 215).

Personuppgiftsansvar

6 § Säkerhetspolisen är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.

Den personuppgiftsansvarige är ansvarig för all behandling av personuppgifter som utförs under dennes ledning eller på dennes vägnar.

Bestämmelsen om personuppgiftsansvar motsvarar 1 kap. 6 § i nuvarande lag (jfr prop. 2018/19:163 s. 216 f). Att Polismyndigheten är personuppgiftsansvarig när myndigheten tillämpar lagen följer av 2 § andra stycket.

2 kap. Behandling av personuppgifter

Grundläggande krav på behandling

Proportionalitet

1 § All behandling av personuppgifter ska vara proportionerlig. En behandling är proportionerlig, om skälet för att utföra den överväger intrånget i de enskilda eller allmänna intressen som kan påverkas.

Av paragrafen framgår den grundläggande principen om att den personuppgiftsbehandling som sker med stöd av lagen ska vara proportionerlig. Bestämmelsen följer av artikel 5.1 i dataskyddskonventionen 108+ och saknar motsvarighet i nuvarande lag. De allmänna övervägandena görs i avsnitt 8.

Av *första meningen* följer att all behandling av personuppgifter ska vara proportionerlig. Denna princip får sitt närmare innehåll i andra meningen. Att proportionalitetsprincipen gäller all behandling innebär att den gäller såväl för varje enskild behandlingsåtgärd som för den samlade behandlingen av personuppgifter som sker inom myndigheten över tid. Det är därmed inte tillräckligt att varje behandlingsåtgärd var för sig varit proportionerlig, om den slutliga effekten inte är det.

Av *andra meningen* följer att proportionalitetskravet innebär en avvägning mellan det allmänna intresset av att utföra behandlingen och de enskilda eller allmänna intressen som kan påverkas av den. Innebörden är att en behandlingsåtgärd, exempelvis att samla in och lagra personuppgifter under viss tid, inte får utföras om resultatet av behandlingen innebär en oproportionerlig påverkan på andra intressen. Det innebär också att tungt vägande skäl för att behandla personuppgifter kan motivera betydande intrång i enskilda och allmänna intressen. Bestämmelsen ger uttryck för prin-

cipen att målet med behandlingen ska vägas mot de intressen som åtgärderna påverkar eller inskränker.

Proportionalitetsprövningen ska göras först då det kunnat konstateras att behandlingsåtgärden i och för sig uppfyller ett behov. Det kan aldrig vara proportionerligt att behandla personuppgifter om det inte behövs (se 11 §) eller inte är befogat (se 8 §) för något ändamål.

Skälet för att utföra behandlingen utgörs av ändamålet med personuppgiftsbehandlingen. Vilken tyngd som ska tillmätas intresset av att utföra behandlingen beror på vilket ändamål det handlar om. När skälet för att utföra behandlingen ska bedömas kan det exempelvis vara aktuellt att besvara frågan om hur allvarligt och hur aktuellt hotet som behandlingen syftar till att förebygga är. Skälet för att utföra en behandling som syftar till att avvärja ett nära förestående terrorbrott väger därmed mycket tungt och kan motivera en omfattande personuppgiftsbehandling. Det kan också finnas ett tungt vägande skäl för personuppgiftsbehandling som syftar till att förebygga säkerhetshot på lång sikt. Så kan vara fallet när det handlar om behandling som syftar till kartläggning och klarläggning av antagonistiska aktörer som anammar konspirativa beteenden för att dölja sin verksamhet och bygger förmåga på lång sikt. Det gäller exempelvis främmande makts informationsinhämtning riktad mot Sverige och svenska intressen. Konsekvenserna av säkerhetshoten som bland annat bekämpas inom kontraspionage och säkerhetsskyddet kan ha betydelse mycket långt fram i tiden eller vara av ett sådant slag att varje enskild åtgärd som främmande makt vidtar inte får omedelbara eller direkta följder. Den samlade konsekvensen av den brottsliga verksamheten inom båda dessa områden kan dock vara att Sveriges territoriella integritet, demokratiska statsskick eller andra grundläggande samhälleliga intressen äventyras. Det kan även röra sig om kartläggning av exempelvis framväxten av nya våldsbejakande miljöer som inte tidigare existerat. Även sådana fenomen eller strömningar kan avse säkerhetshot som inte är omedelbara, men som kan ge allvarliga konsekvenser på lång sikt. De långsiktiga konsekvenserna kan i dessa fall återspeglas i skälen för att utföra olika behandlingsåtgärder.

Med de *enskilda eller allmänna intressen* som avvägningen ska göras mot avses i första hand de grundläggande medborgerliga fri- och rättigheterna. Med enskilda intressen avses i första hand den

personliga integriteten som skyddas av 2 kap. 6 § andra stycket regeringsformen och rätten till privatliv som garanteras av artikel 8.1 Europakonventionen. Dessa rättigheter är ett enskilt intresse som påverkas i olika grad av all personuppgiftsbehandling. När Säkerhetspolisen behandlar personuppgifter i sin operativa verksamhet måste utgångspunkten vara att det rör sig om ett intrång i rättigheten, i vart fall om den registrerade på något sätt kan anses vara kartlagd, övervakad eller misstänkliggjord genom åtgärden. Styrkan av den enskildes intresse av att inte få sina uppgifter behandlade kan bero på hur integritetskänsliga uppgifterna är eller om behandlingen av andra skäl innebär ett betydande ingrepp i den enskildes privata sfär (jfr prop. 2009/10:80 s. 250). Även betydande ingrepp kan motiveras, men endast om skälen för behandlingen har tillräcklig tyngd. Behandling av allmänt tillgänglig information som den enskilde delat med sig av frivilligt, exempelvis på internet, utgör till exempel inte ett lika stort intrång i rätten till privatliv som behandling av uppgifter som inhämtats genom avlyssnade, förtroliga samtal efter beslut om hemliga tvångsmedel. Behandling av känsliga personuppgifter utgör ofta ett större intrång i rätten till privatliv än behandling av andra uppgifter. Intrånget i den personliga integriteten uppkommer även om den enskilde inte är eller någonsin kommer bli medveten om personuppgiftsbehandlingen i fråga. Vid sidan av den personliga integriteten kan behandling medföra påverkan på andra enskilda intressen. Vid utlämnande av personuppgifter till andra länder måste exempelvis risken för att den registrerade utsätts för förföljelse eller tortyr beaktas.

Hur känslig en personuppgift är ur ett fri- och rättighetsperspektiv måste bedömas utifrån den kontext inom vilken uppgiften behandlas. En uppgift om exempelvis sexuell läggning är avsevärt mycket mer känslig i ett samhälle där homosexualitet är kriminaliserat eller där HBTQI-personer riskerar förföljelse. Detsamma kan gälla exempelvis uppgifter om politisk uppfattning eller religiös övertygelse. Behandling av en uppgift som framstår som harmlös i ett sammanhang kan utgöra ett stort intrång i ett annat. Detta gäller alla uppgifter, även de som inte tillhör kategorin känsliga personuppgifter.

Även *allmänna intressen* ska beaktas vid prövningen. Redan av regeringsformens portalstadgande följer att den fria åsiktsbildningen är en av pelarna som bär upp den svenska demokratin. Den fria

åsiktsbildningen skyddas bland annat genom de grundläggande fri- och rättigheterna som framgår av 2 kap. 1 § regeringsformen: yttrandefrihet, informationsfrihet, mötesfrihet, demonstrationsfrihet, föreningsfrihet och religionsfrihet. Motsvarande skydd för grundläggande rättigheter finns i Europakonventionen. I tryckfrihetsförordningen och yttrandefrihetsgrundlagen finns ytterligare bestämmelser som ska främja den fria åsiktsbildningen. Det finns en risk att dessa grundläggande fri- och rättigheter på olika sätt påverkas genom att Säkerhetspolisen behandlar personuppgifter. Det sker en påverkan om exempelvis information samlas in om vilka som deltagit i en demonstration eller i en religiös sammankomst, även om det kan finnas goda skäl för denna åtgärd. Att en säkerhetstjänst behandlar eller ges stora möjligheter att behandla personuppgifter om dem som utnyttjat sin opinionsfrihet kan ha en avhållande effekt. Sådan avhållande effekt på den fria åsiktsbildningen och enskildas vilja att utöva sina grundläggande fri- och rättigheter måste vägas in i prövningen. Avvägningen måste göras mot en befarad eller potentiell risk att individer avhåller sig från att utnyttja sina fri- och rättigheter på grund av åtgärden. Det finns inget krav på att en avhållande effekt faktiskt ska ha uppkommit.

Det finns ofta en naturlig koppling mellan påverkan på enskilda och allmänna intressen. I många fall utgör en behandling en påverkan på båda dessa intressen om än på olika sätt och i olika grad. Även om en enskild frivilligt har delat med sig av uppgifter, exempelvis på internet, kan en omfattande behandling av sådana uppgifter utgöra ett betydande intrång i yttrandefriheten.

Proportionalitetsprövningen utgör en central del av personuppgiftsskyddet vid inhämtning av uppgifter som inte är särskilt reglerad. Det är därför viktigt att prövningen får genomslag vid avgränsningen av de uppgifter som samlas eller hämtas in. För hemliga tvångsmedel och framtagning enligt lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar, är proportionalitet en förutsättning som prövas i särskild ordning. En proportionalitetsprövning enligt denna lag ska dock göras även för sådana uppgifter.

Proportionalitetsprövningen ska utgöra en del av alla bedömningar som följer av denna lag, till exempel när principen om uppgiftsminimering tillämpas (se kommentaren till 2 kap. 14 §) och när behandlingstid bestäms (se kommentaren till 4 kap. 1 §). Prövningen

kan resultera i att behandlingen måste justeras till sin omfattning för att få utföras. Ett exempel är att om det finns ett tungt vägande behov som motiverar behandling av en stor mängd personuppgifter, kan behandlingstiden behöva förkortas (i förhållande till behovet) för att minska intrånget i de allmänna och enskilda intressen som påverkas.

Rättslig grund

2 § Personuppgifter får endast behandlas för att bedriva verksamhet som följer av lag, förordning, internationella åtaganden eller särskilt beslut av regeringen.

I paragrafen anges den yttre ramen för när behandling av personuppgifter är tillåten. De allmänna övervägandena görs i avsnitt 8.3. Bestämmelsen innebär att personuppgifter endast får behandlas för ändamål som följer av en rättslig grund**.** Den rättsliga grunden följer inte av denna lag utan måste anges särskilt i lag eller förordning, följa av ett internationellt åtagande eller framgå genom ett särskilt regeringsbeslut. Den rättsliga grunden måste vara beslutad i enlighet med regeringsformen och uppfylla Europakonventionens legalitetskrav. En rättslig grund som står i strid med en överordnad norm kan inte berättiga en personuppgiftsbehandling. Av 12 kap. 10 § regeringsformen följer att om ett offentligt organ finner att en föreskrift står i strid med en bestämmelse i grundlag eller annan överordnad författning får föreskriften inte tillämpas. En regeringsinstruktion som står i strid med exempelvis 2 kap. 21 § regeringsformen kan därför aldrig utgöra en berättigad rättslig grund.

Säkerhetspolisens uppgifter följer bland annat av polislagen (1984:387) och säkerhetsskyddslagen (2018:585), myndighetens instruktion och regleringsbrev. De krav som ställs på en myndighet att exempelvis diarieföra handlingar, samarbeta med andra myndigheter och lämna ut allmänna handlingar utgör också rättslig grund för personuppgiftsbehandling. När det gäller en personuppgift som omfattas av sekretess, är det som sägs i sekretessbestämmelsen rättslig grund för hur uppgiften får behandlas för att lämnas ut (se vidare kommentaren till 3 kap. 1 §). Lagens tillämpningsområde begränsas emellertid, genom 1 kap. 2 §, till brottsbekämpande verksamhet som rör nationell säkerhet.

I 2 kap. 4–7 §§ framgår de övergripande verksamheterna som lagen avser att reglera. Dessa bestämmelser förtydligar vad som följer av kravet på rättslig grund som anges i denna paragraf.

Författningsenlig och korrekt behandling

3 § Personuppgifter ska behandlas författningsenligt och på ett korrekt sätt.

I paragrafen anges att personuppgifter alltid ska behandlas författningsenligt och på ett korrekt sätt. Allmänna överväganden görs i avsnitt 8.5 Paragrafen motsvarar 2 kap. 6 § i nuvarande lagstiftning (jfr prop. 2018/19:163 s. 222 f.).

Verksamheter för behandling av personuppgifter

Underrättelse- och säkerhetstjänst

4 § I sin uppgift att förebygga, förhindra och upptäcka brottslig verksamhet får Säkerhetspolisen behandla personuppgifter för att

1. kartlägga och klarlägga brottslig verksamhet, eller
2. vidta åtgärder som hindrar eller försvårar brottslig verksamhet.

Ändamålet i paragrafen syftar till att beskriva Säkerhetspolisens underrättelse- och säkerhetsverksamhet och saknar direkt motsvarighet i tidigare lag. Motiven finns i avsnitt 8.4.4.

I första ledet av bestämmelsen hänvisas till Säkerhetspolisens uppdrag att förebygga, förhindra och upptäcka brottslig verksamhet. Den brottsliga verksamhet som Säkerhetspolisen ska bekämpa framgår i huvudsak av 3 § polislagen (1984:387) och förordningen (2022:1719) med instruktion för Säkerhetspolisen. I instruktionen framgår även att Säkerhetspolisen i egenskap av säkerhetstjänst bedriver underrättelse- och säkerhetsarbete (1 §).

Underrättelsearbete innebär att information samlas in, bearbetas och analyseras i syfte att identifiera och bedöma om det föreligger ett hot, när det ännu inte finns misstankar om att något konkret brott har begåtts. Underrättelseverksamhet är i huvudsak inriktad på att upptäcka om en viss, inte närmare specificerad brottslighet har ägt rum, pågår eller kan antas komma att begås. Säkerhetsarbete

innebär att åtgärder vidtas för att på olika sätt förhindra att brott genomförs och för att avvärja hot som i förlängningen kan utvecklas till brott. Det kan till exempel omfatta uppgifter som Säkerhetspolisen utför enligt säkerhetsskyddslagstiftningen eller inom ramen för personskyddsverksamheten. Gränsdragningen mellan underrättelse- och säkerhetsarbete är inte alltid tydlig utan sker ofta parallellt.

Första punkten anger att personuppgifter får behandlas för att kartlägga och klarlägga brottslig verksamhet. Det är betecknande för underrättelseverksamhet. Begreppen kartläggning och klarläggning står inte i motsättning till varandra och inget hindrar att ett underrättelseändamål är att både kartlägga och klarlägga viss brottslig verksamhet.

Kartläggning av brottslig verksamhet inom Säkerhetspolisens ansvarsområde innebär ofta att personuppgifter som inte har någon tydlig koppling till en konkret brottslig gärning behöver behandlas. Kartläggningen kan avse sammanhang eller företeelser i sin helhet. För att kartlägga krävs i många fall att samtliga personuppgifter som förekommer i ett visst avgränsat sammanhang behandlas. Om exempelvis kartläggning sker av en våldsbejakande miljö, kan samma ändamål omfatta samtliga personuppgifter som förekommer i sammanhanget. Ett sådant sammanhang kan exempelvis vara meddelanden från ett nätforum, kommunikation och fotografier från ett it-beslag eller överskottsinformation från ett ärende där hemliga tvångsmedel använts för inhämtning. Vid en kartläggning kan det finnas behov av samtliga uppgifter i ett sådant sammanhang. Exempelvis kan alla personuppgifter som finns i en mobiltelefon som beslagtagits från en person misstänkt för terrorism behövas för kartläggning av dennes nätverk.

Det krävs inte att varje enskild personuppgift går att koppla direkt till den brottsliga verksamheten som kartläggs. Kartläggningen utmärks av att varje enskild informationsdel inte behöver bedömas för sig, utan att bedömningen kan ske avseende en viss kontext eller källa.

Att *klarlägga* en brottslig verksamhet innebär att avslöja okända eller dolda förhållanden. Om en kartläggning syftar till att ge en översikt, innebär klarläggning att insatser fokuseras mot den del av den brottsliga verksamheten där misstankarna är mer konkretiserade. Ett exempel på ett klarläggande är när personuppgifter behandlas

i samband med preventiv tvångsmedelsanvändning enligt lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott. Andra exempel är olika spaningsåtgärder som vidtas i underrättelseverksamhet i samband med att den inriktas mot vissa personer snarare än vissa företeelser eller miljöer.

Av *andra punkten* i paragrafen framgår att personuppgifter får behandlas för att vidta åtgärder som hindrar eller försvårar brottslig verksamhet.

Att *hindra* brottslig verksamhet innebär att åtgärder, som inte utgör förundersökning, vidtas för att förebygga att en brottslig gärning begås. Det kan exempelvis ske genom åtgärder enligt lagen (2022:700) om särskild kontroll av vissa utlänningar. Att Säkerhetspolisen på olika sätt agerar för att en åtalsimmun underrättelseofficer ska förklaras *persona non grata* innebär också att brottslig verksamhet hindras. Ett annat exempel på hindrande av brottslig verksamhet är det uppsökande arbetet som Säkerhetspolisen bedriver mot personer i vissa miljöer, genom bland annat avrådande samtal där myndigheten ger sig till känna för personer som befinner sig i risk för radikalisering.

Att *försvåra* brottslig verksamhet utgörs av olika brottsförebyggande åtgärder, personskyddsverksamhet och åtgärder enligt bland annat säkerhetsskyddslagen (2018:585). Säkerhetsskyddsarbete och andra åtgärder för att försvåra brottslig verksamhet kan ske trots att det inte finns kännedom om någon pågående brottslig verksamhet. Personuppgifter kan i dessa fall behöva behandlas inte endast avseende aktörer som hotar svensk säkerhet utan även avseende personer som riskerar att utsättas för eller vara föremålet för sådan brottslig verksamhet.

Trots att behovet av varje enskild personuppgift inte behöver motiveras vid personuppgiftsbehandling som sker i underrättelseverksamhet krävs att behandlingen är proportionerlig, se kommentaren till 2 kap. 1 §.

Brottsutredning och lagföring

5 § Personuppgifter får behandlas för att utreda och lagföra brott.

Paragrafen anger att personuppgifter får behandlas inom förundersökning och andra utredningar som sker enligt rättegångsbalken.

Paragrafen motsvarar nuvarande 2 kap. 1 § 2 (jfr prop. 2018/19:163 s. 218) med den skillnaden att det inte längre hänvisas till vissa brott. Lagens tillämpningsområde begränsas emellertid, genom 1 kap. 2 §, till brottsbekämpande verksamhet som rör nationell säkerhet. Motiven till bestämmelsen finns i avsnitt 8.4.5.

Övrig verksamhet

6 § Personuppgifter får behandlas för annan verksamhet som bedrivs enligt 2 §.

Paragrafen motsvarar bestämmelsen i nuvarande 2 kap. 1 § 4 och 5 och ger förutsättningar för personuppgiftsbehandling inom lagens tillämpningsområde för ändamål som inte följer direkt av 4 eller 5 § (jfr prop. 2018/19:163 s. 219). Motiven finns i avsnitt 8.4.6.

Av paragrafen följer att det vid sidan av den brottsbekämpande kärnverksamheten kan finnas andra rättsliga grunder för Säkerhetspolisens personuppgiftsbehandling. Bestämmelsen förtydligar att det inte endast är inom de verksamheter som anges i 4 och 5 §§ som personuppgifter får behandlas.

I 2 § anges att uppdrag att bedriva viss verksamhet kan följa av lag, förordning, internationella åtaganden eller särskilt beslut av regeringen. Ändamålet måste alltså vara förenligt med den verksamhet som ska bedrivas enligt en rättslig grund. Olika uppdrag som rör brottsbekämpning avseende nationell säkerhet, i vid mening, följer av bland annat utlännings- och medborgarskapslagstiftningen eller den så kallade TCO-förordningen, (EU) 2021/784, som rör avlägsnande av terrorisminnehåll från internet. Paragrafen omfattar även exempelvis personuppgiftsbehandling till följd av informationsutbyte med motsvarande myndigheter i andra stater som sker till gagn för den utländska myndigheten (jfr prop. 2018/19:163 s. 219).

7 § Säkerhetspolisen får behandla personuppgifter för att fortlöpande utveckla den teknik och metodik som behövs inom denna lags tillämpningsområde (utvecklingsändamål).

Personuppgifter som behandlas endast för utvecklingsändamål får inte behandlas för något annat ändamål.

Paragrafen klargör att personuppgifter får behandlas för att utveckla teknik och metoder inom denna lags tillämpningsområde. Para-

grafen saknar motsvarighet i nuvarande lag. Övervägandena finns i avsnitt 8.4.6.

Av *första stycket* framgår att Säkerhetspolisen får behandla personuppgifter för att bland annat utveckla, testa och utvärdera teknik eller metodik som är avsedd för att bekämpa brott som rör nationell säkerhet. Teknisk utveckling kan handla om att texter av olika slag används för att utvärdera eller vidareutveckla översättningstjänster eller att bildmaterial används för att träna mjukvara som kan identifiera vapen. Det kan även handla om att data används för att träna så kallade AI-modeller för att förbättra myndighetens tekniska förmåga i olika avseenden. Att personuppgifter får behandlas för utvecklingsändamål innebär att personuppgifter som inte har någon koppling till myndighetens brottsbekämpande uppdrag kan behandlas. En förutsättning är dock att den tekniska utvecklingen sker för Säkerhetspolisens brottsbekämpande verksamhet som rör nationell säkerhet. Att personuppgifter får användas för metodutveckling innebär att det är möjligt att exempelvis behandla personuppgifter för att utföra simuleringar eller övningar.

Av *andra stycket* framgår att personuppgifter som behandlats endast för utvecklingsändamål inte får behandlas för något annat ändamål. Det innebär att inledande behandling för utvecklingsändamål medför att personuppgifterna inte får behandlas inom underrättelseverksamheten eller för att utreda brott. Av 5 kap. 6 § framgår att tillgången till personuppgifter ska begränsas till vad var och en behöver för att utföra sina arbetsuppgifter.

Personuppgiftsbehandling måste som regel upphöra i samband med att utvecklingsändamålet har uppnåtts. Det innebär att så kallad träningsdata exempelvis inte får behandlas längre än vad som behövs för ändamålet. Om exempelvis en språkmodell har utvecklats med hjälp av personuppgifter, får modellen givetvis fortsätta att användas även efter att personuppgifterna inte längre får behandlas.

Av 12 § andra stycket 1 framgår att utveckling får ske även med hjälp av uppgifter som inledningsvis behandlats för något annat ändamål.

Vid tillämpningen av denna paragraf ska, i likhet med all behandling, en proportionalitetsprincip tillämpas, se 2 kap. 1 § och kommentaren till den paragrafen. Proportionalitetsprincipen begränsar bland annat vilket slag och hur många uppgifter som får behandlas, hur länge och på vilket sätt. Att intrånget i enskilda och allmänna

intressen måste vägas mot ändamålet med behandlingen påverkar bland annat valet av uppgifter och hur många som får tillgång till dem. Anonymisering eller pseudonymisering av uppgifter är åtgärder som måste övervägas vid denna prövning.

Det är viktigt att möjliggöra tillsyn av den behandling som sker för ändamål enligt denna paragraf. Det innebär bland annat att det kan krävas dokumentation och spårbarhet för personuppgifter som behandlas för teknisk utveckling, se kommentaren till 5 kap. 2 §.

Inledande behandling

8 § Inledande behandling av personuppgifter får ske, om det är befogat för ett ändamål inom någon av de verksamheter som anges i 4–7 §§.

Vid inledande behandling tillämpas inte 13–16 §§.

Paragrafen reglerar behandlingströskel och ändamål för inledande behandling. Paragrafen saknar motsvarighet i nuvarande lagstiftning. Inledande behandling definieras i 1 kap. 5 § och avser bland annat insamling av personuppgifter. Motiven till bestämmelsen finns i avsnitt 8.6.

Av paragrafens *första stycke* följer att inledande behandling endast får ske om det är befogat för ett eller flera ändamål inom de verksamheter som anges i 4–7 §§. Behandlingströskeln, eller behovskriteriet, för inledande behandling är att åtgärden ska vara befogad.

Befogat är ett lägre krav än behövs, som används i 11 §. Uppgifterna ska vara skäliga att behandla i förhållande till ändamålet för den inledande behandlingen. Att behandlingen av uppgifterna ska vara befogad innebär att det måste finnas något som ger stöd för att personuppgifterna som ska inhämtas är relevanta att behandla för ändamålet. Det krävs däremot inte någon sannolikhetsövervikt för att varje uppgift verkligen behövs. Det finns därmed inget krav på att det exempelvis ska finnas belagda misstankar om att någon för Säkerhetspolisen känd aktör förekommer bland de uppgifter som samlas in. Det är tillräckligt att det finns skäl att för det angivna ändamålet undersöka om någon känd aktör förekommer. Inledande behandling får också ske för att söka efter företeelser och hot som är okända men som antas existera. Det kan exempelvis vara befogat att inhämta en läckt databas för att undersöka dess innehåll i förhållande till ett givet ändamål.

Det uppställs inte något krav på ett särskilt och uttryckligt angivet ändamål för inledande behandling. För inledande behandling är kravet på konkretion lägre än ett sådant ändamål som krävs för behandling enligt 11 §. Att behandlingsändamålet ska anges inom någon av de verksamheter som anges i 4–7 §§ innebär att verksamheterna inte i sig är tillräckliga för att inleda behandling. Ändamålet måste inrymmas inom någon av de författningsreglerade verksamheterna och det måste utifrån ändamålet vara möjligt att bedöma om den inledande behandlingen är befogad och om den är proportionerlig (se 1 §). För exempelvis underrättelseinhämtning kan ändamålet avse en viss slags brottslig verksamhet.

Ett mer specifikt ändamål kan emellertid ge förutsättningar till inledande behandling av en större mängd uppgifter, eller uppgifter av känsligare slag, i jämförelse med ett brett formulerat ändamål. Om intrånget i motstående intressen är substantiellt krävs det vid proportionalitetsprövningen ett ändamål av viss tyngd, vilket endast är möjligt att konstatera om det är tillräckligt specifikt.

I *andra stycket* anges att vissa bestämmelser om personuppgifters kvalitet inte ska tillämpas vid inledande behandling. Däremot ska bestämmelserna i bland annat 17 § tillämpas även vid den inledande behandlingen.

I lagen om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar finns regler om att uppgifter som vid inledande behandling har behandlats för ett ändamål under vissa förhållanden kan registreras i en särskild uppgiftssamling enligt samma krav.

Inledande granskning

9 § Efter inledande behandling ska personuppgifter granskas, om det behövs för att säkerställa författningsenlig behandling. Innan granskningen har genomförts får personuppgifterna behandlas endast för granskningsändamål.

Granskningen enligt första stycket ska ske så snart det är möjligt och får inte pågå längre än nödvändigt. Sådan behandling får pågå i högst sex månader.

Granskningen ska utföras av särskilt angivna tjänstemän som har tillräckliga kunskaper för uppgiften. Under granskningen ska tillgången till uppgifterna vara begränsad till vad var och en behöver för att fullgöra uppgiften.

Paragrafen är ny och innehåller bestämmelser om den granskning av personuppgifter som ska ske efter inledande behandling. Motiven framgår av avsnitt 8.12. Inledande behandling definieras i 1 kap. 5 §.

Av *första stycket* framgår att det efter inledande behandling endast är tillåtet att behandla personuppgifter för att granska om uppgifterna kan fortsätta att behandlas författningsenligt. Behandling för andra ändamål, inklusive ändamålet för den inledande behandlingen, är inte tillåtet förrän sådan granskning genomförts. Det innebär exempelvis att uppgifter inte får delges eller tillgängliggöras operativt innan de granskats och det säkerställts att sådan behandling är författningsenlig. Se kommentaren till 11 §.

Av 8 § framgår att behandlingströskeln och kraven på ändamål är lägre för inledande behandling än för annan personuppgiftsbehandling. Granskningen syftar till att fortsatt behandling endast sker av personuppgifter som uppfyller de högre kraven i 11 §. Kravet på granskning gäller endast om det behövs för att säkerställa författningsenlig behandling. Om det är klart att den inledande behandlingen är förenlig med de krav som ställs även för efterföljande behandling, behöver inte uppgifterna granskas. Så kan vara fallet exempelvis då inhämtning sker från databaser där uppgiftsinnehållet till sin typ är känt och det står klart att fortsatt behandling är författningsenlig.

Av *andra stycket* framgår att granskning ska ske så snart som möjligt och inte pågå längre än nödvändigt. Det innebär att granskningen både ska påbörjas och avslutas så snart det är möjligt. Hur länge granskning kan anstå beror bland annat på omständigheterna kring den inledande behandlingen. Om Säkerhetspolisen fått del av ett stort material från en samverkande tjänst eller genomfört ett stort beslag kan prioriteringar i verksamheten medföra att granskning av vissa uppgifter kan behöva anstå en tid. För mer rutinbetonad inledande behandling bör det dock finnas kapacitet att löpande granska uppgifterna. Den yttre gränsen för behandling som sker för granskning är sex månader. Det finns inte några möjligheter att förlänga den tid som granskning får pågå.

Av *tredje stycket* framgår behörighetskraven för att granska uppgifter och hur tillgången till uppgifterna ska begränsas till de som ska utföra granskning. Att granskning endast får ske av särskilt angivna tjänstemän innebär att det genom arbetsordningen framgår att behörigheten följer av viss tjänst eller att uppgiften kan delege-

ras till en medarbetare genom särskilt beslut. Kravet på tillräckliga kunskaper innebär att granskning endast får utföras av de som har kompetens att utföra samtliga prövningar som krävs för att tillförsäkra att personuppgifter behandlas författningsenligt. Det innefattar bland annat proportionalitetsprövningen i 1 §.

Inledande behandling omfattar även personuppgifter som upprättas eller på andra sätt skapas inom myndigheten. Det innefattar exempelvis att en medarbetare nedtecknar personuppgifter i en promemoria. I dessa fall kommer granskningen inte att vara separerad från den inledande behandlingen. Vilka kompetenskrav som ställs för granskning beror på vad granskningen avser. Kraven är att medarbetaren har tillräckliga kunskaper för uppgiften. För personuppgifter som medarbetaren själv upprättat, exempelvis genom att skriva en promemoria, är kravet på tillräckliga kunskaper lägre än för att granska insamlade eller inhämtade uppgifter.

Att det är särskilt angivna tjänstemän som ska utföra granskning innebär inte något krav på att endast ett fåtal eller en begränsad krets medarbetare får ha behörighet att utföra uppgiften. Det finns till exempel inget som hindrar att det är operativ personal som genomför personuppgiftsgranskningen i samband med att uppgifterna analyseras. Detta förutsätter dock att kompetenskravet i paragrafen är uppfyllt för den medarbetaren. Kravet på att granskningen ska utföras av en tjänsteman innebär att det inte är möjligt med helt automatiserad granskning. Fortsatt behandling av personuppgifter efter granskningen sker därmed under individuellt tjänsteansvar. Det hindrar inte att olika verksamhetsstöd används av tjänstemannen för att granska uppgifterna, så länge beslutet om fortsatt behandling inte sker helt automatiserat.

Av andra meningen följer att det under granskningen ska säkerställas att tillgången till uppgifterna begränsas till de som faktiskt behöver tillgång för att utföra granskningen.

10 § De befattningshavare vid Säkerhetspolisen som regeringen föreskriver får besluta att personuppgifter som behandlas med stöd av 9 § även får behandlas av andra tjänstemän och för andra ändamål än granskning, om det är absolut nödvändigt för att fullgöra en uppgift av synnerlig vikt.

Behandling enligt första stycket får pågå i högst trettio dagar och tillgången till sådana personuppgifter ska vara strikt begränsad till vad var och en behöver för att fullgöra uppgiften.

Beslut enligt första stycket ska dokumenteras och omedelbart anmälas till den särskilda tillsynsmyndigheten.

Paragrafen reglerar ett undantag från de begränsningar som följer av 9 § för behandling av uppgifter efter inledande behandling. Bestämmelserna saknar motsvarighet i nuvarande lagstiftning. Övervägandena finns i avsnitt 8.12.5.

De befattningshavare som regeringen föreskriver får, enligt *första stycket*, möjlighet att upphäva begränsningarna i 9 § om att uppgifter måste granskas av särskilt angivna tjänstemän innan de får behandlas operativt. Om det är absolut nödvändigt för att fullgöra en uppgift av synnerlig vikt, får uppgifterna, behandlas för operativa ändamål även utan att de granskats. Detta får då ske direkt efter inledande behandling enligt 8 § och utan att tillgången begränsas till särskilt angivna tjänstemän. Det innebär att det är tillåtet att bland annat spara, överföra, bearbeta, analysera och delge uppgifter utan att personuppgifterna dessförinnan granskats och utan att uppgifterna prövats mot de strängare kraven angående bland annat behov och ändamål, som följer av 11 §. Däremot måste den behandling som görs av uppgifterna uppfylla kravet på proportionalitet i 1 §. Behandling får endast ske för det ändamål som motiverat undantaget. Det innebär att exempelvis att alla inhämtade uppgifter får analyseras, men endast för det ändamål som motiverat undantaget.

Ändamålet måste avse en uppgift som är av synnerlig vikt. Att en uppgift är av synnerlig vikt innebär att behandling får ske för att exempelvis förhindra ett allvarligt och akut hot mot nationell säkerhet. Det kan exempelvis handla om att det finns trovärdig information om ett nära förestående terrorbrott och att uppgifter som inhämtas på olika sätt omedelbart måste behandlas för att identifiera potentiella gärningsmän. Det kan också handla om att ett terrorbrott har genomförts och att uppgifter behöver inhämtas omedelbart för att identifiera och spåra gärningspersoner och eventuella medhjälpare, samt för att förhindra eventuella ytterligare nära förestående terrorbrott som har samband med det begångna terrorbrottet. Behandlingen ska vidare vara absolut nödvändig för att uppgiften ska kunna utföras. Det innebär att det inte ska vara möjligt att utföra uppgiften utan att behandla personuppgifterna med stöd av undantagsbestämmelsen. Det ska finnas en allvarlig risk för att inledande granskning av uppgifterna, enligt 9 §, skulle förfela ändamålet med behandlingen. Behovet av behandlingen ska därför vara tidskritiskt eller på annat sätt vara så angeläget att inledande granskning framstår som oförenligt med behovet av att ut-

föra behandlingen. En sådan behandling kan vara att tillgängliggöra uppgifter till en vidare krets eller att överföra information till andra brottsbekämpande myndigheter eller samverkande tjänster.

Ett beslut enligt första stycket ska vara begränsat till de personuppgifter som behövs för att fullgöra arbetsuppgiften. Däremot behöver de personuppgifter som ska behandlas inte finnas tillgängliga för Säkerhetspolisen då beslutet fattas. Ett beslut kan avse uppgifter där inledande behandling ännu inte skett likväl som uppgifter som redan finns inom myndigheten. Undantaget avser den arbetsuppgift av synnerlig vikt som behandling ska ske för.

Av *andra stycket* framgår att undantag från granskning får pågå i högst trettio dagar. Om det inom denna tid är möjligt att i stället uppnå ändamålet genom att behandla uppgifter som granskats, ska undantagsbeslutet upphävas utan dröjsmål. Vidare framgår att tillgången till de personuppgifter som omfattas av undantaget ska vara strikt begränsad till de medarbetare som behöver dem för att utföra den uppgift som motiverat undantaget. Det kan exempelvis handla om att vissa analytiker får möjlighet att behandla en större mängd lagrad elektronisk kommunikation för att utföra vissa bearbetningar och analyser. När ändamålet är uppnått, eller det kan konstateras att det inte är möjligt att uppnå det, ska behandling av och tillgång till personuppgifterna som omfattas av undantagsbeslutet åter begränsas enligt 9 §.

Enligt *tredje stycket* ska beslutet avfattas skriftligt. Vidare framgår att en anmälan omedelbart ska göras till den särskilda tillsynsmyndigheten. Det innebär att den särskilda tillsynsmyndigheten ska underrättas om att beslut är fattat och vad som medges till följd av detta. Det finns däremot inte något krav på att beslutet ska expedieras. En anmälan kan därför ske muntligen. Av 7 kap. 8 § följer att det är Säkerhets- och integritetsskyddsnämnden som är den särskilda tillsynsmyndigheten.

Fortsatt behandling

11 § Efter inledande granskning får personuppgifter behandlas endast om det behövs för ett särskilt, uttryckligt angivet och berättigat ändamål.

Av paragrafen följer att fortsatt behandling av uppgifter som inhämtats eller på annat sätt inkommit till myndigheten endast får

ske om det behövs för ett konkretiserat ändamål. Bestämmelsen innehåller den generella behandlingströskeln för personuppgiftsbehandling och fastställer att ändamålsprincipen ska gälla för sådan behandling. Paragrafen saknar direkt motsvarighet i nuvarande lagstiftning. Övervägandena finns i avsnitt 8.7.

Paragrafen anger en behandlingströskel som innebär att personuppgifter som behandlas ska *behövas* för att myndigheten ska kunna utföra den arbetsuppgift som följer av ändamålet. Det innebär att det ska finnas ett konkret behov av de uppgifter som behandlas. Begreppet ”behövs” ska i denna bestämmelse ges en självständig betydelse i förhållande till begreppet ”nödvändigt” som återfinns i dataskyddsförordningen och de lagar som genomför EU:s brottsdatadirektiv.

Prövningen av om personuppgifter behövs eller inte avgörs i stor utsträckning av för vilket ändamål de behandlas. I en förundersökning behöver i huvudsak personuppgifter som rör den brottslighet som utreds behandlas. I underrättelseverksamhet kan däremot alla personuppgifter som förekommer i ett visst avgränsat sammanhang behövas för kartläggningen av en viss brottslig verksamhet.

Av paragrafen följer även ändamålsprincipen. Efter inledande behandling krävs att uppgifterna behövs för ett särskilt, uttryckligt angivet och berättigat ändamål. Att ändamålet ska vara *särskilt* innebär att det måste vara tillräckligt preciserat för att det ska kunna avgöras om de personuppgifter som behandlas är adekvata och relevanta för ändamålet med behandlingen eller om för många personuppgifter behandlas, se 14 §. Genom att ändamålet konkretiserar nyttan med att behandla uppgifterna möjliggörs den proportionalitetsprövning som krävs enligt 1 §. Det ändamål som anges för efterföljande behandling är avgörande för proportionalitetsprövningen av bland annat registrering och fortsatt bevarande av uppgiften. Om sådan behandling är känslig ur integritetssynpunkt, krävs ett specifikt ändamål för att kunna genomföra prövningen och för att kunna komma till slutsatsen att detta ändamål väger över de intressen som påverkas. Om intrånget i andra skyddsvärda intressen är substantiellt, krävs det vid proportionalitetsprövningen ett ändamål av viss tyngd, vilket endast är möjligt att konstatera om det är tillräckligt specifikt. Även det särskilda ändamålet måste anges inom de verksamheter som anges i 4–7 §§. Kravet på att ändamålet ska vara särskilt innebär att det måste vara mer konkret och mer

preciserat än vad som är fallet för inledande behandling enligt 8 §. Kravet på ett särskilt, uttryckligt angivet och berättigat ändamål för fortsatt behandling är därför kvalitativt högre än det ändamål som krävs för att få inleda behandling. Ändamålet får alltså inte vara så vagt eller vittomfattande att de prövningar som krävs enligt lagen i praktiken inte blir möjliga att utföra. Ett avgränsat underrättelsearbete kan utgöra ett ändamål. Ett särskilt ändamål kan därmed exempelvis vara en kartläggning av ett visst terroristnätverk i Sverige eller utomlands eller en hotbildsbedömning av en utpekad skyddsperson. Något hinder mot att ange flera parallella ändamål för behandlingen finns inte. Samma krav ställs emellertid för varje ändamål som angivits. Det finns inget krav på att bedömningen ska dokumenteras.

Att ändamålet ska vara *berättigat* innebär att arbetsuppgiften eller verksamhet som Säkerhetspolisen ska utföra måste ha en rättslig grund och att ändamålet ska ha en tydlig koppling till denna verksamhet. Ett berättigat ändamål ska vara förenligt med konstitutionella och andra rättsliga principer. Det innebär att den rättsliga grunden måste vara av den kvalitet som regeringsformen och Europakonventionen uppställer för fri- och rättighetsintrång. Personuppgiftsbehandling grundat på ett beslut från regeringen måste exempelvis avse ett område inom regeringens kompetens.

Finalitetsprincipen

12 § Personuppgifter får inte behandlas för ett ändamål som är oförenligt med ändamålet för den inledande behandlingen.

Första stycket hindrar dock inte att personuppgifter som behandlas enligt 4–6 §§ behandlas för

1. utvecklingsändamål enligt 7 §,
2. vetenskapliga, statistiska eller historiska ändamål inom denna lags tillämpningsområde, eller
3. diarieföring, handläggning och liknande verksamhet inom denna lags tillämpningsområde.

Av paragrafen följer att den så kallade finalitetsprincipen ska tillämpas. Delvis motsvarande bestämmelse återfinns i 2 kap. 3 § andra meningen i nuvarande lag (jfr prop. 2018/19:163 s. 220). De allmänna övervägandena görs i avsnitt 8.8.

I *första stycket* anges huvudregeln att personuppgifter inte får behandlas för något nytt ändamål som är oförenligt med ändamålet för den inledande behandlingen. Av 8 § följer att ändamålet för inledande behandling inte behöver formuleras lika konkret som ändamål för fortsatt behandling. Inom Säkerhetspolisens brottsbekämpande verksamhet kan behandling av personuppgifter för nya ändamål i de allra flesta fall anses förenlig med ändamålet för den inledande behandlingen. Den brottsbekämpande verksamheten som rör nationell säkerhet utmärks av att den i princip avser att skydda statens väsentliga funktioner och samhällets grundläggande intressen. Det innebär att behandling som inletts för ändamål inom exempelvis kontraspionaget är förenliga även med ändamål inom kontraterrorismverksamheten.

Av *andra stycket* framgår att personuppgifter får behandlas för utvecklingsändamål och vetenskapliga, statistiska eller historiska ändamål och administration utan hinder av första stycket.

Vad som avses med utvecklingsändamål enligt *punkten 1* anges i 7 §. Personuppgifter som behandlas inom exempelvis kontraterrorismverksamheten får användas även vid teknikutveckling. *Av punkten 2* följer att forskning får bedrivas på insamlade personuppgifter. Det är endast vetenskapliga, statistiska eller historiska ändamål inom lagens tillämpningsområde som omfattas av undantaget i andra stycket. I *punkten 3* förtydligas att den personuppgiftsbehandling som sker för att uppfylla administrativa krav på en myndighet aldrig kan anses oförenlig med ändamålet för inledande behandling. Bestämmelsen motsvarar nuvarande 2 kap. 2 § (jfr prop. 2018/19:163 s. 219).

Vid sidan av prövningen om oförenliga ändamål ska en proportionalitetsprövning enligt 1 § göras för behandling som sker för nya ändamål. Även behandling för ändamål som är förenliga kan vara oproportionerlig, om konsekvensen för ett enskilt eller allmänt intresse inte är rimligt i förhållande till intresset av att behandla uppgifterna för det nya ändamålet.

Personuppgifters kvalitet

Korrekta uppgifter

13 § Personuppgifter som behandlas ska vara korrekta och, om det är nödvändigt, uppdaterade.

Paragrafen motsvarar nuvarande 2 kap. 7 § första stycket (jfr prop. 2018/19:163 s. 223). Det nuvarande andra stycket har tagits bort utan att någon förändring i sak är avsedd, se kommentaren till 14 §. Förändringen motiveras i avsnitt 8.10.3.

Prövningen enligt denna paragraf sker vid inledande granskning, se 9 §. Om det i ett senare skede framgår att en uppgift inte är korrekt eller uppdaterad, ska det åtgärdas, se 5 kap. 1 §.

Uppgiftsminimering

14 § Personuppgifter som behandlas ska vara adekvata, relevanta och inte för omfattande i förhållande till ändamålet med behandlingen.

Av paragrafen följer kravet på adekvans, relevans och principen om uppgiftsminimering. Bestämmelsen motsvarar delvis 2 kap. 8 § i nuvarande lagstiftning (jfr prop. 2018/19:163 s. 223 f). Den allmänna motiveringen återfinns i avsnitt 8.10.2.

Av *första ledet* framgår kravet på att endast adekvata och relevanta personuppgifter får behandlas. Det är i huvudsak ändamålen för behandling som avgör om en uppgift är adekvat eller relevant. Det innebär att bedömningen är olika om det rör sig om uppgifter som behandlas i en förundersökning, där ändamålet utgörs av misstanke om en konkret gärning, eller uppgifter inom underrättelseverksamhet där det inte är lika tydligt vari den brottsliga verksamheten eller säkerhetshotet består. Som angetts i kommentaren till 4 § kan uppgifter vara adekvata och relevanta att behandla, eftersom de förekommer i en viss kontext eller ett sammanhang som i sin helhet behövs för kartläggningen av viss närmare angiven brottslig verksamhet. Bedömningen behöver i dessa fall inte ske för varje enskild personuppgift. När Säkerhetspolisen beskriver en persons utseende är det endast adekvat att det sker på ett objektivt sätt med respekt för människovärdet.

Av *sista ledet* följer principen om uppgiftsminimering. Vid bedömningen av mängden personuppgifter som får behandlas för ändamålet ska hänsyn inte tas enbart till behovet. Av 1 § framgår att det även ska beaktas att behandlingen utgör en rimlig balans mellan ändamålet för att behandla uppgifterna och andra intressen som påverkas. Även om en stor mängd personuppgifter i och för sig kan behövas, för att exempelvis kartlägga en brottslig verksamhet, kan proportionalitetsprövningen utmynna i att omfattningen måste begränsas för att uppnå proportionalitet. Om det exempelvis handlar om kommunikationsuppgifter från ett it-beslag, kan fortsatt behandling behöva begränsas till uppgifterna från en viss tidsperiod eller mellan vissa personer.

Omfattningen avser inte endast mängden uppgifter. I begreppet finns även en kvalitativ aspekt som innebär att uppgifter inte får vara mer känsliga ur ett fri- och rättighetsperspektiv än nödvändigt. Det innebär att uppgifter som utgör ett stort integritetsintrång inte får behandlas, om det är tillräckligt att behandla mindre känsliga uppgifter.

Ett tillräckligt konkret ändamål och som avser ett tungt vägande allmänintresse kan under vissa omständigheter möjliggöra behandling av en större mängd uppgifter. Exempelvis kan ett stängt diskussionsforum på internet för personer som planerar att resa för att ansluta sig till en terroristorganisation vara adekvat och relevant att behandla i sin helhet, även om varje personuppgift som förekommer där inte går att koppla till någon känd brottslig verksamhet. Principen om uppgiftsminimering får i detta fall mindre betydelse än om det rör sig om sammanhang som inte har en lika tydlig koppling till brottslig verksamhet.

I vissa fall kan inledande behandling ske av fler uppgifter än vad som behövs för ändamålet. Det kan exempelvis vara nödvändigt att inhämta en större mängd uppgifter för att inte direkt avslöja vilka individer som är av intresse för myndigheten. I dessa fall får fortsatt behandling endast ske för de uppgifter som är relevanta för ändamålet.

Prövningen enligt denna paragraf sker vid inledande granskning, se 9 §. Om det i ett senare skede framgår att en uppgift inte är adekvat eller relevant eller för omfattande i förhållande till ändamålet, ska behandlingen upphöra, se 5 kap. 1 §.

Särskilda upplysningar

15 § Om det ändamål som personuppgifter behandlas för inte framgår av sammanhanget eller på något annat sätt, ska det tydliggöras genom en särskild upplysning.

Paragrafen motsvarar nuvarande 3 kap. 3 § med den skillnad att den gäller alla uppgifter och inte endast de som gjorts gemensamt tillgängliga (prop. 2018/19:163 s. 231 och 2009/10:85 s. 369 f). Den allmänna motiveringen finns i avsnitt 8.13.3.

Kravet på att den särskilda upplysningen ska tillföras gäller efter att inledande granskning enligt 9 § har avslutats. Upplysningen kan ofta avse samtliga uppgifter som förekommer i en kontext, om ändamålet inte framgår redan av sammanhanget.

16 § När personuppgifter behandlas för att utreda och lagföra brott som Säkerhetspolisen ansvarar för, ska personuppgifter som rör olika kategorier av registrerade så långt det är möjligt särskiljas. Genom särskiljningen ska det framgå om personen är misstänkt, dömd för brott, brottsoffer eller någon annan som berörs av ett brott.

Om det inte framgår av sammanhanget eller på annat sätt till vilken kategori personen hör, ska det tydliggöras genom en särskild upplysning.

Paragrafen är ny i förhållande till nuvarande lagstiftning. I 2 kap. 9 § brottsdatalagen (2018:1177) finns närliggande krav som gäller då Säkerhetspolisen behandlar personuppgifter med stöd av den lagstiftningen och lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område (jfr prop. 2017/18:232 s. 445 f.). Överväganden finns i avsnitt 8.13.6.

Bestämmelsen gäller endast uppgifter som behandlas för att utreda och lagföra brott. När personuppgifter behandlas i förundersökning följer ofta de olika kategorierna av registrerade av hur uppgifterna struktureras i ärendet och av de krav som gäller enligt annan författning, exempelvis 21 § förundersökningskungörelsen (1947:948). Om uppgifter även behandlas för att exempelvis kartlägga brottslig verksamhet, gäller kravet endast när uppgifterna behandlas för att utreda och lagföra brott.

Bestämmelsen gäller så långt det är möjligt. Detta innebär till exempel att det beror på vilket systemstöd som de aktuella personuppgifterna behandlas med. När personuppgifter behandlas i ett system där själva förundersökningsprotokollet genereras, är möjlig-

heterna att särskilja roller goda och behovet stort. När uppgifter från ett it-beslag som inhämtats inom en förundersökning analyseras med hjälp av ett analysprogram, är däremot möjligheterna att göra det ofta begränsade och det finns inte heller samma behov av att särskilja de olika rollerna i det systemet. Bestämmelsen riktar således in sig främst på uppgifter som behandlas i själva förundersökningsprotokollet.

Särskilda kategorier av personuppgifter

Känsliga personuppgifter

17 § Uppgifter om en person får inte behandlas enbart utifrån sådant som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller uppgifter som rör hälsa, sexualliv eller sexuell läggning.

Första stycket hindrar inte behandling av personuppgifter som har lämnats till Säkerhetspolisen i en anmälan, ansökan eller liknande.

Paragrafen har fått en ny utformning i förhållande till nuvarande 2 kap. 9 § och utgör en del av det förstärkta skyddet för känsliga personuppgifter. Bestämmelsen förbjuder personuppgiftsbehandling, exempelvis genom att föra register, på den grund att individen går att hänföra till en viss grupp inom de uppräknande kategorierna. Motiven till bestämmelsen finns i avsnitt 8.15.

Av *första stycket* framgår att det är förbjudet med behandling som sker *enbart* utifrån uppgifter som avslöjar exempelvis etniskt ursprung eller religiös övertygelse. Det är därmed inte tillåtet att exempelvis samla in och bevara uppgifter enbart på grund av att personen har viss etnicitet eller är medlem av en viss församling. Att sådan omständighet inte får vara skälet till att en persons personuppgifter behandlas innebär inte att det är förbjudet att behandla sådana uppgifter. Säkerhetspolisen har ofta anledning att behandla uppgifter om bland annat politiska åsikter. Exempelvis avseende skyddspersoners partitillhörighet eller då våldsbejakande extremistmiljöer kartläggs. I dessa fall är inte de politiska åsikterna grunden för behandlingen. Inom personskyddet kan skyddspersonens partitillhörighet vara en del av hotbildsanalysen och i underrättelseverksamhet kan en politisk grupperings våldskapital, förmåga och moti-

vation utgöra ändamål för behandling inom verksamhetsgrenarna kontraterrorism eller författningsskydd.

Förbudet mot att utan samtycke antecknas i ett allmänt register enbart på grund av politisk åskådning följer även av 2 kap. 3 § regeringsformen. Förbjudet mot behandling enligt paragrafen är vidare än och omfattar även annan behandling än vad som anses ingå i regeringsformens förbud mot att antecknas i allmänt register och gäller även en person som inte är svensk medborgare.

Förekommer känsliga uppgifter som omfattas av paragrafen i ett sammanhang som i övrigt är relevant, får uppgifterna behandlas på samma sätt som andra uppgifter. Förekomsten av känsliga personuppgifter innebär som regel ett större intrång i enskilda eller allmänna intressen, vilket får betydelse vid proportionalitetsprövningen enligt 1 §, se vidare kommentaren till den bestämmelsen och avsnitt 8.15.4. Se även kommentaren till 14 §.

När det gäller begreppet *ras* i bestämmelsen utgör det ett förtydligande av att dataskyddskonventionens kategorisering av särskilt skyddsvärda personuppgifter gäller fullt ut. Där anges ras och etniskt ursprung som alternativa kategorier. För att undvika missförstånd anges ras i bestämmelsen trots att det inte finns någon vetenskaplig grund för att dela in människor i skilda raser och ur biologisk synpunkt följaktligen inte heller någon grund för att alls använda ordet ras om människor (jfr prop. 2017/18:232 s. 151).

Av *andra stycket* framgår att det inte finns något hinder mot att vidta nödvändiga administrativa åtgärder med känsliga personuppgifter som exempelvis lämnats in till Säkerhetspolisen (jfr prop. 2018/19:163 s. 225 f.). Om det inkommer exempelvis en lista med personer som är aktiva i ett politiskt parti får den diarieföras, trots att uppgifterna inte får behandlas för något annat ändamål.

Av 20 § framgår vad som ska gälla då känsliga personuppgifter behandlas genom sökning och sammanställning.

18 § Genetiska uppgifter får inte behandlas.

Paragrafen motsvarar nuvarande 2 kap. 10 § andra meningen (jfr prop. 2018/19:163 s.225). Genetiska uppgifter definieras i 1 kap. 5 §. Den allmänna motiveringen finns i avsnitt 8.15.1.

Privilegierade uppgifter

19 § Säkerhetspolisen får inte behandla personuppgifter

1. för vilka tystnadsplikt gäller enligt 3 kap. 3 § tryckfrihetsförordningen eller 2 kap. 3 § yttrandefrihetsgrundlagen, eller som omfattas av efterforskningsförbudet i 3 kap. 5 § tryckfrihetsförordningen eller 2 kap. 5 § yttrandefrihetsgrundlagen, eller
2. i sådana meddelanden mellan en person som är misstänkt för brott och hans eller hennes försvarare vilka skyddas enligt 27 kap. 22 § första stycket rättegångsbalken.

Paragrafen är ny och förbjuder Säkerhetspolisen att behandla vissa uppgifter som omfattas av ett särskilt skydd enligt grundlag eller annan lag. Den allmänna motiveringen finns i avsnitt 8.16.

Förbudet omfattar enligt *punkten 1* uppgifter för vilken tystnadsplikt gäller enligt 3 kap. 3 § tryckfrihetsförordningen eller 2 kap. 3 § yttrandefrihetsgrundlagen, eller som omfattas av efterforskningsförbudet i 3 kap. 5 § tryckfrihetsförordningen eller 2 kap. 5 § yttrandefrihetsgrundlagen. De nyssnämnda bestämmelserna skyddar i huvudsak så kallade meddelares rätt till anonymitet. Om Säkerhetspolisen får kännedom om vem som är meddelare, får uppgiften inte behandlas om det inte finns något tillämpligt undantag som gör att tystnadsplikten inte gäller. Av 3 kap. 4 § första stycket 3 samt 7 kap. 22 § första stycket 1 tryckfrihetsförordningen framgår att anonymitet inte gäller för meddelare som gör sig skyldig till bland annat uppror, högförräderi, spionerі eller landsförräderi. Motsvarande bestämmelser finns inom yttrandefrihetsgrundlagens tillämpningsområde i 2 kap. 4 § första stycket 3 respektive 5 kap. 4 § första stycket 1. Sådana uppgifter som undantas rätten till anonymitet omfattas följaktligen inte heller av denna paragrafs tillämpningsområde. Efterforskningsförbudet i 3 kap. 5 § tryckfrihetsförordningen respektive 2 kap. 5 § yttrandefrihetsgrundlagen gäller självständigt. Förbudet mot behandling av sådana uppgifter avser uppgifter som utgör bland annat överskottsinformation eller som Säkerhetspolisen behandlar på annan grund.

Enligt *punkten 2* får Säkerhetspolisen inte heller behandla personuppgifter som förekommer i meddelanden som avses i 27 kap. 22 § rättegångsbalken, mellan en misstänkt och dennes försvarare. De meddelanden som avses är sådan kommunikation mellan en misstänkt och dennes försvarare som sker inom ramen för försvararuppdraget (36 kap. 5 § tredje stycket). Förbudet gäller utan undan-

tag. Hänvisningen till rättegångsbalkens regler avser tillämpningsområdet för förbudet, det vill säga vilken kommunikation som omfattas, men inte genom vilken metod inledande behandling skett. Bestämmelsen gäller således i första hand för personuppgifter som åtkommits på annat sätt än genom hemlig avlyssning av elektronisk kommunikation, som ska raderas redan med stöd av 27 kap. 22 § rättegångsbalken tredje stycket.

Prövningen enligt denna paragraf sker i första hand vid inledande granskning, se 9 §. Det krävs inte någon särskild utredning eller efterforskning för att fastställa att behandlingsförbudet inte är tillämpligt. Det är endast om det går att sluta sig till att personuppgifter rör privilegierad kommunikation som ytterligare efterforskning är nödvändig för att fastställa detta och eventuella undantag är tillämpliga. Om det i ett senare skede framgår att en uppgift omfattas av behandlingsförbudet, ska behandlingen genast upphöra, se 5 kap. 1 §.

Sökbegränsningar

20 § Sökning i syfte att få fram ett urval av personer får grundas på känsliga personuppgifter endast om skälen för att utföra behandlingen uppenbart överväger intrånget i de enskilda eller allmänna intressen som kan påverkas av den.

Bestämmelsen motsvarar delvis nuvarande 2 kap. 12 § och utgör en del i det förstärkta skyddet för känsliga personuppgifter. Den allmänna motiveringen finns i avsnitt 8.15.5.

Känsliga personuppgifter definieras i 5 §. Där framgår att uttrycket omfattar både sådana uppgifter som anges av 17 § samt biometriska och genetiska uppgifter.

Bestämmelsen reglerar behandling som innebär att känsliga personuppgifter används för att skapa sammanställningen av personer som grundas på känsliga personuppgifter. Det kan röra sig om uppgifter som avslöjar etnicitet eller politiska eller religiösa kännetecken för att göra ett urval av personer. Bestämmelsen omfattar även kombinationer av sökbegrepp där endast någon del utgör en känslig personuppgift.

Bestämmelsen omfattar sökningar som resulterar i ett *urval av personer.* Det innebär att paragrafen inte är tillämplig då känsliga

personuppgifter används för att exempelvis göra sökningar efter vissa begrepp i ett dokument eller i en konversation. Bestämmelsen är tillämplig även om sökresultatet endast utgörs av en person, så länge urvalet gjorts utifrån flera personers personuppgifter. Bestämmelsen gäller därmed även sökningar i ett bildmaterial grundat på biometriska uppgifter, trots att endast en persons biometri kan motsvara sökkriteriet. Den gäller dock inte när biometri exempelvis används för att bekräfta att en person är den som avbildats på fotografiet i en passhandling. I dessa fall utgörs behandlingen av en jämförelse och resultatet är inte ett urval. Begreppet sökning är teknikneutralt och innebär en tillämpning av urvalskriterier.

En sökning får grundas på känsliga personuppgifter endast om det vid en proportionalitetsprövning är uppenbart att intresset av att utföra sökningen överväger de intressen som påverkas. Av det följer att skälen för att utföra en viss typ av sökning uppenbart ska väga tyngre än de faktiska eller potentiella allmänna och enskilda intressen som påverkas. Det är därför inte tillräckligt att det finns ett starkt behov eller att det är absolut nödvändigt att göra ett urval grundat på känsliga personuppgifter.

Av rekvisitet *uppenbart* framgår att det inte får råda någon tveksamhet vid prövningen. Det åligger Säkerhetspolisen att kunna visa att behandlingen är författningsenlig, se 5 kap. 2 §. Att en sökning är uppenbart proportionerlig kan antingen följa av att det allmänna intresset av att utföra sökningen väger särskilt tungt i det enskilda fallet eller att intrånget i de intressen som påverkas av sökningen inte är särskilt stort. Beroende på vilka uppgifter som ska grunda ett urval kan det allmänna intresset behöva ha olika tyngd. Det kan exempelvis anses som mer känsligt att göra ett urval som omfattar sökord typiska för etniska, sexuella eller religiösa minoritetsgrupper än motsvarande sökningar som träffar en större andel av befolkningen eller det som kan betecknas som majoritetssamhället.

Att en känslig personuppgift ingår som ett av många urvalskriterier utgör ett mindre intrång än om en känslig personuppgift ensam används för att göra ett urval. En sökning som innefattar religiösa kännetecken kan exempelvis omfatta kännetecken som är unika för en rörelse som ägnar sig åt religiöst motiverad våldsbejakande extremism. I det fallet väger ändamålet att möjliggöra kartläggning ofta tyngre än intrånget i enskildas privatliv eller den potentiella påverkan på religionsfriheten. Om en sökning i stället

omfattar religiösa kännetecken som inte är unika för en sådan rörelse, vilket innebär att samtliga utövare av en viss religion kommer kunna ingå i urvalet, måste ändamålet med sökningen vara betydande. Intrånget i religionsfriheten av att Säkerhetspolisen sammanställer personer efter trosuppfattning är påtagligt. Ändamålet med sökningen har också betydelse. En sökning vars ändamål är att förhindra brott riktade mot exempelvis utövare av en viss religion innebär inte samma intrång som en sökning som syftar till att upptäcka brottslig verksamhet som utövas av en viss grupp.

21 § Om en förundersökning mot en person har lagts ner, om ett åtal har lagts ner eller om en frikännande dom har fått laga kraft, får personen inte längre vara sökbar som misstänkt avseende det brottet.

Paragrafen motsvarar nuvarande 4 kap. 5 § (jfr prop. 2018/19:163 s. 236 och prop. 2009/10:85 s. 348 f). Den allmänna motiveringen finns i avsnitt 8.15.1. Bestämmelsen hindrar inte att det framkommer att personen tidigare varit misstänkt, om personuppgifterna alltjämt behöver behandlas för något annat ändamål än utredande av det aktuella brottet.

Automatiserat beslutsfattande

22 § En persons personuppgifter får inte användas för att fatta automatiserade beslut som har en betydande påverkan för honom eller henne.

Paragrafen motsvarar artikel 9.1 a i dataskyddskonventionen 108+ men har ingen tidigare motsvarighet i nu gällande lag. Bestämmelsen innebär att automatiserat beslutsfattande aldrig ensamt får användas om beslutet påtagligt kan påverka den person som beslutet berör. Övervägandena finns i avsnitt 8.19.1.

Paragrafen hindrar inte att modern teknik används som beslutsstöd. Däremot får inte beslut fattas automatiskt, utan mänsklig inblandning. Den mänskliga inblandningen får inte heller reduceras till att rutinmässigt acceptera automatiserade beslutsförslag. Det krävs att den mänskliga handläggaren har den kompetens, den befogenhet och det underlag som krävs för att kunna fatta ett självständigt beslut. Exempelvis kan en programvara användas för att matcha ett signalement mot övervakningsbilder för att identifiera

en misstänkt person. Om identifieringen sker helt automatiskt och följden blir att en viss person blir misstänkt, måste en människa verifiera resultatet. Beslut om att exempelvis inleda förundersökning får inte ske automatiskt, eftersom det påtagligt påverkar den enskilde att vara föremål för en sådan.

Förbudet mot automatiserat beslutsfattande innebär exempelvis att det inte är tillåtet att efterlysa eller göra en brottsanmälan helt automatiskt. Det är inte heller tillåtet med helt automatiska bedömningar för att förebygga eller förhindra brott, som att exempelvis neka en person tillträde eller förhindra någon att utöva sin tjänst. En registerkontroll enligt säkerhetsskyddslagen (2018:585) utgör inte ett automatiskt beslutsfattande.

3 kap. Informationsutbyte

Behandling för att tillhandahålla information

1 § Uppgifter som behandlas enligt 2 kap. 4–6 §§ får även behandlas för att tillhandahålla information

1. om uppgifterna behövs i

a) brottsbekämpande verksamhet hos en myndighet,

b) en myndighets verksamhet, om informationen tillhandahålls inom ramen för myndighetsöverskridande samverkan mot brott,

c) Försvarsmaktens militära säkerhetstjänst, eller

d) Försvarsmaktens eller Försvarets radioanstalts försvarsunderrättelseverksamhet, eller

2. om uppgifterna behövs i

a) brottsbekämpande verksamhet hos en utländsk myndighet,

b) brottsbekämpande verksamhet hos en mellanfolklig organisation,

c) verksamhet hos utländsk underrättelse- eller säkerhetstjänst, eller

d) ett säkerhets- eller underrättelseorgan i en mellanfolklig organisation som Sverige är medlem i, eller

3. till riksdagen eller regeringen, eller

4. om det sker i överensstämmelse med lag eller förordning.

Paragrafen anger för vilka ändamål Säkerhetspolisen får behandla personuppgifter för att tillgodose behovet av information i annan verksamhet utan prövning enligt 2 kap. 12 §. Övervägandena i denna del finns i avsnitt 8.23.1.

Bestämmelsen motsvarar delvis nuvarande 2 kap. 4 § (jfr prop. 2018/19:163 s. 221 f). Kravet på att det ska finnas särskilda skäl för att behandla uppgifter för att tillhandahålla information

som behövs för Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst och i Försvarets radioanstalts försvarsunderrättelseverksamhet har tagits bort. Till de uppräknade verksamheterna har ett säkerhets- eller underrättelseorgan i en mellanfolklig organisation som Sverige är medlem i lagts till, som anpassning till Sveriges Nato-medlemskap.

Punkten 4 är ny och innebär att personuppgifter får behandlas för att lämnas ut om det sker i överensstämmelse med lag eller förordning. Det innebär att det måste finnas ett berättigat ändamål för utlämnandet men inte att det måste finnas en skyldighet att lämna uppgifter. Ett sådant ändamål kan följa av en sekretessbestämmelse i offentlighets- och sekretesslagen. När det finns en bestämmelse om sekretess, har lagstiftaren tagit ställning till att skyddet för personuppgifter under vissa omständigheter får ge vika för ett allmänt intresse. Sekretessbestämmelsen utgör då den rättsliga grunden för behandlingen.

Till skillnad mot nuvarande reglering ska även den proportionalitetsprövning som följer av 2 kap. 1 § tillämpas vid tillhandahållande, se vidare kommentaren under denna paragraf. När utlämnande sker enligt första stycket är det ofta för ett så angeläget ändamål att ett utlämnande är proportionerligt.

2 § Personuppgifter som behövs för att framställa rättsstatistik ska lämnas till den myndighet som ansvarar för att framställa sådan statistik.

Paragrafen reglerar Säkerhetspolisens uppgiftsskyldighet till den myndighet som ansvarar för rättsstatistiken och motsvarar 2 kap. 15 § i nuvarande lag (jfr prop. 2018/19:163 s. 228). Bestämmelsen är till sin utformning sekretessbrytande.

Utlämnande av personuppgifter till annat land

3 § Om det är förenligt med svenska intressen, får personuppgifter som behandlas med stöd av 2 kap. 4–6 §§ lämnas ut

1. enligt 1 § 2, eller
2. till en annan utländsk myndighet eller mellanfolklig organisation, om utlämnandet följer av en internationell överenskommelse som Sverige har tillträtt efter riksdagens godkännande.

Utlämnande av personuppgifter enligt första stycket får bara ske till mottagare som kan garantera ett tillräckligt skydd för personuppgifterna.

Paragrafen motsvarar delvis nuvarande 2 kap. 16 § (jfr prop. 2018/19:163 s. 228) och avser sekretessbrytande bestämmelser i förhållande till utländska myndigheter och mellanfolkliga organisationer, se 8 kap. 3 § offentlighets- och sekretesslagen (2009:400). Övervägandena finns i avsnitt 8.23.2.

Första stycket hänvisar till de utländska myndigheter och mellanfolkliga organisationer som anges i 1 § 2, det vill säga sådana som antingen har brottsbekämpande uppdrag eller bedriver säkerhets- eller underrättelseverksamhet. Vidare anges att vissa andra utlämnanden som följer av internationella överenskommelser omfattas av paragrafen. Till dessa myndigheter och organisationer får personuppgifter enligt 8 kap. 3 § 1 offentlighets- och sekretesslagen lämnas utan hinder av sekretess. Däremot krävs att utlämnandet är förenligt med svenska intressen.

Andra stycket anger att överföring av personuppgifter till mottagare utomlands bara får ske om mottagaren kan garantera tillräckligt skydd för personuppgifter. Sverige är, i likhet med alla EU:s och EES:s medlemsstater, i dag bundet av dataskyddskonventionen 108, som i de flesta fall utgör en garanti för tillräckligt skydd. Konventionen anger, i artikel 12.2, att de stater som är anslutna till konventionen inte ska uppställa hinder för överföringar endast motiverade av skyddet för personuppgifter. Enligt sin artikel 3.2 a kan vissa kategorier av personuppgifter undantas från konventionens tillämpningsområde, exempelvis de som rör brottsbekämpning. Det kan därför finnas anledning att studera huruvida en medlemsstat gjort undantag från konventionens bestämmelser avseende uppgifter som behandlas hos mottagaren. Om några undantag inte gjorts, bör en tillräcklig skyddsnivå anses föreligga.

För länder som inte tillträtt dataskyddskonventionen får ett tillräckligt skydd för personuppgifter antingen bedömas utifrån nationell lagstiftning (eller regler för den mellanfolkliga organisationen) eller genom avtal eller andra bindande rättsliga instrument för mottagaren. Ett avtal kan vara en del av ett villkor vid överföring av personuppgifter i det enskilda fallet eller utgöra en del av ett standardiserat avtal. Skyddet för personuppgifter måste vara effektivt och bindande för mottagaren. Se artikel 14.3 i dataskyddskonventionen 108+ och det tilläggsprotokoll till dataskyddskonventionen (ETS 181), som Sverige har tillträtt.

Vid bedömningen bör Säkerhetspolisen i samma utsträckning som i dag även kunna beakta att den som ska behandla personuppgifterna kommer att ha tystnadsplikt som omfattar de överförda uppgifterna eller att det garanteras att personuppgifterna inte kommer att behandlas för något annat ändamål än det för vilket de överförs. Även bindande åtaganden om att inte föra personuppgifterna vidare eller att inte använda personuppgifterna efter en viss tidpunkt bör kunna beaktas (jfr prop. 2018/19:163 s. 197).

4 § Personuppgifter som behandlas med stöd av 2 kap. 4–6 §§ får i ett enskilt fall lämnas ut till annan utländsk mottagare än vad som anges i 3 § om

1. sekretess inte hindrar utlämnandet, och
2. skälen för att lämna ut uppgifterna uppenbart överväger intrånget i de enskilda eller allmänna intressen som kan påverkas av utlämnandet.

Paragrafen motsvaras delvis av nuvarande 9 kap. 4 och 5 §§ (jfr prop. 2018/19:163 s. 262–264) och avser överföring av personuppgifter i särskilda situationer. Paragrafen motiveras i avsnitt 8.23.3.

Enligt paragrafen får utlämnande ske till en annan mottagare än som anges i 3 §. Med det avses i huvudsak utlämnande till andra offentliga organ än brottsbekämpande myndigheter och underrättelse- eller säkerhetstjänster samt till privata subjekt. En annan situation som omfattas av paragrafen är utlämnande till en mottagare i ett annat land trots att denne inte kan garantera ett tillräckligt skydd för personuppgifterna. Att bestämmelsen endast får tillämpas i enskilda fall innebär att det inte kan röra sig om ett kontinuerligt informationsutbyte.

Hänvisningen i *första punkten*, till att överföring endast får ske om inte sekretess hindrar det innebär att bestämmelsen inte är sekretessbrytande i förhållande till utländska myndigheter och mellanfolkliga organisationer enligt 8 kap. 3 § 1 offentlighets- och sekretesslagen (2009:400). Innan ett utlämnande får ske ska därför en sekretessprövning göras i det enskilda fallet.

Enligt *andra punkten* får utlämnande ske endast om skälen för att lämna ut uppgifterna uppenbart överväger intrånget i de enskilda eller allmänna intressen som kan påverkas av utlämnandet. Se kommentaren till 2 kap. 1 om proportionalitetsprövningen och 2 kap. 20 § om uppenbarhetsrekvisitet. Utlämnanden med stöd av paragrafen kan ofta avse situationer där intrånget inte är så stort, exempelvis då

Säkerhetspolisen efterfrågar uppgifter om personer från sociala medieplattformar baserade i utlandet. Vid proportionalitetsprövning måste risken för missbruk av personuppgifterna hos mottagaren särskilt beaktas. Finns det en risk för missbruk kan det krävas ett ändamål av betydande tyngd, så som att avvärja eller utreda konkret brottslig verksamhet eller avvärja omedelbar och allvarlig fara för allmän säkerhet (jfr prop. 2018/19:163 s. 262 f).

Elektroniskt utlämnande

5 § Personuppgifter får lämnas ut elektroniskt på annat sätt än genom direktåtkomst, om det inte är olämpligt.

Paragrafen motsvarar 2 kap. 19 § första stycket i nuvarande lag (jfr prop. 2018/19:163 s. 229). Någon ändring i sak är inte avsedd.

6 § Direktåtkomst får medges för personuppgifter som behandlas enligt 2 kap. 4–6 §§ och som

1. Polismyndigheten behöver för att
   a) förebygga, förhindra eller upptäcka brottslig verksamhet,
   b) utreda eller lagföra brott, eller
   c) fullgöra uppgifter enligt utlänningslagen (2005:716) eller lagen (2022:700) om särskild kontroll av vissa utlänningar,
2. Försvarsmakten behöver i sin försvarsunderrättelseverksamhet eller militära säkerhetstjänst, eller
3. Försvarets radioanstalt behöver i sin försvarsunderrättelseverksamhet.

Bestämmelsen motsvarar i huvudsak nuvarande 3 kap. 5 och 6 §§ (jfr prop. 2018/19:163 s. 233 f). Någon saklig förändring är inte avsedd annat än att möjligheten till direktåtkomst inte begränsas till de uppgifter som är gemensamt tillgängliga. Den allmänna motiveringen finns i avsnitt 8.23.2.

Möjligheten omfattar inte uppgifter som behandlas för utvecklingsändamål enligt 2 kap. 7 §. Att utlämnandet måste vara proportionerligt följer av 2 kap. 1 §.

7 § En underrättelse- eller säkerhetstjänst i en stat som omfattas av avtalet om Europeiska ekonomiska samarbetsområdet, i Förenade kungariket eller i Schweiz får medges direktåtkomst till personuppgifter

1. som behandlas för att förebygga, förhindra och upptäcka brottslig verksamhet som innefattar terrorbrott, och
2. om det behövs för samarbetet mot terrorism.

Innan direktåtkomst medges en utländsk underrättelse- eller säkerhetstjänst ska Säkerhetspolisen informera regeringen.

Bestämmelsen motsvarar nuvarande 3 kap. 6 § (jfr prop. 2022/23:116 s. 209 och prop. 2018/19:163 s. 234.) Någon saklig förändring är inte avsedd annat än att möjligheten till direktåtkomst inte begränsas till de uppgifter som är gemensamt tillgängliga. Den allmänna motiveringen finns i avsnitt 8.23.2.

Möjligheten omfattar inte uppgifter som behandlas för utvecklingsändamål enligt 2 kap. 7 §. Att utlämnandet måste vara proportionerligt följer av 2 kap. 1 §.

Sekretessbrytande bestämmelser

8 § Trots sekretess enligt 21 kap. 3 § första stycket, 35 kap. 1 § och 37 kap. 1 § offentlighets- och sekretesslagen (2009:400) har

1. Polismyndigheten rätt att ta del av personuppgifter som behandlas med stöd av 2 kap. 4–6 §§, om myndigheten behöver uppgifterna för att
   a) förebygga, förhindra eller upptäcka brottslig verksamhet,
   b) utreda eller lagföra brott, eller
   c) fullgöra uppgifter enligt utlänningslagen (2005:716) eller lagen (2022:700) om särskild kontroll av vissa utlänningar,
2. Försvarsmakten rätt att ta del av personuppgifter som behandlas med stöd av 2 kap. 4 eller 5 §, om myndigheten behöver uppgifterna i sin försvarsunderrättelseverksamhet eller militära säkerhetstjänst, och
3. Försvarets radioanstalt rätt att ta del av personuppgifter som behandlas med stöd av 2 kap. 4 eller 5 §, om myndigheten behöver uppgifterna i sin försvarsunderrättelseverksamhet.

Paragrafen innehåller en sekretessbrytande uppgiftsskyldighet till de myndigheter som anges i bestämmelsen. Paragrafen motsvarar i huvudsak 2 kap. 16–18 § i nuvarande lag (jfr prop. 2018/19:163 s. 228f). De allmänna motiven finns i avsnitt 8.23.2.

Till skillnad mot nuvarande bestämmelser omfattas utlämnanden som sker med stöd av en sekretessbrytande bestämmelse även av kravet på proportionalitet, se kommentaren till 2 kap. 1 §.

Rätt att meddela föreskrifter

9 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om omfattningen av direktåtkomst enligt 6 och 7 §§ och om behörighet och säkerhet vid sådan åtkomst.

Regeringen kan också meddela föreskrifter om begränsning av möjligheten att lämna ut personuppgifter elektroniskt enligt 5 §.

I paragrafen finns en upplysning om att regeringen kan meddela föreskrifter angående direktåtkomst och om begränsning av möjligheterna att lämna ut personuppgifter elektroniskt. Bestämmelsen motsvarar nuvarande 3 kap. 8 § (jfr prop. 2018/19:163 s. 230).

4 kap. Längsta tid som personuppgifter får behandlas

Bestämmande av behandlingstid

1 § När personuppgifter registreras för ett ändamål eller börjar behandlas för ett nytt ändamål ska Säkerhetspolisen bestämma hur lång tid uppgifterna får behandlas för det ändamålet.

Tiden enligt första stycket får inte vara längre än vad som behövs för ändamålet med behandlingen och inte vara längre än

1. sextio år, om ändamålet för behandlingen hänför sig till sådan säkerhetshotande verksamhet som avses i 18 och 19 kap. brottsbalken och som utövas av främmande makt,
2. fem år, om uppgifterna behandlas endast för utvecklingsändamål, och
3. tjugofem år, om uppgifterna behandlas för något annat ändamål enligt denna lag.

Behandlingstiden får bestämmas gemensamt för personuppgifter som är förenade av sammanhanget. Behandlingstiden ska avse antingen viss tid eller räknas från den senaste registreringen avseende personens anknytning till ändamålet för behandlingen.

Paragrafen reglerar, tillsammans med 2 och 3 §§, längsta tid för behandling av personuppgifter. Motiven till bestämmelsen finns i avsnitt 8.18.

Av *första stycket* framgår att Säkerhetspolisen ska bestämma hur lång tid personuppgifter som längst får behandlas när uppgiften registrerats för ett ändamål eller börjar att behandlas för ett nytt ändamål. Det innebär att uppgifter under inledande granskning enligt 2 kap. 9 §, ska förses med en behandlingstid för det eller de

särskilda ändamål som uppgiften behandlas för enligt 2 kap. 11 §. Detsamma ska gälla uppgifter som börjar behandlas för ett nytt ändamål, exempelvis uppgifter från en förundersökning som börjar behandlas för underrättelseändamål. Behandlingstiden måste vara möjlig för tillsynsmyndigheten att granska. Det ska därför vara möjligt att ta reda på och visa hur länge en uppgift har behandlats för ett ändamål och när behandlingstiden löper ut. Av tredje stycket framgår hur behandlingstiden ska räknas.

Av *andra stycket* framgår den längsta tid som får bestämmas enligt första stycket. Behandlingstiden får aldrig vara längre än vad som behövs för ändamålet. Det innebär exempelvis att uppgifter som regel inte får behandlas för ändamålet att utreda och lagföra brott efter att åtalspreskription inträtt. Uppgifter får inte heller behandlas längre än vad som är adekvat och relevant för ändamålet. Det innebär att ändamålet med behandlingen är avgörande för vilken behandlingstid som får bestämmas.

Enligt *punkten 1* får behandlingstiden bestämmas till som längst sextio år för personuppgifter som behandlas för ändamål som rör säkerhetshotande verksamhet enligt 18 och 19 kap. brottsbalken och som utövas av främmande makt. Med det avses i första hand uppgifter som behandlas inom kontraspionageverksamheten som i nuvarande lagstiftning regleras i 4 kap. 9 § (jfr prop. 2018/19:163 s. 237). Bestämmelsen omfattar även annan brottslig verksamhet än spioneri som utövas av främmande makt.

Enligt *punkten 2* får tid som uppgifter behandlas endast för utvecklingsändamål inte vara längre än fem år. Det gäller uppgifter där inledande behandling skett endast för utvecklingsändamål. Uppgifter som behandlas för andra ändamål får, enligt 12 §, även behandlas för utvecklingsändamål. Sådan behandling får ske så länge uppgifterna behandlas för sitt ursprungliga ändamål, och som högst i fem år därefter. Den längsta behandlingstiden enligt punkten 2 gäller så länge uppgifterna endast behandlas för ändamål inom utvecklingsverksamheten.

Av *punkten 3* framgår att personuppgifter som behandlas för något annat ändamål inom lagens tillämpningsområde får behandlas i högst tjugofem år.

Av *tredje stycket* framgår att behandlingstiden inte behöver avse enskilda personuppgifter utan kan bestämmas gemensamt för alla uppgifter som är förenade av ett sammanhang. Det innebär att

Säkerhetspolisen får ange en behandlingstid för samtliga personuppgifter som förekommer i exempelvis ett dokument, i en film eller i ett avlyssnat samtal.

Vidare framgår att behandlingstiden kan anges på två olika sätt: viss tid eller tid från senaste registrering. En fast behandlingstid som gäller viss tid ska fastställas inom det spann som framgår av andra stycket. Av första stycket framgår att det kan ske då uppgiften behandlas första gången och då uppgiften behandlas för ett nytt ändamål. En löpande behandlingstid avser en viss tid från den senaste registreringen av en uppgift som avser personens anknytning till ändamålet för behandlingen. En sådan behandlingstid innebär att uppgifter som tillförs en person kan förlänga den löpande behandlingstiden för samtliga uppgifter som behandlas om personen för det ändamålet. Säkerhetspolisen avgör vilken metod som ska tillämpas. Inget hindrar att vissa uppgifter om en person behandlas löpande och andra uppgifter behandlas med fast behandlingstid. Så kan exempelvis vara fallet om vissa personuppgifter registreras i en personakt som behandlas med löpande behandlingstid medan andra uppgifter, som förekommer i dokumentet tillsammans med andra personuppgifter, endast behandlas viss tid.

Av 2 kap. 1 § följer att all behandling av personuppgifter ska vara proportionerlig och innebära en rimlig balans mellan intresset av att utföra behandlingen och andra enskilda eller allmänna intressen. Den proportionalitetsavvägning som ska göras enligt 2 kap. 1 § utgör den materiella prövningen då behandlingstid ska bestämmas, inom de gränser som följer av 1 § andra stycket. Vid avvägningen ska behovet av att behandla uppgifterna under en viss tid vägas mot hur behandlingen påverkar andra intressen. Det mest framträdande av de intressen som påverkas är det enskilda intresset av att inte vara registrerad. Även andra intressen, som potentiell påverkan på opinionsfriheterna, måste beaktas vid prövningen.

Behandlingstiden får aldrig bestämmas till en längre tid än vad det finns behov av. Hur länge en uppgift behöver behandlas kan variera beroende på både vilket ändamål som uppgifterna behandlas för och vilken typ av uppgifter det är fråga om.

Rätten till privatliv och personlig integritet påverkas både av mängden uppgifter som behandlas och den tid som behandlingen pågår. Behandling av känsliga personuppgifter och uppgifter av särskilt integritetskänslig art utgör ett större intrång än mer allmänt

hållen information. Den längsta tid som anges i andra stycket är avsedd för de mest angelägna fallen. Det finns därför inte någon presumtion för att uppgifter alltid behöver behandlas under så lång tid.

Det finns inte något krav på att kontinuerligt följa upp det fortsatta behovet av en uppgift under den behandlingstid som bestäms. Det innebär att tiden ofta måste bestämmas utifrån en bedömning av det framtida behovet. För vissa uppgifter kan behovet vara uppenbart under överskådlig tid, exempelvis när det gäller underrättelseofficerare eller personer som kan misstänkas för terrorism. Behovet är i dessa fall även så starkt att de motstående intressena som påverkas får stå tillbaka. I andra fall, exempelvis när det gäller kartläggning av en viss miljö i syfte att klarlägga en viss brottslig verksamhet, kan ändamålets tyngd vad avser mer perifera element av denna miljö komma att avta snabbare. en registrering till följd av att en person endast befunnit sig i en viss krets, varit på en viss plats eller haft en viss bekantskap kan utgöra ett stort intrång i privatlivet och kan efter en tid te sig omotiverat. De behandlingstider som anges i andra stycket ger Säkerhetspolisen en möjlighet att bestämma en funktionell och proportionerlig behandlingstid, men syftar alltså inte till att utgöra den generella tid personuppgifter behandlas inom myndigheten. Den beslutade behandlingstiden måste kunna motiveras vid en eventuell granskning.

Behandlingens upphörande

2 § Personuppgifter får inte behandlas för något ändamål inom denna lags tillämpningsområde efter utgången av det kalenderår då behandlingstiden enligt 1 § löper ut. Om behandlingstiden är kortare än ett år, får uppgifterna inte behandlas efter att den tiden löpt ut. Personuppgifter får inte heller behandlas om det framgår att uppgifterna inte längre behövs för ändamålet med behandlingen.

Bestämmelsen i första stycket hindrar inte att Säkerhetspolisen arkiverar och bevarar allmänna handlingar eller att arkivmaterial lämnas till en arkivmyndighet.

Paragrafen reglerar följden av att den behandlingstid som bestämts enligt 1 § löpt ut. Motiven till bestämmelsen finns i avsnitt 8.18.8.

Paragrafens *första stycke*, reglerar hur behandlingstiden som angetts enligt 1 § ska beräknas. Huvudregeln är att behandling av uppgifterna ska upphöra senast vid årsskiftet det år då behandlingstiden

löper ut. Om behandlingstiden angetts kortare än ett år, ska behandlingen i stället upphöra direkt då tiden löper ut.

Vidare anges att behandling ska upphöra om det framgår att uppgifterna inte längre behövs för ändamålet med behandlingen. Att det måste framgå att behovet upphört innebär att Säkerhetspolisen måste agera på indikationer. Det krävs däremot inte någon kontinuerlig bedömning av behovet inom den beslutade behandlingstiden. Om exempelvis misstankar om brottslig verksamhet helt kan avskrivas på grund av nya uppgifter, kan dessa nya uppgifter innebära att det framgår att behov saknas även för personuppgifter som registrerats dessförinnan.

Av *andra stycket* framgår att den behandlingstid som anges för ändamål inom lagens tillämpningsområde inte gäller arkivändamål som sker efter att behandling för brottsbekämpande ändamål upphört. Det finns inget hinder mot automatiserad behandling för arkivändamål, se dock 5 §.

Förlängning av behandlingstid

3 § Säkerhetspolisen får i ett enskilt fall bestämma att personuppgifter får behandlas under längre tid än vad som följer av 1 § första stycket, om uppgifterna fortfarande behövs för det ändamål som de behandlas för.

Vid ett beslut enligt första stycket får behandlingstiden förlängas med som längst den tid som anges i 1 § andra stycket.

Om den behandlingstid som bestäms enligt första stycket innebär att uppgifter behandlas längre än vad som anges i 1 § andra stycket, ska ett särskilt beslut fattas och den särskilda tillsynsmyndigheten underrättas om det.

Paragrafen innehåller regler för att förlänga behandlingstid i ett enskilt fall. Bestämmelsen motiveras i avsnitt 8.18.6.

Enligt *första stycket* är kravet för att förlänga behandlingstiden att uppgifterna fortfarande behövs för det ändamål som de behandlas för. Behovet kan ha förändrats efter att den första bedömningen gjordes, beroende på händelseutvecklingen som skett därefter. Om en person exempelvis utvandrat eller avtjänar ett längre fängelsestraff kan löpande behandlingstid behöva förlängas, eftersom avsaknaden av nya registreringar inte avspeglar hur relevant det är att alltjämt hålla personen under uppsikt.

Av *andra stycket* följer att ett beslut om att förlänga behandlingstiden som längst får ske med de tider som anges i 1 § andra stycket. Det innebär att behandlingstiden för de flesta uppgifter som längst får förlängas med tjugofem år.

Av tredje stycket framgår att den särskilda tillsynsmyndigheten, Säkerhets- och integritetsskyddsnämnden, ska underrättas om förlängningsbeslut som innebär att den tid som anges i 1 § andra stycket överskrids. Underrättelsen ska ske när beslutet fattas och inte när behandlingstiden faktiskt överskridit de tider som anges i 1 §.

I kommentaren till 1 § utvecklas hur behandlingstiden ska bestämmas utifrån behov och ändamål med behandlingen.

Bestämmande av behandlingstid för uppgifter om barn

4 § När Säkerhetspolisen bestämmer längsta tid för behandling av personuppgifter enligt 1 och 3 §§, ska särskilt beaktas att personuppgifter som rör barn ska omfattas av ett särskilt starkt personuppgiftsskydd.

Paragrafen innehåller regler för att bestämma behandlingstid när personuppgifter rör barn. Bestämmelsen som saknar motsvarighet i nuvarande lag motiveras i avsnitt 8.18.4.

Av paragrafen följer att särskild hänsyn ska tas till personuppgifter som rör barn (jfr 4 kap. 7 § andra stycket i nuvarande lag). Det finns inte några formella skillnader vad gäller den längsta behandlingstiden för barn i förhållande till vuxna. Däremot framgår av paragrafen att barns uppgifter ska omfattas av ett särskilt starkt skydd. Det särskilt starka skyddet för personuppgifter avseende barn markerar att det enskilda intresset att inte vara registrerad väger särskilt tungt för dem. Belastande registrering som avser en ung person får anses utgöra ett större integritetsintrång än en motsvarande registrering för en vuxen. Intrånget över tid får även anses öka i snabbare takt när det gäller registreringar som avser barn.

När det gäller mer perifera uppgifter om ett barn, som inte i nämnvärd utsträckning är belastande för barnet, saknas däremot ofta skäl att vid proportionalitetsprövning särskilja behandlingstiden. Det särskilda skyddet gäller i första hand uppgifter som kan komma att påverka barnet negativt i framtiden. När det gäller uppgifter om att ett barn har utsatts för brott eller befinner sig i samman-

hang som kan vara skadliga, bör vid proportionalitetsavvägningen vägas in att det i dessa fall är till barnets bästa att myndigheten känner till denna omständighet.

Rätt att meddela föreskrifter

5 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

1. att personuppgifter får behandlas för arkivändamål av allmänt intresse eller vetenskapliga, statistiska eller historiska ändamål enligt 2 § andra stycket, och
2. begränsning av behandlingen av personuppgifter för ändamål inom denna lags tillämpningsområde vid digital arkivering.

Paragrafen upplyser om att regeringen kan meddela föreskrifter och den motsvarar nuvarande 4 kap. 11 och 12 §§ (jfr prop. 2018/19:163 s. 238).

5 kap. Säkerhetspolisens skyldigheter

Skyldighet att vidta åtgärder

1 § Om det framgår att personuppgifter behandlas i strid med lag eller annan författning, ska Säkerhetspolisen vidta de åtgärder som krävs för att behandlingen ska bli författningsenlig. Detsamma gäller om åtgärden krävs för att utföra en rättslig förpliktelse.

Om det till följd av första stycket krävs att personuppgifter raderas men uppgifterna behöver finnas kvar av bevisskäl, ska behandlingen av uppgifterna i stället utan onödigt dröjsmål begränsas till detta ändamål.

Paragrafen innehåller registervårdande bestämmelser och den motsvaras delvis av nuvarande 2 kap. 13–14 §§. Övervägandena finns i avsnitt 8.20.2.

Av *första stycket* följer att Säkerhetspolisen har en skyldighet att vidta åtgärder om det framgår att personuppgifter behandlas i strid med lag eller annan författning. Detsamma gäller om åtgärden krävs för att utföra en rättslig förpliktelse. Att personuppgifter behandlas felaktigt kan framgå på olika sätt. Det kan ske i samband med registervårdande insatser, men felaktigheter kan även upptäckas då personuppgifter behandlas operativt genom att exempelvis bearbetas eller delas. Skyldigheten innebär att felaktigheter som konstateras

omedelbart ska rättas till. Om uppgifter inte är korrekta (jfr 2 kap. 13 §) kan en åtgärd vara att uppgifterna rättas eller uppdateras. Vilka åtgärder som är rimliga att vidta får bedömas mot bakgrund av omständigheterna i varje enskilt fall, som till exempel vilka konsekvenser en felaktig eller ofullständig uppgift kan få för den enskilde om uppgifterna lämnas ut eller ligger till grund för en prövning. Om det kan konstateras att uppgifter inte längre behövs eller inte längre är adekvata eller relevanta (jfr 2 kap. 14 §), ska behandlingen upphöra. Detsamma gäller om det framgår att proportionalitetsprövningen som gjorts vid registreringen inte längre kan motivera fortsatt behandling av personuppgifterna (jfr 2 kap. 1 §). Det kan exempelvis bero på förändringar i det allmänna säkerhetsläget eller i den hotbild som legat till grund för behandlingen. Om det skulle uppmärksammas att det saknas rättslig grund för behandlingen (jfr 2 kap. 2 §), ska uppgifterna raderas.

Att de omständigheter som kan föranleda åtgärder enligt paragrafen ska framgå innebär att det inte krävs kontinuerlig granskning av samtliga personuppgifter. Däremot följer det av 2 § att det kan krävas att Säkerhetspolisen har rutiner för registervård, vilket även kan innebära krav på mer systematiska åtgärder för bland annat rättelse, uppdatering och radering, se kommentaren till den bestämmelsen.

Av andra meningen följer att en skyldighet att vidta åtgärder även kan följa av en rättslig förpliktelse. En rättslig förpliktelse kan följa av att tillsynsmyndigheten eller en domstol har förelagt Säkerhetspolisen att vidta en viss åtgärd eller en viss typ av åtgärd (se 7 kap. 6 §). En förpliktelse kan också framgå av annan lag eller förordning meddelad med stöd av lag. I vissa fall kan det finnas villkor för användning av uppgifter som lämnats till Säkerhetspolisen från en samverkande tjänst i annat land. Enligt 6 kap. 3 § lagen (2017:496) om internationellt polisiärt samarbete är sådana villkor om användningsbegränsningar bindande för mottagaren, även om begränsningarna inte överensstämmer med vad som gäller enligt lag.

Av andra stycket följer att uppgifter som behövs som bevis inte ska raderas utan begränsas till detta ändamål. Det innebär att personuppgifter som behandlas i strid med lag inte får raderas om de behövs som bevis. Bevisningen ska avse frågan om personuppgiftsbehandlingen varit felaktig eller för att avgöra andra anknutna frågor, som exempelvis skadeståndsskyldighet enligt 6 kap. 3 §.

Tekniska och organisatoriska åtgärder

2 § Säkerhetspolisen ska, genom lämpliga tekniska och organisatoriska åtgärder, säkerställa och kunna visa att behandlingen av personuppgifter är författningsenlig och att registrerades rättigheter skyddas.

Paragrafen motsvarar 5 kap. 1 § i nuvarande lag (jfr prop. 2018/19:163 s. 238 f.).

Trots att paragrafen överförs från nuvarande lag ställs i vissa avseenden andra krav vid tillämpningen. Den proportionalitetsprövning som ska göras måste säkerställas vid all behandling. Det kan exempelvis finnas skäl att utveckla nya verksamhetsstöd och hålla kontinuerliga utbildningar för denna prövning. Att Säkerhetspolisen ska kunna visa författningsenlighet och att de registrerades rättigheter skyddas kan exempelvis kräva att personuppgiftsbehandling för maskininlärning dokumenteras och motiveras. Dokumentation kan i dessa fall vara nödvändigt för att förstå och kunna granska effekterna av behandlingen i efterhand, då personuppgifterna inte längre finns kvar i verksamheten, se även kommentaren till 8 och 9 §§ samt 7 kap. 8 §. Likt tidigare kan åtgärder som vidtas för att visa att behandlingen är författningsenlig utgöras av exempelvis dokumentation av it-system, behandlingar och vidtagna åtgärder samt teknisk spårbarhet genom loggning och logguppföljning.

3 § Säkerhetspolisen ska när medlen för behandlingen bestäms och vid behandlingen, genom lämpliga tekniska och organisatoriska åtgärder, se till att nödvändiga skyddsåtgärder integreras i behandlingen (inbyggt dataskydd).

Paragrafen motsvarar 5 kap. 2 § i nuvarande lag (jfr prop. 2018/19:163 s. 239). Av 7 kap. 10 § följer en tillkommande skyldighet att i skälig omfattning vidta tekniska åtgärder för att den särskilda tillsynsmyndigheten ska kunna utföra sina arbetsuppgifter på ett ändamålsenligt sätt.

4 § Säkerhetspolisen ska se till att det i automatiserade behandlingssystem som regel inte är möjligt att behandla andra personuppgifter än de som behövs för varje särskilt angivet ändamål med behandlingen (dataskydd som standard).

Paragrafen motsvarar 5 kap. 3 § i nuvarande lag (jfr prop. 2018/19:163 s. 240). Bestämmelsen får särskild betydelse exempelvis när det gäller de personuppgifter som behandlas för utvecklingsändamål och som inte får behandlas för andra ändamål, se 2 kap. 7 § andra stycket.

5 § Säkerhetspolisen ska säkerställa att det i automatiserade behandlingssystem förs loggar över personuppgiftsbehandling i den utsträckning det behövs eller är särskilt föreskrivet.

För behandling som avses i 2 kap. 20 § ska loggar föras.

Paragrafen motsvarar i huvudsak 5 kap. 4 § i nuvarande lag (jfr prop. 2018/19:163 s. 240). I första stycket har ett tillägg gjorts om att loggar ska föras även om det behövs trots att det inte är särskilt föreskrivet.

I *andra stycket*, som är nytt, anges särskilt att loggning ska göras vid sökning som grundas på känsliga personuppgifter enligt 2 kap. 20 §.

Tillgången till personuppgifter

6 § Säkerhetspolisen ska se till att tillgången till personuppgifter begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Paragrafen motsvarar 5 kap. 5 § i nuvarande lag (jfr prop. 2018/19:163 s. 241).

Säkerhetsåtgärder

7 § Säkerhetspolisen ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas, särskilt mot obehörig eller otillåten behandling och mot förlust, förstöring eller annan oavsiktlig skada.

Paragrafen motsvarar 5 kap. 7 § i nuvarande lag (jfr prop. 2018/19:163 s. 242).

Konsekvensbedömning

8 § Om en ny typ av behandling, eller betydande förändringar av redan pågående behandling, kan antas medföra särskild risk för intrång i den registrerades personliga integritet, ska Säkerhetspolisen innan behandlingen påbörjas eller förändringen genomförs bedöma konsekvenserna för skyddet av personuppgifter.

Paragrafen motsvarar, tillsammans med 9 §, nuvarande 5 kap. 6 § (jfr prop. 2018/19:163 s. 242). Den konsekvensbedömning som ska göras kan vara ett stöd vid den proportionalitetsprövning som enligt 2 kap. 1 § ska göras för varje behandling. Betydelsen och utformningen av konsekvensbedömningar kan därför vara annorlunda än enligt nuvarande lag. Se även 7 kap. 9 § om samverkan mellan den särskilda tillsynsmyndigheten och Säkerhetspolisen.

En konsekvensbedömning kan i vissa fall behöva utföras innan inledande behandling av personuppgifter påbörjas med stöd av 2 kap. 7 §. När personuppgifter ska användas för teknisk utveckling måste konsekvensbedömningen även innehålla tillräcklig dokumentation för att den ska vara möjlig att granska för tillsynsmyndigheten. Om det exempelvis handlar om maskininlärningstekniker, kan det vara befogat att ange vilka personuppgifter som ska användas och varför.

Förhandssamråd

9 § Om konsekvensbedömningen visar att det finns en särskild risk för intrång i den registrerades personliga integritet, eller om typen av behandling innebär en särskild risk för intrång, ska Säkerhetspolisen samråda med tillsynsmyndigheten i god tid innan behandlingen påbörjas eller betydande förändringar genomförs (förhandssamråd).

Paragrafen motsvarar, tillsammans med 8 §, nuvarande 5 kap. 6 § (jfr prop. 2018/19:163 s. 242). Den samverkan som enligt 7 kap. 9 § ska ske mellan den särskilda tillsynsmyndigheten och Säkerhetspolisen kan röra bland annat frågor om särskilda risker för intrång. Då kan den särskilda tillsynsmyndigheten ha anledning att lämna synpunkter bland annat i frågan om det är befogat med samråd. Samverkan med den särskilda tillsynsmyndigheten ersätter dock inte kravet på förhandssamråd.

Samarbetsskyldighet

10 § Säkerhetspolisen ska samarbeta med de myndigheter som utövar tillsyn över personuppgiftsbehandling enligt denna lag och föreskrifter som har meddelats i anslutning till lagen.

Paragrafen reglerar samarbetsskyldigheten för Säkerhetspolisen i förhållande till de myndigheter som utövar tillsyn över tillämpningen av lagen och motsvarar i huvudsak nuvarande 5 kap. 8 § (jfr prop. 2018/19:163 s. 243). Motiven till bestämmelsen finns i avsnitt 10.4.5.

Utöver en skyldighet att samarbeta med tillsynsmyndigheten enligt 7 kap. 1 § tillämpas bestämmelsen även i förhållande till den myndighet som har särskild tillsyn över Säkerhetspolisens behandling av personuppgifter enligt lagen, se 7 kap. 9 §.

Dataskyddsombud

11 § Säkerhetspolisen ska inom myndigheten utse ett eller flera dataskyddsombud och anmäla till tillsynsmyndigheten och den särskilda tillsynsmyndigheten när dataskyddsombud utses och entledigas.

Paragrafen motsvarar i huvudsak 5 kap. 9 § i nuvarande lag (jfr prop. 2018/19:163 s. 243). Allmänmotiven finns i avsnitt 8.20.4. Anmälan ska nu göras till både tillsynsmyndigheten och den myndighet som har särskild tillsyn över Säkerhetspolisens behandling av personuppgifter enligt lagen, se 7 kap. 9 §.

12 § Dataskyddsombud ska

1. självständigt kontrollera att Säkerhetspolisen behandlar personuppgifter författningsenligt och på ett korrekt sätt och i övrigt fullgör sina skyldigheter,
2. informera och ge råd till Säkerhetspolisen och de som behandlar personuppgifter under myndighetens ledning om deras skyldigheter vid behandling av personuppgifter,
3. på begäran ge Säkerhetspolisen råd vid en konsekvensbedömning och kontrollera att den genomförs på korrekt sätt,
4. vara kontaktpunkt för enskilda i frågor som rör Säkerhetspolisens behandling av personuppgifter, och
5. samarbeta med tillsynsmyndigheten och den särskilda tillsynsmyndigheten och vara kontaktpunkt för dessa vid förhandssamråd och andra frågor som rör behandling av personuppgifter.

Paragrafen motsvarar i huvudsak 5 kap. 10 § i nuvarande lag (jfr prop. 2018/19:163 s. 243 f). Allmänmotiven finns i avsnitt 8.20.4.

Till den nuvarande lydelsen har ett tillägg gjorts i punkten 5 som innebär att det i dataskyddsombudets uppgifter ingår att samarbeta även med den särskilda tillsynsmyndigheten i frågor som rör behandling av personuppgifter.

Personuppgiftsbiträden

13 § Säkerhetspolisen får, om det är lämpligt, anlita personuppgiftsbiträden för behandling av personuppgifter på myndighetens vägnar. Innan ett personuppgiftsbiträde anlitas ska Säkerhetspolisen försäkra sig om att biträdet kommer att vidta de lämpliga tekniska och organisatoriska åtgärder som krävs för att behandlingen av personuppgifter ska vara författningsenlig och för att skydda registrerades rättigheter.

Personuppgiftsbiträdets behandling av personuppgifter ska regleras i ett skriftligt avtal eller annan skriftlig överenskommelse mellan Säkerhetspolisen och biträdet.

Paragrafen motsvarar 5 kap. 11 § i nuvarande lag (jfr prop. 2018/19:163 s. 245). Den allmänna motiveringen finns i avsnitt 8.22.

14 § Ett personuppgiftsbiträde får inte anlita ett annat personuppgiftsbiträde utan skriftligt tillstånd från Säkerhetspolisen.

Paragrafen motsvarar 5 kap. 12 § i nuvarande lag (jfr prop. 2018/19:163 s. 245). Den allmänna motiveringen finns i avsnitt 8.22.

15 § Ett personuppgiftsbiträde och de som arbetar under biträdets ledning ska behandla personuppgifter i enlighet med instruktioner från Säkerhetspolisen.

Om ett personuppgiftsbiträde bestämmer ändamålen med och medlen för behandlingen, ska biträdet anses vara personuppgiftsansvarig för den behandlingen.

Paragrafen motsvarar 5 kap. 13 § i nuvarande lag (jfr prop. 2018/19:163 s. 245). Den allmänna motiveringen finns i avsnitt 8.22.

16 § Det som sägs om Säkerhetspolisens skyldigheter i 2–8 §§ och 10 § gäller även för personuppgiftsbiträden.

Paragrafen motsvarar 5 kap. 14 § i nuvarande lag (jfr prop. 2018/19:163 s. 246). Den allmänna motiveringen finns i avsnitt 8.22.3. Det ställs i princip samma krav på tekniska och organisatoriska åtgärder för ett personuppgiftsbiträde som för Säkerhetspolisen. Om ett personuppgiftsbiträde vid en konsekvensbedömning enligt 8 § ser en särskild risk för intrång i de registrerades personliga integritet, måste Säkerhetspolisen påkalla samråd med tillsynsmyndigheten.

6 kap. Den registrerades rättigheter

Rätt till registerutdrag

1 § På begäran av en enskild ska Säkerhetspolisen lämna skriftligt besked om personuppgifter som rör honom eller henne behandlas. Om sådana uppgifter behandlas, ska sökanden få skriftlig information om

1. vilka personuppgifter om sökanden som behandlas,
2. varifrån personuppgifterna kommer,
3. den rättsliga grunden och ändamålen med behandlingen,
4. mottagare eller kategorier av mottagare av personuppgifterna, och
5. hur länge personuppgifterna får behandlas.

Uppgifter enligt första stycket, som den sökanden inte redan tagit del av, ska lämnas utan kostnad en gång per år. I andra fall får Säkerhetspolisen ta ut en rimlig avgift.

Paragrafen motsvarar nuvarande 6 kap. 2 § (jfr prop. 2018/19:163 s. 247 ff.). Första stycket har endast ändrats redaktionellt. Den allmänna motiveringen finns i avsnitt 8.19.3.

I andra stycket framgår att rätten till kostnadsfri information gäller endast sådana uppgifter som inte redan lämnats ut till sökanden eller som den sökande på annat sätt kunnat ta del av. Handlingar som den sökande själv lämnat till myndigheten omfattas exempelvis inte av den rätten att kostnadsfritt ta del av personuppgifter.

2 § Säkerhetspolisens skyldighet att lämna information enligt 1 § gäller inte i den utsträckning det är särskilt föreskrivet i lag eller annan författning eller annars framgår av beslut som har meddelats med stöd av författning att uppgifter inte får lämnas ut till den registrerade.

Om förutsättningarna i första stycket är uppfyllda, är Säkerhetspolisen inte skyldig att lämna ut skälen för beslutet. Säkerhetspolisen ska i dessa fall informera sökanden om andra möjligheter att pröva om dennes personuppgifter behandlas författningsenligt.

Paragrafen gör undantag från Säkerhetspolisens informationsskyldighet och motsvarar i huvudsak nuvarande 6 kap. 3 § (jfr prop. 2018/19:163 s. 249). Bestämmelsen motiveras i avsnitt 8.19.4.

Bestämmelsens tredje stycke är nytt och innebär att Säkerhetspolisen ska upplysa den som begär information om möjligheten till kontroll enligt 3 § lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet.

Skadestånd

3 § Den personuppgiftsansvarige ska ersätta den registrerade för den skada och kränkning av den personliga integriteten som orsakats av behandling av personuppgifter i strid med denna lag, eller föreskrifter som har meddelats i anslutning till den.

Paragrafen motsvarar nuvarande 8 kap. 1 § (prop. 2018/19:163 s. 257 f). Den allmänna motiveringen återfinns i avsnitt 8.19.6. Rätten till skadestånd utgör även ett rättsmedel för enskild enligt artikel 9.1 f och 12 i dataskyddskonventionen 108+.

7 kap. Tillsyn

Tillsynsmyndighetens uppgifter

1 § Tillsynsmyndigheten ska

1. utöva allmän tillsyn över personuppgiftsbehandling, och
2. vid förhandssamråd enligt 5 kap. 9 § och när det i övrigt är påkallat ge råd och stöd till Säkerhetspolisen och personuppgiftsbiträden om deras skyldigheter enligt lag eller annan författning.

Paragrafen motsvarar 7 kap. 1 § i nuvarande lag (jfr. prop. 2018/19:163 s. 253 f). Av 2 a § andra stycket förordningen (2007:975) med instruktion för Integritetsskyddsmyndigheten framgår att det är Integritetsskyddsmyndigheten som är tillsynsmyndighet enligt lagen.

Undersökningsbefogenheter

2 § Tillsynsmyndigheten har rätt att av Säkerhetspolisen och personuppgiftsbiträdet på begäran få

1. tillgång till alla personuppgifter som behandlas,

2. upplysningar om och dokumentation av behandlingen av personuppgifter och säkerhets- och skyddsåtgärder,
3. tillträde till lokaler som Säkerhetspolisen eller personuppgiftsbiträdet disponerar samt tillgång till utrustning och andra medel för behandling av personuppgifter, och
4. den hjälp och den information som behövs för tillsynen.

Paragrafen reglerar tillsynsmyndighetens undersökningsbefogenheter och motsvarar nuvarande 7 kap. 3 § (prop. 2018/19:163 s. 254 f.). Motiven till bestämmelsen finns i avsnitt 10.4.3.

Genom hänvisning i 9 § andra stycket framgår att bestämmelsen även gäller den särskilda tillsynsmyndigheten. Den hjälp och information som följer av punkten 4 innebär att Säkerhetspolisen i skälig omfattning måste utbilda och instruera tillsynsmyndigheternas personal i de tekniska system och lösningar som Säkerhetspolisen använder sig av. För att kunna möjliggöra tillsyn över hur personuppgifter behandlas i tekniskt avseende kan det krävas att personal från tillsynsmyndigheten får del av samma utbildning som personal från Säkerhetspolisen.

Förebyggande befogenheter

3 § Om tillsynsmyndigheten bedömer att det finns risk för att personuppgifter kan komma att behandlas i strid med lag eller annan författning, ska myndigheten genom råd, rekommendationer eller påpekanden försöka förmå Säkerhetspolisen eller personuppgiftsbiträdet att vidta åtgärder för att motverka den risken.

Paragrafen motsvarar nuvarande 7 kap. 4 § första stycket (prop. 2018/19:163 s. 255). Motiven till bestämmelsen finns i avsnitt 10.6.

4 § Tillsynsmyndigheten får utfärda en skriftlig varning för att planerad behandling av personuppgifter riskerar att stå i strid med lag eller annan författning. Detsamma gäller om pågående behandling riskerar att stå i strid med lag eller annan författning.

Paragrafen motsvarar nuvarande 7 kap. 4 § andra stycket (prop. 2018/19:163 s. 255). Motiven till bestämmelsen finns i avsnitt 10.6.

Korrigerande befogenheter

5 § Om tillsynsmyndigheten konstaterar att personuppgifter behandlas i strid med lag eller annan författning eller att Säkerhetspolisen eller personuppgiftsbiträdet på något annat sätt inte fullgör sina skyldigheter, får tillsynsmyndigheten

1. genom sådana åtgärder som anges i 3 § försöka förmå Säkerhetspolisen eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig, eller att uppfylla andra skyldigheter,
2. förelägga Säkerhetspolisen eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller att uppfylla andra skyldigheter, eller
3. förbjuda fortsatt behandling om bristen är allvarlig.

Om ett föreläggande utfärdas, ska det av föreläggandet framgå när åtgärderna senast ska vara genomförda och, om det är lämpligt, vilka åtgärder som ska vidtas.

Paragrafen innehåller de korrigerande befogenheterna och den motsvarar nuvarande 7 kap. 5 § (prop. 2018/19:163 s. 255 ff.). Motiven till bestämmelsen finns i avsnitt 10.7.1.

6 § Tillsynsmyndighetens beslut får inte verkställas omedelbart.

Paragrafen utgör ett undantag från de möjligheter till omedelbar verkställighet som följer av 35 § andra och tredje stycket förvaltningslagen (2017:900) och den motsvarar nuvarande 7 kap. 6 § (prop. 2018/19:163 s. 257). Se 12 § angående överklagande av tillsynsmyndighetens beslut. Motiven till bestämmelsen finns i avsnitt 10.7.1.

Särskild tillsyn

7 § Bestämmelser om särskild tillsyn över Säkerhetspolisens behandling av personuppgifter finns i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet.

Paragrafen upplyser om den särskilda tillsyn som Säkerhets- och integritetsskyddsnämnden utövar över Säkerhetspolisens personuppgiftsbehandling. Paragrafen behandlas i avsnitt 10.3.

8 § Den myndighet som utövar tillsyn enligt 7 § (särskild tillsynsmyndighet) och Säkerhetspolisen ska löpande samverka om frågor som rör Säkerhetspolisens skyldigheter enligt lag eller annan författning.

Paragrafen saknar motsvarighet i den tidigare lagen och innebär en skyldighet att etablera och löpande upprätthålla samverkan mellan Säkerhets- och integritetsskyddsnämnden och Säkerhetspolisen. Samverkan ska avse frågor som rör Säkerhetspolisens skyldigheter som personuppgiftsansvarig. De allmänna övervägandena görs i avsnitt 10.5.

Skyldigheten att samverka i det angivna syftet är mer långtgående än den samverkan som avses i 8 § förvaltningslagen (2017:900). Samverkan syftar till att gemensamt försöka motverka att fel begås i verksamheten. Sådan samverkan skulle kunna innebära att Säkerhetspolisen informerar om organisatoriska, tekniska eller metodologiska förändringar i verksamheten som kan innebära en risk. Genom samverkan kan Säkerhets- och integritetsskyddsnämnden bidra med sin syn på olika frågor som rör Säkerhetspolisens skyldigheter.

Samverkan ska vara framåtsyftande och inte vara begränsad till konstaterade förhållanden.

Säkerhetspolisen har i samverkan en möjlighet att lyfta fram verksamhetens behov och de avvägningar som görs mellan dessa behov och andra intressen som påverkas. Samverkan ger nämnden och Säkerhetspolisen en möjlighet att diskutera tillämpningsfrågor utanför de enskilda tillsynsärendena. Hur samverkan ska utövas i det enskilda fallet kräver ingen reglering utan får utvecklas efterhand i samförstånd myndigheterna emellan.

9 § Säkerhetspolisen ska i skälig omfattning vidta de tekniska åtgärder som är nödvändiga för att den särskilda tillsynsmyndigheten ska kunna utföra sina arbetsuppgifter på ett ändamålsenligt sätt.

Den särskilda tillsynsmyndigheten har utöver de befogenheter som följer av särskild lagstiftning även de befogenheter som följer av 2 §.

Paragrafen, som motiveras i avsnitt 10.4.2 och 10.4.4 innehåller dels skyldigheter för Säkerhetspolisen dels kompletterande befogenheter för Säkerhets- och integritetsskyddsnämnden. Av 4 § lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet följer att nämnden har rätt till de uppgifter och upplysningar, den information och det biträde som nämnden begär.

Av *första stycket* följer att Säkerhetspolisen har en skyldighet att i skälig omfattning vidta de tekniska åtgärder som är nödvändiga för att Säkerhets- och integritetsskyddsnämnden ska kunna utöva sitt tillsynsuppdrag på ett ändamålsenligt sätt.

Tekniska åtgärder som kan vara nödvändiga kan exempelvis utgöras av anpassningar av de it-system som Säkerhetspolisen använder i verksamheten. Den särskilda tillsynsmyndighetens behov kan skilja sig från Säkerhetspolisens operativa behov. I skälig omfattning ska hänsyn alltså tas till den verksamhet som Säkerhets- och integritetsskyddsnämnden ska bedriva enligt lagen om tillsyn över viss brottsbekämpande verksamhet då systemen utvecklas, utformas eller köps in. Det kan vidare även vara aktuellt att göra förändringar i redan existerande system. Det kan handla om t.ex. sektionering av information på ett sätt som bättre svarar mot nämndens behov. Möjligheten att söka eller utnyttja automatiska analysverktyg för tillsynsändamål är en annan anpassning som kan komma i fråga. Nämnda åtgärder är endast exempel och ska inte ses som en uttömmande uppräkning av vilka åtgärder som kan komma i fråga. De tekniska funktioner och de syften som ska uppfyllas med dem formuleras av tillsynsmyndigheten.

Att anpassningarna ska ske i skälig omfattning innebär att de inte på ett påtagligt sätt ska påverka den operativa verksamheten negativt. Samtidigt ska det beaktas att en effektiv tillsyn är en förutsättning för att verksamheten alls ska få bedrivas. Att tillsyn i stort och de åtgärder som regleras i denna paragraf medför kostnader och tar resurser i anspråk måste därför, i skälig omfattning, accepteras.

Av *andra stycket* följer att Integritetsskyddsmyndighetens undersökningsbefogenheter enligt 2 § även gäller för Säkerhets- och integritetsskyddsnämnden. Detta således i tillägg till de befogenheter som följer av lagen om tillsyn över viss brottsbekämpande verksamhet. Se kommentaren till 2 §.

8 kap. Överklagande

Överklagande av den personuppgiftsansvariges beslut

1 § Beslut om att inte lämna information eller att ta ut avgift enligt 6 kap. 1 § får överklagas till kammarrätt.

Paragrafen motsvarar delvis 8 kap. 2 § i den nuvarande lagen (jfr prop. 2018/19:163 s. 258) och gäller beslut om att inte lämna ut

information enligt 6 kap. 1 § eller att ta ut avgift. De allmänna övervägandena görs i avsnitt 8.19.7.

Enligt paragrafen ska överklagande av beslut om att inte lämna ut information om personuppgiftsbehandling ske i samma ordning som överklagande beslut enligt offentlighets- och sekretesslagen (2009:400), det vill säga till kammarrätten.

Överklagande av tillsynsmyndighetens beslut

2 § Tillsynsmyndighetens beslut enligt denna lag får överklagas till Försvarsunderrättelsedomstolen.

Paragrafen reglerar överklagande av tillsynsbeslut och skiljer sig från nuvarande lag. De allmänna övervägandena görs i avsnitt 10.7.2.

Försvarsunderrättelsedomstolen är exklusivt forum för överprövning av tillsynsmyndighetens beslut. Denna ordning är motiverad av den känsliga verksamhet som Säkerhetspolisen bedriver och som kan vara föremål för tillsynsmyndighetens beslut.

Tiden för överklagande av tillsynsmyndighetens beslut följer av förvaltningslagen (2017:900).

3 § Vid prövning enligt 2 § ska Försvarsunderrättelsedomstolen tillämpa 2–8, 10–15, 17–26, 28–32 och 38–53 §§ förvaltningsprocesslagen (1971:291) i tillämpliga delar samt 9 §, 10 § första stycket 1 och 15 § lagen (2009:966) om Försvarsunderrättelsedomstol.

Muntliga förhandlingar i domstolen är inte offentliga. Rätten får besluta att en förhandling ska vara offentlig i de delar där det står klart att inga uppgifter för vilka det hos domstolen gäller sådan sekretess som avses i offentlighets- och sekretesslagen (2009:400) kommer att uppenbaras.

När ett beslut överklagas är tillsynsmyndigheten motpart i domstolen. Den särskilda tillsynsmyndigheten ska beredas tillfälle att yttra sig i målet om det behövs.

Bestämmelsen, som är ny, innehåller de processregler som tillämpas vid prövning av överklagande tillsynsbeslut. De allmänna motiven finns i avsnitt 10.7.2.

Första stycket hänvisar till förvaltningsprocesslagens bestämmelser som ska tillämpas vid prövningen.

Av andra stycket framgår att muntlig förhandling i domstolen inte är offentlig om det inte står klart att inga uppgifter för vilken det hos domstolen gäller sådan sekretess kommer att uppenbaras.

Så torde sällan vara fallet. Bestämmelsen motsvarar 4 kap. 11 § i lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar.

Av *tredje stycket* framgår att tillsynsmyndigheten är motpart till Säkerhetspolisen i förfarandet. Säkerhets- och integritetsskyddsnämnden har inte partsställning men ska beredas tillfälle att yttra sig i målet om det behövs. När det överklagade beslutet föranletts av att Säkerhets- och integritetsskyddsnämnden anmält ett förhållande till Integritetsskyddsmyndigheten, bör nämnden yttra sig över de iakttagelser och överväganden som föranlett anmälan.

Överklagandeförbud

4 § Försvarsunderrättelsedomstolens avgöranden får inte överklagas.

De allmänna övervägandena görs i avsnitt 10.7.2. I likhet med övriga avgöranden som fattas av Försvarsunderrättelsedomstolen får inte heller domstolens avgöranden enligt denna lag överklagas.

5 § Övriga beslut enligt denna lag får inte överklagas.

Paragrafen innebär ett förbud mot att överklaga andra beslut enligt denna lag och motsvarar 8 kap. 4 § i den nuvarande lagen (jfr prop. 2018/19:163 s. 259).

Ikraftträdande och övergångsbestämmelser

1. Denna lag träder i kraft den 1 januari 2027.
2. Genom denna lag upphävs lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter.
3. För behandling av personuppgifter som påbörjats innan lagen trätt i kraft får lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter tillämpas fram till och med den 31 december 2029 i stället för den nya lagen.
4. Äldre föreskrifter gäller fortfarande för överklagande av beslut som har meddelats före ikraftträdandet.

Ikraftträdande- och övergångsbestämmelserna motiveras i kapitel 11.

Enligt *punkten 1* träder lagen i kraft den 1 januari 2027.

Punkten 2 anger att lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter upphävs genom den nya lagen. Detta innebär att den äldre lagen, som bär samma namn som den nya, ersätts i sin helhet av den nya regleringen.

I *punkten 3* föreskrivs att personuppgifter som behandlas av Säkerhetspolisen vid ikraftträdandet får fortsätta att behandlas enligt äldre föreskrifter, det vill säga lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter, till och med den 31 december 2029. Denna övergångsperiod på tre år ger Säkerhetspolisen möjlighet att successivt anpassa sin personuppgiftsbehandling till de nya reglerna. Från den 1 januari 2030 ska all behandling ske i enlighet med den nya lagen, vilket innebär att Säkerhetspolisen senast vid denna tidpunkt måste ha genomfört alla nödvändiga anpassningar.

Övergångsbestämmelsen tar enbart sikte på personuppgifter som behandlas vid ikraftträdandet. För alla personuppgifter som Säkerhetspolisen börjar behandla efter ikraftträdandet ska den nya lagen tillämpas fullt ut.

I *punkt 4* föreskrivs att äldre föreskrifter fortfarande ska gälla för överklagande av beslut inom denna lags tillämpningsområde som har meddelats före ikraftträdandet. Med äldre föreskrifter avses här lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter med tillhörande förordning. Punkten tar inte bara sikte på själva överklagandet utan också på till exempel vilken instans som ska överpröva ett beslut.

13.2 Förslaget till lag om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar

1 kap. Allmänna bestämmelser

Lagens tillämpningsområde

1 § Denna lag gäller utöver lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter. Lagen är tillämplig för automatiserad behandling av personuppgifter som registreras eller har registrerats i en särskild uppgiftssamling.

Vid tillämpning av denna lag ska följande bestämmelser i lagen om Säkerhetspolisens behandling av personuppgifter inte tillämpas

– 2 kap. 5, 11, 13–16, 20 och 21 §§,
– 3 kap.,
– 4 kap.,
– 6 kap. 1 och 2 §§, samt
– 7 kap. 2 § 1.

Paragrafen anger tillämpningsområdet för lagen och hur den förhåller sig till bestämmelser i lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter. De allmänna övervägandena finns i avsnitt 9.1.1 och 9.2.

Av *första stycket* följer att lagen innehåller kompletterande bestämmelser till lagen om Säkerhetspolisens behandling av personuppgifter för uppgifter som registreras eller har registrerats i en särskild uppgiftssamling. Vad som avses med registrering och särskild uppgiftssamling följer av definitionen i 2 §. Bestämmelsen innebär att lagen ska tillämpas för behandling av personuppgifter som inledningsvis behandlats enligt lagen om Säkerhetspolisens behandling av personuppgifter och som därefter registreras i en särskild uppgiftssamling. Lagens tillämpningsområde omfattar registreringen och den efterföljande behandlingen i form av bland annat lagring och framtagning. Hänvisningen till lagen om Säkerhetspolisens behandling av personuppgifter innebär vidare att lagen endast är tillämplig vid sådan personuppgiftsbehandling som rör nationell säkerhet i Säkerhetspolisens brottsbekämpande verksamhet. Lagen är endast tillämplig vid automatiserad behandling, vilket innebär att personuppgiftsbehandlingen ska ske med datoriserade behandlingsmedel.

I *andra stycket* anges de bestämmelser i lagen om Säkerhetspolisens behandling av personuppgifter som inte ska tillämpas parallellt med denna lag. Övriga bestämmelser i lagen om Säkerhetspolisens behandling av personuppgifter är tillämpliga även vid registrering och annan behandling av personuppgifter i särskilda uppgiftssamlingar. Det innebär bland annat att de grundläggande kraven som följer av 2 kap. 1–3 §§ lagen om Säkerhetspolisens behandling av personuppgifter ska tillämpas även vid behandling enligt denna lag. Ändamålen för personuppgiftsbehandling enligt denna lag omfattar inte brottsutredning och lagföring i 2 kap. 5 § lagen om Säkerhetspolisens behandling av personuppgifter. Övervägandena i denna del görs i avsnitt 9.10.2. I lagen (2019:547) om förbud mot användning av vissa uppgifter för att utreda brott framgår att

personuppgifter som tagits fram med stöd av denna lag inte får användas i förundersökningar.

Av 2 kap. 9 § lagen om Säkerhetspolisens behandling av personuppgifter framgår att inledande behandling ska följas av att personuppgifter granskas för att säkerställa författningsenlig behandling. Kravet på granskning omfattar även de uppgifter som samlats in för att registreras enligt denna lag, men tar då sikte på förutsättningarna för registrering enligt denna lag. Se avsnitt 9.3.1 för de allmänna motiven i denna del.

De paragrafer i lagen om Säkerhetspolisens behandling av personuppgifter som undantas vid behandling som sker enligt denna lag är sådana att de inte är praktiskt möjliga att tillämpa eller att de förfelar syftet med denna lagstiftning. Det gäller till exempel undantaget från 7 kap. 2 § 1 lagen om Säkerhetspolisens behandling av personuppgifter. Någon möjlighet att ge tillsynsmyndigheter tillgång till uppgifterna i en särskild uppgiftssamling finns inte. Sådan tillgång förutsätter tillstånd från domstol, se 5 kap. 2 §.

Flera av de angivna paragraferna utgör undantag från bestämmelser i dataskyddskonventionen 108+. Dessa undantag är nödvändiga för att skydda nationell säkerhet och de är proportionella i ett demokratiskt samhälle.

Vissa bestämmelser i lagen om Säkerhetspolisens behandling av personuppgifter som ska tillämpas vid behandling av personuppgifter i särskilda uppgiftssamlingar måste tolkas utifrån förutsättningarna i denna lag. Detta gäller 4 kap. 5 § lagen om Säkerhetspolisens behandling av personuppgifter som innebär en skyldighet för Säkerhetspolisen att se till att det i automatiserade behandlingssystem som regel inte är möjligt att behandla andra personuppgifter än de som behövs för varje särskilt angivet ändamål med behandlingen (dataskydd som standard). Registrering enligt denna lag får ske för befogade ändamål, vilket får anses omfattas av kravet i bestämmelsen.

Definitioner

2 § I denna lag används följande uttryck med nedan angiven betydelse.

Uttryck	Betydelse
Särskild uppgiftssamling	En samling med uppgifter som inte får tas fram utan tillstånd och där tillgången till uppgifterna är begränsad genom tekniska eller organisatoriska åtgärder.
Registrering	Införande av uppgifter i en särskild uppgiftssamling.
Framtagning	Tillgängliggörande av personuppgifter som innebär att innehållet i eller innebörden av dem avslöjas.

Paragrafen innehåller definitioner av vissa begrepp som används i denna lag. Definitionerna ersätter hur motsvarande begrepp används i andra sammanhang och är inte avsedda att ha påverkan utanför denna lags tillämpningsområde. Allmänna överväganden görs i avsnitt 9.3.2.

Särskild uppgiftssamling:

Särskild uppgiftssamling är ett juridiskt begrepp. De allmänna motiven i denna del finns i avsnitt 9.4. Det finns inga krav på att uppgifterna ska vara samlade i en viss databas eller på annat sätt tekniskt eller logiskt kopplade till varandra. Det som avgör om en uppgift ingår i en särskild uppgiftssamling är att personuppgiften inte får tas fram utan tillstånd.

En sådan åtkomstbegränsning ska ske genom tekniska och organisatoriska åtgärder. Av 5 kap. 7 § lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter följer Säkerhetspolisens skyldigheter att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas mot bland annat obehörig eller otillåten behandling. Se även 18 kap. 2 a § och 35 kap. 1 a § offentlighets- och sekretesslagen (2009:400).

Registrering:

En registrering är en behandlingsåtgärd som innebär att åtkomsten till personuppgifterna begränsas på så sätt att de omfattas av kraven som ställs på uppgifter i en särskild uppgiftssamling, begreppet avhandlas i avsnitt 9.3. Det kan ske på olika sätt exempelvis genom att uppgifter överförs till särskilda system eller genom att möjligheterna att ta fram personuppgifter på annat sätt begränsas.

Framtagning:

En framtagning innebär att personuppgifter tillgängliggörs. Ett tillgängliggörande avser en interaktion med en människa som innebär att personuppgifter exempelvis visas, används eller tolkas av en medarbetare vid myndigheten. Allmänmotiveringen avseende denna behandlingsåtgärd finns i avsnitt 9.5.

Det är inte en framtagning att flytta eller kopiera en uppgift mellan teknisk hårdvara, plattformar eller system så länge inte uppgifterna eller deras innebörd därigenom avslöjas för en människa. Innehållet eller innebörden av en personuppgift som är registrerad i en särskild uppgiftssamling kan avslöjas på olika sätt. En framtagning kräver inte att personuppgiften i sig visas för en människa. En sökning som resulterar i resultatet träff eller inte träff avslöjar exempelvis innehållet eller innebörden av en eller flera uppgifter i en särskild uppgiftssamling. Detsamma gäller olika automatiserade processer som använder personuppgifter för att göra förutsägelser, sammanfattningar eller andra analyser som därefter tillgängliggörs. Även om ingen personuppgift direkt tillgängliggörs i analysen kan resultatet indirekt avslöja innehållet eller innebörden av de analyserade uppgifterna.

Uppgifter om exempelvis registreringsdatum, storlek, filtyp, lagringsplats, ursprung, åtkomstloggning och viss annan metadata utgör inte personuppgifter och kan därför tas fram och granskas utan tillstånd.

Radering, sammanställning, organisering, indexering, strukturering eller automatiserad översättning är exempel på behandlingar som inte utgör framtagningar så länge personuppgifter inte därigenom tillgängliggörs. Detsamma gäller exempelvis sådan teknisk

behandling som innebär att biometriska uppgifter skapas från biometriskt underlag.

2 kap. Registrering

Registreringsbeslut

1 § Säkerhetspolisen får besluta att personuppgifter ska registreras i en särskild uppgiftssamling, om det är befogat för ett ändamål inom någon av de verksamheter som anges i 2 kap. 4, 6 eller 7 § lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter.

Säkerhetspolisen ska utse de personer som får fatta beslut enligt första stycket. Sådana personer ska ha de särskilda kunskaper och den erfarenhet som uppgiften kräver.

Paragrafen anger att registrering sker genom beslut och reglerar vidare behandlingströskeln för registrering, de ändamål för vilka registrering får ske samt vilka som får fatta registreringsbeslut. Allmänna överväganden görs i avsnitt 9.3.2 och 9.3.6. Uttrycket registrering definieras i 1 kap. 2 §.

Av *första stycket* följer att registrering ska ske genom ett beslut. Vad ett sådant beslut ska innehålla framgår av 2 §. Vidare anges att personuppgifter får registreras om det är befogat för ett ändamål inom någon av de verksamheter som anges i 2 kap. 4, 6 eller 7 § lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter. Det är samma krav som gäller för inledande behandling enligt 2 kap. 8 § lagen om Säkerhetspolisens behandling av personuppgifter, se kommentaren till den bestämmelsen. Att kraven för inledande behandling och registrering är detsamma innebär att de uppgifter som varit befogade att samla in också kan få registreras. En förutsättning är givetvis att behandlingarna, både den inledande behandlingen och registreringen, uppfyller kravet på proportionalitet enligt 2 kap. 1 § lagen om Säkerhetspolisens behandling av personuppgifter. Prövningen av behov och proportionalitet görs mot den informationsmängd som ska registreras och inte mot var och en av de där ingående uppgifterna.

Ett beslut innebär att personuppgifter *ska* registreras. Det innebär att personuppgifter som anges i beslutet ska omfattas av förbud mot framtagning. Det innebär även att ett beslut kan omfatta personuppgifter som ännu inte har samlats in. Det kan exempelvis röra

sig om ett beslut om att en hel databas ska registreras i en särskild uppgiftssamling och hållas uppdaterad genom att regelbundet hämtas in.

Ett ändamål för registrering får inte följa av Säkerhetspolisens övergripande uppdrag att utreda och lagföra vissa brott enligt 2 kap. 5 § lagen om Säkerhetspolisens behandling av personuppgifter. Det beror på att framtagna uppgifter inte får användas i en förundersökning, se 1 § andra stycket lagen (2019:547) om förbud mot användning av vissa uppgifter för att utreda brott.

Av *andra stycket* följer att registreringsbeslut endast får fattas av medarbetare vid Säkerhetspolisen som delegerats uppgiften. Vidare framgår att sådan delegation kräver att personen besitter de särskilda kunskaper och den erfarenhet som krävs för uppgiften. Kravet innebär att beslutsfattare måste ha de insikter och erfarenheter som krävs för att göra intrångsbedömningen och proportionalitetsprövningen. Ett registreringsbeslut kan innebära ett potentiellt intrång och en potentiell kränkning av de registrerades fri- och rättigheter. Det är därför viktigt att beslut fattas av kvalificerade medarbetare och att det finns en möjlighet till individuellt ansvarsutkrävande vid felaktig tillämpning. Det måste framgå eller vara möjligt att ta fram vem som varit beslutsfattare i varje enskilt fall.

Dokumentation

2 § Ett beslut enligt 1 § ska dokumenteras. Av ett registreringsbeslut ska framgå

1. vad de registrerade uppgifterna i huvudsak avser och från vilken källa eller vilka källor de härrör,
2. vilket intrång i enskilda och allmänna intressen som behandling av uppgifterna kan antas medföra,
3. för vilket eller vilka ändamål uppgifterna registreras,
4. hur länge uppgifterna som längst får behandlas (behandlingstid), och
5. de skäl och omständigheter i övrigt som föranlett registreringen.

Varje uppgift i en särskild uppgiftssamling ska kunna spåras till ett beslut enligt första stycket.

Paragrafen anger den formalia som ska uppfyllas vid ett registreringsbeslut. Allmänna överväganden finns i avsnitt 9.3.5.

Av *första stycket* följer dokumentationskravet för registreringsbeslut. Att dessa uppgifter ska anges hindrar inte att Säkerhetspoli-

sen kan utforma registreringsbeslut på det sätt som myndigheten finner lämpligt. Bestämmelsen innehåller däremot minikraven för ett sådant beslut och syftar bland annat till att möjliggöra en effektiv tillsyn.

Enligt *punkten 1* ska det anges vad uppgifterna i huvudsak avser och från vilken källa eller vilka källor de härrör. Det kan röra sig om en beskrivning av vilka uppgifter eller vilken typ av uppgifter som kan förväntas återfinnas i den registrerade uppgiftsmängden och varifrån uppgifterna inhämtats. Exempelvis kan det anges att beslutet omfattar uppgifter från it-beslag från samverkande tjänst eller att det rör sig om information som inhämtats från vissa, närmare angivna, öppna källor. Beskrivningen måste vara tillräckligt detaljerad och hålla sådan kvalitet att den kan tjäna som underlag vid en proportionalitetsbedömning av registreringen. Det hindrar emellertid inte att det inom myndigheten skapas mallar eller annan standardisering, så länge beskrivningen uppfyller sitt syfte.

Det bör utifrån beskrivningen vara möjligt för en lekman såväl som för en expert att sluta sig till vilken källa som uppgifterna härrör ifrån. Det kan innebära att det i vissa fall krävs både en mer avancerad teknisk beskrivning och en beskrivande löptext. I andra fall kan beskrivningen hållas kort eftersom det är uppenbart vilken typ av uppgifter eller källa det rör sig om. Det krävs inte att inledande behandling av personuppgifterna som ska registreras redan skett då beslut fattas. Det innebär att ett beslut om registrering kan omfatta exempelvis en viss databas som uppdateras dagligen. Det måste då framgå av beskrivningen.

Punkten 2 innebär att Säkerhetspolisen ska bedöma och beskriva hur stort intrång registreringen innebär för enskilda eller allmänna intressen. Bedömningen är inte densamma som en proportionalitetsprövning, utan ska beskriva vilka grundläggande fri- och rättigheter som påverkas och i vilken grad. I denna bedömning ska ingen hänsyn tas till behovet av registreringen. Det finns inte något krav på att bedömningen i detalj ska redogöra för de registrerade uppgifterna. Det är tillräckligt att det på ett mer schabloniserat sätt anges hur integritetskänsliga uppgifterna är. En sådan intrångsbedömning ska avse både enskilda och allmänna intressen. Det mest framträdande enskilda intresset som påverkas av en registrering är den personliga integriteten. Med allmänna intressen avses i huvudsak intrång i de positiva opinionsfriheterna, som yttrandefriheten.

Bedömningen måste följa ett logiskt system som innebär att olika slags information kan relateras till varandra. Det kan exempelvis innebära att en skala eller en enhetlig begreppsapparat tillämpas.

Både uppgiftsinnehållet och inhämtningsmetoden påverkar intrångsbedömningen. Den faktiska eller antagna förekomsten av känsliga personuppgifter eller uppgifter som rör enskildas rent privata sfär innebär ett högre integritetsintrång än mer allmänt hållna uppgifter. Insamling av opinionsyttringar som offentliggjorts av den registrerade själv utgör typiskt sett inte ett lika stort integritetsintrång som exempelvis behandling av förtrolig kommunikation. Däremot kan en sådan insamling av öppet tillgänglig information i stället innebära ett intrång i yttrandefriheten eller andra opinionsfriheter.

Säkerhetspolisen väljer själv på vilket sätt intrånget ska graderas. Intrångsbedömningen syftar till att tjäna som underlag för att avgöra om en registrering, framtagning eller annan personuppgiftsbehandling är proportionerlig, se kommentaren till 2 kap. 1 § lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter.

Punkten 3 innebär att ändamålet för registreringen ska anges. Kraven på precision av ändamålet är detsamma som i 2 kap. 8 § lagen om Säkerhetspolisens behandling av personuppgifter, se kommentaren till den paragrafen.

Av *punkten 4* framgår att behandlingstiden ska anges i ett registreringsbeslut. Närmare regler om behandlingstid framgår av 3 §.

Enligt *punkten 5* ska de skäl och omständigheter i övrigt som föranlett registreringen anges. Med det avses en beskrivning av de behov som föranlett registreringen och den proportionalitetsprövning som gjorts. Det kan exempelvis handla om att beskriva de indikatorer som talar för att det i en viss uppgiftsmängd kan vara befogat att söka efter uppgifter som har att göra med terrorrekrytering. Även avvägningen mot intrånget i de registrerades fri- och rättigheter bör beskrivas, om det inte är uppenbart. I vissa fall kan en enkel beskrivning av behovet vara tillräcklig, exempelvis om det rör sig om referensdatabaser som innehåller personuppgifter av mer harmlös karaktär eller om uppgifterna har en tydlig koppling till den säkerhetshotande och brottsliga verksamhet som Säkerhetspolisen har att bekämpa. Eftersom behandlingstiden utgör en viktig komponent i proportionalitetsprövningen, kan det i vissa fall finnas

anledning att ange motiven för hur den bestämts, se kommentaren till 3 §.

I *andra stycket* anges att varje personuppgift som registrerats i en särskild uppgiftssamling måste gå att spåra till ett registreringsbeslut. Syftet är att det alltid ska vara möjligt att kontrollera med stöd av vilket beslut en personuppgift registrerats. Det skapar förutsättningar för en effektiv tillsyn. Bestämmelsen kompletterar de tekniska och organisatoriska åtgärder som Säkerhetspolisen är skyldig att vidta enligt 5 kap. 2–5 §§ lagen om Säkerhetspolisens behandling av personuppgifter.

Behandlingstid

3 § Behandlingstiden i ett registreringsbeslut får inte bestämmas till längre än tio år.

Om behandlingstiden bestäms så att personuppgifter sammanlagt behandlas längre än fem år, ska skälen till det anges särskilt. Den särskilda tillsynsmyndigheten ska underrättas om sådana beslut.

Paragrafen innehåller bestämmelser om behandlingstid för registrerade uppgifter. De allmänna övervägandena görs i avsnitt 9.3.5 och 9.11.

Av 2 § 4 följer att med behandlingstid avses den längsta tid som registrerade uppgifter får behandlas. Tiden ska därmed räknas från registrering.

Av *första stycket* följer att den längsta behandlingstid som får bestämmas genom ett registreringsbeslut är tio år. Behandlingstiden utgör en viktig komponent i den proportionalitetsprövning som ska göras vid registrering, se kommentaren till 4 kap. 1 § lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter. Det innebär att den maximala behandlingstiden som får bestämmas inte ska betraktas som den normala eller generella behandlingstiden.

Av *andra stycket* följer att den särskilda tillsynsmyndigheten ska underrättas om behandlingstider som sammanlagt överskrider fem år. Underrättelseskyldigheten infaller så snart ett beslut innebär att den samlade behandlingstiden överskrider fem år. Det innebär att vid en förlängning av behandlingstiden enligt 4 § ska den nya tiden slås samman med den tid som uppgifterna behandlats dessförinnan.

Tiden ska räknas från när Säkerhetspolisen inledde behandlingen av uppgifterna.

Förlängd behandlingstid

4 § Säkerhetspolisen får besluta att förlänga behandlingstiden, om fortsatt behandling av uppgifterna är befogad för något ändamål som anges i 1 § första stycket.

Vid ett beslut om förlängning av behandlingstiden ska 2 och 3 §§ tillämpas.

Den sammanlagda behandlingstiden får överstiga tjugofem år endast om det finns synnerliga skäl.

Paragrafen ger möjlighet till förlängd behandlingstid. Allmänna överväganden finns i avsnitt 9.11.3.

Av *första stycket* följer att den behandlingstid som, enligt 2 § 4, ska anges i ett registreringsbeslut får förlängas om det vid utgången av den tiden alltjämt kan anses befogat att behandla uppgifterna för något berättigat ändamål. Om uppgifterna har resulterat i relevanta framtagningar, kan det tala för ett fortsatt behov av att behandla uppgifterna. Omvärldsläget och den aktuella hotbilden kan också göra att det är befogat med en förlängd behandlingstid.

Enligt *andra stycket* ska en sådan förlängning ske genom att ett nytt registreringsbeslut fattas. Det innebär att inte endast skälen för fortsatt behandling ska anges utan även övriga uppgifter som följer av 2 §. Om framtagningar eller annan behandling skett, kan bland annat beskrivningen av de registrerade uppgifternas karaktär och intrångsbedömningen behöva revideras utifrån ny kunskap. Hänvisningen till 3 § medför att ett enskilt förlängningsbeslut som längst får avse högst tio ytterligare år. Vidare följer av den hänvisningen att den särskilda tillsynsmyndigheten ska underrättas om beslutet innebär att den sammanlagda behandlingstiden blir längre än fem år.

Av *tredje stycket* följer att det krävs synnerliga skäl för att förlänga behandlingstiden till mer än sammanlagt 25 år. Synnerliga skäl kan vara att uppgifterna är centrala för Säkerhetspolisens förmåga i något avseende eller att de av annan anledning har ett mycket stort värde. Vad som utgör synnerliga skäl ska motiveras utförligt vid ett beslut som innebär att 25-årsgränsen överskrids. Utöver att det ska finnas synnerliga skäl, ska fortsatt behandling av uppgif-

terna även vara proportionerligt enligt 2 kap. 1 § lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter.

3 kap. Framtagning och annan behandling

Framtagning

1 § Uppgifter som är registrerade i en särskild uppgiftssamling får tas fram endast efter tillstånd.

Av paragrafen följer den grundläggande premissen att registrerade uppgifter inte får tas fram om det inte finns ett tillstånd till det. Allmänna överväganden finns i avsnitt 9.5.3.

Vad som avses med att en uppgift tas fram följer av definitionen av framtagning i 1 kap. 2 §. Av 4 kap. 1 § följer att tillstånd lämnas av Försvarsunderrättelsedomstolen. I 3 § finns regler för när en särskilt utsedd befattningshavare vid Säkerhetspolisen får lämna tillstånd till framtagning i brådskande fall.

Bestämmelsen innebär att varken medarbetare vid Säkerhetspolisen eller någon annan är behöriga att läsa eller på annat sätt ta del av registrerade personuppgifter utan tillstånd. Säkerhetspolisens skyldighet att vidta tekniska och organisatoriska åtgärder för att säkerställa detta följer av 5 kap. 2–7 §§ lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter.

2 § Säkerhetspolisen får ansöka om tillstånd till framtagning, om det behövs för ett särskilt ändamål inom någon av de verksamheter som anges i 2 kap. 4, 6 och 7 §§ lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter.

Paragrafen ger förutsättningar för Säkerhetspolisen att ansöka om tillstånd till framtagning. Denna fråga avhandlas i avsnitt 9.8. Vad som avses med att en uppgift tas fram följer av definitionen av framtagning i 1 kap. 2 §. Av 4 kap. 1 § följer att tillstånd lämnas av Försvarsunderrättelsedomstolen.

Säkerhetspolisen får ansöka om framtagning för ett ändamål inom någon av de verksamheter som anges i 2 kap. 4, 6 och 7 §§ lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter. Det innebär att framtagningen får ske för ändamål inom underrättelseverksamheten, utvecklingsverksamheten eller annan

rättslig grund men inte för att utreda brott. Att framtagna uppgifter inte får användas för att utreda brott följer av 1 § andra stycket lagen (2019:547) om förbud mot användning av vissa uppgifter för att utreda brott. Av 4 kap. 2 § framgår vad ansökan ska innehålla. Av 5 kap. 2 § följer att även tillsynsmyndigheterna kan ansöka om framtagning under vissa förhållanden.

3 § De befattningshavare vid Säkerhetspolisen som regeringen föreskriver får besluta om tillstånd till framtagning, om ett inhämtande av domstolens tillstånd skulle medföra en fördröjning som är av väsentlig betydelse för att avvärja en omedelbart förestående fara för människors liv, hälsa eller omfattande förstörelse av egendom.

Ett tillstånd enligt första stycket ska vara förenligt med 5 § och beslutet ska utformas enligt 4 kap. 6 §. Den särskilda tillsynsmyndigheten ska omedelbart underrättas om beslutet. Beslutet ska senast dagen efter att det fattats anmälas till domstolen.

Om ett beslut inte anmälts i rätt tid, får det inte ligga till grund för framtagning och personuppgifter som tagits fram med stöd av beslutet får inte längre behandlas.

Paragrafen ger en möjlighet för vissa befattningshavare vid Säkerhetspolisen att i brådskande och särskilt angelägna fall lämna tillstånd till framtagning. De allmänna övervägandena finns i avsnitt 9.9.

Av *första stycket* följer förutsättningarna för att interimistiskt lämna tillstånd till framtagning. Den första förutsättningen är att inhämtande av domstolens tillstånd skulle medföra en fördröjning eller annan olägenhet av väsentlig betydelse. I detta ligger att ändamålet med åtgärden riskerar att gå förlorat om domstolens tillstånd skulle avvaktas. Den andra förutsättningen är att framtagningen syftar till att Säkerhetspolisen ska kunna avvärja en omedelbart förestående fara för människors liv eller hälsa eller omfattande förstörelse av egendom. Med omedelbart förestående fara avses situationer där det föreligger en konkret fara i närtid. Faran ska avse förverkligande av brott mot liv och hälsa eller omfattande förstörelse av egendom, exempelvis genom terroristbrott. Regeringen utser den eller de befattningshavare vid Säkerhetspolisen som är behöriga att fatta beslut om tillstånd till framtagning.

I *andra stycket* anges, i första meningen, de regler som ska tillämpas för ett beslut enligt första stycket. Ett sådant beslut ska utformas på samma sätt som ett tillstånd från domstolen, se kommentaren

till 4 kap. 5 §. För att lämna tillstånd måste dels förutsättningarna i första stycket vara uppfyllda, dels de som anges i 5 §. Möjligheten att fatta interimistiska beslut enligt paragrafen är avsedda för utpräglade undantagsfall.

Enligt andra meningen ska Säkerhets- och integritetsskyddsnämnden underrättas om att ett beslut fattats. Det kan ske antingen genom att beslutet skickas till nämnden eller genom att nämnden underrättas på annat sätt. Underrättelse ska lämnas omedelbart efter att beslutet fattats. Underrättelsen ska underlätta nämndens inställelse och yttrande till domstolen och en eventuell efterföljande granskning av hur beslutet har tillämpats. Vidare framgår att Säkerhetspolisen senast dagen efter att beslutet fattats ska anmäla det till domstolen. I lagen (1930:173) om beräkning av lagstadgad tid finns bestämmelser om vad som avses med nästföljande dag. I 4 kap. 3 § finns bestämmelser om domstolens prövning av en sådan anmälan.

Av *tredje stycket* följer att ett beslut som inte anmälts i rätt tid, inte får ligga till grund för framtagning och att personuppgifter som tagits fram med stöd av beslutet inte får behandlas. Att personuppgifter som tagits fram genom ett ogiltigt beslut ska raderas eller begränsas följer av 5 kap. 1 § lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter. Av 5 kap. 1 § följer att Säkerhets- och integritetsskyddsnämnden kan besluta om omedelbar radering av uppgifter som tagits fram utan tillstånd.

Övrig behandling

4 § Annan personuppgiftsbehandling än registrering och framtagning får ske

1. för att tekniskt möjliggöra, effektivisera eller förenkla en framtagning,
2. om det behövs för att personuppgifter ska behandlas författningsenligt och på ett korrekt sätt, eller
3. om det behövs för ett särskilt, uttryckligt angivet och berättigat ändamål.

Paragrafen anger under vilka förhållanden annan behandling än registrering och framtagning får ske av personuppgifter som omfattas av lagens tillämpningsområde. Allmänna överväganden görs i avsnitt 9.5.2.

Enligt *punkten 1* får behandling alltid göras för att tekniskt möjliggöra, effektivisera eller förenkla framtagning. Punkten 1 avser att träffa bland annat olika databastekniska åtgärder som krävs för att kunna söka och ta fram personuppgifter. De behandlingar som avses i punkten får ske för ändamålet att generellt förenkla framtagning. En sådan åtgärd behöver därför inte ha någon omedelbar koppling till ett specifikt tillstånd till framtagning. Exempel på de avsedda typerna av behandlingar är indexering av uppgifter i en databas eller konvertering av filer till annat format för att förenkla sökbarhet eller göra uppgifterna kompatibla med viss programvara. Andra behandlingsåtgärder skulle kunna vara att översätta text från främmande språk eller att transkribera ljud till text med hjälp av automatiserad behandling. En annan åtgärd kan vara att skapa biometriska uppgifter av bilder för att möjliggöra och förenkla biometriska sökningar. Sammanställning, organisering eller strukturering av registrerade personuppgifter är andra exempel.

Punkten 2 innebär att behandlingsåtgärder även får ske för att upprätthålla kraven på författningsenlig och korrekt behandling. Det innebär exempelvis att personuppgifter får raderas om de inte längre behövs eller att åtgärder får vidtas för att minska intrånget, som pseudonymisering eller anonymisering.

Av *punkten 3* framgår under vilka omständigheter andra behandlingsåtgärder än de som omfattas av föregående punkter får vidtas. Det kan exempelvis vara olika slags automatiserade analyser som inte sker för att förenkla en framtagning. Exempel på sådana behandlingar kan vara olika slags profilering på individ- eller gruppnivå. Även andra mer aggregerade automatiserade analyser av bland annat aggressivitet, hotnivå eller påverkansförsök i vissa uppgiftsmängder kan ske med stöd av denna punkt. Att uppgifter används för maskininlärning eller annan teknisk utveckling är en annan sådan behandling. Under förutsättning att behandlingen inte utgör en framtagning får behandlingar ske om det behövs för ett särskilt, uttryckligt angivet och berättigat ändamål. Kraven är desamma som för behandling enligt 2 kap. 11 § lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter. För innebörden av begreppet behövs och vad som avses med ett särskilt, uttryckligt angivet och berättigat ändamål, se kommentaren till nyssnämnda paragraf.

De grundläggande kraven för behandling som följer av 2 kap. 1–3 §§ lagen om Säkerhetspolisens behandling av personuppgifter

gäller även behandling enligt denna bestämmelse. Av det följer bland annat ett krav på proportionalitet.

Förutsättningar för tillstånd till framtagning

5 § Tillstånd till framtagning får lämnas endast om
1. behandlingen står i överensstämmelse med lag och Sveriges internationella åtaganden,
2. behandlingen behövs för ändamålet, och
3. det står klart att skälet för att utföra behandlingen överväger intrånget i de enskilda eller allmänna intressen som kan påverkas av den.

En framtagning enligt första stycket får inte förväntas leda till att fler personuppgifter än vad som behövs för ändamålet behandlas.

Ett tillstånd till framtagning ska gälla för viss tid.

Paragrafen reglerar de grundläggande förutsättningarna för tillstånd. Allmänna överväganden finns i avsnitt 9.7.

Av *punkten 1* följer att tillstånd endast får lämnas om åtgärden är förenlig med svensk lag och för Sverige bindande internationella åtaganden. Europakonventionen är ett för Sverige bindande internationellt åtagande som kan påverka förutsättningarna för att meddela tillstånd enligt denna lag.

Av *punkten 2* följer att framtagningen ska behövas för det ändamål som angetts i ansökan. Det innebär att det måste göras en prognos om att framtagningen kan antas leda fram till det resultat som eftersträvas. I prövningen ingår även en bedömning av om det eftersträvade resultatet lika gärna kan uppnås på något mindre ingripande sätt än vad som angetts i ansökan. En sökning i en särskild uppgiftssamling måste dock inte resultera i att personuppgifter tas fram för att anses vara nödvändig. Det kan finnas ett starkt behov att bekräfta att en uppgift inte förekommer likväl som att den förekommer och kan tas fram.

Enligt *punkten 3* ska det stå klart att skälet för att utföra behandlingen överväger intrånget i de enskilda eller allmänna intressen som kan påverkas av den. Vid proportionalitetsbedömningen ska alla relevanta faktorer vägas samman och inte endast de som lyfts i ansökan. Se i övrigt kommentaren till 2 kap. 1 § lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter.

Av *andra stycket* följer att ett tillstånd inte får förväntas medge framtagning av fler uppgifter än vad som behövs för ändamålet. Det

innebär att framtagningen ska ske av uppgifter som är adekvata, relevanta och inte för omfattande för ändamålet. Det ligger i sakens natur att det inte går att på förhand föreskriva i detalj vilka uppgifter som får tas fram med stöd av ett tillstånd, eftersom resultatet i detta skede är okänt. Se även kommentaren till 4 kap. 6 § 4.

Av *tredje stycket* följer att alla tillstånd måste vara begränsade i tid. Det finns inte någon begränsning i lag av hur lång tid ett tillstånd får gälla. Av behovsprincipen följer dock att en åtgärd inte får pågå längre än nödvändigt. En alltför lång giltighetstid innebär också att domstolen inte har möjlighet att kontinuerligt följa upp om tillståndet uppfyller sitt syfte.

4 kap. Handläggningen i domstol

Ansökan om framtagning

1 § Ansökan om tillstånd till framtagning görs hos Försvarsunderrättelsedomstolen.

Paragrafen anvisar forum för tillståndsfrågor. De allmänna övervägandena återfinns i avsnitt 9.6.

Försvarsunderrättelsedomstolen är exklusivt forum för prövning av ansökningar enligt denna lag. I lagen (2009:966) om Försvarsunderrättelsedomstol framgår de närmare bestämmelserna om domstolen.

2 § I ansökan ska sökanden ange

1. vilka kategorier av uppgifter framtagningen ska avse och från vilka typer av källor framtagning ska ske,
2. det särskilda ändamålet med och behovet av framtagningen,
3. vilka sökbegrepp, kategorier av sökbegrepp eller andra urvalskriterier som är avsedda att användas vid framtagningen och, om det finns skäl, med vilken teknik urvalet ska ske,
4. under vilken tid tillståndet ska gälla, och
5. de skäl och omständigheter i övrigt som sökanden vill åberopa till stöd för sin ansökan.

Om sökbegrepp ska innehålla känsliga personuppgifter, eller om urvalet av annan anledning förväntas ske utifrån sådana uppgifter, ska det anges särskilt.

I paragrafen återfinns kraven på en ansökan om tillstånd enligt lagen. De allmänna övervägandena finns i avsnitt 9.8.2.

I *första stycket* anges de formella kraven för att en ansökan ska vara komplett. Syftet är att ge domstolen tillräckligt underlag för sin bedömning och ge den särskilda tillsynsmyndigheten underlag till sitt yttrande. Om domstolen inte anser att en ansökan uppfyller kraven i denna paragraf, får domstolen, enligt 5 § förvaltningsprocesslagen (1971:291) förelägga sökanden att komplettera sin ansökan. En komplettering kan ske skriftligen eller vid sammanträde.

Av *punkten 1* framgår att sökanden ska ange de kategorier av uppgifter och de källor som ansökan avser. Bestämmelsen innebär att sökanden kan begränsa framtagningen till att endast avse en eller flera kategorier av uppgifter eller uppgifter som härrör från vissa källor. En ansökan kan också omfatta alla källor. Mängden personuppgifter som behandlas vid en framtagning har betydelse vid den proportionalitetsavvägning som domstolen ska göra.

En kategori av uppgifter kan exempelvis bestå av uppgifter som är registrerade med stöd av vissa registreringsbeslut, men så behöver inte vara fallet. En kategori kan även avse personuppgifter av ett visst slag, exempelvis text, namn, adresser eller biometri. Av 2 kap. 2 § 1 framgår att det av ett registreringsbeslut ska framgå vad de registrerade uppgifterna i huvudsak avser. Denna beskrivning kan tjäna som underlag för att begränsa behandlingen till en eller flera kategorier av uppgifter. Framtagningen kan även begränsas på andra sätt, som att den endast avser uppgifter från eller till ett visst datum. Det finns inte något krav på att begränsa framtagning. Det är därför möjligt att ange att framtagning ska ske från alla kategorier av uppgifter och alla källor. Det är även möjligt att endast undanta vissa kategorier, exempelvis på grundval av Säkerhetspolisens bedömning av hur känsliga uppgifterna kan antas vara ur integritetshänseende, se 2 kap. 2 § 2 och kommentaren till den bestämmelsen.

Avgränsningen av kategorier måste även vara sådan att domstolen kan förutse vad som kommer att tas fram vid en sökträff. En framtagning ur en databas kan ofta ske genom framtagning av en datapunkt eller en datarad. Framtagning från ostrukturerade data kan kräva att ett helt dokument eller en begränsad del visas. Om det rör sig om bild- eller videomaterial, kan varje enskild fil tas fram eller endast ett utsnitt. Vad som kan tas fram påverkas av vilka källor som ansökan omfattar.

Att källor eller typ av källor ska anges innebär att det är möjligt att inskränka en framtagning till relevanta källor. Om framtagningen

avser att identifiera viss kommunikation, kan framtagningen exempelvis avse endast kommunikationsuppgifter. Ett annat exempel är att ansökan endast avser framtagningar från en viss referensdatabas.

Av 3 kap. 5 § andra stycket framgår att domstolen ska sträva efter att minimera mängden personuppgifter som tas fram till det som behövs för ändamålet. Uppgiftsminimering sker genom begränsningarna som följer av denna punkt tillsammans med de urvalskriterier som ska anges i punkten 3.

Enligt *punkten 2* ska det särskilda ändamålet och behovet av framtagningen motiveras. Kravet på särskilt ändamål är detsamma som ställs enligt 2 kap. 11 § lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter. Det uppställs därmed samma krav på konkretion som för fortsatt behandling enligt den lagen. I ansökan uttrycks ändamålet och domstolen prövar om det är berättigat. Behovet måste motiveras bland annat för att domstolen ska kunna göra den proportionalitetsavvägning som krävs enligt 3 kap. 5 §. Det innebär bland annat att det operativa syftet och den företeelse som ansökan avser att träffa måste anges i ansökan. Det kan exempelvis handla om att ändamålet med framtagningen är att kartlägga en viss terroristmiljö genom att hitta kopplingar mellan individer vilket motiveras av en hotbedömning som gjorts avseende den aktuella miljön. Ett annat exempel är att ändamålet är att ta fram uppgifter ur en inhämtad databas avseende ip-adresser, eftersom det behövs för att identifiera och spåra cyberangrepp utan att exponera sökningen utåt. Ändamålet kan även avse Säkerhetspolisens utvecklingsverksamhet. Exempelvis kan en programvara behöva tränas på ett stort bildmaterial för att identifiera skjutvapen och framtagning vara nödvändig för att utvärdera resultatet. Det kan även vara nödvändigt med tillstånd till framtagning för att kunna upprätthålla krav på registervård i särskilda uppgiftssamlingar.

Av *punkten 3* följer att de sökbegrepp, kategorier av sökbegrepp eller liknande urvalskriterier som är avsedda att användas i en framtagning ska anges. Om det finns behov av det, ska även den teknik som ska användas vid framtagningen framgå.

Sökbegrepp eller andra urvalskriterier är det som resulterar i att uppgifter tas fram. Det är därför naturligt att särskild vikt läggs vid utformningen av dessa, så att inte fler uppgifter tas fram än vad som behövs för ändamålet. Det är tillräckligt att kategorier av sökbegrepp anges, till exempel att sökning kommer att ske på vissa

typer av selektorer. En kategori kan innehålla ett stort antal olika sökord eller parametrar som avser att göra ett visst förutsägbart urval. Andra urvalskriterier än sökbegrepp kan bygga på maskininlärningsteknik eller algoritmiska sökningar. I dessa fall bör beskrivningen omfatta både teknikens förutsättningar och begränsningar samt hur den är tänkt att användas vid ett urval. En ny och för domstolen tidigare oprövad teknik kan behöva förklaras i samband med ansökan. Ett specifikt ändamål och snäva urvalskriterier kan ofta ersätta behovet av andra särskilda villkor för att begränsa intrånget, se 6 § 4 och kommentaren till den bestämmelsen.

Av *punkten 4* följer att Säkerhetspolisen ska ange en tid som ett tillstånd ska gälla. Alla tillstånd måste, enligt 3 kap. 5 § tredje stycket, vara tidsbegränsade. Tidsperiodens längd ska återspegla Säkerhetspolisens faktiska behov av åtgärden.

Av *punkten 5* följer att ansökan ska motiveras. Det innebär att Säkerhetspolisen ska förklara vad den vill göra och varför. Vissa ansökningar kräver inte någon mer utförlig motivering då det redan av beskrivningen av ändamål och behov, i punkten 2, framgår varför ansökningen görs. I andra fall kan det krävas att domstolen får en bakgrund till ansökan, för att kunna bilda sig en uppfattning om förändrade behov, exempelvis vid förhöjt terrorhot eller säkerhetspolitiska förändringar i omvärlden. De omständigheter som gör att Säkerhetspolisen anser att framtagningen är proportionerlig och i överensstämmelse med lag och Sveriges internationella åtaganden bör anges om det avser ett nytt tillstånd. Många gånger kan det krävas att ett tillstånd till framtagning förenas med särskilda villkor för att proportionalitet ska uppnås. Säkerhetspolisen kan lämna förslag på vilka sådana villkor som behövs och hur de bör vara utformade. Skäl och omständigheter i övrigt kan normalt utvecklas vid ett sammanträde men bör anges så utförligt som möjligt redan i ansökan. Detta för att ge den särskilda tillsynsmyndigheten möjlighet att förbereda och utforma sitt yttrande.

Enligt *andra stycket* ska det särskilt anges om sökbegrepp eller urvalet av annan anledning förväntas ske utifrån känsliga personuppgifter. Känsliga personuppgifter måste i vissa fall ingå som urvalskriterier, exempelvis när det gäller religiöst eller politiskt motiverad terrorism. Andra fall är biometriska jämförelser. Det måste dock anges särskilt om känsliga personuppgifter utgör urvalskriterier eller om urvalet av annan anledning kan förväntas ske utifrån sådana

kriterier. Det senare fallet innebär att det måste framgå av ansökan om urval kan ske utifrån uppgifter som i och för sig är harmlösa men som är avslöjande för andra, känsliga personuppgifter. Finns det inte något behov av att använda sökbegrepp som inbegriper känsliga personuppgifter kan domstolen föreskriva ett villkor som förhindrar sådana sökningar.

3 § Ett beslut om framtagning enligt 3 kap. 3 § som anmälts till domstolen ska anses vara en ansökan om framtagning. En sådan anmälan ska prövas skyndsamt.

Domstolen får bestämma att ett beslut som avses i första stycket inte får ligga till grund för framtagning. Domstolen får också besluta att personuppgifter som tagits fram med stöd av ett anmält beslut inte längre får behandlas.

Domstolen får fatta beslut enligt andra stycket innan ansökan slutligen har prövats.

Paragrafen innehåller bestämmelser om domstolens prövningen av interimistiska beslut som Säkerhetspolisen har anmält. Allmänna överväganden görs i avsnitt 9. 9.4.

När Säkerhetspolisen anmält ett beslut om framtagning ska beslutet, enligt *första stycket*, behandlas på samma sätt som en ansökan om tillstånd med samma innehåll. En sådan ansökan ska prövas skyndsamt, enligt de regler som gäller i övrigt för handläggning av ansökningar. Prövningen ska utgå från omständigheterna som är kända då domstolen avgör frågan och inte förutsättningarna som de framstod vid tidpunkten för det intermistiska beslutet.

Därutöver finns möjlighet för domstolen att, enligt *andra stycket*, upphäva beslutet som anmälts och förbjuda behandling av de uppgifter som tagits fram. Om domstolen förbjuder fortsatt behandling, ska de personuppgifter som tagits fram raderas eller begränsas (se 5 kap. 1 § andra stycket lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter). De åtgärder som anges i andra stycket får beslutas då tillståndsfrågan slutligen avgörs, eller enligt tredje stycket.

Enligt *tredje stycket* får domstolen fatta beslut enligt andra stycket innan ansökan slutligen har prövats. Möjligheten att bestämma att ett anmält beslut inte får ligga till grund för framtagning och ett förbud mot att behandla framtagna uppgifter kan begränsas till att avse tiden till dess att frågan om tillstånd prövats. Av 9 § 2 följer att en ordförande ensam kan fatta beslut enligt detta stycke.

Sammanträde

4 § När en ansökan om framtagning har inkommit ska domstolen, om det behövs, hålla sammanträde. Till sammanträdet ska Säkerhetspolisen och den särskilda tillsynsmyndigheten kallas.

Paragrafen innehåller bestämmelser om att muntligt förfarande är huvudregeln i ansökningsprocessen. De allmänna övervägandena finns i avsnitt 9.8.6.

Av *första stycket* framgår att en tillståndsfråga som huvudregel avgörs efter muntligt sammanträde dit Säkerhetspolisen och den särskilda tillsynsmyndigheten ska kallas. Under sammanträdet får sökanden möjlighet att utveckla skälen för ansökan, svara på domstolens frågor och bemöta det som framkommit i ett skriftligt yttrande eller vid sammanträdet. Frågan om när ett sammanträde behövs får lämnas till rättstillämpningen. Om Säkerhetspolisen eller den särskilda tillsynsmyndigheten påkallar sammanträde, bör ett sådant i regel hållas.

Den särskilda tillsynsmyndighetens närvaro vid sammanträde är normalt inte en förutsättning för att pröva tillståndsfrågan när det är Säkerhetspolisen som ansökt om framtagning, se 5 §.

Den särskilda tillsynsmyndighetens yttrande

5 § Innan domstolen avgör en tillståndsfråga ska den särskilda tillsynsmyndigheten ges tillfälle att yttra sig, om det inte är obehövligt.

Paragrafen ger den särskilda tillsynsmyndigheten, Säkerhets- och integritetsskyddsnämnden, möjlighet att yttra sig innan en tillståndsfråga avgörs. Allmänna överväganden görs i avsnitt 9.8.4.

Paragrafen innehåller inte någon anvisning angående vilka frågor som yttrandet ska avse. Nämnden får därför självständigt utveckla sin roll i ansökningsprocessen utifrån sitt övergripande uppdrag, som det kommer till uttryck i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet, förordningen (2007:1141) med instruktion för Säkerhets- och integritetsskyddsnämnden och myndighetens regleringsbrev. Nämndens yttrande kan vara såväl skriftligt som muntligt vid ett sammanträde. Enligt 6 § 4 ska domstolen i tillstånd ange de villkor som behövs för att begränsa intrånget i enskilda eller allmänna intressen samt för att möjliggöra en effektiv

tillsyn. Behovet av och utformningen av sådana villkor kan vara ett område som nämnden bör bevaka genom yttrande. Exempel på sådant villkor kan vara att nämnden ska ha möjlighet att närvara vid en framtagning eller att framtagna uppgifter ska sparas under en tid för att utfallet av en framtagning och dess förenlighet med meddelat tillstånd ska kunna granskas.

Nämnden har, till skillnad från domstolen, genom sin tillsyn möjlighet att få insyn i tillämpningen av meddelade tillstånd. Det kan handla om att nämnden uppfattar att uppgifter tagits fram på ett sätt som inte är förenligt med syftet bakom ett tillstånd. Även andra konsekvenser som inte varit förutsägbara eller framgått av den ursprungliga ansökan kan kommuniceras genom yttrande då tillstånd söks på nytt eller liknande urvalskriterier används. Att nämnden utan hinder av sekretess kan lämna domstolen uppgifter som nämnden fått del av genom sin tillsynsverksamhet framgår av 42 kap. 4 e § offentlighets- och sekretesslagen (2009:400).

Nämnden är inte Säkerhetspolisens motpart i förfarandet och det finns därmed inte heller något krav på att nämnden ska avge sin inställning till ansökan. Om nämnden anser att en ansökan inte kan ligga till grund för en prövning eller om tillstånd av någon anledning inte bör beviljas eller bör förenas med villkor, är det dock lämpligt att nämnden redovisar detta till domstolen.

Domstolen kan avstå från att inhämta yttrande om det är obehövligt. Så kan vara fallet exempelvis om nämnden tidigare yttrat sig i samma eller liknande frågor och förklarat sig inte ha något ytterligare att tillföra eller om det rör mindre ändringar i tidigare meddelade tillstånd som nämnden redan yttrat sig om.

Tillstånd till framtagning

6 § Försvarsunderrättelsedomstolen får lämna tillstånd till framtagning. I tillståndet ska domstolen ange

1. från vilka kategorier av uppgifter och från vilken typ av källor som framtagning får ske,
2. de sökbegrepp, kategorier av sökbegrepp eller andra urvalskriterier som får användas vid framtagning samt, om det finns skäl, med vilken teknik urvalet får ske,
3. under vilken tid tillståndet gäller,
4. de villkor i övrigt som behövs för att begränsa intrånget i enskilda eller allmänna intressen samt för att möjliggöra en effektiv tillsyn, och
5. de skäl som bestämt utgången.

Paragrafen anger vad som måste framgå av ett beslut om tillstånd. Allmänna överväganden finns i avsnitt 9.8.7.

Tillståndet är bindande för hur Säkerhetspolisen tar fram uppgifter som registrerats i en särskild uppgiftssamling. Det är därför angeläget att tillståndet är så tydligt att det är verkställbart och att det är möjligt att utöva tillsyn över framtagningar som sker med stöd av det. Domstolen är inte bunden av ansökan eller vad som framkommit i yttranden under processen. Domstolen kan därför välja att inskränka tillståndet i förhållande till ansökan eller föreskriva de villkor som krävs för att kunna bevilja den.

Enligt *punkten 1* ska de kategorier av personuppgifter som omfattas av tillståndet anges, tillsammans med typen av källor. Ett tillstånd är som regel inte begränsat till framtagningar från de uppgifter som finns registrerade vid ansökningstillfället. Den kategori och de källor som anges kan därför omfatta även uppgifter som ännu inte registrerats.

Av *punkten 2* följer att de särskilda urvalskriterier för framtagningen som ansökan avser ska anges. Domstolen är inte bunden av ansökan och om det finns behov kan justeringar göras i de föreslagna urvalskriterierna. Av 2 § andra stycket framgår att sökanden ska ange om urvalet sker på grundval av känsliga personuppgifter. Om det finns skäl, får domstolen föreskriva eller förbjuda användandet av viss teknik vid framtagningen. Med teknik avses både utpekad mjukvara och en viss, närmare beskriven, teknik.

Av *punkten 3* följer att tillståndets giltighetstid ska anges. Tiden bör anges mellan två bestämda datum och inte exempelvis som ett visst antal månader. Starttiden kan vara dagen för avgörandet eller senareläggas till annat datum. Tillstånd som avser helt nya framtagningar, exempelvis genom tillämpning av ny teknik eller tidigare oprövade sökbegrepp, kan lämpligen ges en kortare giltighetstid för att domstolen ska ha möjlighet att informera sig om och utvärdera dess effekter.

Enligt *punkten 4* kan domstolen ange de särskilda villkor som behövs för att begränsa intrånget i enskilda eller allmänna intressen samt för att möjliggöra en effektiv tillsyn. En ansökan kan vara begränsad på så sätt att ytterligare villkor inte är nödvändiga. I andra fall kan det finnas anledning för domstolen att exempelvis förbjuda framtagning av vissa känsliga personuppgifter, barns personuppgif-

ter eller uppgifter som är äldre än ett visst datum. Det kan ske genom att uppställa villkor om filtrering.

Säkerhetspolisen bör givetvis ha möjlighet att yttra sig i frågan om ett särskilt villkor är tekniskt möjligt och lämpligt att tillämpa. Det kan exempelvis finnas tekniska begränsningar i hur sökresultat kan filtreras. Är det inte möjligt att tillmötesgå kraven på villkor som bedöms nödvändiga, bör ansökan i stället avslås.

Säkerhets- och integritetsskyddsnämnden har i processen möjlighet att föreslå både villkor för att begränsa intrång och villkor som syftar till att möjliggöra en ändamålsenlig tillsyn. När det gäller villkor som syftar till att möjliggöra en effektiv tillsyn har den särskilda tillsynsmyndigheten ett särskilt ansvar, eftersom det endast är nämnden som vet vilka åtgärder som kan underlätta denna verksamhet. Exempel på sådant villkor kan vara att nämnden ska ha möjlighet att närvara vid framtagning eller att framtagna uppgifter ska sparas under en tid för att utfallet av en framtagning ska kunna granskas.

Enligt *punkten 5* ska de skäl som bestämt utgången anges i ett tillstånd, se 30 § andra stycket förvaltningsprocesslagen (1971:291).

Ändring av tillstånd

7 § Domstolen får besluta om ändring av vad som föreskrivits i ett tillstånd.

Paragrafen innehåller bestämmelser om ändring i tillstånd som meddelats. I avsnitt 9.8.8 finns allmänna överväganden i denna del.

Ändring i tillstånd sker efter ansökan eller om domstolen uppmärksammas på någon mindre felaktighet som inte är möjlig att åtgärda genom rättelse. Av 4 § förvaltningsprocesslagen framgår vad en ansökan om ändring ska innehålla.

Domstolen får bedöma om ändringen är av sådant slag att det ska anses kräva ett nytt tillstånd eller om det som föreskrivits i ett befintligt tillstånd kan ändras. Det kan exempelvis röra sig om mindre tillägg avseende sökbegrepp. Det kan också handla om att tiden förlängs för ett tillstånd som är på väg att löpa ut, exempelvis om en förnyad ansökan inte hunnit prövas.

Om en fråga uppmärksammas i ett visst mål, kan domstolen enligt förevarande paragraf justera motsvarande fråga i andra tillstånd, även om dessa tillstånd inte varit föremål för prövningen.

Av 9 § följer att en ordförande ensam kan besluta om ändring i enklare fall.

Domstolen

8 § I fråga om domförhet gäller 9 § lagen (2009:966) om Försvarsunderrättelsedomstol.

Paragrafen innehåller en hänvisning till lagen om Försvarsunderrättelsedomstol gällande domstolens sammansättning och domförhet. Övervägandena finns i avsnitt 9.8.1.

Försvarsunderrättelsedomstolen är den domstol som prövar ansökningar om framtagning av uppgifter från särskilda uppgiftssamlingar, se 1 §. Hänvisningen till lagen om Försvarsunderrättelsedomstol klargör att samma regler om sammansättning och domförhet som gäller för domstolens verksamhet enligt den lagen även ska tillämpas vid handläggning av ärenden enligt denna lag.

Av 9 § lagen om Försvarsunderrättelsedomstol framgår att vid avgörandet ska domstolen som huvudregel bestå av en ordförande och två särskilda ledamöter.

9 § En ordförande eller en vice ordförande får ensam
1. företa förberedande åtgärder och besluta om avskrivning,
2. fatta beslut enligt 3 § tredje stycket, och
3. besluta om ändring enligt 7 §, om ändringen är av enkel beskaffenhet.

Ordföranden får förordna en lagfaren tjänsteman vid domstolen att ensam på domstolens vägnar vidta förberedande åtgärder.

Paragrafen reglerar vilka åtgärder och beslut som kan vidtas av en ensam domare i domstolen, samt möjligheten för ordföranden att delegera vissa uppgifter till en lagfaren tjänsteman. De allmänna övervägandena finns i avsnitt 9.8.1.

Av *första stycket* framgår att en ordförande eller vice ordförande får avgöra vissa frågor utan medverkan av särskilda ledamöter.

Enligt *första punkten* får en ensam domare vidta förberedande åtgärder och besluta om avskrivning. Med förberedande åtgärder

avses handläggningsbeslut som inte innebär ett avgörande i sak, till exempel beslut om att inhämta yttranden eller kompletteringar.

Enligt *andra punkten* får en ensam domare med stöd av 3 § tredje stycket tillfälligt förbjuda verkställigheten av beslut som anmälts. Se kommentaren till den paragrafen.

I *tredje punkten* ges en ensam domare rätt att besluta om ändringar i ett redan meddelat tillstånd, förutsatt att ändringen är av enkel beskaffenhet. Detta kan exempelvis avse en kortare förlängning av tillståndets giltighetstid för att medge framtagningar till dess att domstolen kunnat pröva en förnyad ansökan.

I *andra stycket* ges ordföranden möjlighet att delegera förberedande åtgärder till en lagfaren tjänsteman vid domstolen. Detta avser endast rent processuella åtgärder som inte innebär något ställningstagande i sakfrågan.

10 § Om inte annat följer av denna lag, gäller 3–5, 8, 14, 17–26, 29–32 och 38–53 §§ förvaltningsprocesslagen (1971:291) i tillämpliga delar vid förfarandet i domstolen.

Paragrafen reglerar förhållandet mellan denna lag och förvaltningsprocesslagen. Bestämmelsen klargör att vissa delar av förvaltningsprocesslagen ska tillämpas vid handläggningen i domstolen, om inte annat följer av förevarande lag. De allmänna övervägandena finns i avsnitt 9.8.1.

Genom paragrafen blir bland annat följande bestämmelser i förvaltningsprocesslagen tillämpliga: anhängiggörande av mål (3–5 §§), rättens utredningsskyldighet (8 §), kallelser till sammanträde (14 §), anteckningar vid sammanträde och kommunikation med parter (17–19 §§), vissa bevismedel (20–26 §§), krav på domstolens avgöranden (29–32 §§) samt ett antal övriga bestämmelser om ordning vid förhandling, jäv, laga förfall, ombud, med mera (38–53 §§).

Hänvisningen avser tillämpliga delar av de angivna paragraferna, vilket innebär att bestämmelserna ska tillämpas med beaktande av de särskilda förhållanden som gäller för Försvarsunderrättelsedomstolens verksamhet och de särskilda regler som finns i förevarande lag. Det gäller t.ex. den särskilda tillsynsmyndighetens roll i processen.

Bestämmelsen motsvarar i huvudsak vad som enligt 28 § lagen (2009:966) om Försvarsunderrättelsedomstol gäller för domstolens handläggning av mål om signalspaning.

11 § Muntliga förhandlingar i domstolen är inte offentliga.

Rätten får besluta att en förhandling ska vara offentlig i de delar där det är uppenbart att inga sekretessbelagda uppgifter enligt offentlighets- och sekretesslagen (2009:400) kommer att avslöjas.

Paragrafen reglerar offentligheten vid muntliga förhandlingar i domstolen. De allmänna övervägandena finns i avsnitt 9.8.6.

Av första stycket framgår huvudregeln att muntliga förhandlingar i domstolen inte är offentliga. Bestämmelsen avviker från vad som normalt gäller för domstolsförhandlingar, där huvudregeln är att förhandlingar är offentliga. Detta motiveras av att ärendena enligt denna lag typiskt sett rör uppgifter som omfattas av sekretess med hänsyn till rikets säkerhet.

I andra stycket ges domstolen möjlighet att besluta om att en förhandling ska vara offentlig i de delar där det är uppenbart att inga sekretessbelagda uppgifter kommer att avslöjas. Kravet på att det ska vara uppenbart innebär i praktiken att det ytterst sällan kan bli aktuellt att tillämpa undantaget.

12 § Domstolens avgörande av saken sker genom dom. Andra avgöranden sker genom beslut.

Paragrafen reglerar formen för domstolens avgöranden. De allmänna övervägandena finns i avsnitt 9.8.7.

Av bestämmelsen följer att när domstolen slutligt avgör – det vill säga om tillstånd till framtagning ska meddelas – ska detta ske genom dom. Andra avgöranden, såsom inhibition (se 3 § tredje stycket), processuella beslut eller avskrivning, ska ske genom beslut.

Skiljelinjen mellan dom och beslut har främst betydelse för domstolens handläggning och dokumentation, men påverkar inte möjligheten att överklaga. Enligt 14 § finns nämligen inte någon möjlighet att överklaga domstolens avgöranden.

13 § I fråga om omröstning gäller 16 kap. rättegångsbalken i tillämpliga delar.

Paragrafen reglerar hur omröstning ska ske i domstolen. Bestämmelsen motsvarar vad som enligt 15 § lagen om Försvarsunderrättelsedomstol gäller för domstolens handläggning av mål om signalspaning. De allmänna övervägandena finns i avsnitt 9.8.1.

Genom hänvisningen till 16 kap. rättegångsbalken ska reglerna om omröstning i tvistemål tillämpas i tillämpliga delar. Formuleringen ”i tillämpliga delar” innebär att bestämmelserna ska anpassas till de särskilda förhållanden som gäller i domstolen, där rätten enligt 8 §, jämfört med 9 § lagen (2009:966) om Försvarsunderrättelsedomstol normalt består av en ordförande och två särskilda ledamöter.

Överklagandeförbud

14 § Domstolens avgöranden enligt denna lag får inte överklagas.

Paragrafen innehåller ett förbud mot att överklaga domstolens avgöranden enligt denna lag. Bestämmelsen motsvarar vad som gäller enligt 16 § lagen om Försvarsunderrättelsedomstol. De allmänna övervägandena finns i avsnitt 9.8.1.

Överklagandeförbudet innebär att varken domar eller beslut som meddelas av domstolen enligt denna lag kan överklagas. Detta gäller såväl beslut om tillstånd till framtagning av uppgifter som interimistiska beslut, processuella beslut och andra avgöranden.

5 kap. Tillsyn

Radering

1 § Den särskilda tillsynsmyndigheten får besluta att framtagna uppgifter ska raderas, om det kan konstateras att framtagningen inte har varit förenlig med ett tillstånd enligt denna lag.

Paragrafen ger den särskilda tillsynsmyndigheten korrigerande befogenheter avseende personuppgifter som har tagits fram i strid med tillstånd. De allmänna övervägandena finns i avsnitt 10.7.3.

Om Säkerhets- och integritetsskyddsnämnden kan konstatera att registrerade personuppgifter behandlas på ett sätt som utgör en framtagning trots att det saknas tillstånd, eller att uppgifter behandlas på ett sätt som inte är förenligt med ett meddelat tillstånd, får nämnden besluta om radering. Ett sådant beslut kan inte överklagas och ska verkställas omedelbart, eller vid den senare tidpunkt som nämnden bestämmer.

Bestämmelsen är fakultativ och nämnden kan avstå från att meddela ett beslut, bland annat om Säkerhetspolisen har vidtagit åtgärder enligt 5 kap. 1 § lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter. Detsamma gäller om tillsynsmyndigheten har meddelat ett föreläggande eller beslut enligt 7 kap. 5 § samma lag.

Framtagning för tillsyn

2 § Den särskilda tillsynsmyndigheten har rätt att ansöka om tillstånd till framtagning för tillsynsändamål. I ett enskilt fall har också tillsynsmyndigheten rätt att ansöka om framtagning för ett sådant ändamål.

Säkerhetspolisen ska ges tillfälle att yttra sig över ansökan.

Paragrafen innehåller bestämmelser som medger att den särskilda tillsynsmyndigheten får ansöka om tillstånd till framtagning för tillsynsändamål. De allmänna överväganden finns i avsnitt 10.4.6.

Av *första stycket* följer, i första meningen, att den särskilda tillsynsmyndigheten Säkerhets- och integritetsskyddsnämnden får ansöka om tillstånd till framtagning enligt denna lag. Ändamålet för en sådan framtagning måste vara att utöva tillsyn över Säkerhetspolisens personuppgiftsbehandling. Av andra meningen framgår att även tillsynsmyndigheten, Integritetsskyddsmyndigheten, har rätt att ansöka om framtagning i ett enskilt fall.

Ansökan sker enligt bestämmelserna i 4 kap. Det innebär bland annat att det ställs samma krav på en ansökan om framtagning för tillsynsändamål som för andra ändamål.

Av *andra stycket* framgår att Säkerhetspolisen ska ges tillfälle att yttra sig innan ett tillstånd för tillsynsändamål prövas. Enligt 4 kap. 4 § ska Säkerhetspolisen kallas till sammanträde om domstolen beslutar om det. Genom yttrandet har Säkerhetspolisen möjlighet att reagera på exempelvis om de sökningar eller de urval som nämnden ansökt om är tekniskt möjliga att utföra eller om det finns andra hinder mot att utföra de framtagningar som ansökan avser.

Säkerhets- och integritetsskyddsnämndens rätt, enligt 4 § lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet, att få de uppgifter som den begär av förvaltningsmyndigheter som omfattas av tillsynen, kan inte tillämpas för de uppgifter som är registrerade i en särskild uppgiftssamling. Säkerhetspolisen har

enligt denna lag inte rätt att ta fram uppgifterna utan tillstånd av domstolen. Rätten till biträde omfattar dock rätt till hjälp att utföra de framtagningar som omfattas av ett tillstånd.

Av 1 kap. 1 § andra stycket framgår bland annat att 7 kap. 2 § 1 lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter, om tillsynsmyndighetens tillgång till de personuppgifter som behandlas, inte är tillämplig. Möjligheten att ansöka om tillstånd syftar till att ge undersökningsbefogenheter som är anpassade för tillsyn över denna lag. Av 5 kap. 10 § lagen om Säkerhetspolisens behandling av personuppgifter framgår att Säkerhetspolisen ska samarbeta med tillsynsmyndigheterna. Det innebär att Säkerhetspolisen måste vara behjälplig med att bland annat bistå i att utforma sökbegrepp som är relevanta för tillsynsändamål.

13.3 Förslaget till lag om ändring i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet

1 §

Säkerhets- och integritetsskyddsnämnden (nämnden) ska utöva tillsyn över

1. brottsbekämpande myndigheters användning av hemliga tvångsmedel och kvalificerade skyddsidentiteter,
2. brottsbekämpande myndigheters användning av andra tvångsmedel enligt lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott än de som avses i 1, om inte den som åtgärden utförts hos eller annars riktats mot har närvarat vid åtgärden,
3. Säkerhetspolisens användning av hemliga tvångsmedel vid särskild kontroll av vissa utlänningar, och
4. därmed sammanhängande verksamhet.

Nämnden ska även utöva tillsyn över den behandling av personuppgifter som utförs av Polismyndigheten, Säkerhetspolisen och Ekobrottsmyndigheten enligt brottsdatalagen (2018:1177) och lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område för de syften som anges i 1 kap. 1 § i den sistnämnda lagen, och lagen *(2026:000)* om Säkerhetspolisens behandling av personuppgifter. Tillsynen ska särskilt avse behandling enligt 2 kap. 11 § brottsdatalagen.

Nämnden ska också utöva tillsyn över Polismyndighetens och Säkerhetspolisens tillämpning av lagen (2019:547) om förbud mot användning av vissa uppgifter för att utreda brott. *Nämnden ska även utöva tillsyn över Säkerhetspolisens behandling av personuppgifter enligt lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar.*

Tillsynen ska särskilt syfta till att säkerställa att verksamhet enligt första–tredje styckena bedrivs i enlighet med lag eller annan författning.

Paragrafen ändras på så sätt att hänvisningen i *andra stycket* till lagen om Säkerhetspolisens behandling av personuppgifter avser den nya lagen. Sista meningen i stycket ändras på så sätt att det inte längre anges att tillsynen över Säkerhetspolisens behandling av personuppgifter särskilt ska avse behandling av känsliga personuppgifter. De allmänna övervägandena i denna del görs i avsnitt 10.8.

Tredje stycket ändras på så sätt att tillsynsuppdraget nu omfattar Säkerhetspolisens behandling av personuppgifter enligt lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar. Tillsynen över behandling i särskilda uppgiftssamlingar är särpräglad, bland annat genom att nämnden får söka tillstånd för att kunna ta del av personuppgifter för tillsynsändamål. Se avsnitt 10.4.6. Av tredje stycket följer även att nämnden ska utöva tillsyn över Säkerhetspolisens tillämpning av lagen (2019:547) om förbud mot användning av vissa uppgifter för att utreda brott. Den lagen omfattar numera även personuppgifter som tagits fram från en särskild uppgiftssamling.

13.4 Förslaget till lag om ändring i offentlighets- och sekretesslagen (2009:400)

18 kap. Sekretess till skydd främst för intresset av att förebygga eller beivra brott

2 a §

Sekretess gäller för uppgift i särskilda uppgiftssamlingar, enligt lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar, som lämnar eller kan bidra till upplysning om Säkerhetspolisens verksamhet att förebygga, förhindra och upptäcka brottslig verksamhet.

För uppgift i allmän handling gäller sekretessen i sjuttio år.

Sekretess enligt första stycket hindrar inte en framtagning enligt lagen om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar.

Paragrafen, som är ny, reglerar sekretess för uppgifter i särskilda uppgiftssamlingar som förs enligt lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar. De allmänna övervägandena görs i avsnitt 9.9.4. Sekretessen omfattar

uppgifter som lämnar eller kan bidra till upplysning om Säkerhetspolisens underrättelseverksamhet.

Av andra stycket framgår att sekretessen gäller i sjuttio år.

Tredje stycket upplyser om att sekretessen inte hindrar framtagningar enligt lagen om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar. Framtagningar får som huvudregel endast ske efter att domstolen lämnat tillstånd. Uppgifter som tagits fram ur en särskild uppgiftssamling med stöd av ett sådant tillstånd omfattas därefter inte av denna paragraf.

35 kap. Sekretess till skydd för enskild i verksamhet som syftar till att förebygga eller beivra brott, m.m.

1 a §

Sekretess gäller för uppgift om en enskilds personliga och ekonomiska förhållanden i särskilda uppgiftssamlingar enligt lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar.

För uppgift i allmän handling gäller sekretessen i sjuttio år.

Sekretess enligt första stycket hindrar inte en framtagning enligt lagen om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar

Paragrafen, som är ny, reglerar sekretess för uppgifter i särskilda uppgiftssamlingar som förs enligt lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar. De allmänna övervägandena görs i avsnitt 9.9.4. Sekretessen omfattar uppgifter om en enskilds personliga och ekonomiska förhållanden.

Av andra stycket framgår att sekretessen gäller i sjuttio år.

Tredje stycket upplyser om att sekretessen inte hindrar framtagningar enligt lagen om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar. Framtagningar får som huvudregel endast ske efter att domstolen lämnat tillstånd. Uppgifter som tagits fram ur en särskild uppgiftssamling med stöd av ett sådant tillstånd omfattas därefter inte av denna paragraf.

42 kap. Riksdagens ombudsmän, Justitiekanslern, Säkerhets- och integritetsskyddsnämnden och undersökningskommissioner, m.m.

4 d §

Om Säkerhets- och integritetsskyddsnämnden får en sekretessreglerad uppgift från en myndighet i ett mål om tillstånd enligt lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar, blir sekretessbestämmelsen tillämplig på uppgiften även hos nämnden.

Paragrafen, som är ny, reglerar sekretess hos nämnden i särskilda fall. De allmänna övervägandena görs i avsnitt 9.8.5.

Paragrafen innebär att nämnden i mål om tillstånd enligt lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar får en sekretessreglerad uppgift från en annan myndighet, så överförs den sekretessen. Detta gäller oavsett vilken myndighet som lämnat uppgiften och i vilket skede av målet.

Huvudregeln om konkurrens mellan olika sekretessbestämmelser i 7 kap. 3 § gäller sekretess enligt paragrafen.

4 e §

Sekretess som gäller hos Säkerhets- och integritetsskyddsnämnden enligt 4 d §, 6–8 §§, 15 kap. eller 18 kap. hindrar inte att en uppgift lämnas till en domstol, om uppgiften behövs för en prövning enligt lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar.

Paragrafen, som är ny, reglerar sekretessgenombrott för uppgift hos nämnden som behövs för tillståndsprövning enligt lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar. De allmänna övervägandena görs i avsnitt 9.8.5.

Bestämmelsen bryter sekretess för uppgifter i nämndens tillsynsverksamhet och sådan sekretess som gäller hos alla myndigheter enligt 15 och 18 kap.

Sekretessen bryts endast om den sekretessbelagda uppgiften behövs för tillståndsprövningen. Det är nämnden som bedömer om uppgiften behövs för domstolens prövning. Uppgiften behöver inte direkt omfattas av ansökan för att kunna vara relevant. Det kan exempelvis handla om att nämndens iakttagelser från framtagningar med

stöd av tidigare tillstånd kan behövas för att belysa frågor som rör en aktuell ansökan.

13.5 Förslaget till lag om ändring i lagen (2009:966) om Försvarsunderrättelsedomstol

1 §

Försvarsunderrättelsedomstolen ska pröva frågor om tillstånd till signalspaning enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.

Försvarsunderrättelsedomstolen ska även

1. pröva frågor om tillstånd till framtagning enligt lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar,

2. pröva beslut som ska överklagas till domstolen enligt lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter.

Paragrafen reglerar Försvarsunderrättelsedomstolens uppgifter. Genom det nya andra stycket tillförs Försvarsunderrättelsedomstolen två nya uppgifter. Tidigare hade domstolen endast till uppgift att pröva frågor om tillstånd till signalspaning. De allmänna övervägandena görs i avsnitt 9.6.3 respektive 10.7.2.

Av andra stycket framgår, i *punkten 1*, att Försvarsunderrättelsedomstolen ska pröva frågor om framtagning enligt lagen om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar. Ändringen är en följd av att domstolen i 4 kap. 1 § pekats ut som exklusivt forum för ansökningar om tillstånd till framtagning. I normalfallet prövas frågan om tillstånd efter en ansökan från Säkerhetspolisen. Handläggningsreglerna för mål om tillstånd till framtagning finns i lagen om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar.

Av *punkten 2* framgår att domstolen även ska pröva beslut som ska överklagas till Försvarsunderrättelsedomstolen enligt lagen om Säkerhetspolisens behandling av personuppgifter. Det avser tillsynsmyndighetens överklagbara beslut om förelägganden eller förbud enligt 7 kap. 5 § i den lagen.

2 §

Försvarsunderrättelsedomstolen består av *högst två* ordförande, *högst två* vice ordförande samt minst två och högst *tio* särskilda ledamöter. *En av ordförandena ska vara chef för domstolen.*

Ledamöterna ska vara svenska medborgare och får inte vara underåriga eller i konkurstillstånd eller ha förvaltare enligt 11 kap. 7 § föräldrabalken. Innan en ledamot börjar tjänstgöra i domstolen, ska han eller hon ha avlagt domared.

I lagen (2010:1390) om utnämning av ordinarie domare finns bestämmelser om utnämning av ordförande *tillika chef och övriga* ordförande i domstolen. Vice ordförande och särskilda ledamöter förordnas av regeringen för fyra år.

Paragrafen reglerar Försvarsunderrättelsedomstolens sammansättning. Ändringen innebär att antalet ordförande och särskilda ledamöter har utökats. De allmänna övervägandena finns i avsnitt 9.6.5.

Enligt den tidigare lydelsen bestod domstolen av en ordförande, en eller högst två vice ordförande samt minst två och högst sex särskilda ledamöter. Genom ändringen kan domstolen nu ha högst två ordförande, högst två vice ordförande samt minst två och högst tio särskilda ledamöter. Dessutom anges uttryckligen att en av ordförandena ska vara chef för domstolen.

Utökningen av antalet möjliga ordförande och särskilda ledamöter är en konsekvens av att domstolens verksamhet har utökats med ytterligare arbetsuppgifter enligt 1 §. Med fler ledamöter kan domstolen handlägga både mål om signalspaning och mål om framtagning enligt lagen om särskilda uppgiftssamlingar på ett effektivt sätt utan att handläggningstiderna blir för långa.

Det har också förtydligats att en av ordförandena ska vara chef för domstolen, vilket är naturligt när antalet ordförande kan vara fler än en. I tredje stycket tydliggörs att lagen (2010:1390) om utnämning av ordinarie domare ska tillämpas både på ordförande tillika chef för domstolen och på övriga ordförande.

4 §

Är *en ordförande* förhindrad att tjänstgöra, får en vice ordförande inträda i ordförandens ställe.

Paragrafen reglerar möjligheten för vice ordförande att träda in vid ordförandes förhinder. Ändringen innebär en anpassning till den nya ordningen med möjlighet till flera ordförande. De allmänna övervägandena finns i avsnitt 9.6.5.

Ändringen från *ordföranden* till *en ordförande* är en följdändring med anledning av att domstolen enligt 2 § numera kan ha upp till två ordförande. När någon av dessa är förhindrad att tjänstgöra ska bestämmelsen kunna tillämpas.

Inträder har ersatts med får *inträda*. Genom denna ändring blir det inte längre obligatoriskt för en vice ordförande att träda in vid en ordförandes förhinder, utan det blir i stället en möjlighet som kan utnyttjas efter behov. Detta ger större flexibilitet i domstolens organisation och arbetssätt, vilket är särskilt viktigt när domstolens uppgifter har utökats enligt 1 §.

Den nya konstruktionen innebär att det kan finnas situationer där en ordförande är förhindrad men där arbetsuppgifterna kan omfördelas inom domstolen utan att en vice ordförande behöver träda in. Till exempel kan en annan ordförande ta över, eftersom domstolen nu kan ha två ordförande. Detta bidrar till ett effektivare resursutnyttjande och en mer ändamålsenlig arbetsfördelning inom domstolen.

5 §

Ett integritetsskyddsombud ska bevaka enskildas integritetsintresse i mål vid domstolen *om tillstånd till signalspaning*. Ombudet har rätt att ta del av det som förekommer i målet och att yttra sig.

Paragrafen innehåller bestämmelser om integritetsskyddsombud. Övervägandena finns i avsnitt 9.6.5.

Ändringen innebär ett förtydligande om att regleringen om integritetsskyddsombud avser mål som rör tillstånd till signalspaning och inte mål om tillstånd enligt lagen om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar. Enligt den lagen gäller i stället att den särskilda tillsynsmyndigheten har rätt att närvara och ska kallas till domstolens sammanträden.

9 §

Försvarsunderrättelsedomstolen är domför med *en* ordförande och två särskilda ledamöter. Fler än tre ledamöter får inte delta i ett avgörande.

Paragrafen reglerar domförheten hos domstolen. Ändringen innebär en anpassning till den nya ordningen med möjlighet till flera ordförande. Bestämmelsen är tillämplig vid domstolens prövning av en ansökan om framtagning enligt lagen om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar. Det framgår av en hänvisning i 4 kap. 8 § i den lagen. De allmänna övervägandena finns i avsnitt 9.6.5.

10 a §

I lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar finns regler om handläggningen av mål enligt den lagen.

Paragrafen är ny och innehåller en upplysning om att det finns särskilda handläggningsregler för mål enligt lagen om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar. De allmänna övervägandena finns i avsnitt 9.6.5.

Bestämmelsen har tillkommit som en följd av att Försvarsunderrättelsedomstolen enligt 1 § 2 nu även ska pröva frågor om tillstånd till framtagning enligt lagen om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar. Upplysningsbestämmelsen syftar till att klargöra att 4 kap. i den lagen innehåller särskilda processregler för handläggningen av dessa mål. Dessa specialregler gäller i stället för de allmänna handläggningsbestämmelserna i 11–16 §§ i förevarande lag.

13.6 Förslaget till lag om ändring i lagen (2010:1390) om utnämning av ordinarie domare

1 §

Denna lag avser utnämning av ordinarie domare. Dessa är

1. justitieråd tillika ordförande, justitieråd tillika avdelningsordförande och övriga justitieråd i Högsta domstolen och Högsta förvaltningsdomstolen,
2. president, lagman samt råd tillika vice ordförande på avdelning och övriga råd i hovrätt och kammarrätt,
3. lagman, chefsrådman och rådman i tingsrätt och förvaltningsrätt,
4. tekniska råd,
5. patentråd,
6. ordförande tillika chef och övriga ordförande i Arbetsdomstolen,
7. ordförande *tillika chef och övriga ordförande* i Försvarsunderrättelsedomstolen.

Paragrafens sjunde punkt ändras för att möjliggöra att antalet ledamöter i Försvarsunderrättelsedomstolen utökas. De allmänna motiven finns i avsnitt 9.6.5. I 2 § lagen (2009:966) om Försvarsunderrättelsedomstol finns regler om Försvarsunderrättelsedomstolens sammansättning.

13.7 Förslaget till lag om ändring i lagen (2019:547) om förbud mot användning av vissa uppgifter för att utreda brott

1 §

Uppgifter i underrättelser som Försvarets radioanstalt rapporterat till en annan myndighet i enlighet med lagen (2000:130) om försvarsunderrättelseverksamhet får inte användas för att utreda brott.

Uppgifter som Säkerhetspolisen tagit fram från en särskild uppgiftssamling enligt lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar får inte användas för att utreda brott.

Paragrafen anger att vissa uppgifter inte får användas för att utreda brott. Bestämmelsen ändras genom att den tillförs ett nytt andra stycke. De allmänna motiven finns i avsnitt 9.10.2.

Av andra stycket framgår att uppgifter som tagits fram från en särskild uppgiftssamling enligt lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar inte får användas för att utreda brott.

Det nya andra stycket ska tillämpas på samma sätt som när det gäller uppgifter i underrättelser från Försvarets radioanstalt (se prop. 2018/19:96). Förbudet gäller hos alla brottsbekämpande myndigheter, inte endast hos Säkerhetspolisen.

Enligt paragrafen får de aktuella uppgifterna över huvud taget inte användas för att utreda brott. Förbudet omfattar både användning för att inleda (eller återuppta) en förundersökning och användning i en pågående förundersökning. När det gäller användning i en pågående förundersökning är det otillåtet inte bara att lägga uppgifter till grund för ett beslut, utan också att i brottsutredande syfte till exempel använda uppgifter som utgångspunkt för frågor under ett förhör. Förbudet gäller inte användning av uppgifter för andra syften än att utreda brott, till exempel användning för att förebygga, förhindra och upptäcka brottslig verksamhet (se a. prop. s. 38).

Kommittédirektiv 2023:64

Säkerhetspolisens informationshantering

Beslut vid regeringssammanträde den 11 maj 2023

Sammanfattning

En särskild utredare ska göra en översyn av de bestämmelser som reglerar Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet. Syftet är att skapa ändamålsenliga regler som är anpassade efter dagens behov och möjligheter. Reglerna bör som utgångspunkt ge Säkerhetspolisen ökade möjligheter att behandla personuppgifter, särskilt vad gäller att samla in, sortera, lagra, bearbeta och analysera information med hjälp av tekniska hjälpmedel.

Utredaren ska noga väga myndigheternas behov av att behandla personuppgifter mot den enskildes rätt till skydd för sin personliga integritet. I uppdraget ingår att lämna nödvändiga författningsförslag.

Inom ramen för en översyn av regleringen ska utredaren bl.a.

- beskriva dagens rättsliga möjligheter för Säkerhetspolisen att behandla personuppgifter, särskilt vad gäller att samla in, sortera, lagra, bearbeta och analysera information med hjälp av tekniska hjälpmedel,
- undersöka i vilken utsträckning dagens regelverk försvårar en effektiv informationshantering i Säkerhetspolisens verksamhet,

- lämna förslag som gör att information kan hanteras av Säkerhetspolisen på ett mer ändamålsenligt sätt än i dag, och
- lämna nödvändiga författningsförslag.

Uppdraget ska redovisas senast den 15 november 2024.

Varför behövs det en utredning?

Teknik- och samhällsutvecklingen kräver nya åtgärder

Till Säkerhetspolisens uppgifter hör bland annat att förebygga, förhindra och upptäcka brottslig verksamhet som innefattar brott mot rikets säkerhet eller terrorbrott samt att utreda och beivra sådana brott.

Samhället står ständigt inför stora och föränderliga säkerhetsutmaningar. Hotbilden mot Sverige blir alltmer komplex och det ställer förändrade krav på Säkerhetspolisens förmåga. Digitaliseringen och den tekniska utvecklingen har förändrat samhället i grunden. Förändringen har inneburit att det produceras enorma mängder information. Digitalisering och teknikutveckling har också bidragit till att utveckla hotaktörernas förmåga. Enligt Säkerhetspolisen sker varje dag försök att stjäla uppgifter av betydelse för Sveriges säkerhet och försök att påverka svenskt beslutsfattande på olovliga sätt. Samtidigt bedrivs annan säkerhetshotande verksamhet riktad mot Sverige. Ett förstörande cyberangrepp från främmande makt kan få mycket allvarliga konsekvenser för Sveriges säkerhet och hota jobb, välfärd och konkurrenskraft. Angreppen kan också påverka våra grundläggande fri- och rättigheter, vårt politiska oberoende och vår territoriella suveränitet. Vidare har digitaliseringen gjort extremistmiljöerna globala och tillgängliga för många. Nya digitala plattformar ger förbättrade förutsättningar för kommunikation och möjligheter att hitta och påverka likasinnade.

De möjligheter som teknikutvecklingen innebär behöver tas tillvara också i Säkerhetspolisens arbete. Säkerhetspolisen arbetar ofta initialt utifrån ofullständig information. För att kunna upptäcka okända säkerhetshot måste Säkerhetspolisen samla in stora mängder information, som många gånger är helt öppen, för att analysera vilka uppgifter som kan vara relevanta att agera utifrån, exempelvis för att upp-

täcka spionbrottslighet och förhindra terroristattentat. Säkerhetspolisen måste ha förutsättningar och förmåga att snabbt anpassa sig och utveckla nya metoder och lösningar. Myndighetens uppdrag att bedriva underrättelse- och säkerhetsarbete innebär att huvudfokus ligger på att förebygga, förhindra och upptäcka säkerhetshotande verksamhet. För att lösa uppdraget behöver myndigheten ha tillgång till relevant information och på ett effektivt sätt kunna hantera och bearbeta de stora informationsmängderna. Detta ställer nya krav på Säkerhetspolisens arbetsmetoder och den lagstiftning som reglerar myndighetens informationshantering.

I egenskap av totalförsvarsmyndighet ska Säkerhetspolisen dessutom kunna fullgöra sitt uppdrag vid höjd beredskap och i krig. Det innebär att förutsättningarna för Säkerhetspolisens informationshantering även påverkar myndighetens möjligheter att utföra sina uppgifter inom totalförsvaret. Det försämrade säkerhetsläget i Europa efter Rysslands invasion av Ukraina och Sveriges Natoansökan har ytterligare tydliggjort behovet av att prioritera förmågan inom totalförsvaret. Säkerhetspolisens informationshantering är därför central även utifrån ett totalförsvarsperspektiv.

Stora informationsmängder kan hanteras med tekniska hjälpmedel

Säkerhetspolisen framhåller att det inte längre är möjligt att manuellt granska och strukturera uppgifter med hänsyn till den enorma mängden information som kan vara av intresse för myndighetens verksamhet. Med en sådan ordning kan endast en bråkdel av relevant information analyseras och bedömas. Till skillnad mot tidigare finns det i dag effektiv programvara som kan automatisera informationshanteringen och generera snabbare och mer träffsäkra resultat. Sådan programvara kan exempelvis göra en initial ytlig granskning av stora datamängder och flagga upp information som sannolikt är relevant. En manuell granskning behöver då endast göras av en mindre mängd information som har mer direkt relevans för Säkerhetspolisens uppdrag.

Dagens regelverk behöver ses över

Under 2016 enades EU om en genomgripande dataskyddsreform som skulle vara genomförd under våren 2018. Reformen omfattade dels dataskyddsförordningen ((EU) 2016/679), dels dataskyddsdirektivet (EU) 2016/680). Dataskyddsdirektivet gäller behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder.

Dataskyddsdirektivet har i svensk rätt i huvudsak genomförts genom en ny ramlag, brottsdatalagen (2018:1177), som trädde i kraft den 1 augusti 2018. Verksamhet som rör nationell säkerhet omfattas däremot inte av unionsrätten. Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet omfattas alltså inte av dataskyddsdirektivet och har mot den bakgrunden också undantagits från brottsdatalagens tillämpningsområde (1 kap. 4 § brottsdatalagen).

Jämfört med Polismyndigheten har Säkerhetspolisen en betydligt mer begränsad verksamhet, inriktad på några få områden. Tyngdpunkten ligger på att förebygga, förhindra och upptäcka brottslig verksamhet. Den brottsutredande verksamheten är mer begränsad. Säkerhetspolisen har i uppdrag att skydda Sveriges demokratiska system, medborgarnas fri- och rättigheter och den nationella säkerheten. Säkerhetspolisens verksamhet rör därmed i princip uteslutande nationell säkerhet. Den absoluta merparten av Säkerhetspolisens personuppgiftsbehandling ligger alltså utanför brottsdatalagens tillämpningsområde. I dessa fall gäller lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter (Säkerhetspolisens datalag) och förordningen (2019:1235) om Säkerhetspolisens behandling av personuppgifter. Trots de olikheter i fråga om myndigheternas verksamhet som nämns ovan har Säkerhetspolisens datalag utformats med brottsdatalagens systematik och innehåll som utgångspunkt.

Säkerhetspolisens datalag är visserligen ganska ny men många av bestämmelserna har överförts mer eller mindre oförändrade från tidigare lagstiftning. Det innebär att stora delar av det regelverk som påverkar möjligheterna att behandla personuppgifter kommer från en tid då inte bara hoten mot Sveriges säkerhet utan också de tekniska möjligheterna att behandla personuppgifter var annorlunda än i dag. Regelverket är alltså inte fullt ut anpassat till dagens förhållanden. Vidare står det klart att den tekniska utvecklingen har inneburit att det produceras enorma mängder information och att det

samtidigt har skapats nya möjligheter för Säkerhetspolisen att med hjälp av automatiserade processer behandla stora informationsmängder. Det finns dock enligt nuvarande regelverk tydliga begränsningar för Säkerhetspolisens möjligheter att analysera stora datamängder med hjälp av tekniska hjälpmedel. Säkerhetspolisen anser att förbättrade möjligheter att hantera stora informationsmängder är en förutsättning för att myndigheten ska kunna lösa sitt uppdrag på ett effektivt och framgångsrikt sätt (Säkerhetspolisens hemställan Säkerhetspolisens informationshantering, Ju2022/02624). Sammantaget finns det starka skäl för en översyn av den reglering som styr Säkerhetspolisens behandling av personuppgifter.

Närmare om dagens regelverk och de begränsningar det medför

Regleringen av Säkerhetspolisens personuppgiftshantering fanns tidigare i den numera upphävda polisdatalagen (2010:361). Många av bestämmelserna togs i princip oförändrade in i Säkerhetspolisens datalag och har därför inte fullt ut anpassats till de behov som Säkerhetspolisen har i dag. Dagens regelverk och några av de begränsningar det medför beskrivs nedan.

Rättslig grund och ändamålsbestämmelser

Av 2 kap. 1 § Säkerhetspolisens datalag framgår att personuppgifter får behandlas om det är nödvändigt för att Säkerhetspolisen ska kunna utföra vissa i paragrafen uppräknade uppgifter. Uppgifterna korresponderar i princip med 3 § polislagen (1984:387) som anger Säkerhetspolisens huvudsakliga uppgifter, bl.a. att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott mot rikets säkerhet och terrorbrott samt för att utreda eller lagföra sådana brott. Nödvändighetsrekvisitet innebär i detta sammanhang att personuppgiftsbehandlingen ska behövas för att uppgiften ska gå att fullgöra på ett effektivt sätt (prop. 2018/19:163 s. 65 och 217). När det gäller känsliga personuppgifter krävs dessutom att behandlingen är absolut nödvändig i förhållande till ändamålet (2 kap. 9 § Säkerhetspolisens datalag).

Säkerhetspolisen får bara behandla personuppgifter för särskilda, uttryckligt angivna och berättigade ändamål (2 kap. 3 § Säkerhetspolisens datalag). Att ändamålen ska vara särskilda innebär att de

måste vara tillräckligt specificerade för att ge ledning för bedömningen av vilka uppgifter som är adekvata och relevanta för den aktuella behandlingen och för att det ska kunna avgöras att inte för många uppgifter behandlas. Att ändamålen ska vara berättigade innebär en koppling till den rättsliga grunden.

Personuppgifter får således inte behandlas för ett ändamål som inte är berättigat i förhållande till den tillämpliga rättsliga grunden. I Säkerhetspolisens underrättelseverksamhet, där personuppgifter behöver behandlas på ett tidigt stadium i processen, är det långt ifrån alltid möjligt att ange ändamålen med behandlingen lika tydligt och detaljerat som i annan brottsbekämpande verksamhet. I förarbetena till Säkerhetspolisens datalag framfördes mot den bakgrunden att det får accepteras att beskrivningen av ändamålen inte alltid kan ha samma precision som i annan brottsbekämpande verksamhet. Det finns vidare inget som hindrar att det närmare ändamålet med behandlingen inledningsvis är detsamma som det som anges i bestämmelsen om rättslig grund. Ändamålet får sedan preciseras mer när det är möjligt (prop. 2018/19:163 s. 68).

Trots att Säkerhetspolisens datalag alltså är avsedd att ge generösare ramar för personuppgiftsbehandlingen än brottsdatalagen kan regleringen försvåra en effektiv informationshantering. Bestämmelserna om rättslig grund och ändamål innebär i praktiken att Säkerhetspolisen inte i alla situationer kan inhämta och på annat sätt behandla uppgifter som kan vara avgörande för att till exempel identifiera en okänd terrorist, spion eller annan antagonist eller för att hindra ett attentat. Skälet är att vissa uppgiftssamlingar som Säkerhetspolisen skulle vilja inhämta till stor del innehåller uppgifter om enskilda som inte har eller kan antas ha en klar koppling till Säkerhetspolisens brottsbekämpande verksamhet, men där en delmängd av informationen kan vara avgörande. För att kunna hitta den värdefulla informationen skulle myndigheten behöva inhämta och behandla personuppgifter från hela uppgiftssamlingen, även om det på förhand står klart att majoriteten av uppgifterna inte uppfyller kravet på nödvändighet om man ser på varje uppgift för sig. Om det till exempel kan förmodas att ett attentat planeras eller kan komma att planeras i en viss miljö, digital eller fysisk, kan Säkerhetspolisen behöva inhämta och bearbeta information från hela miljön. Det kan handla om att inhämta informationsmängder från öppna källor, till exempel sådan information som är tillgänglig för var och en via internet. För

att kunna utnyttja den information som finns tillgänglig på ett effektivt sätt skulle Säkerhetspolisen behöva rättsliga förutsättningar för att till exempel samla in och göra jämförelser av fenomen och begrepp som förekommer i sociala medier med hjälp av automatiska processer.

Granskning av uppgifter och kravet på särskilda upplysningar

Om det behövs för att utföra någon av de uppgifter som anges i 2 kap. 1 § Säkerhetspolisens datalag, får personuppgifter göras gemensamt tillgängliga i Säkerhetspolisens verksamhet (3 kap. 2 §). För gemensamt tillgängliga uppgifter ska det genom en särskild upplysning anges för vilket ändamål uppgifterna behandlas om det inte framgår av sammanhanget eller på något annat sätt (3 kap. 3 §). Att en sådan upplysning om ändamålet ska anges har motiverats både av hänsyn till verksamheten och till den personliga integriteten. En upplysning om ändamålet kan också vara en förutsättning för att tillsynsmyndigheten ska kunna kontrollera att viss behandling är berättigad och görs i enlighet med lagens bestämmelser (prop. 2018/19:163 s. 88).

Att tillföra upplysningar om ändamålet med behandlingen av uppgifterna är mycket resurskrävande när det handlar om stora informationsmängder. Samtidigt som sådana upplysningar behöver tillföras måste Säkerhetspolisen också granska om det förekommer känsliga personuppgifter i materialet. Det sker i dag genom att handläggare granskar materialet manuellt. I många fall är det inte möjligt att genomföra en sådan kontroll när det handlar om större informationsmängder. Det kan exempelvis handla om hela trådar i ett forum eller aktiviteter kopplade till en viss person. Det leder i sin tur till att den här typen av inhämtning inte utförs, trots att det skulle kunna vara av stor vikt för Säkerhetspolisens arbete.

Behandling i syfte att utveckla datasystem m.m.

För att på bästa sätt kunna utnyttja de tekniska möjligheter som numera finns att behandla stora informationsmängder automatiskt måste programvarans förmåga utvecklas. För att kunna utveckla programvarans förmåga på ett ändamålsenligt sätt krävs behandling av stora datamängder av olika uppgiftsslag. Med nuvarande regelverks

krav på att behandlingen av personuppgifter ska vara nödvändig i förhållande till den rättsliga grunden är det osäkert om behandling av personuppgifter över huvud taget kan ske i syfte att utveckla datasystem och träna upp modeller för maskininlärning. Enligt Säkerhetspolisen är det viktigt att myndigheten får möjlighet att behandla stora mängder relevanta data i syfte att utveckla tekniska lösningar så att de fungerar på bästa sätt.

Längsta tid för behandling

I 4 kap. Säkerhetspolisens datalag finns bestämmelser om hur länge personuppgifter får behandlas. Syftet med bestämmelserna är att skydda den personliga integriteten. Allmänt gäller att personuppgifter inte får behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen (4 kap. 1 §). Därutöver finns särskilda regler för olika situationer. Personuppgifter som inte har gjorts gemensamt tillgängliga får till exempel inte behandlas längre än ett år efter det att ärendet avslutades, om de behandlas i ett ärende, eller ett år efter det att de behandlades automatiserat första gången, om de inte kan hänföras till ett ärende. Personuppgifter som gjorts gemensamt tillgängliga får inte behandlas längre än tio år efter utgången av det kalenderår då den senaste registreringen gjordes avseende personen.

På grund av den långsiktighet som präglar framför allt kontraspionageverksamheten förlängdes tiden som den typen av uppgifter får behandlas när Säkerhetspolisens datalag infördes. Personuppgifter som hänför sig till sådan säkerhetshotande verksamhet som avses i 18 och 19 kap. brottsbalken och som utövas av främmande makt, får behandlas högst 40 år efter utgången av det kalenderår då den senaste registreringen gjordes avseende personens anknytning till brott eller brottslig verksamhet. Säkerhetspolisen ansåg i samband med lagstiftningsärendet att sådana personuppgifter borde få behandlas som längst i 70 år. Säkerhetspolisen har nu framfört synpunkter på att bestämmelserna i kapitlet medför att uppgifter som i ett senare skede skulle kunna vara avgörande i t.ex. arbetet med kontraspionage eller kontraterrorism inte får behandlas tillräckligt länge. Säkerhetspolisen behöver kunna behandla uppgifterna över tid för att bearbeta informationen och därmed kunna upptäcka mönster eller samband.

Uppdraget att se över Säkerhetspolisens personuppgiftsreglering i syfte att skapa ändamålsenliga regler som är anpassade efter dagens behov

Säkerhetspolisen har pekat på att regelverket som styr myndighetens personuppgiftshantering inte alltid ger förutsättningar för att samla in och behandla uppgifter som kan vara avgörande i verksamheten. Det är mycket angeläget att Säkerhetspolisen har ändamålsenliga bestämmelser i detta avseende. Den nuvarande lagstiftningen fungerar i vissa avseenden väl. Samtidigt stöter Säkerhetspolisen i dag på problem bland annat vid tillämpningen av de i Säkerhetspolisens datalag fundamentala bestämmelserna om rättslig grund och ändamål för behandlingen. Utredarens övergripande uppdrag är därför att göra en översyn av de bestämmelser som reglerar Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet. Syftet är att skapa ändamålsenliga regler som är anpassade efter dagens behov och möjligheter. De författningar som står i fokus är Säkerhetspolisens datalag med tillhörande förordning. Ovan har några av de begränsningar som Säkerhetspolisen lyft fram beskrivits. Uppdraget att göra en översyn av regleringen gäller emellertid inte endast dessa begränsningar.

Beträffande flera andra myndigheter finns förslag eller pågående lagstiftningsarbete som tar sikte på ökade möjligheter att använda dataanalyser och urval för att effektivisera informationshanteringen i verksamheten (se t.ex. dir. 2021:104, En modern dataskyddsreglering för Skatteverket, Tullverket och Kronofogdemyndigheten och förbättrade förutsättningar för en effektiv kontrollverksamhet). Utifrån Säkerhetspolisens uppdrag som nationell säkerhetstjänst och med tanke på Säkerhetspolisens underrättelse- och säkerhetsarbete finns det goda skäl för att myndigheten bör ha ett mer generöst regelverk kring personuppgiftsbehandlingen än många andra myndigheter. I Norge pågår också lagstiftningsarbete för att ge ökade möjligheter för säkerhetstjänsten (Politiets sikkerhetstjeneste) att behandla stora informationsmängder med hjälp av tekniska hjälpmedel.

Mot den bakgrunden bör en utgångspunkt för översynen vara att Säkerhetspolisen ska få ökade möjligheter att behandla personuppgifter, t.ex. genom att samla in, sortera, lagra, bearbeta och analysera information med hjälp av tekniska hjälpmedel. Detta är också utredningens huvudfokus. Reglerna behöver vara teknikneutrala och

flexibla samt ge Säkerhetspolisen möjlighet att utveckla och anpassa arbetet efter samhällsutvecklingen.

Uppdraget omfattar endast Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet, och alltså inte den behandling som ligger inom brottsdatalagens tillämpningsområde. Det ligger heller inte inom ramen för utredarens uppdrag att se över sekretessregleringen som kan påverka vilka uppgifter Säkerhetspolisen har möjlighet att ta del av. Däremot kan det finns behov av sekretessregler för att skydda den informationshantering som utredarens förslag kan medföra.

Utredaren ska

- göra en översyn av de bestämmelser som reglerar Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet,
- beskriva dagens rättsliga möjligheter för Säkerhetspolisen att behandla personuppgifter, särskilt vad gäller att samla in, sortera, lagra, bearbeta och analysera information med hjälp av tekniska hjälpmedel,
- undersöka i vilken utsträckning dagens regelverk försvårar en effektiv informationshantering i Säkerhetspolisens verksamhet,
- lämna förslag som gör att information kan hanteras av Säkerhetspolisen på ett mer ändamålsenligt sätt än i dag, och
- lämna nödvändiga författningsförslag.

Utredaren ska noga väga Säkerhetspolisens behov av att behandla personuppgifter mot den enskildes rätt till skydd för sin personliga integritet. Särskilda integritetsskyddande åtgärder bör därvid övervägas.

Utredaren ska också vid utformningen av förslagen beakta att tillsynsmyndigheterna ska ges förutsättningar att kunna fullgöra sin uppgift att utöva tillsyn över personuppgiftsbehandlingen på ett effektivt sätt. Om det bedöms nödvändigt får utredaren ta upp andra närliggande frågor i samband med de frågeställningar som ska utredas.

Grundläggande fri- och rättigheter ska beaktas

Enligt 2 kap. 6 § andra stycket regeringsformen är var och en skyddad gentemot det allmänna mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Inskränkningar i det grundlagsfästa skyddet kan endast göras genom lag och bara under de förutsättningar som anges i 2 kap. 20–22 och 25 §§ regeringsformen.

Rätten till respekt för privat- och familjelivet och för korrespondens skyddas också av bl.a. artikel 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) och artikel 16 i FN:s konvention om barnets rättigheter (barnkonventionen). Vidare framgår det av artikel 3 i barnkonventionen att vid samtliga åtgärder och beslut som rör barn ska i första hand vad som bedöms vara barnets bästa beaktas.

Detta grundläggande skydd för enskildas integritet är inte absolut. Av såväl regeringsformen som Europakonventionen framgår att skyddet under vissa förutsättningar får begränsas. En begränsning i utövande av rättigheten får göras endast om det sker i enlighet med lag och det är nödvändigt för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. En begränsning får aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den.

Att föreslå grundlagsändringar ingår inte i utredarens uppdrag. De förslag som utredaren lämnar måste alltså vara förenliga med regeringsformen och naturligtvis också med Europakonventionen, barnkonventionen och Sveriges internationella förpliktelser i övrigt.

Dataskyddskonventionen måste beaktas

Eftersom varken dataskyddsdirektivet eller dataskyddsförordningen omfattar behandling av personuppgifter som utförs i verksamhet som rör nationell säkerhet finns det ur EU-rättslig synvinkel inte något som hindrar att regleringen som styr Säkerhetspolisens personuppgiftsbehandling i den delen utformas på ett annat sätt än det EU-rättsliga regelverket. Europarådets ministerkommitté antog 1981 en konvention till skydd för enskilda vid automatisk databehandling av personuppgifter, den s.k. dataskyddskonventionen. Konventionen

var en av de viktigaste inspirationskällorna vid utformningen av EU:s regelverk för dataskydd. Konventionen gäller även i verksamhet som rör nationell säkerhet och Sverige är folkrättsligt bundet av konventionen med dess tilläggsprotokoll. En särreglering av Säkerhetspolisens personuppgiftsbehandling får alltså inte strida mot bestämmelserna i dataskyddskonventionen (se t.ex. prop. 2018/19:163 s. 50).

Eftersom det EU-rättsliga regelverket bygger på och vidareutvecklar dataskyddskonventionen liknar många bestämmelser varandra. I dataskyddskonventionen finns det exempelvis bestämmelser om att personuppgifter ska behandlas på ett korrekt och lagligt sätt och att de ska lagras för särskilt angivna och lagliga ändamål och inte användas på ett sätt som är oförenligt med dessa ändamål samt att de ska bevaras på ett sådant sätt att de registrerade personerna inte kan identifieras under längre tid än vad som är nödvändigt med hänsyn till det ändamål för vilket dessa uppgifter lagras (artikel 5). Till skillnad från i det EU-rättsliga regelverket finns dock möjligheter att göra undantag från de grundläggande bestämmelserna. Undantag får göras endast om en sådan avvikelse medges i nationell lagstiftning och den är nödvändig i ett demokratiskt samhälle för att skydda statens säkerhet, den allmänna säkerheten, statens penningintresse eller brottsbekämpning samt för att skydda den registrerade personen eller andra personers fri- och rättigheter (artikel 9).

Konventionen kompletteras av ett antal av ministerkommittén antagna rekommendationer om hur personuppgifter bör behandlas inom olika områden. En sådan rekommendation rör behandling av stora datamängder (Council of Europe, Guidelines on the Protection of Individuals with regard to the Processing of Personal Data in a World of Big Data, 17 January 2017). I syfte att modernisera konventionen har en översyn av den pågått inom Europarådet. Förhandlingarna resulterade i maj 2018 i att ett ändringsprotokoll antogs. Ändringsprotokollet innebär bland annat att möjligheterna att göra undantag från de grundläggande principerna om dataskydd blir mindre än i nuvarande utformning. Sverige tillhörde de första konventionsstaterna att underteckna protokollet. Ändringsprotokollet träder dock inte i kraft förrän alla parter har ratificerat protokollet (eller om minst 38 parter har gjort det den 11 oktober 2023).

Utredarens förslag måste anpassas till bestämmelserna i dataskyddskonventionen med ändringsprotokoll.

Konsekvensbeskrivningar

Utredaren ska utöver vad som följer av kommittéförordningen (1998:1474) noga analysera vilka konsekvenser de förslag som lämnas har för den personliga integriteten. Utredaren ska också bedöma hur förslagen förhåller sig till Sveriges internationella åtaganden om mänskliga rättigheter.

Kontakter och redovisning av uppdraget

Utredaren ska under arbetet samråda med och hämta in synpunkter och upplysningar från Säkerhetspolisen. Vid behov ska utredaren hämta in synpunkter och upplysningar även från andra myndigheter och aktörer som kan vara berörda. Utredaren ska också följa utvecklingen beträffande de rättsliga förutsättningarna för säkerhetstjänstens informationshantering i Norge, och vid behov även i andra länder. Utredaren ska också hålla sig informerad om och ta hänsyn till relevant arbete som pågår inom Regeringskansliet och kommittéväsendet samt inom ramen för Sveriges internationella åtaganden.

Uppdraget ska redovisas senast den 15 november 2024.

(Justitiedepartementet)

Kommittédirektiv 2024:99

Tilläggsdirektiv till Utredningen om Säkerhetspolisens informationshantering (Ju 2023:02)

Beslut vid regeringssammanträde den 24 oktober 2024

Förlängd tid för uppdraget

Regeringen beslutade den 11 maj 2023 kommittédirektiv om Säkerhetspolisens informationshantering (dir. 2023:64). Uppdraget skulle redovisas senast den 15 november 2024.

Utredningstiden förlängs. Uppdraget ska i stället redovisas senast den 1 april 2025.

(Justitiedepartementet)

Statens offentliga utredningar 2025

Kronologisk förteckning

1. Skärpta krav för svenskt medborgarskap. Ju.
2. Några frågor om grundläggande fri- och rättigheter. Ju.
3. Skatteincitament för forskning och utveckling. En översyn av FoU-avdraget och expertskattereglerna. Fi.
4. Moderna och enklare skatteregler för arbetslivet. Fi.
5. Avgift för områdessamverkan – och andra åtgärder för trygghet i byggd miljö. LI.
6. Plikten kallar! En modern personalförsörjning av det civila försvaret. Fö.
7. Ny kärnkraft i Sverige – effektivare tillståndsprövning och ändamålsenliga avgifter. KN.
8. Bättre förutsättningar för trygghet och studiero i skolan. U.
9. På språklig grund. U.
10. En förändrad abortlag – för en god, säker och tillgänglig abortvård. S.
11. Straffbarhetsåldern. Ju.
12. AI-kommissionens Färdplan för Sverige. Fi.
13. En effektivare organisering av mindre myndigheter – analys och förslag. Fi.
14. En skärpt miljöstraffrätt och ett effektivt sanktionssystem. KN.
15. Stärkta drivkrafter och möjligheter för biståndsmottagare. Volym 1 och 2. S.
16. Ett nytt regelverk för uppsikt och förvar. Ju.
17. Anpassning av svensk rätt till EU:s avskogningsförordning. LI.
18. Ett likvärdigt betygssystem. Volym 1 och 2. U.
19. Kunskap för alla – nya läroplaner med fokus på undervisning och lärande. U.
20. Kommunal anslutning till Utbetalningsmyndighetens verksamhet. Fi.
21. Miljömålsberedningens förslag om en strategi för hur Sverige ska leva upp till EU:s åtaganden inom biologisk mångfald respektive nettoupptag av växthusgaser från markanvändningssektorn (LULUCF). KN.
22. Förbättrad konkurrens i offentlig och privat verksamhet. KN.
23. Ersättningsregler med brottsoffret i fokus. Ju.
24. Publiken i fokus – reformer för ett starkare filmland. Ku.
25. Arbetslivskriminalitet – upplägg, verktyg och åtgärder, fortsatt arbete. A.
26. Tid för undervisningsuppdraget – åtgärder för god undervisning och läraryrkenas attraktivitet. U.
27. En socionomutbildning i tiden. U.
28. Frihet från våld, förtryck och utnyttjande. En jämställdhetspolitisk strategi mot våld och en stärkt styrning av centrala myndigheter. A.
29. Ökad kvalitet hos Samhall och fler vägar till skyddat arbete. A.
30. Enklare mervärdesskatteregler vid försäljning av begagnade varor och donation av livsmedel. Fi.
31. Utmönstring av permanent uppehållstillstånd och vissa anpassningar till miniminivån enligt EU:s migrations- och asylpakt. Ju.
32. Vissa förändringar av jaktlagstiftningen. LI.
33. Skärpta och tydligare krav på vandel för uppehållstillstånd. Ju.
34. Ett modernare konsumentskydd vid distansavtal. Ju.
35. Etableringsboendelagen – ett nytt system för bosättning för vissa nyanlända. A.

36. Skydd för biologisk mångfald i havsområden utanför nationell jurisdiktion. UD.
37. Skärpta villkor för friskolesektorn. U.
38. Att omhänderta barn och unga. S.
39. Digital teknik på lika villkor. En reglering för socialtjänsten och verksamhet enligt LSS. S.
40. Säkrare tivoli. Ju.
41. Pensionsnivåer och pensionsavgiften – analyser på hundra års sikt. S.
42. Säkerhetsskyddslagen – ytterligare kompletteringar. Ju.
43. Säkerställ tillgången till läkemedel – förordnande och utlämnande i bristsituationer. S.
44. Förbättrat stöd i skolan. U.
45. Ökat informationsutbyte mellan myndigheter – några anslutande frågor. Ju.
46. Tryggare idrottsarrangemang. Ju.
47. Spänning i tillvaron – hur säkrar vi vår framtida elförsörjning? KN.
48. Stärkt pandemiberedskap. S.
49. Säkerhetspolisens behandling av personuppgifter. Ju.

Statens offentliga utredningar 2025

Systematisk förteckning

Kulturdepartementet

Publiken i fokus – reformer för ett starkare filmland. [24]

Landsbygds- och infrastrukturdepartementet

Avgift för områdessamverkan – och andra åtgärder för trygghet i byggd miljö. [5]

Anpassning av svensk rätt till EU:s avskogningsförordning. [17]

Vissa förändringar av jaktlagstiftningen. [32]

Socialdepartementet

En förändrad abortlag – för en god, säker och tillgänglig abortvård. [10]

Stärkta drivkrafter och möjligheter för biståndsmottagare Volym 1 och 2. [15]

Att omhänderta barn och unga. [38]

Digital teknik på lika villkor. En reglering för socialtjänsten och verksamhet enligt LSS. [39]

Pensionsnivåer och pensionsavgiften – analyser på hundra års sikt. [41

Säkerställ tillgången till läkemedel – förordnande och utlämnande i bristsituationer. [43]

Stärkt pandemiberedskap. [48]

Utbildningsdepartementet

Bättre förutsättningar för trygghet och studiero i skolan. [8]

På språklig grund. [9]

Ett likvärdigt betygssystem Volym 1 och 2. [18]

Kunskap för alla – nya läroplaner med fokus på undervisning och lärande. [19]

Tid för undervisningsuppdraget – åtgärder för god undervisning och läraryrkenas attraktivitet. [26]

En socionomutbildning i tiden [27]

Skärpta villkor för friskolesektorn. [37]

Förbättrat stöd i skolan [44]

Utrikesdepartementet

Skydd för biologisk mångfald i havsområden utanför nationell jurisdiktion. [36]