Hemlig dataavläsning

– utvärdering och permanent lagstiftning

Betänkande av Utredningen om utvärdering av hemlig dataavläsning

Stockholm 2023

STATENS OFFENTLIGA UTREDNINGAR

SOU 2023:78

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 2023

ISBN 978-91-525-0774-2 (tryck)
ISBN 978-91-525-0775-9 (pdf)
ISSN 0375-250X

Till statsrådet och chefen för Justitiedepartementet

Regeringen beslutade den 22 juni 2022 att ge en särskild utredare i uppdrag att utvärdera lagen (2020:62) om hemlig dataavläsning inför ett ställningstagande till om lagen bör permanentas och om den i så fall bör ändras i något avseende. Hovrättspresidenten Ylva Norling Jönsson förordnades samma dag till särskild utredare.

Den 20 september 2022 förordnades rättssakkunniga Staffan Uhlmann, Justitiedepartementet, som sakkunnig i utredningen. Som experter förordnades samma dag advokaten Maria Adielsson (Sveriges advokatsamfund), chefsrådmannen Märit Bergendahl (Sveriges Domstolar), seniora verksjuristen Marie-Louise Dock Collin (Säkerhetspolisen), seniora juristen Andreas Persson (Integritetsskyddsmyndigheten), handläggaren Daniel Grahn (Polismyndigheten), seniora föredraganden Johanna Herder Toll (Säkerhets- och integritetsskyddsnämnden), juristen Sofie Klahr (Polismyndigheten), kammaråklagaren Mats Ljungqvist (Riksenheten för säkerhetsmål), verksjuristen Micaela Nordberg (Tullverket), enhetschefen Robert Nygren (Säkerhetspolisen), vice chefsåklagaren Helena Rosvall (Ekobrottsmyndigheten) och kammaråklagaren Christoffer Östlind (Åklagarmyndigheten).

Den 18 augusti 2023 entledigades Sofie Klahr från uppdraget som expert och gruppchefen Marie Skåninger (Polismyndigheten) förordnades i hennes ställe.

Hovrättsassessorn Maria Carnheimer har varit sekreterare i utredningen från och med den 1 september 2022.

Arbetet har bedrivits i nära samråd med den sakkunniga och experterna. Betänkandet är därför skrivet i vi-form, även om det har funnits skilda uppfattningar i enskilda sakfrågor. Experterna och den sak-

kunniga har dock i allt väsentligt ställt sig bakom utredningens överväganden och förslag.

Utredningen om utvärdering av hemlig dataavläsning överlämnar härmed betänkandet *Hemlig dataavläsning – utvärdering och permanent lagstiftning* (SOU 2023:78). Uppdraget är med detta slutfört.

Malmö i november 2023

Ylva Norling Jönsson

/Maria Carnheimer

Innehåll

Sammanfattning

Uppdraget

Vårt uppdrag har varit att utvärdera lagen (2020:62) om hemlig dataavläsning och ta ställning till om lagen bör permanentas samt om den i så fall bör ändras i något avseende. Genom lagen om hemlig dataavläsning, som trädde i kraft den 1 april 2020, infördes ett nytt hemligt tvångsmedel som de brottsbekämpande myndigheterna kan använda vid misstankar om allvarlig brottslighet. Lagen är tidsbegränsad till utgången av mars 2025. I uppdraget har bland annat ingått att analysera nyttan och behovet av hemlig dataavläsning, att ta ställning till om lagstiftningen bör permanentas och föreslå de åtgärder som behövs för ett permanentande, att analysera om lagstiftningen har fått en ändamålsenlig och proportionerlig utformning eller om det behövs förändringar i regelverket, samt att lämna förslag på de författningsändringar och andra åtgärder som bedöms nödvändiga. Uppdraget har innefattat att säkerställa att en välfungerande systematik i regelverket kring såväl hemliga som öppna tvångsmedel upprätthålls. Det har också ingått i uppdraget att noga väga behovet av en effektiv brottsbekämpning mot den enskildes rätt till skydd för grundläggande fri- och rättigheter, såsom den personliga integriteten, och säkerställa att förslagen uppfyller högt ställda krav på rättssäkerhet.

Vad är hemlig dataavläsning?

Hemlig dataavläsning är ett verktyg som ger de brottsbekämpande myndigheterna möjlighet att komma åt information som är svårtillgänglig, till exempel på grund av kryptering. Hemlig dataavläsning används i första hand när andra tvångsmedel eller metoder inte är framkomliga alternativ. I praktiken handlar hemlig dataavläsning om att de brottsbekämpande myndigheterna med hjälp av tekniska hjälp-

medel i hemlighet får hämta in uppgifter som är åtkomliga i en dator, en mobiltelefon, ett användarkonto på internet eller något annat avläsningsbart informationssystem. För att få använda hemlig dataavläsning krävs som en grundläggande förutsättning att det är fråga om allvarlig brottslighet, exempelvis spionerі, terroristbrott, grovt dataintrång, grovt narkotikabrott, grovt vapenbrott, våldtäkt eller mord. Hemlig dataavläsning får under vissa närmare förutsättningar användas under en förundersökning, i underrättelseverksamhet och vid särskild utlänningskontroll, liksom i det internationella straffrättsliga samarbetet.

En permanent lagstiftning – avvägningar om behov, effektivitet och integritet

Sverige befinner sig i en situation där brottsligheten har stegrat i omfattning och blivit mer samhällshotande. Som exempel kan nämnas den markanta ökningen av dödligt skjutvapenvåld som skett de senaste åren. Våldsbrottsligheten är i sin tur starkt kopplad till den ökade narkotikabrottsligheten. En betydande ökning av den allvarliga brottsligheten har noterats också i underrättelsemiljön. Även den internationella säkerhetssituationen har fått konsekvenser för Sverige. Kriminellas handlingssätt och hur de kommunicerar är i förändring. Särskilt inom den allvarliga och organiserade brottsligheten används ofta krypterade tjänster och elektronisk utrustning för att kommunicera, i direkt syfte att undgå myndigheternas insyn. Globaliseringen, den tekniska utvecklingen och förändrade kommunikationsvanor har inneburit att de brottsbekämpande myndigheterna inte längre kan ta del av information som tidigare var tillgänglig genom traditionella tvångsmedel. Sedan möjligheten till hemlig dataavläsning infördes har betydelsen av effektiv tillgång till elektronisk bevisning blivit ännu mer framträdande. Detta gäller även i det internationella rättsliga samarbetet, eftersom den allvarliga brottslighet som kan föranleda hemlig dataavläsning inte sällan är av gränsöverskridande natur. Vid en internationell utblick kan det konstateras att i princip alla EU-länder samt USA, Kanada och Australien har lagstadgade möjligheter att använda hemlig dataavläsning, eller en motsvarighet till åtgärden, som ett verktyg i brottsbekämpningen. Det kan konstateras att den svenska tvångsmedelslagstiftningen måste hålla jämna steg med såväl teknik-

och samhällsutvecklingen som den internationella rättsutvecklingen för att fortsatt kunna bekämpa den allvarliga brottsligheten.

De brottsbekämpande myndigheterna har nu haft möjlighet att använda hemlig dataavläsning i drygt 3,5 år. Våra analyser visar att hemlig dataavläsning har kommit till användning i större omfattning än vad som förutsågs när det nya tvångsmedlet infördes. De brottsbekämpande myndigheternas erfarenheter av hemlig dataavläsning har också varit mycket goda. De beskrivningar och praktiska exempel som har lämnats visar att hemlig dataavläsning i många fall har varit ett helt avgörande verktyg i den brottsbekämpande verksamheten. Hemlig dataavläsning har både lett till konkreta uppgifter om brott som redan begåtts och uppgifter som har kunnat användas för att förhindra allvarlig brottslighet. Hemlig dataavläsning har också i flera fall använts för att komma åt information om hur olika typer av grov brottslighet är organiserad och vilka personer som finns högre upp i hierarkin. Eftersom informationen inte varit åtkomlig genom andra tvångsmedel har hemlig dataavläsning i dessa fall inneburit ett genombrott i kampen mot den allvarliga och organiserade brottsligheten. Det står klart att användningen av hemlig dataavläsning är ett effektivt verktyg för att få tillgång till information och att åtgärden har medfört avsevärd nytta i brottsbekämpningen. Vi bedömer sammantaget att det finns ett fortsatt påtagligt behov av hemlig dataavläsning för att kunna bekämpa den allvarliga brottsligheten. Inget talar för att behovet skulle vara av tillfällig natur. Behovet kan inte heller tillgodoses med befintliga bestämmelser om straffprocessuella tvångsmedel. Samtidigt bedömer vi att hemlig dataavläsning innebär risker för den personliga integriteten.

Vi har vägt behovet av en effektiv brottsbekämpning för att förebygga, förhindra, upptäcka och utreda allvarlig brottslighet, effektiviteten av åtgärden och den nytta som möjligheten att använda hemlig dataavläsning har medfört och kan förväntas medföra, mot de integritetsrisker som åtgärden innebär. I denna avvägning har vi även beaktat statens skyldighet att upprätthålla rättstrygghet för enskilda och skydda sina medborgare mot ingrepp i privatlivet från andra. Vi har sammantaget funnit att det är proportionerligt att hemlig dataavläsning blir ett permanent tvångsmedel. Åtgärden bedöms helt nödvändig med hänsyn till intresset av att bekämpa den allvarliga brottsligheten och för att kunna upprätthålla enskildas rättstrygghet och rätt till skydd mot kränkningar från andra enskilda. Vårt förslag om

att permanenta lagstiftningen gäller under förutsättning att tillämpningsområdet är avgränsat på ett tydligt och ändamålsenligt sätt samt att lagstiftningen innehåller särskilda kvalifikationskrav och rättssäkerhetsgarantier som kan balansera de ökade risker som åtgärden innebär för den personliga integriteten. Vi föreslår därför även vissa ändringar i det nuvarande regelverket om hemlig dataavläsning.

Tydligare bestämmelser och ett utökat tillämpningsområde

Våra förslag på ändringar i lagen om hemlig dataavläsning innebär till övervägande del förtydliganden av lagstiftningen. Dessa syftar till att förenkla ansöknings- och beslutsprocessen samt undanröja den osäkerhet som i dag kan finnas angående ett tillstånds omfattning. Vi har i alla våra överväganden strävat efter att upprätthålla en välfungerande systematik i regelverket kring såväl hemliga som öppna tvångsmedel. De viktigaste konsekvenserna av våra förslag är att det blir tydligare under vilka förutsättningar som hemlig dataavläsning får användas, hur det inhämtade materialet ska hanteras och vilka skyldigheter som åligger tillämparen. Vi bedömer att våra förslag om en tydligare och mer förutsebar lagstiftning medför att lagen om hemlig dataavläsning kommer att stå i bättre överensstämmelse med de högt ställda krav på rättssäkerhet och de krav på skydd för enskildas personliga integritet som följer av regeringsformen, Europakonventionen och EU-rätten. Några av våra förslag innebär även en viss utvidgning av tillämpningsområdet för hemlig dataavläsning och att de brottsbekämpande myndigheterna får mer effektiva verktyg i arbetet med att utreda samt förebygga, förhindra och upptäcka viss allvarlig brottslighet. Vid en intresseavvägning mellan behovet av en effektiv brottsbekämpning och den enskildes rätt till skydd för sin personliga integritet har vi funnit att den ökade risk för ingrepp i den personliga integriteten som våra förslag innebär är försvarlig.

Eftersom lagstiftningen om hemlig dataavläsning och andra hemliga tvångsmedel är under utveckling har det också varit nödvändigt att göra en samlad proportionalitetsbedömning av hela det utökade och tilltänkta tillämpningsområdet för hemlig dataavläsning. Flera lagändringar som påverkar tillämpningsområdet för hemlig dataavläsning trädde i kraft så sent som den 1 oktober 2023 och ytterligare lagför-

slag som kan komma att påverka tillämpningsområdet är för närvarande under beredning. Vid en samlad bedömning har vi funnit att hela det utökade och tilltänkta tillämpningsområdet för hemlig dataavläsning är tillräckligt ändamålsenligt och tydligt avgränsat för att kunna skydda enskilda mot godtyckliga ingrepp i deras fri- och rättigheter. Även med beaktande av det samlade integritetsintrång som genomförandet av våra förslag innebär, tillsammans med nuvarande lagstiftning och de ytterligare lagförslag som nu bereds och kan komma att träda i kraft inom kort, är det vår bedömning att regelverket för hemlig dataavläsning ger uttryck för en rimlig avvägning mellan behovet av en effektiv brottsbekämpning och den enskildes rätt till skydd för sin personliga integritet.

Innebörden av hemlig dataavläsning förtydligas

Vi föreslår att innebörden av hemlig dataavläsning förtydligas. Förfarandet vid hemlig dataavläsning omfattar *inhämtning* (avläsning och överföring) samt *bearbetning* (förädling, sortering, filtrering och granskning) av uppgifter. Med hänsyn till hur hemlig dataavläsning fungerar kan det uttryck som för närvarande används för att definiera hemlig dataavläsning – att uppgifter ”läses av eller tas upp” – i vissa avseenden vara missvisade och orsaka tillämpningssvårigheter. Uttrycket ersätts därför med ”inhämtas”. I lagens portalparagraf klargörs således att hemlig dataavläsning innebär att uppgifter, som är avsedda för automatiserad behandling och som är åtkomliga i ett avläsningsbart informationssystem, *inhämtas* i hemlighet och med ett tekniskt hjälpmedel. Genom andra bestämmelser i lagen tydliggörs hur de inhämtade uppgifterna sedan får *bearbetas*. Ändringen medför därför vissa förtydliganden även i andra bestämmelser i lagen.

En tydligare bestämmelse om de olika uppgiftstyperna

I lagen om hemlig dataläsning anges sju olika uppgiftstyper, se 2 § första stycket 1–7. Uppgiftstyperna i 1–5 (kommunikationsavlyssningsuppgifter, kommunikationsövervakningsuppgifter, platsuppgifter, kameraövervakningsuppgifter och rumsavlyssningsuppgifter) har sin motsvarighet i andra permanenta hemliga tvångsmedel. Uppgiftstyperna i 6 och 7 är unika för hemlig dataavläsning. Punkt 6 avser upp-

gifter som finns lagrade i ett avläsningsbart informationssystem men som inte avses i punkt 1–5, och punkt 7 avser uppgifter som visar hur ett avläsningsbart informationssystem används men som inte avses i punkt 1–6. I praktiken innebär denna uppdelning att lagrade uppgifter som inte är att sortera under punkt 1–3 utgör punkt 6-uppgifter och att realtidsuppgifter som inte är att sortera under punkt 1–5 och som visar hur ett informationssystem används utgör punkt 7-uppgifter.

Uppdelningen i olika uppgiftstyper får betydelse redan vid tillståndsgivningen, eftersom det i ett tillstånd till hemlig dataavläsning alltid ska anges vilken uppgiftstyp som får hämtas in. Detta s.k. differentieringskrav har orsakat vissa praktiska tillämpningsproblem. Orsaken är att det sällan före verkställighet går att avgöra hur lagstiftningens kategorisering av olika uppgiftstyper ska appliceras på den information som kan komma att påträffas. Gränsdragningsproblematiken mellan uppgiftstyperna i punkt 6 och 7 har varit särskilt svår. Vi föreslår därför att punkt 6 och 7 slås ihop till en ny punkt 6 som inte gör skillnad på om uppgifterna är lagrade eller om de utgör realtidsuppgifter. Vi bedömer samtidigt att det även fortsatt ska göras en åtskillnad mellan var och en av uppgiftstyperna i 1–5 respektive uppgifter som sorterar under den nya punkten 6. Även om uppdelningen medför vissa praktiska utmaningar bedöms differentieringskravet utgöra en viktig skyddsåtgärd för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan.

Den hittillsvarande tillämpningen visar att det som regel finns ett påtagligt behov av hemlig dataavläsning av flera uppgiftstyper i varje enskilt fall. Ett typiskt tillstånd till hemlig dataavläsning behöver omfatta uppgiftstyperna i 1–3 och den nya punkten 6 för att åtgärden ska bli ändamålsenlig. Risken är annars att tillståndet får mindre räckvidd än avsett och att de brottsbekämpande myndigheterna därmed går miste om relevant information. En annan risk är att inhämtade uppgifter kan komma att betraktas som otillåten tilläggsinformation, om de eftersökta uppgifterna visar sig sortera under en annan punkt än förväntat. Ur rättssäkerhetssynpunkt framstår det som angeläget att fokus vid tillståndsprövningen ligger på den rättsliga prövningen och inte på hur behovet av information tekniskt sett är att kategorisera. Vi föreslår därför en förtydligande huvudregel som innebär att ett tillstånd till hemlig dataavläsning ska omfatta uppgiftstyperna i 1–3 och den nya punkten 6, om inget annat särskilt beslutas eller framgår av andra bestämmelser. Införandet av en sådan huvud-

regel balanseras av att vi samtidigt föreslår tydligare bestämmelser om villkor. Om det vid tillståndsprövningen inte är ändamålsenligt att begränsa vilka *uppgiftstyper* som får inhämtas talar det för att tillståndet bör förenas med villkor som anger vilka *uppgifter* som får inhämtas eller (inte) granskas och som därigenom begränsar åtgärden. Se närmare härom nedan.

Utökade möjligheter att utreda vem som skäligen kan misstänkas

Det finns i dag inte någon möjlighet att använda hemlig dataavläsning som gäller kameraövervakningsuppgifter eller uppgifter hänförliga till den av oss föreslagna nya punkten 6 i syfte att utreda vem som skäligen kan misstänkas för visst brott eller delaktighet i viss brottslighet. Det finns dock situationer, t.ex. i vissa utredningar om allvarliga brott över internet, där det finns ett påtagligt behov av en sådan möjlighet.

Vid exempelvis narkotikahandel under alias på Darknet, grova dataintrång, cyberbrott genom användning av skadlig programvara som t.ex. virus, trojaner eller spionprogram, eller internetrelaterade sexuella övergrepp mot barn används vanligen en komplex digital infrastruktur. Anonymisering och kryptering gör att det är svårt och många gånger omöjligt att genom traditionella tvångsmedel utreda vem eller vilka som ligger bakom den i övrigt fullt synliga brottsligheten. Information härom skulle dock kunna bli åtkomlig genom användning av hemlig dataavläsning som gäller s.k. punkt 6-uppgifter. Åtgärden skulle kunna användas för att hämta in t.ex. sparade bilder, källkoder, loggfiler, noder och andra uppgifter som inte har kommunicerats. Vid en analys av sådana uppgifter skulle sedan digitala spår från olika håll kunna kombineras och utredas parallellt för att upptäcka eventuella samband, vilket många gånger är en förutsättning för att kunna identifiera personerna bakom brottsligheten. Ett exempel som belyser behovet av att använda kameraövervakningsuppgifter för att utreda vem som skäligen kan misstänkas är följande. Många gånger känner de brottsbekämpande myndigheterna till att ett visst informationssystem används som brottsverktyg för att begå allvarlig brottslighet, men saknar samtidigt verktyg för att identifiera den misstänkte. En vanlig invändning vid allvarlig brottslighet som exempelvis internetrelaterade sexuella övergrepp mot barn och narkotikabrottslighet

över internet är att den misstänkte vid tiden för brottet hade lånat ut sin dator eller telefon till någon annan. Genom att aktivera kamerafunktionen på den informationsutrustning som används som brottsverktyg skulle användaren kunna identifieras. En möjlighet att använda hemlig dataavläsning i dessa situationer skulle således innebära en avsevärd nytta för brottsbekämpningen.

En sådan möjlighet innebär samtidigt ökade risker för enskildas personliga integritet och en ökad risk för att ovidkommande drabbas av åtgärden. Vid en intresseavvägning bedömer vi dock att behovet av en möjlighet att använda de olika åtgärderna är så påtagligt att det överväger nackdelarna ur ett integritetsperspektiv. Vi föreslår därför att det ska införas en möjlighet att använda kameraövervakningsuppgifter och den nya punkten 6-uppgifter i syfte att utreda vem som skäligen kan misstänkas för visst brott eller delaktighet i viss brottslighet. Med beaktande av de begränsade tillämpningsområden och de höga kvalifikationskrav som föreslås framstår det integritetsintrång som förslagen innebär som försvarligt i förhållande till behovet och nyttan av att utöka tillämpningsområdet på föreslaget sätt.

Tydligare bestämmelser om verkställighet

Den hittillsvarande tillämpningen visar att kravet på att i tillståndet ange vilken tid tillståndet avser har orsakat vissa tolknings- och tillämpningssvårigheter. Rent generellt får det anses missvisande med tillstånd som avser historiska tidsperioder, eftersom det vid hemlig dataavläsning endast är möjligt att ta del av den information som finns lagrad vid tidpunkten för verkställighet. Vidare har det visat sig svårt och många gånger omöjligt att redan före inhämtningen tidsbestämma lagrad information. Risken med att begränsa ett tillstånd till att endast avse uppgifter som har lagrats under viss tid är att tillståndet får mindre räckvidd än avsett. Lagrade uppgifter kan vara skapade och ändrade vid flera olika tidpunkter samt ingå i komplexa mappstrukturer. Lagrad information går sällan att tidsbestämma före själva inhämtningen. Den hittillsvarande tillämpningen visar också på ett behov av att klargöra under vilken tid som inhämtning av lagrade uppgifter får ske.

Vi föreslår därför att kravet på att ange vilken tid tillståndet avser ska tas bort. I stället föreslår vi att det i ett tillstånd till hemlig data-

avläsning ska anges under vilken tid som verkställighet får ske. Tiden för verkställighet får inte bestämmas längre än nödvändigt och får inte överstiga en månad från dagen för beslutet. Förslaget innebär ett förtydligande av att ett tillstånd till hemlig dataavläsning ska verkställas inom en viss tid som inte får överstiga en månad. Vidare föreslår vi att alla uppgifter som omfattas av tillståndet och som är åtkomliga under verkställighetstiden får hämtas in, om inte annat framgår av tillståndets villkor.

Förslaget innebär att inhämtningen inte längre behöver begränsas till information som lagrats under en viss tid, om det inte är möjligt eller lämpligt med en sådan begränsning. Härigenom undanröjs behovet att på förhand tidsbestämma lagrad information och verkställighetsproblematiken kring historiska tidsperioder för uppgifter som är lagrade i informationssystemet. Ändringen knyter an till vårt förslag om att tidsmässiga villkor som avser själva granskningen av inhämtade uppgifter ska bli mer framträdande.

Tydligare bestämmelser om villkor

Även kravet på att i tillståndet ange villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan har orsakat tolknings- och tillämpningssvårigheter. Det råder en osäkerhet i rättstillämpningen om hur villkor som tillgodoser intresset av att enskilda personliga integritet inte kränks i onödan bör utformas. Villkorskravet har därför inte alltid efterlevts i praktiken.

Vi bedömer att det även fortsatt ska vara obligatoriskt att förena ett tillstånd till hemlig dataavläsning med villkor. Detta utesluter inte att det kan finnas situationer där ett villkor för tillståndet framstår som överflödigt. Vi föreslår därför att det införs en ventil för obehövliga villkor. Vidare bör det tydliggöras vad villkoren ska avse. Vi föreslår därför att det i ett tillstånd till hemlig dataavläsning ska anges vilka uppgifter som inte får granskas och övriga villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan, om sådana villkor inte framstår som obehövliga. Förslaget återknyter dels till förslaget om en tydligare bestämmelse om de olika uppgiftstyperna, dels till förslaget om tydligare bestämmelser om verkställighet. Vårt förslag om villkor balanserar det faktum att det vid tillståndsprövningen ofta inte är ändamålsenligt att begränsa antalet upp-

giftstyper eller att tidsmässigt avgränsa vilka uppgifter som får *inhämtas*. Eftersom sådana avgränsningar dock är möjliga att göra i en inledande bearbetning av de inhämtade uppgifterna, ska det som huvudregel anges villkor för vilka inhämtade uppgifter som inte får *granskas*. Övriga villkor för tillståndet tar sikte på andra omständigheter än granskningen. I de fall som det är möjligt och lämpligt kan övriga villkor avse själva inhämtningen av uppgifter. Villkoren måste anpassas efter omständigheterna i det enskilda fallet. I våra överväganden ger vi exempel på villkor och beskriver hur både inhämtningen och granskningen av inhämtade uppgifter kan avgränsas på ett ändamålsenligt sätt, samtidigt som intresset av att enskildas personliga integritet inte kränks i onödan tillgodoses.

För att syftet med villkorsgivningen ska uppfyllas krävs att villkoren generellt sett håller en högre kvalitet än i dag. Vi föreslår därför att åklagaren, eller i förekommande fall Säkerhetspolisen, i samband med en ansökan om hemlig dataavläsning ska vara skyldig att föreslå de villkor som tillståndet ska förenas med, om sådana villkor inte framstår som obehövliga.

Tydligare bestämmelser om överskottsinformation

Vi föreslår att användningsområdet för överskottsinformation från hemlig dataavläsning förtydligas, i enlighet med vad som redan gäller för hemliga tvångsmedel enligt rättegångsbalken och lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen). Det innebär att åklagare, utan några särskilt stadgade begränsningar, ska få besluta att uppgifter som har kommit fram vid användning av hemlig dataavläsning under förundersökning och enligt reglerna i preventivlagen får användas för ett annat ändamål än det som har legat till grund för åtgärden. För det fall att bestämmelsen om överskottsinformation i inhämtningslagen ändras i enlighet med förslaget i slutbetänkandet *Utökade möjligheter att använda preventiva tvångsmedel 2*, SOU 2023:60, föreslår vi att det, som en följd av förslaget, ska införas en motsvarande reglering om användning av överskottsinformation i inhämtningslagsfallen.

Tydligare bestämmelser om bevarande och förstöring

Vi föreslår att upptagningar och uppteckningar från hemlig dataavläsning under en förundersökning ska bevaras i enlighet med vad som redan gäller för hemliga tvångsmedel enligt rättegångsbalken. Det innebär att allt material som huvudregel ska bevaras. Om den misstänkte medger det ska upptagningar och uppteckningar få förstöras innan förundersökningen har lagts ned eller avslutats eller, om åtal har beslutats, målet har avgjorts slutligt. För det fall att bestämmelsen om bevarande och förstöring i inhämtningslagen ändras i enlighet med förslaget i slutbetänkandet *Utökade möjligheter att använda preventiva tvångsmedel 2*, SOU 2023:60, föreslår vi att det, som en följd av förslaget, ska införas en motsvarande reglering om bevarande och förstöring i inhämtningslagsfallen.

Tydligare bestämmelser om otillåtna uppgifter

Vi föreslår att bestämmelsen om otillåten tilläggsinformation både förtydligas och utvecklas. Förslaget innebär att om otillåtna uppgifter påträffas så ska dessa uppgifter förstöras så snart det är möjligt. Undantaget från huvudregeln om bevarande gäller om upptagningar eller uppteckningar av följande uppgifter påträffas:

1. Uppgiftstyper som inte får inhämtas enligt tillståndet.
2. Uppgifter som inte får inhämtas enligt villkor för tillståndet.
3. Uppgifter som inte får granskas enligt villkor för tillståndet.
4. Uppgifter som omfattas av beslags- eller avlyssningsförbudet.

Ett lagstadgat dokumentationskrav införs

I dag finns ingen lagstadgad skyldighet att dokumentera användningen av hemlig dataavläsning. Vi föreslår att det i lagen om hemlig dataavläsning ska införas ett dokumentationskrav för beslut och åtgärder som rör hemlig dataavläsning. Förslaget motsvarar vad som redan gäller för hemliga tvångsmedel enligt rättegångsbalken och preventivlagen. Ett förslag om att det ska införas ett lagstadgat dokumentationskrav även i inhämtningslagen är för närvarande under bered-

ning, se slutbetänkandet *Utökade möjligheter att använda preventiva tvångsmedel 2*, SOU 2023:60.

Lagstiftningens struktur och placering

Vi föreslår att bestämmelserna om hemlig dataavläsning fortsatt bör regleras i en särskild lag – lagen om hemlig dataavläsning. Vi framhåller samtidigt att det vore önskvärt att bestämmelserna om tvångsmedelsanvändning blev föremål för en fullständig översyn i syfte att förenkla och harmonisera reglerna. I avvaktan på att det görs en samlad översyn av tvångsmedelsbestämmelserna anser vi dock att kraven på systematik, tydlighet och förutsebarhet bäst tillgodoses om hemlig dataavläsning fortsatt regleras i en egen lag.

Ikraftträdande

Lagändringarna föreslås träda i kraft den 1 mars 2025.

Konsekvenser

Ett genomförande av förslagen förbättrar de brottsbekämpande myndigheternas förutsättningar att utreda, förebygga, förhindra och upptäcka allvarlig brottslighet. På sikt kan våra förslag också ha brottsförebyggande effekter och leda till att färre brott begås. Våra förslag får indirekt genomslag även för det internationella straffrättsliga samarbetet. Bättre förutsättningar för internationellt rättsligt samarbete får särskilt stor betydelse vid gränsöverskridande brottslighet som t.ex. internetrelaterade sexuella övergrepp mot barn samt narkotika- eller cyberbrottslighet.

För enskilda innebär våra förslag en ökad risk för den personliga integriteten. De personer som berörs bedöms huvudsakligen vara samma personer som riskerar att bli föremål för andra hemliga tvångsmedel. Våra förslag innebär i flera avseenden också ett förstärkt skydd för enskildas personliga integritet och en ökad rättstrygghet för enskilda. Detta framför allt med hänsyn till statens positiva förpliktelser som innebär en skyldighet att skydda enskilda mot ingrepp i privatlivet från andra. Vissa av förslagen innebär också ett förbättrat

skydd mot otillåtna och obefogade integritetsintrång. Våra förslag i dessa delar bedöms därmed innebära en förstärkt rättssäkerhet för den enskilde.

Att bedöma de ekonomiska konsekvenserna av våra förslag är förenat med flera svårigheter, inte minst eftersom frågan om användning av hemlig dataavläsning i varje enskilt ärende innefattar en prioritering utifrån nyttan respektive resursåtgången av en sådan åtgärd. Hemlig dataavläsning är jämfört med andra tvångsåtgärder ett mycket resurskrävande hemligt tvångsmedel, eftersom åtgärden kräver både ett omfattande förberedelsearbete och en avancerad teknisk förmåga, särskilt anpassad efter det enskilda fallet. Säkerhetspolisen och Tullverket har uppskattat att myndigheternas resursbehov kommer att öka om våra förslag genomförs. De ökade kostnaderna avser huvudsakligen teknikkostnader och personalkostnader för att bibehålla och utveckla egen nödvändig teknisk förmåga på området. Säkerhets- och integritetsskyddsnämnden (SIN) har bedömt att nämndens tillsynsuppdrag, som en följd av våra förslag, kommer att öka i en sådan omfattning att nämnden bör tillföras ytterligare medel för att kunna utföra en effektiv och rättssäker tillsyn. De resursbehov som uppkommer för dessa myndigheter föreslås huvudsakligen finansieras genom att medel tillförs från andra utgiftsområden. Även Polismyndigheten och Sveriges Domstolar, inklusive anslaget för rättsliga biträden, kommer att få vissa ökade kostnader med anledning av våra förslag. Dessa kostnader bedöms dock rymmas inom befintliga anslag. Detsamma gäller de ökade kostnader som kan komma att uppstå för Skatteverket, Finansinspektionen och Kriminalvården. Beträffande övriga berörda aktörer – Åklagarmyndigheten, Ekobrottsmyndigheten och företag som medverkar vid verkställighet – bedöms genomförandet av våra förslag inte medföra några ökade kostnader.

De kostnader som den allvarliga brottsligheten medför är avsevärda. Mer effektiva verktyg för att utreda, förebygga, förhindra och upptäcka allvarlig brottslighet bedöms därför få stora positiva samhällsekonomiska konsekvenser. Våra förslag kan medföra betydande samhällsekonomiska besparingar kopplade till exempelvis rättsväsendet, sjukvården, sociala myndigheter, Skatteverket och Försäkringskassan. Besparingseffekterna är svåra att beräkna, men knappast obetydliga ens för ett enskilt fall.

Summary

This is a translation of the summary into English. Since the translation is intended to be as close to the Swedish original as possible, certain terms and expressions used may not be the same as if similar matters had been described in a different context or forum.

Remit

Our remit has been to evaluate the Secret Data Reading Act (*lagen [2020:62] om hemlig dataavläsning*), hereinafter abbreviated to SDRA, and consider whether the Act should be made permanent and, if so, whether it should be amended in any respect. The SDRA, which entered into force on 1 April 2020, introduced a new covert coercive measure that law enforcement authorities can use in suspected cases of national security crimes and other serious criminal offences. The Act is in force temporarily until the end of March 2025. The remit has included analysing the benefit of and need for secret data reading, taking into consideration whether the legislation should be made permanent and proposing the measures needed to make it permanent, analysing whether the legislation is appropriate and proportionate or whether changes to the regulatory framework are needed, and submitting proposals for the statutory amendments and other measures deemed necessary. The remit has entailed ensuring the maintenance of a well-functioning systematic approach to both covert and open coercive measures in the regulatory framework. The remit also has involved carefully weighing the need for effective law enforcement against the individual's right to protection of their fundamental rights and freedoms, such as personal privacy, and ensuring that the proposals meet the strict requirements of legal certainty.

What is secret data reading?

Secret data reading is a tool that allows law enforcement authorities to access information that is otherwise difficult to access, for example due to encryption. Secret data reading is primarily used when other coercive measures or methods are not viable alternatives. In practice, secret data reading involves the use of technical tools or methods to allow law enforcement authorities to secretly collect data accessible on a computer, on a mobile phone, in an internet user account or in any other readable computer system (electronic device or service). A basic prerequisite for the use of secret data reading is that it must be a matter of serious crime, such as espionage, terrorist offences, gross breach of data security, gross narcotics offences, gross weapons offences, rape or murder. Under certain specific conditions, secret data reading may be used during a preliminary investigation, in intelligence activities and in special controls in respect of certain aliens, as well as in international cooperation in criminal matters.

Permanent legislation – balancing need, efficiency and privacy

Sweden has been affected by an increase in serious crime and the ongoing serious criminal activity has become an increased threat to society. One example is the marked increase in gun related murders in recent years. Violent crime is, in turn, closely linked to the increase in narcotics-related crime. A significant increase in serious crime has also been noted by the intelligence community. The deterioration in the international security situation has also had a direct effect on Sweden. The ways in which criminals act and communicate are changing. In particular, serious and organised crime often makes use of encrypted services and electronic devices to communicate, with the direct aim of preventing access by government agencies. Globalisation, technological developments and changing communication habits have meant that law enforcement authorities are no longer able to access information that was previously accessible by means of traditional coercive measures. Since secret data reading was introduced, effective access to electronic evidence has grown in importance. This is also the case in international judicial cooperation, as the serious

crimes that may give rise to secret data reading are often of a cross-border nature. From an international perspective, it can be seen that virtually all EU Member States, plus the United States, Canada and Australia, have statutory opportunities to use secret data reading or an equivalent measure as a law enforcement tool. It is important for the legislation on coercive measures to keep pace with technological and social developments and developments in international law to make it possible to continue to fight serious crime.

The law enforcement authorities have now been able to use secret data reading for more than three and a half years. Our analyses show that secret data reading has been used more extensively than anticipated when the new coercive measure was introduced. The law enforcement authorities also have a very positive experience of the results of secret data reading. The descriptions and practical examples provided show that, in many cases, secret data reading has been a crucial tool in law enforcement activities. Secret data reading has led to both specific information about crimes that have already been committed and information that could be used to prevent serious crime. Secret data reading has also been used in several cases to access information about how different types of serious crime are organised and to establish which individuals are at higher levels of the hierarchy. As the information was not accessible by means of other coercive measures, secret data reading has meant a breakthrough in the fight against serious and organised crime in these cases. It is clear that the use of secret data reading is an effective tool for gaining access to information and that the measure has been extremely beneficial to law enforcement. Our overall assessment is that there is still a clear need for secret data reading to make it possible to fight serious crime. There is no evidence that this need is temporary, nor can this need be met by existing provisions on coercive measures. At the same time, our assessment is that secret data reading poses risks to personal privacy.

We have weighed the need for effective law enforcement to prevent, deter, detect and investigate serious criminal offences, the effectiveness of the measure and the benefit that the possibility of using secret data reading has brought and can be expected to bring, against the privacy risks that the measure entails. In weighing up these factors, we have also taken into account the public obligation to maintain legal certainty for individuals and to protect citizens from infringement

of their privacy by others. Overall, we have found that it is proportionate to make secret data reading a permanent coercive measure. The measure is deemed essential in the interest of fighting serious crime and to maintain the legal certainty of individuals and their right to protection against violations by other individuals. Our proposal to make the legislation permanent is subject to the condition that the scope of application is clearly and appropriately defined and that the legislation contains specific qualification requirements and procedural safeguards to balance the increased risks to personal privacy posed by the measure. We therefore also propose some amendments to the current regulatory framework on secret data reading.

Clearer provisions and an extended scope of application

Our proposals for amendments to the SDRA largely involve clarifications of the legislation. They aim to simplify the application and decision-making process and eliminate any uncertainty that may currently exist regarding the scope of authorisation. In all our deliberations, we have endeavoured to maintain a well-functioning systematic approach to both covert and open coercive measures in the regulatory framework. The main impact of our proposals is to clarify the conditions under which secret data reading may be used, how the data collected must be managed and the obligations of the person applying the measure. Our assessment is that our proposals for clearer and more predictable legislation entail that the SDRA will be more in line with the strict requirements for legal certainty and the requirements for the protection of individuals' personal privacy that follow from the Instrument of Government (*regeringsformen [1974:152]*), the European Convention on Human Rights and EU law. Some of our proposals also include some extension of the scope of application of secret data reading and provide the law enforcement authorities with more effective tools to investigate, prevent, deter and detect certain serious criminal offences. When balancing the interests of the need for effective law enforcement and the individual's right to protection of their personal privacy, we have found that the increased risk of infringement of personal privacy that our proposals entail is justifiable.

As the legislation on secret data reading and other covert coercive measures is subject to other ongoing revisions, it has also been necessary to make an overall assessment of the proportionality of the entire extended and intended scope of application of secret data reading. Several legislative amendments affecting the scope of application of secret data reading entered into force as recently as 1 October 2023 and further legislative proposals that may affect the scope of application are currently in preparation. In an overall assessment, we have found that the entire extended and intended scope of application of secret data reading is sufficiently appropriately and clearly defined to protect individuals against arbitrary infringement of their rights and freedoms. Moreover, taking into account the overall violation of privacy that the implementation of our proposals entails, combined with current legislation and the additional legislative proposals that are now being prepared and may enter into force shortly, it is our assessment that the regulatory framework for secret data reading provides a reasonable balance between the need for effective law enforcement and the individual's right to protection of their personal privacy.

Clarification of the definition of secret data reading

We propose that the definition and scope of the term secret data reading is clarified. The secret data reading procedure comprises *collection* (data reading and data transfer) and *processing* (refining, sorting, filtering and examining) of data. Given the nature of secret data reading, the term currently used to define secret data reading, i.e. that data is intercepted or recorded, may be misleading in some respects and cause difficulties in application. The term is therefore replaced with 'collection'. The preamble of the Act thus clarifies that secret data reading means that data intended for automated processing and accessible in a readable computer system is *collected* secretly using technical tools or methods. Other provisions of the Act clarify how the data collected may then be *processed*. The amendment therefore also entails some clarifications in other provisions of the Act.

A clearer provision on the different types of data

The SDRA specifies seven different types of data. See Section 2, first paragraph, points 1–7. The data types in points 1–5 (communications content, communications metadata, location data, camera surveillance data and audio surveillance data) have their equivalents in other, permanent, covert coercive measures. The data types in points 6 and 7 are unique to secret data reading. Point 6 refers to data stored in the computer system but not referred to in points 1–5, and point 7 refers to data showing how the computer system is used but not referred to in points 1–6. In practice, this division means that stored data not falling under points 1–3 is point 6 data and that real-time data not falling under points 1–5 and showing how a computer system is used is point 7 data.

The division into different types of data is important at the time the authorisation is issued, as authorisation for secret data reading must always specify the type of data that may be collected. This requirement to differentiate between types of data has caused some problems in the application of the law. This is because it is rarely possible, before collection, to determine how the categorisation of different types of data in the legislation should be applied to the information that may be found. The problem of distinguishing between the types of data in points 6 and 7 has posed a particular challenge. We therefore propose merging points 6 and 7 to form a new point 6 that does not distinguish between stored and real-time data. We also consider that a distinction should continue to be made between each of the types of data in 1–5 and data that falls under the new point 6. Although the division poses some practical challenges, the requirement to differentiate between types of data is considered an important safeguard to ensure that individuals' personal privacy is not violated unnecessarily.

Application of the Act to date shows that there is usually a clear need for covert surveillance of several types of data in each case. A typical authorisation for secret data reading needs to include the types of data in 1–3 and the new point 6 for the measure to achieve its aim. Otherwise, there is a risk of the scope of the authorisation being narrower than intended and thus of law enforcement authorities failing to obtain relevant information. Another risk is that the data collected may be considered to be unauthorised side information if the

data sought turns out to fall under a different point than anticipated. From the point of view of legal certainty, it is important for the assessment of the authorisation to focus on the legal aspects and not on how the need for information can be technically categorised. We therefore propose a clarifying general rule under which authorisation for secret data reading will include the types of data in 1–3 and the new point 6, unless otherwise specifically decided or stated in other provisions. The introduction of such a general rule is balanced by the fact that we also propose clearer provisions on conditions. If it is not appropriate to restrict the *types of data* that may be collected in the assessment prior to the authorisation, this suggests that the authorisation should be subject to conditions specifying which *data* may be collected or (not) examined, thereby limiting the measure. See further details below.

Extended possibilities to investigate who may be suspected on reasonable grounds

There is currently no legal support for the use of secret data reading in relation to camera surveillance data or data related to the new point 6 proposed by us for the purpose of investigating who may be suspected on reasonable grounds of a certain crime or participation in a certain crime. However, there are situations, for example in some investigations into serious online offences, in which such an option is clearly needed.

For example, drug trafficking under aliases on the dark web, gross breach of data security, cybercrime through the use of malicious software such as viruses, trojans or spyware, or internet-related child sexual abuse typically use a complex digital infrastructure. Anonymisation and encryption make it difficult, and often impossible, to use traditional coercive measures to investigate who is behind otherwise highly visible crime. This information could, however, be accessed through the use of secret data reading of point 6 data. The measure could be used to collect, for example, saved images, source codes, log files, nodes and other data that has not been communicated. When analysing such data, digital clues from different sources could be combined and investigated in parallel to detect possible links, which is often necessary to be able to identify the individuals behind the crime. The following is an example that highlights the need to use camera sur-

veillance data to investigate who may be suspected on reasonable grounds. In many cases, law enforcement authorities know that a particular computer system is being used as a tool to commit serious criminal offences, but lack the tools to identify the suspect. A common objection in serious crimes such as online child sexual abuse and online narcotics offences is that the suspect had lent their computer or phone to someone else at the time of the offence. By activating the camera function on the technical device used as a tool to commit crime, the user could be identified. An option to use secret data reading in these situations would thus be considerably beneficial to law enforcement.

At the same time, such an option entails higher risks to the personal privacy of individuals and a higher risk of the measure affecting innocent third parties. However, after having weighed the interests against each other, our assessment is that the need for the option to use the various measures is so substantial that it outweighs the disadvantages from a privacy perspective. We therefore propose the introduction of an option to use camera surveillance data and the new point 6-data for the purpose of investigating who may be suspected on reasonable grounds of a certain crime or participation in a certain crime. Considering the limited scope of application and the high qualification requirements proposed, the invasion of privacy that the proposals entail appears justified in relation to the need to extend the scope of application as proposed and the benefit of doing so.

Clearer provisions on enforcement

The application to date shows that the requirement to specify in the authorisation the period to which the authorisation relates has caused some difficulties in interpretation and application. Generally speaking, authorisations relating to periods of time in the past may be considered misleading since, in the case of secret data reading, it is only possible to access the information stored at the time of collection. Furthermore, it has proved difficult and often impossible to date stored information prior to it being collected. The risk of limiting an authorisation to only data that has been created during a certain period of time is that the scope of the authorisation is narrower than intended. Stored data may be created and modified at different

points in time and be part of complex directory structures. It is rarely possible to date stored information before it is collected. The application to date also shows a need to clarify the period during which stored data may be collected.

We therefore propose that the requirement to specify the period to which the authorisation relates be removed. Instead, we propose that an authorisation for secret data reading should specify the period of time during which enforcement may take place. The enforcement period may not be longer than necessary and may not exceed one month from the date of the decision. The proposal entails clarification that an authorisation for secret data reading must be enforced within a certain period of time, which may not exceed one month. Furthermore, we propose that all data covered by the authorisation and accessible during the enforcement period may be collected, unless otherwise stated in the conditions of the authorisation.

The proposal means that the data collected no longer needs to be limited to information created during a certain time period, unless such a limitation is possible or appropriate. This eliminates the need to date stored information in advance and the enforcement problems relating to periods of time in the past for data stored in the computer system. The amendment ties in with our proposal to make time-related conditions relating to the actual examination of data collected more central.

Clearer provisions on conditions

The requirement to specify conditions in the authorisation to ensure that the personal privacy of individuals is not violated unnecessarily has also given rise to difficulties in interpretation and application. There is uncertainty in the application of the law regarding how conditions to ensure that individuals' personal privacy is not unnecessarily violated should be worded. The conditions requirement has therefore not always been complied with in practice.

Our assessment is that it should continue to be mandatory to attach conditions to an authorisation for secret data reading. This does not exclude the possibility that there may be situations in which a condition for the authorisation appears to be superfluous. We therefore propose to introduce a mechanism to avoid unnecessary condi-

tions. Furthermore, it should be made clear what the conditions should refer to. We therefore propose that an authorisation for secret data reading should specify the data that may not be examined and other conditions to ensure that the personal privacy of individuals is not violated, unless such conditions appear to be unnecessary. The proposal relates to the proposal for a clearer provision on the different types of data and to the proposal for clearer provisions on enforcement. Our proposal on conditions balances the fact that it is often inappropriate to limit the number of types of data or to limit the data that may be *collected* to a certain period of time when making assessments prior to authorisations. However, since such limitations are possible in the initial processing of the data collected, conditions should, as a general rule, be specified for the data collected which may not be *examined*. Other conditions refer to circumstances other than the examination. Where possible and appropriate, other conditions may relate to the process of collecting data itself. The conditions must be adapted to the circumstances in each case. In our considerations, we provide examples of conditions and describe how both collecting data and examining data collected may be subject to appropriate limits, while ensuring that the personal privacy of individuals is not violated.

To fulfil the purpose of setting conditions, the conditions must generally be of a higher quality than today. We therefore propose that, in connection with an application for secret data reading, the prosecutor or, where applicable, the Security Service should be obliged to propose the conditions for the authorisation, unless such conditions appear to be unnecessary.

Clearer provisions on surplus information

We propose that the scope of use of surplus information from secret data reading be clarified in accordance with that which already applies to covert coercive measures under the Code of Judicial Procedure (*rättegångsbalken [1942:740]*) and the Act (2007:979) on measures to prevent certain particularly serious crimes (*preventivlagen*), hereinafter abbreviated to APSC. This means that, without any specific restrictions, prosecutors may decide that data collected through the use of secret data reading during a preliminary investigation and under the rules of the ASPC may be used for a purpose other than

that on which the measure was based. In the event that the provision on surplus information in the Act (2012:278) on Collecting Data relating to Electronic Communications as Part of the Intelligence Activities of Law Enforcement Authorities (*inhämtningslagen*), hereinafter abbreviated to ACEC, is amended in accordance with the proposal in the final report *Extended opportunities to use preventive coercive measures 2*, SOU 2023:60, we propose that, as a result of the proposal, a corresponding regulation on the use of surplus information be introduced in cases of secret data reading under the rules of the ACEC.

Clearer provisions on preservation and destruction

We propose that recordings and notes from secret data reading during a preliminary investigation be preserved in accordance with that which already applies to covert coercive measures under the Code of Judicial Procedure. This means that, in principle, all material should be preserved. With the suspect's consent, recordings and notes may be destroyed before the preliminary investigation has been closed or terminated or, if a decision to prosecute has been made, a final decision has been made in the case. In the event that the provision on preservation and destruction in the ACEC is amended in accordance with the proposal in the final report *Extended opportunities to use preventive coercive measures 2*, SOU 2023:60, we propose that, as a result of the proposal, a corresponding regulation on preservation and destruction be introduced in cases of secret data reading under the rules of the ACEC.

Clearer provisions on unauthorised data

We propose that the provision on unauthorised side information be both clarified and developed. The proposal means that if unauthorised data is found, it must be destroyed as soon as possible. The exception to the principle of preservation applies if recordings or notes of the following data are found:

1. Types of data that may not be collected under the authorisation.
2. Data that may not be collected under the conditions of the authorisation.
3. Data that may not be examined under the conditions of the authorisation.
4. Data subject to prohibition of seizure or interception.

Introduction of a statutory documentation requirement

There is currently no statutory obligation to document the use of secret data reading. We propose that a documentation requirement for decisions and measures relating to secret data reading be introduced in the SDRA. The proposal corresponds to that which already applies to covert coercive measures under the Code of Judicial Procedure and the APSC. A proposal to also introduce a statutory documentation requirement in the ACEC is currently under preparation. See the final report *Extended opportunities to use preventive coercive measures 2*, SOU 2023:60.

Structure and location of the legislation

We propose that the provisions on secret data reading should continue to be regulated in a separate Act: the SDRA. At the same time, we emphasise that it would be desirable for the provisions on coercive measures to be fully reviewed with a view to simplifying and harmonising the rules. However, pending an overall review of the coercive measures provisions, we consider that the requirements for systematisation, clarity and predictability are best met if secret data reading continues to be regulated in a separate Act.

Entry into force

It is proposed that these legislative amendments enter into force on 1 March 2025.

Impacts

Implementation of the proposals will improve the ability of law enforcement authorities to investigate, prevent, deter and detect serious criminal offences. In the long term, our proposals may also have a crime prevention impact and lead to fewer offences being committed. Our proposals also have an indirect impact on international judicial cooperation in criminal matters. Improving the conditions for international judicial cooperation is particularly important for cross-border crime such as internet-related child sexual abuse, narcotics crime or cybercrime.

For individuals, our proposals represent an increased risk to their personal privacy. The persons concerned are considered to be mainly the same persons who risk being subject to other covert coercive measures. In several respects, our proposals also strengthen the protection of individuals' personal privacy and increase legal certainty for individuals. This is particularly the case in view of the 'positive obligations' of the State to protect individuals against infringement of their private lives by others. Some of the proposals also improve the protection against unauthorised and unjustified invasion of privacy. Our proposals in these areas are thus deemed to entail greater legal certainty for the individual.

There are several difficulties linked to assessing the financial consequences of our proposals, not least because the question of using secret data reading involves prioritisation based on the benefits of and resources required for such a measure in each individual case. Compared to other coercive measures, secret data reading is a very resource-intensive covert coercive measure, as it requires both extensive preparatory work and advanced technical capacity, specifically adapted to the individual case. The Swedish Security Service and Swedish Customs have estimated that the government agencies' resource requirements will increase if our proposals are implemented. The increased costs relate mainly to technical and personnel costs to maintain and develop the necessary in-house technical capacity in this area. The Swedish Commission on Security and Integrity Protection (SIN) has assessed that, as a result of our proposals, the Commission's supervisory tasks will increase to such an extent that the Commission should be provided with additional resources to be able to carry out effective, legally certain supervision. It is proposed that the resource

requirements that arise for these government agencies be financed mainly by allocating funds from other areas of expenditure. The Swedish Police Authority and the Courts of Sweden, including the appropriation for legal counsels, will also incur some increased costs as a result of our proposals. However, these costs are expected to be accommodated within existing appropriations. The same applies to the increased costs that may arise for the Swedish Tax Agency, the Swedish Financial Supervisory Authority (FI) and the Swedish Prison and Probation Service. With regard to other affected actors (the Swedish Prosecution Authority, the Swedish Economic Crime Authority and companies involved in enforcement), the implementation of our proposals is not deemed to entail any increased costs.

The costs of serious criminal offences are considerable. More effective tools for investigating, preventing, deterring and detecting serious criminal offences are therefore expected to have major positive economic consequences. Our proposals can lead to significant economic savings in areas such as the judicial system, healthcare, social services, taxation and social insurance. The savings are difficult to calculate, but hardly insignificant even for an individual case.

1 Författningsförslag

1.1 Förslag till lag om ändring i lagen (2020:62) om hemlig dataavläsning

Härigenom föreskrivs i fråga om lagen (2020:62) om hemlig dataavläsning som gäller till utgången av mars 2025

dels att lagen ska fortsätta gälla utan begränsning till viss tid,

dels att 1, 2, 4 a, 4 b, 8, 9, 14, 17, 18, 23, 27–29 och 31 §§ ska ha följande lydelse,

dels att rubrikerna närmast före 2 och 27 §§ ska ha följande lydelse,

dels att det ska införas en ny paragraf, 34 §, och närmast före 34 § en ny rubrik av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	1 §
Hemlig dataavläsning innebär att uppgifter, som är avsedda för automatiserad behandling, i hemlighet och med ett tekniskt hjälpmedel *läses av eller tas upp* i ett avläsningsbart informationssystem.	Hemlig dataavläsning innebär att uppgifter, som är avsedda för automatiserad behandling *och som är åtkomliga* i ett avläsningsbart informationssystem, *inhämtas* i hemlighet och med ett tekniskt hjälpmedel.
I lagen avses med	
avläsningsbart informationssystem: en elektronisk kommunikationsutrustning eller ett användarkonto till, eller en på motsvarande sätt avgränsad del av, en kommunikationstjänst, lagringstjänst eller liknande tjänst,	
kommunikationsavlyssningsuppgifter: uppgifter om innehåll	*kommunikationsavlyssningsuppgifter*: uppgifter om innehåll i

i meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller *någon* annan adress,

kommunikationsövervakningsuppgifter: uppgifter om meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller *någon* annan adress,

meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller *en* annan adress,

kommunikationsövervakningsuppgifter: uppgifter om meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller *en* annan adress,

platsuppgifter: uppgifter om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits,

kameraövervakningsuppgifter: uppgifter som framkommer genom optisk personövervakning,

rumsavlyssningsuppgifter: uppgifter som avser tal i enrum, samtal mellan andra eller förhandlingar vid sammanträden eller andra sammankomster som allmänheten inte har tillträde till.

Typer av uppgifter* som får *läsas av eller tas upp	***Uppgiftstyper* som får *hämtas in***
2 §	
Tillstånd till hemlig dataavläsning får *beviljas för att läsa av eller ta upp*	Tillstånd till hemlig dataavläsning får *avse*
1. kommunikationsavlyssningsuppgifter,	
2. kommunikationsövervakningsuppgifter,	
3. platsuppgifter,	
4. kameraövervakningsuppgifter,	
5. rumsavlyssningsuppgifter,	5. rumsavlyssningsuppgifter *eller*
6. uppgifter som *finns lagrade* i ett avläsningsbart informationssystem men som inte avses i 1–5, *eller*	6. uppgifter som *är åtkomliga* i ett avläsningsbart informationssystem men som inte avses i 1–5.

7. uppgifter som visar hur ett avläsningsbart informationssystem används men som inte avses i 1–6.

Vid hemlig dataavläsning som gäller kommunikationsavlyssnings- eller kommunikationsövervakningsuppgifter får meddelanden som överförs eller har överförts i ett elektroniskt kommunikationsnät även hindras från att nå fram.

Ett tillstånd enligt första stycket omfattar uppgiftstyperna i första stycket 1–3 och 6, om inget annat särskilt beslutas eller framgår av andra bestämmelser.

4 a §[1]

Ett tillstånd enligt 4 § får endast avse ett avläsningsbart informationssystem som används, eller som det finns särskild anledning att anta har använts eller kommer att användas, av den misstänkte.

Ett tillstånd enligt 4 § som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter får även avse ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att den misstänkte *under den tid som tillståndet avser* har kontaktat eller kommer att kontakta.

Ett tillstånd enligt 4 § som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter får även avse ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att den misstänkte har kontaktat eller kommer att kontakta.

Ett tillstånd enligt 4 § som gäller kameraövervakningsuppgifter får endast avse en plats där den misstänkte kan antas komma att uppehålla sig. En sådan plats får dock inte vara någons stadigvarande bostad.

Trots tredje stycket får ett tillstånd enligt 4 § som gäller kameraövervakningsuppgifter avse den skäligen misstänkte i stället för en viss plats, om det finns särskilda skäl för det. Den hemliga dataavläsningen får då endast användas på en plats där den misstänkte kan antas komma att uppehålla sig. En sådan plats får dock inte vara någons stadigvarande bostad.

[1] Senaste lydelse 2023:540.

4 b §[2]

Ett tillstånd till hemlig dataavläsning som gäller *kommunikationsavlyssningsuppgifter* får, om åtgärden är av synnerlig vikt för utredningen, även beviljas för att utreda vem som skäligen kan misstänkas för brottet eller brotten vid en förundersökning om brott som avses i 27 kap. 18 b § andra stycket rättegångsbalken.

Ett tillstånd till hemlig dataavläsning som gäller *uppgiftstyperna i 2 § första stycket 1–4 eller 6* får, om åtgärden är av synnerlig vikt för utredningen, även beviljas för att utreda vem som skäligen kan misstänkas för brottet eller brotten vid en förundersökning om brott som avses i 27 kap. 18 b § andra stycket rättegångsbalken.

Hemlig dataavläsning enligt första stycket får endast avse ett avläsningsbart informationssystem som

1. det finns särskild anledning att anta att gärningsmannen eller någon annan som har medverkat till brottet eller brotten *under den tid som tillståndet avser* har använt eller kommer att använda, eller

1. det finns särskild anledning att anta att gärningsmannen eller någon annan som har medverkat till brottet eller brotten har använt eller kommer att använda, eller,

2. det finns synnerlig anledning att anta att gärningsmannen eller någon annan som har medverkat till brottet eller brotten *under den tid som tillståndet avser* har kontaktat eller kommer att kontakta.

2. *om tillståndet gäller uppgiftstyperna i 2 § första stycket 1–3 eller 6,* det finns synnerlig anledning att anta att gärningsmannen eller någon annan som har medverkat till brottet eller brotten har kontaktat eller kommer att kontakta.

Ett tillstånd enligt första stycket som gäller kameraövervakningsuppgifter får inte verkställas på en plats som är någons stadigvarande bostad.

Trots tredje stycket får tillståndet verkställas på en sådan plats, om det finns synnerliga skäl att anta att den person som åtgärden riktar sig mot uppehåller sig i direkt

[2] Senaste lydelse 2023:540.

anslutning till det avläsningsbara informationssystem som tillståndet avser.

8 §

Hemlig dataavläsning enligt 7 § får avse ett avläsningsbart informationssystem som används, eller som det finns särskild anledning att anta har använts eller kommer att användas, av en person som anges i den bestämmelsen.

Hemlig dataavläsning som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter får även avse ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att en person som anges i 7 § *under den tid som tillståndet avser* har kontaktat eller kommer att kontakta.

Hemlig dataavläsning som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter får även avse ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att en person som anges i 7 § har kontaktat eller kommer att kontakta.

9 §[3]

Ett tillstånd till hemlig dataavläsning får beviljas för att *läsa av eller ta upp* uppgifter i ett avläsningsbart informationssystem som används, eller som det finns särskild anledning att anta har använts eller kommer att användas, av en utlänning som omfattas av

Ett tillstånd till hemlig dataavläsning får beviljas för att *inhämta* uppgifter i ett avläsningsbart informationssystem som används, eller som det finns särskild anledning att anta har använts eller kommer att användas, av en utlänning som omfattas av

1. ett utvisningsbeslut enligt 2 kap. 1 § lagen (2022:700) om särskild kontroll av vissa utlänningar, eller

2. ett avvisnings- eller utvisningsbeslut enligt 8 kap. eller 8 a kap. utlänningslagen (2005:716) om det finns sådana omständigheter i fråga om utlänningen som avses i 2 kap. 1 § lagen om särskild kontroll av vissa utlänningar.

Ett tillstånd till hemlig dataavläsning som gäller kommunikationsavlyssnings-, kommunika-

Ett tillstånd till hemlig dataavläsning som gäller kommunikationsavlyssnings-, kommunika-

[3] Senaste lydelse 2022:711.

tionsövervaknings- eller platsuppgifter får också beviljas för att *läsa av eller ta upp* uppgifter i ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att utlänningen *under den tid som tillståndet avser* har kontaktat eller kommer att kontakta.

tionsövervaknings- eller platsuppgifter får också beviljas för att *hämta in* uppgifter i ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att utlänningen har kontaktat eller kommer att kontakta.

Tillståndet får beviljas endast om Migrationsverket, regeringen eller en domstol har beslutat att 5 kap. 5 och 6 §§ lagen om särskild kontroll av vissa utlänningar samt denna lag ska tillämpas på utlänningen. Det förfarande och de förutsättningar som gäller för ett beslut om att 5 kap. 5 och 6 §§ lagen om särskild kontroll av vissa utlänningar ska tillämpas i fråga om utlänningen gäller också för ett beslut i fråga om hemlig dataavläsning.

Ett tillstånd får beviljas endast om det finns synnerliga skäl och det är av betydelse för att klarlägga om

1. utlänningen tillhör eller verkar för en organisation eller grupp som planlägger eller förbereder brott enligt terroristbrottslagen (2022:666) eller om det finns en risk för att utlänningen kan komma att engagera sig i en sådan organisation eller grupp,
2. det finns risk för att utlänningen själv planlägger eller förbereder brott som avses i 1, eller
3. det finns risk för att utlänningen själv eller tillsammans med andra medverkar i eller på annat sätt främjar ett allvarligt brott som rör Sveriges säkerhet.

Ett tillstånd får inte avse rumsavlyssningsuppgifter.

14 §[4]

Frågor om hemlig dataavläsning prövas av rätten på ansökan av åklagaren. En ansökan om hemlig dataavläsning enligt 9 § ska dock göras av Säkerhetspolisen.

Om ansökan avser den skäligen misstänkte enligt 4 a § fjärde stycket eller 6 § fjärde stycket, ska åklagaren i samband med ansö-

Åklagaren*, eller i förekommande fall Säkerhetspolisen*, ska i samband med ansökan föreslå sådana villkor som avses i 18 §

[4] Senaste lydelse 2023:540.

kan föreslå sådana villkor som avses i 18 § första stycket 4.	första stycket 4, *om sådana villkor inte framstår som obehövliga.*

17 §[5]

Om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen eller för möjligheterna att förebygga, förhindra eller upptäcka den brottsliga verksamheten att inhämta rättens *tillstånd* i en fråga om hemlig dataavläsning, får tillstånd ges av åklagaren i avvaktan på rättens beslut. Ett sådant tillstånd får dock aldrig avse hemlig dataavläsning vid särskild utlänningskontroll enligt 9 §.	Om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen eller för möjligheterna att förebygga, förhindra eller upptäcka den brottsliga verksamheten att inhämta rättens *beslut* i en fråga om hemlig dataavläsning, får tillstånd ges av åklagaren i avvaktan på rättens beslut. Ett sådant tillstånd får dock aldrig avse hemlig dataavläsning vid särskild utlänningskontroll enligt 9 §.

Om åklagaren har gett ett tillstånd enligt första stycket, ska åklagaren snarast möjligt skriftligt anmäla beslutet till rätten. I anmälan ska skälen för åtgärden anges. Rätten ska skyndsamt pröva ärendet. Om rätten finner att det inte finns skäl för åtgärden, ska den upphäva beslutet.

Om åklagarens beslut har verkställts innan rätten gjort en prövning som avses i andra stycket, ska rätten pröva om det funnits skäl för åtgärden. Om rätten finner att det saknats sådana skäl, får de uppgifter som *lästs av eller tagits upp* inte användas i en brottsutredning till nackdel för den som har omfattats av åtgärden, eller för någon annan som uppgifterna avser.	Om åklagarens beslut har verkställts innan rätten gjort en prövning som avses i andra stycket, ska rätten pröva om det funnits skäl för åtgärden. Om rätten finner att det saknats sådana skäl, får de uppgifter som *hämtats in* inte användas i en brottsutredning till nackdel för den som har omfattats av åtgärden, eller för någon annan som uppgifterna avser.

[5] Senaste lydelse 2023:540.

18 §[6]

I ett tillstånd till hemlig dataavläsning ska följande anges:

1. vilken tid tillståndet *avser*,	1. *under* vilken tid *som verkställighet får ske*,
2. vilket avläsningsbart informationssystem tillståndet avser,	
3. vilken *typ av uppgift* enligt 2 § första stycket som får *läsas av eller tas upp*,	3. vilken *uppgiftstyp* enligt 2 § första stycket som får *inhämtas*,
4. villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan, och	4. *vilka uppgifter som inte får granskas och övriga* villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan, *om det inte framstår som obehövligt*, och
5. vem som är skäligen misstänkt för brottet eller brotten, *vid åtgärd som gäller rumsavlyssningsuppgifter*.	5. vem som är skäligen misstänkt för brottet eller brotten, *om sådan uppgift finns*.

Om tillståndet avser en plats enligt 4 a § tredje stycket, 6 § tredje stycket eller 7 § tredje stycket ska även platsen anges i tillståndet. Om tillståndet är förenat med ett tillträdestillstånd enligt 12 §, ska det anges i beslutet.

Om tillståndet avser den skäligen misstänkte enligt 4 a § fjärde stycket eller 6 § fjärde stycket, ska det anges i beslutet.

Tiden för *tillståndet* får inte bestämmas längre än nödvändigt. *När det gäller tid som infaller efter beslutet* får *tiden* inte överstiga en månad från dagen för beslutet.	Tiden för *verkställighet* får inte bestämmas längre än nödvändigt *och* får inte överstiga en månad från dagen för beslutet.

23 §

Den teknik *som används i samband med* hemlig dataavläsning ska anpassas efter *det tillstånd som beviljats*. *Tekniken får inte göra det möjligt att läsa av eller ta upp*	*Vid verkställighet av* hemlig dataavläsning ska teknik *och tillvägagångssätt* anpassas efter *tillståndet*. Om *någon annan uppgiftstyp än vad som anges i tillståndet*

[6] Senaste lydelse 2023:540.

någon annan typ av uppgift än vad som anges i tillståndet. Om *sådana uppgifter har lästs av eller tagits upp* ska upptagningar och uppteckningar av dessa uppgifter omedelbart förstöras och Säkerhets- och integritetsskyddsnämnden underrättas.

har hämtats in ska upptagningar och uppteckningar av dessa uppgifter omedelbart förstöras och Säkerhets- och integritetsskyddsnämnden underrättas. *Upptagningar och uppteckningar av uppgifter som inte får inhämtas eller granskas enligt villkor meddelade med stöd av 18 § första stycket 4 ska förstöras i de delar de innehåller sådana uppgifter så snart det står klart att sådana uppgifter har inhämtats eller granskats.*

Uppgifter som anges i första stycket får inte användas i en brottsutredning till nackdel för den som har omfattats av åtgärden eller för någon annan som uppgifterna avser.

Förbud att *läsa av eller ta upp* vissa uppgifter

Förbud att *hämta in* vissa uppgifter

27 §[7]

Hemlig dataavläsning enligt 2 § första stycket 6 *eller 7* får inte avse uppgifter som enligt 27 kap. 2 § rättegångsbalken hindrar beslag.

Hemlig dataavläsning enligt 2 § första stycket 6 får inte avse uppgifter som enligt 27 kap. 2 § rättegångsbalken hindrar beslag.

Hemlig dataavläsning som gäller kommunikationsavlyssnings- eller rumsavlyssningsuppgifter får inte avse uppgifter i telefonsamtal, samtal eller andra meddelanden eller tal där någon som yttrar sig, på grund av bestämmelserna i 36 kap. 5 § andra–sjätte styckena rättegångsbalken, inte skulle ha kunnat höras som vittne om det som har sagts eller på annat sätt kommit fram.

Om det under verkställigheten kommer fram uppgifter som omfattas av första eller andra stycket ska *verkställigheten* omedelbart avbrytas *och* upptagningar och uppteckningar omedelbart förstö-

Om det under *eller efter* verkställigheten kommer fram uppgifter som omfattas av första eller andra stycket ska *granskningen av dessa uppgifter* omedelbart avbrytas. Upptagningar och upp-

[7] Senaste lydelse 2023:540.

ras i de delar som de omfattas av förbudet.

teckningar *ska* omedelbart förstöras i de delar som de omfattas av förbudet.

28 §[8]

När hemlig dataavläsning används eller har använts under en förundersökning ska det som gäller för hemlig avlyssning av elektronisk kommunikation enligt 27 kap. 23 a och 24 §§ rättegångsbalken *i lydelsen före den 1 oktober 2023* tillämpas för åtgärden. Det som gäller för hemlig rumsavlyssning ska dock tillämpas för hemlig dataavläsning som gäller rumsavlyssningsuppgifter.

När hemlig dataavläsning används eller har använts under en förundersökning ska det som gäller för hemlig avlyssning av elektronisk kommunikation enligt 27 kap. 23 a och 24 §§ rättegångsbalken tillämpas för åtgärden. Det som gäller för hemlig rumsavlyssning ska dock tillämpas för hemlig dataavläsning som gäller rumsavlyssningsuppgifter.

För underrättelse till en enskild vid hemlig dataavläsning under förundersökning gäller 27 kap. 31–33 §§ rättegångsbalken. Det som anges där om

– hemlig kameraövervakning ska tillämpas för hemlig dataavläsning som gäller kameraövervakningsuppgifter

– hemlig rumsavlyssning ska tillämpas för hemlig dataavläsning som gäller rumsavlyssningsuppgifter

– hemlig avlyssning av elektronisk kommunikation ska tillämpas för hemlig dataavläsning i övrigt

– telefonnummer, annan adress eller en viss elektronisk kommunikationsutrustning ska avse avläsningsbart informationssystem.

29 §[9]

När hemlig dataavläsning används eller har använts i fall som anges i 7 § ska 12 och 13 §§ lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott *i lydelsen före den 1 oktober 2023* tillämpas.

När hemlig dataavläsning används eller har använts i fall som anges i 7 § ska 12 och 13 §§ lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott tillämpas.

[8] Senaste lydelse 2023:540.
[9] Senaste lydelse 2023:540.

För underrättelse till en enskild vid hemlig dataavläsning i fall som anges i 7 § gäller 16–18 §§ lagen om åtgärder för att förhindra vissa särskilt allvarliga brott. Det som anges där om

– hemlig kameraövervakning ska tillämpas för hemlig dataavläsning som gäller kameraövervakningsuppgifter

– hemlig avlyssning av elektronisk kommunikation ska tillämpas för hemlig dataavläsning i övrigt

– telefonnummer, annan adress eller en viss elektronisk kommunikationsutrustning ska avse avläsningsbart informationssystem.

Lydelse enligt SOU 2023:60	*Föreslagen lydelse*
31 §	
När hemlig dataavläsning används eller har använts i fall som anges i 10 § ska 6 och *8* §§ lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet *i lydelsen före den 1 januari 2025* tillämpas. Det som anges där om inhämtning av uppgifter ska tillämpas för hemlig dataavläsning.	När hemlig dataavläsning används eller har använts i fall som anges i 10 § ska 6 och *7* §§ lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet tillämpas. Det som anges där om inhämtning av uppgifter ska tillämpas för hemlig dataavläsning.
Uppgifter som har kommit fram vid hemlig dataavläsning enligt 10 § får användas i en förundersökning endast efter tillstånd till hemlig dataavläsning enligt 4 eller 5 § som gäller kommunikationsövervaknings- eller platsuppgifter. Utan ett sådant tillstånd får dock inhämtade uppgifter ligga till grund för beslut om att inleda en förundersökning.	

Nuvarande lydelse	*Föreslagen lydelse*
	Dokumentation
	34 §
	Beslut och åtgärder som rör hemlig dataavläsning ska dokumenteras.

---

1. Denna lag träder i kraft den 1 mars 2025.

2. Äldre föreskrifter gäller fortfarande för tillstånd som har beviljats före ikraftträdandet.

3. För uppgifter från hemlig dataavläsning som har verkställts före ikraftträdandet gäller 28, 29 och 31 §§ i den äldre lydelsen.

2 Utredningens uppdrag och arbete

2.1 Utredningens uppdrag

Genom lagen (2020:62) om hemlig dataavläsning, som trädde i kraft den 1 april 2020, infördes ett nytt hemligt tvångsmedel – hemlig dataavläsning – som de brottsbekämpande myndigheterna under vissa förutsättningar kan använda vid misstankar om allvarlig brottslighet. Lagen är tidsbegränsad till utgången av mars 2025. Vi har haft i uppdrag att utvärdera den nya lagen. I uppdraget har bland annat ingått att

- analysera nyttan och behovet av hemlig dataavläsning,
- ta ställning till om bestämmelserna i lagen om hemlig dataavläsning bör göras permanenta,
- oavsett vilket ställningstagande som görs, analysera vilka åtgärder som behövs för ett permanentande och lämna förslag på dessa,
- analysera om lagstiftningen har fått en ändamålsenlig och proportionerlig utformning samt om kontrollmekanismerna och övriga rättssäkerhetsgarantier är tillräckliga,
- ta ställning till om det bör göras förändringar i regelverket i syfte att uppnå en mer effektiv brottsbekämpning, samtidigt som respekten för grundläggande fri- och rättigheter, såsom rätten till respekt för privatlivet, liksom kraven på rättssäkerhet, säkerställs,
- lämna förslag på nödvändiga författningsändringar och andra åtgärder samt
- bedöma behovet av följdändringar och säkerställa att en välfungerande systematik i regelverket kring såväl hemliga som öppna tvångsmedel upprätthålls.

Vi har även haft möjlighet att inom ramen för uppdraget överväga andra frågor som har samband med de frågeställningar som ska utredas. Utförligare redogörelser för uppdragets olika delar presenteras löpande i samband med våra överväganden. Utredningsdirektiven i dess helhet finns också bifogade som en bilaga till betänkandet.

2.2 Avgränsningar

Lagstiftningen om straffprocessuella tvångsmedel är ett prioriterat område för lagstiftaren. I våra överväganden måste vi förhålla oss till att hela rättsområdet är under utveckling. Även lagen om hemlig dataavläsning har förändrats sedan den nya lagen trädde i kraft för snart fyra år sedan. Tillämpningsområdet för hemlig dataavläsning har utökats både med hänsyn till straffskärpningar på straffrättens område och med hänsyn till lagändringar i annan lagstiftning som är knuten till lagen om hemlig dataavläsning. Dessutom har det i lagen om hemlig dataavläsning helt nyligen införts flera utökade möjligheter att använda åtgärden, se propositionen *Hemliga tvångsmedel – effektiva verktyg för att förhindra och utreda allvarliga brott,* prop. 2022/23:126. Vidare har flera andra utredningar, parallellt med vår utredning, haft i uppdrag att utreda näraliggande frågor. Dessa utredningar har lämnat olika lagförslag som både direkt och indirekt berör tillämpningsområdet för hemlig dataavläsning. Lagförslagen bereds för närvarande i Regeringskansliet och framgår av betänkandena *Bättre möjligheter att verkställa frihetsberövanden*, SOU 2022:50, *Datalagring och åtkomst till elektronisk information*, SOU 2023:22, och *Utökade möjligheter att använda preventiva tvångsmedel 2*, SOU 2023:60. Inom ramen för vårt uppdrag har vi inte haft anledning att ifrågasätta eller vidareutveckla dessa överväganden och förslag om hemlig dataavläsning. Eftersom förslagen för närvarande är under beredning har vi inte heller funnit anledning att lämna egna förslag i samma frågor. Vårt uppdrag, bortsett från den del som avser den hittillsvarande tillämpningen av hemlig dataavläsning, förutsätter dock att vi förhåller oss till hela det utökade tillämpningsområdet för hemlig dataavläsning. I våra samlade bedömningar och intresseavvägningar i kapitel 7 och 8 har vi därför beaktat såväl nyligen ikraftträdda lagändringar på området som de ytterligare lagförslag som för närvarande är under beredning och

som kan förväntas träda i kraft inom de närmsta åren. Vi har inte kunnat beakta material som har publicerats efter utgången av oktober 2023.

2.3 Utredningens arbete

Vi påbörjade vårt arbete i september 2022 och har hållit regelbundna sammanträden med experterna och den sakkunniga under hela utredningstiden. Totalt har åtta sammanträden hållits, varav ett tvådagarsmöte i internatform. Utredningen har inför varje sammanträde upprättat promemorior som i arbetets slutskede i allt väsentligt har motsvarat slutprodukten i detta betänkande.

I oktober 2022 var två personer från Polismyndigheten inbjudna till vårt inledande sammanträde för att bl.a. beskriva det praktiska förfarandet vid verkställighet av hemlig dataavläsning. Vi har under utredningsarbetet gjort myndighetsbesök hos Säkerhetspolisen. Visst samråd har skett med Utredningen om preventiva tvångsmedel eftersom denna utredning har behandlat frågor som vårt arbete har anknytning till. Härutöver har utredningen haft kontakt med företrädare för Post- och telestyrelsen samt företrädare för Telia Company AB (Telia), HI3G Access AB (Tre), Telenor Sverige AB (Telenor) och Tele2 Sverige AB (Tele2).

3 Bakgrund och allmänt om gällande rätt

3.1 Bakgrund

3.1.1 Tidigare förslag om hemlig dataavläsning

Det första förslaget till lagstiftning om hemlig dataavläsning lades fram år 2005 av Beredningen för rättsväsendets utveckling (BRU). BRU hade inget uttalat direktiv att utreda frågan om hemlig dataavläsning, men hade bl.a. i uppdrag att överväga på vilket sätt brottsutredningsverksamheten ytterligare kunde förbättras. Under arbetets gång påtalades från flera håll att det fanns ett behov av ett nytt hemligt tvångsmedel i svensk rätt – hemlig dataavläsning. Lagstiftning om hemlig dataavläsning, eller motsvarighet till åtgärden, fanns redan i flera länder och Danmark hade år 2002 som första nordiska land infört bestämmelser om dataaflæsning i retsplejeloven.

BRU:s lagförslag om hemlig dataavläsning lämnades i delbetänkandet *Tillgång till elektronisk kommunikation i brottsutredningar m.m.*, SOU 2005:38. Förslaget innebar att bestämmelser om hemlig dataavläsning skulle införas i en ny och inledningsvis tidsbegränsad lag. I betänkandet framhölls att den senaste kraftiga och snabba teknikutvecklingen, främst möjligheterna till kryptering och anonymisering, utnyttjades av kriminella som verktyg i grov brottslig verksamhet. BRU ifrågasatte om de då befintliga tvångsmedlen var tillräckliga i alla situationer. BRU kom till slutsatsen att det knappast fanns några alternativ till hemlig dataavläsning för att få fram den gömda informationen. Beredningen konstaterade att det handlade om svåra intresseavvägningar, men bedömde att det integritetsintrång som typiskt sett uppkommer vid användning av dataavläsning inte är så stort att det får hindra en lagstiftning på området. Utformningen av bestämmelserna i lagförslaget anslöt i stor utsträckning till då befintlig regler-

ing avseende hemlig teleavlyssning och hemlig kameraövervakning. Beredningen konstaterade att det fanns ett behov av metoden och att den framstod som effektiv, men betonade samtidigt att närmare detaljer i de frågorna inte var helt enkla att bedöma innan tvångsmedlet tillämpats under en tid. Förslaget som lämnades var därför att lagstiftningen om hemlig dataavläsning, i vart fall till en början, skulle vara tidsbegränsad.

Under remissbehandlingen framförde såväl olika myndigheter som privata aktörer kritik mot förslaget. Kritiken avsåg framför allt det stora integritetsintrång som åtgärden skulle innebära. Både behovet och den förväntade effektiviteten av det nya tvångsmedlet ifrågasattes. Beredningens lagförslag kom därför inte att genomföras. En mer utförlig sammanfattning av 2005 års lagförslag återfinns i betänkandet *Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet*, SOU 2017:89 s. 105 ff.

Frågan om hemlig dataavläsning togs några år senare upp på nytt av Utredningen om vissa hemliga tvångsmedel, i betänkandet *Hemliga tvångsmedel mot allvarliga brott*, SOU 2012:44. Utredningen hade bl.a. i uppdrag att utvärdera vissa tidsbegränsade lagar som reglerade hemliga tvångsmedel. Under arbetets gång framhöll brottsbekämpande myndigheter på nytt att det fanns ett behov av att hemlig dataavläsning infördes som ett hemligt tvångsmedel. Myndigheterna hänvisade därvid till 2005 års förslag. Utredningen konstaterade att uppdraget inte innefattade att utreda frågan om hemlig dataavläsning, men gjorde i betänkandet ett antal anmärkningar om hemlig dataavläsning. I samband därmed påpekade utredningen angelägenheten av att frågan skulle utredas (se a. SOU s. 765 ff.).

Regeringen har även i sin nationella strategi mot terrorism särskilt framhållit att de brottsbekämpande myndigheterna måste ges förutsättningar att, trots den tekniska utvecklingen, kunna upprätthålla förmågan att inhämta information (*Förebygga, förhindra och försvåra – Den svenska strategin mot terrorism*, skr. 2015/15:146 s. 16 f.).

3.1.2 Utredningen om hemlig dataavläsning

Regeringen beslutade i maj 2016 att tillkalla en särskild utredare med uppdrag att utreda om svenska brottsbekämpande myndigheter skulle ges möjlighet att använda hemlig dataavläsning (dir. 2016:36). Utred-

ningen lämnade i november 2017 sina överväganden och förslag i delbetänkandet *Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet*, SOU 2017:89.

I betänkandet konstaterades att såväl den tekniska utvecklingen som brotts- och samhällsutvecklingen bidragit till att traditionella hemliga tvångsmedel tappat i effektivitet. Vidare konstaterades att det saknades tydligt lagstöd för att använda hemlig dataavläsning som verkställighetsmetod för andra hemliga tvångsmedel (se a. SOU s. 116 ff.). Mot denna bakgrund analyserade utredningen behovet av att införa hemlig dataavläsning som ett nytt hemligt tvångsmedel. Utredningen fann sammanfattningsvis att de brottsbekämpande myndigheterna hade ett tungt vägande behov av hemlig dataavläsning både under och utanför en förundersökning. Metoden förväntades vidare vara effektiv för att bekämpa allvarlig brottslighet. Utredningen kom vid en integritetsriskanalys till slutsatsen att det är proportionerligt att införa regler om hemlig dataavläsning. Detta under förutsättning att reglerna balanserar de ökade integritetsriskerna och de risker för informationssäkerheten som kan uppstå. Utformningen av lagförslaget anslöt därför i stor utsträckning till befintlig reglering avseende hemliga tvångsmedel, med motsvarande kontrollmekanismer och rättssäkerhetsgarantier. Förslaget som lämnades var att det skulle införas en ny lag med bestämmelser om hemlig dataavläsning. Den nya lagen skulle enligt förslaget tidsbegränsas till att gälla i fem år efter införandet, för att en utvärdering av tvångsmedlet skulle kunna göras när lagen tillämpats en tid. Utredningens experter ställde sig i allt väsentligt bakom utredningens överväganden och förslag. Till betänkandet fogades två särskilda expertyttranden. Advokatsamfundets expert delade inte utredningens bedömning beträffande proportionalitetsavvägningen och uttryckte även vissa materiella synpunkter på lagstiftningen. Därtill framhöll flera av experterna att det för operatörer som tillhandahåller allmänt tillgängliga kommunikationsnät borde införas en skyldighet att samarbeta med de brottsbekämpande myndigheterna.

3.1.3 Remissinstanserna

Förslaget fick ett blandat mottagande hos remissinstanserna. Kritiken avsåg huvudsakligen utredningens proportionalitetsavvägningar. Flera remissinstanser framförde kritik beträffande analysen av behovet, tillämpningsområdet och den förväntade effektiviteten av det nya tvångsmedlet. Man påpekade även olika risker för den personliga integriteten och informationssäkerheten. Den övervägande delen av remissinstanserna, såväl myndigheter som privata aktörer, ställde sig dock positiva till utredningens analyser och lagförslag. För en sammanställning av remissyttrandena, se Ju2017/08898/Å.

3.1.4 Lagrådets yttrande och prop. 2019/20:64

Regeringen beslutade efter remissbehandlingen att inhämta Lagrådets yttrande över lagförslagen. Lagrådet framhöll i sitt yttrande av den 18 november 2019 bl.a. följande allmänna synpunkter.

> Lagrådet bedömer att det underlag som presenteras är tillräckligt för att motivera att hemlig dataavläsning införs som ett nytt hemligt tvångsmedel. Mot denna bakgrund, och med beaktande av att hemlig dataavläsning alltid ska prövas av domstol som ska underrätta Säkerhets- och integritetsskyddsnämnden om beslutet, anser Lagrådet att förslagen kan läggas till grund för lagstiftning.
>
> I sammanhanget måste emellertid framhållas vikten av att det säkerställs att Säkerhets- och integritetsskyddsnämnden har förutsättningar att på ett effektivt sätt utöva tillsyn och efterhandskontroll samt att det görs en ingående utvärdering av behovet, nyttan och proportionaliteten innan det fattas beslut om huruvida lagstiftningen ska förlängas eller permanentas.

Lagrådet hade även vissa materiella synpunkter på lagförslaget. Beträffande den valda lagstiftningstekniken anförde Lagrådet följande.

> Den valda lagstiftningstekniken, att reglera hemlig dataavläsning i en egen lag, innebär dels att många av de föreslagna bestämmelserna i stora delar är likalydande med bestämmelser i gällande tvångsmedelslagstiftning, dels att hänvisningar görs till flera andra lagar. Regelverket blir därmed mer svåröverskådligt än om bestämmelserna om hemlig dataavläsning hade arbetats in i den befintliga lagstiftningen; detta särskilt eftersom hemlig dataavläsning i stor utsträckning utgör en ny verkställighetsform av redan existerande hemliga tvångsmedel.

> Lagstiftningstekniken ställer stora krav på tillämparen och ökar riskerna för misstag. Eftersom det är fråga om en tillfällig lagstiftning får emellertid den valda metoden accepteras. För det fall det blir fråga om att förlänga eller permanenta hemlig dataavläsning bör dock lagstiftningstekniken övervägas på nytt.

Lagrådets yttrande i dess helhet finns som en bilaga till den påföljande propositionen *Hemlig Dataavläsning*, 2019/20:64. I propositionen följde regeringen i allt väsentligt utredningens förslag, med de justeringar som Lagrådet förordade. Regeringen gick också på experternas linje i frågan om operatörernas medverkansskyldighet. Justitieutskottet ställde sig bakom regeringens förslag (bet. 2019/20:JuU19) och riksdagen beslutade den 19 februari 2020 att införa en ny lag om hemlig dataavläsning.

3.2 Lagen (2020:62) om hemlig dataavläsning

3.2.1 Inledning

Lagen (2020:62) om hemlig dataavläsning trädde i kraft den 1 april 2020. Det är en tidsbegränsad lag som gäller till och med utgången av mars 2025. Lagen kompletteras av regler i förordningen (2020:172) om hemlig dataavläsning.

I förarbetena till lagen slås fast att hemlig dataavläsning utgör ett komplement till andra tvångsmedel (se prop. 2019/20:64 s. 93). Många av de uppgifter som kan hämtas in genom hemlig dataavläsning kan de brottsbekämpande myndigheterna få tillstånd att hämta in genom andra tvångsmedel. I många fall motsvaras dock inte rätten att hämta in uppgifterna av en faktisk möjlighet att göra så. Det beror till stor del på att internetbaserad kommunikation allt oftare har krypterat innehåll som inte kan fångas upp i ett läs- eller avlyssningsbart skick genom traditionella tvångsmedel (se SOU 2017:89 s. 115 och a. prop. s. 56). De traditionella sätten att verkställa hemliga tvångsmedel har blivit mindre effektiva eftersom de inte är anpassade till modern kommunikationsutrustning. Hemlig dataavläsning har därför införts som ett verktyg för att återställa de brottsbekämpande myndigheternas förmåga (se a. prop. s. 125). Den nya lagen ger under vissa förutsättningar de brottsbekämpande myndigheterna tillgång till dels en särskild verkställighetsform av andra hemliga tvångsmedel, dels ett självständigt hemligt tvångsmedel som ger tillgång till uppgifter som

inte är åtkomliga genom andra hemliga tvångsmedel. Det handlar i det senare avseendet i korthet om att myndigheterna i hemlighet och i realtid kan komma åt uppgifter som finns lagrade i en kommunikationsutrustning eller som visar hur denna används.

3.2.2 Vad är hemlig dataavläsning?

Hemlig dataavläsning är ett hemligt tvångsmedel som de brottsbekämpande myndigheterna kan få tillstånd att använda sig av vid misstanke om allvarlig brottslighet. Tvångsmedlet innebär i praktiken att den brottsbekämpande myndigheten, i hemlighet och med ett tekniskt hjälpmedel, bereder sig tillgång till teknisk utrustning som kan användas för kommunikation. I lagen definieras detta som ett avläsningsbart informationssystem. Det kan handla om t.ex. datorer, mobiltelefoner eller olika användarkonton till lagrings- och kommunikationstjänster. Syftet med tillståndet är att myndigheten ska kunna ta del av uppgifter som finns i den fysiska utrustningen eller tjänsten. Detta innefattar såväl lagrade uppgifter (t.ex. innehållet i e-post och textmeddelanden, besökta webbsidor och lagrade dokument) som uppgifter i realtid (t.ex. telefon- och videosamtal samt textmeddelanden). Hemlig dataavläsning ger även den brottsbekämpande myndigheten möjlighet att bl.a. använda en teknisk utrustnings mikrofon- och kamerafunktioner samt genom positioneringsfunktionerna fastställa den geografiska platsen för utrustningen.

Metoden för hemlig dataavläsning skiljer sig från verkställighet av andra hemliga tvångsmedel. Verkställighet av traditionella hemliga tvångsmedel sker genom inhämtning av uppgifter från operatörer alternativt genom kamera- eller avlyssningsutrustning som tillhör de brottsbekämpande myndigheterna. Vid verkställighet av hemlig dataavläsning hämtas uppgifterna i stället in från den berördes egna kommunikationsutrustning, t.ex. en dator eller en mobiltelefon. Metoden för hemlig dataavläsning kan sägas innefatta två delar, dels att den brottsbekämpande myndigheten i hemlighet bereder sig tillgång till det avläsningsbara informationssystemet, dels att myndigheten hämtar in och tar del av uppgifter som finns åtkomliga i systemet.

3.2.3 Legaldefinitionen av hemlig dataavläsning

Legaldefinitionen av hemlig dataavläsning framgår av 1 § första stycket lagen om hemlig dataavläsning.

> Hemlig dataavläsning innebär att uppgifter, som är avsedda för automatiserad behandling, i hemlighet och med ett tekniskt hjälpmedel läses av eller tas upp i ett avläsningsbart informationssystem.

Definitionen tar sin utgångspunkt i definitioner av andra hemliga tvångsmedel. Den knyter också an till straffbestämmelsen om dataintrång i 4 kap. 9 c § brottsbalken, eftersom regleringen innebär att åtgärder som annars är straffbara som dataintrång blir tillåtna i vissa fall. Nedan följer en kort förklaring av uttrycken i legaldefinitionen av hemlig dataavläsning. En mer utförlig beskrivning återfinns i prop. 2019/20:64 s. 101 ff. och 209 ff.

Uppgifter avsedda för automatiserad behandling

Att uppgifterna är ”avsedda för automatiserad behandling” är ett teknikneutralt uttryck som knyter an till straffbestämmelsen om dataintrång och motsvarande uttryck i denna bestämmelse. Uttrycket innebär att uppgifterna ska vara anpassade för en teknisk process genom vilken uppgifterna behandlas av ett avläsningsbart informationssystem. Det täcker i sin tur in alla uppgifter som kan uttryckas i en för en dator anpassad och läsbar form, t.ex. program, applikationer eller information. Det är för tillämpningen utan betydelse var uppgifterna finns eller förvaras i systemet. Uppgifterna behöver inte finnas i informationssystemet vid tidpunkten för tillståndet utan kan tillföras systemet under tillståndstiden.

I hemlighet och med ett tekniskt hjälpmedel

Att åtgärden genomförs ”i hemlighet” innebär att den som blir föremål för åtgärden inte ska känna till den. Uttrycket ”tekniskt hjälpmedel” är teknikneutralt och dess innebörd utvecklas närmare nedan i avsnitt 3.2.12.

Läses av eller tas upp

Att uppgifterna ”läses av” kan ta sikte både på den tekniska process som exempelvis gör viss information läsbar, och på den process som innebär att den brottsutredande myndigheten tar faktisk del av innehållet i informationen. Uttrycket att uppgifterna ”tas upp” tydliggör att uppgifterna får granskas såväl i realtid som i efterhand.

Avläsningsbart informationssystem

Med uttrycket ”avläsningsbart informationssystem” avses det system som innehåller de uppgifter som de brottsbekämpande myndigheterna ska få tillgång till. Uttrycket definieras i 1 § andra stycket lagen om hemlig dataavläsning. Där slås inledningsvis fast att en elektronisk kommunikationsutrustning utgör ett avläsningsbart informationssystem. Uttrycket har samma innebörd som i annan tvångsmedelsreglering och innefattar all slags befintlig och framtida teknisk utrustning som kan användas för elektronisk kommunikation, t.ex. datorer, mobiltelefoner och servrar. Enligt definitionen kan ett avläsningsbart informationssystem avse inte bara fysisk utrustning, också ett användarkonto till, eller på motsvarande sätt avgränsad del av, en kommunikationstjänst, lagringstjänst eller liknande tjänst. Gemensamt för tjänsterna är att det är möjligt att få åtkomst till uppgifter i dem från olika elektroniska kommunikationsutrustningar oberoende av var uppgifterna är lagrade, efter angivande av t.ex. inloggningsuppgifter. Uttrycket omfattar t.ex. internetbaserade meddelande- och telefonitjänster. Med lagringstjänst avses s.k. molntjänster. Uppgifter i dessa lagras på en annan geografisk plats än i den egna fysiska utrustningen. Med uttrycket liknande tjänster avses tjänster vars primära syfte inte är kommunikation eller lagring men som innefattar en sådan möjlighet, t.ex. spel- eller bokningstjänster. Avgränsningen av vilken utrustning som omfattas av tillståndet ska göras utifrån vad som framstår som rimligt med hänsyn till det aktuella informationssystemet (se a. prop. s. 211).

3.2.4 Uppgifter som kan hämtas in med hemlig dataavläsning

I 2 § första stycket lagen om hemlig dataavläsning anges i sju punkter vilka typer av uppgifter som får läsas av eller tas upp efter tillstånd till hemlig dataavläsning. Uppräkningen är uttömmande.

1. kommunikationsavlyssningsuppgifter,
2. kommunikationsövervakningsuppgifter,
3. platsuppgifter,
4. kameraövervakningsuppgifter,
5. rumsavlyssningsuppgifter,
6. uppgifter som finns lagrade i ett avläsningsbart informationssystem men som inte avses i 1–5, eller
7. uppgifter som visar hur ett avläsningsbart informationssystem används men som inte avses i 1–6.

De sju uppgiftstyperna kan i sin tur delas in i två huvudkategorier. Beträffande uppgiftstyperna i punkt 1–5 har hemlig dataavläsning närmast karaktären av verkställighetsmetod för andra hemliga tvångsmedel. Uppgiftstyperna motsvarar huvudsakligen uppgifter som redan innan lagstiftningens ikraftträdande fick hämtas in enligt andra bestämmelser om hemliga tvångsmedel. Det råder dock inte fullständig överensstämmelse eftersom inhämtningen av uppgiftstyperna kan verkställas på annat sätt än traditionellt. Exempelvis kan den brottsutredande myndigheten vid verkställighet av punkt 3 använda positioneringsfunktionen i en mobiltelefon. Hemlig dataavläsning omfattar inte heller s.k. basstationstömningar som är vanligt förekommande vid hemlig övervakning av elektronisk kommunikation (se prop. 2019/20:64 s. 107 och 211 f.). Uppgiftstyperna i punkt 6 och 7 motsvaras inte av några uppgifter som är åtkomliga genom andra hemliga tvångsmedel. Hemlig dataavläsning utgör i detta avseende ett helt nytt hemligt tvångsmedel. I det följande redogörs kort för de olika uppgiftstyperna och deras respektive definition enligt 1 § andra stycket lagen om hemlig dataavläsning. En närmare beskrivning av de olika uttrycken återfinns i a. prop. s. 106 ff. och 213 f.

Kommunikationsavlyssningsuppgifter

Uppgifterna definieras som ”uppgifter om innehåll i meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller någon annan adress”. Motsvarande uppgifter får hämtas in genom hemlig avlyssning av elektronisk kommunikation, se 27 kap. 18 § rättegångsbalken.

Kommunikationsövervakningsuppgifter

Dessa uppgifter definieras som ”uppgifter om meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller någon annan adress”. Kommunikationsavlyssningsuppgifter, dvs. uppgifter om vad ett meddelande innehåller, omfattas alltså inte av uppgiftstypen. Motsvarande uppgifter får hämtas in genom hemlig övervakning av elektronisk kommunikation enligt 27 kap. 19 § första stycket 1 rättegångsbalken och vid inhämtning enligt 1 § 1 inhämtningslagen. Inhämtningslagen är tillämplig i de brottsbekämpande myndigheternas underrättelseverksamhet och reglerar vilka uppgifter om elektronisk kommunikation som myndigheterna inom ramen för denna verksamhet får inhämta från teleoperatörer. När det gäller hemlig dataavläsning i inhämtningslagsfallen får tillståndet endast avse kommunikationsövervakningsuppgifter i förfluten tid, se 10 § tredje stycket lagen om hemlig dataavläsning.

Platsuppgifter

Platsuppgifter är ”uppgifter om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits”. Motsvarande uppgifter får hämtas in genom hemlig övervakning av elektronisk kommunikation enligt 27 kap. 19 § första stycket 3 rättegångsbalken och vid inhämtning enligt 1 § 3 inhämtningslagen. Verkställighet av hemlig dataavläsning kan, som ovan angetts, ske genom t.ex. användning av positioneringsfunktionen i en mobiltelefon. Detta ger ofta mer exakta platsuppgifter än vid en traditionell s.k. basstationstömning.

Kameraövervakningsuppgifter

Med kameraövervakningsuppgifter avses ”uppgifter som framkommer genom optisk personövervakning”. Motsvarande uppgifter får hämtas in genom hemlig kameraövervakning, se 27 kap. 20 a § rättegångsbalken.

Rumsavlyssningsuppgifter

Rumsavlyssningsuppgifter definieras som ”uppgifter som avser tal i enrum, samtal mellan andra eller förhandlingar vid sammanträden eller andra sammankomster som allmänheten inte har tillträde till”. Motsvarande uppgifter får hämtas in genom hemlig rumsavlyssning, se 27 kap. 20 d § rättegångsbalken.

Lagrade uppgifter

Punkt 6 avser uppgifter som finns lagrade i ett avläsningsbart informationssystem, men som inte avses i punkt 1–5. Uppgifterna ska finnas lagrade i informationssystemet när avläsningen eller upptagningen genomförs. Det saknar betydelse hur uppgifterna lagrats. Exempel på lagrade uppgifter är datafiler såsom text-, bild- och ljudfiler, men också program- eller systemfiler. Tillämpningen är sekundär i förhållande till punkt 1–5. Exempelvis faller lagrade uppgifter i form av uppgifter i skickade meddelanden under punkt 1 och s.k. metadata kan falla under såväl punkt 2 som 3. Ett sparat utkast till ett meddelande är däremot att kategorisera som en punkt 6-uppgift. I avsnitt 6.2.5 återkommer vi närmare till olika metadata och kategoriseringen av de olika uppgiftstyperna.

Uppgifter om hur systemet används

Punkt 7 avser uppgifter som visar hur ett avläsningsbart informationssystem används men som inte avses i punkt 1–6. Det handlar om användning som inte leder till att information lagras, t.ex. vilka lösenord, program eller applikationer som används, eller utkast till meddelanden som inte sparas. Tillämpningen är sekundär till övriga punkter.

3.2.5 Tillämpningsområde

Bestämmelserna om hemlig dataavläsning gäller under vissa närmare angivna förutsättningar både under och utanför en förundersökning. I avsnitt 3.2.8 och 3.2.9 nedan utvecklas de särskilda kraven för hemlig dataavläsning under respektive utanför en förundersökning närmare. Tillämpningsområdet för hemlig dataavläsning har sedan den tillfälliga lagen trädde i kraft utökats, framför allt genom de lagändringar som trädde i kraft den 1 oktober 2023, se *Hemliga tvångsmedel – effektiva verktyg för att förhindra och utreda allvarliga brott,* prop. 2022/23:126. Genom lagändringarna utökades tillämpningsområdet för de bakomliggande hemliga tvångsmedlen enligt rättegångsbalken och preventivlagen, vilket fick genomslag även för hemlig dataavläsning. Vi redogör närmare för dessa utökningar av tillämpningsområdet för hemlig dataavläsning i kapitel 7 och 8. I avsnitt 3.3.2 redogörs för hur straffskärpningar på straffrättens område och andra lagändringar kan påverka tillämpningsområdet för hemlig dataavläsning. En viktig utgångspunkt i lagstiftningen om hemlig dataavläsning är att den är teknikneutral. Syftet med en sådan lagstiftning är att den ska stå sig över tid, vilket också innebär att tillämpningsområdet för lagen kan ändras i takt med den tekniska utvecklingen. Avgörande för lagens tillämpningsområde är alltså befintlig teknik i förhållande till lagstiftningens – och tillståndsgivningens – närmare avgränsningar (jfr SOU 2017:89 s. 115).

3.2.6 Ändamålen med hemlig dataavläsning

I lagen om hemlig dataavläsning finns inte några uttryckliga principer om åtgärdens ändamål. Precis som för övriga hemliga tvångsmedel kommer ändamålen i stället till uttryck i lagens materiella bestämmelser. Genom avgränsningar tydliggörs i de materiella reglerna i vilka fall hemlig dataavläsning får användas för olika ändamål (se prop. 2019/20:64 s. 111). Ändamålet skiljer sig åt beroende på om åtgärden används under eller utanför en förundersökning. De brottsbekämpande myndigheterna använder huvudsakligen hemlig dataavläsning under förundersökning. Ändamålet är då detsamma som vid användning av hemliga tvångsmedel enligt 27 kap. rättegångsbalken. Det övergripande ändamålet med alla hemliga tvångsmedel under förundersökning är att åtgärderna ska bidra till att vissa brott kan utredas

och att eventuell bevisning kan säkras, jfr 23 kap. 2 § rättegångsbalken. Under vissa förutsättningar får hemlig dataavläsning också användas utanför förundersökning i underrättelseverksamhet. Med underrättelseverksamhet avses verksamhet som består i att samla in, bearbeta och analysera information för att klarlägga om viss brottslig verksamhet har utövats eller kan komma att utövas. Uttrycket preventiva tvångsmedel används ibland för att beteckna hemliga tvångsmedel i underrättelseverksamhet. Förutsättningar för användning av hemliga tvångsmedel i underrättelseverksamhet regleras förutom i lagen om hemlig dataavläsning även i preventivlagen (2007:979), inhämtningslagen (2012:278) och lagen (2022:700) om särskild kontroll av vissa utlänningar (LSU). Ändamålet med såväl hemlig dataavläsning som andra hemliga tvångsmedel med stöd av preventivlagen är att förhindra vissa särskilt allvarliga brott (jfr 5 § preventivlagen). På motsvarande sätt är ändamålet med hemliga tvångsmedel med stöd av inhämtningslagen att förebygga, förhindra eller upptäcka sådan brottslighet som anges i den lagen (jfr 2 § inhämtningslagen). Slutligen är ändamålet med hemliga tvångsmedel vid särskild utlänningskontroll att klarlägga om vissa utvisade utlänningar, vars utvisningsbeslut inte går att verkställa, under vissa i lagen angivna förutsättningar utgör kvalificerade hot mot Sveriges säkerhet. Detta kan utläsas av 5 kap. 1, 5–6 §§ LSU.

3.2.7 Grundläggande förutsättningar för hemlig dataavläsning – proportionalitet och differentiering

Vid all tvångsmedelsanvändning gäller proportionalitetsprincipen som allmän princip. För att tydliggöra detta har principen lagfästs i de olika tvångsmedelslagarna och så även i 3 § lagen om hemlig dataavläsning. Principen innebär att hemlig dataavläsning i fråga om art, styrka, räckvidd och varaktighet ska stå i rimlig proportion till vad som står att vinna med tvångsåtgärden.

Regeringen uttalade i förarbetena att det vid proportionalitetsbedömningen ska beaktas att hemlig dataavläsning bör vara sekundär till andra tvångsmedel. Regeringen avvisade dock vad vissa remissinstanser anförde om att uttryckligen göra hemlig dataavläsning subsidiärt till andra tvångsmedel (se prop. 2019/20:64 s. 110 och 116). Regeringens uttalande innebär att hemlig dataavläsning är ett så ingripande tvångsmedel att det ska användas endast när andra tvångs-

medel inte är framkomliga alternativ. Den som ansöker om hemlig dataavläsning måste därmed utreda eller tömma ut möjligheterna till andra åtgärder innan ansökan görs. Det är dock inte något krav att övriga tvångsmedel har prövats och misslyckats för att tillstånd till hemlig dataavläsning ska kunna ges. En utgångspunkt är att det kan vara proportionerligt att använda hemlig dataavläsning om andra åtgärder för att komma åt uppgifterna inte är tillräckliga, skulle vara väsentligt svårare att genomföra eller kan förväntas leda till större integritetsintrång (se SOU 2017:89 s. 346 och a. prop. s. 214).

Principen gäller under hela förfarandet, dvs. såväl vid tillståndsprövningen som vid verkställigheten (se a. prop. s. 111 med hänvisningar till SOU 1995:47 s. 324 och prop. 2005/06:178 s. 101). Proportionalitetsprincipen ska beaktas självmant och löpande av de brottsbekämpande myndigheterna. I proportionalitetsprövningen innefattas att beakta vilka eventuella risker åtgärden medför för informationssäkerheten och företagshemligheter eller annan känslig information. Proportionalitetsprincipen har också betydelse för hur ett tillstånd ska utformas och vilka villkor som det ska förenas med. Principen får särskilt stor betydelse när en ansökan om hemlig dataavläsning avser flera uppgiftstyper eftersom intrånget i den enskildes personliga integritet då typiskt sett blir större. Utgångspunkten är att varje tillstånd till hemlig dataavläsning ska differentierats och ges med restriktivitet. Differentieringen innebär att behovet av uppgifter i varje enskilt fall ska vara styrande för vad hemlig dataavläsning får och ska kunna användas för i det enskilda fallet (se SOU 2017:89 s. 314 och prop. 2019/20:64 s. 92 f.). Under förutsättning att det bedöms proportionerligt finns dock inte något formellt hinder mot att ett tillstånd om dataavläsning omfattar samtliga uppgiftstyper.

3.2.8 Krav för tillstånd i förundersökningsfallen

I 4–6 a §§ lagen om hemlig dataavläsning framgår vad som gäller för hemlig dataavläsning under en förundersökning. Beträffande punkt 1–5 i första stycket 2 § gäller som utgångspunkt i huvudsak motsvarande krav som stadgas för de bakomliggande tvångsmedlen i 27 kap. rättegångsbalken. Eftersom det är fråga om flera olika bakomliggande tvångsmedel, skiljer sig kraven för hemlig dataavläsning åt (se kursiverat i framställningen nedan). När hemlig dataavläsning används som

ett självständigt tvångsmedel enligt 2 § första stycket 6 och 7 lagen om hemlig dataavläsning motsvarar kraven vad som gäller för hemlig avlyssning av elektronisk kommunikation.

Behovet av åtgärden - synnerlig vikt

Inledningsvis ställs som krav att tvångsåtgärden ska vara av ”synnerlig vikt” för utredningen. Detta framgår av 4 §, 4 b § första stycket, 5 § och 6 § första stycket lagen om hemlig dataavläsning. Innebörden av kravet är detsamma som för andra hemliga tvångsmedel och avgörs i det enskilda fallet. Åtgärden behöver inte nödvändigtvis ge avgörande bevisning för fällande dom. Vid bedömningen ska metoden ha en framträdande plats. Åtgärden får inte tillåtas om det som kan vinnas är åtkomligt med andra, mindre ingripande metoder. Synnerlig vikt kan anses föreligga om andra åtgärder inte är tillräckliga, väsentligt svårare att genomföra än hemlig dataavläsning eller förväntas leda till ett större integritetsintrång (se SOU 2017:89 s. 351 f. och prop. 2019/20:64 s. 117 f.).

Allvarlig brottslighet

I lagen om hemlig dataavläsning ställs vidare krav på att det ska vara fråga om viss allvarlig brottslighet. Enligt 4 § kan alla de brott som kan leda till hemlig avlyssning av elektronisk kommunikation också leda till hemlig dataavläsning. Detta gäller med undantag för hemlig dataavläsning som avser *rumsavlyssningsuppgifter.* Åtgärden får i detta avseende endast tillåtas vid förundersökning om sådana brott som kan föranleda hemlig rumsavlyssning, se 6 §.

Skälig misstanke

En förutsättning för att tillstånd till hemlig dataavläsning ska beviljas är att någon är skäligen misstänkt för brottet eller brotten, se 4 §. Undantag från huvudregeln görs i 4 b och 5 §§.

Hemlig dataavläsning avseende *kommunikationsavlyssningsuppgifter* får enligt 4 b § första stycket användas för att utreda vem som skäligen kan misstänkas för brott vid en förundersökning om brott

som avses i 27 kap. 18 b § andra stycket rättegångsbalken. Syftet med den hemliga dataavläsningen ska vara att identifiera en misstänkt gärningsman. Om det finns en skäligen misstänkt person kan hemlig dataavläsning användas i syfte att identifiera ytterligare personer som skälig misstanke kan riktas mot. I 4 b § andra stycket anges kraven på samband mellan den person som den hemliga dataavläsningen riktas mot och det informationssystem som avläsningen avser. Kraven motsvarar de krav som gäller enligt 27 kap. 18 b § tredje stycket rättegångsbalken. Hemlig dataavläsning enligt 4 b § får alltså användas under samma förutsättningar som hemlig avlyssning av elektronisk kommunikation får används för att utreda vem som skäligen kan misstänkas för brott (se prop. 2022/23:126 s. 240 f.).

Hemlig dataavläsning avseende *kommunikationsövervaknings- eller platsuppgifter* får enligt 5 § användas för att utreda vem som skäligen kan misstänkas för ett brott vid en förundersökning om brott som avses i 27 kap. 19 b § andra stycket rättegångsbalken. Hemlig dataavläsning enligt 5 § får alltså användas vid samma brott som när det gäller hemlig övervakning av elektronisk kommunikation som används för att utreda vem som skäligen kan misstänkas för brott. I 5 § andra stycket anges att det ska vara fråga om ett avläsningsbart informationssystem som har använts vid ett brott, eller i anslutning till en brottsplats vid brottstidpunkten eller som av någon annan anledning är av synnerlig vikt för utredningen (se prop. 2019/20:64 s. 219 och prop. 2022/23:126 s. 241).

Krav på bestämd plats eller koppling till informationssystem

Enligt 4 a § första stycket och 6 § andra stycket krävs som huvudregel att det finns en koppling mellan den misstänkte och informationssystemet. Beviskravet för kopplingen är angett till ”särskild anledning att anta”. I 4 a § andra stycket stadgas ett undantag från huvudregeln som gäller *kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter.* För dessa uppgiftstyper får tillståndet, om inte annat anges i 4 b eller 5 §§, även avse ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att den misstänkte under tillståndstiden har kontaktat eller kommer att kontakta.

Regeringen gjorde i lagstiftningsarbetet det principiella ställningstagandet att verkställighet genom hemlig dataavläsning ska vara underkastad ett platskrav (se prop. 2019/20:64 s. 120). Hemlig dataavläsning avseende *kameraövervakningsuppgifter* måste därför enligt 4 a § tredje stycket avse en plats där den misstänkte kan antas uppehålla sig. En sådan plats får dock inte vara någons stadigvarande bostad. Hemlig dataavläsning av *rumsavlyssningsuppgifter* får enligt 6 § tredje stycket endast användas på en plats där det finns särskild anledning att anta att den misstänkte kommer uppehålla sig. Är platsen någon annan stadigvarande bostad än den misstänktes, får tillstånd beviljas endast om det finns synnerlig anledning att anta att den misstänkte kommer att uppehålla sig där. Sedan den 1 oktober 2023 är det möjligt att, i undantagsfall och under vissa i lagen närmare angivna omständigheter, knyta ett tillstånd till den skäligen misstänkte i stället för till viss plats. Detta framgår av 4 a § fjärde stycket och 6 § fjärde stycket (se prop. 2022/23:126 s. 240 och 242).

Hemlig dataavläsning som gäller *kameraövervaknings- eller rumsavlyssningsuppgifter* får aldrig användas på en plats dit tillträdestillstånd enligt 13 § inte får beviljas, se 6 a §.

3.2.9 Krav för tillstånd i underrättelsefallen

I 7–10 §§ lagen om hemlig dataavläsning framgår vad som gäller för hemlig dataavläsning utanför en förundersökning i underrättelseverksamhet. I dessa fall finns bestämmelser om hemlig tvångsmedelsanvändning i preventivlagen, lagen om särskild kontroll av vissa utlänningar och inhämtningslagen. Som utgångspunkt gäller i huvudsak motsvarande krav för hemlig dataavläsning som stadgas för det bakomliggande tvångsmedlet. I övrigt, dvs. när hemlig dataavläsning används som ett självständigt tvångsmedel enligt 2 § första stycket 6 och 7, motsvarar kraven vad som gäller för hemlig avlyssning av elektronisk kommunikation.

Preventivlagsfallen

Med preventivlagen avses lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott. Lagen syftar framför allt till att ge Säkerhetspolisen bättre förutsättningar att bedriva sin verksam-

het. Förutsättningarna för tillstånd till hemlig dataavläsning i preventivlagsfallen regleras i 7 § lagen om hemlig dataavläsning. Kraven motsvarar i huvudsak kraven för tillstånd för tvångsmedelsanvändning enligt preventivlagen. I brottskatalogen ingår bl.a. spioneri och terroristbrott. Tillstånd till hemlig dataavläsning får i preventivlagsfallen aldrig avse rumsavlyssningsuppgifter. Vidare ställs krav på att åtgärden ska vara av ”synnerlig vikt” för att förhindra aktuell brottslighet. Innebörden av uttrycket är densamma som i förundersökningsfallen. Skillnaden är att åtgärden inte syftar till att utreda brott, utan till att förhindra att ett planerat brott begås. Av 8 § framgår att platskravet och huvudregeln om koppling mellan den enskilde och informationssystemet är detsamma som i förundersökningsfallen.

Särskild utlänningskontroll

Lagen (2022:700) om särskild kontroll av vissa utlänningar (LSU) är tillämplig på en begränsad grupp av utlänningar som bedöms utgöra kvalificerade hot mot Sveriges säkerhet. Lagen träde i kraft den 1 juli 2022 och ersatte då den tidigare lagen (1991:572) om särskild utlänningskontroll. Den nya LSU fick genomslag i lagen om hemlig dataavläsning på så sätt att hänvisningen i 9 § lagen om hemlig dataavläsning ändrades från den gamla till den nya lagen. LSU innehåller bl.a. möjligheter att använda hemliga tvångsmedel mot utlänningar som är utvisade, men vars utvisningsbeslut inte är möjliga att verkställa. Förutsättningarna för tillstånd till hemlig dataavläsning vid särskild utlänningskontroll regleras i 9 § lagen om hemlig dataavläsning. Kraven för hemlig dataavläsning motsvarar i huvudsak vad som gäller för tvångsmedelsanvändning enligt den bakomliggande lagen. Ett tillstånd till hemlig dataavläsning får därför aldrig avse rumsavlyssningsuppgifter. Genom en lagändring den 1 juli 2022 togs den tidigare begränsningen att hemlig dataavläsning vid särskild utlänningskontroll inte får avse kameraövervakningsuppgifter bort. Begränsningen togs bort till följd av att det i den nya LSU samtidigt infördes en ny möjlighet till hemlig kameraövervakning. Samtidigt ändrades hänvisningen i 9 § fjärde stycket lagen om hemlig dataavläsning. Ändringen gjordes till följd av att lagen (2013:148) om straff för terroristbrott upphävdes och ersattes av en ny terroristbrottslag (2022:666). Den nya terroristbrottslagen har ett delvis annat innehåll jämfört med tidigare

lagstiftning, vilket innebär att tillämpningsområdet för hemlig dataavläsning enligt 9 § förändrades i motsvarande mån. Platskravet och huvudregeln på koppling mellan enskild och informationssystem är detsamma som i förundersökningsfallen. Ett tillstånd får beviljas endast om det finns ”synnerliga skäl” och det är av betydelse för att klarlägga om utlänningen tillhör eller verkar för en organisation eller grupp som planlägger eller förbereder brott enligt terroristbrottslagen, eller om det finns risk för att utlänningen kan komma att engagera sig i en sådan organisation eller grupp, det finns risk för att utlänningen själv planlägger eller förbereder sådant brott eller det finns risk för att utlänningen, själv eller tillsammans med andra, medverkar i eller på annat sätt främjar ett allvarligt brott som rör Sveriges säkerhet. Kravet på synnerliga skäl motsvarar det generella kravet på synnerlig vikt.

Inhämtningslagsfallen

Med inhämtningslagen avses lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet. I inhämtningslagen regleras vilka uppgifter som de brottsbekämpande myndigheterna får hämta in från teleoperatörer utanför en förundersökning. Kraven för att använda hemlig dataavläsning i inhämtningslagsfallen regleras i 10 § lagen om hemlig dataavläsning. Kraven motsvarar i huvudsak kraven för tillstånd för tvångsmedelsanvändning enligt inhämtningslagen. Tillståndet får därför endast avse historiska kommunikationsövervaknings- och platsuppgifter och endast tillåtas för att förebygga, förhindra eller upptäcka viss allvarlig och samhällsfarlig brottslighet som räknas upp i 2 § inhämtningslagen. Det ställs inte upp något krav på koppling mellan en enskild och informationssystemet i inhämtningslagsfallen. En skillnad är att det för tillstånd om hemlig dataavläsning krävs att åtgärden ska vara av ”synnerlig vikt”, vilket är ett högre krav än det som gäller för annan tvångsmedelsanvändning enligt inhämtningslagen.

3.2.10 Förbud och tillträdestillstånd

Förbud mot hemlig dataavläsning i vissa fall

I 11 § lagen om hemlig dataavläsning stadgas förbud mot hemlig dataavläsning i vissa fall. Förbudet omfattar dels verksamheter där tystnadsplikt gäller enligt bestämmelser i tryckfrihetsförordningen och yttrandefrihetsgrundlagen, dels verksamheter som bedrivs av vissa särskilt utpekade yrkeskategorier som omfattas av tystnadsplikt, däribland advokater, viss sjukvårdspersonal och präster. Förbudet är utformat med regeln om förbud mot hemlig rumsavlyssning beträffande vissa platser som förebild, jfr 27 kap. 22 a § första stycket rättegångsbalken.

Bestämmelsen i 11 § lagen om hemlig dataavläsning kompletteras av 27 § andra och tredje stycket samma lag. Bestämmelsen i 27 § knyter an till bestämmelserna i 36 kap. 5 § rättegångsbalken. I 27 § första stycket stadgas inledningsvis att hemlig dataavläsning beträffande uppgiftstyperna i 2 § första stycket 6 och 7 inte får avse uppgifter som omfattas av det s.k. beslagsförbudet i 27 kap. 2 § rättegångsbalken. Enligt 27 § andra stycket får hemlig dataavläsning som gäller kommunikationsavlyssnings- eller rumsavlyssningsuppgifter inte avse uppgifter som omfattas av det s.k. avlyssningsförbudet. Om det vid verkställighet av hemlig dataavläsning framkommer uppgifter som omfattas av något av förbuden, ska verkställigheten omedelbart avbrytas. De upptagningar och uppteckningar som omfattas av förbud ska omedelbart förstöras. Förbudet i dessa delar motsvarar vad som gäller enligt det s.k. avlyssningsförbudet i 27 kap. 22 § rättegångsbalken och 11 § preventivlagen.

Tillträdestillstånd

Enligt 12 § lagen om hemlig dataavläsning får den verkställande myndigheten ansöka om tillstånd för att i hemlighet skaffa sig tillträde till och installera tekniska hjälpmedel på en plats som annars är skyddad mot intrång (t.ex. enligt bestämmelsen om hemfridsbrott i 4 kap. 6 § brottsbalken). Regleringen har utformats med 27 kap. 25 a § rättegångsbalken som förebild, en bestämmelse som reglerar tillträdestillstånd vid hemlig kameraövervakning eller hemlig rumsavlyssning. Det råder dock inte fullständig överensstämmelse mellan bestämmelserna.

Det krävs t.ex. enligt 12 § lagen om hemlig dataavläsning att det finns särskild anledning att anta att det avläsningsbara informationssystemet finns tillgängligt på den plats som tillträdestillståndet avser. Med uttrycket avses att det ska finnas någon faktisk omständighet som med viss styrka talar för att informationssystemet ska finnas på platsen. Tillståndet får inte vara generellt utformat utan ska avse en viss bestämd plats. Om platsen är en bostad som stadigvarande används av någon annan än den misstänkte eller motsvarande person får tillståndet beviljas endast om det finns ”synnerlig anledning” att anta att informationssystemet finns där. Uttrycket innebär att man ska vara praktiskt taget säker på att informationssystemet finns på platsen (se a. prop. s. 144 f. och 227 f.). Enligt 13 § lagen om hemlig dataavläsning får ett tillträdestillstånd aldrig avse en plats som är fredad genom förbudet mot hemlig dataavläsning enligt 11 §. Förbudet överensstämmer med vad som stadgas i 27 kap. 22 a § första stycket rättegångsbalken.

3.2.11 Tillståndsprövningen

Domstolsprövning

Som huvudregel meddelas beslut om hemlig dataavläsning av rätten, på ansökan av åklagare. En ansökan om hemlig dataavläsning vid särskild utlänningskontroll ska dock göras av Säkerhetspolisen, se 14 § lagen om hemlig dataavläsning. Ordningen är alltså densamma som för övriga tvångsmedel, med det undantaget att rätten fattar beslut om hemlig dataavläsning även i inhämtningslagsfallen. Åklagare kan i undantagsfall fatta interimistiskt beslut om hemlig dataavläsning. Sådana beslut ska enligt 17 § andra stycket prövas skyndsamt av rätten. Av 19 § framgår att rättegångsbalkens forumregler för tvångsmedel i brottmål gäller även hemlig dataavläsning under en förundersökning. I preventivlagsfallen prövas frågor om hemlig dataavläsning av den tingsrätt som är behörig enligt 6 § preventivlagen. Frågor om hemlig dataavläsning vid särskild utlänningskontroll och i inhämtningslagsfallen prövas av Stockholms tingsrätt. Detta motsvarar vad som gäller enligt 5 kap. 11 § lagen om särskild kontroll av vissa utlänningar.

Offentligt ombud, sammanträde och förfarandet

När ansökan eller anmälan om hemlig dataavläsning kommit in till rätten, ska rätten så snart som möjligt utse ett offentligt ombud i ärendet och hålla ett sammanträde. Detta framgår av 16 § första stycket lagen om hemlig dataavläsning. Regleringen innebär ett ovillkorligt krav på att ett offentligt ombud ska närvara vid domstolsprövningen i ärenden om hemlig dataavläsning. Bestämmelsen avviker i detta avseende i viss mån från andra hemliga tvångsmedel. Även den som ansökt om hemlig dataavläsning ska närvara vid sammanträdet. Genom hänvisningar i paragrafens andra stycke gäller rättegångsbalkens regler om offentliga ombud. På själva förfarandet tillämpas enligt 19 § i huvudsak reglerna i rättegångsbalken om handläggning vid domstol av frågor om tvångsmedel i brottmål och om överklagande av beslut i sådana frågor, om inte något annat anges i lagen. Det förenklade förfarande som enligt 27 kap. 28 a § rättegångsbalken gäller vid prövning av frågor om hemlig avlyssning av elektronisk kommunikation är dock inte tillämpligt vid hemlig dataavläsning. Handläggningen av ärenden om hemlig dataavläsning ska ske skyndsamt, vilket överensstämmer med regleringen för övriga hemliga tvångsmedel.

Interimistiska beslut

Enligt 17 § lagen om hemlig dataavläsning har åklagaren vissa möjligheter att bevilja interimistiska beslut om hemlig dataavläsning. Förutsättningarna för detta är desamma som gäller för andra interimistiska beslut om hemliga tvångsmedel, se 27 kap. 21 a § rättegångsbalken och 6 a § preventivlagen. Interimistiska beslut får beviljas under en förundersökning för alla uppgiftstyper. Utanför en förundersökning får interimistiska beslut beviljas i preventivlagsfallen och inhämtningslagsfallen för alla uppgiftstyper undantaget rumsavlyssningsuppgifter. Om rätten vid sin prövning av det interimistiska beslutet finner att det saknats skäl för tillstånd, får uppgifterna inte användas i en brottsutredning till nackdel för den som omfattats av åtgärden, eller för någon annan som uppgifterna avser. Uppgifterna kan dock användas såväl till någons fördel som i underrättelseverksamhet.

Beslutet

Av 18 § första stycket lagen om hemlig dataavläsning framgår vad som ska anges i ett tillstånd till hemlig dataavläsning. Bestämmelsen är tillämplig på både rättens och åklagarens beslut. Uppräkningen motsvarar i princip rättegångsbalkens krav på vad ett beslut om hemligt tvångsmedel ska innehålla:

1. vilken tid tillståndet avser,
2. vilket avläsningsbart informationssystem tillståndet avser,
3. vilken typ av uppgift enligt 2 § första stycket som får läsas av eller tas upp,
4. villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan, och
5. vem som är skäligen misstänkt för brottet eller brotten, vid åtgärd som gäller rumsavlyssningsuppgifter.

Tiden för tillståndet enligt *punkt 1* får inte bestämmas längre än nödvändigt. När det gäller tid som infaller efter beslutet får tiden inte överstiga en månad från dagen för beslutet, se 18 § fjärde stycket. Det finns dock ingen lagstadgad bortre tidsgräns för tiden innan beslutet beviljades. Vid tillståndsgivningen bör rätten dock, bl.a. med beaktande av proportionalitetsprincipen, begränsa de uppgifter som får tas upp. Detta kan få betydelse t.ex. beträffande lagrade uppgifter och historiska uppgifter om meddelanden.

Enligt *punkt 2* måste uppgifterna om informationssystemet vara så specificerade att det går att verkställa åtgärden och förhindra förväxlingsrisk samt i förekommande fall bedöma kopplingen mellan det avläsningsbara informationssystemet och den som åtgärden avser. Vidare ska det av tillståndet framgå vad själva åtgärden får användas för.

Av *punkt 3* framgår att krävs uttryckligt tillstånd för var och en av uppgiftstyperna i 2 § första stycket. Det får stor betydelse för såväl anpassningar av verkställighetstekniken som för vilka uppgifter som kan komma att betraktas som otillåten tilläggsinformation enligt 23 §.

Kravet i *punkt 4* avviker från rättegångsbalkens reglering om hemliga tvångsmedel, där villkor som huvudregel endast ska anges när det finns skäl till det, se 27 kap. 21 § sjätte stycket rättegångsbalken. Syftet

med villkorskravet är att begränsa integritetsintrånget. Om en ansökan om hemlig dataavläsning som gäller kameraövervakningsuppgifter eller rumsavlyssningsuppgifter avser den skäligen misstänkte i stället för en viss plats, ska åklagaren i samband med ansökan till rätten föreslå sådana villkor. Detta framgår av 14 § andra stycket lagen om hemlig dataavläsning.

Vad som stadgas i *punkt 5* motsvarar vad som gäller enligt 27 kap. 21 § femte stycket rättegångsbalken vid tillstånd till hemlig rumsavlyssning.

I 18 § andra stycket lagen om hemlig dataavläsning stadgas att om tillståndet avser en plats enligt 4 a § tredje stycket, 6 § tredje stycket eller 7 § tredje stycket ska även platsen anges i tillståndet. Om tillståndet är förenat med ett tillträdestillstånd ska det anges i beslutet. Av 18 § tredje stycket framgår att om tillståndet avser den skäligen misstänkte enligt 4 a § fjärde stycket eller 6 § fjärde stycket, ska det anges i beslutet. Kraven på vad ett tillstånd till hemlig dataavläsning ska innehålla motsvarar i huvudsak vad som gäller för bakomliggande tvångsmedel och ska tillämpas på motsvarande sätt, se 27 kap. 21 § rättegångsbalken och 8 § preventivlagen. Den närmare innebörden av 18 § utvecklas i prop. 2019/20:64 s. 154 ff. och 232 ff. samt i prop. 2022/23:126 s. 245.

Överklagande och sekretess

Rättens beslut utgör ett slutligt beslut som kan överklagas. Även åklagarens beslut kan överklagas, jfr 19 § lagen om hemlig dataavläsning. Ärenden om hemlig dataavläsning omfattas av sekretess. Det innebär t.ex. att rättens beslut om hemlig dataavläsning får sekretessbeläggas, vilket också görs regelmässigt. I avsnitt 3.3.1 redogörs kort för tillämpliga sekretessbestämmelser.

3.2.12 Verkställigheten

Tillåtna tekniska metoder

Ett beslut i frågor om hemlig dataavläsning får enligt 20 § lagen om hemlig dataavläsning verkställas omedelbart, vilket motsvarar vad som gäller för andra hemliga tvångsmedel. Enligt 22 § får de verkställande

myndigheterna använda de tekniska hjälpmedel som behövs för avläsningen och upptagningen. Om det är nödvändigt får systemskydd brytas eller kringgås och tekniska sårbarheter utnyttjas. Med tekniska hjälpmedel avses både hårdvara och mjukvara. Bestämmelsen är utformad på ett teknikneutralt sätt. Gränsen för vilken verkställighetsmetod som kan tillåtas avgörs i övrigt av bestämmelserna om teknikanpassning och otillåten tilläggsinformation i 23 §, aktsamhetskravet i 25 §, rättens tillståndsbeslut enligt 18 § samt proportionalitetsprincipen i 3 §.

Teknikanpassning och otillåten tilläggsinformation

Enligt 23 § lagen om hemlig dataavläsning ska den teknik som används i samband med hemlig dataavläsning anpassas efter det tillstånd som beviljats. Tekniken får alltså inte göra det möjligt att läsa av eller ta upp andra uppgiftstyper än vad som anges i tillståndet. Sådana uppgifter är att anse som s.k. otillåten tilläggsinformation. Upptagningar och uppteckningar av otillåten tilläggsinformation ska omedelbart förstöras. Otillåten tilläggsinformation får inte användas i en brottsutredning till nackdel för den som har omfattats av åtgärden eller för någon annan som uppgifterna avser. Bestämmelsen motsvarar det som gäller enligt 17 § tredje stycket när hemlig dataavläsning verkställts efter ett interimistiskt beslut från åklagare som rätten sedan anser inte borde ha beviljats.

Särskilt om hindrande av meddelanden

Vid verkställigheten får meddelanden, under förutsättning att tillståndet avser kommunikationsavlyssnings- eller kommunikationsövervakningsuppgifter, hindras från att nå fram. Detta framgår av 2 § andra stycket lagen om hemlig dataavläsning, jfr 27 kap. 19 § andra stycket rättegångsbalken. Något särskilt tillstånd från rätten krävs alltså inte i detta avseende. Åtgärden är dock inte tillåten i inhämtningslagsfallen, se 10 § andra stycket lagen om hemlig dataavläsning.

Operatörernas medverkansskyldighet och tystnadsplikt

Enligt 24 § lagen om hemlig dataavläsning är operatörer skyldiga att på begäran av den verkställande myndigheten medverka i samband med verkställighet av hemlig dataavläsning. Skyldigheten att medverka gäller för den som bedriver anmälningspliktig verksamhet enligt 2 kap. 1 § lagen (2022:482) om elektronisk kommunikation. Den omfattar bl.a. operatörer av mobiltelefoni och internet. Den som medverkar har rätt till ersättning av den verkställande myndigheten för vissa kostnader som uppstår. Närmare om vad medverkan kan avse och föreskrifter om ersättning framgår av 3 och 4 §§ förordningen om hemlig dataavläsning.

En särskild regel om operatörernas tystnadsplikt vid medverkan finns i 32 § lagen om hemlig dataavläsning. Den är utformad med nuvarande 9 kap. 31 § lagen om elektronisk kommunikation som förebild. Innebörden av bestämmelsen är att den operatör som har fått del av eller tillgång till uppgifter som hänför sig till användning av hemlig dataavläsning inte obehörigen får föra vidare eller utnyttja det han eller hon fått del av eller tillgång till.

Aktsamhetskravet

Eftersom verkställighet av hemlig dataavläsning innebär intrång i ett informationssystem finns det ett aktsamhetskrav i lagens 25 §. När ett beslut om hemlig dataavläsning verkställs får någon olägenhet eller skada inte förorsakas utöver vad som är absolut nödvändigt. Bestämmelsen är utformad efter vissa förebilder i rättegångsbalken, se 27 kap. 25 a § femte stycket och 28 kap. 6 § första stycket rättegångsbalken. Vidare stadgas att informationssäkerheten i andra avläsningsbara informationssystem än det tillståndet avser inte får åsidosättas, försämras eller skadas till följd av verkställigheten. När verkställigheten av hemlig dataavläsning avslutas ska informationssystemet inte lämnas i sämre skick än när verkställigheten påbörjades. Vidare ska ett tekniskt hjälpmedel som har använts tas bort, avinstalleras eller annars göras obrukbart så snart det kan ske efter att tiden för tillståndet har gått ut eller tillståndet upphävts.

I 26 § lagen om hemlig dataavläsning stadgas att personer som får verkställa hemlig dataavläsning ska vara särskilt lämpade för uppdraget och ha särskilda kunskaper om informationssäkerhet samt den sär-

skilda kompetens, utbildning och erfarenhet som i övrigt är nödvändig. Den verkställande myndigheten ansvarar för att dessa krav uppfylls.

Överskottsinformation, granskning, bevarande och förstöring samt underrättelse till enskilda

I 28 § första stycket lagen om hemlig dataavläsning behandlas frågor om överskottsinformation samt granskning, bevarande och förstöring av information som samlats in med stöd av hemlig dataavläsning under förundersökning. Genom hänvisningar motsvarar bestämmelsen vad som i dessa avseenden gällde för hemlig avlyssning av elektronisk kommunikation respektive hemlig rumsavlyssning enligt 27 kap. rättegångsbalken fram till den 1 oktober 2023.

Om hemlig dataavläsning har använts i preventivlagsfallen gäller på motsvarande sätt vad som i dessa avseenden gällde för hemliga tvångsmedel enligt 12–13 §§ preventivlagen fram till den 1 oktober 2023. Detta framgår av 29 § första stycket lagen om hemlig dataavläsning. Motiven bakom de nyligen justerade bestämmelserna i 28–29 §§ lagen om hemlig dataavläsning framgår av prop. 2022/23:126 s. 246 f. När det gäller hemlig dataavläsning vid särskild utlänningskontroll och i inhämtningslagsfallen motsvarar reglerna om överskottsinformation samt granskning, bevarande och förstöring det som gäller enligt den bakomliggande regleringen. Detta framgår genom hänvisningar i 30 och 31 §§ lagen om hemlig dataavläsning.

För underrättelse till enskild vid hemlig dataavläsning under förundersökning och i preventivlagsfallen gäller samma regler som för bakomliggande tvångsmedel. Detta framgår av 28 § andra stycket lagen om hemlig dataavläsning som hänvisar till 27 kap. 31–33 §§ rättegångsbalken respektive 29 § andra stycket lagen om hemlig dataavläsning som hänvisar till 16–18 §§ preventivlagen. Det finns inte någon underrättelseskyldighet till enskild vid hemlig dataavläsning vid särskild utlänningskontroll eller i inhämtningslagsfallen. Detta beror på att det varken i lagen om särskild kontroll av vissa utlänningar eller i inhämtningslagen finns bestämmelser om sådan underrättelseskyldighet (se prop. 2019/20:64 s. 167 ff. och 241 ff.).

3.2.13 Tillsyn och parlamentarisk kontroll

Säkerhets- och integritetsskyddsnämnden

Säkerhets- och integritetsskyddsnämnden (SIN) är en statlig myndighet som bl.a. utövar tillsyn över brottsbekämpande myndigheters användning av hemliga tvångsmedel, inklusive hemlig dataavläsning. När rätten har beslutat i frågor om hemlig dataavläsning ska den enligt 21 § lagen om hemlig dataavläsning skyndsamt underrätta SIN om beslutet. Underrättelseskyldigheten omfattar alla rättens beslut. Den omfattande underrättelseskyldigheten syftar dels till att inför den kommande utvärderingen få en överblick över beslutsprocessen och hur de brottsbekämpande myndigheterna har följt lagen, dels till att ge ett bättre underlag för en effektiv tillsyn (se prop. 2019/20:64 s. 175). Nämnden ska också underrättas om otillåten tilläggsinformation har lästs av eller tagits upp. Detta framgår av 23 § första stycket. Hur denna underrättelse ska ske regleras i 2 § förordningen om hemlig dataavläsning.

SIN lämnar årligen rapporter om sin tillsynsverksamhet (se nämndens årsredovisningar för åren 2020–2022, dnr 25-2021, 28-2022 och 20-2023). Utöver den löpande granskningen som följer av 21 och 23 §§ lagen om hemlig dataavläsning, har SIN genomfört ett antal särskilda granskningar av användningen av hemlig dataavläsning. SIN:s första granskning avsåg ett antal tillstånd till hemlig dataavläsning som hade meddelats under år 2020 (se nämndens uttalande med beslut av den 15 december 2021, dnr 92-2020). Nämnden fann vid den granskningen inte tillräckliga skäl att ifrågasätta de bedömningar som gjorts i de granskade ärendena, men noterade ett antal frågeställningar. Dessa gällde huvudsakligen långa tidsperioder, differentiering av uppgiftstyper, avsaknaden av villkor enligt 18 § första stycket 4 samt huruvida 2 § första stycket 7 medger inhämtning av enbart realtidsuppgifter eller också historiska uppgifter. I våra överväganden kapitel redogör vi närmare för SIN:s tillsyn beträffande användningen av hemliga tvångsmedel i allmänhet och hemlig dataavläsning i synnerhet.

Parlamentarisk kontroll

Regeringen lämnar årligen en skrivelse om användningen av hemliga tvångsmedel till riksdagen. Skrivelsen baseras på den redovisning som Åklagarmyndigheten varje år sammanställer tillsammans med Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen och Tullverket. Den parlamentariska granskningen omfattar även lagen om hemlig dataavläsning. Redovisningen innehåller bl.a. uppgifter om antalet meddelade tillstånd, hur många personer som varit föremål för åtgärderna och om uppgifterna som kommit fram gjort nytta. Den parlamentariska kontrollen av hemlig dataavläsning är avsedd att vid sidan av andra rättssäkerhetsgarantier, som t.ex. domstolsprövningen och olika materiella begränsningar av tillämpningsområdet, fylla en viktig funktion och bidra till allmänhetens insyn i myndigheternas tvångsmedelsanvändning. Granskningen är även avsedd att bidra till att det finns tillgång till nödvändiga data för utvärderingen av lagen inför ställningstagande om den ska permanentas (se prop. 2019/20:64 s. 173).

De brottsbekämpande myndigheterna har haft tillgång till hemlig dataavläsning sedan den 1 april 2020. Av den redovisning som hittills har presenterats framgår sammanfattningsvis att hemlig dataavläsning har kommit till användning i väsentligt större omfattning än vad som förutsetts, men att de brottsbekämpande myndigheterna upplever nyttan något lägre jämfört med övriga hemliga tvångsmedel (se Åklagarmyndighetens redovisningar över användningen av vissa hemliga tvångsmedel under 2020–2022). Regeringen har vid sina sammanfattande bedömningar kommit till slutsatsen att myndigheternas användning av hemlig dataavläsning har varit ett ändamålsenligt och nödvändigt instrument i brottsbekämpningen (se skr. 2021/22:79 och 2022/23:30). I kapitel 6 redogörs mer ingående för de brottsbekämpande myndigheternas redovisningar och för regeringens bedömningar av användningen av hemlig dataavläsning.

3.3 Lagstiftning och lagstiftningsarbete av betydelse

3.3.1 Annan relevant lagstiftning

I samband med att lagen om hemlig dataavläsning infördes trädde ett antal följdändringar om hemlig dataavläsning i annan lagstiftning i kraft. Av relevans i nu aktuellt avseende är lagen (2000:562) om internationell rättslig hjälp i brottmål och lagen (2017:1000) om en europeisk arresteringsorder som båda omfattas av hemlig dataavläsning. Vidare omfattas hemlig dataavläsning indirekt av de generella bestämmelserna om hemliga tvångsmedel i offentlighets- och sekretesslagen (OSL) samt uttryckligen av de specifika bestämmelserna i 18 kap. 19 § och 44 kap. 5 § OSL (se prop. 2019/20:64 s. 182 ff. och 253 f.). Behandlingen av personuppgifter vid användning av hemliga dataavläsning regleras huvudsakligen i brottsdatalagen (2018:1177). Lagen är subsidiär i förhållande till annan lag eller förordning. De brottsbekämpande myndigheterna har härutöver särskilda registerförfattningar som innehåller regler till skydd för den personliga integriteten när personuppgifter behandlas i den brottsbekämpande verksamheten och när de överförs till annan verksamhet.

3.3.2 Betydelsen av straffskärpningar och andra lagändringar

Tillämpningsområdet för hemlig dataavläsning under förundersökning är som utgångspunkt knutet till straffskalans nedre gräns, på det sätt att minst två års fängelse måste vara föreskrivet för det aktuella brottet för att åtgärden ska få användas. Metoden för att bestämma tillämpningsområdet kombineras av både brottskataloger och straffvärdeventiler. Straffskärpningar på straffrättens område kan därför innebära en utvidgning av tillämpningsområdet för hemlig dataavläsning. Sedan lagen om hemlig dataavläsning trädde i kraft har t.ex. skärpta straff för vapen- och sprängmedelsbrott införts, se *En strängare syn på hantering av vapen och explosiva varor*, prop. 2019/20:200. Lagändringarna, som trädde i kraft den 1 december 2020, innebär bl.a. att fler vapenbrott bedöms som grova och synnerligen grova samt att vapensmuggling och att smuggling av explosiva varor har införts som egna brott. Minimistraffet för brotten grov smuggling av vapen respektive explosiva varor innebär att det avseende dessa brott är möjligt att använda hemlig dataavläsning, med undantag för rumsavlyss-

ningsuppgifter, under en förundersökning samt i inhämtningslagsfallen. Minimistraffet för de synnerligen grova smugglingsbrotten av vapen och explosiva varor innebär vidare att det för dessa brott är möjligt att använda hemlig dataavläsning även avseende rumsavlyssningsuppgifter. En närmare genomgång av de straffskärpningar som i övrigt har skett sedan lagen om hemlig dataavläsning trädde i kraft och hur dessa kan påverka tillämpningsområdet för hemlig dataavläsning framgår av betänkandet *Utökade möjligheter att använda hemliga tvångsmedel*, SOU 2022:19, s. 101 ff.

Tillämpningsområdet för hemlig dataavläsning utanför en förundersökning är genom olika hänvisningar i 7–10 §§ lagen om hemlig dataavläsning knuten till annan lagstiftning. Lagändringar som sker i preventivlagen, lagen om särskild kontroll av vissa utlänningar, terroristbrottslagen och inhämtningslagen kan därför komma att påverka också tillämpningsområdet för hemlig dataavläsning. Exempelvis fick det nya dokumentationskravet i 27 kap. 35 § rättegångsbalken genomslag även för hemlig dataavläsning vid särskild utlänningskontroll. Detta framgår av hänvisningen i 9 § tredje stycket lagen om hemlig dataavläsning till 5 kap. 5 och 6 §§ lagen om särskild kontroll av vissa utlänningar (se avsnitt 8.5.5).

3.3.3 Lagstiftningsarbete som berör lagen om hemlig dataavläsning

Inom Regeringskansliet har pågått och pågår lagstiftningsarbete som på olika sätt berör hemlig dataavläsning och därmed har betydelse för detta betänkande. Arbete som har publicerats efter utgången av oktober 2023 har inte kunnat beaktas.

Rättssäkerhetsgarantier och hemliga tvångsmedel

Utredningen om rättssäkerhetsgarantier vid användningen av vissa hemliga tvångsmedel har bl.a. haft i uppdrag se över hur rättssäkerhetsgarantierna och mekanismerna som ska skydda den personliga integriteten när hemliga tvångsmedel för särskilt allvarlig eller på annat sätt samhällsfarlig brottslighet används (se dir. 2017:16). Utredningen överlämnande i augusti 2018 sitt slutbetänkande *Rättssäkerhetsgarantier och hemliga tvångsmedel,* SOU 2018:61. I betänkandet föreslogs

att bestämmelserna om s.k. överskottsinformation i rättegångsbalken och preventivlagen skulle förändras. Utredningen föreslog också en förändring av bestämmelsen i rättegångsbalken om när upptagningar och uppteckningar från hemliga tvångsmedel ska bevaras och förstöras. Vidare föreslogs att det skulle införas en lagstadgad dokumentationsplikt i såväl rättegångsbalken som preventivlagen. Utredningens analyser och förslag godtogs med vissa lagtekniska justeringar i det fortsatta lagstiftningsarbetet. Lagändringar i dessa avseenden trädde i kraft den 1 oktober 2023, se propositionen *Hemliga tvångsmedel – effektiva verktyg för att förhindra och utreda allvarliga brott*, 2022/23:126. Ändringarna omfattar inte hemlig dataavläsning eftersom lagen om hemlig dataavläsning trädde i kraft efter att Utredningen om rättssäkerhetsgarantier vid användningen av vissa hemliga tvångsmedel redovisat sitt uppdrag. Det dokumentationskrav som infördes i rättegångsbalken fick dock genomslag för hemlig dataavläsning vid särskild utlänningskontroll. Utredningens lagförslag och nyligen ikraftträdda lagändringar i relevanta delar redogörs närmare för i kapitel 8.

Utökade möjligheter att använda hemliga tvångsmedel

Utredningen om utökade möjligheter att använda hemliga tvångsmedel har haft i uppdrag att se över delar av regleringen om hemliga tvångsmedel (se dir. 2020:104). Syftet med översynen har varit att ta ställning till hur hemliga tvångsmedel ska kunna användas i en större utsträckning för att bekämpa allvarlig brottslighet. Utredningen har även haft att bedöma behovet av följdändringar i bl.a. lagen om hemlig dataavläsning. I tilläggsdirektiv utvidgades uppdraget till att även omfatta vissa frågor om underrättelse till enskilda samt frågan om hemliga tvångsmedel bör få användas för att lokalisera vissa anhållna eller dömda personer (se dir. 2022:13). Utredningen lämnade i april 2022 sitt delbetänkande *Utökade möjligheter att använda hemliga tvångsmedel*, SOU 2022:19. I delbetänkandet föreslogs bl.a. en rad ändringar i rättegångsbalken beträffande hemliga tvångsmedel. I konsekvens härmed föreslogs även följdändringar i lagen om hemlig dataavläsning. Utredningens analyser och förslag godtogs med vissa lagtekniska justeringar i det fortsatta lagstiftningsarbetet. Lagändringarna trädde i kraft den 1 oktober 2023, se *Hemliga tvångsmedel – effektiva verktyg för att förhindra och utreda allvarliga brott*, prop. 2022/23:126. För lagen

om hemlig dataavläsning innebar lagändringarna huvudsakligen följande.

- En utvidgning av brottskatalogen och en ny straffvärdeventil för viss flerfaldig brottslighet (4 §).
- En ny möjlighet att inhämta uppgifter om meddelanden i realtid (5 § första stycket).
- Utökade möjligheter att utreda vem som skäligen kan misstänkas (4 b §).
- Nya möjligheter att knyta åtgärder till en skäligen misstänkt person i stället för en viss plats (4 a § fjärde stycket, 6 § fjärde stycket, 14 § andra stycket och 18 § tredje stycket).
- En utvidgad möjlighet till interimistiska åklagarbeslut (17 §).

Utredningen slutredovisade sitt uppdrag i oktober 2022, i slutbetänkandet *Bättre möjligheter att verkställa frihetsberövanden*, SOU 2022:50. I slutbetänkandet föreslås att det i 27 kap. rättegångsbalken ska införas en möjlighet att under vissa närmare förutsättningar använda hemlig övervakning av elektronisk kommunikation i syfte att eftersöka någon som är anhållen eller häktad. I konsekvens härmed föreslås att det i lagen om hemlig dataavläsning ska införas en möjlighet att under vissa närmare förutsättningar och i samma syfte använda hemlig dataavläsning som gäller kommunikationsövervaknings- och platsuppgifter. Vidare föreslås att det ska införas en ny lag med tillhörande förordning med bestämmelser som möjliggör användning av hemlig övervakning av elektronisk kommunikation och hemlig dataavläsning som gäller plats- och kommunikationsövervakningsuppgifter i syfte att lokalisera dömda personer som håller sig undan från en frihetsberövande påföljd. Härutöver föreslås ett antal ändringar i rättegångsbalkens regler om underrättelse till enskilda. Ändringsförslagen omfattar även vad som gäller om underrättelse till enskilda vid hemlig dataavläsning, eftersom 28 § andra stycket lagen om hemlig dataavläsning hänvisar till rättegångsbalkens regler härom. Betänkandet har remissbehandlats och bereds för närvarande i Regeringskansliet. Utredningens lagförslag och nyligen ikraftträdda lagändringar i relevanta delar redogörs närmare för i kapitel 7 och 8.

Utredningen om preventiva tvångsmedel

Utredningen om preventiva tvångsmedel har haft i uppdrag att överväga flera frågor kopplade till möjligheterna att använda hemliga tvångsmedel i preventivt syfte utanför en förundersökning (se dir. 2021:102, 2021:113, 2022:32, 2022:104 och 2023:9). Uppdraget har bl.a. innefattat att överväga om tillämpningsområdet för hemlig dataavläsning utanför en förundersökning ska utvidgas. Utredningen har även haft att bedöma behovet av följdändringar i bl.a. lagen om hemlig dataavläsning. Uppdraget delredovisades den 24 oktober 2022, i delbetänkandet *Utökade möjligheter att använda preventiva tvångsmedel*, SOU 2022:52. I delbetänkandet föreslogs en utökning av preventivlagens tillämpningsområde till att omfatta även viss särskilt allvarlig brottslig verksamhet som utövas inom en organisation eller grupp. I konsekvens härmed föreslogs även vissa följdändringar i lagen om hemlig dataavläsning. Utredningens analyser och förslag godtogs med vissa lagtekniska justeringar i det fortsatta lagstiftningsarbetet. Lagändringarna trädde i kraft den 1 oktober 2023, se *Hemliga tvångsmedel – effektiva verktyg för att förhindra och utreda allvarliga brott*, prop. 2022/23:126.

Uppdraget slutredovisades den 12 oktober 2023, i slutbetänkandet *Utökade möjligheter att använda preventiva tvångsmedel 2*, SOU 2023:60. Betänkandet är för närvarande under beredning. Utredningens lagförslag och nyligen ikraftträdda lagändringar i relevanta delar redogörs närmare för i kapitel 7 och 8.

Datalagringsutredningen

2021 års datalagringsutredning har haft i uppdrag att se över den lagstiftning som medför en skyldighet för tillhandahållare av elektroniska kommunikationstjänster att lagra uppgifter om elektronisk kommunikation för brottsbekämpande syften m.m. (se dir. 2021:58 och 2023:2). I uppdraget har bl.a. ingått att göra en översyn av frågorna om territorialitet och jurisdiktion på området. Datalagringsutredningens uppdrag redovisades den 30 maj 2023, i betänkandet *Datalagring och åtkomst till elektronisk information*, SOU 2023:22. Utredningens förslag berör hemlig dataavläsning i flera avseenden. Enligt utredningens förslag ska det införas ny lag om lagring av uppgifter om elektronisk kommunikation i syfte att bekämpa grov brottslig-

het. Enligt förslaget ska s.k. utökad riktad lagring bl.a. kunna avse en person som är eller har varit föremål för hemliga tvångsmedel, hemlig dataavläsning inkluderat. Vidare föreslår utredningen en anpassningsskyldighet för tillhandahållare av s.k. Noik (nummeroberoende interpersonella kommunikationstjänster) så att beslut om hemlig avlyssning och hemlig övervakning av elektronisk kommunikation samt inhämtning enligt inhämtningslagen kan verkställas mot sådana tillhandahållare. Förslaget bedöms påverka hemlig dataavläsning indirekt på så sätt att beslut om hemlig dataavläsning i viss mån kan komma att ersättas med nyssnämnda, i regel mindre ingripande, hemliga tvångsmedel. Utredningen föreslår också en lagreglering som förtydligar vad som gäller för viss inhämtning av elektronisk information som lagras utanför Sverige (s.k. exekutiv jurisdiktion). De straffprocessuella tvångsmedel som den föreslagna lagen bedöms tillämplig på är hemlig dataavläsning och genomsökning på distans. Betänkandet bereds för närvarande i Regeringskansliet. Utredningens överväganden och lagförslag i relevanta delar redogörs närmare för i avsnitt 4.2.3 och 10.2.3.

4 Hur förhåller sig hemlig dataavläsning till andra tvångsmedel?

4.1 Allmänt om straffprocessuella tvångsmedel

4.1.1 Inledning

I kapitel 3 har vi redogjort för att hemlig dataavläsning är ett självständigt hemligt tvångsmedel som under vissa förutsättningar kan användas av de brottsbekämpande myndigheterna både under och utanför en förundersökning. Hemlig dataavläsning kan bl.a. användas för att verkställa flera andra olika hemliga tvångsmedel. Åtgärden utgör ett komplement till andra tvångsmedel och ska i första hand användas när andra tvångsmedel inte är framkomliga alternativ. Gränsdragningsfrågor kan därför uppkomma i förhållande till vissa andra tvångsmedel. I detta kapitel redogör vi översiktligt för systemet med straffprocessuella tvångsmedel och för vissa relevanta gränsdragningsfrågor.

4.1.2 Straffprocessuella tvångsmedel och hemliga tvångsmedel

Det finns inte någon definition av vad som är ett straffprocessuellt tvångsmedel. Med uttrycket avses emellertid åtgärder som har en funktion inom straffprocessen men som inte utgör straff eller andra sanktioner (se t.ex. *Hemliga tvångsmedel mot allvarliga brott*, prop. 2013/14:237 s. 43). I doktrin har straffprocessuella tvångsmedel beskrivits som sådana direkta ingripanden mot person eller egendom som görs i myndighetsutövning och som utgör intrång i någons rättssfär (se Lindberg, *Straffprocessuella tvångsmedel – när och hur får de användas?*, 2022, version 5, JUNO, s. 47).

Hemliga tvångsmedel intar en särställning bland de straffprocessuella tvångsmedlen genom det hemlighållande som åtgärderna kräver. Vid användning av hemliga tvångsmedel hålls den berörde alltid omedveten om åtgärderna, men det kan samtidigt antas att dessa sker mot hans eller hennes vilja. Den som har utsatts för ett hemligt tvångsmedel ska som huvudregel i efterhand underrättas om tvångsmedelsanvändningen, men det finns också undantag från underrättelseskyldigheten. De intrång i den personliga integriteten som hemliga tvångsmedel innebär medför att åtgärderna är att beteckna som tvångsmedel.

Hemlig dataavläsning är som angetts ett tidsbegränsat hemligt tvångsmedel som upphör att gälla vid utgången av mars 2025. Till de permanenta hemliga tvångsmedlen räknas hemlig avlyssning av elektronisk kommunikation (HAK), hemlig övervakning av elektronisk kommunikation (HÖK), hemlig kameraövervakning (HKÖ) och hemlig rumsavlyssning (HRA). Inhämtning enligt den s.k. inhämtningslagen, lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (IHL), är också att anse som ett hemligt tvångsmedel (se prop. 2011/12:55 s. 110 f.). Även kvarhållande och kontroll av försändelse, s.k. postkontroll, är ett hemligt tvångsmedel. Eftersom reglerna om postkontroll inte har någon omedelbar betydelse för hemlig dataavläsning behandlas åtgärden inte vidare i detta betänkande. Utmärkande för de olika hemliga tvångsmedlen är att de omgärdas av särskilda kontrollmekanismer och andra rättssäkerhetsgarantier. För hemliga tvångsmedel gäller bl.a. särskilda bestämmelser om domstolstillstånd, tillsyn och hur överskottsinformation får användas. Verkställighet av hemliga tvångsmedel sker alltid utan den berördes vetskap. Det finns även exempel på s.k. öppna straffprocessuella tvångsmedel som under vissa förutsättningar kan verkställas utan att den som är föremål för åtgärden är närvarande eller har underrättats på förhand, t.ex. beslag och husrannsakan. För dessa tvångsmedel saknas sådana bestämmelser som är utmärkande för de hemliga tvångsmedlen och som t.ex. reglerar obligatorisk domstolsprövning, tillsyn och hantering av överskottsinformation. Kvalifikationskraven för användning av öppna tvångsmedel är också generellt lägre ställda.

4.1.3 Allmänna principer för tvångsmedelsanvändning

För att beskriva hur hemlig dataavläsning förhåller sig till andra straffprocessuella tvångsmedel bör något sägas om de allmänna principer som gäller vid all tvångsmedelsanvändning, dvs. legalitetsprincipen, ändamålsprincipen, behovsprincipen och proportionalitetsprincipen. De gäller både vid beslut om och vid verkställighet av sådana åtgärder. Principerna kompletterar de enskilda bestämmelserna om straffprocessuella tvångsmedel. Det innebär i sin tur att principerna också är av betydelse när det gäller gränsdragningen mellan hemlig dataavläsning och andra tvångsmedel.

Legalitetsprincipen

Legalitetsprincipen innebär att en åtgärd måste ha stöd i lag. Användning av straffprocessuella tvångsmedel förutsätter alltså en bestämmelse i lag som medger intrång i den enskildes rättssfär. Bestämmelserna om hemlig dataavläsning utgör som alla straffprocessuella tvångsmedel lagreglerade inskränkningar i det grundläggande skydd för privatlivet och den personliga integriteten som tillförsäkras enskilda i bl.a. regeringsformen och Europakonventionen. I avsnitt 5.4 redogör vi närmare för under vilka förutsättningar sådana inskränkningar kan göras.

Ändamålsprincipen

Ändamålsprincipen innebär att en myndighets befogenhet att använda ett tvångsmedel ska vara bundet till det ändamål för vilket tvångsmedlet har beslutats. Principen kan härledas bl.a. från 2 kap. 21 § regeringsformen. Enligt denna bestämmelse får begränsningar i de grundläggande fri- och rättigheterna endast göras för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Några uttryckliga principer om ändamålen med användningen av hemlig dataavläsning och andra hemliga tvångsmedel framgår inte av lagtext. Ändamålen får i stället utläsas av de brottsbekämpande myndigheternas uppgifter och de olika regleringarnas materiella bestämmelser. I avsnitt 3.2.6 har vi redogjort för ändamålen med hemlig dataavläsning. En ändamålsprövning bör ske före behovs- och proportionali-

tetsprövningen. Om tvångsmedlet inte ska användas för det ändamål som är avsett, spelar det ingen roll om det finns ett påtagligt behov och åtgärden framstår som proportionerlig. Enligt ändamålsprincipen kan man inte heller använda ett tvångsmedel i syfte att få fram överskottsinformation (se *Rättssäkerhetsgarantier och hemliga tvångsmedel*, SOU 2018:61 s. 42).

Behovsprincipen

Enligt behovsprincipen får en myndighet använda ett tvångsmedel endast när det finns ett påtagligt behov och en mindre ingripande åtgärd inte är tillräcklig. Det är motsvarande överväganden som gör sig gällande vid proportionalitetsprövningen. Behovsprincipen innebär också att ett tvångsmedel ska upphöra så snart syftet med det har uppnåtts eller det av andra skäl inte längre finns behov av det. Ibland talar man om s.k. indikationskrav i stället för behov, dvs. krav på att den förväntade nyttan av åtgärden ska nå upp till en viss nivå. Det behovs- och indikationskrav som ställs på hemlig dataavläsning är att åtgärden ska vara av ”synnerlig vikt” eller motsvarande för ändamålet med åtgärden, se avsnitt 3.2.8 och 3.2.9. Uttrycket innefattar ett kvalitetskrav när det gäller de upplysningar som åtgärden kan ge. Vid bedömningen av om det är av synnerlig vikt att hemlig dataavläsning ska få användas i ett enskilt fall ska själva metoden för uppgiftsinhämtningen ha en framträdande plats.

Proportionalitetsprincipen

Proportionalitetsprincipen innebär i korthet att ett tvångsmedel endast får tillgripas om skälen för åtgärden – i fråga om art, styrka, räckvidd och varaktighet – står i rimlig proportion i förhållande till vad som står att vinna med åtgärden. Även om proportionalitetsprincipen gäller som en allmän princip vid all tvångsmedelsanvändning, har lagstiftaren ansett det angeläget att lagfästa principen och ge den en framträdande plats i såväl lagen om hemlig dataavläsning som i övriga tvångsmedelslagar, se avsnitt 3.2.7.

4.2 Gränsdragningen mot andra hemliga tvångsmedel

4.2.1 Permanent lagstiftning om hemliga tvångsmedel

Den permanenta lagstiftningen om användning av hemliga tvångsmedel under förundersökning finns i 27 kap. rättegångsbalken. Här finns bestämmelser om HAK, HÖK, HKÖ och HRA. Permanenta bestämmelser om användning av hemliga tvångsmedel utanför förundersökning i underrättelseverksamhet finns i lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen), lagen (2022:700) om särskild kontroll av vissa utlänningar (LSU) och lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen, IHL). De hemliga tvångsmedel som får användas enligt både preventivlagen och LSU är HAK, HÖK och HKÖ. HRA är däremot inte tillåtet. Frågan är dock för närvarande under beredning. Inhämtning med stöd av IHL motsvarar i stora delar användning av HÖK. En skillnad är att 1 § 1 IHL endast kan användas för att inhämta uppgifter i förfluten tid. Även denna fråga är emellertid under beredning (se betänkandet *Utökade möjligheter att använda preventiva tvångsmedel 2,* SOU 2023:60). De materiella förutsättningarna för att få tillstånd till de olika hemliga tvångsmedlen skiljer sig åt, beroende på vilket slags åtgärd som avses och för vilket ändamål den vidtas. En utförlig beskrivning av de permanenta hemliga tvångsmedlen och tillståndskraven för dessa återfinns i betänkandet *Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet*, SOU 2017:89 s. 76 ff. Som framgår i avsnitt 3.3 är regelverken för hemliga tvångsmedel för närvarande föremål för pågående lagstiftningsarbete.

4.2.2 Gränsdragningen mellan hemlig dataavläsning och andra hemliga tvångsmedel

Tillståndsrekvisiten för hemlig dataavläsning med stöd av 2 § första stycket 1–5 lagen om hemlig dataavläsning är huvudsakligen desamma som för bakomliggande hemliga tvångsmedel. Vissa materiella skillnader mellan hemlig dataavläsning och andra hemliga tvångsmedel ska dock framhållas. Här kan särskilt nämnas att det för hemlig data-

avläsning enligt 11 § råder förbud mot avläsning av vissa informationssystem. Vidare ställs enligt 25–26 §§ särskilda krav på den verkställande myndigheten och på upprätthållandet av informationssäkerheten eftersom hemlig dataavläsning innebär risker för informationssäkerheten. Motsvarande bestämmelser saknas för andra hemliga tvångsmedel. De flesta uppgifter som kan hämtas in med hemlig dataavläsning kan dock för samma ändamål hämtas in med andra hemliga tvångsmedel. Hemlig dataavläsning innebär i detta avseende en viss dubbelreglering (jfr *Hemlig dataavläsning,* prop. 2019/20:64 s. 93). I de flesta fall bör emellertid gränsdragningen mot andra hemliga tvångsmedel vara uppenbar, eftersom hemlig dataavläsning i första hand ska användas när andra tvångsmedel inte är framkomliga alternativ. I de fall gränsdragningsfrågor ändå uppkommer får dessa avgöras genom en behovs- och proportionalitetsprövning.

Vid behovsprövningen får metoden som angett en framträdande plats. Metoden för hemlig dataavläsning skiljer sig från verkställighet av andra hemliga tvångsmedel. Metoden ger åtkomst till inhämtade uppgifter som andra hemliga tvångsmedel inte kan fånga upp i ett läs- eller avlyssningsbart skick. Metoden ger även åtkomst till uppgifter som inte kan hämtas in med andra hemliga tvångsmedel (se avsnitt 3.2.4). Andra hemliga tvångsmedel verkställs som regel genom inhämtning av uppgifter från operatörer alternativt genom kamera- eller avlyssningsutrustning som tillhör och monteras av de brottsbekämpande myndigheterna. Vid HAK, HÖK eller inhämtning enligt IHL hämtas uppgifterna in på väg till eller från någons kommunikationsutrustning. Vid HKÖ och HRA hämtas uppgifter in genom den kamera- eller avlyssningsutrustning som placeras av de brottsbekämpande myndigheterna på en fysisk plats, efter ett särskilt tillträdestillstånd.

När hemlig dataavläsning verkställs hämtas uppgifterna in från en kommunikationsutrustning som den berörde använder eller kontaktar, t.ex. en dator eller en mobiltelefon, ett USB-minne eller en server. Hemlig dataavläsning kan alltså inte användas för att göra s.k. basstationstömningar som är vanligt förekommande vid HÖK. Vid verkställighet av hemlig dataavläsning kan det i vissa fall vara nödvändigt att komma närmare informationssystemet eller ha det i sin fysiska besittning, t.ex. om hårdvara ska användas eller om det inte är möjligt att på distans installera programvara. För att i hemlighet kunna installera sådana tekniska hjälpmedel på en fysisk plats som annars

är skyddad mot intrång krävs ett särskilt tillträdestillstånd. Tillståndet ges enligt lagen om hemlig dataavläsning endast under vissa närmare förutsättningar. Ett tillträdestillstånd får t.ex. endast avse en plats där det finns särskild anledning att anta att det avläsningsbara informationssystemet finns tillgängligt. Ett tillträdestillstånd för hemlig dataavläsning kan alltså inte användas för att montera kamera- eller avlyssningsutrustning på platsen. Regleringen om hemlig dataavläsning tar sikte på aktivering av en kamera- eller mikrofonfunktion i t.ex. en mobiltelefon och inte på montering av en fast kamera eller mikrofon (jfr a. prop. s. 145). Inte heller i övrigt kan ett beslut om hemlig dataavläsning användas för att verkställa andra hemliga tvångsmedel. Det är i praktiken visserligen vanligt förekommande att flera olika hemliga tvångsmedel används parallellt, men för var och en av åtgärderna krävs alltså särskilda beslut och i förekommande fall även särskilda tillträdestillstånd. Detta utesluter givetvis inte gemensam handläggning vid domstolen.

Proportionalitetsprincipen är lagfäst såväl i lagen om hemlig dataavläsning som i övriga tvångsmedelslagar. En avgörande skillnad är att det i lagen om hemlig dataavläsning finns ett differentieringskrav. Kravet innebär att behovet av uppgifter i varje enskilt fall ska vara styrande för vad hemlig dataavläsning får och ska kunna användas för. Att hemlig dataavläsning utgör ett komplement till andra tvångsmedel innebär bl.a. att andra tvångsmedel kan komma att användas parallellt med hemlig dataavläsning. Mot denna bakgrund bör det också vara den totala effekten av tvångsmedelsanvändningen som bedöms inom ramen för proportionalitetsprövningen (jfr Säkerhets- och integritetsskyddsnämndens uttalande med beslut av den 15 december 2021, dnr 92-2020, s. 10 f.).

Det blir alltså ytterst vid rättens, eller i förekommande fall åklagarens, tillståndsprövning i det enskilda fallet som gränsdragningen mot andra hemliga tvångsmedel görs. Eftersom behovs- och proportionalitetsprinciperna ska beaktas under hela förfarandet kan nya bedömningar göras även i tiden därefter.

4.2.3 Förslaget om en anpassningsskyldighet för tillhandahållare av Noik

Hemlig dataavläsning ska som utgångspunkt bara användas om det saknas mindre ingripande sätt att få tillgång till samma information. För närvarande är ett lagförslag om en lagstadgad anpassningsskyldighet, som bland annat innebär en skyldighet att samarbeta och anpassa verksamheten så att hemliga tvångsmedel kan verkställas, för tillhandahållare av s.k. Noik under beredning. Förslaget innebär i praktiken att viss information som tidigare var åtkomlig endast genom hemlig dataavläsning kan komma att bli åtkomlig även genom HAK, HÖK och inhämtning enligt IHL, dvs. i regel mindre ingripande hemliga tvångsmedel än hemlig dataavläsning. Förslaget är framlagt av 2021 års datalagringsutredning, i betänkandet *Datalagring och åtkomst till elektronisk information*, SOU 2023:22, s. 418 ff. Bakgrunden till lagförslaget är i korthet följande. En stor majoritet av de kommunikationstjänster som i dag används utgörs av internetbaserade s.k. OTT-tjänster (*over-the-top*, dvs. operatörsoberoende tjänster) i stället för traditionella teletjänster. OTT-tjänster finns av olika slag, och några exempel på OTT-tjänster som utgör kommunikationstjänster är Apple Imessage och Apple Facetime, Facebook Messenger, Snapchat, Google Messages, Kik Messenger, Telegram och Whatsapp. Inom den EU-rättsliga regleringen och i lagen (2022:482) om elektronisk kommunikation (LEK) används begreppet nummeroberoende interpersonella kommunikationstjänster (Noik) som ett samlingsbegrepp för de OTT-tjänster som används för interpersonell kommunikation. Tillhandahållare av Noik har i dag inte någon anpassningsskyldighet för hemliga tvångsmedel eller någon datalagringsskyldighet motsvarande den som de traditionella teleoperatörerna har. Det sker således ingen datalagring för brottsbekämpande ändamål vad gäller kommunikation genom Noik. Den ökade användningen av sådana tjänster har i sin tur inneburit försämrade möjligheter för de brottsbekämpande myndigheterna att använda HAK, HÖK och inhämtning enligt IHL. Kommunikation genom Noik är många gånger totalsträckskrypterad, vilket innebär att ingen annan än avsändare och mottagare kan få tillgång till kommunikationen i klartext. Vare sig tillhandahållaren av kommunikationstjänsten eller den som har tillstånd till HAK, HÖK eller inhämtning enligt IHL kan alltså läsa sådana meddelanden eller ibland ens trafikuppgifter i klartext. Kryp-

tering fyller en mycket viktig funktion för att skydda kommunikation i förhållande till externa aktörer, men de tekniska lösningarna får inte utformas på ett sådant sätt att de omöjliggör användningen av hemliga tvångsmedel. En sådan ordning åsidosätter det allmänna intresset i demokratiska samhällen av att kunna förebygga, förhindra, upptäcka och utreda allvarlig brottslighet. 2021 års datalagringsutredning har bl.a. mot denna bakgrund föreslagit en lagrings- och anpassningsskyldighet för tillhandahållare av Noik. Bestämmelserna föreslås införas i LEK. Förslagen innebär en skyldighet för dessa tjänsteleverantörer att lagra vissa uppgifter och att bedriva sin verksamhet så att HAK, HÖK samt inhämtning enligt IHL kan verkställas.

Företrädare för de brottsbekämpande myndigheterna har till vår utredning framhållit att förslaget om skyldigheter för tillhandahållare av Noik utgör en nödvändig anpassning till den tekniska utvecklingen och ändrade kommunikationsvanor. Kraven avseende anpassning för att hemliga tvångsmedel ska kunna verkställas bör rimligen vara samma för alla leverantörer av publikt tillgängliga kommunikationstjänster, oavsett om tjänsterna är nummerbaserade eller nummeroberoende. Vidare, om tillhandahållare av Noik omfattas av en anpassningsskyldighet vid beslut om HAK, HÖK och inhämtning enligt IHL, kommer behovet av att använda hemlig dataavläsning att minska. Hemlig dataavläsning innebär som huvudregel både större integritetsrisker och större risker för informationssäkerheten än andra hemliga tvångsmedel. Därtill kommer att HAK, HÖK och inhämtning enligt IHL generellt sett både är enklare att verkställa och mindre resurskrävande än hemlig dataavläsning. Övervägande skäl talar därmed för datalagringsutredningens förslag, även ur denna utrednings perspektiv. Samma företrädare har samtidigt understrukit att hemlig dataavläsning kommer fortsätta att vara ett oundgängligt verktyg i de brottsbekämpande myndigheternas verksamhet, oavsett om datalagringsutredningens förslag om en anpassningsskyldighet för tillhandahållare av Noik genomförs eller inte. Exempelvis kan hemlig dataavläsning, till skillnad från övriga hemliga tvångsmedel, ge tillgång till information som enbart finns lagrad på ett informationssystem och aldrig har kommunicerats genom en kommunikationstjänst. Vidare har hemlig dataavläsning även fortsatt stor betydelse i fall där kommunikation sker via tjänster som inte omfattas av den föreslagna anpassningsskyldigheten för HAK och HÖK, exempelvis för att tjänsterna inte tillhandahålls publikt.

Frågan om en anpassningsskyldighet för tillhandahållare av Noik ligger utanför vårt uppdrag. Det kan dock rent allmänt konstateras att det såväl ur ett integritets- som informationssäkerhetsperspektiv finns stora fördelar att vinna om hemlig dataavläsning i vissa fall kan ersättas med mindre ingripande hemliga tvångsmedel. Vi återkommer kort i kapitel 12 till hur förslaget kan komma att påverka användningen av hemlig dataavläsning. Här konstaterar vi också att förslaget kan komma att medföra minskade kostnader för hemlig dataavläsning.

4.3 Gränsdragningen mot vissa andra tvångsmedel

4.3.1 Beslag m.m.

Beslag är ett straffprocessuellt tvångsmedel som innebär att en brottsbekämpande myndighet tillfälligt tar hand om annans egendom. Beslag kan göras om föremålet ”skäligen kan antas” ha betydelse i vissa angivna avseenden. Beslag får under förundersökning göras för de olika ändamål som framgår av 27 kap. 1 § första stycket rättegångsbalken. I bestämmelsen gör man skillnad på 1) bevisbeslag (1 och 5 p), 2) återställandebeslag (2 p) och 3) förverkandebeslag (3 p). Sedan den 1 juni 2022 finns det ytterligare en beslagsgrund; beslag av föremål som kan användas 4) för att utföra en genomsökning på distans (4 p). I avsnitt 4.3.4 återkommer vi till det nya tvångsmedlet genomsökning på distans. En mer allmän redogörelse för bestämmelserna om beslag återfinns i SOU 2017:89 s. 95 ff. Beslagsreglerna har till viss del reviderats i samband med vissa lagändringar som trädde i kraft den 1 juni 2022, se *Modernare regler för användningen av tvångsmedel*, prop. 2021/22:119. Lagändringarna innebar även att förbudet mot att beslagta meddelanden mellan en misstänkt och en närstående avskaffades, detta fanns tidigare i 27 kap. 2 § rättegångsbalken. I 27 kap. 11 § infördes en möjlighet att i vissa fall dröja med en underrättelse till den som drabbas av beslag. Vidare infördes i 27 kap. 11 b och c §§ särskilda bestämmelser om närvaro i samband med att handlingar i en beslagtagen elektronisk kommunikationsutrustning genomsöks. I 27 kap. 17 a–e §§ infördes möjligheter att under vissa förutsättningar kopiera handlingar som omfattas av beslag. I praktiken innebär dessa bestämmelser en lagreglerad möjlighet att säkra elektroniskt lagrad information. Slutligen infördes även en skyldighet för enskilda att i

vissa fall medverka till biometrisk autentisering för att öppna en mobiltelefon eller liknande, se 27 kap. 17 f §.

Reglerna om husrannsakan och beslag har ett funktionellt samband på så sätt att en husrannsakan ofta är nödvändig för att möjliggöra ett beslag. Gränsdragningen mellan hemlig dataavläsning och husrannsakan behandlas i följande avsnitt. Vad gäller beslag i it-miljöer bör redan här nämnas att det inte är tillåtet att använda beslag för att få fram information som kan hämtas in genom hemliga tvångsmedel på teleområdet (jfr t.ex. *Hemliga tvångsmedel – offentliga ombud och en mer ändamålsenlig reglering*, prop. 2002/03:74 s. 45 f.). En operatör kan t.ex. ha uppgifter om elektroniska meddelanden och om innehållet i sådana meddelanden lagrade, antingen elektroniskt eller i pappersform. Det anses då strida mot allmänna principer att använda beslag som ett substitut för att få tillgång till sådana uppgifter. Samma förbud gäller beträffande edition och husrannsakan. Reglerna om HAK, HÖK och inhämtning enligt IHL reglerar nämligen exklusivt möjligheterna att från en operatör hämta in uppgifter om elektronisk kommunikation. Detta gäller under förutsättning att det handlar om en operatör i den mening som avses i lagen (2022:482) om elektronisk kommunikation samt att informationen faller under operatörens tystnadsplikt enligt samma lag. Det har hävdats att motsvarande exklusivitet bör gälla för hemlig dataavläsning, även om frågan inte togs upp särskilt under lagstiftningsarbetet (se Lindberg, *Straffprocessuella tvångsmedel – när och hur får de användas?*, 2022, version 5, JUNO, s. 525 och 869 f.). Det innebär att beslag, husrannsakan och edition inte är tillåtna tvångsmedel för att hos operatörer få fram sådan information som reglerna i 2 § första stycket 1–3 lagen om hemlig dataavläsning är avsedda att träffa. Motsvarande information kan dock finnas på andra ställen än hos operatören, t.ex. i den berördes telefon, och då gäller ingen sådan exklusivitet.

4.3.2 Husrannsakan m.m.

Ett annat straffprocessuellt tvångsmedel av intresse i sammanhanget är husrannsakan. Bestämmelserna om husrannsakan i 28 kap 1 § rättegångsbalken gäller under förundersökning. I detta avsnitt redogörs särskilt för husrannsakan under förundersökning i it-miljöer. En all-

män redogörelse för bestämmelserna om husrannsakan under förundersökning finns i SOU 2017:89 s. 95 ff.

Husrannsakan kan användas i it-miljöer för att söka igenom lokalt lagrade uppgifter i elektronisk kommunikationsutrustning som tagits i beslag eller som påträffats vid husrannsakan. Uttrycket ”elektronisk kommunikationsutrustning” har i detta fall samma innebörd som i lagen om hemlig dataavläsning (se prop. 2021/22:119 s. 67 f.). Husrannsakan kan användas redan vid misstanke om lindrigare brottslighet och kräver som huvudregel inte rättens tillstånd. Husrannsakan sker som huvudregel i den berördes närvaro. Det finns inget krav på att den som husrannsakan vidtas hos ska närvara, men det finns inte heller något hinder mot att så sker. Det är därmed möjligt att utföra en husrannsakan, trots att det inte är ett hemligt tvångsmedel, utan att den berörde vet om detta. Underrättelse om åtgärderna kan då vänta till dess den kan lämnas utan men för utredningen, se 28 kap. 1 § och 7 § andra stycket rättegångsbalken.

Husrannsakan i it-miljöer uppvisar således vissa likheter med ett tillträdestillstånd för att verkställa hemlig dataavläsning. Betydande skillnader finns dock både när det gäller beslutsordningen och de bakomliggande kraven. För gränsdragningen är det av avgörande betydelse att åtgärderna har olika ändamål. Frågan om gränsdragningen mellan tillträdestillstånd och husrannsakan berördes i propositionen om hemlig dataavläsning (se prop. 2019/20:64 s. 145 f.). Regeringen såg då ingen risk för gränsdragningsproblem. Regeringen menade att även om själva verkställigheten av både en husrannsakan och ett tillträdestillstånd i vissa fall kommer att ske på samma sätt (intrång i en viss lokal) är ändamålen bakom respektive åtgärd olika. Vi ansluter oss till regeringens bedömning i detta avseende. Ändamålet med husrannsakan är huvudsakligen att eftersöka föremål som kan tas i beslag eller att utröna omständigheter som kan vara av betydelse för utredningen om ett brott, se 28 kap. 1 § rättegångsbalken. Syftet med ett tillträdestillstånd är att kunna installera de tekniska hjälpmedel som behövs för att verkställa hemlig dataavläsning. Ett tillträdestillstånd avseende hemlig dataavläsning kan därför aldrig användas för att samtidigt genomföra husrannsakan på platsen och vice versa.

4.3.3 Tillfälligt omhändertagande av elektronisk kommunikationsutrustning

I 23 kap. 9 a § rättegångsbalken regleras förutsättningarna för tillfälligt omhändertagande av elektronisk kommunikationsutrustning under förundersökning, t.ex. i en förhörssituation. Uttrycket elektronisk kommunikationsutrustning är teknikneutralt och har samma innebörd som i annan tvångsmedelsreglering. Det handlar t.ex. om datorer eller mobiltelefoner. Sedan den 1 juni 2022 kan tillfälligt omhändertagande av elektronisk kommunikationsutrustning även ske vid genomsökning på distans, se 28 kap. 10 f § rättegångsbalken. Bestämmelsen har utformats med 23 kap. 9 a § rättegångsbalken som förebild. Enligt båda bestämmelserna får ett omhändertagande av elektronisk kommunikationsutrustning ske om det kan antas att utredningen annars försvåras. Det handlar i båda fallen om ett kortvarigt omhändertagande där ändamålet med åtgärden är att undanröja risken för att brottsutredningen försvåras. Den omhändertagna utrustningen får inte undersökas och inte heller i övrigt får några åtgärder vidtas med egendomen (se prop. 2015/16:68 s. 73 och prop. 2021/22:119 s. 182). Ändamålet skiljer sig alltså helt från ändamålet med hemlig dataavläsning.

Utanför förundersökning finns särskilda bestämmelser om bl.a. husrannsakan samt tillfälligt omhändertagande och efterföljande undersökning av elektronisk kommunikationsutrustning. I 5 kap. 3 och 4 §§ lagen (2022:700) om särskild kontroll av vissa utlänningar regleras förutsättningarna för användandet av dessa tvångsmedel vid särskild utlänningskontroll. Av regleringen framgår att det endast är vid en husrannsakan, kroppsvisitation eller kroppsbesiktning enligt nämnda lag som en polisman har rätt att tillfälligt omhänderta och undersöka elektronisk kommunikationsutrustning. Det är alltså inte tillåtet att verkställa hemlig dataavläsning genom att tillfälligt ta hand om kommunikationsutrustning vid någon annan åtgärd (jfr resonemanget ovan i avsnitt 4.3.2, se även prop. 2019/20:64 s. 157). I praktiken uppkommer därför inte heller några gränsdragningsproblem mot tillfälligt omhändertagande av kommunikationsutrustning.

4.3.4 Genomsökning på distans

Den 1 juni 2022 infördes genomsökning på distans som ett nytt tvångsmedel i rättegångsbalken, se prop. 2021/22:119 *Modernare regler för användningen av tvångsmedel*. I likhet med lagen om hemlig dataavläsning har regleringen om genomsökning på distans vuxit fram som en anpassning till brotts- och teknikutvecklingen för att ge de brottsbekämpande myndigheterna mer effektiva utredningsverktyg i it-miljöer. Tidigare saknades lagstöd för att eftersöka information som inte fysiskt fanns på platsen för husrannsakan eller i själva beslagsföremålet. Genomsökning på distans har införts som ett självständigt tvångsmedel för att kunna eftersöka handlingar som är externt lagrade och som därför inte omfattas av regleringen om husrannsakan. Det nya tvångsmedlet utgör ett komplement till husrannsakan i it-miljöer och har utformats med bestämmelserna om husrannsakan som förebild.

Genomsökning på distans innebär att söka efter handlingar som finns lagrade i ett avläsningsbart informationssystem utanför den elektroniska kommunikationsutrustning som används för att utföra genomsökningen, se 28 kap. 10 a § rättegångsbalken. Uttrycket ”avläsningsbart informationssystem” har samma innebörd som i 1 § andra stycket lagen om hemlig dataavläsning. Verkställighet av åtgärden innebär sökning efter ”handlingar”. Uttrycket har samma innebörd som i 2 kap. 3 § tryckfrihetsförordningen. Vid genomsökning på distans sker det alltså inte någon differentiering mellan olika typer av handlingar. Handlingarna förutsätts finnas lagrade i informationssystemet när åtgärden genomförs. Handlingarna ska vidare finnas lagrade utanför den elektroniska kommunikationsutrustningen, t.ex. i en extern server eller i s.k. molntjänster. Genomsökning på distans kan precis som husrannsakan användas redan vid misstanke om lindrigare brottslighet och kräver som huvudregel inte rättens tillstånd. De närmare förutsättningarna för hur genomsökningen får genomföras framgår av 28 kap. 10 b och c §§ rättegångsbalken. Om genomsökningen görs i samband med en husrannsakan tillämpas samma regler om närvaro som vid husrannsakan. Det innebär att genomsökning på distans, precis som beslag och husrannsakan, kan ske utan att den som är föremål för åtgärden är närvarande eller har underrättats på förhand, se 28 kap. 10 e och g §§ rättegångsbalken. Den enskilde har, när genomsökning inte sker inom ramen för en husrannsakan, i vissa fall rätt att närvara vid genomsökningen. Detta överensstämmer med

vad som gäller vid genomsökning av elektronisk kommunikationsutrustning som tagits i beslag enligt 27 kap. 11 b § rättegångsbalken. Vidare ska den enskilde underrättas om åtgärden så snart det kan ske utan men för utredningen. Hemlig dataavläsning sker alltid i hemlighet och med möjlighet att i vissa fall underlåta att underrätta den enskilde om åtgärden.

Ändamålet med genomsökning på distans sammanfaller alltså delvis med ändamålet för hemlig dataavläsning. Alternativet för att få fram samma handlingar skulle därmed kunna vara att använda hemlig dataavläsning. I en konkret situation är det t.ex. möjligt att använda såväl genomsökning på distans som hemlig dataavläsning för att hämta in uppgifter som finns lagrade i en krypterad chattapplikation. En genomsökning på distans tillsammans med en it-forensisk undersökning kan i likhet med hemlig dataavläsning ge tillgång till omfattande information. Lagstiftningarna är alltså överlappande, även om genomsökning på distans i dag inte kan användas utanför en förundersökning. Ett förslag om att det ska införas en sådan möjlighet är dock under beredning (se SOU 2023:60).

En väsentlig skillnad mellan tvångsmedlen är att metoden för genomsökning på distans skiljer sig från metoden för hemlig dataavläsning. Genomsökning på distans får endast verkställas genom autentisering, dvs. t.ex. genom ansiktsigenkänning, fingeravtryck eller inloggningsuppgifter. Tvångsmedlet tillåter alltså inte användning av tekniska hjälpmedel som installation av hård- eller mjukvara, kringgående av systemskydd eller utnyttjande av tekniska sårbarheter. Genomsökning på distans får inte heller användas för löpande övervakning. Åtgärden är endast avsedd att ge en ögonblicksbild av det material som finns lagrat vid ett tillfälle. Däremot saknas för genomsökning på distans motsvarande uttryckliga krav på en begränsning av åtkomsten till historiska uppgifter som finns i lagen om hemlig dataavläsning. Även beslutsordningen och de bakomliggande kraven för ett tillstånd till de olika åtgärderna skiljer sig åt. Genomsökning på distans kan som angetts användas redan vid lindrigare brottslighet eller när bevisning behöver hämtas in i direkt anslutning till ett beslag. Avgörande för gränsdragningen är att hemlig dataavläsning endast får användas när alla andra åtgärder, dvs. även genomsökning på distans, har utretts eller uttömts. I behovs- och proportionalitetsavvägningen får beaktas de väsentliga skillnader mellan de olika tvångsmedlen som ovan redogjorts för.

5 Allmänna utgångspunkter

5.1 Uppdraget

Lagen om hemlig dataavläsning har en begränsad giltighetstid och gäller till utgången av mars 2025. Vårt huvudsakliga uppdrag är att utvärdera lagen och ta ställning till om den bör permanentas och om regleringen i så fall bör förändras i något avseende. Uppdraget har också innefattat att, oavsett vilket ställningstagande som görs, analysera vilka åtgärder som behövs för ett permanentande och lämna förslag på dessa. Uppdraget förutsätter en noggrann avvägning mellan de olika intressen som berörs. Ytterst handlar det om balansen mellan å ena sidan samhällets behov av en effektiv brottsbekämpning till skydd för medborgarna och å andra sidan enskildas rätt till personlig integritet och rättssäkerhet i förhållande till staten. Det är nödvändigt att de brottsbekämpande myndigheterna både nationellt och i det internationella samarbetet har tillgång till ändamålsenliga och verkningsfulla verktyg för att effektivt kunna utreda, förebygga, upptäcka och förhindra allvarlig brottslighet. Samtidigt innebär de brottsbekämpande myndigheternas användning av hemlig dataavläsning ett betydande ingrepp i den enskildes personliga integritet och en förhöjd risk för informationssäkerheten. Detta ställer i sin tur höga krav på rättssäkerheten i regelverket och att intrånget i den personliga integriteten minimeras. Inledningsvis finns därför anledning att göra avstamp i några allmänna utgångspunkter för våra överväganden.

5.2 De brottsbekämpande myndigheternas uppgifter

Användning av hemlig dataavläsning bör i likhet med all tvångsmedelsanvändning förstås mot bakgrund av de brottsbekämpande myndigheternas uppgifter. Till de brottsbekämpande myndigheterna hör Polismyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten, Tullverket,

Kustbevakningen, Skatteverket och Försvarsmakten (genom militärpolisen). En kort beskrivning av dessa myndigheters brottsbekämpande verksamheter och uppgifter återfinns i förarbetena till lagen om hemlig dataavläsning, SOU 2017:89 s. 67 f. och prop. 2019/20:64 s. 32.

Vissa av de brottsbekämpande myndigheterna kan under vissa närmare förutsättningar använda hemlig dataavläsning både under och utanför en förundersökning. Användningen av hemlig dataavläsning begränsas även utifrån särskilda i lagen angivna kvalifikationskrav samt allmänna principer för tvångsmedelsanvändning. Dessa krav och principer har vi redogjort för i avsnitt 3.2 och 4.1. Under förundersökning använder de brottsbekämpande myndigheterna hemlig dataavläsning i syfte att utreda brott och säkra bevisning inför en eventuell rättegång. I dessa fall förutsätter tvångsmedelsanvändningen att det finns en konkret brottsmisstanke. Utanför förundersökning används hemlig dataavläsning i de brottsbekämpande myndigheternas underrättelseverksamhet och vid särskild utlänningskontroll. Syftet med hemlig dataavläsning i dessa fall är att förebygga, förhindra eller upptäcka brottslig verksamhet i ett skede när det ännu inte finns konkreta misstankar om att ett brott har begåtts.

5.3 En stegrande brottsutveckling och en ny teknisk verklighet

5.3.1 Inledning

Vid införandet av lagen om hemlig dataavläsning angavs att de brottsbekämpande myndigheternas behov av hemlig dataavläsning hade växt fram för att möta den brottsutveckling som skett parallellt med en snabb teknisk utveckling och förändrade kommunikationsvanor. För förståelsen av det fortsatta behovet av hemlig dataavläsning inleder vi med en kort beskrivning av de senaste årens brottsutveckling och den nya tekniska verklighet som de brottsbekämpande myndigheterna arbetar i.

5.3.2 Brottsutvecklingens betydelse

När det gäller brottsutvecklingen har inte minst den markanta ökningen av dödligt skjutvapenvåld medfört ett behov av adekvata verktyg för de brottsbekämpande myndigheterna. Våldsbrottsligheten är i sin tur starkt kopplad till den ökade narkotikabrottsligheten. En betydande förändring har skett även i underrättelsemiljön de senaste åren. Brottsligheten har utvecklats och blivit mer samhällshotande. Även den europeiska säkerhetssituationen har påverkats, inte minst av det pågående kriget i Ukraina och den allvarliga situation som för närvarande utspelar sig i Mellanöstern. Detta får i sin tur konsekvenser för Sveriges säkerhet. Även den fleråriga pandemin har påverkat underrättelsehoten. Den har bland annat bidragit till att förstärka polariseringen i samhället och gett upphov till konspirationsteorier. Detta utnyttjas både av främmande makt och våldsbejakande extremister. Allt fler extremister hittar gemenskap på nätet. Med teknikutvecklingen stärks såväl främmande makts som våldsbejakande extremisters förmågor. Digitala plattformar skapar mötesplatser för radikalisering och rekrytering. Här sker också planering och uppmaningar till ideologiskt motiverad brottlighet. De digitala plattformarna underlättar för unga personer att medverka, vilket i sin tur innebär att allt fler unga attraheras av nätbaserad och gränslös extremism. Det är fråga om föränderliga och komplexa hotbilder, något som präglar de brottsbekämpande myndigheternas arbete. Samtidigt är sårbarheterna i Sverige stora eftersom lagstiftningen har svårt att hålla jämna steg med utvecklingen (jfr Säkerhetspolisens årsberättelse 2021). Hur de senaste årens brottsutveckling i stort har sett ut och vilken betydelse den haft har utförligt redogjorts för i delbetänkandet *Utökade möjligheter att använda preventiva tvångsmedel*, SOU 2022:52 s. 125 ff. Redogörelsen beskriver hur utvecklingen har påverkat de brottsbekämpande myndigheternas behov av att använda tvångsmedel i underrättelseverksamhet, men är likaledes gällande för den brottsutredande verksamheten.

5.3.3 Teknikutveckling och förändrade kommunikationsvanor

Teknikutvecklingen de senaste åren har varit mycket snabb. I dag använder 95 procent av svenskarna Internet och nästan alla gör det dagligen (se rapporten *Svenskarna och internet 2023*, oktober 2023, Svenska Internetstiftelsen). Utvecklingen är inte unik för Sverige.

Antalet personer som dagligen använde internet i Eurozonen år 2003 var 18 procent. År 2021 hade den siffran stigit till 82 procent (se *Statistics Eurostat [Elektronisk resurs]*, Eurostat, Luxembourg, 2004-, http://ec.europa.eu/eurostat). Det innebär också att medvetenheten om riskerna med informationssäkerheten har ökat, varför det har uppstått legitima skäl för att skydda vissa förehavanden på internet från insyn. Samma utveckling har påverkat de kriminellas möjligheter att kommunicera utan insyn. Den allvarliga och organiserade brottsligheten kräver samordning och kommunikation, vilket i sin tur lämnar digitala spår. Uppgifter om elektronisk kommunikation är många gånger helt avgörande för en framgångsrik brottsbekämpning. Brottsförebyggande rådet (Brå) bedömer t.ex. att den digitala kommunikationen är central för nästan alla former av narkotikahantering (Brå 2021:10 s. 151 f.). Samtidigt blir de kriminella aktörerna alltmer säkerhetsmedvetna. Särskilt inom den allvarliga och organiserade brottsligheten används ofta krypterade tjänster och elektronisk utrustning för att kommunicera, i direkt syfte att undgå myndigheternas insyn. Globaliseringen, den tekniska utvecklingen och förändrade kommunikationsvanor har inneburit att de brottsbekämpande myndigheterna inte längre kan ta del av information som tidigare var tillgänglig genom traditionella tvångsmedel. Den information som tidigare var åtkomlig genom traditionella tvångsmedel finns numera ofta lagrad i krypterade enheter och tjänster. Denna utveckling har tidigare beskrivits mer ingående i förarbetena till lagen om hemlig dataavläsning (se SOU 2017:89 s. 153 ff. och prop. 2019/20:64 s. 66 ff.) och alldeles nyligen av Utredningen om preventiva tvångsmedel (se SOU 2022:52 s. 140 ff.).

Sedan lagen om hemlig dataavläsning infördes har betydelsen av effektiv tillgång till elektronisk bevisning blivit ännu mer framträdande. Det visar inte minst användningen av material från de krypterade kommunikationstjänsterna Encrochat, Sky ECC och Anom. Den information som den svenska polisen har fått ut ur dessa krypterade tjänster har lett till ett stort antal domar där flera hundra personer har dömts till fängelsestraff. Brottsvinster från dessa domar, inklusive förverkande, beräknas fram till december 2022 ha uppgått till över 100 miljoner kronor (*Inrapporterade domar baserade på kryptoinformation fram till och med 22 december 2022*, statistikuppgifter sammanställda av Omega och Polismyndigheten). Störst uppmärksamhet har Encrochat fått. Det var under våren 2020 som franska myn-

digheter tillsammans med Europol lyckades tillgängliggöra innehållet i den krypterade kommunikationstjänsten Encrochat. Härigenom kunde information inhämtas från telefoner som använde tjänsten, vilket innebar att den franska polisen i relativ närtid kunde läsa miljontals meddelanden som handlade om bland annat detaljerade mordplaner, narkotika- och vapenleveranser samt penningtvätt. Svensk polis fick därefter tillgång till uppgifter från de användarkonton som befann sig i Sverige eller hade kontakt med användare i Sverige, och kunde i relativ närtid följa kriminella aktörers brottsplaner. Tillgången till Encrochat ledde till ett stort antal ingripanden inom ramen för ”Operation Robinson” (*Lärdomar av Encrochat – analysprojekt Robinson*, NOA, maj 2021, s. 5). Erfarenheterna av de krypterade informationstjänsterna har även lett till ökade kunskaper om kriminella aktörers motiv, tillvägagångssätt och den kriminella miljöns strukturer. Erfarenheterna visar bl.a. att de kriminella aktörerna har ett högt säkerhetsmedvetande och att de överlag har goda möjligheter att knyta de kontakter som krävs för att ostört och framgångsrikt kunna fortsätta bedriva sin brottsliga verksamhet (se a. rapport s. 3, 5 och 31).

Samtidigt innebär den fortsatta teknik- och kommunikationsutvecklingen att det praktiska användningsområdet för hemlig avlyssning och hemlig övervakning av elektronisk kommunikation begränsas. Exempelvis kan införandet av den femte generationens mobilnät (5G) medföra tillämpning av ytterligare krypterings- och autentiseringsprocesser som syftar till att höja säkerheten, men samtidigt riskerar att väsentligt försvåra möjligheterna att verkställa hemliga tvångsmedel. Vidare kan förändrade tekniska förfaranden vid s.k. roaming medföra att information bara kan avläsas av operatören i det land som ett visst abonnemang utfärdats i, med följd att information som hade kunnat avläsas från ett utländskt abonnemang som används i Sverige blir otillgänglig för de brottsbekämpande myndigheterna här. Dessutom kan mängden information som över huvud taget kan inhämtas genom hemlig avlyssning och hemlig övervakning av elektronisk kommunikation komma att begränsas genom teknikutvecklingen. Som nyss angetts är det inte bara kommunikationen i sig som är föremål för kryptering, utan det sker också en utveckling av möjligheterna att kryptera innehållet i kommunikationsutrustning och lagringsmedier.

5.3.4 Ett rättsområde i utveckling

Lagstiftningen om straffprocessuella tvångsmedel är ett prioriterat område för lagstiftaren. Regleringarna om såväl öppna som hemliga tvångsmedel har de senaste åren genomgått omfattande förändringar. Lagstiftningen har moderniserats och anpassats till följd av att brottsutvecklingen har förändrats i takt med teknikutvecklingen och förändrade kommunikationsvanor. Nya och utvidgade möjligheter till tvångsmedelsanvändning har införts i syfte att effektivisera brottsbekämpningen. Det handlar till stor del om att tvångsmedelsanvändningen har anpassats till it-miljön och den ökade användningen av tekniska lösningar som förändrar förutsättningarna för åtkomst, såsom kryptering. Hemlig dataavläsning är ett exempel på en sådan anpassning som har införts för att återställa de brottsbekämpande myndigheternas förmåga att få tillgång till information.

Ett flertal utredningar har nyligen föreslagit ytterligare utvidgningar av möjligheterna att använda tvångsmedel i brottsbekämpningen. Några av dessa har dessutom lämnat förslag som direkt berör hemlig dataavläsning. Viss ny lagstiftning samt nyligen lagda lagförslag som har betydelse för vår utredning har översiktligt presenterats i avsnitt 3.3. Härutöver finns ytterligare exempel förändringar som indirekt är av intresse för vårt arbete. Här ska särskilt nämnas reglerna om beslag och husrannsakan som nyligen har anpassats efter de brottsbekämpande myndigheternas behov i den nya tekniska verkligheten, se avsnitt 4.3.1. Vidare har vi i avsnitt 4.3.4 redogjort för det nya tvångsmedlet genomsökning på distans.

Den omständigheten att rättsområdet är i pågående utveckling försvårar såväl överblicken av befintliga straffprocessuella tvångsmedel som bedömningen av olika integritetsintrång.

5.4 Grundläggande bestämmelser till skydd för den personliga integriteten

5.4.1 Inledning

Bestämmelserna om hemlig dataavläsning utgör lagreglerade inskränkningar i det grundläggande skydd för privatlivet och den personliga integriteten som tillförsäkras enskilda i bl.a. regeringsformen och Europakonventionen. Grundläggande bestämmelser om dessa fri-

och rättigheter återfinns även i andra internationella instrument som är rättsligt bindande för Sverige. Häribland kan nämnas FN:s konvention om medborgerliga och politiska rättigheter samt EU:s rättighetsstadga. EU:s rättighetsstadga säkerställer ett likvärdigt skydd för grundläggande fri- och rättigheter som Europakonventionen i de fall unionsrätten ska tillämpas.

Skyddet för privatlivet och den personliga integriteten är inte absolut utan får inskränkas. Sådana inskränkningar kräver formellt lagstöd och får enligt de olika instrumenten endast göras under vissa närmare angivna förutsättningar. Bestämmelserna på området finns översiktligt redovisade på flera ställen, bland annat i förarbetena till lagen om hemlig dataavläsning, se SOU 2017:89 s. 68 ff. och prop. 2019/20:64 s. 32 ff. Utredningen om preventiva tvångsmedel har härutöver helt nyligen gjort en genomgång av unionsrätten i förhållande till hemliga tvångsmedel och europarättslig praxis angående hemliga tvångsmedel, se SOU 2022:52 s. 58 ff. och 45 ff. Något kort ska nämnas även här om skyddet för den personliga integriteten och rätten till privatliv så som det kommer till uttryck i regeringsformen och i Europakonventionen. I våra överväganden återkommer vi till dessa olika hänsyn som måste tas vid all tvångsmedelslagstiftning och som alltså utgör rättsliga utgångspunkter för vårt uppdrag.

5.4.2 Skyddet för den personliga integriteten i regeringsformen

Grundlagsskyddet för den personliga integriteten regleras i 2 kap. 6 § regeringsformen. Enligt bestämmelsen är var och en gentemot det allmänna skyddad mot bland annat undersökning av brev eller annan förtrolig försändelse och mot hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande. Vidare tillerkänns enskilda, gentemot det allmänna, ett generellt skydd mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Skyddet kan enligt 2 kap. 20 och 21 §§ regeringsformen begränsas genom lag för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. En begränsning får aldrig gå utöver vad som är nödvändigt med hänsyn till ändamålet och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen. Inte heller får en begränsning göras enbart på grund av

politisk, religiös, kulturell eller annan sådan åskådning. Undantagsregleringen är ägnad att understryka kravet på att lagstiftaren öppet och noggrant redovisar sina syften när en fri- och rättighetsinskränkande lag beslutas (se *om ändring i regeringsformen*, prop. 1975/76:209 s. 153).

5.4.3 Rätten till privat- och familjeliv enligt Europakonventionen

Europeiska konventionen av den 4 november 1950 om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) är sedan år 1995 inkorporerad i svensk lag. Enligt 2 kap. 19 § regeringsformen får lag eller annan föreskrift inte meddelas i strid med Sveriges åtaganden på grund av Europakonventionen. Enligt artikel 8.1 i konventionen har var och en rätt till respekt för sitt privatliv och familjeliv, sitt hem och sin korrespondens. Med korrespondens avses olika former för att överföra meddelanden mellan individer. Överföring av meddelanden med hjälp av t.ex. telefon och datorer omfattas av konventionens skydd för korrespondens (se Danelius, *Mänskliga rättigheter i europeisk praxis*, femte upplagan, 2015, s. 432).

Skyddet enligt artikel 8.1 är omfattande och täcker en mängd olika aspekter av den enskildes privata förhållanden. Vid användning av hemliga tvångsmedel måste beaktas inte bara privatlivet för personen som tvångsmedlet riktas mot, utan även privatlivet hos den som t.ex. ringer till en avlyssnad telefon. Vidare innefattar rätten till respekt för privatlivet både ett förbud för staten att göra otillåtna ingrepp i privatlivet och en skyldighet för staten att genom bl.a. lagstiftning och andra åtgärder skydda den enskilde mot sådana ingrepp från andra (se bl.a. K.U. mot Finland punkterna 47–49). En förutsättning för att staten ska kunna leva upp till kraven på att upprätthålla rättstryggheten för enskilda är att staten har en väl fungerande och effektiv brottsbekämpning. Detta krav innebär bl.a. att myndigheterna måste ha tillgång till effektiva utredningsverktyg, även i it-miljön, för att utreda brott som innefattar allvarliga kränkningar. När så inte har varit fallet har staten ansetts kränka de rättigheter som följer av artikel 8. Ett exempel på detta var Europadomstolens mål K.U. mot Finland. I målet hade en okänd person lagt upp en kränkande kontaktannons avseende ett 12-årigt barn på en dejting-

sajt. Europadomstolen fann att avsaknaden av en möjlighet enligt finsk rätt att inhämta uppgift från en operatör om vem som använt IP-adressen, vilket hindrade att personen kunde identifieras, utgjorde en kränkning av artikel 8. Europadomstolen uttalade i domen att konfidentialitet för kommunikation och yttrandefrihet ibland måste få vika för brottsbekämpande ändamål.

De grundläggande rättigheterna i artikel 8.1 får enligt artikel 8.2 Europakonventionen inte inskränkas annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till statens säkerhet, den allmänna säkerheten, landets ekonomiska välstånd eller till förebyggande av oordning eller brott eller till skydd för hälsa eller moral eller för andra personers fri- och rättigheter. Lagen måste i sin tur uppfylla rimliga anspråk på rättssäkerhet, såsom att skydda mot godtycke, vara tillgänglig för allmänheten och vara förutsebar. För att inskränkningen ska betraktas som nödvändig i ett demokratiskt samhälle måste det enligt Europadomstolen finnas ett angeläget samhälleligt behov. Konventionsstaterna har ett visst eget tolkningsutrymme även om Europadomstolen förbehåller sig rätten att i det enskilda fallet pröva frågan. Bedömningen av om inskränkningen är nödvändig ska enligt praxis bl.a. göras utifrån hur väsentlig rättigheten är, vad åtgärden består i och det eftersträvade syftet. Inskränkningen måste vara proportionerlig i förhållande till det syfte som ska tillgodoses (se Danelius, a.a., s. 370).

5.5 Principiella utgångspunkter för våra intresseavvägningar

5.5.1 Tillvägagångssätt och underlag – avvägningar om behov, nytta och integritet

Lagstiftningen om hemlig dataavläsning ska tillgodose samhällets behov av en effektiv brottsbekämpning till skydd för medborgarna och deras personliga integritet. Samtidigt kan hemlig dataavläsning utgöra en risk för enskildas rätt till personlig integritet och rättssäkerhet i förhållande till staten. Balansen mellan de olika intressena innebär både viktiga och svåra avvägningar. Det är av grundläggande betydelse i en rättsstat att enskildas rätt till skydd för den personliga integriteten och rättssäkerheten respekteras. För en effektiv brottsbekämpning är det samtidigt nödvändigt att det finns ändamålsenliga

och verkningsfulla verktyg för de brottsbekämpande myndigheterna att använda som hjälpmedel i enskilda fall. Eftersom staten är skyldig att tillhandahålla en effektiv brottsbekämpning som kan utgöra skydd för enskildas integritet utgör brottsbekämpningen en grundläggande samhällsfunktion. Regleringen av hemliga tvångsmedel måste därför som utgångspunkt följa med i tiden för att möta de behov som uppstår till följd av förändringar i samhället och den tekniska utvecklingen.

Huruvida hemlig dataavläsning kan anses nödvändigt i ett demokratiskt samhälle förutsätter en analys av nyttan och behovet av åtgärden. Nyttan och behovet ska i sin tur vägas mot de risker som användningen av tvångsmedlet innebär för den personliga integriteten. Samtidigt måste beaktas att avsaknaden av effektiva åtgärder kan innebära en risk för att staten inte kan tillgodose enskildas rätt till skydd mot kränkningar från andra enskilda och att sörja för att rättsväsendet effektivt ingriper när en kränkning ägt rum. Avslutningsvis måste en övergripande proportionalitetsbedömning göras. Vi återkommer nedan till en kort förklaring av de centrala begreppen behov, nytta, personlig integritet och proportionalitet. Det är först efter inledande avvägningar utifrån dessa perspektiv som det är möjligt att göra en bedömning i frågan om lagstiftningen bör permanentas. Det ska i sammanhanget understrykas att lagstiftning om hemliga tvångsmedel endast kan anses ändamålsenlig och proportionerlig om den innehåller ett tydligt avgränsat tillämpningsområde, tillräckliga kvalifikationskrav, rättssäkerhetsgarantier och andra kontrollmekanismer som balanserar den ökade integritetsrisken. Det sagda innebär att varje förslag till förändring i regelverket måste bygga på samma noggranna analyser och intresseavvägningar.

Inför våra analyser måste vi kartlägga hur hemlig dataavläsning har tillämpats sedan lagens ikraftträdande. För att kunna bedöma om det finns ett fortsatt reellt och angeläget behov av hemlig dataavläsning bör först den hittillsvarande nyttan av hemlig dataavläsning analyseras. De integritetsintrång som åtgärden hittills har inneburit får ge ledning i våra avvägningar om förväntade risker för den personliga integriteten. Samtidigt måste de risker för den personliga integriteten som kan följa med avsaknaden av effektiva brottsbekämpande åtgärder beaktas. Våra analyser bör, i den utsträckning det är möjligt, grunda sig på ett empiriskt underlag avseende bl.a. den hittillsvarande tillämpningen av hemlig dataavläsning. Underlaget bör vara så brett som möjligt och innefatta såväl kvantitativa som kvalitativa uppgif-

ter om tillämpningen av hemlig dataavläsning. Vårt underlag i dessa delar består huvudsakligen i de årliga redovisningar som finns om hemlig tvångsmedelsanvändning samt de erfarenheter som experter från de brottsbekämpande myndigheterna har delat med sig av vid möten och i underlag till utredningen. Även Säkerhets- och integritetsskyddsnämndens tillsynsmaterial beträffande användningen av hemlig dataavläsning utgör ett viktigt underlag för våra analyser. Användningen av hemlig dataavläsning har dessutom varit ett särskilt fokusområde för nämndens tillsynsarbete under åren 2021 och 2022. På grundval av analyserna måste sedan resonemang föras där argument som talar för tvångsmedlet prövas och bryts mot argument som talar i motsatt riktning (se t.ex. Integritetsskyddskommitténs betänkande *Skyddet för den personliga integriteten*, SOU 2007:22, del 1 s. 176 f.). Det är endast om hemlig dataavläsning därefter framstår som nödvändigt, proportionellt och försvarligt i ett demokratiskt samhälle som åtgärden ska tillåtas.

5.5.2 Regleringen måste uppfylla kraven på rättssäkerhet och kraven på skydd för den personliga integriteten

Intresseavvägningarna bakom lagen om hemlig dataavläsning har resulterat i att tvångsmedlet omgärdas av ett antal kontrollmekanismer och andra rättssäkerhetsgarantier. Dessa har bl.a. tillkommit för att möta de krav som regeringsformen och Europakonventionen ställer på användning av hemliga tvångsmedel. Syftet är att säkerställa att både reglerna om hemlig dataavläsning och deras tillämpning lever upp till högt ställda rättssäkerhetskrav, men också att intrånget i den personliga integriteten och riskerna för informationssäkerheten minimeras.

Det är en självklar utgångspunkt att reglerna om hemlig dataavläsning måste leva upp till högt ställda krav på rättssäkerhet. Både regeringsformen och Europakonventionen ställer i detta avseende krav på förutsebara, tydliga och precisa regler. I kravet på rättssäkerhet ligger även att regleringen ska innefatta ett skydd mot missbruk. Det innebär att bestämmelser om hemlig dataavläsning måste innehålla begränsningar till skydd för den personliga integriteten. Europakonventionen ställer vidare krav på oberoende förhands- och efterhandskontroll samt bestämmelser som gör sådan kontroll möjlig, t.ex. genom krav på dokumentation av beslut och åtgärder samt underrättelser till dem som berörts. Det behöver också finnas bestämmelser

om hur den information som inhämtas får behandlas och för vilka ändamål. En brist i något avseende kan uppvägas av andra delar av systemet. Exempelvis kan en relativt vid tillämpningsbestämmelse vägas upp av krav på domstolsprövning och en obligatorisk proportionalitetsprövning. Systemet måste därför bedömas utifrån ett helhetsperspektiv (jfr *Rättssäkerhetsgarantier och hemliga tvångsmedel*, SOU 2018:61 s. 115 f.).

5.5.3 Regelverkets struktur och överensstämmelse med andra tvångsmedel

I utredningsuppdraget ligger att säkerställa en välfungerande systematik i regelverket. Uppdraget innefattar därför också ett krav att på nytt överväga lagstiftningstekniken.

Den allmänna strävan efter en välfungerande systematik får betydelse även för den del av uppdraget som innebär att vi ska bedöma behovet av följdändringar i regelverket i syfte att uppnå en mer effektiv brottsbekämpning. Förändringar i regelverket förutsätter som konstaterats ovan självklart att respekten för grundläggande fri- och rättigheter, liksom kraven på rättssäkerhet, säkerställs. I förarbetena till lagen om hemlig dataavläsning underströk regeringen att hemlig dataavläsning ska vara ett verktyg som ska återställa de brottsbekämpande myndigheternas förmåga (prop. 2019/20:64 s. 125). Vi ansluter oss till dessa utgångspunkter vid våra överväganden om förändringar i regelverket. Regeringen har vidare uttalat att det är av väsentlig betydelse att hemlig dataavläsning kan användas i motsvarande fall som de andra hemliga tvångsmedlen. Det finns annars risk för att vissa allvarliga brott inte kan utredas när det visar sig vara omöjligt att använda andra hemliga tvångsmedel (a. prop. s. 124).

Både frågan om lagstiftningsteknik och frågan om lagstiftningens överensstämmelse med andra tvångsmedel kompliceras av att det inte finns någon sammanhållen reglering om hemliga tvångsmedel. Vidare är rättsområdet som tidigare framhållits under utveckling. Ny lagstiftning på tvångsmedelsområdet har nyligen trätt i kraft och flera lagförslag är för närvarande under beredning. Som vi i avsnitt 5.3.4 redogjort för, pågår parallellt med arbetet i vår utredning annat lagstiftningsarbete som har direkt betydelse för och påverkan på regleringen om hemlig dataavläsning. Vår utgångspunkt är att regleringen om hemlig dataavläsning så långt det är möjligt bör utformas så att

den inte utan bärande skäl avviker från reglering om andra, såväl öppna som hemliga, tvångsmedel. Detta för att uppfylla kraven på systematik, överskådlighet och tydlighet. Vi måste emellertid i alla våra överväganden göra självständiga bedömningar utifrån ändamålen med hemlig dataavläsning, med utgångspunkt i de höga krav som regeringsformen och Europakonventionen ställer på lagstiftningen. Exempelvis kan det i vissa fall finnas skäl att höja kraven för när hemlig dataavläsning får användas i förhållande till andra tvångsmedel. Detta eftersom verkställighet av hemlig dataavläsning kan innebära en ökad risk för den personliga integriteten (se prop. 2019/20:64 s. 115).

5.6 Behov

5.6.1 Utgångspunkter för behovsanalysen

I de brottsbekämpande myndigheternas uppgifter ingår som konstaterats bl.a. att förebygga, förhindra och upptäcka brottslig verksamhet samt att utreda brott. För att de brottsbekämpande myndigheterna ska kunna fullgöra sina uppgifter har myndigheterna behov av information av olika slag. Hemliga tvångsmedel är ett av de verktyg som de brottsbekämpande myndigheterna kan få tillstånd att använda för att tillgodose behovet av information. Vid behovsanalysen måste vi därför beakta angelägenheten av informationsbehovet och möjligheterna att erhålla informationen på annat sätt än genom hemlig dataavläsning. Förutsättningarna att inhämta informationen på annat sätt beaktas även i effektivitets- och proportionalitetsbedömningarna.

Bedömningen av om det fortsatt finns ett faktiskt och angeläget behov av hemlig dataavläsning gör vi utifrån var och en av de uppgiftstyper som omfattas av hemlig dataavläsning:

1. kommunikationsavlyssningsuppgifter,
2. kommunikationsövervakningsuppgifter,
3. platsuppgifter,
4. kameraövervakningsuppgifter,
5. rumsavlyssningsuppgifter,

6. övriga lagrade uppgifter och
7. övriga uppgifter som visar hur viss teknisk utrustning används.

Uppgifter som kan hämtas in med stöd av punkt 1–5 motsvarar huvudsakligen uppgifter som de brottsbekämpande myndigheterna kan få tillstånd att hämta in genom hemlig avlyssning och övervakning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning (se avsnitt 3.2.4). När det gäller uppgiftstyperna i punkt 1–5 utgår vi därför från att det finns ett faktiskt och angeläget behov för de brottsbekämpande myndigheterna att kunna hämta in sådan information. I de årliga parlamentariska redovisningarna har annat inte framkommit än att användningen av de bakomliggande och beprövade hemliga tvångsmedlen har varit ett ändamålsenligt och nödvändigt instrument i brottsbekämpningen (se t.ex. senast skr. 2021/22:79 och 2022/23:30). Beträffande uppgiftstyperna i punkt 1–5 gör vi därför en analys av i vilken utsträckning det finns ett reellt behov av hemlig dataavläsning som metod för att kunna komma åt uppgifterna.

Uppgifter som kan hämtas in med stöd av punkt 6 och 7 avser uppgifter som i princip inte är möjliga att i hemlighet eller löpande få tillgång till genom andra hemliga tvångsmedel. Merparten av dessa uppgifter, såvitt vi kan bedöma endast med undantag av realtidsuppgifter enligt punkt 7, kan de brottsbekämpande myndigheterna dock hämta in under förundersökning genom öppna tvångsmedel som beslag och genomsökning på distans (i förening med en it-forensisk undersökning). Ett lagförslag om att genomsökning på distans ska kunna användas även i underrättelseverksamhet är för närvarande föremål under beredning (se betänkandet *Utökade möjligheter att använda preventiva tvångsmedel 2*, SOU 2023:60). En it-forensisk undersökning innebär, förenklat uttryckt, en teknisk undersökning av en elektronisk informationsbärare – t.ex. en mobiltelefon – som den brottsbekämpande myndigheten har fysisk tillgång till. Myndigheten kan vid den it-forensiska undersökningen kringgå olika systemskydd för att få tillgång till information som finns lagrad i mobiltelefonen eller som visar hur den används. Eftersom sådana uppgifter används frekvent i brottsutredningar kan det även när det gäller de uppgifter som kan hämtas in med stöd av punkt 6 och 7 anses klarlagt att det finns ett behov av dessa. Även beträffande uppgiftstyperna i punkt 6 och 7 får därför frågan om behovet av att kunna hämta in uppgifterna genom hemlig dataavläsning en framträdande plats (jfr

prop. 2019/20:64 s. 68 f.). Som vi har beskrivit i kapitel 4 sker inhämtning av information genom öppna tvångsmedel dock under andra förutsättningar än vid hemlig dataavläsning, se även avsnitt 5.8.2 nedan.

Den nytta som hemlig dataavläsning har inneburit för brottsbekämpningen beträffande de olika uppgiftstyperna blir en viktig indikation på om det finns ett fortsatt grundläggande behov av hemlig dataavläsning. En behovsanalys bör baseras inte enbart på de hittillsvarande effekterna av hemlig dataavläsning, utan också bygga på en prognos av framtida behov grundad på hur samhällsutvecklingen ser ut i stort. De brottsbekämpande myndigheternas behov av hemlig dataavläsning som metod i den brottsbekämpande verksamheten påverkas direkt av brottsutvecklingen i förening med teknikutvecklingen och förändrade kommunikationsvanor. I förarbetena till lagen om hemlig dataavläsning har ingående redogjorts för detta samspel (se särskilt kapitel 6–8 i SOU 2017:89). Det är därför angeläget att vid vår behovsanalys även ta hänsyn till utvecklingen på dessa områden de senaste åren (se avsnitt 5.3 ovan.) Slutligen utgår vi även från beskrivningar av den praktiska tillämpningen av hemlig dataavläsning som vi hämtat in från experter vid de brottsbekämpande myndigheterna. På samma sätt som när frågan tidigare utretts finns det skäl att, som utgångspunkt, låta de brottsbekämpande myndigheternas uppfattning om behovet av att använda hemlig dataavläsning väga tungt (jfr SOU 2017:89 s. 290).

5.7 Nytta och effektivitet

5.7.1 Hur mäter vi nytta och effektivitet?

Att bedöma nyttan av och effektiviteten i hemliga tvångsmedel är generellt sett en komplicerad uppgift. Eftersom hemlig dataavläsning är ett relativt nytt hemligt tvångsmedel ligger det en särskild svårighet i att dra långsiktiga slutsatser om nyttan och effekterna med åtgärden. En annan svårighet är att flera andra hemliga tvångsmedel ofta används parallellt med hemlig dataavläsning. Resultaten av olika åtgärder och olika hemliga tvångsmedel samverkar ofta med varandra på ett sätt som gör det svårt att avgöra vilken nytta en enskild åtgärd haft. Att lyfta ut hemlig dataavläsning från helheten kan därför både bli problematiskt och missvisande. När det gäller hemliga tvångsmedel i preventivt syfte ligger en särskild problematik i att bedöma vad som

är orsaken till att ett visst brott i ett visst fall inte kommer till stånd. Att risken inte förverkligas kan bero på andra vidtagna åtgärder än hemliga tvångsmedel liksom helt andra omständigheter, oberoende av de brottsbekämpande myndigheternas insatser. Även denna kausalitetsproblematik gör det svårt att mäta nyttan av hemlig dataavläsning mot en förutbestämd effekt. När användning av hemliga tvångsmedel tidigare utvärderats har det bedömts att nytta och effektivitet på grund av frågornas komplexitet i allmänhet inte lämpar sig särskilt bra för att mätas i siffror och andelstal relaterade till vissa följder (se *Hemliga tvångsmedel mot allvarliga brott*, SOU 2012:44 s. 481). Regeringen har inte heller ansett det ändamålsenligt eller lämpligt att slå fast vilka resultat som ska nås vid användningen av hemliga tvångsmedel, eller i förväg bestämma att en viss procentandel ska leda till vissa väntade resultat (se t.ex. skr. 2021/22:79 s. 43).

Frågan är då vilka effekter som ska anses utgöra nytta av användningen av hemlig dataavläsning. Det är, särskilt om jämförelser ska ske med andra hemliga tvångsmedel, trots de betänkligheter som redovisats ovan svårt att helt undvika förenklade andelsresonemang. Detta beror till stor del på hur det tillgängliga jämförelsematerialet är utformat. Det jämförelsematerial som finns att tillgå är de brottsbekämpande myndigheternas och regeringens årliga redovisningar om användningen av hemliga tvångsmedel. Åklagarmyndigheten sammanställer tillsammans med Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen och Tullverket varje år en redovisning om användningen av hemliga tvångsmedel. Redovisningen sker i enlighet med regeringsuppdrag och avser olika uppgifter om tillämpningen av hemliga tvångsmedel under föregående år. Redovisningen om nyttan av hemliga tvångsmedel har enligt regeringsuppdrag skett på samma sätt sedan år 2016. Den sammanställning som Åklagarmyndigheten gör varje år ligger sedan till grund för den parlamentariska granskning som årligen sker av den hemliga tvångsmedelsanvändningen (se avsnitt 3.2.13). De brottsbekämpande myndigheterna har haft tillgång till hemlig dataavläsning sedan den 1 april 2020. Det innebär att Åklagarmyndigheten hittills har lämnat tre redovisningar till regeringen om användningen av hemlig dataavläsning, avseende åren 2020–2022. Sedan lagens ikraftträdande har hemlig dataavläsning i skrivande stund varit föremål för parlamentarisk kontroll vid två tillfällen, avseende användning av åtgärden under åren 2020 och 2021 (se skr. 2021/22:79 och 2022/23:30). Regeringens skrivelse avseende

år 2022 lämnas till riksdagen först i december 2023 och omfattas därmed inte av vår analys.

I Åklagarmyndighetens årliga sammanställningar redovisas nyttan i den brottsutredande verksamheten genom anonymiserade exempel från tillämpningen och statistiska uppgifter. Den statistiska redovisningen sker i sin tur antalsmässigt (avseende antalet tillstånd, personer, avslag i domstol och interimistiska beslut), genom uppgifter om de olika tvångsmedlens varaktighet samt i form av andelstal (dvs. det procenttal där tvångsmedlet har gett viss effekt). Redovisningen i form av andelstal sker beträffande hemlig avlyssning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning enligt rättegångsbalken samt beträffande hemlig dataavläsning under förundersökning. Redovisningen i denna del bygger på uppskattningar av nyttan gjorda av de åklagare som varit förundersökningsledare. I redovisningen anges andelen utredningar där användningen av respektive hemligt tvångsmedel har lett till att:

- uppgifter har utgjort underlag i en förhörssituation,
- effektiv spaning har kunnat genomföras,
- annat tvångsmedel har använts mot den misstänkte,
- uppgifterna har bidragit till utredning om brottsutbyte,
- misstankarna mot den misstänkte har stärkts,
- den misstänkte har kunnat avföras från utredningen,
- den misstänkte har kunnat åtalas,
- uppgifterna har åberopats som bevisning i en stämningsansökan,
- uppgifterna har bidragit till att något tvångsmedel använts mot en annan person i samma förundersökning,
- uppgifterna har använts för att utreda brott i en annan förundersökning, eller
- uppgifterna har på annat sätt har bidragit till att utredningen kunnat föras framåt.

När det gäller nyttan av användningen av hemliga tvångsmedel i underrättelseverksamhet illustreras Polismyndighetens och Tullverkets användning genom anonymiserade exempel. Säkerhetspolisens an-

vändning av hemliga tvångsmedel i underrättelseverksamhet ingår inte i den årliga redovisningen av nyttan. En sådan redovisning bedöms inte kunna ske utan skada för verksamheten. Säkerhetspolisens redovisning ska därför enligt regeringsuppdrag endast avse antalet meddelade beslut om hemlig dataavläsning med undantag av hemlig dataavläsning vid särskild utlänningskontroll, antalet beslut som fattats med stöd av bestämmelserna i inhämtningslagen samt det totala antalet meddelade tillstånd om hemliga tvångsmedel i övrigt. Något andelsmässigt jämförelsematerial i underrättelseverksamhet finns inte att tillgå. Trots detta anses minst samma nytta av tvångsmedelsanvändning kunna förväntas i underrättelseverksamhet som i den brottsutredande verksamheten. Som skäl för detta har anförts att det får anses allmänt vedertaget att användningen av hemliga tvångsmedel är ett effektivt verktyg i den brottsutredande verksamheten. Vidare pekar den redovisning som finns om användning av inhämtning enligt inhämtningslagen på motsvarande nytta i underrättelseverksamhet (se t.ex. skr. 2021/22:79 s. 45 och 33 f.). Det har därför ansetts att det bör godtas som en allmän utgångspunkt att användning av hemliga tvångsmedel kan komma till nytta även i underrättelsestadiet, där informationsinhämtning utgör verksamhetens kärna. Erfarenheter från tvångsmedelsanvändning i det brottsutredande arbetet har därför i tidigare utredningar använts som underlag för analys av effekter av hemliga tvångsmedel i underrättelseverksamhet (se t.ex. SOU 2022:52 s. 164 f. med där gjorda hänvisningar). Vi ansluter oss till dessa allmänna utgångspunkter även i vår analys.

5.7.2 Utgångspunkter för nytto- och effektivitetsanalysen

För att kunna analysera nyttan och effektiviteten av hemlig dataavläsning krävs en kartläggning av tillämpningen. Det kan mot bakgrund av ovanstående redogörelse konstateras att kvantitativa effekter och andelsresonemang utgör trubbiga instrument för att mäta nytta och effektivitet. Kvantitativa uppgifter kan därför endast tjäna som utgångspunkt för en fortsatt och mer resonerande analys (jfr SOU 2012:44 s. 481). För att närmare kunna bedöma nyttan och effektiviteten av hemlig dataavläsning krävs en bedömning av de kvalitativa effekterna. Med kvalitativa effekter avses i sammanhanget att åtgärden i ett enskilt fall har gett den information som dataavläs-

ningen syftade till. Eftersom en nytto- och effektivitetsanalys bör vara så bred som möjligt har experter från de brottsbekämpande myndigheterna också lämnat beskrivningar och konkreta anonymiserade exempel från den hittillsvarande tillämpningen av hemlig dataavläsning. I likhet med vad som gäller beträffande behovet finns det skäl att, på samma sätt som när frågan tidigare har utretts, som utgångspunkt låta de brottsbekämpande myndigheternas uppfattning om nyttan och effektiviteten i att använda hemlig dataavläsning väga tungt (jfr SOU 2017:89 s. 290).

5.8 Risker för den personliga integriteten

5.8.1 Begreppet personlig integritet

Som framgår i avsnitt 5.4 finns ett grundlagsstadgat skydd för den enskildes privatliv – den personliga integriteten. Uttrycket personlig integritet är inte entydigt definierat, men används för att beskriva en rätt för den enskilde att skyddas mot fysiska och psykiska intrång i sin privata sfär (jfr t.ex. SOU 2007:22 del I s. 63 ff.). Det är svårt att formulera en beskrivning som pekar ut alla de situationer där individen har rätt att få sin integritet respekterad och skyddad. Trots detta är det nödvändigt att veta vad som avses när begreppet används. Det är en självklar utgångspunkt att innebörden måste vara tillräckligt tydlig för att det ska vara möjligt att avgöra vad som innebär en kränkning eller ett otillbörligt intrång. När det gäller hemliga tvångsmedel uttryckte Utredningen om vissa hemliga tvångsmedel att den personliga integritetens kärnområden, dvs. sådant som rör individen och dennes personlighet, var det relevanta för den analys som utredningen hade att göra. Inom den personliga integritetens kärnområden omfattas enligt utredningen information om den enskilde inklusive identifieringsdata avseende den enskildes bild, namn och liknande. Utredningen konstaterade också att varje befogenhet för staten att bereda sig tillgång till personlig information om den enskilde och varje nyttjande av sådan information leder till ingrepp i den personliga integriteten. Graden av integritetsintrång varierar med tvångsmedlets utformning och tillämpning (se SOU 2012:44 s. 480). Vi ansluter oss till dessa bedömningar.

5.8.2 Utgångspunkter för integritetsriskanalysen

Omständigheter som innebär en ökad risk för den personliga integriteten är t.ex. om åtgärden innebär att fler personer blir föremål för tvångsmedel, om fler utomstående utsätts för integritetsintrång eller om mer integritetskänslig information kommer till de brottsbekämpande myndigheternas kännedom. Att tvångsmedelsanvändning sker utanför förundersökning kan innebära en ökad risk för den personliga integriteten (jfr prop. 2019/20:64 s. 87 och SOU 2022:52 s. 173).

Det har tidigare framhållits att hemlig dataavläsning generellt sett innebär en ökad risk för enskildas personliga integritet i jämförelse med andra hemliga tvångsmedel. Detta beror huvudsakligen på att hemlig dataavläsning kan ge tillgång till fler och mer fullständiga uppgifter om enskilda än andra hemliga tvångsmedel. Eftersom hemlig dataavläsning potentiellt sett kan ge tillgång till omfattande information om enskilda kan åtgärden också innebära en utökad möjlighet att kartlägga enskildas liv (se prop. 2019/20:64 s. 83 ff.). Hemlig dataavläsning kan alltså leda till betydande integritetsintrång. Samtidigt påverkas graden av integritetsintrång av vilken eller vilka uppgiftstyper som avses och hur verkställigheten av tvångsmedlet utformas. Det ska redan här framhållas att det är omständigheterna i det enskilda fallet som ytterst styr hur stort ett integritetsintrång en viss tvångsmedelsanvändning utgör (se t.ex. *Hemlig rumsavlyssning*, prop. 2005/06:178 s. 43 f. och *Hemliga tvångsmedel mot allvarliga brott*, prop. 2013/14:237 s. 70).

Omfattningen av de integritetskränkningar som hemlig dataavläsning har medfört är inte minst mot denna bakgrund svåra att mäta. Vi kommer i våra integritetsriskanalyser att försöka identifiera både de risker som hemlig dataavläsning kan anses ha medfört samt värdera dessa risker och analysera hur de förhåller sig till de risker som förväntades. Om och hur det kan förhindras att riskerna leder till oönskade konsekvenser behandlas sedan i proportionalitetsavvägningarna i våra överväganden om hur den materiella lagstiftningen bör utformas för att fördelarna med hemlig dataavläsning ska balanseras mot riskerna med detsamma.

Bedömningen om hemlig dataavläsning har inneburit ökade risker för den personliga integriteten gör även vi med utgångspunkt från en jämförelse med vilka andra möjligheter som finns att komma över motsvarande uppgifter (se ovan i avsnitt 5.6.1). Vid bedömningen av

om användning av hemlig dataavläsning innebär risker för enskildas personliga integritet utgår vi från en jämförelse med användningen av permanenta hemliga tvångsmedel (se avsnitt 4.2.1). Dessa hemliga tvångsmedel har utvärderats vid flera tillfällen och då i allt väsentligt ansetts fungera väl samt bedömts uppfylla de krav som uppställs enligt både regeringsformen och Europakonventionen. För en samlad redogörelse av tidigare översyner, se t.ex. delbetänkandet *Utökade möjligheter att använda hemliga tvångsmedel*, SOU 2022:19 s. 404 ff. Vi utgår därmed från att de permanenta hemliga tvångsmedlen fortsatt är nödvändiga och godtagbara ur integritetssynpunkt. Vid integritetsriskanalysen gör vi även en jämförelse med vissa öppna tvångsmedel: beslag, husrannsakan och genomsökning på distans. Anledningen är att dessa åtgärder, trots att de inte räknas till de hemliga tvångsmedlen, till sin natur uppvisar flera likheter med hemlig dataavläsning, inte minst ur integritetsrisksynpunkt. Det kan på goda grunder argumenteras för att integritetsintrånget är större om en omfattande mängd uppgifter hämtas in i hemlighet med stöd av 2 § första stycket 6 och 7 lagen om hemlig dataavläsning, än om det sker med stöd av öppna tvångsmedel. Det skulle samtidigt kunna hävdas att beslag och genomsökning på distans i vissa avseenden kan innebära ett större integritetsintrång än hemlig dataavläsning. Dessa öppna tvångsmedel kan användas vid misstanke om lindrigare brottslighet än hemlig dataavläsning och under vissa förutsättningar utan föregående underrättelse. Vidare saknas för de öppna tvångsmedlen uttryckliga krav på att redan innan beslutet verkställs ta ställning till hur gammal information som verkställande myndighet ska få ta del av. De öppna tvångsmedlen omgärdas inte heller av samma kontrollmekanismer och rättssäkerhetsgarantier som de hemliga tvångsmedlen. För hemlig dataavläsning finns t.ex. särskilda förbudsregler, förbud mot användning av otillåten tilläggsinformation och regler om hur överskottsinformation ska hanteras. Dessa regler syftar till att balansera upp de risker som hemlig dataavläsning annars skulle kunna innebära för den personliga integriteten.

Eftersom hemlig dataavläsning generellt sett innebär ökade risker för den personliga integriteten måste dessa risker vägas särskilt noga mot behov samt nytta och effektivitet. Regeringen har flera gånger uttalat att det integritetsintrång som hemliga tvångsmedel medför kan accepteras, om det belagda behovet och nyttan av de hemliga tvångs-

medlen är tillräckligt stora (se t.ex. skr. 2021/22:79 s. 42). Vi ansluter oss till denna utgångspunkt.

Utöver myndigheternas årliga redovisningar och särskilda beskrivningar som lämnats till utredningen utgör Säkerhets- och integritetsskyddsnämndens tillsynsmaterial om den hittillsvarande tillämpningen av hemlig dataavläsning ett särskilt viktigt underlag vid våra integritetsriskanalyser.

5.9 Proportionalitet och avvägningar mellan intressena

Vi har tidigare i vår framställning redogjort för proportionalitetsprincipen, se avsnitt 4.1.3. En förutsättning för att hemlig dataavläsning ska kunna permanentas är att åtgärden är proportionerlig i förhållande till bl.a. behov, effektivitet och personlig integritet. Även om det konstateras ett fortsatt angeläget samhälleligt behov och en reell nytta måste riskerna för den personliga integriteten minimeras. För att regleringen ska kunna anses ändamålsenlig och proportionerlig måste riskerna därför balanseras med ett tydligt avgränsat tillämpningsområde, tillräckliga kvalifikationskrav, kontrollmekanismer och andra rättssäkerhetsgarantier. Regleringen måste med andra ord utformas så att missbruk förhindras och att ändamålsglidningar mot t.ex. omotiverade kartläggningar eller övervakningar av privatlivet inte kan förekomma.

Verkställighet av hemlig dataavläsning innebär såväl intrång i den tekniska utrustning som åtgärden avser som installation av hård- eller mjukvara i systemet. En proportionalitetsbedömning måste därför göras även i förhållande till de risker för informationssäkerheten som hemlig dataavläsning har inneburit. I betänkandet *Informations- och cybersäkerhet i Sverige – Strategi och åtgärder för säker information i staten*, SOU 2015:23, har informationssäkerhet definierats på följande sätt.

> Informationssäkerhet innebär en strävan att skydda information så att den alltid finns när den behövs (tillgänglighet), att det går att lita på att den är korrekt och inte manipulerad eller förstörd (riktighet), att endast behöriga personer får ta del av den (konfidentialitet) och att det går att följa hur och när informationen har hanterats och kommunicerats (spårbarhet). Informationssäkerhet omfattar såväl administrativa som tekniska åtgärder för att skydda information.

Det kan konstateras att informationssäkerhet har en central plats i samhället. Vikten av en fungerande informationssäkerhet måste därför vägas mot vikten av en effektiv brottsbekämpning. I förarbetena till lagen om hemlig dataavläsning konstaterades att hemlig dataavläsning medför större risker för informationssäkerheten än andra tvångsmedel. En viktig utgångspunkt för våra avvägningar i denna del är att det inte kan accepteras att hemlig dataavläsning leder till minskad informationssäkerhet i någon annan utrustning än den som åtgärden avser. I sådant fall ska hemlig dataavläsning inte tillåtas. Däremot kan det som utgångspunkt accepteras att hemlig dataavläsning innebär minskad informationssäkerhet i den tekniska utrustning som åtgärden avser. Detta förutsätter dock att riskerna balanseras mot en väl avvägd och tydlig reglering. I sammanhanget kan noteras att risker för informationssäkerheten kan, men inte behöver, påverka frågor om risker för den personliga integriteten (se prop. 2019/20:64 s. 90 ff. och 118).

Vid proportionalitetsavvägningen är det särskilt viktigt att noggrant pröva samtliga omständigheter och väga dem som talar för mot dem som talar mot att tillåta hemlig dataavläsning. En grundläggande utgångspunkt bör vara att hemlig dataavläsning för en viss uppgiftstyp endast är proportionerlig om andra åtgärder för att komma åt uppgifterna inte är tillräckliga, skulle vara väsentligt svårare att genomföra än hemlig dataavläsning eller kan förväntas leda till större integritetsintrång än hemlig dataavläsning (se a. prop. s. 110). Som konstaterats kan hemlig dataavläsning potentiellt sett ge tillgång till mycket omfattande information om enskilda. Detta måste självklart beaktas vid proportionalitetsbedömningen. Vi återkommer i våra överväganden därför även till hur proportionaliteten i det enskilda fallet bör beaktas före verkställighet, under inhämtningsfasen samt i bearbetnings- och granskningsfasen.

6 Bör bestämmelserna om hemlig dataavläsning göras permanenta?

6.1 Uppdraget

I detta kapitel behandlar vi den del av uppdraget som avser den övergripande frågan om bestämmelserna om hemlig dataavläsning bör permanentas. I samband med att lagen om hemlig dataavläsning infördes uttalade regeringen följande (se prop. 2019/20:64 s. 100 f.).

> Hemlig dataavläsning kan på goda grunder förväntas vara ett effektivt tvångsmedel i den brottsbekämpande verksamheten, vilket talar för att åtgärden borde införas i permanent lagstiftning. Mot att lagstiftningen görs permanent kan anföras att det rör sig om en ny utredningsmetod som dessutom innebär vissa risker för den personliga integriteten. Många lagar och bestämmelser som rör hemliga tvångsmedel har inledningsvis begränsats i tiden. Sådan tidsbegränsning föreslogs t.ex. i förarbetena till lagen om hemlig rumsavlyssning (prop. 2005/06:178) och lagen om hemlig kameraövervakning (prop. 1995/96:85). Skälet till att lagarna tidsbegränsats har huvudsakligen varit att nya tvångsmedel ger upphov till risker för otillbörliga integritetsintrång, varför ett fördjupat underlag kan behövas inför ett ställningstagande till om lagen i fråga bör permanentas (prop. 2005/06:178 s. 47). Av samma skäl bör därför även den nu föreslagna lagen tidsbegränsas.
>
> Det kan antas att hemlig dataavläsning till en början endast kommer att kunna användas i ett begränsat antal fall. När lagen om hemlig rumsavlyssning infördes begränsades dess giltighetstid till tre år. Vid utvärderingen av buggning och preventiva tvångsmedel (SOU 2009:70) konstaterades att antalet fall av hemlig rumsavlyssning var så få att det inte utifrån dessa gick att dra några säkra slutsatser om tvångsmedlets effektivitet eller praktiska värde. Regeringen bedömer att det finns risk för att tre års giltighetstid för lagen om hemlig dataavläsning skulle leda till samma resultat. Lagen bör därför, som utredningen föreslår, gälla i fem år från dess införande. En senare utvärdering av den tidsbegränsade lagen minimerar enligt regeringens mening risken för att lagen görs perma-

> nent utan ett fullgott underlag, vilket är en farhåga som framförs av Svenska advokatsamfundet, Internetstiftelsen och Svenska Journalistförbundet. Vid en framtida utvärdering och beredning kommer nyttan, behovet och proportionaliteten av hemlig dataavläsning återigen att analyseras och bedömas.

Även Lagrådet framhöll i sitt yttrande över lagförslaget vikten av att det sker ingående utvärdering av behovet, nyttan och proportionaliteten innan det fattas beslut om lagstiftningen ska förlängas eller permanentas (se prop. 2019/20:64 s. 316 f.).

Frågan om bestämmelserna om hemlig dataavläsning bör permanentas innefattar inledande analyser av nyttan och behovet av hemlig dataavläsning, vilket i sin tur kräver inledande avvägningar mot integritetsintresset. Fortsatta sådana analyser och avvägningar gör vi i kapitel 7 och 8, i direkt anslutning till våra ställningstaganden om lagstiftningens utformning. Här återkommer vi även till analyser och avvägningar mot de risker för informationssäkerheten som hemlig dataavläsning innebär. I kapitel 9 behandlar vi frågan om var bestämmelserna rent lagtekniskt bör placeras.

6.2 Förväntningarna på hemlig dataavläsning och den hittillsvarande tillämpningen

6.2.1 Ett efterfrågat verktyg i kampen mot allvarlig brottslighet

Lagen om hemlig dataavläsning infördes den 1 april 2020 som en särskild och tidsbegränsad lag. Vid införandet av den nya lagen var hemlig dataavläsning ett sedan länge efterfrågat verktyg i kampen mot allvarlig brottslighet. Hemlig dataavläsning infördes som ett komplement till övriga hemliga tvångsmedel för att effektivisera brottsbekämpningen och för att återställa de brottsbekämpande myndigheternas förmåga att inhämta och ta del av information. Bestämmelserna om hemlig dataavläsning utformades med samma höga kvalifikationskrav som då befintliga hemliga tvångsmedel. Hemlig dataavläsning under förundersökning har, precis som andra hemliga tvångsmedel under förundersökning, framför allt använts i ärenden rörande narkotikabrottslighet och våldsbrott (se tabell 6.1–6.2 och 6.4–6.5). När det gäller Säkerhetspolisens användning av hemlig dataavläsning och andra hemliga tvångsmedel särredovisas denna (se avsnitt 5.7.1). Vi

redogör i avsnitten 6.3.3–6.3.5 separat för användningen av hemlig dataavläsning och andra hemliga tvångsmedel utanför förundersökning.

Vid införandet av den nya lagen uppskattades att hemlig dataavläsning inte skulle kunna användas i alla ärenden där det fanns behov av åtgärden. Som huvudsakligt skäl till den bedömningen anfördes det omfattande förberedelsearbete och de tekniska svårigheter som verkställighet av hemlig dataavläsning innebär. Hemlig dataavläsning är dessutom mycket resurskrävande. Räknat i antal verkställda tillstånd bedömdes tillämpningen av hemlig dataavläsning, åtminstone till en början, bli jämförbar med tillämpningen av hemlig rumsavlyssning. Bedömningen byggde på en försiktig uppskattning som vid tidpunkten naturligtvis var svår att göra. Förväntningarna på hemlig dataavläsning var att verktyget, i de fall där det kunde användas, skulle ge betydligt bättre tillgång till information än då befintliga hemliga tvångsmedel. Hemlig dataavläsning bedömdes i dessa fall bli ett effektivt tvångsmedel i den brottsbekämpande verksamheten (se prop. 2019/20:64 s. 81 f.).

6.2.2 Hemlig dataavläsning bedömdes innebära vissa risker för den personliga integriteten

Vid införandet av den nya lagen konstaterades att det fanns ett påtagligt behov av hemlig dataavläsning, när informationen inte är åtkomlig genom traditionella hemliga tvångsmedel. Samtidigt bedömdes hemlig dataavläsning i flera avseenden innebära ökade risker för enskildas personliga integritet. Eftersom det var fråga om ett helt nytt och oprövat tvångsmedel fanns goda skäl att inte underskatta integritetsriskerna. När det gäller de enskilda uppgiftstyperna bedömdes hemlig dataavläsning avseende de sekundära uppgiftstyperna i 2 § första stycket 6 och 7 lagen om hemlig dataavläsning innebära en ökad risk för den personliga integriteten. Hemlig dataavläsning avseende platsuppgifter enligt 2 § första stycket 3 samma lag bedömdes medföra en viss ökad risk för den personliga integriteten. Hemlig dataavläsning avseende övriga uppgiftstyper bedömdes inte medföra någon beaktansvärd ökad risk för den personliga integriteten. Själva verkställighetsmetoden ansågs i sig kunna innebära en viss ökad risk (se SOU 2017:89 s. 301 ff. och a. prop. s. 83 ff.). Den omständigheten att hemlig dataavläsning potentiellt skulle kunna användas till långtgående kartläggningar och övervakningar av den som åtgärden riktas

mot bedömdes bidra till en allvarligt ökad risk för integritetsintrång (se a. SOU s. 306 och a. prop. s. 92). Dessa förväntade risker valde lagstiftaren att balansera genom en differentiering av de olika uppgiftstyperna redan vid tillståndsgivningen. Vidare valde lagstiftaren att ansluta utformningen av bestämmelserna till reglering avseende traditionella och beprövade hemliga tvångsmedel, med motsvarande höga kvalifikationskrav, kontrollmekanismer och rättssäkerhetsgarantier.

Eftersom närmare detaljer i fråga om bl.a. integritetsintrång är svåra att bedöma på förhand begränsades lagstiftningen om hemlig dataavläsning, till en början och inför en kommande utvärdering, till att gälla under fem år.

6.2.3 Hemlig dataavläsning har använts i större utsträckning än förväntat

De brottsbekämpande myndigheterna har nu haft möjlighet att använda hemlig dataavläsning i drygt 3,5 år. Det kan konstateras att hemlig dataavläsning har använts i större utsträckning än förväntat, såväl under förundersökning som i underrättelseverksamhet (se avsnitt 6.3.1 och 6.3.3–6.3.5). Utanför Säkerhetspolisens verksamhet har hemlig dataavläsning i inhämtningslagsfallen använts mer sällan och i preventivlagsfallen inte alls (t.o.m. 2022). När det gäller användningen av hemlig dataavläsning vid särskild utlänningskontroll redovisas dessa siffor inte öppet (se avsnitt 6.3.4 och 6.3.5).

De kvantitativa förväntningarna på hemlig dataavläsning byggde som angetts på en prognos som vid tidpunkten var svår att göra. Det kan därför vara mer intressant att notera att antalet tillstånd till hemlig dataavläsning har ökat för varje år (tabell 6.1–6.2 och 6.21). En orsak till att hemlig dataavläsning har använts i allt större utsträckning är de brottsbekämpande myndigheternas ökande förmåga att överbrygga de tekniska svårigheter som förutspåddes. En annan förklaring är de senaste årens stegrande brottsutveckling. Även om kvalifikationskraven för att tillämpa hemlig dataavläsning är höga, har brottsutvecklingen i sig lett till ett utökat användningsområde för hemlig dataavläsning.

6.2.4 Hemlig dataavläsning har använts i ett begränsat antal fall och mot få personer

Hemlig dataavläsning har både i absoluta tal och jämfört med andra hemliga tvångsmedel använts i ett begränsat antal fall. Tillstånden till hemlig dataavläsning har i jämförelse med andra hemliga tvångsmedel inte heller riktats mot något stort antal personer (se tabell 6.1–6.2 och 6.4–6.5). I vilken utsträckning som hemlig dataavläsning har använts i jämförelse med öppna tvångsmedel eller andra metoder för informationsinhämtning går inte med någon säkerhet att uttala sig om eftersom det inte sker någon redovisning av den användningen. Användningen av ett hemligt tvångsmedel med så höga kvalifikationskrav som hemlig dataavläsning bör dock rimligtvis, i jämförelse med användningen av flertalet andra utredningsmetoder, vara begränsad.

Eftersom kvalifikationskraven för hemlig dataavläsning ansluter till vad som gäller för permanenta hemliga tvångsmedel, ska åtgärden ha riktats mot personer där det finns konkreta misstankar om koppling till viss allvarlig brottslighet eller brottslig verksamhet. Hemlig dataavläsning har med andra ord riktats mot samma personkrets som andra hemliga tvångsmedel.

6.2.5 Hemlig dataavläsning har regelmässigt använts avseende flera uppgiftstyper samtidigt

Hemlig dataavläsning har under förundersökning regelmässigt använts avseende flera uppgiftstyper samtidigt. Tillstånd till uppgiftstyperna i 2 § första stycket 1–3 samt 6 och 7 har varit vanligast, medan tillstånd till uppgiftstyperna i punkt 4–5 samma bestämmelse har varit sällsynta (se tabell 6.2). Enligt företrädare för de brottsbekämpande myndigheterna har tillämpningen av de olika uppgiftstyperna utanför förundersökning sett ut på motsvarande sätt, med den anmärkningen att hemlig dataavläsning avseende rumsavlyssningsuppgifter inte är tillåtet utanför förundersökning.

Ett skäl till att ansöka om hemlig dataavläsning för flera uppgiftstyper är att det ofta är svårt att i förväg avgöra vilken typ av uppgifter som kan vara av vikt för den enskilda utredningen. Ett annat skäl är att det inte alltid är givet hur lagstiftningens kategorisering av olika uppgiftstyper ska appliceras på de uppgifter som kan komma att påträffas i ett enskilt fall. Vissa av uppgiftstyperna överlappar dessutom

varandra. En differentiering av uppgiftstyperna redan vid tillståndsgivningen är därför ofta svår att göra. Det ska understrykas att problematiken inte ligger i att det saknas möjlighet att anpassa tekniken efter tillståndet. Problemen hänför sig till svårigheterna med att förutse var i informationssystemet som den eftersökta information kan komma att anträffas och de överlappningar som finns beträffande vissa uppgiftstyper. Uppgifter i en elektronisk kommunikationsutrustning kan vara betydligt svårare att överblicka än uppgifter i fysiska dokument. En mobiltelefon, en surfplatta eller en dator är exempel på informationsbärare som kan innehålla en stor mängd information. Informationen kan i sin tur vara av vitt skilda slag. Det kan handla om realtidsuppgifter eller information som finns lagrad i komplexa mappstrukturer och olika applikationer eller samlade på annat sätt. Vissa uppgifter blir synliga först när en fil eller applikation öppnas. Ett praktiskt exempel är hemlig dataavläsning av en mobiltelefon i syfte att eftersöka information om viss narkotikabrottslighet. Vid en sådan dataavläsning kan relevant information komma att anträffas i eller om meddelanden, men även i form av t.ex. skärmbilder eller fotografier på narkotika som i sin tur innehåller metadata om tid och plats. Även information om hur telefonen används kan vara relevant. Uppgifter om meddelanden och innehåll i meddelanden som skickas eller har skickats är att hänföra till uppgiftstyperna i punkterna 1 och 2. Utkast till meddelanden är dock att anse som punkt 6-uppgifter. En skärmbild av ett skickat meddelande kan utgöra en punkt 6-uppgift, men bara om uppgiften inte kan läsas av med stöd av punkt 1–3 eftersom tillämpningen av punkt 6 är sekundär i förhållande till dessa punkter. Det är många gånger svårt att avgöra om en uppgift ska kategoriseras under punkt 6 eller punkt 7, eftersom det kan vara en slump huruvida en uppgift som visar hur ett avläsningsbart informationssystem används lagras eller inte. Platsuppgifter, även i form av metadata, är att betrakta som punkt 3-uppgifter. Samma typ av information kan alltså, både genom slump och beroende på hur den berörde hanterar uppgiften i informationssystemet, komma att sortera under olika uppgiftstyper. Det innebär också att ett tillstånd till hemlig dataavläsning som begränsats till vissa utgiftstyper eller till information som lagrats under viss tid kan få mindre räckvidd än avsett om användaren av det informationssystem som ska avläsas har lagrat information på visst sätt eller manipulerat tidsmarkörer. Det sagda illustrerar varför ett tillstånd till hemlig dataavläsning ofta måste omfatta

flera uppgiftstyper för att åtgärden ska bli ändamålsenlig. Brottsbekämpande myndigheter riskerar annars att antingen missa relevant information eller att denna kan komma att betraktas som otillåten tilläggsinformation enligt 23 § lagen om hemlig dataavläsning.

Företrädare för de brottsbekämpande myndigheterna har därför framhållit att själva syftet med hemlig dataavläsning kan komma att motverkas om inhämtningen begränsas för mycket redan i inhämtningsfasen. Med hänsyn till hur mycket information som potentiellt skulle kunna inhämtas har samtidigt framhållits att det alltid sker en begränsning redan i inhämtningsfasen i den mån det är möjligt och ändamålsenligt. Utöver proportionalitetsaspekten talar även resurs- och effektivitetsskäl för en sådan begränsning. Den stora sållningen av information har i praktiken dock skett efter inhämtningsfasen, i bearbetnings- och granskningsfasen.

Vi återkommer i avsnitt 7.3 till den övergripande frågan om vilka uppgifter som ska kunna hämtas in genom hemlig dataavläsning och i avsnitt 8.4.4 till frågan om under vilken tidsperiod ett tillstånd ska få verkställas och om uppgifter som lagrats före denna tidsperiod ska omfattas av tillståndet.

6.2.6 Hemlig dataavläsning föregås oftast av ett annat hemligt tvångsmedel

Utöver antalet uppgiftstyper är det intressant att titta på hur den samlade tvångsmedelsanvändningen har sett ut. Någon samlad kartläggning går emellertid inte att utläsa av myndigheternas årliga redovisningar. Företrädare för de brottsbekämpande myndigheterna har dock till utredningen uppgett att hemlig dataavläsning i praktiken ofta har använts först efter att ett annat hemligt tvångsmedel har verkställts. I det typiska ärendet har behovet av hemlig dataavläsning framkommit vid verkställighet av en hemlig avlyssning av elektronisk kommunikation. I regel är det först efter att det bedömts föreligga tekniska förutsättningar för hemlig dataavläsning som den brottsbekämpande myndigheten har valt att gå vidare med en ansökan om tillstånd till en sådan åtgärd.

6.2.7 Tillståndstider och villkor i tillstånd till hemlig dataavläsning

Tillståndstiderna i realtid har för hemlig dataavläsning varit kortare än för övriga hemliga tvångsmedel (se tabell 6.6). När det gäller inhämtning av historiska uppgifter saknas jämförelsematerial eftersom övriga hemliga tvångsmedel, förutom HÖK, i princip inte kan användas för detta ändamål. När det gäller hemlig dataavläsning finns i likhet med öppna tvångsmedel och HÖK inte någon lagstadgad bortre gräns för inhämtning av historiska uppgifter, dvs. lagrad information. Beträffande lagrad information har det vid hemlig dataavläsning förekommit långa tillståndstider (se Säkerhets- och integritetsskyddsnämndens uttalande med beslut av den 15 december 2021, dnr 92-2020, s. 9 f.). I några fall har myndigheterna fått tillstånd att hämta in flera år gammal information genom hemlig dataavläsning.

Förekomsten av och innehållet i de villkor som ett tillstånd till hemlig dataavläsning ska förenas med redovisas inte i myndigheternas årliga skrivelser. Säkerhets- och integritetsskyddsnämnden (SIN) fann i en tidig första granskning att det har förekommit tillstånd till hemlig dataavläsning som saknat obligatoriska villkor för tvångsmedelsanvändningen (se t.ex. a. uttalande s. 11 f.). SIN har därefter under 2022 inlett en granskning om villkorskravet vid användningen av hemlig dataavläsning. Vi återkommer i avsnitt 8.4.5 till dessa granskningar.

6.2.8 Vilken nytta har hemlig dataavläsning inneburit?

De brottsbekämpande myndigheterna sammanställer varje år en redovisning om användningen av hemliga tvångsmedel. Nyttan av vissa hemliga tvångsmedel redovisas i form av vilka specifika resultat – effekter – användningen av åtgärden inneburit under föregående år. Nyttan redovisas i antal brottsmisstankar och andelstal (det procenttal där åtgärden har gett viss effekt) jämte anonymiserade exempel från tillämpningen. Redovisningen omfattar det antal brottsmisstankar där förundersökning, såvitt avser den brottsmisstanke för vilket det aktuella tvångsmedlet har beviljats, antingen lagts ner eller gått till åtal under föregående år (se avsnitt 5.7.1). Av de årliga redovisningarna kan konstateras att den kvantitativt uppskattade nyttan av hemlig dataavläsning generellt sett har varit något lägre än för de permanenta hemliga tvångsmedlen. Det förekommer också relativt sett stora varia-

tioner avseende såväl vilken typ av effekt som avses som vilken uppgiftstyp som jämförs, se avsnitt 6.3.2 och tabell 6.10–6.20. Samtidigt visar uppgifter som företrädare för de brottsbekämpande myndigheterna har lämnat till utredningen att de kvalitativa effekterna av hemlig dataavläsning har varit mycket positiva. I avsnitt 6.4 presenteras flera anonymiserade exempel där hemlig dataavläsning har använts för att hämta in avgörande information som inte varit åtkomlig genom andra tvångsmedel.

Skillnaderna i redovisad nytta kan ha flera förklaringar. I avsnitt 5.7.1 har vi förklarat varför kvantitativa uppgifter i sig är ett trubbigt instrument när de används för att mäta nyttan av ett hemligt tvångsmedel. Även mot bakgrund av hur själva nyttoredovisningen av hemlig dataavläsning sker finns särskild anledning att bedöma de redovisade resultaten med viss försiktighet.

Den redovisade nyttan bygger helt på subjektiva uppskattningar gjorda av den åklagare som varit förundersökningsledare i det aktuella ärendet. Redovisningen går till på sätt att åklagaren, först efter att åtal väckts eller förundersökningen lagts ner, fyller i en blankett och uppskattar om och i så fall vilken effekt som ett visst tvångsmedel gett. Beträffande hemlig dataavläsning har ansvarig åklagare därtill att uppskatta vilken uppgiftstyp som har lett till en viss effekt. Även kvantitativt jämförande analyser måste betraktas som osäkra. Det ligger i sakens natur att det allmänt sett är vanskligt att jämföra ett nytt hemligt tvångsmedel med permanenta och beprövade sådana. Vanligen är verkställigheten av hemlig dataavläsning av olika orsaker förenad med större svårigheter än verkställighet av andra tvångsmedel. Hemlig dataavläsning kräver ett omfattande förberedelsearbete och tekniska svårigheter kan uppstå inför och under verkställigheten. Antalet redovisade tillstånd till hemlig dataavläsning motsvarar därför inte antalet verkställda tillstånd. Den redovisade kvantitativa nyttan av hemlig dataavläsning är därför lägre än den faktiska nyttan.

Med dessa anmärkningar går vi över till en redogörelse för myndigheternas årliga redovisningar om användningen av hemliga tvångsmedel under åren 2020–2022. I de redovisningarna används genomgående förkortningarna HAK (hemlig avlyssning av elektronisk kommunikation), HÖK (hemlig övervakning av elektronisk kommunikation), HKÖ (hemlig kameraövervakning), HRA (hemlig rumsavlyssning) och HDA (hemlig dataavläsning). I vår framställning nedan använder vi oss därför också av dessa förkortningar.

6.3 Myndigheternas redovisningar om användningen av hemliga tvångsmedel åren 2020–2022

6.3.1 Kvantitativa uppgifter om användningen under förundersökning

I detta avsnitt redogör vi för de kvantitativa uppgifter som jämte nyttoredovisningen har redovisats avseende tillämpningen av HDA under förundersökning åren 2020–2022. Härmed avses uppgifter om antalet redovisade tillstånd, antalet personer som har varit föremål för HDA, tvångsmedlets varaktighet, antalet avslag i domstol samt antalet interimistiska beslut. Parallellt och i jämförande syfte redogör vi även för de motsvarande kvantitativa uppgifter som redovisats beträffande tillämpningen av HAK, HÖK, HKÖ och HRA enligt rättegångsbalken under samma period. Kvantitativa uppgifter om Säkerhetspolisens användning av hemliga tvångsmedel särredovisas i avsnitt 6.3.3 nedan.

Antalet tillstånd

Inledning

Med antalet tillstånd till HDA avses det antal tillstånd som under förundersökning har meddelats beträffande olika elektroniska informationssystem. Ett beslut av domstol kan innefatta flera tillstånd. Exempelvis räknas ett domstolsbeslut om tillstånd till HDA avseende en misstänkt och två olika elektroniska informationssystem som två tillstånd i statistiken. Ett förlängt tillstånd räknas som ett nytt tillstånd. Med antalet redovisade tillstånd till HAK, HÖK, HKÖ eller HRA avses det antal tillstånd som under förundersökning har meddelats beträffande olika teleadresser eller andra adresser. Exempelvis räknas ett domstolsbeslut om tillstånd till HAK avseende en misstänkt och fyra olika teleadresser som fyra tillstånd. Samma person kan alltså vara föremål för flera tillstånd om han eller hon använder sig av flera olika adresser eller elektroniska informationssystem eller om han eller hon är misstänkt för flera brott.

Antalet redovisade tillstånd

Under 2022 gavs 649 tillstånd till HDA. Motsvarande siffra för 2021 var 589 och under de nio månader som HDA kunde användas under 2020 gavs 306 tillstånd till HDA. Mellan år 2021 och 2022 ökade alltså antalet tillstånd till HDA med cirka tio procent.

Historiskt sett har antalet tillstånd till HAK och HÖK ökat från år till år. År 2020 gavs 5 072 tillstånd till HAK och 13 497 tillstånd till HÖK. Året efter bröts den ökande trenden. Då gavs 3 926 tillstånd till HAK och 12 989 tillstånd till HÖK. År 2022 gavs 4 108 tillstånd till HAK och 13 146 tillstånd till HÖK. Som förklaring till den markanta minskningen av antalet tillstånd till HAK (och därmed även det minskade antalet avlyssnade personer) under 2021 har de redovisande myndigheterna anfört huvudsakligen följande. En sannolik förklaring är att många utredningar har byggt på information från de krypterade tjänsterna Encrochat, Sky ECC och Anom, som kommit myndigheterna tillhanda genom internationellt rättsligt samarbete. Genom information från dessa tjänster har kommunikation kunnat säkras och behovet av HAK kan därför ha minskat tillfälligt. Att minskningen varit särskilt markant gällande brottstyperna narkotikabrott och narkotikasmuggling samt våldsbrott talar i samma riktning, då den absoluta merparten av utredningar som byggt på material från de krypterade tjänsterna har rört den typen av brottslighet. När det gäller minskningen avseende antalet tillstånd till HÖK under 2021 har de redovisande myndigheterna anfört att denna relativt sett är mindre eftersom den skett från historiskt höga nivåer. Det stora antalet tillstånd förklaras med att de misstänkta ofta byter telefoner eller telefonnummer. Minskningen var troligtvis tillfällig och helt orelaterad till att HDA under samma period infördes som ett nytt hemligt tvångsmedel.

Antalet tillstånd till HKÖ och HRA har historiskt sett och över tid varit relativt få. År 2020 gavs 211 tillstånd till HKÖ och 2021 var motsvarande siffra 242. Under 2022 gavs 239 tillstånd till HKÖ. Under perioden 2017–2019 varierade antalet tillstånd till HKÖ mellan 131 och 153. Under 2020 gavs 135 tillstånd till HRA och 2021 var motsvarande siffra 166. Under 2022 gavs 79 tillstånd till HRA. Under perioden 2017–2019 varierade antalet tillstånd till HRA mellan 77 och 130.

Antalet redovisade tillstånd fördelade på brottstyp

Av tabell 6.1 framgår att HDA till övervägande del har använts under förundersökningar om narkotikabrottslighet och våldsbrott. Detta motsvarar hur användningen av HAK, HÖK, HKÖ och HRA har sett under samma period, och även historiskt.

Tabell 6.1 Antalet tillstånd fördelat på brottstyp

Antalet tillstånd (procentuell fördelning inom parentes)

	Narkotika-brott	Våldsbrott	Sexualbrott m.m.	Tillgrepps-brott	Ekonomiska brott	Övriga brott
2022						
HDA	**376 (58 %)**	**151 (23 %)**	**43 (7 %)**	**1 (0 %)**	**18 (3 %)**	**60 (9 %)**
HAK	1 875 (46 %)	1 406 (34 %)	39 (1 %)	15 (0 %)	167 (4 %)	606 (15 %)
HÖK	2 593 (20 %)	7 278 (55 %)	149 (1 %)	579 (4 %)	516 (4 %)	2 031 (16 %)
HKÖ	162 (68 %)	36 (15 %)	8 (3 %)	3 (1 %)	2 (1 %)	28 (12 %)
HRA	44 (56 %)	29 (37 %)	0 (0 %)	0 (0 %)	0 (0 %)	6 (7 %)
2021						
HDA	**343 (58 %)**	**123 (21 %)**	**12 (2 %)**	**0 (0 %)**	**35 (6 %)**	**76 (13 %)**
HAK	2 017 (51 %)	1 223 (31 %)	69 (2 %)	26 (1 %)	182 (5 %)	409 (10 %)
HÖK	3 375 (26 %)	6 651 (51 %)	191 (1 %)	788 (6 %)	451 (3 %)	1 533 (12 %)
HKÖ	133 (55 %)	57 (24 %)	6 (2 %)	5 (2 %)	10 (4 %)	31 (13 %)
HRA	82 (49 %)	76 (46 %)	0 (0 %)	0 (0 %)	0 (0 %)	8 (5 %)
2020						
HDA	**127 (41 %)**	**138 (45 %)**	**14 (5 %)**	**0 (0 %)**	**11 (4 %)**	**16 (5 %)**
HAK	2 317 (46 %)	1 881 (37 %)	91 (2 %)	21 (0,5 %)	95 (2 %)	667 (13 %)
HÖK	2 849 (21 %)	7 357 (55 %)	175 (1 %)	871 (6 %)	433 (3 %)	1 812 (14 %)
HKÖ	129 (61 %)	50 (24 %)	1 (1 %)	0 (0 %)	2 (1 %)	29 (13 %)
HRA	61 (45 %)	70 (52 %)	0 (0 %)	0 (0 %)	0 (0 %)	4 (3 %)

Källa: Åklagarmyndighetens redovisningar av användningen av vissa hemliga tvångsmedel under 2020–2022 (publicerade i maj år 2021, 2022 respektive 2023).

Antalet redovisade tillstånd fördelade på uppgiftstyp

Av tabell 6.2 framgår att HDA oftast har beviljats för såväl avlyssningsuppgifter (1 p), övervakningsuppgifter (2 p), platsuppgifter (3 p) som elektroniskt lagrade uppgifter (6 p) och övriga uppgifter som visar hur viss teknisk utrustning används (7 p). De brottsbekämpande myndigheterna har alltså regelmässigt fått tillstånd till att ta del av upp-

giftstyperna i punkt 6 och 7 i samband med att de fått tillstånd till att ta del av uppgiftstyperna i punkt 1–3.

Av samma tabell framgår också att tillstånd till HDA som omfattar kameraövervaknings- och rumsavlyssningsuppgifter (4 och 5 p), har varit sällsynta. Detta gäller även de tillstånd till HDA som har meddelats på begäran av utländsk myndighet, se tabell 6.3. Det ska framhållas att såväl antalet tillstånd till HDA som till andra hemliga tvångsmedel med anledning av internationell rättslig hjälp har varit relativt få. Med detta i beaktande kan noteras att det inte har förekommit något beviljat tillstånd till HDA beträffande kameraövervakningsuppgifter på begäran av utländsk myndighet. Det kan samtidigt noteras att det under motsvarande period inte heller förekommit hemlig kameraövervakning på begäran av annat land. Senast detta förekom var år 2016 (se Redovisning av användningen av vissa hemliga tvångsmedel under 2016, Åklagarmyndigheten, ÅM 2016-308, maj 2017, s. 28). Eventuella avslag framgår inte av de statistiska uppgifterna. År 2020 meddelades på begäran av utländsk myndighet tre tillstånd till HDA avseende rumsavlyssningsuppgifter. Härutöver har tillstånd till HDA avseende denna uppgiftstyp inte förekommit. Även hemlig rumsavlyssning på begäran av utländsk myndighet är sällsynt.

Uppgifterna i tabellen bekräftar vad Säkerhets- och integritetsskyddsnämnden (SIN) kom fram till i sin första särskilda granskning av tillämpningen av hemlig dataavläsning (se nämndens uttalande med beslut av den 15 december 2021, dnr 92-2020, s. 7).

Tabell 6.2 Antalet tillstånd till HDA fördelade på brottstyp och uppgiftstyp

Avser tillämpningen år 2022 (2021 och 2020 inom parentes)

HDA 2 § 1 st.	Narkotika-brott	Våldsbrott	Sexualbrott m.m.	Tillgrepps-brott	Ekonomiska brott	Övriga brott
1 p.						
2022	373	149	40	1	18	60
(2021)	(333)	(117)	(12)	(0)	(35)	(73)
(2020)	(117)	(97)	(9)	(0)	(9)	(14)
2 p.						
2022	370	150	40	0	18	60
(2021)	(329)	(113)	(6)	(0)	(20)	(73)
(2020)	(118)	(97)	(9)	(0)	(11)	(14)
3 p.						
2022	356	149	40	0	16	56
(2021)	(327)	(108)	(4)	(0)	(20)	(73)
(2020)	(116)	(97)	(4)	(0)	(5)	(14)
4 p.						
2022	3	2	0	0	0	0
(2021)	(0)	(0)	(2)	(0)	(0)	(2)
(2020)	(0)	(8)	(0)	(0)	(3)	(0)
5 p.						
2022	6	2	0	0	2	0
(2021)	(25)	(8)	(1)	(0)	(0)	(1)
(2020)	(4)	(30)	(0)	(0)	(0)	(1)
6 p.						
2022	356	147	43	0	18	58
(2021)	(336)	(117)	(4)	(0)	(20)	(72)
(2020)	(114)	(93)	(14)	(0)	(9)	(14)
7 p.						
2022	356	146	40	0	18	58
(2021)	(329)	(113)	(3)	(0)	(20)	(73)
(2020)	(107)	(91)	(13)	(0)	(9)	(14)

Källa: Åklagarmyndighetens redovisningar av användningen av vissa hemliga tvångsmedel under 2020–2022 (publicerade i maj år 2021, 2022 respektive 2023).

Antalet redovisade tillstånd m.a.a. internationell rättslig hjälp

Härutöver har HDA även använts efter en begäran om internationell rättslig hjälp i brottmål eller en europeisk utredningsorder. För 2022 redovisades fem tillstånd till HDA i detta avseende. Dessa tillstånd riktades i sin tur mot sammanlagt tre personer. Motsvarande siffror för 2021 var 14 tillstånd och fyra personer. Avseende år 2020 redo-

visades 20 tillstånd avseende elva personer. Av tabell 6.3 framgår hur tillstånden har fördelat sig mellan de olika uppgiftstyperna, jämfört med antalet redovisade tillstånd och personer avseende HAK, HÖK, HKÖ och HRA i samma avseende. Såväl antalet tillstånd till HDA som till andra hemliga tvångsmedel har varit relativt få. Enskilda ärenden kan därmed få ett stort genomslag i statistiken. Exempelvis riktades HRA år 2021 mot nio misstänkta personer vid sammanlagt 49 tillstånd. Av dessa tillstånd lämnades 48 i samma ärende.

Tabell 6.3 Hemliga tvångsmedel på begäran av utländsk myndighet

Avser antalet tillstånd (antalet personer inom parentes)

	Antal tillstånd (personer) m.a.a. internationell rättslig hjälp		
HDA 2 § 1 st.	**2020**	**2021**	**2022**
1 p. Avlyssningsuppgifter	20 (11)	14 (4)	5 (3)
2 p. Övervakningsuppgifter	20 (11)	14 (4)	5 (3)
3 p. Platsuppgifter	20 (11)	14 (4)	5 (3)
4 p. Kameraövervakningsuppgifter	0 (0)	0 (0)	0 (0)
5 p. Rumsavlyssningsuppgifter	3 (2)	0 (0)	0 (0)
6 p. Övriga lagrade uppgifter	20 (11)	14 (4)	5 (3)
7 p. Övriga användningsuppgifter	20 (11)	14 (4)	5 (3)
HAK	20 (10)	62 (24)	36 (11)
HÖK	132 (35)	126 (37)	207 (80)
HKÖ	0 (0)	0 (0)	3 (2)
HRA	1 (1)	49 (9)	7 (5)

Källa: Åklagarmyndighetens redovisningar av användningen av vissa hemliga tvångsmedel under 2020–2022 (publicerade i maj år 2021, 2022 respektive 2023).

Antalet personer

Inledning

Antalet personer som har varit föremål för ett hemligt tvångsmedel under förundersökning redovisas uppdelat på respektive tvångsmedel. En person kan ha varit föremål för flera olika hemliga tvångsmedel och räknas i så fall flera gånger. En sammanräkning av antalet personer som redovisas för vart och ett av de olika tvångsmedlen ger därför inte en korrekt bild av hur många individer som totalt sett har varit föremål för hemliga tvångsmedel. Samma person kan också ha varit föremål för hemliga tvångsmedel med anledning av flera olika

brottstyper. Eftersom redovisningen sker uppdelat per brottstyp är det totala antalet individer som varit föremål för respektive hemligt tvångsmedel sannolikt lägre än redovisat.

Antalet redovisade personer som varit föremål för hemliga tvångsmedel

Enligt redovisningen riktades HDA år 2022 mot sammanlagt 365 personer, vilket motsvarar en ökning med cirka 17 procent jämfört med föregående år. År 2021 riktades HDA mot 311 personer och motsvarande siffra för år 2020 (april-december) var 170 personer.

Historiskt sett har antalet personer som varit föremål för HAK ökat från år till år fram till år 2020 då 1 704 personer var föremål för HAK. Året efter var motsvarande siffra 1 384 och år 2022 var 1 465 personer föremål för HAK. Även antalet personer som varit föremål för HÖK har ökat i princip varje år fram till år 2020. Detta år var 3 490 personer föremål för HÖK. År 2021 var motsvarande siffra 3 310 och år 2022 var 3 314 personer föremål för HÖK. Under 2020 var 212 personer föremål för HKÖ. Motsvarande siffra för 2021 var 235 och år 2022 var 250 personer föremål för HKÖ. Under 2020 användes HRA mot 80 personer. Motsvarande siffra för 2021 var 79 och år 2022 var 60 personer föremål för HRA.

Antalet redovisade personer fördelade på brotts- och uppgiftstyp

När det gäller redovisningen av det totala antalet personer som har varit föremål för HDA respektive HAK, HÖK, HKÖ och HRA framgår av tabell 6.4 hur dessa fördelar sig på de olika brottstyperna. Av uppgifterna framgår att HDA framför allt har använts i ärenden rörande narkotikabrottslighet och våldsbrott. Detta motsvarar hur fördelningen under samma period, och även historiskt, har sett ut beträffande tillämpningen av HAK, HÖK, HKÖ och HRA enligt rättegångsbalken.

Tabell 6.4 Antalet personer fördelade på brottstyp

Avser antalet personer (procentuell fördelning inom parentes)

	Narkotika-brott	Våldsbrott	Sexualbrott m.m.	Tillgrepps-brott	Ekonomiska brott	Övriga brott
2022						
HDA	**184 (50 %)**	**88 (24 %)**	**31 (9 %)**	**1 (0 %)**	**12 (3 %)**	**49 (14 %)**
HAK	635 (43 %)	500 (34 %)	16 (1 %)	11 (1 %)	45 (3 %)	258 (18 %)
HÖK	859 (26 %)	1 375 (41 %)	41 (1 %)	230 (7 %)	153 (5 %)	656 (20 %)
HKÖ	177 (71 %)	37 (15 %)	8 (3 %)	2 (1 %)	2 (1 %)	24 (9 %)
HRA	32 (53 %)	22 (37 %)	0 (0 %)	0 (0 %)	0 (0 %)	6 (10 %)
2021						
HDA	**148 (48 %)**	**88 (28 %)**	**10 (3 %)**	**0 (0 %)**	**15 (5 %)**	**50 (16 %)**
HAK	663 (48 %)	452 (33 %)	30 (2 %)	10 (1 %)	61 (4 %)	168 (12 %)
HÖK	989 (30 %)	1 314 (40 %)	81 (2 %)	276 (8 %)	152 (5 %)	498 (15 %)
HKÖ	133 (57 %)	44 (19 %)	6 (2 %)	8 (3 %)	13 (6 %)	31 (13 %)
HRA	36 (46 %)	38 (48 %)	0 (0 %)	0 (0 %)	0 (0 %)	5 (6 %)
2020						
HDA	**87 (51 %)**	**52 (31 %)**	**9 (5 %)**	**0 (0 %)**	**9 (5 %)**	**13 (8 %)**
HAK	744 (44 %)	614 (36 %)	30 (2 %)	14 (1 %)	38 (2 %)	264 (15 %)
HÖK	979 (28 %)	1454 (42 %)	61 (2 %)	322 (9 %)	149 (4 %)	525 (15 %)
HKÖ	130 (61 %)	52 (25 %)	1 (1 %)	0 (0 %)	2 (1 %)	27 (12 %)
HRA	41 (51 %)	37 (46 %)	0 (0 %)	0 (0 %)	0 (0 %)	2 (3 %)

Källa: Åklagarmyndighetens redovisningar av användningen av vissa hemliga tvångsmedel under 2020–2022 (publicerade i maj år 2021, 2022 respektive 2023).

Av tabell 6.5 framgår hur det totala antalet redovisade personer som varit föremål för HDA fördelar sig på de olika uppgiftstyperna. Som ovan angetts kan samma person ha varit föremål för HDA angående flera olika uppgiftstyper.

Tabell 6.5 Antalet personer fördelade på brottstyp och uppgiftstyp

Avser tillämpningen av HDA år 2022 (2021 och 2020)

HDA 2 § 1 st.	Narkotika-brott	Våldsbrott	Sexualbrott m.m.	Tillgrepps-brott	Ekonomiska brott	Övriga brott
1 p.						
2022	180	87	28	1	12	49
(2021)	(145)	(85)	(10)	(0)	(15)	(49)
(2020)	(69)	(37)	(7)	(0)	(3)	(10)
2 p.						
2022	178	87	28	0	12	49
(2021)	(142)	(83)	(6)	(0)	(10)	(49)
(2020)	(72)	(37)	(7)	(0)	(7)	(10)
3 p.						
2022	174	86	28	0	10	45
(2021)	(142)	(77)	(4)	(0)	(10)	(50)
(2020)	(68)	(37)	(4)	(0)	(3)	(10)
4 p.						
2022	3	2	0	0	0	0
(2021)	(0)	(0)	(2)	(0)	(0)	(2)
(2020)	(0)	(1)	(0)	(0)	(1)	(0)
5 p.						
2022	5	2	0	0	2	0
(2021)	(12)	(6)	(1)	(0)	(0)	(1)
(2020)	(2)	(10)	(0)	(0)	(0)	(1)
6 p.						
2022	175	85	31	0	12	47
(2021)	(148)	(86)	(4)	(0)	(10)	(48)
(2020)	(67)	(36)	(9)	(0)	(3)	(10)
7 p.						
2022	175	84	28	0	12	47
(2021)	(143)	(81)	(3)	(0)	(10)	(49)
(2020)	(66)	(34)	(8)	(0)	(3)	(10)

Källa: Åklagarmyndighetens redovisningar av användningen av vissa hemliga tvångsmedel under 2020–2022 (publicerade i maj år 2021, 2022 respektive 2023).

Tvångsmedlens varaktighet

Av tabell 6.6 framgår den tid som har redovisats beträffande tvångsmedlens varaktighet. De redovisade värdena anges i hela dagar. Del av dag räknas som hel dag. Vid förlängning, oavsett om en sådan skett direkt eller efter ett uppehåll, är detta redovisat som samma avlyssning. Endast den faktiska tiden har angetts, vilket innebär att bara de

dagar som avlyssning eller motsvarande faktiskt skett är medräknade i redovisningen.

Enligt tabellen är de redovisade tiderna för HDA genomgående kortare än motsvarande tider som har redovisats för HAK, HKÖ och HRA under samma period. Det är endast den faktiska avlyssningstiden, dvs. realtidsavlyssningen, som redovisas i tabellen. Inhämtning av historiska uppgifter redovisas inte eftersom HAK, HKÖ och HRA inte kan användas för detta ändamål. HÖK kan med de begränsningar som följer av datalagringsreglerna användas för att inhämta historiskt lagrade uppgifter. När det gäller HDA finns inte någon lagstadgad bortre gräns för inhämtning av historiska uppgifter. SIN konstaterade i sin särskilda granskning att såväl de granskade ansökningarna om som tillstånden till HDA i flera fall hade innefattat anmärkningsvärt långa tidsperioder. I flera fall uppgick tidsperioderna till flera år (se a. uttalande s. 9 f.). Detta innebär att myndigheterna har kunnat inhämta flera år gammal lagrad information genom HDA.

Tabell 6.6 Tvångsmedlens varaktighet

Avser den faktiska avlyssningstiden i totalt antal dagar

Tid	HDA	HAK	HKÖ	HRA
Genomsnittlig tid				
2022	20	48	40	32
(2021)	(27)	(45)	(35)	(45)
(2020)	(60)	(39)	(48)	(54)
Mediantid				
2022	13	30	30	19
(2021)	(26)	(30)	(26)	(27)
(2020)	(35)	(29)	(34)	(31)
Längsta tid				
2022	119	282	253	168
(2021)	(115)	(652)	(210)	(256)
(2020)	(211)	(354)	(292)	(292)
Kortaste tid				
2022	1	1	1	7
(2021)	(1)	(1)	(1)	(2)
(2020)	(10)	(1)	(1)	(2)

Källa: Åklagarmyndighetens redovisningar av användningen av vissa hemliga tvångsmedel under 2020–2022 (publicerade i maj år 2021, 2022 respektive 2023).

Avslag i domstol

En ansökan kan avse flera elektroniska informationssystem eller adresser. Ett negativt beslut från en domstol avseende en ansökan som innehåller flera sådana informationssystem eller adresser kan därför resultera i flera avslag.

År 2022 avslog domstol åklagares begäran om HDA under förundersökning i tre ärenden (ansökningarna rörde fyra misstänkta personer). Motsvarande siffra för 2021 var tre (ansökningarna rörde sex misstänkta personer) och år 2020 avslog domstol åklagares begäran om HDA i ett ärende. Av tabell 6.7 framgår hur antalet avslag fördelat sig mellan de olika uppgiftstyperna. I tabellen framgår även det redovisade antalet avslag för HAK, HÖK, HKÖ och HRA enligt rättegångsbalken under samma period.

Tabell 6.7 Avslag i domstol

HDA per uppgiftstyp jämfört med HAK, HÖK, HKÖ och HRA

	Avslag		
HDA 2 § 1 st.	**2020**	**2021**	**2022**
1 p. Avlyssningsuppgifter	1	5	4
2 p. Övervakningsuppgifter	1	5	4
3 p. Platsuppgifter	1	5	4
4 p. Kameraövervakningsuppgifter	0	0	0
5 p. Rumsavlyssningsuppgifter	0	0	0
6 p. Övriga lagrade uppgifter	1	6	4
7 p. Övriga användningsuppgifter	1	5	4
HAK	14	28	14
HÖK	102	100	87
HKÖ	2	6	2
HRA	0	13	2

Källa: Åklagarmyndighetens redovisningar av användningen av vissa hemliga tvångsmedel under 2020–2022 (publicerade i maj år 2021, 2022 respektive 2023).

Interimistiska beslut

Under 2022 fattade åklagare i nio ärenden totalt 24 interimistiska beslut om HDA under förundersökning. Motsvarande siffra för 2021 var totalt tolv interimistiska beslut i tio ärenden. År 2020 fattade åklagare i ett ärende två interimistiska beslut om HDA. Samtliga beslut fastställdes av domstol. Av tabell 6.8 framgår hur de interimi-

stiska besluten har fördelat sig mellan de olika uppgiftstyperna. Av tabellen framgår även antalet interimistiska beslut under förundersökning avseende HAK, HÖK och HKÖ under samma period.

Tabell 6.8 Interimistiska beslut

Beslutet fastställt av domstol om inte annat anmärks

	Interimistiska beslut		
HDA 2 § 1 st.	**2020**	**2021**	**2022**
1 p. Avlyssningsuppgifter	1	12	24
2 p. Övervakningsuppgifter	1	12	24
3 p. Platsuppgifter	1	11	24
4 p. Kameraövervakningsuppgifter	0	0	0
5 p. Rumsavlyssningsuppgifter	0	0	0
6 p. Övriga lagrade uppgifter	1	11	20
7 p. Övriga användningsuppgifter	1	12	21
HAK	329	304[1]	298[2]
HÖK	139[3]	114	241[4]
HKÖ	37	50	54[5]

[1] Varav ett beslut upphävdes av domstol.

[2] Varav tre beslut upphävdes av domstol.

[3, 4] Varav fyra beslut upphävdes av domstol.

[5] Varav två beslut upphävdes av domstol.

Källa: Åklagarmyndighetens redovisningar av användningen av vissa hemliga tvångsmedel under 2020–2022 (publicerade i maj år 2021, 2022 respektive 2023).

6.3.2 Kvantitativa uppgifter om nyttan under förundersökning

Inledning

I detta avsnitt redogör vi för de kvantitativa uppgifter som har redovisats beträffande nyttan av HDA respektive HAK, HKÖ och HRA under förundersökning åren 2020–2022. Eftersom HDA endast användes i ett fåtal ärenden under 2020 särredovisades nyttan av åtgärden detta år. Vi inleder därför detta avsnitt med en separat redogörelse för den redovisade nyttan avseende användningen av HDA under förundersökning år 2020. Därefter presenterar vi i tabellform den redovisade nyttan avseende användningen av HDA under förundersökning under åren 2021 och 2022. Nyttan redovisas uppdelat efter uppgiftstyp enligt 2 § första stycket 1–7 lagen om hemlig dataavläsning. Redovisningen av nyttan av HDA ska enligt regeringsuppdrag ske på motsvarande sätt som redovisningen av nyttan av HAK,

HKÖ och HRA under förundersökning. Vi presenterar därför parallellt, i jämförande syfte med anförda anmärkningar, den redovisade nyttan avseende användningen av HAK, HKÖ och HRA enligt rättegångsbalken under samma period.

Redovisad nytta under förundersökning år 2020

Lagen om hemlig dataavläsning trädde i kraft den 1 april 2020. Under de nio månader som HDA kunde användas detta år förekom hemlig dataavläsning i 60 ärenden, varav sju ärenden avslutades före årsskiftet 2020/2021. I minst ett av de avslutade ärendena verkställdes aldrig tvångsmedlet. Myndigheternas nyttoredovisning avseende HDA detta år omfattade således endast sju ärenden, med sammanlagt tolv misstänkta personer. Av redovisningen framgår följande. I två ärenden har uppgifterna från HDA medfört att effektiv spaning har kunnat genomföras. I ett ärende med tre misstänkta har uppgifterna bidragit till att de misstänkta har kunnat avföras från utredningen. I ett ärende har uppgifterna på annat sätt bidragit till att utredningen kunnat föras framåt. Uppgifterna framgår av *Redovisning av användningen av vissa hemliga tvångsmedel under 2020*, Åklagarmyndigheten, maj 2021.

Eftersom HDA endast förekom i ett fåtal ärenden under 2020 går det inte att göra några nyttojämförelser för perioden. För fullständighetens skull presenterar vi ändå i tabell 6.9 den redovisade nyttan av HAK, HKÖ och HRA detta år. I de ärenden som omfattas av nyttoredovisningen år 2020 användes HAK vid 1 517 brottsmisstankar, HKÖ vid 151 brottsmisstankar och HRA vid 71 brottsmisstankar.

Tabell 6.9 Redovisad nytta år 2020 - HAK, HKÖ och HRA enligt RB

Antalet brott och uppskattat andelstal där åtgärden gett viss effekt

	HAK		HKÖ		HRA	
Nytta/effekt	Antal	Andel	Antal	Andel	Antal	Andel
1. Uppgifterna har utgjort underlag i förhörssituation	740	49 %	76	50 %	20	28 %
2. Effektiv spaning har kunnat genomföras	768	51 %	123	81 %	43	61 %
3. Annat tvångsmedel har använts mot den misstänkte	504	33 %	73	48 %	20	28 %
4. Uppgifterna har bidragit till utredning om brottsutbyte	125	8 %	28	19 %	3	4 %
5. Misstankarna mot den misstänkte har stärkts	735	48 %	85	56 %	24	34 %
6. Den misstänkte har kunnat avföras från utredningen	149	10 %	4	3 %	3	4 %
7. Den misstänkte har kunnat åtalas	507	33 %	54	36 %	11	15 %
8. Uppgifterna har åberopats som bevisning i en stämningsansökan	450	30 %	52	34 %	11	15 %
9. Annat tvångsmedel har använts mot annan person i samma förundersökning	300	20 %	41	27 %	13	18 %
10. Uppgifterna har använts för att utreda brott i en annan förundersökning	83	5 %	5	3 %	5	7 %
11. Uppgifterna har på annat sätt fört utredningen framåt	598	39 %	68	45 %	24	34 %

Källa: Åklagarmyndighetens Redovisning av användningen av vissa hemliga tvångsmedel under 2020 (maj 2021).

Redovisad nytta under förundersökning åren 2021–2022

För år 2021 omfattar nyttoredovisningen för HDA 89 ärenden med totalt 155 misstänkta personer. För år 2022 är motsvarande siffror 123 ärenden med totalt 317 misstänkta personer. Ett beslut om HDA kan i sin tur innefatta en eller flera olika uppgiftstyper. Vid en jämförelse med nyttoredovisningen av andra hemliga tvångsmedel under samma period har HAK använts vid 1 393 brott (1 534 år 2021), HKÖ vid 232 brott (224 år 2021) och HRA vid 77 brott (47 år 2021).

Med ”brott” avses i detta sammanhang brottsmisstanke riktad mot person. Om flera personer är misstänkta för samma gärning, kan det innebära att flera brott redovisas i statistiken.

I tabell 6.10–6.20 nedan redogör vi för den redovisade kvantitativa nyttan av HDA under och efter förundersökning jämfört med den motsvarande redovisade nyttan av HAK, HKÖ och HRA enligt rättegångsbalken under samma period.

Som kommer att framgå i det följande kan det vid en jämförelse av nyttan av HDA kan konstateras att det förekommer relativt stora variationer, beroende dels på typ av nytta, dels på vilken uppgiftstyp som jämförs. Det kan också konstateras att nyttan av HDA har ökat under 2022 jämfört med föregående år. Som exempel kan följande statistikuppgifter framhållas. Under 2022 har avlyssningsuppgifter (1 p) lett till stärkta misstankar mot den misstänkte i 32 procent av ärendena, jämfört med 16 procent 2021. För lagrade uppgifter (6 p) gäller motsvarande i 31 procent av ärendena under 2022, jämfört med 15 procent 2021. I 23 procent av ärendena under 2022 har avlyssningsuppgifter (1 p) även bidragit till att den misstänkte kunnat åtalas, vilket kan jämföras med tio procent 2021. I 21 procent av ärendena under 2022 har övervaknings- respektive platsuppgifter (2 och 3 p) bidragit till att den misstänkte har kunnat åtalas. Motsvarande andel var 2021 nio respektive åtta procent. Tillstånd till HDA som omfattar kameraövervaknings- och rumsavlyssningsuppgifter (4 och 5 p) har varit sällsynta och endast förekommit i en handfull ärenden. Mot denna bakgrund går det inte att dra några andra slutsatser av nyttan avseende HDA beträffande dessa uppgiftstyper, än att det har förekommit ärenden där dessa varit till nytta för utredningen.

Tabell 6.10 Uppgifterna har utgjort underlag i en förhörssituation

Antalet brott och uppskattat andelstal där åtgärden gett effekt

HDA	2021		2022	
	Antal	Andel	Antal	Andel
1 p. Avlyssningsuppgifter	22	15 %	74	24 %
2 p. Övervakningsuppgifter	21	15 %	61	20 %
3 p. Platsuppgifter	15	11 %	63	21 %
4 p. Kameraövervakningsuppgifter	0	0 %	–[1]	–
5 p. Rumsavlyssningsuppgifter	0	0 %	2	100 %
6 p. Övriga lagrade uppgifter	21	14 %	70	23 %
7 p. Övriga användningsuppgifter	14	10 %	58	19 %
HAK	664	43 %	593	43 %
HKÖ	104	46 %	108	47 %
HRA	21	45 %	46	60 %

[1] Ingen redovisad.

Källa: Åklagarmyndighetens redovisningar av användningen av vissa hemliga tvångsmedel under 2021 och 2022 (maj 2022 respektive maj 2023).

Tabell 6.11 Uppgifterna har medfört att effektiv spaning har kunnat genomföras

Antalet brott och uppskattat andelstal där åtgärden gett effekt

HDA	2021		2022	
	Antal	Andel	Antal	Andel
1 p. Avlyssningsuppgifter	44	30 %	90	30 %
2 p. Övervakningsuppgifter	42	30 %	89	29 %
3 p. Platsuppgifter	39	30 %	86	29 %
4 p. Kameraövervakningsuppgifter	1	25 %	–[1]	–
5 p. Rumsavlyssningsuppgifter	10	43 %	0	0 %
6 p. Övriga lagrade uppgifter	36	24 %	82	27 %
7 p. Övriga användningsuppgifter	33	24 %	79	26 %
HAK	763	50 %	732	53 %
HKÖ	156	70 %	162	70 %
HRA	25	53 %	55	71 %

[1] Ingen redovisad.

Källa: Åklagarmyndighetens redovisningar av användningen av vissa hemliga tvångsmedel under 2021 och 2022 (maj 2022 respektive maj 2023).

Tabell 6.12 Uppgifterna har bidragit till att annat tvångsmedel använts mot den misstänkte

Antalet brott och uppskattat andelstal där åtgärden gett effekt

HDA	2021		2022	
	Antal	Andel	Antal	Andel
1 p. Avlyssningsuppgifter	17	12 %	60	20 %
2 p. Övervakningsuppgifter	16	11 %	57	19 %
3 p. Platsuppgifter	14	11 %	54	18 %
4 p. Kameraövervakningsuppgifter	0	0 %	–[1]	–
5 p. Rumsavlyssningsuppgifter	0	0 %	2	100 %
6 p. Övriga lagrade uppgifter	15	10 %	57	19 %
7 p. Övriga användningsuppgifter	13	9 %	52	17 %
HAK	441	29 %	452	32 %
HKÖ	86	38 %	93	40 %
HRA	15	32 %	26	34 %

[1] Ingen redovisad.

Källa: Åklagarmyndighetens redovisningar av användningen av vissa hemliga tvångsmedel under 2021 och 2022 (maj 2022 respektive maj 2023).

Tabell 6.13 Uppgifterna har bidragit till utredning om brottsutbyte

Antalet brott och uppskattat andelstal där åtgärden gett effekt

HDA	2021		2022	
	Antal	Andel	Antal	Andel
1 p. Avlyssningsuppgifter	4	3 %	20	7 %
2 p. Övervakningsuppgifter	4	3 %	14	5 %
3 p. Platsuppgifter	3	2 %	14	5 %
4 p. Kameraövervakningsuppgifter	0	0 %	–[1]	–
5 p. Rumsavlyssningsuppgifter	0	0 %	0	0 %
6 p. Övriga lagrade uppgifter	5	3 %	19	6 %
7 p. Övriga användningsuppgifter	3	2 %	14	5 %
HAK	129	8 %	81	6 %
HKÖ	22	10 %	16	7 %
HRA	5	11 %	8	10 %

[1] Ingen redovisad.

Källa: Åklagarmyndighetens redovisningar av användningen av vissa hemliga tvångsmedel under 2021 och 2022 (maj 2022 respektive maj 2023).

Tabell 6.14 Uppgifterna har lett till stärkta misstankar mot den misstänkte

Antalet brott och uppskattat andelstal där åtgärden gett effekt

HDA	2021		2022	
	Antal	Andel	Antal	Andel
1 p. Avlyssningsuppgifter	23	16 %	99	32 %
2 p. Övervakningsuppgifter	21	15 %	90	29 %
3 p. Platsuppgifter	19	14 %	90	30 %
4 p. Kameraövervakningsuppgifter	2	50 %	–[1]	–
5 p. Rumsavlyssningsuppgifter	3	13 %	2	100 %
6 p. Övriga lagrade uppgifter	22	15 %	96	31 %
7 p. Övriga användningsuppgifter	17	12 %	87	28 %
HAK	665	43 %	583	42 %
HKÖ	93	42 %	113	49 %
HRA	18	38 %	50	65 %

[1] Ingen redovisad.

Källa: Åklagarmyndighetens redovisningar av användningen av vissa hemliga tvångsmedel under 2021 och 2022 (maj 2022 respektive maj 2023).

Tabell 6.15 Uppgifterna har bidragit till att den misstänkte kunnat avföras från utredningen (efter förundersökning)

Antalet brott och uppskattat andelstal där åtgärden gett effekt

HDA	2021		2022	
	Antal	Andel	Antal	Andel
1 p. Avlyssningsuppgifter	6	4 %	20	7 %
2 p. Övervakningsuppgifter	6	4 %	19	6 %
3 p. Platsuppgifter	6	5 %	19	6 %
4 p. Kameraövervakningsuppgifter	2	50 %	–[1]	–
5 p. Rumsavlyssningsuppgifter	4	17 %	0	0 %
6 p. Övriga lagrade uppgifter	5	3 %	16	5 %
7 p. Övriga användningsuppgifter	4	3 %	16	5 %
HAK	156	10 %	135	10 %
HKÖ	15	7 %	13	6 %
HRA	1	2 %	6	8 %

[1] Ingen redovisad.

Källa: Åklagarmyndighetens redovisningar av användningen av vissa hemliga tvångsmedel under 2021 och 2022 (maj 2022 respektive maj 2023).

Tabell 6.16 Uppgifterna har bidragit till att den misstänkte kunnat åtalas (efter förundersökning)

Antalet brott och uppskattat andelstal där åtgärden gett effekt

HDA	2021		2022	
	Antal	Andel	Antal	Andel
1 p. Avlyssningsuppgifter	15	10 %	71	23 %
2 p. Övervakningsuppgifter	13	9 %	63	21 %
3 p. Platsuppgifter	10	8 %	64	21 %
4 p. Kameraövervakningsuppgifter	1	25 %	–[1]	–
5 p. Rumsavlyssningsuppgifter	0	0 %	2	100 %
6 p. Övriga lagrade uppgifter	14	9 %	70	23 %
7 p. Övriga användningsuppgifter	9	7 %	61	20 %
HAK	494	32 %	431	31 %
HKÖ	89	40 %	80	34 %
HRA	13	28 %	32	42 %

[1] Ingen redovisad.

Källa: Åklagarmyndighetens redovisningar av användningen av vissa hemliga tvångsmedel under 2021 och 2022 (maj 2022 respektive maj 2023).

Tabell 6.17 Uppgifterna har åberopats som bevisning i stämningsansökan (efter förundersökning)

Antalet brott och uppskattat andelstal där åtgärden gett effekt

HDA	2021		2022	
	Antal	Andel	Antal	Andel
1 p. Avlyssningsuppgifter	9	6 %	59	19 %
2 p. Övervakningsuppgifter	10	7 %	51	17 %
3 p. Platsuppgifter	9	7 %	53	18 %
4 p. Kameraövervakningsuppgifter	1	25 %	–[1]	–
5 p. Rumsavlyssningsuppgifter	0	0 %	2	100 %
6 p. Övriga lagrade uppgifter	12	8 %	59	19 %
7 p. Övriga användningsuppgifter	8	6 %	49	16 %
HAK	461	30 %	400	29 %
HKÖ	76	34 %	69	30 %
HRA	14	30 %	32	42 %

[1] Ingen redovisad.

Källa: Åklagarmyndighetens redovisningar av användningen av vissa hemliga tvångsmedel under 2021 och 2022 (maj 2022 respektive maj 2023).

Tabell 6.18 Uppgifterna har bidragit till att något tvångsmedel använts mot annan person i samma förundersökning (överskottsinformation)

Antalet brott och uppskattat andelstal där åtgärden gett effekt

HDA	2021		2022	
	Antal	Andel	Antal	Andel
1 p. Avlyssningsuppgifter	15	10 %	44	14 %
2 p. Övervakningsuppgifter	14	10 %	41	13 %
3 p. Platsuppgifter	13	10 %	38	13 %
4 p. Kameraövervakningsuppgifter	0	0 %	–[1]	–
5 p. Rumsavlyssningsuppgifter	1	4 %	2	100 %
6 p. Övriga lagrade uppgifter	14	9 %	41	13 %
7 p. Övriga användningsuppgifter	12	9 %	38	12 %
HAK	293	19 %	219	16 %
HKÖ	42	19 %	32	14 %
HRA	10	21 %	28	36 %

[1] Ingen redovisad.

Källa: Åklagarmyndighetens redovisningar av användningen av vissa hemliga tvångsmedel under 2021 och 2022 (maj 2022 respektive maj 2023).

Tabell 6.19 Uppgifterna har använts för utredning av brott i en annan förundersökning (överskottsinformation)

Antalet brott och uppskattat andelstal där åtgärden gett effekt

HDA	2021		2022	
	Antal	Andel	Antal	Andel
1 p. Avlyssningsuppgifter	11	8 %	22	7 %
2 p. Övervakningsuppgifter	10	7 %	17	6 %
3 p. Platsuppgifter	10	8 %	16	5 %
4 p. Kameraövervakningsuppgifter	1	25 %	–[1]	–
5 p. Rumsavlyssningsuppgifter	3	13 %	0	0 %
6 p. Övriga lagrade uppgifter	11	7 %	20	7 %
7 p. Övriga användningsuppgifter	9	7 %	16	5 %
HAK	70	5 %	138	10 %
HKÖ	12	5 %	12	5 %
HRA	6	13 %	6	8 %

[1] Ingen redovisad.

Källa: Åklagarmyndighetens redovisningar av användningen av vissa hemliga tvångsmedel under 2021 och 2022 (maj 2022 respektive maj 2023).

Tabell 6.20 Uppgifterna har på annat sätt bidragit till att utredningen kunnat föras framåt

Antalet brott och uppskattat andelstal där åtgärden gett effekt

HDA	2021		2022	
	Antal	Andel	Antal	Andel
1 p. Avlyssningsuppgifter	27	18 %	91	30 %
2 p. Övervakningsuppgifter	28	20 %	85	28 %
3 p. Platsuppgifter	25	19 %	81	27 %
4 p. Kameraövervakningsuppgifter	1	25 %	–[1]	–
5 p. Rumsavlyssningsuppgifter	4	17 %	0	0 %
6 p. Övriga lagrade uppgifter	26	17 %	113	37 %
7 p. Övriga användningsuppgifter	24	18 %	81	26 %
HAK	489	32 %	570	41 %
HKÖ	61	27 %	110	47 %
HRA	18	38 %	50	65 %

[1] Ingen redovisad.

Källa: Åklagarmyndighetens redovisningar av användningen av vissa hemliga tvångsmedel under 2021 och 2022 (maj 2022 respektive maj 2023).

6.3.3 Särskilt om Säkerhetspolisens tvångsmedelsanvändning

Säkerhetspolisens tvångsmedelsanvändning ingår inte i den statistik som har redovisats i det föregående, utan denna redovisas varje år separat och samlat. Redovisningen sker i en totalsiffra beträffande 1) antalet tillstånd till HAK, HÖK, HKÖ och HRA enligt rättegångsbalken samt antalet tillstånd till preventiva tvångsmedel, 2) antalet beslut som fattats med stöd av inhämtningslagen respektive 3) antalet tillstånd till HDA. Uppgiften om antalet tillstånd inkluderar såväl initiala beslut som förlängning av tillståndstiden. Redovisningen omfattar dock inte HDA vid särskild utlänningskontroll. Säkerhetspolisen redovisar inte heller hur tillstånden till HDA fördelar sig på olika uppgiftstyper eller om tvångsmedlen har varit till nytta i verksamheten. I Säkerhetspolisens verksamhet gavs under 2022 292 tillstånd till HDA och under 2021 var motsvarande siffra 234. Under de nio månader som HDA kunde användas under 2020 gavs 130 tillstånd till HDA.

En jämförelse kan göras med tillstånd till andra hemliga tvångsmedel i Säkerhetspolisens verksamhet under motsvarande period, se tabell 6.21. Av tabellen framgår att HDA relativt sett har använts i

stor utsträckning i Säkerhetspolisens verksamhet. Det ska samtidigt framhållas att antalet tillstånd till hemliga tvångsmedel i underrättelseverksamhet är helt beroende av karaktären på de ärenden som Säkerhetspolisen hanterar varje år. Vissa ärenden kan medföra att många tvångsmedelsbeslut fattas, medan andra ärenden inte behöver föranleda något tvångsmedelsbeslut alls. Förändringarna i antalet tillstånd under perioden 2020–2022 ligger därmed inom vad som kan betraktas som normala årliga variationer (jfr t.ex. Åklagarmyndighetens redovisning av användningen av vissa hemliga tvångsmedel under 2022, maj 2023, s. 63).

Tabell 6.21 Säkerhetspolisen – antalet tillstånd till olika hemliga tvångsmedel

Preventiv tvångsmedelsanvändning

	2020	2021	2022
HDA enligt HDA-lagen	130	234	292
HAK, HÖK, HKÖ, HRA enligt RB och preventivlagen	486	494	562
Inhämtning enligt inhämtningslagen (IHL)	119	148	203

Källa: Åklagarmyndighetens redovisningar av användningen av vissa hemliga tvångsmedel under 2020–2022 (publicerade i maj år 2021, 2022 respektive 2023).

6.3.4 Särskilt om användningen i preventivlagsfallen

Inom Åklagarmyndigheten är det Riksenheten för säkerhetsmål som handlägger ärenden enligt lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen). Utöver de ärenden som samtidigt har hanterats av Säkerhetspolisen, och som tidigare har redogjorts för, har det hittills inte förekommit några HDA-ärenden i preventivlagsfallen (t.o.m. 2022). Det kan anmärkas att Polismyndighetens tillämpning av preventivlagen generellt sett har varit begränsad.

6.3.5 Särskilt om användningen i inhämtningslagsfallen

Polismyndigheten och Tullverket redovisar varje år i antal beslut den inhämtning av uppgifter som skett i underrättelseverksamhet med stöd av inhämtningslagen (IHL). Med inhämtningslagen avses lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverk-

samhet. I redovisningen från år 2021 redovisas även statistik för tillämpningen av HDA enligt 10 § lagen om hemlig dataavläsning (dvs. HDA i inhämtningslagsfallen). Detta år ansöktes endast om två tillstånd till HDA i inhämtningslagsfallen. Under år 2022 ansöktes inte om något sådant beslut. Det förhållandet att möjligheten till HDA inte har utnyttjats mer i underrättelseverksamheten kan bero på vilka ärenden som har prioriterats. En av de stora begränsningarna ligger enligt de brottsbekämpande myndigheterna i att den nuvarande regleringen inte tillåter avläsning av fler uppgiftstyper, exempelvis s.k. punkt 6-och 7-uppgifter. Detta innebär i sin tur att den arbetsinsats som för närvarande krävs för att använda HDA inte alltid står i proportion till det mervärde som materialet ger i underrättelseverksamheten i jämförelse med inhämtning enligt IHL.

Samtidigt kan det noteras att Polismyndighetens underrättelseverksamhet de senaste åren i ökande omfattning har använt IHL som verktyg. År 2021 fattade Åklagarmyndigheten sammanlagt 599 beslut enligt IHL (varav 12 avslag), på ansökningar från Polismyndigheten och Tullverket. Det innebär en marginell ökning från år 2020 då myndigheten fattade sammanlagt 551 beslut om inhämtning (varav 15 avslag). Under 2022 fattade Åklagarmyndigheten sammanlagt 727 beslut om inhämtning (varav 23 avslag). Det kan därmed konstateras att det skett en markant ökning sedan föregående år. Orsaken till detta är enligt myndigheternas redovisning sannolikt det svåra och omfattande konfliktläge som råder inom den organiserade brottsligheten i Sverige, där inhämtning enligt aktuell lagstiftning är till stor hjälp vid kartläggning och identifiering av aktörer (se Åklagarmyndighetens redovisning av användningen av vissa hemliga tvångsmedel under 2022, maj 2023, s. 64 f.).

6.4 Praktiska exempel från den hittillsvarande tillämpningen

För att åskådliggöra vilken betydelse som användningen av HDA har haft för brottsbekämpningen har i de årliga redovisningarna redogjorts för totalt nio anonymiserade ärenden där HDA har använts och kommit till nytta. För år 2021 redovisades följande tre ärenden (jfr Åklagarmyndighetens redovisning av användningen av vissa hemliga tvångsmedel under 2021, s. 48 f.).

Exempel 1.1. Grovt narkotikabrott, huvudman bakom storskalig narkotikaförsäljning kunde identifieras och dömas

Polisen fattade misstankar om att en viss person sålde narkotika. I samband med en husrannsakan i personens bostad togs bland annat en dator och en mobiltelefon i beslag. Vid undersökning av dessa anträffades listor som förmodades vara försäljningslistor samt skärmdumpar från Flugsvamp 3.0, som då fungerade som en marknadsplats för försäljning av narkotika på internet. Genom vidare spaning fattades misstankar om att personen låg bakom ett visst säljaralias på Flugsvamp 3.0. Den fysiska spaning som bedrevs mot personen gjorde att misstankarna stärktes. Efter ett par veckor försvann annonserna från det identifierade aliaset, varpå spaningen också avbröts. Spaningen återupptogs senare efter att annonser från aliaset åter dykt upp på Flugsvamp 3.0. Polis noterade att den som kunde misstänkas återkommande skickade rekommenderade postförsändelser. En av dessa kontrollerades och visade sig innehålla en relativt stor mängd heroin. Den som kunde misstänkas blev därefter frihetsberövad. Efter att personen hade frihetsberövats beviljades HDA beträffande kontot på Flugsvamp 3.0 samt en krypterad e-postadress. Därigenom kunde bevisning säkras som visade dels att den som kunde misstänkas också var den som brukade kontot och e-postadressen, dels i vilken omfattning försäljningen hade skett. Genom bland annat denna bevisning kom personen att dömas för grovt narkotikabrott. Påföljden bestämdes till ett fleråriget fängelsestraff.

Exempel 1.2. Sprängattentat, flera personer kunde identifieras och dömas

Inom ramen för en förundersökning hade åklagare ansökt och beviljats tillstånd till HAK och HDA mot en misstänkt person. Genom HDA framkom att den misstänkte hade en hotbild riktad mot sig och att hen, av den anledningen, ville införskaffa sprängmedel. I samband med att en livsmedelsbutik några veckor därefter sprängdes kom den avlyssnade personen, tillsammans med ytterligare två personer, att frihetsberövas. Samtidigt uppmärksammades att den avlyssnade personen varit i kontakt med en fjärde person och gett denne instruktioner om att hämta sprängmedel i en annan stad. Detta ledde till att även denna fjärde person kunde frihetsberövas, men också till att en av de som inledningsvis hade frihetsberövats kunde avskrivas från samtliga misstankar. Genom den hemliga dataavläsningen kunde det ledas i bevis att den avlyssnade personen avsåg att skaffa sprängmedel. Bevisningen som låg till grund för åtalet kom i stor omfattning att röra sig om de avlyssnade samtalen, vad som framkommit vid samtalstrafik och positionering samt den hemliga dataavläsningen. Två av personerna dömdes för allmänfarlig ödeläggelse, misshandel och grovt brott mot lagen om brandfarliga och explosiva varor. Den tredje personen dömdes för grovt brott mot lagen om brandfarliga och explosiva varor. Påföljderna som dömdes ut motsvarade fleråriga fängelsestraff.

Exempel 1.3. Grovt dopningsbrott, huvudman bakom försäljning av dopningspreparat kunde identifieras och dömas

Hemliga tvångsmedel, däribland HDA, beviljades med anledning av misstanke om att det tillverkades narkotika på en viss plats. Genom den hemliga dataavläsningen kunde en misstänkt persons konversationer via krypterade applikationer läsas av. Av dessa framgick att personen bjöd ut dopningspreparat till försäljning samt att hen diskuterade olika dopningspreparat med andra personer. Personen åtalades och dessa konversationer åberopades som bevisning. Domstolen fann att uppgifterna från konversationerna tydligt visade att den åtalade hade handlat med dopningspreparat. Den åtalade dömdes för grovt dopningsbrott och ytterligare ett brott. Påföljden bestämdes till fängelse.

För år 2022 redovisades följande sex ärenden (jfr Åklagarmyndighetens redovisning av användningen av vissa hemliga tvångsmedel under 2022, s. 55 ff.).

Exempel 2.1. Grovt narkotikabrott, en narkotikaaffär kunde följas i realtid, varvid flera personer i brottskedjan kunde identifieras och gripas

I en krypterad chatt kunde avläsas att brukaren av den telefon mot vilken HDA riktades gjorde en beställning av ett större narkotikaparti. Med säljaren gjordes det upp var narkotikan skulle överlåtas och kodord som skulle användas för att bekräfta säljarens identitet. Samtidigt kunde man i HDA:n avläsa att köparen uppdrog åt annan transportör att åka till den med säljaren bestämda adressen och att transportören fick kodordet. Genom fysisk spaning kunde man konstatera att två bilar kom till den bestämda adressen och samtidigt skickades foto på respektive bil i en gruppchatt som kunde avläsas med HDA. Spanare kunde därigenom bekräfta att det var foto på samma fordon som kommit till adressen. Därefter såg spanare hur person från det ena fordonet kontaktade föraren i det andra fordonet, samtalade kort och fick ett paket överlämnat. Efter att paketet överlämnats så fick brukaren av telefonen som avlästes en bekräftelse från transportören om att ”det var klart”. Därefter bekräftade även säljaren till köparen att leverantören nu överlämnat paketet. Direkt efter detta skickades en ny leveransadress och leverantören för säljaren började köra mot denna adress. Sedermera stoppades fordonet med transportören och ett större narkotikabeslag gjordes. Även leverantören stoppades på väg till den nya adressen och även här gjordes större narkotikabeslag. Köparen, brukaren av telefonen mot vilken HDA riktades, greps även han med den avlästa telefonen på sig. Samma kväll gjordes husrannsakan i leverantörens bostad där ytterligare större narkotikabeslag gjordes. På denna adress greps även en ytterligare person som det senare visade sig var den som fortlöpande uppdragit åt leverantören att köra till viss adress och leverera.

Exempel 2.2. Grovt narkotikabrott, flera personer i brottskedjan kunde identifieras och dömas

Misstanke fanns att en viss gruppering köpte och sålde stora mängder narkotika, varför flera personer kom att misstänkas för grovt narkotikabrott. HDA användes mot flera av de misstänkta personerna. Genom denna kunde exempelvis bevisas att en större summa pengar transporterades av en kurir mellan två svenska städer och att pengarna avsåg ersättning för inköp av en större mängd cannabis. Detta genom att det var möjligt att läsa textkonversationer mellan de misstänkta om hur biljetter bokades, pengar överfördes och uppdraget gavs till kuriren. Det kunde även säkras fotografier av en större summa pengar, som väl stämde överens med konversationer om hur stort vederlag som skulle betalas. Det inhämtade materialet åberopades i målet och bidrog starkt till att de åtalade kunde dömas i denna del.

Exempel 2.3. Grovt vapenbrott, flera personer i brottskedjan kunde identifieras och dömas

I ett ärende med förgreningar till andra länder uppstod misstankar om att ett antal individer köpte och sålde vapen. Genom HDA kunde konversationer från olika applikationer säkras. Det kunde konstateras att de misstänkta ofta skrev om vapen och det säkrades även filmer som visade när vapen provsköts. Efter en tids spaning kunde tillslag göras mot grupperingen. Vid detta togs ett antal vapen i beslag, däremot inte några telefoner. Det senare innebar att all bevisning i form av chattar kom från HDA. Genom den bevisningen kunde de misstänkta åtalas och dömas för innehav och försäljning av fler vapen än de som fanns i beslag.

Exempel 2.4. Grovt vapenbrott, en person kunde identifieras och dömas

Polis hittade vid husrannsakan ett vapen, vilket togs i beslag. Någon dag senare kom via HDA in uppgifter som tydde på att den som HDA:n riktades mot var innehavaren av vapnet. Det var fråga om uppgifter från en chattapplikation där personen skrev att hans vapen hade tagits i beslag ett visst datum. Personen skrev även vilken typ av vapen det var, vilket stämde överens med beslaget. Detta, tillsammans med viss annan bevisning, var avgörande för att personen senare skulle kunna åtalas och dömas för grovt vapenbrott.

Exempel 2.5. Synnerligen grovt narkotikabrott, en narkotikaaffär kunde följas i realtid och en person högt upp i brottskedjan kunde identifieras och dömas

Genom HDA kunde en chatt läsas av i realtid. Genom denna var det möjligt att få fram uppgifter om hur en person instruerade en annan person att på flera olika platser överlämna narkotika. Konversationerna visade

även hur uppdragsgivaren instruerade den andra personen att lagerhålla narkotika i sin bostad. Det fanns även ett flertal andra konversationer mellan uppdragsgivaren och andra personer. Genom dessa var det möjligt att visa att verksamheten bedrevs i organiserad form och i större omfattning. Det var också möjligt att visa att uppdragsgivaren var den som styrde verksamheten. Dessa uppgifter var sedan avgörande för att uppdragsgivaren kunde åtalas och dömas för synnerligen grovt narkotikabrott.

Exempel 2.6. Grovt narkotikabrott, flera personer i brottskedjan kunde identifieras och dömas

I en utredning om grovt narkotikabrott beviljades tillstånd till HAK och HDA. Genom avlyssnade telefonsamtal kunde konstateras att två personer planerade en resa till en annan stad och att syftet föreföll vara att hämta narkotika. Detta kunde sedan jämföras med material från HDA där chattmeddelanden skickades om vilken adress de skulle färdas till samt, sedan resan gjorts, vad det var som hade hämtats. I chattmeddelanden beskrevs även utseendet på den väska som narkotikan förvarades i, vilket i förlängningen gjorde det möjligt att åtala även beställaren av narkotikan. Tre personer åtalades och dömdes för involvering i införskaffandet och transporten av narkotikan.

Härutöver har experter från de brottsbekämpande myndigheterna inkommit med egna beskrivningar av tillämpningen jämte ytterligare exempel på anonymiserade ärenden där HDA har använts och kommit till nytta. Detta gäller med undantag från Säkerhetspolisens beskrivningar av tillämpningen som av verksamhetsskäl har lämnats muntligen. Företrädare för Säkerhetspolisen har till utredningen redogjort för flera praktiska exempel där tillämpningen av hemlig dataavläsning har lett till avgörande information för att förebygga, förhindra eller upptäcka allvarlig brottslighet. Det har också framhållits att även om HDA vid särskild utlänningskontroll inte används särskilt frekvent, är åtgärden ett mycket viktigt redskap som kan bidra med helt avgörande information rörande personer som av Migrationsverket eller regeringen bedöms utgöra ett kvalificerat säkerhetshot här i landet. Den nytta som den hittillsvarande tillämpningen av HDA har medfört i underrättelseverksamhet är därför enligt Säkerhetspolisen mycket hög.

När det gäller HDA i inhämtningslagsfallen har Åklagarmyndigheten framhållit att underrättelseverksamhet i allt väsentligt är ett långsiktigt arbete och därför är det inte möjligt att ännu bedöma den fulla nyttan av HDA i dessa fall. Av Åklagarmyndighetens årliga redo-

visningar framgår att information om elektronisk kommunikation i allmänhet är väsentlig för myndigheternas underrättelseverksamhet och att de inhämtningsmöjligheter som inhämtningslagen medger har varit avgörande för att inleda förundersökningar avseende en lång rad grova brott (se t.ex. Åklagarmyndighetens redovisning av användningen av vissa hemliga tvångsmedel under 2021, maj 2022, s. 57 ff.).

Ett generellt exempel på en vanligt förekommande situation under en brottsutredning är när det finns en risk för att den berörde gör sig av med sin mobiltelefon. I en sådan situation är de brottsbekämpande myndigheterna många gånger beroende av HDA för att kunna inhämta information.

Företrädare för de olika brottsbekämpande myndigheterna har lämnat följande anonymiserade exempel på ärenden där HDA har använts för att säkra bevisning som inte varit åtkomlig genom andra tvångsmedel.

Exempel 3.1. Grov narkotikasmuggling, flera personer i brottskedjan kunde identifieras och dömas

Sommaren 2022 ankom en försändelse från Panama till en flygplats i Tyskland. Narkotikasökhund markerade på försändelsen och paketet röntgades. I försändelsen fanns en fruktpress och i botten på pressen fann man ett utrymme av metall som det borrades in i. Rester av pulver följde med borren och ett snabbtest visade på kokain. Enbart mängden narkotika gjorde att man misstänkte att det var fråga om ett grovt narkotikasmugglingsbrott.

En misstänkt person fick en avisering från fraktföretaget om att hen kunde hämta försändelsen på en fraktterminal i Malmö. I aviseringen framgick ett telefonnummer som det togs ett beslut om HAK på. Genom HAK framkom uppgifter om att det fanns fler misstänkta och att dessa använde sig av olika krypterade chattapplikationer, varför det uppstod ett behov av HDA. Åklagaren beslutade om kontrollerad leverans för att knyta huvudmännen till smugglingen och fattade ett interimistiskt beslut om HDA. Det framstod som särskilt angeläget att identifiera organisatören eller organisatörerna bakom smugglingen eftersom den huvudmisstänkte var en ung person som misstänktes vara utsatt för visst tvång att utföra gärningen. Eftersom det inte gick att få fram narkotikan ur fruktpressen utan att göra åverkan på pressen, beslutade åklagaren att genomföra den kontrollerade leveransen med narkotikan kvar i fruktpressen.

Genom HDA framkom avgörande uppgifter, b.la fick man lokaliseringsuppgifter om hur den misstänkte rörde sig efter uthämtningen av försändelsen på fraktterminalen. Vidare kunde man utläsa ur kommunikationerna i chattapplikationerna att det fanns en organisatör som använde ett särskilt namn. Organisatören anvisade hur den misstänkte skulle göra för att öppna fruktpressen och ta fram narkotikan. I det efter-

följande utredningsarbetet lyckades utredarna med olika metoder att identifiera organisatören. Vidare framkom genom HDA att det fanns motspanare på elsparkcykel i området som försökte identifiera möjliga polisspanare. Både samtal och meddelanden från HDA-materialet ingick i förundersökningen. Mottagaren av fruktpressen och organisatören åtalades för grov narkotikasmuggling. Tingsrätten, som dock inte fann utrett att någon av de tilltalade hade haft någon mer drivande roll i narkotikaverksamheten, biföll åtalet. Påföljden för de båda tilltalade bestämdes till fleråriga fängelsestraff. Domen överklagades till hovrätten som fastställde tingsrättens dom.

Exempel 3.2. Synnerligen grovt narkotikabrott, flera personer i brottskedjan, däribland organisatörer, kunde identifieras och dömas

På grund av underrättelseinformation inkommen till Tullverket inleddes en förundersökning om storskalig narkotikasmuggling till Sverige från bland annat Spanien. Kartläggningen och utredningen av brotten visade på ett kriminellt nätverk med flera inblandade. HAK inleddes mot några misstänkta. Under pågående avlyssning framkom att de misstänkta använde krypterade medier för att kommunicera. De misstänkta nämnde vid flera tillfällen att de skulle skriva till varandra i stället. HDA beviljades och därigenom kunde vissa av konversationerna läsas. Av dessa framgick narkotikabeställningar och leveranser av narkotika. Med hjälp av HDA kunde även konstateras att organisationen smugglade narkotika i postflödet. Det skickades också bilder via de krypterade applikationerna som visade märkning på paketen med narkotika. Vidare kunde man genom HDA bekräfta de misstänktas roller i organisationen och identifiera mottagare till den insmugglade narkotikan. Sex personer greps och stora mängder narkotika beslagtogs. Konversationerna åberopades som bevisning i den efterföljande rättegången. Alla sex personer åtalades och dömdes både i tingsrätten och hovrätten till fleråriga fängelsestraff för bland annat synnerligen grova narkotikabrott. Vid bestämmandet av fängelsestraffens längd togs bl.a. hänsyn till de inblandades olika roller i brottsligheten.

Under förundersökningen i ovanstående exempel kunde det också genom analys av bland annat uppgifterna från HDA identifieras andra misstänkta som det inleddes förundersökning mot. Även i den förundersökningen användes HDA med framgång.

Exempel 3.3. Grov våldtäkt mot barn, material på skyddade lagringsplattformer kunde läsas av, flera personer kunde identifieras och dömas

En person var vid flera tillfällen misstänkt för innehav av stora mängder barnpornografiskt material. Under de tidigare utredningarna kunde polisen inte komma åt materialet som förvarades på skyddade lagringsplattformer. Genom användning av HDA kunde polisen läsa av uppgifterna och bevissäkra materialet. Vid tidpunkten för gripandet planerade den miss-

tänkte grova övergrepp mot barn. Vidare kunde ytterligare personers inblandning i brotten klarläggas. Personerna åtalades och dömdes till fleråriga fängelsestraff.

Exempel 3.4. Mord och grovt narkotikabrott, beställaren av ett mord kunde identifieras och dömas

I en utredning hade en misstänkt tillhörande ett kriminellt nätverk beordrat ett mord på en person tillhörande ett annat nätverk. Den misstänkte anvisade unga personer att utföra diverse ärenden, såsom förmedling av narkotika och vapen. Den misstänkte kommunicerade via krypterade applikationer som lästes av med HDA. I samband med tillslag blev den misstänkte varnad av en person som, av ren tillfällighet, uppmärksammat att polisen befann sig utanför den misstänktes bostad. Varningen ledde till att den misstänkte hann ta sönder sina telefoner innan polisen kunde gripa hen. Tack vare att HDA hade använts i utredningen innan tillslaget gjordes hade material och bevisning till stora delar redan säkrats. Detta ledde i sin tur till att den misstänkte åtalades och dömdes till flera års fängelse för mord och grovt narkotikabrott.

Exempel 3.5. Synnerligen grovt narkotikabrott m.m., flera personer i brottskedjan, däribland organisatörer, kunde identifieras och dömas

I utredningen, som handlade om synnerligen grovt narkotikabrott och grova dopingbrott, lyckades hela kedjan från huvudman och lagerhållare till försäljare etc. identifieras och dömas. Genom HDA kunde krypterade konversationer och samtal avlyssnas och åberopas som bevisning i rätten. Flera personer, däribland organisatörer, åtalades och dömdes till fleråriga fängelsestraff.

Exempel 3.6. Grov våldtäkt mot barn, raderad information kunde säkras, en person identifierades och åtalades

I samband med ett tillslag framkom att den misstänkte hade raderat all information i det informationssystem som hade använts i kontakterna med målsäganden. Någon bevisning om brottet kunde därför inte säkras genom den forensiska undersökningen. Trots att informationen hade raderats kunde omfattande chattkonversationer och uppgifter om mötestidpunkter och platser mellan den misstänkte och målsäganden läsas av och säkras genom HDA. Den misstänkte åtalades och dömdes av tingsrätten till ett flerårigt fängelsestraff. I tingsrättens bedömning av åtalet ingick analys av HDA-material. Domen överklagades till hovrätten som ogillade åtalet.

Exempel 3.7. Förberedelse till mord m.m., mordplaner kunde avslöjas och mord förhindras genom precisa platsuppgifter i realtid, flera personer identifierades och dömdes

Genom användning av HDA framkom uppgifter om att de misstänkta hade långgående planer på att ta livet av en annan person. Under tiden för insatsen begick de misstänkta ett grovt rån för att skaffa ett fordon. Samtidigt kunde mycket preciserade uppgifter om de misstänktas lokalisering i realtid lämnas till spaningspersonal med hjälp av HDA. Med denna information kunde spaningspersonalen dirigeras och gripa de misstänkta på brottsplatsen för det grova rånet och på så sätt förhindra mordplanerna. Sådana precisa platsuppgifter hade inte varit möjligt att få in genom inhämtning av andra lokaliseringsuppgifter än HDA. Sex personer åtalades och dömdes för olika brott till fleråriga fängelsestraff.

Exempel 3.8. Synnerligen grovt narkotikabrott, huvudmännen i ett kriminellt nätverk kunde kopplas till ett stort narkotikabeslag, ytterligare ett tiotal personer i brottskedjan identifierades och dömdes

I ärendet hade utredarna en god bild av vem som var en av huvudmännen bakom en narkotikasmuggling, men den misstänkte hade hittills inte gått att knyta till narkotikahanteringen i tillräcklig utsträckning. Ett beslag av stora mängder narkotika gjordes vid Öresundsbron. Genom användningen av HDA kunde utredarna ta del av chattkonversationer där huvudmannen chattade om beslaget. Huvudmannen avslöjade detaljinformation om narkotikan, däribland den exakta mängd narkotika som beslagtagits. Flera tillslag gjordes i ärendet och sammanlagt beslagtogs narkotika till ett gatuvärde av drygt 80 miljoner kronor. Sammanlagt 15 personer åtalades och de uppgifter som hade hämtas in genom HDA användes som central bevisning i målet. Av de åtalade dömdes 13 personer, inklusive huvudmännen, till fleråriga fängelsestraff för synnerligen grovt narkotikabrott. Domen överklagades till hovrätten som ännu inte har hållit huvudförhandling.

Exempel 3.9. Människorov m.m., människorov kunde avbrytas genom precisa platsuppgifter i realtid, flera personer identifierades och dömdes

I ett ärende mottog en förälder en bild på sin son med en pistol tryckt mot sonens huvud. Av meddelandet framgick att sonen var kidnappad och att en lösensumma skulle betalas annars skulle sonen dödas. Ett flertal tvångsmedelsåtgärder vidtogs mot några personer i ärendet som, av olika anledningar, bedömdes som skäligen misstänkta. Åtgärderna gav dock inget resultat och den kidnappade sonen kunde inte lokaliseras. Genom användning av HDA kunde dock uppgifter om var en av de misstänkta befann sig inhämtas. Dessa uppgifter var helt avgörande eftersom spaningsinsatserna var inriktade på en helt annan plats. Sonen kunde kort därefter hittas och samtidigt kunde en av de misstänkta gripas på platsen. Under utredningen häktades åtta personer och ytterligare två

personer efterlystes internationellt. Åtta personer åtalades och dömdes för olika brott till fleråriga fängelsestraff.

Exempel 3.10. Grovt vapenbrott m.m., flera högt uppsatta personer i kriminellt nätverk kunde identifieras och dömas

I ärendet befann sig en av de misstänkta huvudmännen utomlands. Huvudmannen kommunicerade med misstänkta personer i Sverige genom krypterade applikationer som polisen kunde ta del av genom HDA. I en gruppchatt diskuterades leverans och försäljning av narkotika varpå en av de misstänkta angav att hen kände sig hotad och ville ha ett vapen. Huvudmannen förklarade att hen kunde ordna fram ett vapen med tillhörande ammunition men att vapnet bara fick användas för att ”skjuta mot människor eftersom ammunition är en bristvara”. Några dagar senare framkom information om leveranstillfälle av vapen och narkotika i chatten, vilket gjorde att polisen kunde gripa både leverantör och mottagare. Sammanlagt nio personer, inklusive huvudmännen, åtalades och dömdes i tingsrätten för olika brott till bl.a. fleråriga fängelsestraff. Huvudmännen överklagade domen till hovrätten där huvudförhandling i målet för närvarande pågår.

Exempel 3.11. Förberedelse till mord m.m., överskottsinformation från HDA kunde avslöja mordplaner och förhindra mord samt avslöja ett synnerligen grovt narkotikabrott, flera personer identifierades och dömdes

I ärendet användes HDA för att hämta in bevisning om ett mord som var begånget sedan en tid tillbaka. Av de inhämtade uppgifterna kunde polisen dock snabbt konstatera att det fanns långtgående planer på att mörda en annan person. Ytterligare misstänkta kunde identifieras och insatser kunde riktas mot även dessa personer. HDA gav sammantaget utredarna tillgång till bilder på vapen och uppgifter om vem som var måltavlan och vilka som skulle utföra mordet. Stora polisresurser sattes in och mordet kunde genom dessa uppgifter förhindras. Åtal väcktes avseende förberedelse till mord och rättegång i målet är planerad att äga rum under slutet av 2023. Vidare delades överskottsinformation från HDA till andra förundersökningar. Ett av dessa ärenden resulterade i att sex personer, inklusive en huvudman, åtalades och dömdes till fleråriga fängelsestraff för synnerligen grovt narkotikabrott. I detta ärende utgjorde chattar från HDA helt avgörande bevisning.

Exempel 3.12. Synnerligen grovt narkotikabrott, flera personer i brottskedjan, däribland huvudmannen bakom en storskalig narkotikaförsäljning, kunde identifieras och dömas

Genom att HDA användes i ärendet kunde en person identifieras som en av ledarna bakom en storskalig narkotikahantering. Trots att personen befann sig på en fängelseanstalt lyckades hen förmedla diverse uppdrag åt mycket unga gärningspersoner. Uppdragen beskrevs av de misstänkta i krypterade chattar som polisen kunde ta del av genom HDA. De inblandade personerna åtalades för synnerligen grovt narkotikabrott och dömdes till långa fängelsestraff.

Exempel 3.13. Förberedelse till mord m.m., flera personer kunde identifieras och åtalas

Förundersökningen handlade initialt om misstankar om medhjälp till mord men genom att ta del av bilder från HDA uppkom ytterligare brottsmisstankar. Bilderna avsåg olika delar till bomber som tillverkades. Det fanns även bilder på måltavlor och det fördes diskussioner om när och hur platser borde rekognoseras och hur de själva kunde säkerställa att de inte skulle komma till skada. Bevisning om de misstänktas inblandning och uppsåt till brotten kunde säkras genom de avlästa uppgifterna. Åtal väcktes mot 28 misstänkta personer avseende förberedelse till mord, grovt vapenbrott och grovt narkotikabrott. Huvudförhandling pågår för närvarande.

Exempel 3.14. Förberedelse till mord, mordplaner kunde avslöjas och mord förhindras

I ett ärende fick man under en tidsperiod om 3–5 veckor information vid HDA om tre olika mordplaner, av och även mot de som besluten riktades mot. Det var därför möjligt att agera så att planerna aldrig kunde komma till sin fullbordan genom att kontrollera, gripa eller vidta andra åtgärder.

Exempel 3.15. Grova insiderbrott, avgörande bevisning kunde säkras, antalet personella frihetsberövanden och tiden för dessa kunde minimeras, flera personer kunde identifieras och åtalas

Genom HDA erhölls kommunikation som var avgörande för utredningen i ärendet om grova insiderbrott. Efter att ha säkrat denna bevisning genom HDA mot misstänkt nr 2 gjordes tillslag mot i ärendet tre misstänkta personer. I samband med gripande av misstänkt nr 2 kunde inte den för utredningen relevanta telefonen beslagtas. Misstänkt nr 2 ville inledningsvis inte tillstå att han hade telefonen, men med stöd av uppgifter från bland annat HDA kunde, vid förhör med misstänkt, den för ärendet relevanta telefonen lokaliseras. Utan HDA kunde utredningen gått miste om vik-

tig kommunikation. Viss sms-konversation mellan misstänkt nr 1 och 2 var avgörande för möjligheten att väcka åtal mot de tre misstänkta i ärendet. Genom HDA kunde viktiga konversationer säkras i ett tidigt skede av utredningen. Detta medförde att tiden för respektive frihetsberövande för de tre misstänka personerna kunde minimeras. I stället för it-forensisk undersökning och genomgång av beslag efter gripanden kunde förhörsledarna omgående ställa rätt frågor till de misstänkta, vilket medförde kortare frihetsberövanden. Utredningsinformation från HDA gjorde också att utredningen direkt kunde riktas mot rätt misstänkta. Utan information från HDA hade tillslaget sannolikt omfattat tvångsmedel mot fler personer. HDA medförde färre och kortare frihetsberövanden, vilket var till gagn för enskilda och gjorde att användningen av statens resurser kunde optimeras. Samtliga tre misstänkta åtalades och dömdes i tingsrätten. Domen har ännu inte vunnit laga kraft.

Exempel 3.16. Näringspenningtvätt, grova brott och grova bokföringsbrott, en gärningsperson kunde identifieras och åtalas, misstankar mot en annan person kunde avskrivas

HDA hade beviljats beträffande en misstänkt i ett ärende rörande grova bokföringsbrott och grova näringspenningtvättsbrott. Uppgifterna från HDA gjorde att en annan person kom att misstänkas och denne person kom sedermera att åtalas och dömas i ärendet. Det var uppgifterna från HDA som gjorde att personen alls kom att misstänkas och utan dessa uppgifter hade personen inte identifierats som gärningsman. Uppgifterna från HDA visade också att den initialt misstänkte personen inte hade en central roll i brottsupplägget. Misstankarna mot den personen försvagades och personen avfördes från förundersökningen i de delarna. Påföljden i tingsrätten mot den person som åtalades och dömdes blev ett flerårigt fängelsestraff. Domen överklagades till hovrätten. Även hovrätten dömde den tilltalade för de åtalade brotten och skärpte därtill fängelsestraffet.

6.5 Hemlig dataavläsning bör vara ett permanent tvångsmedel

Bedömning: Det är utifrån avvägningar om nytta, behov och integritet proportionerligt att hemlig dataavläsning blir ett permanent tvångsmedel. Detta gäller under förutsättning att tillämpningen balanseras med kontrollmekanismer och andra rättssäkerhetsgarantier samt regler för att minska riskerna för den personliga integriteten och informationssäkerheten.

Förslag: Hemlig dataavläsning ska införas som ett permanent tvångsmedel.

6.5.1 Inledning

Hemlig dataavläsning förekom endast i ett fåtal ärenden under de nio månader som åtgärden kunde användas under år 2020. Det huvudsakliga underlaget för våra sammanfattande slutsatser avser därför tillämpningen av hemlig dataavläsning under åren 2021–2022.

Hemlig dataavläsning har regelmässigt använts avseende flera uppgiftstyper samtidigt. Vi gör därför en samlad bedömning av den information som i dag kan inhämtas genom hemlig dataavläsning när vi tar ställning till den övergripande frågan om hemlig dataavläsning bör bli ett permanent tvångsmedel. I våra överväganden om hur den materiella lagstiftningen bör utformas återkommer vi sedan till närmare analyser av var och en av de olika uppgiftstyperna. Om inte annat anmärks avser våra bedömningar och inledande avvägningar den hittillsvarande tillämpningen av hemlig dataavläsning såväl under som utanför en förundersökning.

6.5.2 Hemlig dataavläsning har medfört avsevärd nytta och det finns ett påtagligt behov av hemlig dataavläsning

Eftersom hemlig dataavläsning huvudsakligen används för att komma åt samma typ av information som myndigheterna tidigare fick del av genom andra tvångsmedel får såväl behovet som nyttan av hemlig dataavläsning anses belagda sedan länge. Hemlig dataavläsning har ju också beskrivits som ett sätt att behålla de brottsbekämpande myndigheternas förmåga att inhämta information när de befintliga tvångsmedlen inte längre räcker till.

Den omständigheten att den kvantitativt uppskattade nyttan av hemlig dataavläsning generellt sett är något lägre än för de permanenta tvångsmedlen påverkar inte den bedömningen. Det synes även kunna förklaras av att det är fråga om ett nytt hemligt tvångsmedel som kräver omfattande förarbete för framgångsrik verkställighet. När det gäller hemlig avlyssning och hemlig övervakning av elektronisk kommunikation hämtas informationen vanligen in via operatörer som kontrollerar nätet och vid hemlig kameraövervakning och hemlig rumsavlyssning kan verkställighet ske med hjälp av t.ex. en fastighetsägare. Verkställighet av hemlig dataavläsning innebär att brottsbekämpande myndigheter med olika tekniska hjälpmedel ska försöka ta sig in i en viss elektronisk utrustning, ibland genom att bryta system-

skydd. Vid hemlig dataavläsning har lagstiftaren och myndigheterna således inte samma inflytande över de faktorer som styr huruvida ett tillstånd går att verkställa som vad gäller andra hemliga tvångsmedel. Att hemlig dataavläsning har tillämpats i ökande omfattning talar i sig både för att åtgärden har medfört nytta för brottsbekämpningen och för att det finns ett fortsatt påtagligt behov av hemlig dataavläsning i den brottsbekämpande verksamheten. Som vi inledningsvis har redogjort för finns emellertid betänkligheter med att analysera nytta och effektivitet mot bakgrund av statistik och kvantitativa andelstal. Även med hänsyn till att det är fråga om ett nytt hemligt tvångsmedel är det svårt att dra några mer långtgående slutsatser av dessa siffror. Hemlig dataavläsning ställer höga krav på att verkställighetstekniken fungerar i det enskilda fallet. De brottsbekämpande myndigheterna arbetar ständigt med att förbättra teknik och metoder vad gäller möjligheten att hämta in uppgifter med stöd av hemlig dataavläsning, men också med att analysera och strukturera det inhämtade materialet. Om de brottsbekämpande myndigheterna får fortsatt tillgång till hemlig dataavläsning kan verkställighetsfrekvensen och därmed den kvantitativa nyttan av hemlig dataavläsning på goda grunder förväntas öka.

Samtidigt som redovisningen av den kvantitativa nyttan måste värderas försiktigt bör de erfarenheter om den hittillsvarande tillämpningen som företrädare från de brottsbekämpande myndigheterna delat med sig av få väga tungt. De beskrivningar och praktiska exempel som har lämnats visar att hemlig dataavläsning i många fall har varit ett helt avgörande verktyg i den brottsbekämpande verksamheten. Hemlig dataavläsning har både lett till konkreta uppgifter om brott som redan begåtts och uppgifter som har kunnat användas för att förhindra allvarlig brottslighet. Hemlig dataavläsning har också i flera fall använts för att komma åt information om hur olika typer av grov brottslighet är organiserad och vilka personer som finns högre upp i hierarkin. Eftersom informationen inte hade varit åtkomlig genom andra tvångsmedel har hemlig dataavläsning i dessa fall inneburit ett genombrott för bekämpningen av den allvarliga och organiserade brottsligheten. Den hittillsvarande tillämpningen får sammantaget anses ha medfört en avsevärd nytta i brottsbekämpningen. För detta talar också den omständigheten att hemlig dataavläsning huvudsakligen utgör ett sätt att återställa de brottsbekämpande myndigheternas förmåga att ta del av information. Hemlig dataavläsning utgör

ett nödvändigt komplement till såväl hemliga som öppna tvångsmedel, när de brottsbekämpande myndigheternas förmåga att ta del av information begränsas genom den tekniska utvecklingen.

Den nytta som hemlig dataavläsning har haft i den brottsbekämpande verksamheten visar att det finns ett fortsatt påtagligt behov av hemlig dataavläsning. Även i denna del får de brottsbekämpande myndigheternas uppgifter väga tungt. Mot bakgrund av hur hemlig dataavläsning har tillämpats i förening med den teknik- och brottsutveckling som har skett de senaste åren, är det också tydligt att det finns ett fortsatt påtagligt och reellt behov av hemlig dataavläsning för att bekämpa den allvarliga brottsligheten. Behovet har inte minskat utan snarast ökat sedan frågan senast övervägdes av lagstiftaren. Inget talar för att behovet skulle vara av tillfällig natur.

Det behov och den nytta som konstaterats måste vägas mot de integritetsaspekter som användningen av hemlig dataavläsning kan innebära. Dessa avvägningar behandlar vi i det följande.

6.5.3 Hemlig dataavläsning innebär ökad risk för intrång i enskildas personliga integritet

All användning av hemliga tvångsmedel innebär risker för den personliga integriteten. Som tidigare understrukits är det ytterst omständigheterna i det enskilda fallet som styr hur stort integritetsintrång en viss åtgärd utgör. Mot bakgrund av vad som framkommit om den hittillsvarande tillämpningen kan vi göra några inledande och generella bedömningar beträffande vilka risker för den personliga integriteten som hemlig dataavläsning har medfört.

Inledningsvis finns det skäl att framhålla de starka kontrollmekanismer och andra rättssäkerhetsgarantier som omgärdar regelverket för hemlig dataavläsning. Exempelvis bidrar den obligatoriska domstolsprövningen med det ovillkorliga kravet på offentligt ombud, vars främsta uppgift är att värna enskildas och tredje mans intressen, till att skapa ett rättssäkert system. Vi återkommer i kapitel 8 till alla de kontrollmekanismer och andra rättssäkerhetsgarantier som gäller för hemlig dataavläsning.

På grund av de höga kvalifikationskrav som krävs för att tillämpa hemlig dataavläsning kan vi utgå från att åtgärden har riktats mot samma personkrets som riskerar att bli föremål för andra hemliga tvångsmedel. Risken för att enskilda har utsatts för hemliga tvångs-

medel bara för att de befunnit sig på en viss plats eller har en anhörig som umgås i fel kretsar bedöms därför inte ha ökat med hemlig dataavläsning. Däremot kan informationsinhämtning med stöd av 2 § första stycket 6 och 7 lagen om hemlig dataavläsning ha lett till att fler personer indirekt har berörts av hemliga tvångsmedel än annars. Exempelvis kan en sådan informationsinhämtning omfatta även uppgifter om utomstående personer som finns lagrade på den berördes mobiltelefon. Motsvarande risk finns även vid användning av öppna tvångsmedel som husrannsakan, beslag och genomsökning på distans. Det förtjänar i sammanhanget att åter understrykas att antalet tillstånd till hemlig dataavläsning inte motsvarar antalet verkställda tillstånd. De tillstånd som inte har gått att verkställa har naturligtvis inte heller medfört något integritetsintrång.

Hemlig dataavläsning har ofta har föregåtts av ett annat tvångsmedel för att klarlägga behovet och utreda möjligheterna till verkställighet. Riskbedömningen måste i dessa fall göras utifrån den samlade tvångsmedelsanvändningen. Förfaringssättet bedöms dock inte i sig ha inneburit något avsevärt ökat integritetsintrång, utan talar tvärtom för att hemlig dataavläsning har använts först när andra tvångsmedel inte varit framkomliga alternativ (se avsnitt 6.2.6).

De praktiska erfarenheterna av hemlig dataavläsning visar att de brottsbekämpande myndigheterna av olika skäl har haft svårt att redan i inhämtningsfasen begränsa inhämtningen. Ett tillstånd till hemlig dataavläsning har därför regelmässigt kommit att omfatta flera uppgiftstyper, inklusive de uppgiftstyper i 2 § första stycket 3, 6 och 7 lagen om hemlig dataavläsning som inför lagens ikraftträdande bedömdes innebära en ökad risk för enskildas personliga integritet. Det har också förekommit tillstånd till hemlig dataavläsning som har omfattat flera år långa historiska tidsperioder och det har förekommit tillstånd som inte har förenats med obligatoriska villkor. Hemlig dataavläsning har därför sannolikt kunnat ge tillgång till en stor mängd information om enskilda. Det har emellertid inte framkommit något som talar för att hemlig dataavläsning generellt sett har lett till avsevärt ökade eller omotiverade integritetsintrång i form av t.ex. för långtgående kartläggningar. Den hittillsvarande tillämpningen visar sammantaget inte heller på någon ändamålsglidning av lagstiftningen, dvs. att tillämpningsområdet för hemlig dataavläsning skulle ha sträckt sig utanför vad som avsågs när åtgärden infördes.

Vid integritetsriskbedömningen måste beaktas att risken för ett motsvarande integritetsintrång finns även vid användning av andra öppna och hemliga tvångsmedel. I princip alla de uppgifter som kan hämtas in med stöd av hemlig dataavläsning kan också hämtas in med andra tvångsmedel och utan föregående underrättelse (se t.ex. avsnitt 5.6.1). Det finns inga formella hinder mot att flera tvångsmedel samtidigt riktas mot en och samma person, förutsatt att det bedöms proportionerligt. I detta sammanhang måste den nya tekniska verkligheten beaktas. Den information som tidigare var åtkomlig genom olika traditionella tvångsmedel finns numera regelmässigt lagrad i krypterade enheter och tjänster. Hemlig dataavläsning utgör därmed en nödvändig följd av den digitala utvecklingen för att de brottsbekämpande myndigheterna inte ska förlora sin förmåga att inhämta information. Mobiltelefonen är ett exempel på en informationsbärare med möjligheter att lagra stora mängder privat information. Hemlig dataavläsning av en mobiltelefon *kan* därför i det enskilda fallet innebära inhämtning av en stor mängd uppgifter och en kartläggning av den berörde. Men en fullständig inhämtning av alla uppgifter i en mobiltelefon behöver inte nödvändigtvis innebära ett stort integritetsintrång. Integritetsintrånget beror i det enskilda fallet på hur den berörde väljer att använda sin mobiltelefon. Är det fråga om en s.k. brottstelefon som används tillfälligt och endast i brottsligt syfte är det mindre sannolikt att en fullständig inhämtning av alla uppgifter i mobiltelefonen ger information av mer känslig eller privat karaktär. På motsvarande sätt *kan* hemlig dataavläsning avseende platsuppgifter ge mer precisa uppgifter om geografisk positionering än en traditionell s.k. basstationstömning vid hemlig övervakning av elektronisk kommunikation. Graden av integritetsintrång varierar dock även här i det enskilda fallet. I stadsmiljö kan en brottsbekämpande myndighet inhämta information om geografisk positionering med relativt god precision redan genom en basstationstömning. På landsbygden är det ofta längre mellan basstationerna. I dessa regioner ger därför platsuppgifter inhämtade genom hemlig dataavläsning ofta mer precisa positioneringsuppgifter än en basstationstömning. Detta kan i sin tur innebära en större risk för integritetsintrång.

Även själva verkställighetsmetoden, dvs. det intrång i fysiska utrymmen eller i teknisk utrustning som hemlig dataavläsning innebär, kan i sig innebära en viss ökad risk för den personliga integriteten. I jämförelse med risken för den personliga integriteten som själva

inhämtningen av uppgifter med hemlig dataavläsning innebär bedöms dock sådana intrång utgöra en mindre risk.

När det gäller den hittillsvarande tillämpningen kan därför den generella slutsatsen dras att hemlig dataavläsning kan, men behöver inte, innebära större risker för den personliga integriteten än andra tvångsmedel. När det gäller de enskilda uppgiftstyperna bedömer vi sammantaget att hemlig dataavläsning avseende uppgiftstyperna i punkterna 3, 6 och 7 inte innebär ökade risker för den personliga integriteten i sådan utsträckning som befarades. Hemlig dataavläsning har hittills endast använts under en begränsad tid och i ett begränsat antal fall. Det går inte att utesluta att tillämpningen av hemlig dataavläsning i enskilda fall har inneburit ökade risker för den personliga integriteten. Med dessa reservationer är det mot bakgrund av den hittillsvarande tillämpningen vår samlade bedömning att hemlig dataavläsning generellt sett inte innebär någon avsevärt ökad risk för den personliga integriteten.

Det har tidigare ansetts att det integritetsintrång som hemlig dataavläsning i sig innebär inte bör vara att anse som större enbart av det skälet att ändamålet med användningen av åtgärden är preventivt i stället för brottsutredande (jfr *Tvångsmedel för att förebygga eller förhindra allvarlig brottslighet*, Ds 2005:21 s. 168). Samtidigt saknas det på underrättelsestadiet en konkret brottsmisstanke och det finns därför en större risk för att tvångsmedlet i vissa fall används mot en person som senare visar sig inte vara delaktig i brott. Att tvångsmedelsanvändningen sker utanför förundersökning har tidigare framhållits som en ökad risk för den personliga integriteten (jfr prop. 2019/20:64 s. 87). Den risk för integritetsintrång som preventiva tvångsmedel i sig för med sig måste därför alltid vägas särskilt noga mot behov och effektivitet samt balanseras med rättssäkerhetsgarantier (jfr *Utökade möjligheter att använda preventiva tvångsmedel,* SOU 2022:52 s. 173).

6.5.4 Hemlig dataavläsning innebär även ett stärkt skydd för enskildas integritet

Rätten till skydd för den personliga integriteten handlar inte enbart om risken för att brottsbekämpning innebär oproportionerlig tvångsmedelsanvändning. Den handlar också om enskildas rätt till skydd mot kränkningar från andra enskilda och att rättsväsendet effektivt ingriper när en kränkning har ägt rum. Vi har i avsnitt 5.4.3 närmare

redogjort för detta och för hur artikel 8.1 Europakonventionen innefattar en skyldighet för staten att upprätthålla rättstryggheten för enskilda. Vid integritetsriskbedömningen blir därför också ändamålet med hemlig dataavläsning en viktig aspekt. Hemlig dataavläsning syftar till att allvarlig brottslighet ska kunna förebyggas, förhindras, upptäckas och utredas. Detta kan innebära en upprättelse för eventuella brottsoffer och i förlängningen leda till att gärningspersonen hindras från att begå brott, vilket i sig innebär en ökad rättstrygghet i samhället.

Den hittillsvarande användningen av hemlig dataavläsning bedöms som ovan konstaterats ha lett till förbättrade möjligheter att såväl utreda som att förebygga, förhindra och upptäcka allvarlig brottslighet mot enskilda. I detta avseende har hemlig dataavläsning också inneburit ett förstärkt skydd för enskildas personliga integritet.

6.5.5 Det är proportionerligt att permanenta bestämmelserna om hemlig dataavläsning

I samband med att lagen om hemlig dataavläsning infördes konstaterade regeringen att det som var känt om behovet av hemlig dataavläsning och åtgärdens effektivitet vägde så tungt att de aktuella inskränkningar av de rättigheter och det skydd som tillkommer enskilda enligt regeringsformen, Europakonventionen och EU:s rättighetsstadga var godtagbara (se a. prop. s. 96 ff.). En grundläggande förutsättning för att staten ska kunna leva upp till kraven på att upprätthålla rättstryggheten för enskilda är vidare att staten har en väl fungerande och effektiv brottsbekämpning. Detta krav innebär bl.a. att myndigheterna måste ha tillgång till effektiva utredningsverktyg för att kunna utreda brott som innefattar allvarliga kränkningar. Som tidigare redogjorts för har hemlig dataavläsning införts för att återställa de brottsbekämpande myndigheternas förmåga att inhämta information som inte längre är åtkomlig genom traditionella hemliga tvångsmedel. Hemlig dataavläsning får därmed anses väl förenligt med statens skyldigheter att uppfylla sina åtaganden enligt artikel 8 i Europakonventionen, jfr målet K.U mot Finland (se avsnitt 5.4.3).

En grundläggande förutsättning för att permanenta bestämmelserna om hemlig dataavläsning är dock att åtgärden kan anses proportionerlig i förhållande till nytta, integritet och behov. I det föregående har vi separat behandlat dessa olika frågor. Även om bestämmelserna om hemlig dataavläsning har varit i kraft en förhållandevis kort tid,

bedömer vi att underlaget från den hittillsvarande tillämpningen är tillräckligt omfattande för att kunna göra en övergripande analys av dessa frågor. Vi har konstaterat att den hittillsvarande tillämpningen av hemlig dataavläsning har medfört avsevärd nytta och effektivitet i brottsbekämpningen och att det finns ett fortsatt påtagligt behov av hemlig dataavläsning. Det saknas mindre ingripande alternativ till hemlig dataavläsning för att få samma effekt och nytta. Vi anser därför att åtgärden är nödvändig med hänsyn till intresset av att bekämpa den allvarliga brottsligheten. Vi har även konstaterat att hemlig dataavläsning i vissa avseenden kan medföra risker för enskildas personliga integritet. Åtgärden har i andra avseenden inneburit en förstärkning av enskildas rätt till skydd mot allvarliga brott, dvs. en ökad rättstrygghet och ett förstärkt skydd för den personliga integriteten.

Vid en avvägning bedömer vi att den ökade risk för den personliga integriteten som hemlig dataavläsning kan innebära är försvarlig för att kunna ge de brottsbekämpande myndigheterna mer effektiva verktyg. Vår slutsats är därmed att det är proportionerligt att de brottsbekämpande myndigheterna får använda hemlig dataavläsning som tvångsmedel, såväl under som utanför en förundersökning. Vår bedömning gäller även med beaktande av att preventiv tvångsmedelsanvändning i sig anses medföra en ökad integritetsrisk. Det finns inget som tyder på att behovet av hemlig dataavläsning skulle vara av tillfällig natur eller att reglerna av andra skäl bör vara tidsbegränsade. Vi föreslår därför att bestämmelserna ska permanentas.

För att regleringen ska kunna anses ändamålsenlig och proportionerlig är det en förutsättning att tillämpningsområdet avgränsas på ett ändamålsenligt och tydligt sätt samt att riskerna för den personliga integriteten och informationssäkerheten balanseras med tillräckliga kvalifikationskrav, kontrollmekanismer och andra rättssäkerhetsgarantier. Regleringen måste med andra ord vara utformad så att missbruk förhindras och att ändamålsglidningar mot t.ex. omotiverade kartläggningar eller övervakningar av privatlivet inte kan förekomma. Vi redovisar våra närmare överväganden i detta avseende och vidare proportionalitetsavvägningar i kapitel 7–8. Där behandlar vi frågor om hur den materiella lagstiftningen bör utformas för att uppnå en mer effektiv brottsbekämpning, samtidigt som respekten för grundläggande fri- och rättigheter, liksom kraven på rättssäkerhet och informationssäkerhet, säkerställs. Frågan om placeringen av bestämmelserna återkommer vi till i kapitel 9.

7 Tillämpningsområdet för hemlig dataavläsning

7.1 Uppdraget

Vi har i kapitel 6 kommit fram till att det utifrån avvägningar om nytta, behov och integritet är proportionerligt att hemlig dataavläsning blir ett permanent tvångsmedel, såväl under som utanför en förundersökning. Frågeställningarna i detta kapitel handlar om huruvida tillämpningsområdet för hemlig dataavläsning är ändamålsenligt och proportionerligt avgränsat samt om det bör göras förändringar i regelverket i syfte att uppnå en mer effektiv brottsbekämpning.

I avsnitt 7.2 föreslår vi att innebörden av hemlig dataavläsning ska förtydligas. I avsnitt 7.3 behandlar vi den övergripande frågan om vilka uppgiftstyper som hemlig dataavläsning ska omfatta. Beslut om hemlig dataavläsning ska vara tydliga och förutsebara. Vi föreslår därför vissa förtydliganden avseende uppgiftstyperna i 2 § första stycket lagen om hemlig dataavläsning. Stora delar av tillämpningsområdet för hemlig dataavläsning har helt nyligen setts över av andra utredningar. I avsnitt 7.4 och 7.5 presenterar vi de lagändringar om utökade möjligheter att använda hemlig dataavläsning som nyligen har trätt i kraft alternativt förväntas träda i kraft inom kort. Vi ställer oss sammantaget bakom de föreslagna utökningarna av tillämpningsområdet för hemlig dataavläsning. I avsnitt 7.4.4 föreslår vi för egen del att det ska införas utökade möjligheter att använda hemlig dataavläsning i syfte att utreda vem som skäligen kan misstänkas för ett visst brott eller delaktighet i viss brottslighet. I avsnitt 7.6 gör vi avslutningsvis en övergripande proportionalitetsbedömning, där vi beaktar det samlade integritetsintrång som de olika utökningarna av tillämpningsområdet för hemlig dataavläsning kan medföra.

7.2 Bör innebörden av hemlig dataavläsning förtydligas?

Förslag: Det ska klargöras att hemlig dataavläsning innebär att uppgifter, som är avsedda för automatiserad behandling och som är åtkomliga i ett avläsningsbart informationssystem, inhämtas i hemlighet och med ett tekniskt hjälpmedel.

Skälen för vårt förslag

Innebörden av hemlig dataavläsning bör förtydligas

Hemlig dataavläsning har använts som benämning på det nya tvångsmedlet alltsedan frågan officiellt kom upp på regeringens agenda år 2005 (se betänkandet *Tillgång till elektronisk kommunikation i brottsutredningar m.m.*, SOU 2005:38, och dir. 2016:36). Uttrycket är ursprungligen hämtat från den danska förebilden *dataaflæsning* (se retsplejeloven § 791 b), men motsvarar också den terminologi som används i vissa andra länder. Hemlig dataavläsning är ett samlingsbegrepp för den process som sker när information, med tillämpning av lagen om hemlig dataavläsning, inhämtas från ett avläsningsbart informationssystem, bearbetas och tillgängliggörs för senare granskning. Att på ett teknikneutralt sätt juridiskt beskriva den närmare innebörden av hemlig dataavläsning är förenat med svårigheter.

Lagen om hemlig dataavläsning inleds med en definition som beskriver och avgränsar innebörden av hemlig dataavläsning. Där anges att hemlig dataavläsning innebär att uppgifter, som är avsedda för automatiserad behandling, i hemlighet och med ett tekniskt hjälpmedel *läses av eller tas upp* (vår kursivering) i ett avläsningsbart informationssystem. Legaldefinitionen av hemlig dataavläsning tar sin utgångspunkt i definitioner av andra hemliga tvångsmedel och straffbestämmelsen om dataintrång (se avsnitt 3.2.3).

Metoden för hemlig dataavläsning är emellertid unik. Hemlig dataavläsning kan användas för att hämta in olika typer av uppgifter och inbegriper därför en rad olika tillvägagångssätt. Processen för själva inhämtandet av uppgifter beskrivs på olika sätt i definitionerna av de bakomliggande hemliga tvångsmedlen. I inhämtningslagen används genomgående uttrycket *inhämtning* för att beskriva tvångsmedlet.

I bestämmelsen om hemlig avlyssning av elektronisk kommunikation anges att meddelanden *avlyssnas eller tas upp* genom ett tekniskt hjälpmedel *för återgivning av innehållet i meddelandet*, se 27 kap. 18 § rättegångsbalken. Hemlig övervakning av elektronisk kommunikation innebär enligt 27 kap. 19 § rättegångsbalken att vissa i bestämmelsen närmare angivna uppgifter *hämtas in*. Hemlig kameraövervakning innebär enligt definitionen i 27 kap. 20 a § rättegångsbalken *optisk personövervakning*. Med hemlig rumsavlyssning avses enligt 27 kap. 20 d § rättegångsbalken *avlyssning eller upptagning* av tal eller samtal, med ett tekniskt hjälpmedel som är avsett att *återge ljud*. Under lagstiftningsarbetet som föregick lagen om hemlig dataavläsning valdes uttrycket ”läses av eller tas upp” för att beskriva metoden för hemlig dataavläsning. Uttrycket har viss förebild i den danska förlagan där metoden beskrivs som *aflæsning*. Med ”läses av eller tas upp” avses dock enligt de svenska förarbetena inte bara själva inhämtningen av uppgifterna. Uttrycket tar enligt förarbetena sikte både på den tekniska process som utförs av en dator eller annat tekniskt hjälpmedel för att exempelvis göra informationen läsbar och på den process som sker när den som ska granska uppgifterna tar del av informationsinnehållet. Med ”tas upp” avses att tydliggöra att uppgifterna kan sparas och att de får granskas såväl i realtid som i efterhand (se SOU 2017:89 s. 336 samt prop. 2019/20:64 s. 102 f. och 210).

Lagrådet angav i sitt yttrande över förslaget till en lag om hemlig dataavläsning att definitionen ”läses av eller tas upp” framstår som ofullständig genom att det inte kommer till uttryck att den verkställande myndigheten, efter att uppgifterna tagits upp i ett avläsningsbart informationssystem, hämtar in uppgifterna för att ta del av dem. Regeringen höll med om att det i definitionen visserligen inte uttryckligen anges att de verkställande myndigheterna hämtar in uppgifterna för att ta del av dem efter att de tagits upp. Regeringen ansåg dock att definitionen på ett tillräckligt tydligt sätt ger uttryck för att myndigheterna får tillåtelse att ta del av de uppgifter som tagits upp. Regeringen framhöll att definitionen av hemlig dataavläsning i det sammanhanget är uppbyggd på samma sätt som definitionerna av hemlig avlyssning av elektronisk kommunikation och hemlig rumsavlyssning. Även där anses det inrymmas i den åtgärd som vidtas att de brottsbekämpande myndigheterna får tillgodogöra sig den information som tagits upp. I dessa bestämmelser anges emellertid att åtgärden sker med eller genom ett tekniskt hjälpmedel, i syfte att återge

ljud alternativt innehållet i meddelandet (vår anmärkning). Regeringen framhöll därtill att definitionen inte heller avviker principiellt från reglerna om beslag, där det inte särskilt föreskrivs att de brottsbekämpande myndigheterna får tillgodogöra sig informationen i det material som har tagits i beslag (se a. prop. s. 103).

Det framstår som naturligt att lagstiftaren under lagstiftningsarbetet med lagen om hemlig dataavläsning valde den terminologi som överensstämmer med utländska förebilder. Den hittillsvarande tillämpningen visar dock att det finns goda skäl att på nytt överväga definitionen av hemlig dataavläsning. Företrädare för både domstolarna och de brottsbekämpande myndigheterna har till utredningen framfört att uttrycket ”läses av eller tas upp” i vissa avseenden kan vara missvisande och orsaka tillämpningssvårigheter. Uttrycket får nämligen betydelse för tillämpningen av andra bestämmelser i lagen om hemlig dataavläsning, bestämmelser som inte bara tar sikte på själva metoden för åtgärden. Uttrycket ”läses av eller tas upp” återkommer i 2, 9, 17, 18, 23 §§ och i rubriken till 27 § lagen om hemlig dataavläsning. Den nuvarande definitionen riskerar att bli missvisande eftersom bestämmelserna i 2, 9, 17 och 18 §§ tar tydligt sikte på själva inhämtningen av uppgifter, medan förbudsbestämmelserna i 23 och 27 §§ i praktiken både handlar om verkställighet och om hur otillåtna uppgifter som oavsiktligt har hämtats in ska hanteras. Vi återkommer i avsnitt 8.5.6 närmare till dessa bestämmelser. Definitionen av hemlig dataavläsning kan även indirekt komma att påverka tillämpningen av andra bestämmelser i lagen, t.ex. villkorsbestämmelsen i 18 § första stycket 4. Som kommer att framgå i avsnitt 8.4.5 utgör villkor som avser själva granskningen av de inhämtade uppgifterna ett viktigt skydd för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan. Villkor som avser inhämtningsfasen är däremot i vissa fall svåra att uppfylla. Den nuvarande definitionen kan medföra att villkor som egentligen var avsedda att tillämpas under antingen inhämtningsfasen eller granskningsfasen blir styrande under hela processen, vilket i sin tur kan medföra oavsiktliga hinder för verkställighet. Innebörden av hemlig dataavläsning bör därför förtydligas.

Uttrycket ”läses av eller tas upp” ska ersättas med ”inhämtas”

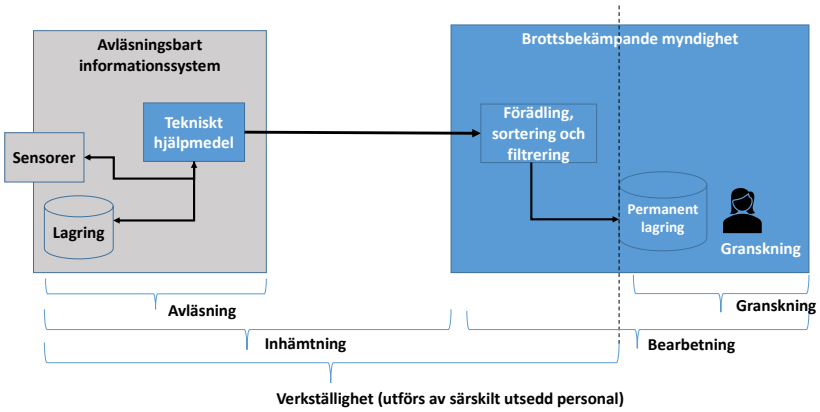
Hemlig dataavläsning innebär legala inskränkningar i den enskildes grundläggande fri- och rättigheter. Det är därför angeläget att definitionen av hemlig dataavläsning avgränsas på ett tydligt och korrekt sätt. Nedan illustreras i ett förenklat flödesschema hur hemlig dataavläsning går till i praktiken.

1. Ansökan om och tillstånd till hemlig dataavläsning

   Frågor om hemlig dataavläsning prövas av rätten på ansökan av åklagare eller Säkerhetspolisen, se 14 § lagen om hemlig dataavläsning. Tillstånd till hemlig dataavläsning meddelas av rätten. Kraven på tillståndet framgår av 18 § lagen om hemlig dataavläsning. Tillståndet utgör en del av själva beslutet som i sin tur ska förenas med villkor. Vi återkommer till olika frågor om ansökan och tillstånd i avsnitt 8.4. Förfarandet vid hemlig dataavläsning omfattar *inhämtning* och *bearbetning* (inklusive *granskning*) av den inhämtade informationen, se figur 7.1.

   Ett typiskt tillstånd till hemlig dataavläsning omfattar uppgiftstyperna i 2 § första stycket 1–3 samt 6 och 7 lagen om hemlig dataavläsning. Det innebär som utgångspunkt att alla lagrade uppgifter och realtidsuppgifter som sorterar under dessa punkter och som under verkställighetsperioden är åtkomliga i det avläsningsbara informationssystemet omfattas av tillståndet. Ett tillstånd till hemlig dataavläsning ska dock som huvudregel förenas med villkor som avgränsar tillståndet. Exempelvis kan ett tillstånd avgränsas genom villkor som innebär att vissa mejl som finns i de inhämtade filerna inte får *granskas*, t.ex. mejl som har upprättats eller ändrats före ett visst datum.

Figur 7.1 Inhämtning (avläsning och överföring) samt bearbetning (förädling, sortering, filtrering och granskning) av uppgifter



2. Inhämtning (avläsning och överföring) av uppgifter

Den initiala process som sker vid hemlig dataavläsning kallas ofta *avläsning*. Efter avläsningen *överförs* information från det avläsningsbara informationssystemet till den brottsbekämpande myndigheten. Uttrycket inhämtning kan därför användas för att beskriva både avläsning och överföring av information. Med denna terminologi ingår hela inhämtningen i verkställigheten. Verkställigheten omfattar, efter inhämtningen, emellertid även viss förädling, sortering och filtrering. Av figur 7.1. framgår att verkställighetsfasen omfattar de moment som finns till vänster om den streckade linjen. I 26 § lagen om hemlig dataavläsning anges att hemlig dataavläsning ska verkställas av särskilt utsedd personal. Den personalen finns hos den verkställande myndigheten, dvs. Polismyndigheten, Säkerhetspolisen eller Tullverket. Verkställighet av hemlig dataavläsning innebär försök till alternativt inhämtning av uppgifter i enlighet med meddelat tillstånd. Hur verkställigheten sker anpassas efter förhållandena i det enskilda fallet. Eftersom granskning av information från hemlig dataavläsning är mycket resurskrävande strävar den verkställande myndigheten efter att inte hämta in mer information än nödvändigt. Verkställigheten begränsas också av krav på teknikanpassning i kombination med de villkor som avgränsar ett tillstånd. Med verkställighetsperioden eller verkställighetstiden avses hela den tid under vilken

inhämtning av uppgifter, med beaktande av villkoren för tillståndet, får ske (se avsnitt 8.4.4 och 8.4.5). Bestämmelser om genomförandet av hemlig dataavläsning finns huvudsakligen i 22–26 §§ lagen om hemlig dataavläsning. Vi återkommer till dessa verkställighetsbestämmelser i avsnitt 8.5.

Den information som i vårt exempel läses av och förs över i inhämtningsfasen består alltså av uppgifter som under verkställighetstiden finns åtkomliga i datorn, i mejlkontot.

3. Bearbetning (förädling, sortering, filtrering och granskning) av uppgifter

   I anslutning till inhämtningen *bearbetas* den inhämtade informationen. Bearbetningen kan vara såväl maskinell som manuell och den kan ske både i realtid och i efterhand. I bearbetningsfasen förekommer att rådata *förädlas* i form av t.ex. uppackning eller avkodning för att informationen ska bli läsbar. Den inledande bearbetningen omfattar även *sortering* och *filtrering* och syftar till att information, som överensstämmer med tillståndet, tillgängliggörs för *granskning*. Om det under bearbetningen påträffas otillåtna uppgifter, dvs. uppgifter som strider mot tillståndets villkor eller förbudsbestämmelserna, sorteras även sådana uppgifter bort. Därefter lagras den kvarvarande informationen och tillgängliggörs för efterföljande granskning. Vid denna senare del av bearbetningen sker själva analysen av informationen. I avsnitt 8.5 återkommer vi till frågor om hur den information som har hämtats in genom hemlig dataavläsning får och ska hanteras. I det avsnittet återkommer vi också särskilt till hanteringen av bortsorterad eller bortfiltrerad information.

   I vårt exempel sker alltså i anslutning till inhämtningen en tidig bearbetning av den inhämtade informationen. Endast mejl som omfattas av granskningsvillkoren för tillståndet får granskas och analyseras av beställaren.

Det är vår bedömning att innebörden av hemlig dataavläsning bör kunna utläsas i lagtexten. Redan det förhållandet att det inte tydligt framgår av ordalydelsen om begreppsparet ”läses av eller tas upp” syftar både på inhämtningen och den efterföljande granskningen av inhämtade uppgifter eller inte gör att det finns skäl att överväga definitionen av hemlig dataavläsning. Med hänsyn till hur hemlig data-

avläsning utförs och hur andra bestämmelser är uppbyggda finns dessutom flera goda skäl att begränsa legaldefinitionen till själva inhämtningen av uppgifter medan bearbetningen, inklusive granskningen, av desamma regleras i lagen utan att definieras som en del av själva dataavläsningen. En sådan ordning skulle vara tydligare och innebära att tillämpningen av övriga bestämmelser i lagen bättre överensstämmer med lagstiftarens avsikter. Att inhämtade uppgifter får bearbetas och granskas följer redan både direkt och indirekt av andra bestämmelser i lagen.

De tekniska metoderna för verkställigheten av hemlig dataavläsning kan se olika ut och förändras över tid. Det begrepp som beskriver själva processen för informationsinhämtningen bör därför vara teknikneutralt. I förarbetena bakom bestämmelsen om hemlig övervakning av elektronisk kommunikation anges att uttrycket ”hämtas in” avser att markera att tyngdpunkten vid tvångsmedelsanvändningen ligger på den myndighet som begär och får rättens tillstånd till åtgärden (se prop. 1992/93:200 s. 332). I betänkandet bakom lagen om hemlig dataavläsning angavs att det som avses med ”läses av eller tas upp” är just ”inhämtning” och att det begreppet ryms i begreppen avläsning och upptagning (se a. SOU s. 498). Uttrycket ”inhämtning” framstår visserligen inte heller som en optimal definition, men uttrycket särskiljer på ett tydligare sätt än tidigare själva inhämtningen från granskningen av de uppgifter som inhämtas.

Vi föreslår därför att det nuvarande uttrycket ”läses av eller tas upp” i 1 § lagen om hemlig dataavläsning ska ersättas med uttrycket ”inhämtas”. Vårt förslag innebär en tydligare och därmed mer förutsebar lagstiftning. Någon ändring i sak är inte avsedd. Ett förtydligande av legaldefinitionen innebär ett indirekt förtydligande av övriga bestämmelser i lagen om hemlig dataavläsning. Förslaget innebär på detta sätt en förstärkt rättssäkerhetsgaranti. Ett tydligt särskiljande av inhämtningsfasen från granskningsfasen bedöms också kunna medföra bättre förutsättningar för utformningen av tydliga villkor (se exempel 1–3 i avsnitt 8.4.5). Detta innebär i sin tur ett starkare skydd för enskildas personliga integritet.

7.3 Uppgiftstyper och differentiering

7.3.1 Vilka uppgiftstyper ska omfattas av hemlig dataavläsning?

Bedömning: Tillstånd till hemlig dataavläsning bör även fortsättningsvis medföra rätt att hämta in alla de uppgiftstyper som i dag omfattas av hemlig dataavläsning.

Skälen för vår bedömning

Utgångspunkter

Hemlig dataavläsning omfattar i dag sju separata uppgiftstyper, uppräknade i 2 § första stycket lagen om hemlig dataavläsning:

1. kommunikationsavlyssningsuppgifter,
1. kommunikationsövervakningsuppgifter,
2. platsuppgifter,
3. kameraövervakningsuppgifter,
4. rumsavlyssningsuppgifter,
5. övriga lagrade uppgifter och
6. övriga uppgifter som visar hur viss teknisk utrustning används.

Inför att den nya lagen om hemlig dataavläsning infördes genomfördes omfattande behovsanalyser. Man fann då ett påtagligt behov av hemlig dataavläsning för att läsa av eller ta upp (dvs. hämta in) alla nuvarande sju uppgiftstyper i syfte att bekämpa den allvarliga brottsligheten, såväl under som utanför en förundersökning (se SOU 2017:89 s. 247 ff. och prop. 2019/20:64 s. 69 ff.). Vi delar dessa slutsatser. Behovsanalyserna är gjorda i närtid och företrädare för de brottsbekämpande myndigheterna har också vidhållit vad som tidigare anförts i utförliga behovsbeskrivningar. Dessa finns redovisade i en bilaga till det tidigare betänkandet, se a. SOU s. 603 ff. Mot bakgrund av vad som i kapitel 6 konstaterats om den hittillsvarande tillämpningen får det anses klarlagt att det finns ett fortsatt påtagligt och reellt behov av att kunna använda hemlig dataavläsning som metod för att hämta

in alla de uppgiftstyper som i dag omfattas av åtgärden. Den hittillsvarande tillämpningen visar också att hemlig dataavläsning beträffande alla uppgiftstyper, om än i varierande omfattning, har medfört nytta i den brottsbekämpande verksamheten. När det gäller avvägningar mot de integritetsintrång som de enskilda uppgiftstyperna kan innebära har lagstiftaren valt att balansera dessa risker både genom ett allmänt differentieringskrav och specifika kvalifikationskrav. Kvalifikationskraven har utformats med de permanenta hemliga tvångsmedlen som förebilder. Regelverket för hemlig dataavläsning omgärdas härutöver av motsvarande kontrollmekanismer och andra rättssäkerhetsgarantier som de permanenta hemliga tvångsmedlen. Vi återkommer till dessa i kapitel 8.

Sedan lagen om hemlig dataavläsning trädde i kraft har frågan om utökade möjligheter att använda såväl öppna som hemliga tvångsmedel utretts. Nya och utvidgade möjligheter till tvångsmedelsanvändning har nyligen införts och ytterligare förslag är för närvarande under beredning (se avsnitt 5.3.4). I våra överväganden och integritetsavvägningar måste vi förhålla oss till den pågående utvecklingen. När det specifikt gäller tillämpningsområdet för hemlig dataavläsning har detta nyligen utökats i huvudsakligen motsvarande mån som tillämpningsområdet för de permanenta hemliga tvångsmedlen. Ändamålet med hemlig dataavläsning är att utreda vissa allvarliga brott samt att förebygga, förhindra eller upptäcka viss allvarlig brottslighet. Hemlig dataavläsning kan förenklat beskrivas som en ny metod att få åtkomst till samma slags uppgifter som bakomliggande hemliga tvångsmedel och vissa öppna tvångsmedel som beslag, husrannsakan och genomsökning på distans ger tillgång till. Vår utgångspunkt är därför att det är av väsentlig betydelse att hemlig dataavläsning kan användas i motsvarande fall som andra hemliga tvångsmedel, men även vissa öppna tvångsmedel. Det finns annars risk för att allvarlig brottslighet inte kan bekämpas när viss information är oåtkomlig genom traditionella tvångsmedel. I våra integritetsriskbedömningar nedan utgår vi därför också från en jämförelse med vilka andra möjligheter som finns att komma åt motsvarande uppgifter.

Kommunikationsavlyssnings- och kommunikationsövervakningsuppgifter

Hemlig dataavläsning avseende kommunikationsavlyssnings- och kommunikationsövervakningsuppgifter kan jämställas med en metod för att verkställa hemlig avlyssning och hemlig övervakning av elektronisk kommunikation samt viss inhämtning enligt inhämtningslagen. Kvalifikationskraven för att få använda hemlig dataavläsning avseende dessa uppgiftstyper överensstämmer huvudsakligen med kvalifikationskraven för hemlig avlyssning av elektronisk kommunikation. Hemlig dataavläsning avseende kommunikationsavlyssnings- och kommunikationsövervakningsuppgifter bedöms därför inte innebära någon beaktansvärd ökad risk för den personliga integriteten. Motsvarande bedömningar gjordes även inför ikraftträdandet av lagen om hemlig dataavläsning, utifrån dåvarande förhållanden (se a. SOU s. 302 och a. prop. s. 85).

Platsuppgifter

Hemlig dataavläsning avseende platsuppgifter kan jämställas med en metod för att verkställa hemlig övervakning av elektronisk kommunikation och viss inhämtning enligt inhämtningslagen. Platsuppgifter från hemlig dataavläsning kan, men behöver inte, ge mer precisa uppgifter om geografisk positionering än nämnda hemliga tvångsmedel. Detta får anses innebära en viss ökad risk för den personliga integriteten. Motsvarande bedömning gjordes även inför ikraftträdandet av lagen om hemlig dataavläsning, utifrån dåvarande förhållanden (se a. SOU s. 302 och a. prop. s. 86). Lagstiftaren har valt att balansera den ökade integritetsrisken bl.a. genom att sätta kvalifikationskraven för att hämta in platsuppgifter högre än för hemlig övervakning av elektronisk kommunikation. Kraven för att använda hemlig dataavläsning avseende platsuppgifter motsvarar därför de som gäller för hemlig avlyssning av elektronisk kommunikation. Den ökade integritetsrisk som hemlig dataavläsning avseende platsuppgifter kan innebära får vid en avvägning accepteras för att kunna ge de brottsbekämpande myndigheterna mer effektiva åtgärder (jfr a. prop. s. 94).

Kameraövervaknings- och rumsavlyssningsuppgifter

Hemlig dataavläsning avseende kameraövervaknings- och rumsavlyssningsuppgifter kan jämställas med en metod för att verkställa hemlig kameraövervakning respektive hemlig rumsavlyssning. Kvalifikationskraven för att få använda hemlig dataavläsning avseende dessa uppgiftstyper överensstämmer med kvalifikationskraven för de bakomliggande hemliga tvångsmedlen. Hemlig dataavläsning avseende kameraövervaknings- och rumsavlyssningsuppgifter bedöms därför inte innebära någon beaktansvärd ökad risk för den personliga integriteten. Motsvarande bedömningar gjordes även inför ikraftträdandet av lagen om hemlig dataavläsning, utifrån dåvarande förhållanden (se a. SOU s. 303 och a. prop. s. 86).

Lagrade uppgifter och uppgifter som visar hur viss utrustning används

Hemlig dataavläsning med stöd av 2 § första stycket 6 lagen om hemlig dataavläsning innebär inhämtning av elektroniskt lagrade uppgifter som inte omfattas av uppgiftstyperna i punkt 1–5. I författningskommentaren anges att det saknar betydelse hur uppgifterna har lagrats, dvs. om de har lagrats genom en medveten handling av en person eller till följd av en inställning i informationssystemet som användaren inte har känt till. Det saknar vidare betydelse om uppgifterna är varaktigt eller temporärt lagrade eller i vilket format de har lagrats. Uppgifterna ska dock finnas lagrade i informationssystemet när inhämtningen genomförs (jfr a. prop. s. 213). Förenklat uttryckt avses uppgifter som inte har kommunicerats, t.ex. fotografier, utkast till meddelanden, upprättade anteckningar eller kontaktböcker. Sådana uppgifter är inte åtkomliga genom andra hemliga tvångsmedel. Enligt experterna i utredningen kallas uppgifterna ibland för husrannsakningsuppgifter eftersom de under vissa förutsättningar kan hämtas in genom husrannsakan, beslag och genomsökning på distans.

Hemlig dataavläsning med stöd av 2 § första stycket 7 lagen om hemlig dataavläsning innebär inhämtning av uppgifter som visar hur ett avläsningsbart informationssystem används, men som inte omfattas av uppgiftstyperna i punkt 1–6. Med sådana uppgifter avsågs enligt förarbetena realtidsuppgifter om vad en användare av ett informationssystem använder detta till. Som exempel angavs vilka program eller applikationer som körs, elektroniska anteckningar som

görs men inte sparas och hur informationssystemet i andra avseenden används (se a. SOU s. 343). Säkerhets- och integritetsskyddsnämnden har i sin första särskilda granskning av tillämpningen av hemlig dataavläsning noterat att domstolar har beviljat tillstånd till hemlig dataavläsning enligt punkt 7 både för historisk tid och för realtid (se nämndens uttalande med beslut av den 15 december 2021, dnr 92-2020, s. 10). Av såväl bestämmelsens ordalydelse som förarbetena framgår dock att hemlig dataavläsning med stöd av punkt 7 bara kan avse uppgifter i realtid. Om det finns *lagrade* uppgifter som visar hur ett avläsningsbart informationssystem *har* använts måste de uppgifterna falla under någon av punkterna 1–6.

Att uppgiftstyperna i punkt 6 och 7 är sekundära i förhållande till övriga punkter innebär att en uppgift bara kan vara en punkt 6- eller 7-uppgift om den inte kan sorteras under punkt 1–5. Uppgifter som avses i punkt 7 är vidare sekundära i förhållande till uppgifter i punkten 6, vilket innebär att endast en begränsad mängd uppgifter faller under punkten 7. Detta eftersom de flesta uppgifter som går in i ett informationssystem lagras, om inte långsiktigt så i vart fall kortsiktigt eller tillfälligt. Realtidsuppgifter som härrör från användandet av en dator (t.ex. öppnande av filer, uppstart eller stängning av program och anslutning av externa lagringsmedier) kan t.ex. sparas ner en kortare tid i internminnet eller tillfälligt i processorn. Om sådana uppgifter avläses i realtid kan de falla under punkten 7, men om uppgifterna finns lagrade – om än bara tillfälligt – när inhämtningen genomförs är det inte helt klart om uppgifterna bör kategoriseras under punkten 6 och inte under punkten 7. Vissa uppgifter lagras inte alls. Det kan t.ex. handla om tangenttryckningar. Det kan alltså förefalla slumpmässigt vilka uppgifter som lagras och vilka som inte gör det. Det innebär att uppgiftstyperna i punkt 6 och 7 sällan kan särskiljas. Tillstånd för att kunna ta del av punkt 7-uppgifter förekommer därför i praktiken i princip alltid i förening med ett tillstånd till punkt 6-uppgifter (se tabell 6.2 i kapitel 6). Som påpekats i förarbetena skulle det vara stötande om de brottsbekämpande myndigheternas förmåga till brottsbekämpning skulle bero på en teknisk slump (se a. prop. s. 79). Hemlig dataavläsning bör därmed även fortsättningsvis kunna användas för att i hemlighet och i realtid ta del av vad som sker på den tekniska utrustning som åtgärden avser och alltså fånga upp både sådana uppgifter som lagras och sådana som inte lagras, inte minst eftersom lagstiftningen ska vara teknikneutral. Vi återkommer i föl-

jande avsnitt till frågan om det är ändamålsenligt att göra skillnad på uppgiftstyperna.

Merparten av de uppgifter som kan hämtas in med stöd av uppgiftstyperna i 2 § första stycket 6 och 7 kan som konstaterats i och för sig hämtas in under förundersökning även med stöd av öppna tvångsmedel. Sedan lagen om hemlig dataavläsning trädde i kraft har det införts utökade möjligheter att hämta in motsvarande uppgifter med öppna tvångsmedel. Vidare är frågan om genomsökning på distans ska kunna användas även i underrättelseverksamhet för närvarande under beredning (se slutbetänkande *Utökade möjligheter att använda preventiva tvångsmedel 2*, SOU 2023:60). Mot denna bakgrund skulle det kunna påstås att informationsinhämtning med stöd av dessa uppgiftstyper inte innebär någon beaktansvärd ökad risk för den personliga integriteten. Hemlig dataavläsning utförs emellertid i hemlighet och behovet av uppgiftstyperna föreligger även i underrättelsefallen, där det för närvarande inte finns någon annan möjlighet att hämta in motsvarande uppgifter. En viktig skillnad är att hemlig dataavläsning av uppgiftstyperna i punkt 6 och 7, till skillnad från åtkomst till motsvarande uppgifter genom öppna tvångsmedel, kan innebära en löpande övervakning av det informationssystem som åtgärden avser, i anslutning till att det används. Ytterligare en skillnad som är relevant är att det vid genomsökning på distans inte är tillåtet att bryta systemskydd. Det krävs då att de brottsbekämpande myndigheterna har tillgång till inloggningsuppgifter eller motsvarande för att kunna skaffa sig åtkomst till informationssystemet (jfr prop. 2021/22:119 s. 82). Vi bedömer sammantaget att hemlig dataavläsning med stöd av 2 § första stycket 6 och 7 innebär en viss ökad risk för den personliga integriteten jämfört med andra möjligheter att hämta in motsvarande information. Detta överensstämmer i princip med de bedömningar som, utifrån dåvarande förhållanden, gjordes inför ikraftträdandet av lagen om hemlig dataavläsning (se SOU 2017:89 s. 304 ff. och a. prop. s. 86 f.).

Lagstiftaren har valt att balansera de ökade integritetsriskerna bl.a. genom att låta kvalifikationskraven för att få använda hemlig dataavläsning avseende uppgiftstyperna i punkt 6 och 7 motsvara de som gäller för hemlig avlyssning av elektronisk kommunikation. Det ska noteras att de formella rekvisiten härför är desamma som för hemlig kameraövervakning (jfr a. SOU s. 304 ff. och a. prop. s. 87). De ökade risker för den personliga integriteten som hemlig dataavläsning av uppgifter som faller under punkterna 6 och 7 kan innebära framstår mot

denna bakgrund som försvarliga. Riskerna får accepteras för att de brottsbekämpande myndigheterna ska kunna behålla de effektiva åtgärder som den tillfälliga lagen om hemlig dataavläsning medfört (jfr a. prop. s. 95 ff.).

Sammanfattande bedömning

Utifrån avvägningar om nytta, behov och integritet framstår det som både ändamålsenligt och proportionerligt att hemlig dataavläsning även fortsättningsvis får omfatta samma uppgiftstyper som i dag. Med hänsyn till hur hemlig dataavläsning har tillämpats i praktiken bör det övervägas om det är ändamålsenligt att differentiera olika uppgiftstyper och i sådant fall på vilket sätt.

7.3.2 Beslut om hemlig dataavläsning ska vara tydliga och förutsebara

Förslag: Uppgiftstyperna i punkt 6 och 7 ska tas bort. I stället ska det införas en ny punkt 6 som avser hemlig dataavläsning av uppgifter som är åtkomliga i ett avläsningsbart informationssystem, men som inte avses i 2 § första stycket 1–5 lagen om hemlig dataavläsning.

Ett tillstånd till hemlig dataavläsning ska omfatta uppgiftstyperna i den nu föreslagna bestämmelsen 2 § första stycket 1–3 och 6 lagen om hemlig dataavläsning, om inget annat särskilt beslutas eller framgår av andra bestämmelser.

Skälen för våra förslag

De olika uppgiftstyperna och gränsdragningsfrågor

Den obligatoriska domstolsprövningen i kombination med kravet på offentligt ombud utgör en av de starkaste rättssäkerhetsgarantierna vid hemlig dataavläsning. En omsorgsfull och rättssäker domstolsprövning förutsätter i sin tur en tydlig och förutsebar lagstiftning. Tillstånd till hemlig dataavläsning är, precis som andra tillstånd till hemliga tvångsmedel, belagda med sekretess. Det uppstår därför inte

någon gemensam praxis på samma sätt som i andra rättsområden som handläggs vid domstolarna. Mot denna bakgrund framstår det som särskilt angeläget att regleringen om hemlig dataavläsning är förutsebar, tydlig och precis. Detta är också en förutsättning för att lagstiftningen ska uppfylla de krav som både regeringsformen och Europakonventionen ställer. Vi återkommer i kapitel 8 närmare till de olika rättssäkerhetsgarantier som omgärdar regelverket.

Ett tillstånd till hemlig dataavläsning innebär inte per automatik rätt att ta del av alla de uppgiftstyper som räknas upp i lagens 2 §. Lagstiftaren har i stället valt en lösning där bedömningen av vilka uppgiftstyper som får hämtas in alltid ska göras i det enskilda fallet. Det innebär med andra ord ett krav på att de olika uppgiftstyperna ska differentieras redan vid tillståndsgivningen. Vid införandet av den nya lagen bedömdes differentieringskravet, tillsammans med de höga kvalifikationskraven för användandet av hemlig dataavläsning, utgöra en ur integritetssynpunkt viktig skyddsåtgärd (se prop. 2019/20:64 s. 92 och 107). En grundläggande förutsättning för hemlig dataavläsning är att syftet uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktas mot eller för något annat motstående intresse. Differentieringskravet hindrar därför inte att ett tillstånd innefattar flera eller alla sju uppgiftstyper, så länge det kan anses proportionerligt i det enskilda fallet.

Den hittillsvarande tillämpningen visar också att tillstånd till hemlig dataavläsning regelmässigt har omfattat flera uppgiftstyper. De flesta tillstånd har omfattat uppgiftstyperna i punkt 1–3 samt 6 och 7. Företrädare för de brottsbekämpande myndigheterna har också framhållit att det i brottsbekämpningen typiskt sett finns ett påtagligt behov av sådan information som är att hänföra till dessa uppgiftstyper. Motsvarande information inhämtas regelmässigt med stöd av både öppna och hemliga tvångsmedel, i syfte att bekämpa allvarlig brottslighet. Tillstånd till hemlig dataavläsning avseende uppgiftstyperna i punkt 4 och 5 har varit mer sällsynta. Också denna tillämpning får anses som en både väntad och ändamålsenlig användning av lagstiftningen, eftersom även de bakomliggande tvångsmedlen hemlig kameraövervakning och hemlig rumsavlyssning används relativt sällan. Inte heller i övrigt har det framkommit något i den hittillsvarande tillämpningen som tyder på en ändamålsglidning (se kapitel 6). I avsnitt 6.2.5 har vi mer ingående redogjort för varför ett ändamålsenligt tillstånd till hemlig dataavläsning ofta behöver avse inhämtning av

större mängder information på ett visst informationssystem. I avsnittet framgår att samma typ av information, både genom teknisk slump och beroende på hur den enskilda användaren aktivt hanterar uppgiften i informationssystemet, kan komma att sortera under olika uppgiftstyper. Det går därför sällan att före verkställighet av hemlig dataavläsning avgöra hur lagstiftningens kategorisering av olika uppgiftstyper ska appliceras på den information som kan komma att påträffas.

I förarbetena förutsågs att det skulle kunna uppstå gränsdragningsfrågor. Man ansåg dock att risken för överlappning mellan uppgiftstyperna och svåra gränsdragningar inte skulle överdrivas, eftersom det är möjligt att meddela tillstånd till hemlig dataavläsning avseende fler än en av punkterna samtidigt (jfr SOU 2017:89 s. 503). Gränsdragningsproblematiken mellan punkt 6 och 7 uppmärksammades inte särskilt. Eftersom det kan vara svårt att förutse huruvida uppgifter som visar hur ett avläsningsbart informationssystem används lagras eller inte kan uppgiftstyperna i punkt 6 och 7 sällan särskiljas i praktiken. Det är av samma skäl svårt att ge konkreta exempel på uppgifter som med säkerhet sorterar under punkt 7. Praktiska exempel på gränsdragningsfall mellan punkt 6 och 7 är applikationer som körs. Tangenttryckningar som kan registreras med en s.k. keylogger eller inloggning på en router i realtid är exempel på uppgifter som bör sortera under punkten 7. En lagstiftning som inte gör skillnad på uppgiftstyperna i punkt 6 och 7 skulle dock framstå som tydligare och mer förutsebar.

Gränsdragningssvårigheter mellan vissa uppgiftstyper och den praktiska tillämpningen av hemlig dataavläsning väcker frågan om det är ändamålsenligt och förenligt med kraven på tydlighet och förutsebarhet att dela in information i flera olika uppgiftstyper. Nuvarande lagstiftning ger intryck av att det är enkelt att dela upp information på detta sätt, trots att det i praktiken är förenat med stora svårigheter. Information som är att hänföra till uppgiftstyperna i punkt 1–3 samt 6 och 7 utgör dessutom typiskt sett information som myndigheterna, i utredningar där hemlig dataavläsning är aktuell, har ett påtagligt behov av för en effektiv brottsbekämpning. En lagstiftning där det uttryckligen framgår att de brottsbekämpande myndigheterna regelmässigt har behov av dessa uppgiftstyper skulle därför framstå som tydligare och mer förutsebar. Samtidigt förekommer enskilda ärenden där det endast finns behov av eller skäl att meddela

tillstånd avseende en eller några av de sju uppgiftstyperna. Det finns flera exempel på när en sådan begränsning framgår redan av lagtext. I lagen om hemlig dataavläsning regleras t.ex. tre olika situationer där hemlig dataavläsning i dag endast får användas avseende uppgiftstyperna i punkt 1, 2 eller 3:

- tillstånd till hemlig dataavläsning av ett informationssystem som tillhör någon annan än den berörde, se 4 a § andra stycket, 8 § andra stycket och 9 § andra stycket lagen om hemlig dataavläsning,
- tillstånd till hemlig dataavläsning för att utreda vem som skäligen kan misstänkas för ett brott, se 4 b och 5 §§ lagen om hemlig dataavläsning och
- tillstånd till hemlig dataavläsning i inhämtningslagsfallen, se 10 § lagen om hemlig dataavläsning.

Hemlig dataavläsning ska fortsatt differentieras i varje enskilt fall

I ett tillstånd till hemlig dataavläsning ska alltid anges vilken uppgiftstyp som får hämtas in. Vi delar tidigare bedömningar om att differentieringskravet vid tillståndsgivningen utgör en viktig skyddsåtgärd för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan. Det framstår därför som fortsatt ändamålsenligt att i varje enskilt fall avgöra vilken eller vilka uppgiftstyper som får hämtas in med stöd av hemlig dataavläsning. Rent faktiskt går det också att särskilja uppgifter som faller under var och en av punkt 1–5 samt i vart fall uppgifter som faller under punkt 6 eller 7 redan vid tillståndsgivningen. Lagstiftningen bedöms därför också vara tillräckligt tydlig och förutsebar. I de fall där det kan uppstå gränsdragnings- eller överlappningsfrågor mellan uppgiftstyperna får dessa accepteras. Som framhållits i förarbetena är det möjligt att ansöka om tillstånd till hemlig dataavläsning avseende fler än en av punkterna samtidigt. I många ärenden är det svårt att på förhand förutse var i informationssystemet som den eftersökta informationen kommer att anträffas. De flesta tillstånd till hemlig dataavläsning omfattar också flera uppgiftstyper. Detta förhållande utgör dock inte skäl att frångå differentieringskravet. I enskilda fall kommer det även fortsättningsvis att finnas behov av eller skäl att meddela tillstånd avseende endast en eller några av uppgiftstyperna. En fortsatt åtskillnad mellan var och en av

uppgiftstyperna i punkt 1–5 samt uppgifter som faller under punkt 6 eller 7 framstår sammantaget som både ändamålsenlig och förenlig med kraven på tydlighet och förutsebarhet. När det gäller den inbördes uppdelningen mellan de sekundära uppgiftstyperna i punkt 6 och 7 gör vi dock motsatt bedömning, se vidare nedan.

Ett tydligare fokus på villkor

Uppdelningen av uppgifter i uppgiftstyperna 1–5 bygger på hur de andra hemliga tvångsmedlen är uppbyggda. Utöver den skyddsåtgärd som differentieringskravet innebär bidrar uppdelningen till att säkerställa en välfungerande systematik i regelverket för hemliga tvångsmedel. Vi kan emellertid konstatera att uppdelningen medför vissa praktiska utmaningar och att uppgiftstyperna i 6 och 7 saknar motsvarighet i de andra hemliga tvångsmedlen. Om det inte är möjligt eller ändamålsenligt att redan vid tillståndsprövningen begränsa inhämtningen till vissa *uppgiftstyper* enligt 2 § kan tillståndet emellertid förenas med villkor enligt 18 § första stycket 4 som anger *vilka uppgifter* som får *inhämtas eller granskas* och som därigenom begränsar åtgärden. Villkor enligt 18 § första stycket 4 kan ta sikte på i stort sett vilka omständigheter som helst. Vid prövningen av vilka villkor som ett eventuellt tillstånd bör förenas med är rätten således inte låst till lagstiftningens kategorisering av uppgiftstyper. Ibland kan det till exempel vara mer effektivt att göra skillnad på lagrade uppgifter respektive realtidsuppgifter än på de olika uppgiftstyper som anges i lagstiftningen.

Exempel på lagrade uppgifter som kan hämtas in genom hemlig dataavläsning är uppgifter om innehållet i krypterade meddelanden som har skickats (punkt 1), vem som har skickat dessa meddelanden (punkt 2), var en viss teknisk utrustning tidigare har funnits (punkt 3), och innehåll som finns lagrat på en viss teknisk utrustning men som inte har kommunicerats, däribland kamerabilder, dokument, utkast till meddelanden och kontaktlistor (punkt 6). Exempel på realtidsuppgifter som kan hämtas in genom hemlig dataavläsning är innehållet i pågående krypterade telefonsamtal (punkt 1), var viss teknisk utrustning befinner sig genom t.ex. användning av utrustningens positioneringsfunktion (punkt 3), identifiering genom aktivering av den tekniska utrustningens kamerafunktion (punkt 4), innehållet i

pågående samtal genom aktivering av den tekniska utrustningens mikrofon (punkt 5), samt lösenord genom användande av en s.k. keylogger som registrerar tangenttryckningar (punkt 7).

Om syftet med den hemliga dataavläsningen endast är att ta del av viss kommunikation som de brottsbekämpande myndigheterna misstänker komma äga rum under ett visst tidsintervall kan ett villkor ange att inhämtning endast får avse realtidsuppgifter eller uppgifter som tillkommer eller ändras under verkställighetstiden. Ett villkor kan också avse granskningsfasen, t.ex. att endast filer som är skapade eller ändrade under ett visst tidsintervall får granskas. I avsnitt 8.4.5 återkommer vi till våra förslag på ändringar i den nuvarande villkorsbestämmelsen, i syfte att ge villkoren en mer framträdande roll vid tillståndsgivningen. Våra förslag om ett tydligare fokus på villkor har bäring på våra förslag i det följande.

Uppgiftstyperna i punkt 6 och 7 ska läggas samman i en ny punkt

Vårt förslag

Vi föreslår att uppgiftstyperna i 2 § första stycket 6 och 7 lagen om hemlig dataavläsning ska tas bort. I stället ska det införas en ny punkt 6 som ska avse inhämtning av uppgifter som är åtkomliga i ett avläsningsbart informationssystem, men som inte avses i 2 § första stycket 1–5 lagen om hemlig dataavläsning.

Behov, nytta och effektivitet

Som vi ovan har redogjort för kan uppgifter som hämtas in med stöd av 2 § första stycket 6 och 7 sällan särskiljas före inhämtningen. Företrädare för de brottsbekämpande myndigheterna har uppgett att behovet av de båda uppgiftstyperna är lika stort, vilket bekräftas av den hittillsvarande tillämpningen. Som vi också har framhållit är det angeläget att fokus vid domstolsprövningen ligger på den rättsliga prövningen och inte på hur de olika uppgifterna tekniskt sett ska kategoriseras. Det framstår därför som mer motiverat med en bestämmelse som inte skiljer på om de sekundära uppgifterna är lagrade eller om de utgör realtidsuppgifter. En sådan ordning är också mer teknikneutral eftersom det i dagsläget kan förefalla slumpmässigt

huruvida viss information lagras eller inte. En bestämmelse vars tillämpning är beroende av en viss utrustnings tekniska utformning är typiskt sett mindre lämplig.

Förslaget innebär alltså en mer teknikneutral lagstiftning som undanröjer otydligheter, både för enskilda och för rättstillämparen. Lagstiftningen kommer på detta sätt också bättre att uppfylla kravet på förutsebarhet. Eftersom en sammanslagning av punkterna 6 och 7 på detta sätt kan bidra till en mer ändamålsenlig lagstiftning kan förslaget också förväntas vara effektivt och medföra nytta för brottsbekämpningen.

Förslaget innebär en viss ökad risk för den personliga integriteten

Frågan är då vilka risker som vårt förslag innebär för den personliga integriteten. Redan i dag meddelas tillstånd till hemlig dataavläsning avseende punkt 6 och 7 regelmässigt samtidigt. Vårt förslag syftar inte till att en större mängd uppgifter ska hämtas in, utan till att förenkla ansöknings- och beslutsprocessen samt undanröja den osäkerhet som i dag kan finnas angående ett tillstånds omfattning. En kombination av olika mindre risker kan dock ge anledning att värdera den samlade risken högre. Vi har ovan konstaterat att det endast är en begränsad mängd uppgifter som i dag faller under uppgiftstypen i punkt 7. Det finns samtidigt ingenting som tyder på att den tekniska utvecklingen kommer att avstanna. Den snabba tekniska utvecklingen kan innebära att uppgiftstypen i punkt 7 i framtiden kommer att omfatta en större mängd uppgifter än i dag. Detta skulle kunna innebära en viss ökad risk för den personliga integriteten. De positiva effekterna av vårt förslag är att användningen av hemlig dataavläsning blir både tydligare och mer förutsebar. Det är vår samlade bedömning att förslaget, särskilt i kombination med en tydlig villkorsreglering (se avsnitt 8.4.5), inte medför några beaktansvärt ökade risker för den personliga integriteten jämfört med den nuvarande lagstiftningen. Förslaget bedöms således som försvarligt ur integritetssynpunkt.

En förtydligande huvudregel

Vårt förslag

Vi föreslår att ett tillstånd till hemlig dataavläsning ska omfatta uppgiftstyperna i nu föreslagna 2 § första stycket 1–3 och 6 (dvs. nuvarande 2 § första stycket 1–3 samt 6 och 7) lagen om hemlig dataavläsning, om inget annat särskilt beslutas eller framgår av andra bestämmelser.

Behov, nytta och effektivitet

Den kategorisering av uppgiftstyper som i dag ska ske redan vid tillståndsgivningen är, som konstaterats, i de flesta fall mycket svår eller omöjlig att göra. Det ska i sammanhanget åter framhållas att det ur rättssäkerhetssynpunkt är angeläget att fokus vid tillståndsprövningen ligger på den rättsliga prövningen och inte på hur behovet av information tekniskt sett är att kategorisera.

Gränsdragningsproblematik förekommer även beträffande de permanenta hemliga tvångsmedlen. Exempelvis är ett tillstånd till hemlig avlyssning av elektronisk kommunikation (HAK) i princip omöjligt att verkställa utan att också få in s.k. HÖK-uppgifter. I lagstiftningen har man löst detta genom att låta ett tillstånd till hemlig avlyssning av elektronisk kommunikation även ge rätt att vidta sådana åtgärder som kan omfattas av ett tillstånd till hemlig övervakning av elektronisk kommunikation, se 27 kap. 18 § andra stycket rättegångsbalken. Vi bedömer att starka skäl talar för att även lagstiftningen om hemlig dataavläsning bör vara transparent med den gränsdragningsproblematik som kan uppstå mellan uppgiftstyper. Vid hemlig dataavläsning behöver inhämtningen omfatta alla uppgiftstyper i punkt 1–3 för att inhämtningen ska fånga in motsvarande information som en s.k. HAK kan ge. Beroende på hur uppgifterna är att kategorisera finns i princip alltid ett samtidigt behov av att hämta in punkt 6- och 7-uppgifter. Dessa uppgifter motsvarar också huvudsakligen uppgifter som regelmässigt hämtas in med öppna tvångsmedel. Det sagda illustrerar vad vi tidigare framhållit om att de brottsbekämpande myndigheterna i de flesta fall har behov av uppgifter som är att sortera under de nuvarande punkterna 1–3 respektive 6 och 7.

I ljuset av den hittillsvarande tillämpningen och de brottsbekämpande myndigheternas behov av information framstår det därför som tydligare och mer ändamålsenligt med en bestämmelse som klargör att ett tillstånd till hemlig dataavläsning som huvudregel innebär att alla uppgiftstyper, med undantag för kameraövervaknings- och rumsavlyssningsuppgifter, som är åtkomliga i ett visst informationssystem får hämtas in. Det ska framhållas att ett tillstånd enligt huvudregeln inte nödvändigtvis innebär att all åtkomlig information får hämtas in, eftersom tillståndets omfattning även styrs av villkoren för detsamma.

Vårt förslag innebär en lagstiftning som speglar verkligheten bättre och som undanröjer otydligheter, både för enskilda och för rättstillämparen. Lagstiftningen kommer på detta sätt också bättre att uppfylla kravet på rättssäkerhet och förutsebarhet.

Vårt förslag innebär också att hemlig dataavläsning kommer att harmoniera bättre med det nya tvångsmedlet genomsökning på distans. Som vi har redogjort för i avsnitt 4.3.4 är reglerna om hemlig dataavläsning respektive genomsökning på distans till viss del överlappande. Det innebär att det kan uppstå situationer där åklagare kan välja att fatta ett beslut om genomsökning på distans eller ansöka om ett tillstånd till hemlig dataavläsning. Starka skäl talar därför för att regelverken så långt det är möjligt bör harmoniera. Genomsökning på distans innebär att söka efter *handlingar* som finns lagrade i ett avläsningsbart informationssystem utanför den elektroniska utrustningen. Vid genomsökning på distans sker det alltså inte någon differentiering mellan olika typer av handlingar. I förarbetena till bestämmelsen framhålls att uppgifter i en elektronisk kommunikationsutrustning kan vara svåra att överblicka jämfört med uppgifter i fysiska dokument. En mobiltelefon, dator eller en surfplatta kan innehålla mycket information av vitt skilda slag, lagrad i komplexa mappstrukturer och olika applikationer eller samlade på annat sätt. Vissa uppgifter blir synliga först när användaren har öppnat en fil eller applikation. Detta innebär att det inte på förhand, innan utrustningen har genomsökts, går att överblicka vilken slags information som kan finnas där (se *Modernare regler för användningen av tvångsmedel*, prop. 2021/22:119 s. 68). Som vi ovan har redogjort för uppstår samma svårigheter vid hemlig dataavläsning. Vi bedömer sammantaget att det finns ett påtagligt behov av en förtydligande huvudregel. Eftersom hemlig dataavläsning på detta sätt kan användas mer ändamålsenligt kan vårt förslag

också förväntas vara effektivt och medföra avsevärd nytta för brottsbekämpningen.

Förslaget innebär en viss ökad risk för den personliga integriteten

En förutsättning för vårt förslag om en huvudregel är att det är det kan anses försvarligt ur integritetssynpunkt. Vi har både i kapitel 6 och ovan avseende var och en av de olika uppgiftstyperna redogjort för våra integritetsriskbedömningar. Vi har inte funnit att det skulle vara förenat med några avsevärt större risker för den personliga integriteten att hämta in information genom hemlig dataavläsning än att hämta in motsvarande information på annat sätt. Vi har också kommit till slutsatsen att det även fortsättningsvis i varje enskilt fall ska avgöras vilken typ eller vilka typer av uppgifter som får hämtas in med stöd av hemlig dataavläsning. Införandet av en förtydligande huvudregel innebär alltså inte att lagens krav på differentiering av de olika uppgiftstyperna slopas. Det föreslås inte heller någon förändring av lagens strukturella uppbyggnad, där de olika kvalifikationskraven för hemlig dataavläsning är knutna till de olika uppgiftstyperna. Huvudregeln utesluter således inte att det i det enskilda fallet kan finnas behov av eller skäl att meddela tillstånd avseende en eller några av uppgiftstyperna. Som framhållits ovan framgår sådana begränsningar i vissa fall redan av lagtext, se t.ex. 4 a–5 och 8–10 §§ lagen om hemlig dataavläsning. Det är självklart alltid som utgångspunkt legalitetsprincipen samt behovs-, ändamåls- och proportionalitetsprinciperna som styr om ett tillstånd till hemlig dataavläsning ska beviljas och hur det i så fall ska avgränsas.

Förslaget innebär att de flesta tillstånd till hemlig dataavläsning även fortsättningsvis kommer att omfatta uppgiftstyperna i nuvarande 2 § första stycket 1–3 samt 6 och 7 lagen om hemlig dataavläsning. För att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan bör det, i de fall där en begränsning till olika uppgiftstyper inte lämpligen kan ske redan vid tillståndsgivningen, i stället anges tydliga villkor för tillståndet enligt 18 § första stycket 4 lagen om hemlig dataavläsning. Ett tillstånd till hemlig dataavläsning enligt huvudregeln kan som ovan beskrivits begränsas genom villkor om att t.ex. endast en viss typ av filer skapade eller ändrade under ett visst tidsintervall får granskas. Ett sådant villkor innebär förenklat att diffe-

rentieringen till viss del förskjuts från inhämtningsfasen till granskningsfasen. Det ska framhållas att redan själva inhämtningen av uppgifter, såväl historiskt som i realtid, anses utgöra ett ingrepp i den personliga integriteten. Detta gäller även om de brottsbekämpande myndigheterna aldrig tar del av de uppgifterna och oavsett om uppgifterna kommer till användning (jfr bl.a. 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 m.fl. punkterna 115 och 116 och där hänvisade rättsfall). Det intrånget är dock sekundärt i förhållande till om och när materialet gås igenom i en granskningsfas. Vi återkommer i avsnitt 8.4.5 till våra överväganden om villkorskravet och till olika exempel på hur villkor skulle kunna se ut i enskilda fall. I avsnitt 8.5.6 behandlar vi frågan om hur information som har hämtats in i enlighet med ett tillstånd, men som inte får granskas enligt villkoren, ska hanteras.

Vårt förslag syftar inte till att en större mängd uppgifter ska hämtas in, utan till att förenkla ansöknings- och beslutsprocessen samt undanröja den osäkerhet som i dag kan finnas angående ett tillstånds omfattning. En kombination av olika mindre risker kan dock ge anledning att värdera den samlade risken högre. En konstruktion med en huvudregel innefattar dessutom i sig en risk för att förslaget leder till att tillstånd enligt huvudregeln beviljas även i de fall där det egentligen endast finns skäl att bevilja tillstånd till en eller några av punkterna. Detta får anses innebära en viss ökad risk för den personliga integriteten. De positiva effekterna av vårt förslag är att användningen av hemlig dataavläsning blir både tydligare och mer förutsebar. Förslaget harmonierar också bättre med det nya tvångsmedlet genomsökning på distans. Vidare bör förslaget medföra en ökad användning av tydliga villkor enligt 18 § första stycket 4 lagen om hemlig dataavläsning. Som kommer att framgå i det följande har villkorskravet inte alltid efterlevts i praktiken. Det är vår samlade bedömning att förslaget, i kombination med en tydlig villkorsreglering, inte medför några beaktansvärt ökade risker för den personliga integriteten jämfört med den nuvarande lagstiftningen. Förslaget bedöms således som försvarligt ur integritetssynpunkt.

Proportionalitet

En förutsättning för att våra förslag ska kunna anses proportionerliga är att regelverket för hemlig dataavläsning även fortsättningsvis omgärdas av starka rättssäkerhetsgarantier som t.ex. en obligatorisk domstolsprövning och en tydlig villkorsreglering. Vi återkommer i kapitel 8 till de rättssäkerhetsgarantier och kontrollmekanismer som gäller för hemlig dataavläsning. En annan förutsättning är att höga krav även fortsättningsvis ska ställas för att hemlig dataavläsning ska få användas. Med detta i beaktande övergår vi i följande avsnitt till olika frågor om ett utökat tillämpningsområde för hemlig dataavläsning.

7.4 Utökade möjligheter att använda hemlig dataavläsning under en förundersökning

7.4.1 Kvalifikationskraven för de permanenta hemliga tvångsmedlen utgör naturliga utgångspunkter

Bedömning: Vid hemlig dataavläsning under en förundersökning i syfte att hämta in uppgifter enligt 2 § första stycket 1–5 lagen om hemlig dataavläsning bör kvalifikationskraven som utgångspunkt även fortsättningsvis huvudsakligen motsvara vad som gäller för de bakomliggande tvångsmedlen. Vid hemlig dataavläsning under en förundersökning för att hämta in uppgifter enligt nu föreslagna 2 § första stycket 6 lagen om hemlig dataavläsning bör kvalifikationskraven som utgångspunkt även fortsättningsvis motsvara vad som gäller för hemlig avlyssning av elektronisk kommunikation.

Skälen för vår bedömning

Den grundläggande systematiken

Bestämmelserna om hemlig dataavläsning under förundersökning är utformade med de permanenta hemliga tvångsmedlen i rättegångsbalken som förebilder. Kvalifikationskraven som avgränsar användningsområdet varierar beroende på vilken uppgiftstyp som avses. Syftet med de olika kraven är att balansera de olika risker för den personliga

integriteten som användningen av de olika uppgiftstyperna kan innebära. Vid hemlig dataavläsning i syfte att hämta in uppgifter enligt 2 § första stycket 1–5 lagen om hemlig dataavläsning gäller huvudsakligen motsvarande krav som gäller för de bakomliggande tvångsmedlen. Vid hemlig dataavläsning för att hämta in uppgifter enligt nu föreslagna 2 § första stycket 6 (nuvarande punkt 6 och 7) gäller motsvarande krav som gäller för hemlig avlyssning av elektronisk kommunikation. Systematiken i bestämmelserna om de permanenta hemliga tvångsmedlen enligt rättegångsbalken är sådan att samma förutsättningar gäller för tillstånd till hemlig kameraövervakning som för hemlig avlyssning av elektronisk kommunikation. Vidare ger ett tillstånd till hemlig avlyssning av elektronisk kommunikation rätt att vidta de åtgärder som kan omfattas av ett tillstånd till hemlig övervakning av elektronisk kommunikation. Detta innebär i praktiken att ett tillstånd till hemlig dataavläsning avseende uppgiftstyperna i nu föreslagna 2 § första stycket 1–4 och 6 som utgångspunkt får beviljas vid förundersökning om brott som kan föranleda hemlig avlyssning av elektronisk kommunikation. Det innebär vidare att ett tillstånd till hemlig dataavläsning enligt 2 § första stycket 5 som utgångspunkt får beviljas vid förundersökning om brott som kan föranleda hemlig rumsavlyssning. Utformningen av de olika kvalifikationskraven har i förarbetena motiveras genom utförliga analyser (jfr prop. 2019/20:64 s. 112 ff.).

Våra utgångspunkter och hur vi förhåller oss till aktuella lagändringar

Vi delar tidigare bedömningar om att utformningarna av kvalifikationskraven för de olika uppgiftstyperna är ändamålsenligt och proportionerligt avgränsade. Någon ändring beträffande kvalifikationskraven föreslås alltså inte. Det är således även vår uppfattning att kvalifikationskraven för hemlig dataavläsning under förundersökning som utgångspunkt bör korrespondera med de bakomliggande tvångsmedlen hemlig avlyssning av elektronisk kommunikation och hemlig rumsavlyssning. Detta är vår utgångspunkt även med beaktande av att tillämpningsområdena för dessa hemliga tvångsmedel nyligen har utökats.

Utredningen om utökade möjligheter att använda hemliga tvångsmedel hade i uppdrag att se över delar av regleringen om hemliga

tvångsmedel enligt rättegångsbalken. I delbetänkandet *Utökade möjligheter att använda hemliga tvångsmedel* (SOU 2022:19) föreslog utredningen också flera författningsändringar om utökade möjligheter att använda hemliga tvångsmedel enligt rättegångsbalken. Eftersom det finns ett starkt sakligt och systematiskt samband mellan de permanenta hemliga tvångsmedlen och hemlig dataavläsning omfattade flera av utredningens överväganden även hemlig dataavläsning. I syfte att upprätthålla en välfungerande systematik i regelverket om hemliga tvångsmedel föreslogs att tillämpningsområdet för hemlig dataavläsning skulle utökas i motsvarande mån som tillämpningsområdet för de bakomliggande tvångsmedlen. Utredningen framhöll även regeringens uttalande om att det är av väsentlig betydelse att hemlig dataavläsning kan användas i motsvarande fall som de befintliga hemliga tvångsmedlen (se a. SOU s. 18, 106 f., 172 och 257 f. med där gjorda hänvisningar). Utredningens analyser och förslag godtogs med vissa lagtekniska justeringar i det fortsatta lagstiftningsarbetet. Lagändringar i dessa avseenden trädde i kraft den 1 oktober 2023, se *Hemliga tvångsmedel – effektiva verktyg för att förhindra och utreda allvarliga brott*, prop. 2022/23:126.

Vidare lämnade samma utredning i sitt slutbetänkande, *Bättre möjligheter att verkställa frihetsberövanden* (SOU 2022:50), förslag om att hemlig övervakning av elektronisk kommunikation ska kunna användas i syfte att lokalisera olika kategorier av eftersökta personer. I konsekvens härmed föreslog utredningen att det skulle införas en möjlighet att använda hemlig dataavläsning avseende plats- och kommunikationsövervakningsuppgifter i motsvarande syfte. Dessa lagförslag är för närvarande under beredning.

Redan de systematiska skäl som framhålls i förarbetena talar starkt för att det är ändamålsenligt att tillämpningsområdet för hemlig dataavläsning utökas i motsvarande mån som tillämpningsområdet för de bakomliggande tvångsmedlen. I betänkandena som ligger till grund för lagförslagen presenteras ingående analyser av behov, förväntad effektivitet och nytta samt noggranna intresseavvägningar. Dessa har i sin tur godtagits i det fortsatta lagstiftningsarbetet. Inom ramen för vårt uppdrag har vi inte funnit anledning att ifrågasätta eller vidareutveckla dessa tidigare analyser och intresseavvägningar. Med dessa utgångspunkter bedömer vi de aktuella lagändringarna och lagförslagen om ett utökat tillämpningsområde för hemlig dataavläsning som både ändamålsenliga och proportionerliga. I de följande avsnitten

redogör vi därför endast helt kort för aktuella lagändringar och lagförslag och stannar i huvudsak vid att hänvisa till dessa. Endast i frågan om utökade möjligheter att utreda vem som skäligen kan misstänkas gör vi en något annan bedömning. Detta framgår av våra överväganden i avsnitt 7.4.4 nedan.

7.4.2 En utvidgad brottskatalog

De ursprungliga brottskatalogerna

En av förutsättningarna för att få använda hemlig dataavläsning är att det är fråga om viss allvarlig brottslighet. Brottskatalogen för hemlig dataavläsning, med undantag för hemlig dataavläsning avseende rumsavlyssningsuppgifter, framgick ursprungligen av 4 § första stycket 1–3 lagen om hemlig dataavläsning. Bestämmelsen var utformad med den dåvarande brottskatalogen för hemlig avlyssning av elektronisk kommunikation i 27 kap. 18 § andra stycket rättegångsbalken (i dess lydelse före den 1 oktober 2023) som förebild. Brottskatalogen för hemlig dataavläsning avseende rumsavlyssningsuppgifter motsvarade den som gällde för hemlig rumsavlyssning. Detta framgick av dåvarande 6 § första stycket lagen om hemlig dataavläsning.

Lagändringar om utvidgade brottskataloger

Den 1 oktober 2023 utvidgades möjligheterna att använda hemlig avlyssning och hemlig övervakning av elektronisk kommunikation samt hemlig kameraövervakning till att omfatta förundersökningar om:

- grovt dataintrång,
- grovt sexuellt övergrepp, sexuellt utnyttjande av barn, sexuellt övergrepp mot barn, grovt sexuellt övergrepp mot barn, utnyttjande av barn för sexuell posering, grovt utnyttjande av barn för sexuell posering, utnyttjande av barn genom köp av sexuell handling, sexuellt ofredande mot barn eller grovt sexuellt ofredande mot barn,
- kontakt för att träffa ett barn i sexuellt syfte, om det kan antas att brottet inte endast leder till böter,

- grovt bedrägeri, om gärningen har begåtts med hjälp av elektronisk kommunikation,
- grovt barnpornografibrott och barnpornografibrott som inte är ringa,
- grovt skyddande av brottsling,
- grovt penningtvättsbrott eller näringspenningtvätt, grovt brott,
- grovt insiderbrott, samt
- utpressning, mened, övergrepp i rättssak eller skyddande av brottsling om det kan antas att brottets straffvärde överstiger fängelse i tre månader.

I konsekvens härmed utvidgades även brottskatalogen för hemlig dataavläsning, med undantag för hemlig dataavläsning avseende rumsavlyssningsuppgifter, på motsvarande sätt. Den utvidgade brottskatalogen framgår av 4 § lagen om hemlig dataavläsning som hänvisar till 27 kap. 18 a § andra stycket rättegångsbalken.

I motiven bakom förslagen framhålls att de uppräknade brottstyperna anses särskilt svårutredda, på grund av att de typiskt sett begås i en miljö där det råder tystnadskultur eller att användning av modern teknik gör det svårt att identifiera en skäligen misstänkt för brott som kan vara systemhotande eller i övrigt är särskilt angelägna att bekämpa. Utredningens analyser och intresseavvägningar godtogs i huvudsak i det fortsatta lagstiftningsarbetet. Den s.k. golvregeln, som innebär att det beträffande utpressning, mened, övergrepp i rättssak och skyddande av brottsling krävs att det kan antas att brottets straffvärde överstiger fängelse i tre månader, tillkom dock på inrådan av Lagrådet. Vi gör ingen annan bedömning utan hänvisar till dessa ställningstaganden, se prop. 2022/23:126 s. 104 ff. och 239.

7.4.3 Nya straffvärdeventiler för viss flerfaldig brottslighet

De ursprungliga straffvärdeventilerna

I 4 § första stycket 4 lagen om hemlig dataavläsning fanns ursprungligen en s.k. straffvärdeventil som angav att tillstånd till åtgärden får ges om det med hänsyn till omständigheterna kan antas att brottets

straffvärde överstiger fängelse i två år. Bestämmelsen gällde vid tillstånd till hemlig dataavläsning, med undantag för hemlig dataavläsning avseende rumsavlyssningsuppgifter. Bestämmelsen var utformad med den dåvarande straffvärdeventilen för hemlig avlyssning av elektronisk kommunikation i 27 kap. 18 § andra stycket rättegångsbalken (i dess lydelse före den 1 oktober 2023) som förebild. Hemlig dataavläsning avseende rumsavlyssningsuppgifter får endast användas vid förundersökning om sådana brott som kan föranleda hemlig rumsavlyssning. Detta framgår av 6 § första stycket lagen om hemlig dataavläsning som hänvisar vidare till den straffvärdeventil i 27 kap. 20 d § andra stycket rättegångsbalken som gäller för hemlig rumsavlyssning.

Lagändringar om nya straffvärdeventiler

Den 1 oktober 2023 infördes nya straffvärdeventiler som gör det möjligt att i vissa situationer beakta en flerfaldig brottslighets samlade straffvärde vid bedömningen av om hemliga tvångsmedel ska få användas. Beträffande hemlig avlyssning och hemlig övervakning av elektronisk kommunikation samt hemlig kameraövervakning infördes en ny straffvärdeventil i förundersökningar om flerfaldig brottslighet som kan antas ha utövats i organiserad form eller systematiskt. Förutsättningarna för tillämpning av den nya straffvärdeventilen är att:

- en och samma person är skäligen misstänkt för samtliga brott,
- det kan antas att den samlade brottslighetens straffvärde överstiger fängelse i två år,
- det kan antas att vart och ett av brotten har utgjort ett led i en brottslighet som har utövats i organiserad form eller systematiskt, och
- det för vart och ett av brotten är föreskrivet fängelse i ett år eller mer.

Denna nya straffvärdeventil framgår bl.a. av 27 kap. 18 a § andra stycket 22 a–d rättegångsbalken. I konsekvens härmed infördes även en motsvarande straffvärdeventil för hemlig dataavläsning, med undantag för hemlig dataavläsning avseende rumsavlyssningsuppgifter. Detta framgår av 4 § lagen om hemlig dataavläsning som hänvisar till 27 kap. 18 a § andra stycket rättegångsbalken.

För hemlig rumsavlyssning infördes samtidigt en ny straffvärdeventil i 27 kap. 20 d § andra stycket 6 a–d rättegångsbalken. Enligt den tidigare straffvärdeventilen fick tillstånd åtgärden ges om det med hänsyn till omständigheterna kunde antas att brottets straffvärde översteg fängelse i fyra år och det var fråga om viss, i bestämmelsen uppräknad, brottslighet. Förutsättningarna för tillämpning av den nya straffvärdeventilen är att:

- en och samma person är skäligen misstänkt för samtliga brott,
- det kan antas att den samlade brottslighetens straffvärde överstiger fängelse i fyra år,
- det kan antas att vart och ett av brotten har utgjort ett led i en brottslighet som har utövats i organiserad form eller systematiskt, och
- det för vart och ett av brotten inte är föreskrivet lindrigare straff än fängelse i sex månader eller det är fråga om försök, förberedelse eller stämpling till ett sådant brott.

I konsekvens härmed utökades möjligheten att använda hemlig dataavläsning avseende rumsavlyssningsuppgifter på motsvarande sätt. Den nya straffvärdeventilen för hemlig dataavläsning avseende rumsavlyssningsuppgifter framgår fortsatt av 6 § första stycket lagen om hemlig dataavläsning som i sin tur hänvisar till den nya bestämmelsen i 27 kap. 20 d § andra stycket rättegångsbalken.

I motiven bakom förslagen framhålls bl.a. följande. Som en konsekvens av hur dagens regler är utformade kan i normalfallet misstankar om systematisk brottslighet bestående av t.ex. flera skattebrott, stölder eller bedrägerier falla utanför tillämpningsområdet för hemliga tvångsmedel. Dessa typer av brott, som sedda för sig inte alltid är särskilt allvarliga, utgör exempel på vad som kan vara viktiga inkomstkällor för kriminella nätverk som ägnar sig åt betydligt allvarligare brottslighet än så. Utredningens analyser och intresseavvägningar godtogs i huvudsak i det fortsatta lagstiftningsarbetet. Vi gör ingen annan bedömning utan hänvisar till dessa ställningstaganden, se prop. 2022/23:126 s. 94 ff. och 239.

7.4.4 Nya möjligheter att utreda vem som skäligen kan misstänkas för visst brott eller delaktighet i viss brottslighet

Förslag: Det ska införas utökade möjligheter till hemlig dataavläsning avseende kameraövervakningsuppgifter samt uppgiftstyperna i nu föreslagna 2 § första stycket 2, 3 och 6 lagen om hemlig dataavläsning, om åtgärden är av synnerlig vikt för utredningen, för att utreda vem som skäligen kan misstänkas för brottet eller brotten vid en förundersökning om brott som avses i 27 kap. 18 b § andra stycket rättegångsbalken. En sådan hemlig dataavläsning ska endast få avse ett avläsningsbart informationssystem som

1. det finns särskild anledning att anta att gärningsmannen eller någon annan som har medverkat till brottet eller brotten har använt eller kommer att använda, eller,
2. om tillståndet gäller uppgiftstyperna i nu föreslagna 2 § första stycket 2, 3 eller 6 lagen om hemlig dataavläsning, det finns synnerlig anledning att anta att gärningsmannen eller någon annan som har medverkat till brottet eller brotten har kontaktat eller kommer att kontakta.

Ett tillstånd till hemlig dataavläsning avseende kameraövervakningsuppgifter för att utreda vem som skäligen kan misstänkas får inte verkställas på en plats som är någons stadigvarande bostad, annat än om det finns synnerliga skäl att anta att den person som åtgärden riktar sig mot uppehåller sig i direkt anslutning till det avläsningsbara informationssystemet.

Skälen för våra förslag

Hemlig dataavläsning kräver som huvudregel en skäligen misstänkt

Hemlig dataavläsning får som utgångspunkt användas endast om någon är skäligen misstänkt för brott. Ett undantag från denna huvudregel finns i 5 § första stycket lagen om hemlig dataavläsning. Enligt den bestämmelsen får hemlig dataavläsning avseende kommunikationsövervaknings- eller platsuppgifter, om åtgärden är av synnerlig vikt för utredningen, beviljas för att utreda vem som skäligen kan misstänkas

för brottet eller brotten vid en förundersökning om brott som avses i 27 kap. 19 b § andra stycket rättegångsbalken. Detta överensstämmer med vad som gäller för hemlig övervakning av elektronisk kommunikation enligt 27 kap. 20 § andra stycket rättegångsbalken. Även hemlig kameraövervakning kan i undantagsfall användas för att fastställa vem som skäligen kan misstänkas för brottet, se 27 kap. 20 c § rättegångsbalken. Något motsvarande undantag finns inte för hemlig dataavläsning avseende kameraövervakningsuppgifter. Utredningen om hemlig dataavläsning analyserade inte frågan närmare. I det efterföljande lagstiftningsarbetet hade regeringen svårt att se tillräckliga behov av åtgärden och lämnade därför inte heller något förslag härom (se prop. 2019/20:64 s. 125).

Lagändringar om nya möjligheter att använda kommunikationsavlyssningsuppgifter i syfte att utreda vem som skäligen kan misstänkas för brott

Den 1 oktober 2023 infördes en ny möjlighet att använda hemlig avlyssning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas för ett visst brott eller delaktighet i viss brottslighet. Lagändringen framgår av 27 kap. 18 b § rättegångsbalken. I konsekvens härmed infördes även en möjlighet att i motsvarande syfte använda hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter, se 4 b § lagen om hemlig dataavläsning. Bestämmelsen hänvisar tillbaka till 27 kap. 18 b § andra stycket rättegångsbalken.

Åtgärden ska enligt lagändringarna kunna ske i realtid och det krävs att den är av synnerlig vikt för utredningen. De nya bestämmelserna innehåller också en avgränsning i fråga om vilket avläsningsbart informationssystem som åtgärden får avse. Som huvudregel krävs att brottet eller brottsligheten kan leda till hemlig rumsavlyssning. Huvudregeln kompletteras med en brottskatalog över viss allvarlig brottslighet.

I motiven framhålls flera situationer där behovet av den föreslagna åtgärden är påtagligt. Det redogörs för flera typiska exempel där brottsbekämpande myndigheter har kännedom om att en viss ip-adress eller ett visst telefonnummer kan knytas till brott, men där numret eller adressen inte är möjlig att koppla till en viss person. Det kan t.ex. handla om bedrägerier eller utpressning över telefon, internetrelaterade sexualbrott eller annan it-brottslighet. Utredningens analyser och intresseavvägningar godtogs i det fortsatta lagstiftningsarbetet. Vi

gör ingen annan bedömning utan hänvisar till dessa ställningstaganden, se prop. 2022/23:126 s. 117 ff. och 240.

Utökade möjligheter till hemlig dataavläsning avseende punkt 2, 3 och 6-uppgifter i syfte att utreda vem som skäligen kan misstänkas för brott

Tidigare överväganden

Utredningen om utökade möjligheter att använda hemliga tvångsmedel övervägde även om det bör införas en möjlighet till hemlig dataavläsning avseende uppgiftstyperna i nuvarande 2 § första stycket 6 och 7 i syfte att utreda vem som skäligen kan misstänkas för brott eller delaktighet i viss brottslighet. Utredningen bedömde dock att det inte bör införas en sådan möjlighet. Man ifrågasatte inledningsvis om det över huvud taget finns ett behov av sådana uppgifter i ett så tidigt skede av utredningen. Så snart någon är skäligen misstänkt kan ju hemlig dataavläsning i stället ske enligt bestämmelserna i 4 § lagen om hemlig dataavläsning. I det läget kan det fattas beslut om hemlig dataavläsning avseende uppgiftstyperna i punkt 6 och 7. Vidare ansåg utredningen att redan möjligheten att inhämta kommunikationsavlyssningsuppgifter innan det finns en skäligen misstänkt utgör en nyhet och en ökad risk för att personer som visar sig vara ovidkommande drabbas av tvångsmedlet. Den omständigheten att hemlig dataavläsning utgör en tidsbegränsad försökslagstiftning som ska utvärderas innebar enligt utredningen att det är motiverat med särskild försiktighet. Sammantaget bedömde utredningen att övervägande skäl talade emot en möjlighet att använda uppgiftstyperna i 2 § första stycket 6 och 7 lagen om hemlig dataavläsning i syfte att utreda vem som skäligen kan misstänkas för brott. Utredningen konstaterade samtidigt att det kan vara motiverat att på nytt överväga frågan i samband med att lagen utvärderas, se SOU 2022:19 s. 302 f. I det vidare lagstiftningsarbetet ansåg regeringen att det saknades tillräckligt underlag för att frångå utredningens bedömning. Man konstaterade dock att det fanns skäl att överväga frågan i ett annat sammanhang och att frågan därför hade lämnats över till Utredningen om utvärdering av hemlig dataavläsning, se prop. 2022/23:126 s. 123.

Vårt förslag

Vi föreslår att det ska införas utökade möjligheter att använda hemlig dataavläsning avseende uppgiftstyperna i nu föreslagna 2 § första stycket 2, 3 och 6 lagen om hemlig dataavläsning (nuvarande 2 § första stycket 2, 3, 6 och 7), dvs. alla uppgifter som kan hämtas in genom hemlig dataavläsning med undantag för kameraövervaknings- och rumsavlyssningsuppgifter, i syfte att utreda vem som skäligen kan misstänkas för ett visst brott eller delaktighet i viss brottslighet. Kvalifikationskraven för den föreslagna åtgärdens tillämpning bör motsvara de som gäller för användning av hemlig avlyssning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas för ett visst brott eller delaktighet i viss brottslighet.

Behov, nytta och effektivitet

Det främsta skälet för vårt förslag är att det i flera fall finns ett påtagligt behov av att kunna ta del av sådana uppgifter som avses i nuvarande punkterna 6 och 7 i ett tidigt skede av en brottsutredning. Som vi framhållit i avsnitt 6.2.5 och 7.3.2 går det emellertid sällan på förhand att särskilja uppgifter som av lagstiftaren kategoriseras under punkt 1–3 från uppgifter som faller under nuvarande punkt 6 och 7. Vid inhämtning av nuvarande punkt 6- och 7-uppgifter föreligger med andra ord oftast ett behov av att hämta in även uppgifter som är att kategorisera under punkterna 1–3, jfr systematiken i 27 kap. 18 § andra stycket rättegångsbalken. Redan i dag är det enligt 4 b § lagen om hemlig dataavläsning möjligt att hämta in punkt 1-uppgifter (kommunikationsavlyssningsuppgifter) för att utreda vem som skäligen kan misstänkas. Vid sådan inhämtning finns alltså redan i dag en risk för få in s.k. metadata som är att kategorisera under nuvarande punkterna 6 eller 7, och som därmed utgör otillåten tilläggsinformation enligt 23 § lagen om hemlig dataavläsning. Sammantaget talar såväl systematiska som ändamålsenliga skäl för att det föreligger ett påtagligt behov av att införa en möjlighet att i angivet syfte hämta in såväl sådana uppgifter som avses i nuvarande punkt 6 och 7 som sådana uppgifter som avses i punkt 2 och 3. Användningen av Darknet, krypterade applikationer och viss annan digital kommunikation bygger på anonymiseringsåtgärder och användning av alias. Darknet är en anonymiserad och krypterad del av internet med mark-

nadsplatser som har beskrivits som ett ”Ebay för illegala varor” (se Brå 2021:10 s. 100 f. och 152). Vid brott över internet, exempelvis narkotikahandel under alias på Darknet, grova dataintrång, cyberbrott genom användning av s.k. ransomware (skadlig programvara, exempelvis virus, trojaner eller spionprogram, som planteras i syfte att utpressa en person eller organisation) eller internetrelaterade sexuella övergrepp mot barn, används vanligen en komplex digital infrastruktur. Anonymiseringen och krypteringen gör det svårt och många gånger omöjligt att genom traditionella tvångsmedel utreda vem eller vilka som ligger bakom den i övrigt fullt synliga brottsligheten. Detta utgör oacceptabla hinder i den brottsbekämpande verksamheten. Genom teknik- och brottsutveckling har det alltså uppstått ett behov av nya sätt för att kunna identifiera en gärningsman, vilket tidigare ofta kunde ske genom traditionella tvångsmedel. Information om vem som ligger bakom den allvarliga brottsligheten skulle kunna bli åtkomlig genom hemlig dataavläsning med stöd av nuvarande 2 § första stycket 6 och 7 lagen om hemlig dataavläsning.

Som Säkerhetspolisen har anfört i sitt remissvar över den tidigare utredningens bedömning kan det handla om uppgifter i form av sparade bilder eller loggfiler som visar vilka program som brukar användas i ett avläsningsbart informationssystem. Dessa uppgifter kan leda till att en skäligen misstänkt kan identifieras (jfr Säkerhetspolisens remissvar av den 7 september 2022, dnr 2022-12651-2).

Företrädare för Polismyndigheten har framhållit följande. Om uppgiftstyperna i nuvarande punkt 6 och 7 fick användas i syfte att utreda vem som skäligen kan misstänkas för brott skulle Polismyndigheten kunna hämta in uppgifter som är åtkomliga på exempelvis en server. Detta skulle i sin tur innebära en möjlighet att analysera bl.a. källkoder, loggfiler, noder och andra uppgifter som inte har kommunicerats. Vid en sådan analys kan digitala spår från olika håll kombineras och utredas parallellt för att upptäcka eventuella samband, vilket många gånger är en förutsättning för att kunna identifiera personerna bakom brottsligheten. Om det däremot saknas centrala delar av information reduceras möjligheten att dra korrekta slutsatser i analysen. Därmed försämras också möjligheterna att komma vidare i utredningen. Vid internetrelaterade sexuella övergrepp mot barn sker en stor del av kommunikationen, dvs. text och fildelning, via olika Darknetforum. Initialt uppstår misstanke om brott då en fil föreställande dokumenterade sexuella övergrepp mot barn påträffas. Filen

kan ha skickats från alias 1 till alias 2 via ett sådant forum. I vissa fall kan ett fåtal intressanta personer identifieras, men i detta skede kan ingen av dessa personer anses som skäligen misstänkt för brottet. En möjlighet att i en sådan situation hämta in uppgifter genom hemlig dataavläsning skulle öka förutsättningarna för att komma vidare i utredningen. Det ska i sammanhanget understrykas att denna typ av allvarlig brottslighet ofta saknar nationella gränser. Personerna bakom brottsligheten är vanligen utspridda i olika länder. En förutsättning för att kunna upptäcka, avbryta och utreda den kriminella verksamheten är att de brottsbekämpande myndigheterna kan använda effektiva hemliga tvångsmedel mot exempelvis servrar och krypterade informationssystem som används i kriminella syften. Avsaknaden av den möjligheten gör att man i Sverige inte kommer vidare i vissa brottsutredningar och inte heller kan biträda andra länder i deras utredningar rörande allvarlig brottslighet. Detta innebär också en risk för att Sverige blir ett land där det är attraktivt att placera digital infrastruktur som används för illegala syften. Det har avslutningsvis framhållits att behovet av att hämta in åtkomstuppgifter för att kunna identifiera gärningspersoner inte är begränsat till komplexa digitala infrastrukturer. Behovet föreligger tvärtom beträffande alla typer av informationssystem. När det gäller en mobiltelefon kan exempelvis uppgifter i form av en telefonlista, fotografier eller uppgifter om nätverk innebära att en snabb identifiering kan göras redan i ett tidigt skede av utredningen.

Vi bedömer sammantaget att det föreligger ett påtagligt behov av uppgifterna även i ett initialt skede av utredningen.

Eftersom hemlig dataavläsning i dessa avseenden kan användas för att få fram avgörande information som på grund av anonymisering och kryptering inte går att ta del av genom andra tvångsmedel kan åtgärden förväntas vara effektiv och medföra avsevärd nytta för brottsbekämpningen.

Åtgärden innebär en viss ökad risk för den personliga integriteten

Förslaget innebär en utökning av tillämpningsområdet för hemlig dataavläsning som kan komma att leda till inhämtning av större mängder information än i dag. Eftersom syftet med åtgärden är att utreda vem som skäligen kan misstänkas är det ofrånkomligt att tvångs-

medlet kan komma att riktas mot en mer obestämbar krets av personer. Förslaget innebär därmed ökade risker för enskildas personliga integritet och en ökad risk för att ovidkommande drabbas av åtgärden. Graden av integritetsintrång kan variera beroende på tillståndets utformning och vilket avläsningsbart informationssystem som den hemliga dataavläsningen riktar sig mot. Hur kännbar åtgärden är ur integritetssynpunkt måste alltid bedömas utifrån omständigheterna i det enskilda fallet. Ett exempel på när åtgärden kan leda till identifiering av en skäligen misstänkt samtidigt som graden av integritetsintrång bedöms som låg är när åtgärden riktar sig mot en s.k. proxyserver där den ende användaren av proxyservern är den person som utför det aktuella brottet, t.ex. i en utredning om grovt dataintrång (jfr Säkerhetspolisens remissvar av den 7 september 2022, dnr 2022-12651-2). Inte heller ett tillstånd där åtgärden riktas mot en avgränsad del av Darknet bedöms vara förenat med några större integritetsrisker.

Vårt förslag innebär också bättre möjligheter för de brottsbekämpande myndigheterna att upptäcka och utreda allvarlig brottslighet. I detta avseende innebär förslaget ett förstärkt skydd för enskildas personliga integritet.

Åtgärden bedöms vara proportionerlig

De ökade risker för den personliga integriteten som åtgärden kan innebära bör balanseras mot särskilda krav för den föreslagna åtgärdens användande. De intresseavvägningar som tidigare har gjorts beträffande möjligheten att använda hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter för att utreda vem som skäligen kan misstänkas gör sig gällande även här. Vi hänvisar därför till dessa ställningstaganden, se prop. 2022/23:126 s. 117 ff. och 240. Kraven bör därför motsvara vad som gäller för kommunikationsavlyssningsuppgifter enligt 4 b § lagen om hemlig dataavläsning. Det innebär att den föreslagna åtgärden måste vara av synnerlig vikt för utredningen och att tillämpningsområdet för åtgärdens användande ska begränsas genom särskilda krav på brottets eller brottslighetens allvar. Huvudregeln att det ska röra sig om brott där straffvärdet motsvarar fängelse fyra år eller mer, jämte en särskild brottskatalog, se 27 kap. 18 b § andra stycket rättegångsbalken. Vidare ska det ställas särskilda krav på sam-

band mellan den person som den hemliga dataavläsningen riktas mot och det informationssystem som avläsningen avser, motsvarande de krav som gäller enligt 27 kap. 18 b § tredje stycket rättegångsbalken.

De höga kvalifikationskrav som föreslås bedöms utgöra en kraftig begränsning av möjligheten att använda den föreslagna åtgärden. Det påtagliga behov som konstaterats motiverar varför förslaget är proportionerligt även i förhållande till övriga bestämmelser i lagen, närmast 4 a och 5 §§ lagen om hemlig dataavläsning, särskilt eftersom tillämpningsområdet torde bli begränsat. De uppräknade bestämmelserna omfattar färre uppgiftstyper men har vidare brottskataloger än den som nu föreslås och som redan gäller enligt 4 b § samma lag. Det ska framhållas att utöver de höga specifika kvalifikationskrav som föreslås, gäller proportionalitetsprincipen som ett helt grundläggande krav för ett tillstånd till hemlig dataavläsning. Även med beaktande av de höga kvalifikationskrav som föreslås och övriga rättssäkerhetsgarantier som redan omgärdar förslaget kan åtgärden innebära vissa ökade integritetsrisker. Åtgärden bör därför tillämpas med restriktivitet, t.ex. i situationer som de ovan exemplifierade. För att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan bör åtgärden också begränsas genom tydliga villkor för tillståndet enligt 18 § första stycket 4 lagen om hemlig dataavläsning. Vi återkommer i avsnitt 8.4.5 till våra överväganden om villkorskravet och till olika exempel på villkor.

Vid en samlad intresseavvägning framstår behovet och nyttan av att kunna utöka tillämpningsområdet på föreslaget sätt som så påtagligt att det integritetsintrång som förslaget kan innebära bedöms som försvarligt.

Hemlig dataavläsning avseende kameraövervaknings- och rumsavlyssningsuppgifter i syfte att utreda vem som skäligen kan misstänkas för brott

Tidigare överväganden

Under lagstiftningsarbetet med lagen om hemlig dataavläsning resonerade regeringen kring frågan om det bör införas en möjlighet till hemlig dataavläsning avseende kameraövervakningsuppgifter i syfte att utreda vem som skäligen kan misstänkas för brott eller delaktighet i viss brottslighet. Regeringen konstaterade att sådan kamera-

övervakning som enligt rättegångsbalken får användas för att identifiera en misstänkt endast får avse den plats där brottet har begåtts eller en nära omgivning till denna plats. Sådana fall kan t.ex. vara när ett narkotikaparti hittas på en viss plats. Då kan en kamera monteras på platsen för att iaktta vilka som besöker den. Behovet av hemlig dataavläsning i ett sådant fall, eller andra fall där hemlig kameraövervakning får användas för att identifiera en misstänkt, ansågs däremot inte särskilt stort. Företrädare för Säkerhetspolisen framförde i sitt remissyttrande att det fanns ett behov av hemlig dataavläsning för att genom en teknisk utrustnings kamera eller mikrofon kunna identifiera en misstänkt person. Regeringen ifrågasatte inte att det kunde finnas fall där det skulle vara verksamhetsmässigt värdefullt att kunna ta upp sådana uppgifter som Säkerhetspolisen föreslog. Regeringen framhöll att hemlig dataavläsning ska vara ett verktyg som ska återställa de brottsbekämpande myndigheternas förmåga och att Säkerhetspolisens förslag skulle innebära en inte obetydlig utvidgning i förhållande till då gällande reglering. Förutom integritetsintrånget såg regeringen svårigheter att säkerställa att åtgärden uppfyller det platskrav som ställs på rumsavlyssningsuppgifter. Regeringen lämnade därför varken förslag om att införa en möjlighet till hemlig dataavläsning avseende kameraövervakningsuppgifter eller rumsavlyssningsuppgifter i syfte att utreda vem som skäligen kan misstänkas för brott eller delaktighet i viss brottslighet.

Vårt förslag

Vi föreslår att det ska införas en möjlighet att använda hemlig dataavläsning avseende kameraövervakningsuppgifter i syfte att utreda vem som skäligen kan misstänkas för ett visst brott eller delaktighet i viss brottslighet. Kvalifikationskraven för den föreslagna åtgärdens tillämpning föreslås motsvara i huvudsak de som gäller för användning av hemlig avlyssning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas för ett visst brott eller delaktighet i viss brottslighet. Vid inhämtning av kameraövervakningsuppgifter i angivet syfte har vi dock inte funnit skäl att göra undantag från huvudregeln om att informationssystemet i fråga måste antas ha använts eller kommer att användas av gärningsmannen eller någon annan som har medverkat till brottet eller brotten. Ett tillstånd till

hemlig dataavläsning avseende kameraövervakningsuppgifter i angivet syfte ska inte heller få verkställas på en plats som är någons stadigvarande bostad, annat än om det finns synnerliga skäl att anta att den person som åtgärden riktar sig mot uppehåller sig i direkt anslutning till det avläsningsbara informationssystemet. Vidare får hemlig dataavläsning som gäller kameraövervakningsuppgifter aldrig användas på en plats dit tillträdestillstånd enligt 13 § inte får beviljas.

Behov, nytta och effektivitet

Redan systematiska och ändamålsenliga skäl talar för att tillämpningsområdet för kameraövervakningsuppgifter bör korrespondera med tillämpningsområdet för hemlig kameraövervakning. Det främsta skälet för vårt förslag är emellertid att det i flera fall finns ett påtagligt behov av att kunna ta del av kameraövervakningsuppgifter i ett tidigt skede av en brottsutredning.

När det gäller hemlig dataavläsning avseende rumsavlyssningsuppgifter för att identifiera en skäligen misstänkt gör vi följande principiella ställningstagande. Vi delar Säkerhetspolisens bedömning om att det finns ett påtagligt behov av hemlig dataavläsning avseende rumsavlyssningsuppgifter för att kunna identifiera en skäligen misstänkt person. Som vi fastslagit i avsnitt 7.4.1 utgör dock tillämpningsområdet för de permanenta hemliga tvångsmedlen en naturlig utgångspunkt för utformningen av tillämpningsområdet för hemlig dataavläsning. Eftersom det inte är tillåtet med hemlig rumsavlyssning för att identifiera en skäligen misstänkt, har frågan om att införa en sådan möjlighet avseende rumsavlyssningsuppgifter inte tidigare övervägts. Av samma skäl går inte heller vi vidare med någon analys om huruvida det bör införas en sådan möjlighet. För det fall som tillämpningsområdet för det bakomliggande tvångsmedlet utvidgas bör dock frågan åter övervägas.

Bland personer som ägnar sig åt allvarlig brottslighet är det väl känt hur man ska agera för att undgå upptäckt. Kriminellas användning av Darknet samt legitima tjänster t.ex. som anonyma abonnemang och s.k. proxyservrar i syfte att minimera digitala avtryck och undvika identifiering kan nämnas som exempel på detta. Många gånger känner de brottsbekämpande myndigheterna till att ett visst informationssystem används som brottsverktyg för att begå allvarlig brottslighet,

men saknar samtidigt verktyg för att identifiera den misstänkte. En vanlig invändning vid allvarlig brottslighet som exempelvis internetrelaterade sexualbrott mot barn och narkotikabrottslighet över internet är att den misstänkte vid tiden för brottet hade lånat ut sin dator eller telefon till någon annan. Eftersom information om vem som använder ett visst informationssystem sällan är åtkomlig genom traditionella tvångsmedel innebär detta att brottsbekämpande myndigheter många gånger inte kommer vidare i dessa utredningar. Eftersom teknik- och brottsutvecklingen fortsätter i snabb takt är behovet av mer effektiva verktyg i brottsbekämpningen i detta avseende påtagligt.

Tekniska framsteg har samtidigt gjort det möjligt att införa effektiva verktyg. Möjligheten att använda hemlig dataavläsning avseende kameraövervakningsuppgifter för att utreda vem som skäligen kan misstänkas för brott skulle kunna ge avgörande upplysningar om vem som ligger bakom brottsligheten i fråga. Genom att vid givet tillfälle aktivera kamerafunktionen på den informationsutrustning som man ringat in som brottsverktyg skulle myndigheten enkelt kunna identifiera den misstänkte. En invändning om t.ex. en utlånad dator skulle då kunna prövas i ett tidigt skede av utredningen, vilket i sin tur skulle innebära en tidig möjlighet att avskriva misstänkta från utredningen. Säkerhetspolisen lämnade under lagstiftningsarbetet med lagen om hemlig dataavläsning följande exempel på ett typfall som kan illustrera behovet av hemlig dataavläsning avseende bl.a. kameraövervakningsuppgifter för att identifiera en skäligen misstänkt person (se SOU 2017:89 s. 624).

> Efter ett fullbordat terroristattentat i ett av våra grannländer får Säkerhetspolisen information om att en av de misstänkta gärningsmännen dagarna före dådet har haft kontakt med ett svenskt mobiltelefonnummer. Det rör sig om ett anonymt kontantkort. Misstanken i Sverige rör medhjälp till terroristbrott. Vid verkställighet av HÖK visar det sig att utrustningen inte används för vanliga telefonsamtal utan att den har varit uppkopplad mot internet vid ett flertal tillfällen.
>
> HDA skulle ge möjlighet att installera ett tekniskt hjälpmedel så att utrustningens position blir klarlagd. Samtidigt kan åtgärden ge möjlighet att med hjälp av telefonens kamera och mikrofon identifiera personen som använder utrustningen.

De brottsbekämpande myndigheternas behov av hemlig dataavläsning avseende kameraövervakningsuppgifter för att identifiera en skäligen misstänkt person får sammantaget anses påtagligt. En sådan möjlighet skulle innebära ett genombrott för brottsbekämpningen på denna

punkt. Åtgärden skulle kunna användas dels för att identifiera misstänkta i utredningar som annars måste läggas ner, dels för att kunna skriva av personer från vidare misstanke. Förslaget får därför förväntas vara effektivt och medföra avsevärd nytta för brottsbekämpningen.

Åtgärden innebär en viss ökad risk för den personliga integriteten

Förslaget innebär en utökning av tillämpningsområdet för hemlig dataavläsning som kan komma att leda till inhämtning av större mängder information än i dag. Förslaget innebär ökade risker för enskildas personliga integritet och en ökad risk för att personer utan koppling till brottslighet drabbas av åtgärden. Detta gäller särskilt i de fall som åtgärden verkställs på en plats som kan vara någons bostad. Graden av integritetsintrång kan dock variera beroende på tillståndets utformning och vilket avläsningsbart informationssystem som den hemliga dataavläsningen avser. Hur kännbar åtgärden är ur integritetssynpunkt måste alltid bedömas utifrån omständigheterna i det enskilda fallet.

Följande kan dock konstateras. Förbudet mot att hämta in kameraövervakningsuppgifter i någons stadigvarande bostad har sin förebild i rättegångsbalken. Enligt 27 kap. 25 a § rättegångsbalken får ett tillstånd som avser hemlig kameraövervakning aldrig avse tillträde för installation av tekniska hjälpmedel i någons stadigvarande bostad. Verkställighet av hemlig dataavläsning avseende kameraövervakningsuppgifter skiljer sig dock från verkställighet av hemlig kameraövervakning. Vid hemlig kameraövervakning sker inhämtning av uppgifter genom kamerautrustning som tillhör och monteras av de brottsbekämpande myndigheterna. Vid hemlig dataavläsning som gäller kameraövervakningsuppgifter i syfte att utreda vem som är skäligen misstänkt krävs inget installationsmoment eller tillträdestillstånd eftersom verkställighet sker genom aktivering av kamerafunktionen i det informationssystem som tillståndet avser. Sådan hemlig dataavläsning kan också under vissa omständigheter innebära större möjligheter än hemlig kameraövervakning att avgränsa åtgärden på ett sådant sätt att integritetsintrånget för utomstående minimeras. Se vidare angående villkor för tillståndet nedan. Åtgärden bedöms på detta sätt kunna ge en säkrare träffbild och innebära en lägre risk för att drabba personer utan koppling till brottslighet i förhållande till användning av hemlig kameraövervakning i samma syfte. Hemlig data-

avläsning som gäller kameraövervakningsuppgifter behöver alltså inte innebära motsvarande integritetsintrång som hemlig kameraövervakning. Mot denna bakgrund och med beaktande av att det finns ett påtagligt behov av åtgärden har vi funnit det motiverat att göra ett avsteg från systematiken och huvudregeln om att hemlig dataavläsning som gäller kameraövervakningsuppgifter inte får verkställas på en plats som är någons stadigvarande bostad. Vårt förslag innebär i denna del en ökad risk för den personliga integriteten, eftersom det föreslagna undantaget utgör en inskränkning i det grundläggande skyddet för privat- och familjelivet. Vi återkommer i proportionalitetsbedömningen nedan till våra överväganden i detta avseende.

Vårt förslag innebär också bättre möjligheter för de brottsbekämpande myndigheterna att upptäcka och utreda allvarlig brottslighet. I detta avseende innebär förslaget ett förstärkt skydd för enskildas personliga integritet.

Åtgärden bedöms vara proportionerlig

De ökade risker för den personliga integriteten som åtgärden kan innebära bör balanseras mot särskilda krav för åtgärdens användande. Kravet på att hemlig kameraövervakning för att identifiera en skäligen misstänkt endast får avse den plats där brottet har begåtts eller en nära omgivning till denna plats är anpassad efter hur tekniken för den åtgärden fungerar, i syfte att tillgodose olika integritetsaspekter med åtgärden. Som vi redogjort för i det föregående skiljer sig metoden för hemlig dataavläsning på ett avgörande sätt från verkställighet av hemlig kameraövervakning. Det är därför inte ändamålsenligt att utforma kraven för den föreslagna åtgärdens användande med bestämmelsen i 27 kap. 20 c § rättegångsbalken som förebild. Med hänsyn till hur metoden för hemlig dataavläsning fungerar framstår det som mer motiverat att göra avsteg från systematiken i rättegångsbalken och i stället balansera de ökade riskerna mot särskilda krav på brottets allvar och krav på samband mellan den person som den hemliga dataavläsningen riktas mot och det informationssystem som avläsningen avser. De intresseavvägningar som tidigare har gjorts beträffande hemlig avlyssning av elektronisk kommunikation och hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter i motsvarande syfte gör sig till stora delar gällande även här. Vi hänvisar därför till

dessa ställningstaganden, se prop. 2022/23:126 s. 117 ff. och 240, samt till våra överväganden i det ovanstående. Huvudsakligen motsvarande krav som gäller för hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter i motsvarande syfte ska därför gälla även för nu föreslagen åtgärd. Det innebär att den nu föreslagna åtgärden måste vara av synnerlig vikt för utredningen och att tillämpningsområdet för åtgärdens användande ska begränsas genom särskilda krav på brottets eller brottslighetens allvar. Huvudregeln att det ska röra sig om brott där straffvärdet motsvarar fängelse i fyra år eller mer, jämte en särskild brottskatalog, se 27 kap. 18 b § andra stycket rättegångsbalken. Vidare ska det ställas särskilda krav på samband mellan den person som den hemliga dataavläsningen riktas mot och det informationssystem som avläsningen avser, motsvarande de krav som gäller enligt 27 kap. 18 b § tredje stycket första punkten rättegångsbalken. Det har dock inte framkommit ett tillräckligt starkt behov av att, jämlikt andra punkten i samma bestämmelse, tillåta avläsning av något annat informationssystem än det som kan antas användas av den person som åtgärden riktar sig mot. Verkställighet av hemlig dataavläsning som gäller kameraövervakningsuppgifter för att utreda vem som skäligen kan misstänkas innebär en realtidsaktivering av kamerafunktionen på det informationssystem som tillståndet avser. Av proportionalitetsskäl ska åtgärden därför endast kunna avse ett informationssystem som det finns särskild anledning att anta att gärningsmannen eller någon annan som har medverkat till brottet eller brotten har använt eller kommer att använda. Tillämpningsområdet blir därmed mer begränsat jämfört med vad som redan gäller och vad som ovan föreslås gälla för hemlig dataavläsning avseende uppgiftstyperna i 1–3 och 6 i samma syfte.

Slutligen ska ett tillstånd till hemlig dataavläsning avseende kameraövervakningsuppgifter i angivet syfte inte få verkställas på en plats som är någons stadigvarande bostad. Ett sådant förbud motsvarar vad som gäller för hemlig kameraövervakning enligt rättegångsbalken och hemlig dataavläsning avseende kameraövervakningsuppgifter under en förundersökning, jfr 4 a § tredje och fjärde styckena lagen om hemlig dataavläsning. När det gäller hemlig dataavläsning avseende kameraövervakningsuppgifter i angivet syfte talar övervägande skäl för att i särskilda undantagsfall kunna göra avsteg från denna huvudregel och systematik. Skälen härför är följande.

Vi har ovan konstaterat att det finns ett påtagligt behov av hemlig dataavläsning avseende kameraövervakningsuppgifter för att identifiera en skäligen misstänkt person, exempelvis för att identifiera personer involverade i pågående terrorbrott. Ett annat exempel på brottslighet som åtgärden är särskilt ägnad att ta sikte på är internetrelaterade sexuella övergrepp mot barn. Eftersom sådan brottslighet vanligen begås i eller från en bostad, riskerar ett förbud mot att verkställa åtgärden på en plats som är någons stadigvarande bostad att motverka syftet med förslaget. I de fall som den brottsbekämpande myndigheten kan ringa in ett informationssystem, dvs. brottsverktyget i fråga, till ett bostadsområde, men inte tillräckligt snävt för att kunna använda mindre ingripande tvångsmedel eller metoder i syfte att identifiera den skäligen misstänkte, skulle ett undantagslöst förbud innebära att det inte går att utreda vem eller vilka som ligger bakom den i övrigt fullt synliga brottsligheten.

Ett undantag som möjliggör kameraövervakning i någons privata bostad utgör ett ingrepp i det grundlagsstadgade skyddet för privat- och familjelivet. Under ovan angivna förutsättningar bedöms dock en möjlighet till verkställighet av den föreslagna åtgärden på en plats som kan vara någons stadigvarande bostad som nödvändig, med hänsyn till intresset av att bekämpa nyssnämnd allvarlig brottslighet samt skydda brottsoffers och potentiella brottsoffers fri- och rättigheter. Vi föreslår därför att förbudet mot att verkställa föreslagen åtgärd på en plats som är någons stadigvarande bostad ska förses med ett särskilt undantag. Med hänsyn till det integritetsintrång som åtgärden kan innebära ska undantaget utformas på ett sätt som innebär att tillämpningsområdet för åtgärden blir mycket begränsat. Det ska krävas att det finns synnerliga skäl att anta att den person som åtgärden riktar sig mot uppehåller sig i direkt anslutning till det avläsningsbara informationssystem som tillståndet avser. Kravet på ”synnerliga skäl” är högt ställt och innebär att det på grund av tillförlitliga uppgifter ska vara så gott som säkert att så är fallet, jfr 27 kap. 18 b § tredje stycket andra punkten rättegångsbalken. Kravet ska beaktas vid verkställigheten och är uppfyllt exempelvis om det kan säkerställas att den som åtgärden riktar sig mot vid denna tidpunkt använder sig av informationssystemet i fråga. Som en helt grundläggande förutsättning krävs också att åtgärden är av ”synnerlig vikt” för utredningen, se 4 b § första stycket lagen om hemlig dataavläsning. Även detta krav är högt ställt. En självklar utgångspunkt är att hemlig dataavläsning

som gäller kameraövervakningsuppgifter i angivet syfte ska användas först sedan andra mindre ingripande metoder och tvångsmedel har uttömts. Detta framgår både av allmänna principer och av 3 § lagen om hemlig dataavläsning. Kravet på synnerlig vikt för utredningen innefattar således både ett kvalitetskrav på de uppgifter som kan förväntas erhållas med åtgärden och ett krav på att syftet med åtgärden i princip inte är möjligt att uppnå på något annat sätt. Med så högt ställda krav för åtgärdens användande bedömer vi det som proportionerligt att införa en möjlighet att verkställa hemlig dataavläsning som gäller kameraövervakningsuppgifter i angivet syfte även på en plats som kan vara någons stadigvarande bostad.

Det ska framhållas att hemlig dataavläsning som gäller kameraövervakningsuppgifter aldrig får användas på en plats dit tillträdestillstånd enligt 13 § inte får beviljas. Detta förbud framgår av nuvarande 6 a § lagen om hemlig dataavläsning. Ett förslag om att bestämmelsen i 6 a § ska upphöra att gälla och att en motsvarande förbudsbestämmelse i stället ska införas i en ny 11 a § samma lag är för närvarande under beredning, se SOU 2023:60. Eftersom det förslaget inte innebär någon förändring av förbudet i sak, kommer förbudet under alla omständigheter att omfatta även vårt förslag. Några författningsändringar i detta avseende är alltså inte nödvändiga.

De ökade integritetsrisker som förslaget trots detta innebär medför att åtgärden och i synnerhet det föreslagna undantaget bör tillämpas med restriktivitet. Intresset av att den berördes personliga integritet inte kränks i onödan och att ovidkommande personers integritet skyddas så långt det är möjligt bör därför säkerställas genom tydliga villkor för åtgärdens användande enligt 18 § första stycket 4 lagen om hemlig dataavläsning. Det bör krävas att det av ansökan eller tillhörande underlag tydligt framgår hur informationssystemet i fråga har ringats in och att tillståndet utifrån denna information utformas med särskilda villkor för åtgärdens användande, anpassade efter det enskilda fallet. Eftersom hemlig dataavläsning avseende kameraövervakningsuppgifter endast avser inhämtning av realtidsuppgifter bör villkoren ta tydligt sikte på verkställighetsperioden. Det kan i många fall vara nödvändigt med villkor om åtgärder som exempelvis spaning i samband med verkställigheten, för att kunna säkerställa att integritetsintrånget för den enskilde och risken för att utomstående drabbas minimeras. Se exempel 5–7 i avsnitt 8.4.5.

Under dessa förutsättningar framstår det samlade integritetsintrång som förslaget kan innebära som försvarligt i förhållande till behovet och nyttan av att utöka tillämpningsområdet på föreslaget sätt.

7.4.5 Nya möjligheter att hämta in kommunikationsövervakningsuppgifter i realtid i syfte att utreda vem som skäligen kan misstänkas för brott

Tidigare begränsningar till förfluten tid

Vid ikraftträdandet av den nya lagen fick hemlig dataavläsning avseende kommunikationsövervakningsuppgifter i syfte att utreda vem som skäligen kan misstänkas för brott endast avse förfluten tid. Skälen för begränsningen kommenterades inte närmare i förarbetena (jfr prop. 2019/20:64 s. 124 f. och SOU 2017:89 s. 259 f.). Motsvarande begränsning gällde vid tidpunkten även vid hemlig övervakning av elektronisk kommunikation i syfte att utreda vem som kan misstänkas för brott, se dåvarande 27 kap. 20 § andra stycket rättegångsbalken. Någon närmare motivering till denna begränsning angavs inte heller i förarbetena (jfr prop. 2011/12:55 s. 72 och SOU 2009:1 s. 113–116).

Lagändringar om slopade begränsningar

Den 1 oktober 2023 infördes en möjlighet att vid hemlig övervakning av elektronisk kommunikation inhämta uppgifter om meddelanden i realtid i syfte att utreda vem som skäligen kan misstänkas för brott. Lagändringen innebar att den tidigare begränsningen till historiska uppgifter slopades, se 27 kap. 19 b § rättegångsbalken. I konsekvens härmed slopades motsvarande begränsning för hemlig dataavläsning avseende kommunikationsövervakningsuppgifter, se 5 § lagen om hemlig dataavläsning.

I motiven bakom förslagen framhålls att det finns ett påtagligt behov av uppgifter om meddelanden i realtid, i synnerhet i fråga om komplexa cyberbrott. Andra exempel som tas upp är internetrelaterade sexualbrott mot barn, inklusive barnpornografibrott (se SOU 2022:19 s. 204 ff.). Utredningens analyser och intresseavvägningar godtogs i det fortsatta lagstiftningsarbetet. Vi gör ingen annan bedömning utan

hänvisar till dessa ställningstaganden, se prop. 2022/23:126 s. 137 f. och 241.

7.4.6 Nya möjligheter att knyta hemlig dataavläsning avseende kameraövervaknings- och rumsavlyssningsuppgifter till en person

Det ursprungliga platskravet

Frågan om anknytning mellan person och tvångsmedel avseende kameraövervaknings- och rumsavlyssningsuppgifter har varit föremål för överväganden i flera tidigare lagstiftningsarbeten (se t.ex. prop. 1994/95:227 s. 20–22, prop. 1995/96:85 s. 30–32 och prop. 2013/14:237 s. 96 och 97). Lagstiftaren har inte vid något av dessa tillfällen funnit tillräckliga skäl att knyta ett sådant tvångsmedel till en person i stället för till en plats. Även när lagen om hemlig dataavläsning infördes ansågs att det fanns starka betänkligheter med att knyta ett tillstånd avseende kameraövervaknings- och rumsavlyssningsuppgifter till en person i stället för till en viss plats. Regeringen gjorde då samma principiella bedömningar som tidigare. Tillstånd till hemlig dataavläsning avseende kameraövervaknings- och rumsavlyssningsuppgifter var därför ursprungligen, precis som tillstånd till de bakomliggande tvångsmedlen, underkastade ett undantagslöst platskrav (se prop. 2019/20:64 s. 86 och 118 ff.).

Nya möjligheter att knyta tillstånd till person i stället för plats

Den 1 oktober 2023 infördes en möjlighet att kunna knyta ett tillstånd till hemlig rumsavlyssning och hemlig kameraövervakning till den skäligen misstänkte i stället för till en plats. De nya bestämmelserna infördes i 27 kap. 20 b § tredje stycket, 20 e § tredje stycket samt 21 § första och sjätte styckena rättegångsbalken. I konsekvens härmed infördes även en möjlighet att knyta ett tillstånd till hemlig dataavläsning avseende rumsavlyssnings- och kameraövervakningsuppgifter till den skäligen misstänkte i stället för till en viss plats. De nya bestämmelserna framgår av 4 a § fjärde stycket, 6 § fjärde stycket, 14 § andra stycket och 18 § tredje stycket lagen om hemlig dataavläsning. Bestämmelserna är utformade som undantagsbestämmel-

ser, på sätt att åtgärden får användas endast om det finns särskilda skäl för den. Tillämpningsområdet begränsas ytterligare genom olika begränsningar i fråga om platsen. Vidare får villkorskravet en betydligt större betydelse än tidigare eftersom åklagaren är skyldig att i samband med ansökan föreslå de villkor som ska gälla för åtgärden.

Bakgrunden till lagändringarna är de överväganden om platskravet som gjordes av Utredningen om utökade möjligheter att använda hemliga tvångsmedel (SOU 2022:19). Utredningen konstaterar i sitt betänkande att förutsättningarna för bedömningen har ändrats sedan frågan senast övervägdes. Sammanfattningsvis framhålls följande. Med hänsyn till kriminellas riskmedvetenhet är det numera alltmer sällan som hemlig rumsavlyssning och hemlig kameraövervakning kan verkställas i ett avgränsat utrymme. Den tendens till uppluckring av platsbegreppet som kan skönjas i rättsutvecklingen kan inte förstås på något annat sätt än som en anpassning av rättstillämpningen till denna utveckling. Praxis om hur preciserad platsangivelsen måste vara varierar också kraftigt. Det är vidare relativt vanligt att de brottsbekämpande myndigheterna avstår från att ansöka om tillstånd eftersom en specifik plats inte kan anges. Sammantaget bedöms det nuvarande platskravet kunna leda till oacceptabla hinder i den brottsbekämpande verksamheten. Beträffande hemlig dataavläsning framhålls särskilt att det ställningstagande som togs inför införandet av lagen om hemlig dataavläsning bör ses i ljuset av att det för de bakomliggande tvångsmedlen hemlig rumsavlyssning och hemlig kameraövervakning inte fanns något alternativ till att knyta tillståndet till en viss plats. I propositionen fördes det inte några resonemang om andra möjligheter än en platsangivelse för att begränsa integritetsintrånget och reglerna utformades med de bakomliggande hemliga tvångsmedlen som förebild (se a. SOU s. 332 f.). Utredningens analyser och intresseavvägningar godtogs i det fortsatta lagstiftningsarbetet. Vi gör ingen annan bedömning utan hänvisar till dessa ställningstaganden, se prop. 2022/23:126 s. 143 ff., 240 och 242.

7.4.7 Förslaget om hemlig dataavläsning i syfte att verkställa ett frihetsberövande

Bakgrund

Det har tidigare inte varit möjligt att använda hemlig övervakning av elektronisk kommunikation eller hemlig dataavläsning avseende kommunikationsövervaknings- eller platsuppgifter i syfte att lokalisera en person för att verkställa ett frihetsberövande. Utredningen om utökade möjligheter att använda hemliga tvångsmedel hade bl.a. i uppdrag att ta ställning till om hemlig övervakning av elektronisk kommunikation ska få användas för att lokalisera personer som är häktade i sin frånvaro efter att en förundersökning har avslutats, eller som har uteblivit eller avvikit från verkställighet av påföljd (se dir. 2022:13). För att upprätthålla en välfungerande systematik i regelverket för hemliga tvångsmedel övervägde utredningen även hemlig dataavläsning som metod för att lokalisera de kategorier av eftersökta personer som omfattades av uppdraget. Utredningens överväganden och förslag framgår av slutbetänkandet *Bättre möjligheter att verkställa frihetsberövanden* (SOU 2022:50). Betänkandet bereds för närvarande i Regeringskansliet.

Förslaget om hemlig dataavläsning i syfte att verkställa anhållning och häktning

I SOU 2022:50 föreslås att det ska införas en möjlighet att använda hemlig övervakning av elektronisk kommunikation i syfte att eftersöka en person som är anhållen eller häktad. Det kan t.ex. handla om någon som anhållits eller häktats i sin utevaro eller som avvikit från häktet. Det krävs att åtgärden är av synnerlig vikt för att personen ska kunna lokaliseras. I konsekvens härmed föreslås att det i lagen om hemlig dataavläsning ska införas en motsvarande möjlighet att i det nu angivna syftet använda hemlig dataavläsning avseende kommunikationsövervaknings- och platsuppgifter. Respektive tvångsmedel ska kunna användas endast om det är fråga om brott eller brottslighet som hade kunnat föranleda användning av tvångsmedlet i utredningssyfte. Tillståndsprövningen ska göras av allmän domstol och åklagare ska ha samma möjlighet som annars att i brådskande fall meddela interimistiskt beslut. Lagförslagen innebär alltså att det in-

förs ett nytt ändamål med såväl hemlig övervakning av elektronisk kommunikation som hemlig dataavläsning avseende kommunikationsövervaknings- och platsuppgifter.

Inom ramen för vårt uppdrag har vi inte funnit anledning att ifrågasätta eller vidareutveckla dessa överväganden och förslag, se a. SOU s. 84 ff., 95 ff. och 167 f. Eftersom förslagen för närvarande är under beredning finns det inte någon anledning för oss att lämna ett eget förslag i frågan.

Förslaget om hemlig dataavläsning i syfte att verkställa en påföljd

I SOU 2022:50 föreslås också att det ska införas bestämmelser som möjliggör användning av hemlig övervakning av elektronisk kommunikation och hemlig dataavläsning som gäller kommunikationsövervaknings- och platsuppgifter i syfte att lokalisera personer som håller sig undan från en frihetsberövande påföljd. De nya bestämmelserna föreslås regleras i en ny lag. Den föreslagna lagens bestämmelser är till stora delar utformade med bestämmelserna i 27 kap. rättegångsbalken och lagen om hemlig dataavläsning som förebilder. Flera av bestämmelserna i den nya lagen hänvisar även till 27 kap. rättegångsbalken och lagen om hemlig dataavläsning. Enligt den nya lagen krävs att den eftersökte är dömd till fängelse, rättspsykiatrisk vård eller sluten ungdomsvård samt att tvångsmedlet är av synnerlig vikt för att personen ska kunna lokaliseras. Vidare krävs att den dom som ska verkställas omfattar brott eller brottslighet som kan leda till respektive hemligt tvångsmedel enligt reglerna i 27 kap. rättegångsbalken respektive lagen om hemlig dataavläsning, eller att den eftersökte dömts till rättspsykiatrisk vård med särskild utskrivningsprövning. Tillstånd enligt den nya lagen prövas av Stockholms tingsrätt på ansökan av åklagaren. Om det är fara i dröjsmål har åklagare möjlighet att ge tillstånd i avvaktan på rättens beslut. Den nya lagen innebär alltså att det indirekt införs ett nytt ändamål med såväl hemlig övervakning av elektronisk kommunikation som hemlig dataavläsning avseende kommunikationsövervaknings- och platsuppgifter.

Inom ramen för vårt uppdrag har vi inte funnit anledning att ifrågasätta eller vidareutveckla dessa överväganden och förslag, se a. SOU s. 104 ff. och 155 ff. Eftersom förslagen för närvarande är

under beredning finns det inte någon anledning för oss att lämna ett eget förslag i frågan.

7.5 Utökade möjligheter att använda hemlig dataavläsning utanför en förundersökning

7.5.1 Kvalifikationskraven för de permanenta hemliga tvångsmedlen utgör naturliga utgångspunkter

Bedömning: Vid hemlig dataavläsning utanför en förundersökning i syfte att hämta in uppgifter enligt 2 § första stycket 1–4 lagen om hemlig dataavläsning bör kvalifikationskraven som utgångspunkt även fortsättningsvis huvudsakligen motsvara vad som gäller för de bakomliggande tvångsmedlen. Vid hemlig dataavläsning utanför en förundersökning för att hämta in uppgifter enligt nu föreslagna 2 § första stycket 6 lagen om hemlig dataavläsning bör kvalifikationskraven som utgångspunkt även fortsättningsvis motsvara vad som gäller för hemlig avlyssning av elektronisk kommunikation.

Skälen för vår bedömning

Den grundläggande systematiken

Hemlig dataavläsning får, förutom i en förundersökning, användas utanför en förundersökning i underrättelseverksamhet och vid särskild utlänningskontroll. Kvalifikationskraven som avgränsar tillämpningsområdet varierar beroende på vilken uppgiftstyp som avses. Kraven för hemlig dataavläsning utanför en förundersökning är ännu närmre knutna till tillämpningsområdet för de bakomliggande tvångsmedlen än vad bestämmelserna om hemlig dataavläsning under en förundersökning är. Detta beror på att bestämmelserna om hemlig dataavläsning utanför en förundersökning i stor utsträckning hänvisar vidare till bestämmelser i preventivlagen, lagen om särskild kontroll av vissa utlänningar, terroristbrottslagen och inhämtningslagen. Det innebär i sin tur att lagändringar som sker i hänvisade lagrum direkt påverkar tillämpningsområdet för hemlig dataavläsning utanför en förundersökning. Som exempel på en ny lagändring som har på-

verkat tillämpningsområdet för hemlig dataavläsning i bl.a. preventivlagsfallen kan nämnas den utvidgade spioneribestämmelsen som trädde i kraft den 1 januari 2023 (se *Utlandsspionerі*, prop. 2021/22:55).

Syftet med de olika kvalifikationskraven är att balansera de olika risker för den personliga integriteten som användningen av hemlig dataavläsning utanför en förundersökning kan innebära. Vid hemlig dataavläsning i syfte att hämta in uppgifter enligt 2 § första stycket 1–4 lagen om hemlig dataavläsning gäller som utgångspunkt och i huvudsak motsvarande krav som gäller för de bakomliggande tvångsmedlen. Eftersom hemlig rumsavlyssning i dag inte är tillåtet utanför förundersökning, är det inte heller tillåtet med hemlig dataavläsning avseende rumsavlyssningsuppgifter. Vi återkommer i avsnitt 7.5.3 och 7.5.4 till frågan om det bör införas en sådan möjlighet. Vid hemlig dataavläsning i underrättelseverksamhet och vid särskild utlänningskontroll som avser inhämtning av uppgifter enligt nuvarande 2 § första stycket 6 och 7 lagen om hemlig dataavläsning gäller motsvarande krav som gäller för hemlig avlyssning av elektronisk kommunikation. Utformningen av de olika kvalifikationskraven på detta sätt har i förarbetena motiveras genom utförliga analyser (jfr prop. 2019/ 20:64 s. 126 ff.).

Våra utgångspunkter och hur vi förhåller oss till aktuella lagändringar och lagförslag

Vi delar tidigare bedömningar om att utformningarna av de olika kvalifikationskraven för hemlig dataavläsning utanför en förundersökning är ändamålsenligt och proportionerligt avgränsade. Någon ändring i denna systematik föreslås alltså inte. Det är således även vår uppfattning att kvalifikationskraven för hemlig dataavläsning utanför en förundersökning som utgångspunkt bör korrespondera med de bakomliggande tvångsmedlen. Detta är vår utgångspunkt även med beaktande av att tillämpningsområdena för dessa hemliga tvångsmedel nyligen har utökats och föreslås utökas ytterligare.

Utredningen om utökade möjligheter att använda preventiva tvångsmedel hade i uppdrag att se över delar av regleringen om preventiva tvångsmedel. I utredningens betänkanden, *Utökade möjligheter att använda preventiva tvångsmedel 1–2* (SOU 2022:52 och 2023:60), föreslog utredningen flera författningsändringar som innebär utökade möjligheter att använda preventiva tvångsmedel. I konsekvens härmed föreslog utredningen att tillämpningsområdet för hemlig data-

avläsning i underrättelseverksamhet skulle utökas i motsvarande mån. Utredningens lagförslag i SOU 2022:52 godtogs i huvudsak i det fortsatta lagstiftningsarbetet och trädde i kraft den 1 oktober 2023, se prop. 2022/23:126. Lagförslagen i SOU 2023:60 är för närvarande under beredning.

Vidare föreslog Utredningen om utökade möjligheter att använda hemliga tvångsmedel i sitt slutbetänkande utökade möjligheter att använda hemlig övervakning av elektronisk kommunikation vid särskild utlänningskontroll. I konsekvens härmed föreslog utredningen att tillämpningsområdet för hemlig dataavläsning vid särskild utlänningskontroll skulle utökas i motsvarande mån, se betänkandet *Bättre möjligheter att verkställa frihetsberövanden* (SOU 2022:50). Dessa lagförslag är för närvarande under beredning.

Redan de systematiska skäl som framhålls i förarbetena talar starkt för att tillämpningsområdet för hemlig dataavläsning utanför en förundersökning ska utökas i motsvarande mån som tillämpningsområdet för de bakomliggande tvångsmedlen. I betänkandena som ligger till grund för lagförslagen presenteras ingående analyser av behov, förväntad effektivitet och nytta samt noggranna intresseavvägningar. Dessa har i sin tur godtagits i det fortsatta lagstiftningsarbetet. Inom ramen för vårt uppdrag har vi inte funnit anledning att ifrågasätta eller vidareutveckla dessa tidigare analyser och intresseavvägningar. Med dessa utgångspunkter bedömer vi de aktuella lagändringarna och lagförslagen om ett utökat tillämpningsområde för hemlig dataavläsning utanför en förundersökning som både ändamålsenliga och proportionerliga. I det följande redogör vi därför endast helt kort för aktuella lagändringar och lagförslag och stannar i huvudsak vid att hänvisa till dessa.

7.5.2 Nya möjligheter att använda hemlig dataavläsning i preventivlagsfallen för att förhindra allvarlig brottslighet som förekommer inom kriminella nätverk

Bakgrund

Utredningen om utökade möjligheter att använda preventiva tvångsmedel hade bl.a. i uppdrag att överväga i vilken utsträckning det ska införas utökade möjligheter att använda preventiva tvångsmedel för att förhindra allvarlig brottslighet som förekommer inom ramen för

kriminella nätverk. Bakgrunden till uppdraget var det våld i form av skjutningar och sprängningar som har ökat tydligt i Sverige de senaste åren. Antalet skjutningar med dödlig utgång har enligt statistik från Brå ökat sedan 2010-talet. Denna brottslighet har i sin tur stark koppling till kriminella nätverk. En faktor som försvårar utredningar av sådan brottslighet är att de brottsbekämpande myndigheterna ofta har betydande svårigheter att få information om brotten, inte bara från personer i kriminella nätverk utan också från boende i de utsatta områden där skjutningar ofta äger rum. Möjligheten att använda hemliga tvångsmedel i underrättelseskedet anses därför helt central för att kunna bekämpa de kriminella miljöerna (se dir. 2021:102). Utredningens överväganden och förslag framgår av betänkandet *Utökade möjligheter att använda preventiva tvångsmedel* (SOU 2022:52).

Nya möjligheter att förhindra allvarlig brottslighet inom kriminella nätverk

Den 1 oktober 2023 infördes utökade möjligheter att använda preventiva tvångsmedel för att förhindra allvarlig brottslighet som förekommer inom ramen för kriminella nätverk. Lagändringarna innebär i korthet följande. Det utökade tillämpningsområdet har samma kvalifikationskrav och ändamål som preventivlagen. Tvångsmedelsanvändningen syftar till att förhindra viss brottslig verksamhet som utövas inom en organisation eller en grupp. Det utökade tillämpningsområdet innefattar brotten:

- mord, människorov, allmänfarlig ödeläggelse eller grov allmänfarlig ödeläggelse,
- grovt narkotikabrott eller synnerligen grovt narkotikabrott,
- grovt vapenbrott eller synnerligen grovt vapenbrott,
- grov narkotikasmuggling, synnerligen grov narkotikasmuggling, grov vapensmuggling, synnerligen grov vapensmuggling, grov smuggling av explosiv vara eller synnerligen grov smuggling av explosiv vara, och
- grovt brott eller synnerligen grovt brott enligt lagen om brandfarliga och explosiva varor.

Lagändringarna infördes i preventivlagen, huvudsakligen i en ny 1 a §, och tidsbegränsades till fem år efter införandet. I konsekvens härmed utökades även tillämpningsområdet för hemlig dataavläsning i preventivlagsfallen på motsvarande sätt, se 7 § första stycket 2, 15 § andra och tredje styckena samt 18 § andra stycket lagen om hemlig dataavläsning. Samtidigt koncentrerades tillståndsprövningen inom det utvidgade tillämpningsområdet till vissa tingsrätter, se 6 § andra stycket preventivlagen. Det innebär att utredningens analyser och intresseavvägningar huvudsakligen godtogs i det fortsatta lagstiftningsarbetet. Vi gör ingen annan bedömning utan hänvisar till dessa ställningstaganden, se prop. 2022/23:126 s. 66 och 243.

Det kan noteras att 7 § lagen om hemlig dataavläsning sedan den 1 oktober 2023 innehåller en hänvisning till den nya bestämmelsen i 1 a § preventivlagen, vilken alltså är tidsbegränsad och upphävs den 1 oktober 2028. Någon motsvarande ändring sker inte avseende lagen om hemlig dataavläsning. Detta innebär att om ingen ändring genomförs före den 1 oktober 2028 kommer 7 § lagen om hemlig dataavläsning att innehålla en hänvisning till den upphävda 1 a § preventivlagen. Vid införandet av den nya 1 a § preventivlagen och den nya hänvisningen i 7 § lagen om hemlig dataavläsning pekade regeringen på behovet av en utvärdering av reglerna inför ett ställningstagande till om de ska permanentas, se prop. 2022/23:126 s. 84 och 85. Vid en sådan utvärdering kan det förväntas att ett ställningstagande också görs i fråga om hänvisningen i 7 § lagen om hemlig dataavläsning. Vi föreslår därför inte någon särskild lagändring för att återställa hänvisningen i 7 § lagen om hemlig dataavläsning den 1 oktober 2028.

7.5.3 Förslaget om att hemlig dataavläsning avseende rumsavlyssningsuppgifter ska kunna användas i preventivlagsfallen

Utredningen om preventiva tvångsmedel har bl.a. haft i uppdrag att ta ställning till om hemlig rumsavlyssning och hemlig dataavläsning avseende rumsavlyssningsuppgifter bör kunna användas för att förhindra allvarlig brottslighet (se dir. 2022:104).

I SOU 2023:60 föreslår utredningen att det ska införas en möjlighet att använda hemlig rumsavlyssning i preventivt syfte. I konsekvens härmed föreslår utredningen att tillämpningsområdet för hemlig data-

avläsning i preventivlagsfallen utökas i motsvarande mån. Betänkandet bereds för närvarande i Regeringskansliet.

Inom ramen för vårt uppdrag har vi inte funnit anledning att ifrågasätta eller vidareutveckla dessa överväganden och förslag. Eftersom förslagen för närvarande är under beredning finns det inte någon anledning för oss att lämna ett eget förslag i frågan.

7.5.4 Förslaget om att hemlig dataavläsning avseende kameraövervaknings- och rumsavlyssningsuppgifter ska kunna knytas till en person i preventivlagsfallen

Utredningen om preventiva tvångsmedel har bl.a. haft i uppdrag att ta ställning till om tillstånd till hemlig kameraövervakning och hemlig dataavläsning avseende kameraövervakningsuppgifter utanför en förundersökning bör kunna knytas till en person. Eftersom utredningen lämnade förslag om att hemlig rumsavlyssning och hemlig dataavläsning avseende rumsavlyssningsuppgifter bör få användas för att förhindra allvarlig brottslighet, omfattade uppdraget även att ta ställning till om sådana tillstånd bör kunna knytas till en person (se dir 2022:104).

I SOU 2023:60 föreslår utredningen att det ska införas en möjlighet att knyta ett tillstånd till hemlig kameraövervakning, hemlig rumsavlyssning och hemlig dataavläsning som gäller kameraövervakningseller rumsavlyssningsuppgifter i preventivt syfte till den person som åtgärden riktas mot i stället för till en viss plats, om det finns särskilda skäl för det. Betänkandet bereds för närvarande i Regeringskansliet.

Inom ramen för vårt uppdrag har vi inte funnit anledning att ifrågasätta eller vidareutveckla dessa överväganden och förslag. Eftersom förslagen för närvarande är under beredning finns det inte någon anledning för oss att lämna ett eget förslag i frågan.

7.5.5 Förslaget om att hemlig dataavläsning ska kunna användas vid särskild utlänningskontroll för att lokalisera vissa utlänningar

Bakgrund

I lagen (2022:700) om särskild kontroll av vissa utlänningar finns en bestämmelse om användning av hemlig övervakning av elektronisk kommunikation i syfte att lokalisera en utlänning som inte fullgör sin anmälningsskyldighet enligt lagen. Tidigare var denna möjlighet begränsad till uppgifter om var en elektronisk kommunikationsutrustning finns eller har funnits. Några närmare överväganden beträffande denna begränsning framgår inte av förarbetena. Någon möjlighet att använda hemlig dataavläsning i syfte att lokalisera utlänningar som inte fullgjort sin anmälningsskyldighet finns inte. I förarbetena redovisas inte heller några överväganden om hemlig dataavläsning i syfte att lokalisera utlänningar som inte fullgjort sin anmälningsskyldighet. Utredningen om utökade möjligheter att använda hemliga tvångsmedel har redogjort för sina överväganden och förslag på området i betänkandet *Bättre möjligheter att verkställa frihetsberövanden* (SOU 2022:50). Betänkandet bereds för närvarande i Regeringskansliet.

Förslaget om en ny bestämmelse vid särskild utlänningskontroll i syfte att lokalisera vissa utlänningar

I SOU 2022:50 s. 126 f. och 168 föreslås att möjligheten använda hemlig övervakning av elektronisk kommunikation i syfte att lokalisera en utlänning som inte fullgör sin anmälningsskyldighet ska utökas till att omfatta alla slags uppgifter som kan omfattas av hemlig övervakning av elektronisk kommunikation. I konsekvens härmed föreslås att det ska införas en motsvarande möjlighet att använda hemlig dataavläsning avseende kommunikationsövervaknings- och platsuppgifter, se 9 § lagen om hemlig dataavläsning.

Inom ramen för vårt uppdrag har vi inte funnit anledning att ifrågasätta eller vidareutveckla dessa överväganden och förslag. Eftersom förslagen för närvarande är under beredning finns det inte någon anledning för oss att lämna ett eget förslag i frågan.

7.5.6 Förslaget om utökade möjligheter att använda hemlig dataavläsning i inhämtningslagsfallen

Bakgrund

Inhämtningslagen har de senaste åren använts i ökande omfattning som verktyg i Polismyndighetens underrättelseverksamhet. Åtgärder enligt inhämtningslagen har också återkommande konstaterats fylla en viktig funktion samt innebära en reell nytta i det brottsbekämpande arbetet (se t.ex. *Redovisning av användningen av hemliga tvångsmedel under 2021*, reg. skr. 2022/23:30). Trots detta har möjligheten till hemlig dataavläsning i inhämtningslagsfallen endast utnyttjats i några enstaka fall (se avsnitt 6.3.5). Detta kan bero på vilka ärenden som har prioriterats, men också att bestämmelsen i 10 § lagen om hemlig dataavläsning är svårtillämpad. Som vi har redogjort för i avsnitt 6.2.5 och 7.3.2 kan det vara förenat med svårigheter att särskilja de olika uppgiftstyperna. I inhämtningslagsfallen är det endast tillåtet att hämta in kommunikationsövervakningsuppgifter avseende förfluten tid eller platsuppgifter. Risken för inhämtning av otillåten tilläggsinformation kan därför vara ett skäl till att bestämmelsen inte har tillämpats mer frekvent. Sådana tekniska begränsningar utgör dock inte i sig skäl att utöka tillämpningsområdet för hemlig dataavläsning i inhämtningslagsfallen. Det finns inte heller något som tyder på att den tekniska utvecklingen kommer att avstanna och att nya metoder kan utvecklas för att kunna använda 10 § mer effektivt.

Förslaget om utökade möjligheter att använda hemlig dataavläsning i inhämtningslagsfallen

Utredningen om preventiva tvångsmedel har bl.a. haft i uppdrag att ställning till om, och i så fall på vilket sätt, tillämpningsområdet för inhämtningslagen bör utvidgas (se dir. 2022:32).

I SOU 2023:60 föreslår utredningen ett utvidgat tillämpningsområde för inhämtningslagen genom en utökad brottskatalog. Utredningen föreslår också att uppgifter om meddelanden ska få hämtas in i realtid. I konsekvens härmed föreslår utredningen att tillämpningsområdet för hemlig dataavläsning i inhämtningslagsfallen utökas i motsvarande mån. Betänkandet bereds för närvarande i Regeringskansliet.

Inom ramen för vårt uppdrag har vi inte funnit anledning att ifrågasätta eller vidareutveckla dessa överväganden och förslag. Eftersom förslagen för närvarande är under beredning finns det inte någon anledning för oss att lämna ett eget förslag i frågan.

7.6 Det utökade tillämpningsområdet för hemlig dataavläsning är proportionerligt avgränsat

Bedömning: Hela det utökade och tilltänkta tillämpningsområdet för hemlig dataavläsning är ändamålsenligt och proportionerligt avgränsat, under förutsättning att bestämmelserna balanseras med kontrollmekanismer och andra rättssäkerhetsgarantier för att minimera riskerna för den personliga integriteten och informationssäkerheten.

Skälen för vår bedömning

Vi delar tidigare bedömningar om att tillämpningsområdet för hemlig dataavläsning vid tidpunkten för lagens ikraftträdande, utifrån de förutsättningar som då rådde, var ändamålsenligt och proportionerligt avgränsat. Lagstiftningen om hemlig dataavläsning och andra hemliga tvångsmedel är emellertid under utveckling. Flera lagändringar som påverkar tillämpningsområdet för hemlig dataavläsning har helt nyligen trätt i kraft och andra förslag kan förväntas träda i kraft inom kort. Härutöver föreslår vi i detta betänkande ytterligare förtydliganden och utökningar av tillämpningsområdet. I de analyser som vi i kapitel 6 har gjort av den hittillsvarande tillämpningen av hemlig dataavläsning har det inte varit möjligt att beakta alla dessa utökningar. Det är därför nödvändigt att avslutningsvis göra en samlad proportionalitetsbedömning av hela det utökade och tilltänkta tillämpningsområdet för hemlig dataavläsning. I kapitel 12 återkommer vi till en särskild analys av vad våra förslag i detta betänkande får för konsekvenser bl.a. för enskilda.

När det gäller behovet av ett utökat tillämpningsområde ska åter framhållas att det är av väsentlig betydelse att hemlig dataavläsning kan användas i motsvarande fall som andra hemliga tvångsmedel och även vissa öppna tvångsmedel. De slutsatser som vi har dragit om

nyttan och effektiviteten av hemlig dataavläsning kan redan mot denna bakgrund förväntas gälla även för det utökade tillämpningsområdet. Det kan också åter konstateras att det saknas mindre ingripande alternativ till hemlig dataavläsning för att få samma effekt och nytta. En förutsättning för att få tillämpa hemlig dataavläsning är att andra tvångsmedel inte är framkomliga alternativ. De brottsbekämpande myndigheternas behov av mer effektiva verktyg är påtagligt. Vi anser därför att alla införda och föreslagna utökningar av tillämpningsområdet som vi har redogjort för i detta kapitel är nödvändiga med hänsyn till intresset av att bekämpa den allvarliga brottsligheten och att skydda medborgarna, några av samhällets mest grundläggande funktioner.

Det utökade tillämpningsområdet för hemlig dataavläsning innebär sammanfattningsvis vissa ökade integritetsrisker för enskilda. Det innebär en risk för att mer information, som för den enskilde kan vara av känslig art, kommer till de brottsbekämpande myndigheternas kännedom. Det utökade tillämpningsområdet innebär också att hemlig dataavläsning kan komma att användas i fler fall och för lindrigare brott än i dag, förutsatt att den samlade brottsligheten är av allvarligt slag. Ett utökat tillämpningsområde innebär alltså att fler personer kan komma att bli föremål för hemlig dataavläsning. Det innebär också att fler misstänkta personer kan avskrivas i ett tidigare skede och att man kan undvika att dessa personer utsätts för hemliga tvångsmedel i onödan. Information som kan hämtas in i ett tidigt skede bedöms generellt sett även kunna leda till förkortade utredningstider och förkortade häktningstider. Våra förslag i avsnitt 7.4.4 avseende illustrerar detta på ett tydligt sätt. Motsvarande information som kan hämtas in med stöd av våra förslag kan hämtas in redan i dag, fast med stöd av öppna tvångsmedel i ett senare skede i utredningen och då med den risken att för utredningen avgörande information redan gått förlorad.

Kvalifikationskraven för hemlig dataavläsning överensstämmer, även med beaktande av det utökade tillämpningsområdet, huvudsakligen med bakomliggande tvångsmedel. Vi kan därför utgå från att de personer som riskerar att beröras av hemlig dataavläsning huvudsakligen är samma personer som riskerar att bli föremål för andra hemliga tvångsmedel. Det utökade tillämpningsområdet innebär härutöver en viss ökad risk för att personer som senare visar sig vara ovidkommande utsätts för hemlig dataavläsning. Tredje man riskerar att utsättas för integritetsintrång genom att exempelvis kommuni-

cera med eller befinna sig i närheten av en person som är föremål för hemlig dataavläsning. Hur många ovidkommande personer som berörs av det utökade tillämpningsområdet är svårt att uppskatta. I samband med en tidigare utvärdering av hemlig tvångsmedelslagstiftning gjordes en omfattande kartläggning och analys av tillämpningen av vissa hemliga tvångsmedel. Sammanfattningsvis konstaterades då att det inte med någon exakthet gick att mäta i vilken utsträckning tredje man hade avlyssnats eller övervakats genom de undersökta tvångsmedlen. Samtidigt framhölls att ett visst integritetsintrång för tredje man inte går att undvika vid något hemligt tvångsmedel (se *Hemliga tvångsmedel mot allvarliga brott*, SOU 2012:44, s. 517 f.). Det ska i sammanhanget också framhållas att de utökningar och förtydliganden av lagstiftningen som har skett och som nu föreslås sker med beaktande av utvecklingen av de tekniska verktyg som finns tillgängliga för brottsbekämpande myndigheter. Den utvecklingen innebär i sin tur allt större möjligheter att använda hemlig dataavläsning på ett sådant sätt att integritetsintrånget för utomstående minimeras. Lagen om hemlig dataavläsning ställer också uttryckliga krav på teknikanpassning och integritetsbegränsande villkor i varje enskilt fall, se 23 § och 18 § första stycket 4 lagen om hemlig dataavläsning. I de avseenden som tillämpningsområdet förtydligas innebär detta en förstärkt rättssäkerhet och ett starkare skydd för enskildas personliga integritet. Det utökade tillämpningsområdet innebär också bättre möjligheter för de brottsbekämpande myndigheterna att förebygga, förhindra, upptäcka och utreda allvarlig brottslighet. Det kan alltså antas att våra förslag kommer att leda till att fler brott mot enskilda både kommer att förhindras och lagföras. I dessa avseenden innebär det utökade tillämpningsområdet en ökad rättstrygghet och ett förstärkt skydd för enskildas personliga integritet. Vid en samlad bedömning finner vi att den ökade risk för den personliga integriteten som det utökade tillämpningsområdet kan innebära är försvarlig.

Vår slutsats är därmed att hela det utökade och tilltänkta tillämpningsområdet för hemlig dataavläsning är både ändamålsenligt och proportionerligt avgränsat. Vår bedömning gäller även med beaktande av att preventiv tvångsmedelsanvändning i sig kan anses medföra en ökad integritetsrisk. Våra slutsatser förutsätter att bestämmelserna balanseras med kontrollmekanismer och andra rättssäkerhetsgarantier för att minimera riskerna för den personliga integriteten och informationssäkerheten. Dessa frågeställningar behandlas i nästa kapitel.

8 Kontrollmekanismerna och andra rättssäkerhetsgarantier

8.1 Uppdraget

Hemlig dataavläsning innebär inskränkningar i rättigheter som skyddas av bl.a. regeringsformen, Europakonventionen och EU-rätten. Bestämmelserna om hemlig dataavläsning motiveras av intresset av att bekämpa allvarlig brottslighet, vilket är ett godtagbart ändamål för sådana inskränkningar (se avsnitt 5.4). Vi har i de två senaste kapitlen konstaterat att det finns ett angeläget samhälleligt behov av hemlig dataavläsning och att de ingrepp i den personliga integriteten som åtgärden medför är såväl nödvändiga som proportionerliga i förhållande till ändamålet med hemlig dataavläsning. I detta kapitel övergår vi till den del av uppdraget som innebär att vi ska analysera om lagstiftningens kontrollmekanismer och andra rättssäkerhetsgarantier är tillräckliga. Våra slutsatser och förslag i kapitel 6 och 7 bygger också på att respekten för grundläggande fri- och rättigheter, liksom kraven på rättssäkerhet, samtidigt kan säkerställas.

Inledningsvis i detta kapitel redogör vi kort för vad som i sammanhanget innefattas i uttrycken kontrollmekanismer och andra rättssäkerhetsgarantier samt för våra utgångspunkter och avgränsningar. Därefter övergår vi till våra analyser och frågan om det finns behov av förändringar i regelverket i några avseenden.

8.2 Rättssäkerhetsgarantier vid hemlig dataavläsning

8.2.1 Den grundläggande strukturen

Lagen om hemlig dataavläsning omgärdas av olika kontrollmekanismer och andra rättssäkerhetsgarantier för att möta de höga krav som bl.a. regeringsformen, Europakonventionen och EU-rätten ställer på lagstiftningen, se avsnitt 5.4 och 5.5.2 med där gjorda hänvisningar. De olika rättssäkerhetsgarantier som gäller för hemlig dataavläsning kan delas in i följande övergripande kategorier.

- precisa lagregler och begränsningar
- tillståndsprövning och annan förhandskontroll
- rättssäkerhetsgarantier vid verkställighet
- informationssäkerhet
- regler om sekretess, tystnadsplikt och partsinsyn
- regler om underrättelse i efterhand till enskilda
- tillsyn och annan efterhandskontroll.

Regleringen om hemlig dataavläsning är utformad med bestämmelserna om de permanenta hemliga tvångsmedlen i rättegångsbalken som förebild. Endast i vissa avseenden avviker lagstiftningens struktur från den som gäller för de bakomliggande tvångsmedlen. Vi återkommer i det följande till var och en av dessa avvikelser. Syftet med dessa har genomgående varit att ytterligare stärka rättssäkerhetsgarantierna för hemlig dataavläsning.

8.2.2 Våra utgångspunkter och avgränsningar

Det saknas anledning att göra förändringar i den grundläggande strukturen för hemlig dataavläsning. De permanenta hemliga tvångsmedlen och de rättssäkerhetsgarantier som gäller för dessa har genom åren varit föremål för flera statliga översyner och utvärderingar. Generellt sett har regelverket i allt väsentligt ansetts fungera väl och dessutom ansetts tillgodose de krav som ställs på lagstiftning om hemliga tvångsmedel (se t.ex. SOU 2012:44 och prop. 2019/20:64 s. 147 ff. med där gjorda hänvisningar). Stora delar av regelverket har senast

setts över av Utredningen om rättssäkerhetsgarantier vid användningen av vissa hemliga tvångsmedel, i slutbetänkandet *Rättssäkerhetsgarantier och hemliga tvångsmedel*, SOU 2018:61. Utredningen fann i sin översyn att de rättssäkerhetsgarantier som gäller för de permanenta hemliga tvångsmedlen i allt väsentligt överensstämmer med de krav som ställs på lagstiftning om hemliga tvångsmedel. Bestämmelserna om hur överskottsinformation får användas bedömdes dock icke förenliga med kraven i Europakonventionen. Utredningen föreslog därför vissa lagändringar i rättegångsbalken och preventivlagen i detta avseende. Utredningen föreslog även vissa lagändringar beträffande hanteringen av det inhämtade materialet. Utredningens analyser och förslag godtogs med vissa lagtekniska justeringar i det fortsatta lagstiftningsarbetet. Lagändringar i dessa avseenden trädde i kraft den 1 oktober 2023, se *Hemliga tvångsmedel – effektiva verktyg för att förhindra och utreda allvarliga brott*, prop. 2022/23:126. Med hänsyn till det strukturella sambandet mellan regelverken gör utredningens slutsatser och förslag sig gällande även beträffande hemlig dataavläsning.

I de delar där lagstiftningen om hemlig dataavläsning överensstämmer med beprövade regler som återkommande har bedömts uppfylla de höga krav som ställs på lagstiftningen har vi inte funnit anledning att göra några förnyade analyser. I dessa avseenden hänvisar vi därför till de ställningstaganden som gjordes i SOU 2018:61. När det gäller sådana rättssäkerhetsgarantier som är specifika för hemlig dataavläsning måste vi dock göra förnyade bedömningar i frågan om dessa är tillräckliga. Detsamma gäller när det i övrigt kan finnas anledning att höja rättssäkerhetskraven för hemlig dataavläsning i förhållande till bakomliggande tvångsmedel.

Flera av de materiella bestämmelserna i lagen om hemlig dataavläsning har helt nyligen setts över av andra utredningar. Nya och reviderade bestämmelser i lagen om hemlig dataavläsning har därför nyligen trätt i kraft eller kan förväntas träda i kraft inom kort. Härutöver föreslår vi i detta betänkande ytterligare förändringar i regelverket. Den omständigheten att rättsområdet är under utveckling försvårar självklart analysen av kontrollmekanismerna och de andra rättssäkerhetsgarantierna för hemlig dataavläsning. Det är likväl viktigt att våra analyser baseras på en helhetsbedömning. Våra analyser sker därför med beaktande både av den utvidgning av tillämpningsområdet som nyligen har trätt i kraft och de lagförslag vi själva lägger alternativt ställer oss bakom i detta betänkande. Om inget annat sär-

skilt framgår omfattar våra analyser bestämmelserna om hemlig dataavläsning såväl under som utanför en förundersökning.

8.3 Lagstiftningen om hemlig dataavläsning är tillräckligt förutsebar, tydlig och avgränsad

Bedömning: Bestämmelserna om hemlig dataavläsning uppfyller de krav på förutsebarhet, tydlighet och avgränsning som ställs på lagstiftningen. Den hittillsvarande tillämpningen visar att det trots detta kan finnas skäl att öka förutsebarheten och tydligheten i vissa av bestämmelserna, i syfte att ytterligare stärka rättssäkerheten.

Skälen för vår bedömning

För att användningen av hemlig dataavläsning ska vara rättssäker krävs att lagstiftningen är förutsebar och tydlig samt att det finns tillräckliga begränsningar till skydd för den personliga integriteten.

När det gäller regelverkets struktur har såväl bestämmelserna om hemlig dataavläsning som bakomliggande tvångsmedel i 27 kap. rättegångsbalken kritiserats för att vara svåröverskådliga. Bestämmelserna innehåller ofta hänvisningar i flera led vilket försvårar tillämpningen. Däremot förefaller det vara få bestämmelser som i sig själva ger upphov till tolkningssvårigheter eller tillämpningsproblem. Själva strukturen i det nuvarande regelverket om hemlig dataavläsning bedöms därför inte strida mot kraven i regeringsformen och Europakonventionen (jfr SOU 2018:61 s. 116 f.). På sikt vore det emellertid önskvärt med en större redaktionell översyn av reglerna om tvångsmedelsanvändning. Vi återkommer i kapitel 9 till våra överväganden i frågan om hur bestämmelserna om hemlig dataavläsning bäst struktureras och placeras för att uppfylla de krav som ställs på lagstiftningen.

När det gäller de materiella bestämmelserna har vi i kapitel 7 redogjort för de utökningar av tillämpningsområdet för hemlig dataavläsning som nu föreslås, alternativt helt nyligen har trätt i kraft eller kan förväntas träda i kraft inom kort. Mot bakgrund av våra överväganden med där gjorda hänvisningar bedömer vi sammantaget att tillämpningsområdet för hemlig dataavläsning är avgränsat på ett sätt som uppfyller de krav som följer av regeringsformen, Europakonven-

tionen och EU-rätten. Det sagda gäller såväl i fråga om vilken brottslighet som den personkrets som hemlig dataavläsning kan användas mot. Såvitt kan bedömas framstår nyligen ikraftträdda och nu föreslagna bestämmelser som tillräckligt begränsade och tydliga för att det ska vara förutsebart under vilka omständigheter som hemlig dataavläsning kan komma att användas. Vi har utifrån den hittillsvarande tillämpningen identifierat ett fåtal bestämmelser i lagen om hemlig dataavläsning som har gett upphov till vissa tolkningssvårigheter eller tillämpningsproblem. Även Säkerhets- och integritetsskyddsnämndens (SIN) granskningar av användningen av hemlig dataavläsning har väckt vissa frågor angående hur lagen har följts och hur den ska tillämpas. Otydligheterna som har framkommit bedöms inte vara av sådan art att nuvarande lagstiftning står i strid med skyddet för de grundläggande fri- och rättigheterna. Iakttagelserna ger ändå skäl att öka tydligheten och förutsebarheten i lagstiftningen i ett antal avseenden. En tydligare lagstiftning ger bättre förutsättningar för en omsorgsfull domstolsprövning, vilket i sin tur innebär ett starkare skydd för rättssäkerheten. Frågor om innebörden av hemlig dataavläsning samt gränsdragningssvårigheter mellan de olika uppgiftstyperna och differentieringskravet har vi redan behandlat i avsnitt 7.2 och 7.3. I avsnitten 8.4.3–8.4.7 nedan presenterar vi våra överväganden angående tillståndets innehåll och i avsnitten 8.5.2–8.5.6 redovisar vi våra överväganden avseende bestämmelser om överskottsinformation och andra frågor om hantering av det inhämtade materialet. I kapitel 10 behandlar vi frågor som har anknytning till jurisdiktion och territorialitet. I övrigt har vi inte funnit anledning att anmärka på förutsebarheten, tydligheten eller begränsningarna i de materiella bestämmelserna.

8.4 Tillståndsprövningen och annan förhandskontroll

8.4.1 Domstolsprövningen m.m.

Bedömning: Systemet med domstolsprövning för hemlig dataavläsning uppfyller de rättssäkerhetskrav som ställs på lagstiftningen. Systemet med offentliga ombud bidrar till att uppfylla dessa krav.

Skälen för vår bedömning

Ett beslut om hemlig dataavläsning fattas som huvudregel av domstol. Eftersom det i inhämtningslagen inte uppställs något krav på föregående domstolsprövning skiljer sig lagstiftningen beträffande hemlig dataavläsning i detta hänseende från vad som gäller för det bakomliggande tvångsmedlet. Att på detta sätt höja rättssäkerhetskraven för hemlig dataavläsning i inhämtningslagsfallen har i förarbetena motiverats på följande sätt (se prop. 2019/20:64 s. 148).

> Vid bedömningen av vilken myndighet som bör anförtros beslutsbehörigheten vid hemlig dataavläsning bör vägas in att hemlig dataavläsning skiljer sig från inhämtning enligt inhämtningslagen på så sätt att hemlig dataavläsning, i vart fall vid verkställigheten, är ett mer ingripande tvångsmedel. Även om syftet med tvångsmedlen är detsamma kan hemlig dataavläsning dessutom ge mer exakta uppgifter om lokalisering än uppgifter enligt inhämtningslagen. Detta talar enligt regeringen för att domstolar är mer lämpade att fatta besluten. Dessutom framstår det som olämpligt att ha olika beslutsmyndigheter för ett och samma tvångsmedel.

Vi delar denna bedömning. Systemet med domstolsprövning överensstämmer med de krav på en oberoende förhandskontroll som ställs vid användning av hemliga tvångsåtgärder. Även det system med offentliga ombud som gäller för hemlig dataavläsning har bedömts bidra till att uppfylla kraven avseende en oberoende förhandskontroll (se SOU 2018:61 s. 134 ff. och 153 ff.).

Kravet på sammanträde och offentligt ombud vid domstolsprövningen är ovillkorligt. Det förenklade förfarande som enligt 27 kap. 28 a § rättegångsbalken gäller vid prövning av vissa frågor om hemlig avlyssning av elektronisk kommunikation är inte tillämpligt vid prövning av frågor om hemlig dataavläsning. Bestämmelsen om ett förenklat förfarande infördes den 1 augusti 2020 och innebär i korthet en möjlighet till undantag i vissa fall från huvudregeln att sammanträde ska hållas. Om det redan finns ett tillstånd till hemlig avlyssning av elektronisk kommunikation och en ny ansökan eller anmälan gäller samma person och grundas på samma omständigheter som det tidigare tillståndet, men avser ett annat telefonnummer, en annan adress eller en annan elektronisk kommunikationsutrustning än det tidigare tillståndet får rätten pröva frågan utan att utse ett offentligt ombud och utan att hålla sammanträde, om ett sådant skulle vara utan betydelse. När rätten har prövat frågan ska ett offentligt ombud utses skyndsamt och underrättas om rättens beslut. Det förenklade för-

farandet syftar till att möta problematiken med kriminella, framför allt inom den organiserade brottsligheten, som systematiskt byter eller använder sig av flera sim-kort och kommunikationsutrustningar. I förarbetena övervägdes inte möjligheten att införa ett motsvarande undantag för hemlig dataavläsning (jfr SOU 2018:30). Metoden för hemlig dataavläsning skiljer sig från bakomliggande tvångsmedel och åtgärden innebär generellt ett större integritetsintrång. Vi bedömer redan mot denna bakgrund att det inte är lämpligt att införa ett motsvarande förenklat förfarande för hemlig dataavläsning. Kravet på sammanträde och offentligt ombud vid domstolsprövningen av frågor om hemlig dataavläsning ska därför fortsatt vara ovillkorligt.

Det är självklart nödvändigt att prövningen även i praktiken lever upp till de krav som ställs. Den hittillsvarande tillämpningen visar att antalet avslagsbeslut från domstol avseende tillstånd till hemlig dataavläsning, i likhet med vad som gäller för övriga hemliga tvångsmedel, är få (se tabell 6.7 i kapitel 6). Redan den omständigheten att hemlig dataavläsning är ett mycket resurskrävande tvångsmedel ställer krav på att en ansökan om åtgärden måste vara välgrundad. Statistiken innebär dock inte att domstolar rutinmässigt har godtagit ansökningar om hemlig dataavläsning. Inför varje beslut om hemlig dataavläsning finns ett ovillkorligt krav på att rätten utser ett offentligt ombud och håller ett sammanträde i ärendet. Under sammanträdet kan det offentliga ombudet eller domaren väcka frågor om t.ex. ansökans omfattning, huruvida det finns möjlighet till mindre ingripande åtgärder eller om misstankegraden tillräckligt hög. Enligt uppgifter från utredningens experter förekommer det också att domstolen därefter begränsar tillståndet eller förenar det med ytterligare villkor. Det förekommer också att åklagaren vid sammanträdet justerar eller återkallar sin ansökan, något som inte speglas i statistiken. Dessa omständigheter kan sammantaget anses tala för att hemlig dataavläsning har använts med urskiljning och omsorg. Eftersom besluten är relativt få till antalet är det svårt att dra några mer långtgående slutsatser. Som framgår av kapitel 6 förekommer också att enskilda ärenden får stort genomslag i statistiken.

SIN har i sina granskningar av användningen av hemlig dataavläsning framfört vissa anmärkningar mot tillståndsprövningen när det gäller tillståndens varaktighet och innehåll. Vi återkommer i avsnitten 8.4.3–8.4.6 till våra överväganden i dessa avseenden. Själva systemet med en obligatorisk domstolsprövning bedöms dock uppfylla

de rättssäkerhetskrav som ställs på lagstiftningen. Det obligatoriska kravet på offentliga ombud bedöms i sin tur bidra till att uppfylla dessa krav.

8.4.2 Systemet med interimistiska beslut

Bedömning: Systemet med interimistiska beslut för hemlig dataavläsning, i kombination med en obligatorisk domstolsprövning, uppfyller de rättssäkerhetskrav som ställs på lagstiftningen.

Skälen för vår bedömning

I undantagsfall har åklagare möjlighet att i avvaktan på rättens beslut fatta ett interimistiskt beslut om hemlig dataavläsning, se 17 § lagen om hemlig dataavläsning. Bestämmelsen innefattar en möjlighet att fatta interimistiskt beslut om ett tillträdestillstånd för eventuell installation av hårdvara eller annan teknisk utrustning. Förutsättningarna för ett interimistiskt åklagarbeslut vid hemlig dataavläsning är i huvudsak desamma som för de permanenta hemliga tvångsmedlen (jfr 27 kap. 21 a § rättegångsbalken och 6 a § preventivlagen). Ett interimistiskt tillstånd till hemlig dataavläsning får inte avse hemlig dataavläsning vid särskild utlänningskontroll. Interimistiska beslut om hemlig dataavläsning är, till skillnad från vid inhämtning enligt inhämtningslagen, tillåtna även i inhämtningslagsfallen. Vi delar tidigare bedömning om att det saknas bärande skäl mot en sådan beslutanderätt. Åtgärden omgärdas av samma höga kvalifikationskrav och starka rättssäkerhetsgarantier som i övrigt uppställs för interimistiska åklagarbeslut om hemliga tvångsmedel. Mot denna bakgrund saknas anledning att tro att möjligheten till interimistiska åklagarbeslut i inhämtningslagsfallen skulle leda till negativa konsekvenser för enskildas rättssäkerhet (jfr prop. 2019/20:64 s. 153 f. och *Hemliga tvångsmedel mot allvarliga brott*, prop. 2013/14 s. 141).

Tidigare fick åklagare fatta interimistiska beslut om hemlig rumsavlyssning och hemlig dataavläsning avseende rumsavlyssningsuppgifter endast under krigstid eller liknande extraordinära omständigheter. Detta framgick av 2 och 28 §§ i den numera upphävda lagen (1988:97) om förfarandet hos kommunerna, förvaltningsmyndig-

heterna och domstolarna under krig eller krigsfara m.m. Den 1 oktober 2023 infördes en möjlighet för åklagare att fatta interimistiska beslut om hemlig rumsavlyssning även i fredstid. Samtidigt infördes därför en motsvarande möjlighet för åklagare att fatta interimistiska beslut om hemlig dataavläsning avseende rumsavlyssningsuppgifter (jfr prop. 2019/20:64 s. 152 ff.). Lagändringarna infördes i 27 kap. 21 a § rättegångsbalken respektive 17 § lagen om hemlig dataavläsning. Även dessa åtgärder omgärdas av samma höga kvalifikationskrav och starka rättssäkerhetsgarantier som i övrigt uppställs för interimistiska åklagarbeslut om hemliga tvångsmedel. I betänkandet *Utökade möjligheter att använda hemliga tvångsmedel*, SOU 2022:19, presenteras ingående analyser av behov, förväntad effektivitet och nytta samt noggranna intresseavvägningar beträffande de aktuella lagändringarna. Utredningens analyser och intresseavvägningar godtogs i det fortsatta lagstiftningsarbetet. Vi gör ingen annan bedömning utan hänvisar till dessa ställningstaganden, se prop. 2022/23:126 s. 162 ff. och 244 f.

Systemet med interimistiska beslut för hemliga tvångsmedel har tidigare ansetts uppfylla de rättssäkerhetskrav som ställs på lagstiftningen (se SOU 2018:61 s. 139 f.). Även den hittillsvarande tillämpningen talar för att möjligheten till interimistiska åklagarbeslut om hemlig dataavläsning har använts med urskiljning och omsorg. Av tabell 6.8 i kapitel 6 framgår att antalet interimistiska beslut om hemlig dataavläsning är få och att domstol inte i något av dessa fall har ändrat beslutet. Detta motsvarar hur möjligheten till interimistiska åklagarbeslut avseende de permanenta hemliga tvångsmedlen används. Av regeringens årliga redovisningar framgår att även dessa beslut är relativt sett få till antalet och att det är ovanligt att beslutet upphävs vid den efterföljande obligatoriska domstolsprövningen. Vi drar mot denna bakgrund slutsatsen att åklagare som fattar interimistiska beslut om hemlig dataavläsning generellt sett har goda kunskaper om förutsättningarna för åtgärden. Möjligheten till interimistiska åklagarbeslut om hemlig dataavläsning har således utnyttjats på ett korrekt sätt.

Möjligheten att meddela interimistiska åklagarbeslut om hemlig dataavläsning avseende rumsavlyssningsuppgifter är ny och omfattas därför inte av statistiken. Motsvarande slutsatser bör dock kunna dras även i detta avseende. Det saknas anledning att tro att risken för felaktiga bedömningar skulle vara högre i detta avseende (jfr SOU 2022:19 s. 364 f.). Systemet med interimistiska beslut för hemlig dataavläsning,

i kombination med en obligatorisk domstolsprövning, får sammantaget anses uppfylla de rättssäkerhetskrav som ställs på lagstiftningen.

8.4.3 Tillståndets innehåll

Bedömning: Kraven i 18 § lagen om hemlig dataavläsning på vad ett tillstånd till hemlig dataavläsning ska innehålla uppfyller de rättssäkerhetskrav som ställs på lagstiftningen. Den hittillsvarande tillämpningen visar att det trots detta kan finnas skäl att öka förutsebarheten och tydligheten i vissa av bestämmelserna, i syfte att ytterligare stärka rättssäkerheten.

Skälen för vår bedömning

Kraven på innehållet i ett tillstånd till hemlig dataavläsning syftar till att tillgodose skyddet för den enskilde. Tillståndet måste vara så tydligt, precist och detaljrikt så att beslutet kan verkställas på ett rättssäkert sätt, samt för att underlätta efterhandskontroll. En viktig utgångspunkt är att åtgärdens omfattning alltid uttryckligen ska framgå av tillståndet (se t.ex. SIN:s uttalande med beslut av den 29 mars 2023, dnr 43-2022). På så sätt kan eventuella konsekvenser för den enskildes personliga integritet följas upp.

Kraven på vad rättens, och i förekommande fall åklagarens, tillstånd till hemlig dataavläsning ska innehålla framgår av 18 § lagen om hemlig dataavläsning. I bestämmelsens första stycke framgår att det i tillståndet ska anges vilken tid tillståndet avser (1 p), vilket avläsningsbart informationssystem tillståndet avser (2 p), vilken eller vilka uppgiftstyper som får läsas av eller tas upp, dvs. hämtas in (3 p), villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan (4 p), och vem som är skäligen misstänkt för brottet eller brotten, vid åtgärd som gäller rumsavlyssningsuppgifter (5 p). Av bestämmelsens andra stycke framgår att om tillståndet avser en plats eller om tillståndet är förenat med ett tillträdestillstånd ska detta anges i tillståndet. I tredje stycket stadgas att om beslutet avser den skäligen misstänkte enligt 4 a § fjärde stycket eller 6 § fjärde stycket ska det anges i beslutet. I fjärde stycket anges att tiden för tillståndet inte får bestämmas längre än nödvändigt. När det gäller tid

som infaller efter beslutet får tiden inte överstiga en månad från dagen för beslutet. Bestämmelsen i 18 § lagen om hemlig dataavläsning är utformad med de tillståndskrav som gäller för de permanenta hemliga tvångsmedlen som förebild, se 27 kap. 21 § rättegångsbalken. Denna bestämmelse har tidigare funnits väl förenlig med de rättssäkerhetskrav som ställs på lagstiftningen beträffande innehållet i beslut om att tillåta tvångsåtgärder (se SOU 2018:61 s. 143 ff.).

Som vi ovan har konstaterat visar den hittillsvarande tillämpningen av hemlig dataavläsning att det trots detta kan finnas skäl att öka förutsebarheten och tydligheten i vissa av bestämmelserna när det gäller tillståndets innehåll. I avsnitt 8.4.4 behandlar vi frågan om under vilken tidsperiod ett tillstånd ska få verkställas och frågan om uppgifter som har lagrats före denna tidsperiod ska omfattas av tillståndet. Som kommer att framgå i det följande hänger frågorna om tid och villkor nära samman. I avsnitt 8.4.5 går vi därför över till våra överväganden om kravet på villkor för tillståndet. I avsnitt 8.4.6 behandlar vi kravet på att ange vilket avläsningsbart informationssystem som tillståndet avser. Avslutningsvis behandlar vi i avsnitt 8.4.7 frågan om när det ska framgå av tillståndet vem som är skäligen misstänkt. I övrigt har vi inte funnit anledning att anmärka mot bestämmelserna om tillståndets innehåll.

8.4.4 Förtydliganden om tillståndets varaktighet

Förslag: I ett tillstånd till hemlig dataavläsning ska anges under vilken tid som verkställighet får ske.

Tiden för verkställighet får inte bestämmas längre än nödvändigt och får inte överstiga en månad från dagen för beslutet.

Förslaget innebär ett förtydligande av att ett tillstånd till hemlig dataavläsning ska verkställas inom en viss tid som inte får överstiga en månad. Enligt förslaget får alla uppgifter som omfattas av tillståndet och som under verkställighetstiden är åtkomliga i det avläsningsbara informationssystemet hämtas in, om inte annat framgår av tillståndets villkor.

Skälen för vårt förslag

Nuvarande bestämmelse om tillståndets varaktighet

I ett tillstånd till hemlig dataavläsning ska det enligt 18 § första stycket 1 lagen om hemlig dataavläsning alltid anges vilken tid tillståndet avser. När det gäller tid som infaller efter beslutet får tiden inte överstiga en månad från dagen för beslutet. Om det finns behov av tvångsmedlet under en längre period än så krävs ett nytt beslut. Det finns inte någon lagstadgad bortre tidsgräns för tiden innan tillståndet beviljades, dvs. för inhämtning av information som under verkställighetstiden är åtkomlig i informationssystemet. Detta kan få betydelse för inhämtning av lagrade eller historiska uppgifter. I förarbetena till lagen om hemlig dataavläsning har uttalats att rätten vid tillståndsgivningen, t.ex. av integritetsskäl, bör begränsa de uppgifter som får tas upp även såvitt avser tiden före beslutet, eftersom tiden inte får vara längre än vad som är nödvändigt i det enskilda fallet (se prop. 2019/20:64 s. 234.).

Svårigheterna med att tidsbestämma lagrad information och andra verkställighetsfrågor

Den hittillsvarande tillämpningen av hemlig dataavläsning visar att verkställighetstiderna avseende inhämtning som sker i realtid har varit förhållandevis korta och därmed väl förenliga med de krav som ställs (se kapitel 6, avsnitt 6.2.7 och tabell 6.6). När det gäller inhämtning av lagrade eller historiska uppgifter saknas det jämförelseunderlag. SIN konstaterade i sin första särskilda granskning av användningen av hemlig dataavläsning att såväl de granskade ansökningarna som tillstånden i flera fall hade innefattat anmärkningsvärt långa tillståndstider. I några ärenden hade tillstånden innefattat historiska uppgifter under tidsperioder på från tre till som längst sju år. Ansvariga åklagare tillfrågades av nämnden om sina olika överväganden i de granskade ärendena. I ett ärende uppgav åklagaren att det var fråga om omfattande brottslighet i näringsverksamhet som pågått under lång tid. Åklagaren uppgav vidare att hemlig dataavläsning behövdes under så lång tid som sju år eftersom det fanns underrättelseinformation om den brottsliga verksamheten från denna tidpunkt. Det bedömdes nödvändigt att få uppgift om den misstänktes nätverk för att kunna

kartlägga verksamheten och förstå brottsupplägget över tid. I ett annat ärende lämnade åklagaren en mer praktisk förklaring till den sökta tidsperioden, som i det fallet uppgick till drygt tre år. Av åklagarens svar framgick bl.a. följande. Ansökan avsåg en spegling av innehållet i telefonen. Anledningen till tillståndstidens startdatum var att den misstänkte innehaft den aktuella teleadressen sedan dess. Enligt information från polisen var det inte tekniskt möjligt att i tid avgränsa speglingen utifrån ett senare datum. Tillståndet hade för att begränsa integritetsintrånget förenats med ett villkor om att information som lagrats i telefonen före ett visst datum inte fick läsas. Nämnden fann sammantaget inte tillräckliga skäl att i de granskade ärendena ifrågasätta de bedömningar som gjorts gällande tillståndstidens längd. Nämnden framhöll samtidigt att vikten av att åklagaren gör en noggrann prövning av nödvändigheten i varje enskilt fall och att en restriktiv hållning alltid bör intas (se nämndens uttalande med beslut av den 15 december 2021, dnr 92-2020, s. 9 f.).

Den hittillsvarande tillämpningen visar att bestämmelsen om tillståndstid har orsakat vissa verkställighetsproblem. SIN har i sin första granskning lyft fram ett ärende där åklagaren hade ansökt om och fått tillstånd till hemlig dataavläsning avseende både lagrade uppgifter och uppgifter i realtid. Efter att verkställigheten misslyckades ansökte åklagaren om förlängning av tillståndet, och inkluderade den historiska tidsperioden i sin begäran. I motsvarande situation i ett annat ärende hade åklagaren vid ansökan om förlängning inte inkluderat den tidigare beviljade historiska tidsperioden. På fråga från nämnden uppgav åklagaren i det sistnämnda ärendet att hen utgått från att det ”tidigare beslutet täckt åtgärden bakåt i tiden och att det nya tillståndet täckt åtgärden framåt i tiden.” Nämnden konstaterade att åklagarnas till synes olika förhållningssätt i förening med de verkställighetsproblem som kan uppstå vid hemlig dataavläsning aktualiserar frågan under hur lång tid nya verkställighetsförsök kan göras. Nämnden uttalade härvid följande (se a. uttalande, s. 14).

> Enligt 20 § lagen om hemlig dataavläsning får ett beslut i frågor om hemlig dataavläsning verkställas omedelbart. En utgångspunkt tycks vara att det inte finns något hinder mot att avläsning äger rum flera gånger under tillståndstiden och att uppgifter som lagrats under den tiden läses av.[1] Någon reglering eller på annat sätt uttalad tidpunkt för när ett tillstånd senast bör verkställas finns inte. Enligt den princip som gäller för tvångs-

[1] Se Lindberg, Lag (2020:62) om hemlig dataavläsning 2 § 6, Karnov 2021-11-24, (JUNO).

medelsanvändning i allmänhet bör dock ett tvångsmedelsbeslut alltid verkställas i så nära anslutning till beslutet som möjligt.[2]

Nämnden anser att det ligger nära till hands att applicera motsvarande synsätt vid verkställighet av ett tillstånd till hemlig dataavläsning. Det skulle i så fall innebära att ett nytt tillstånd behövs för möjligheten till fortsatta verkställighetsförsök när viss tid förflutit. I de fall ansökan och tillstånd innefattar hemlig dataavläsning även i realtid framstår det som lämpligt att låta den i lag angivna tidsbegränsningen på en månad utgöra den bortre gränsen också för möjligheten till fortsatta verkställighetsförsök avseende historiska uppgifter. Nämndens uppfattning i denna del överensstämmer således med hur frågan har hanterats i ett av ärendena ovan.

Ett tillstånd till hemlig dataavläsning ska verkställas inom en månad

Vårt förslag

Vi föreslår att bestämmelsen om tillståndstid i 18 § första stycket 1 lagen om hemlig dataavläsning ändras på sätt att det i ett tillstånd till hemlig dataavläsning ska anges under vilken tid som verkställighet får ske. Tiden för verkställighet får inte bestämmas längre än nödvändigt och får inte överstiga en månad från dagen för beslutet.

Förslaget innebär ett tydliggörande av att ett tillstånd till hemlig dataavläsning avseende lagrade uppgifter som avses i 2 § första stycket 1–3 och 6 kommer att omfatta inhämtning av alla uppgifter som under verkställighetstiden är åtkomliga i informationssystemet, om inte annat framgår av tillståndets villkor. Genom förslaget tas kravet på att ange ”vilken tid tillståndet avser” bort. Förslaget innebär att själva inhämtningen av uppgifter inte längre behöver begränsas tidsmässigt, om det inte är möjligt eller ändamålsenligt med en sådan begränsning. Förslaget innebär också ett förtydligande av att denna del av tillståndet endast avser under vilken tid som inhämtningen får verkställas och inte vilken historisk eller framtida tidsperiod som de inhämtade uppgifterna får avse. Ändringen knyter an till vårt förslag i avsnitt 8.4.5 om att tidsmässiga villkor som avser själva granskningen av inhämtade uppgifter bör bli mer framträdande. Vi återkommer i det avsnittet till olika exempel på hur tidsmässiga villkor kan utformas. Som kommer att framgå i det följande innebär förslaget en mer ändamålsenlig lagstiftning som speglar verkligheten bättre, som harmonierar mer med annan tvångsmedelslagstiftning och som undanröjer de oklarheter om tidsperioder och verkställighet som har upp-

[2] JO 1997/98 s. 165.

stått i rättstillämpningen. Vårt förslag innebär därmed en förstärkt rättssäkerhetsgaranti.

Förslaget föranleder en justering av de bestämmelser i lagen som ställer krav på viss koppling mellan den enskilde och ett informationssystem ”under den tid som tillståndet avser” (se 4 a § andra stycket, 4 b § andra stycket, 8 § andra stycket och 9 § andra stycket lagen om hemlig dataavläsning). Som en följd av vårt förslag utgår detta tidsmässiga krav. Någon ändring i sak är inte avsedd. Kravet på koppling mellan den enskilde och ett informationssystem ska alltså fortsatt gälla. Vidare innebär våra förslag i det följande att tidsmässiga villkor för tillståndet enligt 18 § första stycket 4 kommer att få en annan praktisk betydelse än i dag, se nedan och i avsnitt 8.4.5.

Behov, nytta och effektivitet

Nuvarande ordning innebär att en brottsbekämpande myndighet som vill hämta in uppgifter som redan finns lagrade i ett informationssystem måste ansöka om tillstånd till hemlig dataavläsning avseende tidsperioder som ligger bakåt i tiden. Det finns flera betänkligheter med en sådan ordning. Frågan är inledningsvis om den är helt rättvisande. Att vid ett tillfälle hämta in information som sedan flera år funnits lagrad på informationssystemet innebär ju inte att verkställigheten har pågått under flera år. Det blir därför missvisande att tala om ”historiska” tidsperioder, eftersom det vid hemlig dataavläsning endast är möjligt att ta del av den information som under verkställighetstiden är åtkomlig i informationssystemet.

Ett ännu större problem med nuvarande ordning är att det kan vara svårt att tidsbestämma lagrade filer, något som också framhölls i förarbetena. Exempelvis kan lagrade filer vara skapade vid en viss tidpunkt och ändrade vid en eller flera andra tidpunkter (se a. prop. s. 234). Vidare kan tidsinställningar i ett informationssystem enkelt ändras och tidsmarkörer därigenom manipuleras. Svårigheterna med att tidsbestämma information innebär i sin tur att brottsbekämpande myndigheter riskerar att missa stora delar av den information som man eftersöker. En tidsbegränsning bakåt i tiden redan vid tillståndsgivningen kan med andra ord komma att innebära oavsiktliga begränsningar av ett tillstånd, vilket också företrädare för de brottsbekämpande myndigheterna har framhållit. Det är väsentligt att ett tillstånd

till hemlig dataavläsning även i praktiken kan användas för att hämta in all den information som tillståndet är avsett att omfatta. I annat fall kan själva syftet med hemlig dataavläsning komma att motverkas. Behovet av att förtydliga bestämmelsen om tillståndets varaktighet i syfte att uppnå en mer effektiv brottsbekämpning framstår därmed som påtagligt.

En bestämmelse som i stället för tidsperioder knyter an till verkställighetsperioden framstår som mer ändamålsenlig. Det finns goda skäl att i detta avseende avvika från vad som gäller för de bakomliggande hemliga tvångsmedlen. Verkställighet av hemlig dataavläsning är generellt sett mer tekniskt komplicerad än verkställighet av de permanenta hemliga tvångsmedlen. Den nuvarande bestämmelsen om tillståndstid har därför orsakat osäkerhet och tillämpningsproblem när det gäller frågan om under hur lång tid verkställighetsförsök kan göras. Vidare förekommer problematiken med tidsbestämmande av lagrade uppgifter enbart för hemlig dataavläsning. Vi föreslår därför att det i tillståndet ska anges under vilken som tid tillståndet får verkställas. Den nuvarande maximala tiden om en månad framstår som rimlig och i överensstämmelse med tidigare bedömningar om lagstiftningens förenlighet med Sveriges internationella åtaganden (jfr SOU 2018:61 s. 143 f.). Om verkställigheten inte lyckas inom denna period, krävs ett nytt tillstånd för fortsatta verkställighetsförsök. Förslaget innebär i detta avseende ett tydliggörande av vad som redan gäller (jfr a. uttalande s. 14).

Förslaget bidrar även till en mer rättvisande bild av åtgärden. Att det under en begränsad tid hämtas in historisk information som sedan flera år funnits lagrad på informationssystemet innebär ju inte den berörde under flera år har varit föremål för hemlig dataavläsning. Rent faktiskt blir den berörde utsatt för hemlig dataavläsning endast under den period som beslutet verkställs. Förslaget bidrar därmed också till att jämförelsen av tillståndstider mellan de permanenta hemliga tvångsmedlen och hemlig dataavläsning blir mer rättvisande än i dag, eftersom det bara är den faktiska tiden som tvångsmedlen har verkställts som redovisas (se tabell 6.6 i kapitel 6).

Förslaget innebär ett tydliggörande av att ett tillstånd till hemlig dataavläsning avseende lagrade uppgifter enligt 2 § första stycket 1–3 och 6 kommer att omfatta inhämtning av alla uppgifter som under verkställighetstiden är åtkomliga i det avläsningsbara informationssystemet, om inte annat framgår av tillståndets villkor. Detta fram-

går indirekt genom ändringen av den nuvarande bestämmelsen. Vi bedömer att ett förtydligande härom varken är nödvändigt eller lämpligt att införa i lagtext. Den föreslagna bestämmelsen harmonierar bättre med öppna tvångsmedel som husrannsakan, beslag och genomsökning på distans, där det saknas en tidsgräns i förhållande till vilken information som den brottsbekämpande myndigheten får ta del av. Beslag och genomsökning på distans av ett informationssystem uppvisar stora likheter med hemlig dataavläsning (se avsnitt 4.3 och 7.3). Som vi tidigare har framhållit är det av väsentlig betydelse att hemlig dataavläsning kan användas i motsvarande fall som dessa öppna tvångsmedel. I annat fall finns risk för att viss allvarlig brottslighet inte kan bekämpas när viktig information är oåtkomlig genom traditionella tvångsmedel. Vårt förslag bidrar därmed till att bättre säkerställa en välfungerande systematik i regelverket för olika tvångsmedel.

Eftersom hemlig dataavläsning på detta sätt kan användas mer ändamålsenligt kan förslaget förväntas vara effektivt och medföra avsevärd nytta för brottsbekämpningen.

Förslaget innebär risker för den personliga integriteten

Syftet med förslaget är att undanröja de osäkerheter som i dag kan råda om ett tillstånds omfattning, inte att en större mängd uppgifter ska granskas eller att det ska ske mer omfattande kartläggningar. Förslaget innebär dock att en större mängd lagrade uppgifter kan komma att hämtas in med stöd av hemlig dataavläsning jämfört med i dag. Vi bedömer att inhämtning av uppgifter som är lagrade, eller för den delen har daterats långt bakåt i tiden, inte per automatik innebär ett mer omfattande integritetsintrång. Hur stort integritetsintrånget är beror i det enskilda fallet på hur stor mängd och vilken typ av information om den berörda personen som den hemliga dataavläsningen ger tillgång till. Även med beaktande härav får förslaget generellt sett anses innebära en ökad risk för den personliga integriteten, eftersom mer information kan komma att hämtas in.

I de konkreta fall som förslaget innebär en ökad risk för den personliga integriteten måste denna risk balanseras mot tillräckligt begränsande villkor för att åtgärden ska kunna anses proportionerlig. Förslaget medför därmed att villkor som anger under vilken tid som inhämtningen får verkställas eller vilka uppgifter (avgränsat till en viss

tidsperiod) som inte får granskas kommer att bli mer framträdande. Vi återkommer till villkorsbestämmelsen och exempel på olika tidsmässiga villkor i nästa avsnitt. Redan nu ska följande framhållas. Villkor enligt 18 § första stycket 4 lagen om hemlig dataavläsning syftar till att gagna skyddet för den personliga integriteten. Ett tillstånd till hemlig dataavläsning bör, om det är lämpligt och ändamålsenligt, avgränsas i tiden inte bara avseende tiden för verkställighet utan också genom tidsmässiga villkor beträffande vilka uppgifter som får inhämtas eller granskas. Detta för att åtgärden ska kunna anses proportionerlig. Enligt motiven till den nuvarande bestämmelsen om att tiden för ett tillstånd till hemlig dataavläsning inte får bestämmas längre än nödvändigt ”bör rätten” med hänsyn härtill begränsa de uppgifter som får tas upp såvitt avser tiden före beslutet (se a. prop. s. 234.). Den hittillsvarande tillämpningen visar dock att tidsmässiga begränsningar av lagrade uppgifter redan i inhämtningsfasen kan motverka själva syftet med dataavläsningen. Som ovan framhållits kan alltför snäva avgränsningar både leda till att de brottsbekämpande myndigheterna får svårt att verkställa tillståndet och att de går miste om viktig information. Villkor bör i dessa fall endast appliceras vid granskningen, efter att man har fått en bild av vilken information som finns i informationssystemet. Detta är en omständighet som måste beaktas vid proportionalitetsbedömningen och utformningen av eventuella villkor. I de fall det är möjligt och ändamålsenligt, bör tidsmässiga villkor som tar sikte redan på inhämtningsfasen uppställas (se t.ex. exempel 4 i avsnitt 8.4.5 nedan). I de fall det inte är möjligt att sätta upp tidsmässiga villkor som begränsar själva inhämtningen av uppgifter bör det i de allra flesta fall vara möjligt att sätta upp tidsmässiga villkor som begränsar vilka uppgifter som får gås igenom i en granskningsfas. Redan själva inhämtningen av uppgifter utgör visserligen ett ingrepp i den personliga integriteten. Det intrånget är dock sekundärt i förhållande till om och när materialet gås igenom i en granskningsfas (se avsnitt 7.3.2). Vi återkommer i avsnitt 8.5 till frågor om hur det inhämtade materialet ska hanteras.

Om tillståndet medger det finns inget hinder mot att inhämtning äger rum flera gånger under verkställighetstiden. Även detta förhållande utgör en omständighet som måste beaktas vid proportionalitetsbedömningen och vid utformningen av eventuella villkor för tillståndet. Som utgångspunkt gäller alltså att verkställigheten kan fortgå under hela verkställighetstiden.

Förslaget bedöms vara proportionerligt

En förutsättning för att förslaget ska kunna anses proportionerligt är alltså att de ökade riskerna balanseras genom villkor som begränsar tillståndet till skydd för den personliga integriteten. Under denna förutsättning framstår behovet och nyttan av förslaget vid en samlad intresseavvägning som så påtagligt att det integritetsintrång som det kan innebära bedöms som försvarligt. Förslaget bedöms därmed proportionerligt, dvs. nödvändigt med hänsyn till intresset av att bekämpa den allvarliga brottsligheten.

8.4.5 Förtydligande om villkor för tillståndet

Förslag: I ett tillstånd till hemlig dataavläsning ska anges vilka uppgifter som inte får granskas och övriga villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan, om det inte framstår som obehövligt.

Åklagaren, eller i förekommande fall Säkerhetspolisen, ska i samband med en ansökan om hemlig dataavläsning föreslå de villkor som tillståndet bör förenas med, om sådana villkor inte framstår som obehövliga.

Skälen för vårt förslag

Nuvarande bestämmelse om villkor för tillståndet

I 18 § första stycket 4 lagen om hemlig dataavläsning finns ett ovillkorligt krav på att ett tillstånd till hemlig dataavläsning ska innehålla villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan. I förarbetena har det uttalats att sådana villkor kan ta sikte på i stort sett vilka omständigheter som helst som kan gagna skyddet för den personliga integriteten (se prop. 2019/20:64 s. 156).

Villkorsbestämmelsen motsvarar vad som gäller för bakomliggande tvångsmedel, med den skillnaden att det vid ett tillstånd till hemlig dataavläsning är obligatoriskt att tillståndet innehåller villkor för åtgärdens tillämpning. Vid användning av de permanenta hemliga tvångsmedlen ska villkor endast anges när det finns skäl till det, se 27 kap.

21 § sjätte stycket rättegångsbalken. Skälet till att kravet på ett tillstånd till hemlig dataavläsning i detta avseende är högre ställt har inte motiverats särskilt i förarbetena (se t.ex. a. prop. s. 156 f.).

Den 1 oktober 2023 infördes en möjlighet att kunna knyta ett tillstånd till hemlig rumsavlyssning och hemlig kameraövervakning till den skäligen misstänkte i stället för till en plats. Vid sådana tillstånd är det, precis som vid den nya möjligheten till hemlig dataavläsning i motsvarande fall, obligatoriskt att ange villkor för tillståndet. I förarbetena till bestämmelserna bedömdes det nödvändigt med ett obligatoriskt krav på villkor för att minska onödiga integritetsintrång:

> Kravet på angivande av en specifik plats i beslutet måste ersättas av krav på andra villkor som begränsar risken för onödiga integritetsintrång. Utan sådana villkor kan man inte skapa tillräckliga garantier för att åtgärden är proportionerlig i det konkreta fallet. Det bör därför vara ett oeftergivligt krav att tillståndet förenas med sådana villkor.

Det infördes samtidigt ett lagstadgat krav som innebär att åklagaren i samband med en sådan ansökan ska föreslå de villkor som ska gälla för tillståndet, se 27 kap. 21 § första stycket rättegångsbalken och 14 § andra stycket lagen om hemlig dataavläsning. Kravet motiverades huvudsakligen på följande sätt.

> I en situation där villkor inte bara är obligatoriska utan nödvändiga – vilket vi bedömer dem vara om platskravet tas bort – anser vi dock att frågan kommer i annan dager. Vi menar att ett lagstadgat krav på att åklagaren föreslår villkor kan förväntas leda till att villkoren ägnas mer uppmärksamhet och även får en högre kvalitet. Risken för att beslut meddelas utan villkor torde minska påtagligt. Vår bedömning är därför att det i en ansökan om tillstånd som knyts till den skäligen misstänkte bör ankomma på åklagaren att i samband med sin framställan till rätten, t.ex. i den promemoria som ges in till rätten, föreslå sådana begränsande villkor som man anser lämpliga.

Förarbetsuttalandena framgår av SOU 2022:19 s. 344, se vidare om lagändringarna i prop. 2022/23:126 s. 153 ff. och 244 samt avsnitt 7.4.6 med där gjorda hänvisningar.

Villkorskravet har orsakat tolkningssvårigheter och verkställighetsproblem

Förekomsten av och innehållet i de villkor som ett tillstånd till hemlig dataavläsning ska förenas med redovisas inte i myndigheternas årliga skrivelser. I dessa delar har vi därför inhämtat relevanta uppgifter från SIN:s tillsynsverksamhet och från företrädare för de brottsbekämpande myndigheterna. Det kan konstateras att det råder en osäkerhet i rättstillämpningen om hur man bör ange villkor som tar sikte på att tillgodose intresset av att enskilda personliga integritet inte kränks i onödan. SIN har i sina granskningar funnit att villkorskravet inte alltid har efterlevts i praktiken. I en tidig granskning av användningen av hemlig dataavläsning noterade SIN att det i stor utsträckning förekom tillstånd som saknade villkor, trots att det är ett lagstadgat krav (se nämndens uttalande med beslut av den 15 december 2021, dnr 92-2020). SIN återkom under 2023 med en granskning av villkor vid ansökan om hemlig dataavläsning. Granskningen omfattade 121 tillstånd som förenats med villkor. Nämnden fann bl.a. att det i ungefär 90 procent av tillstånden förekom standardiserade villkor. Nämnden konstaterade avslutningsvis att det utifrån de granskade ärendena stod klart att användningen av villkor inte har utgjort den rättssäkerhetsgaranti som var avsikten när lagen om hemlig dataavläsning infördes. Nämnden hänvisade vidare till vår utredning om utvärdering av lagen och uttalade att det finns anledning att överväga en förändring av regleringen gällande villkor eller andra mekanismer i lagstiftningen för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan (se nämndens uttalande med beslut av den 20 juni 2023, dnr 80-2022). Även företrädare för de brottsbekämpande myndigheterna har bekräftat att kravet på att ett tillstånd till hemlig dataavläsning ska förenas med villkor har orsakat både tolkningssvårigheter och verkställighetsproblem. Den hittillsvarande tillämpningen visar på flera rättssäkerhetsbrister.

Avsaknad av villkor

Såväl ansökningar om som tillstånd till hemlig dataavläsning har ofta saknat villkor. Ansvariga åklagare har i samband med SIN:s första granskning anmodats att redogöra för vilka överväganden som gjorts i samband med sådana ansökningar när det gäller villkor eller begräns-

ningar av åtgärden för att värna den enskildes integritet. I de fall där villkor inte har angetts i tillståndet har uppfattningen varit att ansökan utformats på sådant sätt att den misstänktes personliga integritet inte kränks i onödan. Att därutöver uppställa villkor ”endast för villkorets skull” har ansetts överflödigt. I något fall har ansvarig tekniker från polisen varit med på sammanträdet och redogjort för hur åtgärden skulle verkställas, vilket varit anledningen till att något villkor inte angetts. Nämnden uttalade i samband med sin första granskning att det i och för sig är positivt att frågor kring verkställighet och integritet har diskuterats vid rättens sammanträden, men att avsaknaden av villkor i tillstånden innebär att det inte är möjligt att i efterhand kontrollera att en hantering som uppges ha diskuterats i samband med tillståndsprövningen efterlevs (se nämndens uttalande med beslut av den 15 december 2021, dnr 92-2020, s. 11 f.).

Standardiserade villkor

När ett tillstånd till hemlig dataavläsning har förenats med villkor har dessa villkor ofta varit av standardiserat slag, exempelvis:

- ”HDA ska verkställas så att minsta möjliga överskottsinformation hämtas in.”
- ”HDA ska verkställas så att minsta möjliga integritetsintrång görs.”

Eftersom ändamålsprincipen, behovsprincipen och proportionalitetsprincipen redan gäller vid alla beslut om och all tillämpning av hemlig dataavläsning utgör standardiserade villkor av denna typ inte något förstärkt integritetsskydd. Ur rättssäkerhetssynpunkt framstår standardiserade och intetsägande villkor som lika problematiskt som avsaknaden av villkor.

Verkställighetshindrande villkor

Det har även förekommit att de villkor som föreskrivits varit alltför begränsande och att verkställigheten därför inte har gått att genomföra, exempelvis:

- ”Avläsning av uppgifter får bara avse uppgifter om brottet.”

- ”Endast uppgifter när den misstänkte deltar i samtalet får hämtas in.”
- ”HDA får bara avse kommunikation med den misstänkte.”
- ”Endast uppgifter i molntjänster i Sverige får hämtas in.”

Villkor som tar sikte på att göra specifika filtreringar av detta slag redan vid själva inhämtningen är enligt företrädare för de verkställande myndigheterna tekniskt omöjliga att uppfylla. Det är t.ex. inte möjligt att endast hämta in de uppgifter som berör brottet utan att först bedöma vilka av de tillgängliga uppgifterna som är av detta slag (exemplet i den första punkten ovan). Några av de exempel på villkor som anges i förarbetena till lagen om hemlig dataavläsning har också visat sig vara svåra att uppfylla i praktiken (jfr prop. 2019/20:64 s. 233). De verkställande myndigheterna har på ett generellt plan kunnat konstatera att villkor som tagit sikte på inhämtningsfasen och inte på granskningsfasen typiskt sett har varit svåra att verkställa (jfr avsnitt 6.2.5). Det är t.ex. omöjligt att på förhand veta när ett samtal kommer att äga rum, vilka personer som kommer att delta och vad som då kommer att avhandlas. Ett tillstånd med villkor om att endast samtal med en viss person får inhämtas är således inte verkställbart. Dessa begränsningar är inte unika för just hemlig dataavläsning utan fungerar likadant för övriga hemliga tvångsmedel. Ett tillstånd med villkor om att endast samtal med en viss person får granskas är däremot verkställbart. I de fall det är omöjligt eller osäkert om det är möjligt att följa villkoret så kan tillståndet inte verkställas. Problematiken har dock blivit mer framträdande vid hemlig dataavläsning p.g.a. kravet på obligatoriska villkor i kombination med kravet på teknikanpassning.

En utgångspunkt vid verkställighet av hemlig dataavläsning är att tekniken och tillvägagångssättet ska anpassas efter tillståndet och inte tvärtom (jfr 23 § lagen om hemlig dataavläsning och avsnitt 8.5.6 nedan). SIN har i sina granskningar framhållit att tekniska förutsättningar eller eventuella begränsningar i systemen inte ska vara avgörande för hur en ansökan om ett hemligt tvångsmedel utformas (se t.ex. nämndens uttalande med beslut av den 29 mars 2023, dnr 43-2022, s. 7). Det är verkställande myndighet som är skyldig att se till att de tekniska anpassningar som har gjorts och de riktlinjer eller motsvarande som har upprättats är tillräckliga. Någon kritik har inte fram-

förts av tillsynsmyndigheterna i detta avseende. Det har således inte framkommit något som ger anledning att ifrågasätta den teknik och de metoder som används vid verkställighet av hemlig dataavläsning.

En ventil för situationer när villkor är obehövliga

Det är viktigt att användningen av villkor i praktiken utgör den rättssäkerhetsgaranti som har varit lagstiftarens avsikt. Bestämmelsen om villkor för tillståndet måste därför bli tydligare och lättare att tillämpa än i dag.

Inledningsvis måste vi överväga om det även fortsättningsvis ska vara obligatoriskt att förena ett tillstånd till hemlig dataavläsning med villkor. Finns det skäl att fortsatt ställa kraven, eller rättssäkerhetsgarantierna, för hemlig dataavläsning högre än för bakomliggande tvångsmedel och i så fall varför?

Sedan lagen om hemlig dataavläsning trädde i kraft har regelverket kring såväl hemliga som öppna tvångsmedel förändrats i flera avseenden. I vissa avseenden är villkorskravet numera lika högt ställt för de bakomliggande tvångsmedlen som för hemlig dataavläsning (se ovan angående de nya bestämmelserna i 27 kap. 21 § första stycket rättegångsbalken och 14 § andra stycket lagen om hemlig dataavläsning). Förekomsten av villkor är en omständighet som är av stor betydelse vid proportionalitetsbedömningen eftersom villkoren påverkar integritetsintrånget. Skyldigheten att föreskriva särskilda villkor till skydd för den personliga integriteten innebär att domstolen måste begränsa utrymmet för den brottsbekämpande myndigheten att använda hemlig dataavläsning. Med villkor för tillståndet kan garantier skapas för att åtgärden blir proportionerlig och rättssäker i det enskilda fallet. Villkor kan samtidigt göra det möjligt att tillåta en hemlig dataavläsning som utan villkor hade ansetts som oproportionerlig. Förekomsten av villkor underlättar också tillsynsmyndighetens efterhandskontroll. Även Utredningen om rättssäkerhetsgarantier vid användningen av vissa hemliga tvångsmedel har bedömt att bestämmelserna om särskilda villkor till skydd för den personliga integriteten är viktiga och bidragande till att regelverket kring innehållet i tillståndsbesluten uppfyller kraven enligt Europakonventionen (se SOU 2018:61 s. 149 f.).

Hemlig dataavläsning kan i förhållande till andra hemliga tvångsmedel innebära en ökad risk för den personliga integriteten (se kapi-

tel 6). Redan mot denna bakgrund talar starka skäl för att även fortsättningsvis ställa rättssäkerhetskraven för hemlig dataavläsning högt. Härtill kommer att tillämpningsområdet för hemlig dataavläsning nyligen har utvidgats och vi lämnar i detta betänkande ytterligare förslag som kan behöva balanseras med tydliga villkor för att åtgärden ska kunna anses rättssäker och proportionerlig i det enskilda fallet (se avsnitt 7.3.2, 7.4.4 och 8.4.4). Det är vår samlade bedömning att förekomsten av villkor som begränsar risken för onödiga integritetsintrång i de allra flesta fall är nödvändiga för att skapa tillräckliga garantier för att den hemliga dataavläsningen blir proportionerlig och rättssäker i det konkreta fallet.

Det sagda utesluter inte att det kan finnas situationer där ett villkor för tillståndet framstår som överflödigt. Standardiserade och intetsägande villkor ”för villkorens skull” fyller ingen funktion. Sådana villkor kan tvärtom skapa en felaktig föreställning om att intrånget har balanserats tillräckligt mot den enskildes personliga integritet samt försvåra eller omöjliggöra efterhandskontroll. Om det i ett enskilt fall framstår som obehövligt med villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan, ska det därför inte krävas att tillståndet förenas med villkor (jfr ventilen i 27 kap. 10 § första stycket sista meningen rättegångsbalken som avser undantag från försegling eller märkning av beslagtaget föremål). En sådan ordning framstår ur rättssäkerhetsperspektiv både som mer tydlig och som mer anpassad till verkliga förhållanden. Möjligheten att låta bli att förena ett tillstånd med villkor bör användas med viss restriktivitet. Om det finns anledning att tro att villkor kan vara av betydelse, bör tillståndet förenas med villkor. Förslaget bedöms inte leda till någon beaktansvärd ökning av integritetsriskerna eftersom förslaget är snävt utformat och dessutom tar sikte på situationer där risken för onödiga kränkningar i den personliga integriteten redan är omhändertagen utan särskilda villkor. Det nuvarande ovillkorliga kravet på att ett tillstånd till hemlig dataavläsning ska förenas med villkor ska därför förses med en ventil för fall där villkor framstår som obehövliga.

Villkor om vilka uppgifter som inte får granskas och övriga villkor för tillståndet

Det bör också tydliggöras vad villkoren ska avse. Vi föreslår att det i ett tillstånd till hemlig dataavläsning ska anges vilka uppgifter som inte får granskas och övriga villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan, om det inte framstår som obehövligt. Vårt förslag återknyter till hur hemlig dataavläsning går till i praktiken och till vår definition av de olika uttrycken *inhämtning* och *granskning*, se avsnitt 7.2 och figur 7.1. De praktiska exempel på villkor som vi redogör för i det följande har lyfts fram av utredningens experter efter samråd med personer som har till uppgift att verkställa tillstånd till hemlig dataavläsning.

Som vi har redogjort för i det föregående samt i avsnitt 6.2.5 och 7.3.2 är det i de allra flesta fall svårt eller omöjligt att uppställa villkor som tar sikte på inhämtningsfasen. Vid t.ex. hemlig dataavläsning av lagrade filer på en dator, sorterade i komplexa mappstrukturer som har skapats och ändrats vid olika tillfällen, kan det motverka syftet med åtgärden om inhämtningen tidsbegränsas alltför snävt. Det är oftast inte heller möjligt att redan i inhämtningsfasen filtrera ut särskilda mejl eller filer utan att först ha hämtat in de databasfiler eller mappstrukturer där de enskilda mejlen eller filerna lagras. Ett annat exempel är hemlig dataavläsning av en mobiltelefon som används av flera personer, men där endast en användares aktiviteter är intressanta. En sådan filtrering är i regel omöjlig att göra redan i inhämtningsfasen. Däremot är sådana filtreringar möjliga att göra i en tidig bearbetning av uppgifterna, inför en granskning. Med hänsyn härtill framstår det som nödvändigt ur integritetssynpunkt att det i villkoren ska anges ”vilka uppgifter som inte får granskas”. Genom sådana villkor ska det tydligt framgå vilka uppgifter som får gås igenom av behöriga personer i en granskningsfas, efter inhämtning och inledande (maskinell eller manuell) bearbetning av uppgifterna. Det förhållandet att det i villkoren ska anges vilka uppgifter som *inte* får granskas hindrar inte att villkoren formuleras som att endast vissa angivna uppgifter *får* granskas. Avgörande är att villkoren ur ett integritets- och rättssäkerhetsperspektiv är tydligt utformade. Som vi har framhållit i avsnitt 8.4.4 ovan bör villkor om det är möjligt och ändamålsenligt ta sikte på tidsmässiga avgränsningar, men kan också avse andra begränsningar. Vi återkommer i avsnitt 8.5.6 till frågan om hur den in-

formation som inte får granskas enligt villkoren ska hanteras. Exempel på villkor som avser vilka uppgifter som får/inte får granskas:

Exempel 1
Efter att uppgifterna hämtats in får endast uppgifter [från ett visst datum/ som avser kommunikation med NN/vissa uppgifter] granskas.

Exempel 2
Vid analys av de inhämtade uppgifterna får inte uppgifter [före ett visst datum] granskas.

Ett mer specifikt exempel är en dator i hemmet som man misstänker att den berörde använder för att sprida barnpornografiska bilder, men att samma dator också används i legala syften av andra familjemedlemmar, t.ex. en sambo. Det ligger dock i sakens natur att det oftast är först efter att datorn har lästs av som det är möjligt att avgöra vilka kommunikationstjänster och därtill hörande användarkonton som finns åtkomliga i datorn samt vem som använder dessa. I ett sådant fall, där information om sambons kommunikation bedöms vara utan relevans i ärendet, skulle villkor som avser vilka uppgifter som inte får granskas kunna utformas så här:

Exempel 3
Efter att uppgifterna hämtats in får inte uppgifter, såsom kommunikation från mejlkonton eller andra användarkonton, tillhörande [sambon till NN] granskas.

Härutöver föreslår vi att det i ett tillstånd till hemlig dataavläsning ska anges ”övriga villkor för tillståndet”. Villkoren måste anpassas efter omständigheterna i det enskilda fallet. I de fall det är möjligt och ändamålsenligt att uppställa villkor som tar sikte på inhämtningsfasen bör inhämtningen begränsas genom villkor. Om så inte sker finns det en risk att åtgärden i efterhand inte framstår som proportionerlig. Om det genom övriga villkor kan göras en snäv avgränsning av tillståndet redan i inhämtningsfasen kan villkor som avser vilka uppgifter som inte får granskas framstå som obehövliga. Såväl villkor om vilka uppgifter som inte får granskas som övriga villkor för tillståndet kan ibland framstå som obehövliga. En bedömning måste som ovan framhållits alltid göras i det enskilda fallet. I de fall som det är möjligt att göra en åtskillnad mellan lagrade uppgifter och realtidsuppgifter redan i inhämtningsfasen bör detta göras. Om åtgärden exempelvis endast avser ett visst samtal eller möte som man miss-

tänker kommer att äga rum bör på motsvarande sätt uppställas villkor som innebär att inhämtningen endast får avse realtidsuppgifter alternativt uppgifter som tillkommer under verkställighetsperioden:

Exempel 4
Inhämtning får inte omfatta kommunikationsavlyssnings- eller platsuppgifter som har tillkommit före verkställighetsperioden.

Vid hemlig dataavläsning avseende kameraövervaknings- eller rumsavlyssningsuppgifter enligt 2 § första stycket 4 eller 5, dvs. vid inhämtning av realtidsuppgifter genom användning av olika sensorer, bör sådana villkor vara tämligen enkla att ställa upp, exempelvis:

Exempel 5
Verkställighet av kameraövervaknings- eller rumsavlyssningsuppgifter får endast ske när det genom spaning eller på annat sätt bekräftats att NN möter upp XX och i nära anslutning till mötet.

Exempel 6
Verkställighet av kameraövervaknings- eller rumsavlyssningsuppgifter får inte ske när NN befinner sig på [viss plats etc.]. De uppgifter som behövs för att bedöma om NN befinner sig på [platsen] får dock tas upp.

Exempel 7
Verkställighet av kameraövervaknings- eller rumsavlyssningsuppgifter får inte ske under [viss tid/på viss plats etc.].

Åklagaren ska föreslå de villkor som tillståndet bör förenas med

För att syftet med villkorsgivningen ska uppfyllas krävs att villkoren generellt sett håller en högre kvalitet än i dag. Vi föreslår därför att åklagaren, eller i förekommande fall Säkerhetspolisen, i samband med en ansökan om hemlig dataavläsning ska vara skyldig att föreslå de villkor som tillståndet ska förenas med.

I förarbetena till lagen om hemlig dataavläsning avfärdades tanken på att åklagaren i samband med ansökan skulle föreslå villkor för tillståndet. Regeringen såg inte något behov av en sådan bestämmelse eftersom det inte fanns något motsvarande krav beträffande bakomliggande tvångsmedel. Regeringen uttalade dock att det vid sammanträdet kan finnas anledning för den som söker om tillstånd att motivera sin ansökan genom att på ett övergripande plan beskriva hur

tvångsmedlet ska verkställas. Vidare framhöll regeringen att domstolen, vid eventuella oklarheter eller behov av kompletteringar, dessutom har möjlighet att genom frågor skaffa sig ett tillräckligt underlag för att fatta beslut i ärendet, inklusive villkor för att skydda enskildas personliga integritet (se prop. 2019/20:64 s. 156 f.).

Vi gör motsatt bedömning eftersom vi finner att den hittillsvarande tillämpningen visar på ett påtagligt behov av att åklagaren i samband med en ansökan om hemlig dataavläsning föreslår vilka villkor som tillståndet bör förenas med. Utifrån den nuvarande regleringen är frågan om villkor ytterst rättens ansvar. Det finns emellertid anledning att framhålla åklagarens ansvar för en ansökan om hemliga tvångsmedel i allmänhet och hemlig dataavläsning i synnerhet eftersom det är fråga om en så tekniskt komplicerad verkställighetsmetod. Vid rättens tillståndsprövning tecknas vanligtvis beslutet om tillstånd till ett hemligt tvångsmedel på åklagarens ansökningshandling. Ansökan får därför betydelse för hur tillståndet utformas. Som har framgått av SIN:s granskningar finns risken för att ofullständigheter som reds ut vid sammanträdet inte kommer till uttryck i villkor. Även om rätten har det yttersta ansvaret för beslutet så åligger det åklagaren att utforma ansökan så att den både uppfyller de formella kraven och ger korrekta förutsättningar för prövningen (jfr SIN:s uttalande med beslut av den 29 mars 2023, dnr 43-2022). Eftersom hemlig dataavläsning är en tekniskt komplicerad metod varierar förutsättningarna för såväl verkställighet som utformningen av villkor markant mellan olika ärenden. Redan mot denna bakgrund är det svårt för rätten att genom frågor skaffa sig ett fullgott underlag för att utforma egna villkor eller kunna bedöma om ett villkor utgör hinder för verkställighet. Åklagaren är den som, tillsammans med de tekniker som ska genomföra verkställigheten, har bäst insyn i utredningen. Åklagaren bör också redan i samband med en ansökan noga ha övervägt de närmare förutsättningarna för verkställighet och hur integritetsintrånget kan begränsas. Vi bedömer därför att det vid en ansökan om tillstånd om hemlig dataavläsning bör ankomma på åklagaren att, t.ex. redan i den ansökan eller det tillhörande underlag som ges in till rätten, föreslå sådana villkor som anses lämpliga. Om åklagaren anser det obehövligt att förena ett tillstånd med villkor bör i stället detta anges i samband med ansökan. Åklagaren bör också motivera varför hen anser det obehövligt att förena tillståndet med villkor. Frågan om villkor kommer fortsatt ytterst att vara rättens ansvar. Rätten är självklart inte

bunden av åklagarens förslag utan måste t.ex. ta ställning till om villkoren är tillräckliga eller om ett eventuellt tillstånd ska förenas med andra eller ytterligare villkor.

Ett lagstadgat krav på att åklagaren föreslår villkor kan förväntas leda till att villkoren blir mer framträdande och får en högre kvalitet. Risken för beslut utan nödvändiga villkor, beslut med illusoriska villkor eller beslut med verkställighetshindrande villkor bör därmed minska påtagligt (jfr SOU 2022:19 s. 344 f.). Förslaget bedöms, tillsammans med förslaget om ett förtydligande av bestämmelsen om uppgiftstyperna och en tydligare bestämmelse om verkställighetstid (se avsnitt 7.3.2 och 8.4.4), leda till en högre andel verkställbara beslut. Det medför i sin tur att antalet verkställda tillstånd till hemlig dataavläsning kommer att överensstämma bättre med antalet beviljade tillstånd. Jämförelsen mot antalet meddelade tillstånd till andra hemliga tvångsmedel kommer därmed också att bli mer rättvisande (se kapitel 6 och vidare i kapitel 12). Vi bedömer sammantaget att kravet på åklagaren att föreslå villkor, tillsammans med ventilen för obehövliga villkor, säkerställer att användningen av villkor även i praktiken utgör den rättssäkerhetsgaranti som har varit lagstiftarens avsikt.

8.4.6 Särskilt om kravet att ange vilket avläsningsbart informationssystem tillståndet avser

Bedömning: Kravet på att i tillståndet ange vilket avläsningsbart informationssystem som tillståndet avser uppfyller de rättssäkerhetskrav som ställs på lagstiftningen.

Skälen för vår bedömning

Nuvarande bestämmelse om angivande av informationssystem

Utmärkande för hemlig dataavläsning är att informationen inhämtas från ett avläsningsbart informationssystem. De högt ställda beviskraven för att bedöma kopplingen mellan informationssystemet och den som åtgärden avser, när sådan prövning krävs, framstår som väl avvägda (se prop. 2019/20:64 s. 122 f.) Även de undantag från huvudregeln om krav på koppling mellan den enskilde och informations-

systemet som finns framstår som förenliga med de rättssäkerhetskrav som ställs (se a. prop. s. 123 ff. och SOU 2022:19 s. 284 ff.).

I ett tillstånd till hemlig dataavläsning ska det enligt 18 § första stycket 2 lagen om hemlig dataavläsning anges vilket avläsningsbart informationssystem som tillståndet avser. Enligt förarbetena betyder detta att det i tillståndet måste anges vilket specifikt informationssystem tillståndet gäller för. När det gäller fysiska informationssystem som t.ex. en mobiltelefon eller en dator kan detta ske genom att exempelvis ett visst serienummer, IMEI-nummer, MAC-adress eller andra uppgifter som möjliggör identifiering. Uppgifterna måste i vart fall vara så specificerade att det går att verkställa åtgärden och att det är möjligt att bedöma kopplingen mellan informationssystemet och den som åtgärden avser, när sådan prövning krävs, för att utesluta förväxlingsrisk med andra informationssystem (se a. prop. s. 232 f.). När tillståndet gäller immateriella informationssystem anges lämpligen det användarkonto eller andra avgränsade delar av tjänsterna som åtgärden ska vidtas i. Det kan vara exempelvis en e-postadress eller ett användarnamn till ett konto på sociala medier eller annan internetbaserad tjänst.

Bestämmelsen om specificering av informationssystemet utgör alltså en rättssäkerhetsgaranti till skydd för den som berörs av åtgärden, men den syftar också till att minska risken för att personer som är ovidkommande för åtgärden drabbas. Det innebär att rätten redan vid tillståndsgivningen måste kunna ta ställning till den konkreta åtgärd som avses, vilket innefattar såväl frågor om åtgärdens omfattning som frågan om förväxlingsrisk.

Tolkningssvårigheter och verkställighetsproblem har uppstått avseende immateriella informationssystem

Specificering av fysiska informationssystem har såvitt känt inte vållat några problem i praktiken. När det gäller immateriella informationssystem har den hittillsvarande tillämpningen visat att det har uppstått vissa tolkningssvårigheter både vid tillståndsgivningen och vid verkställighet angående hur specifikt ett avläsningsbart informationssystem måste anges.

SIN har vid granskningen av användningen av hemlig dataavläsning uppmärksammat att åklagarens ansökningar om hemlig dataavläsning inte alltid har varit tillräckligt specificerade. Ansökningarna som

SIN har granskat har bl.a. omfattat sociala medier och andra internetbaserade tjänster, utan angivande av användarkonto eller någon på motsvarande sätt avgränsad del av tjänsterna. Det medför enligt SIN att delar av den prövning som ska göras av rätten i praktiken har förskjutits till åklagaren eller den verkställande myndigheten. Det innebär också en förväxlingsrisk eftersom det är möjligt att på t.ex. en mobiltelefon, surfplatta eller dator använda flera olika användarkonton till en internetbaserad tjänst. Enligt SIN är det därför inte tillräckligt att ansökan och tillstånd till hemlig dataavläsning utformas så att tvångsåtgärden avser ett till den misstänkte hörande, men inte med ett användarnamn eller liknande specificerat, konto som finns på en internetbaserad tjänst. Det är inte heller tillräckligt att tjänsten används med hjälp av en viss elektronisk utrustning. Se nämndens uttalanden med beslut av den 29 mars 2023, dnr 43-2022, respektive den 20 juni 2023, dnr 44-2022.

SIN:s granskningar visar på brister i den praktiska tillämpningen när det gäller specificeringen av immateriella informationssystem. Vi bedömer dock att kravet på att i tillståndet ange vilket avläsningsbart informationssystem som tillståndet avser är tydligt och uppfyller de rättssäkerhetskrav som ställs på lagstiftningen. I de fall åtgärden inte är tillräckligt specificerad, ska den inte heller tillåtas. Vi bedömer inte att det finns något behov av ändringar i regelverket i detta avseende. Nämndens uttalande ger dock anledning att framhålla följande. Specifika uppgifter om vilka kommunikations- och lagringstjänster och därtill hörande användarkonton eller motsvarande som finns åtkomliga i en elektronisk kommunikationsutrustning är av naturliga skäl oftast inte möjliga att specificera på förhand, innan informationssystemet har lästs av. I praktiken kan det därför ibland bli fråga om hemlig dataavläsning i två steg. I det första steget får ansökan och tillståndet avse själva informationssystemet, exempelvis en mobiltelefon med visst IMEI-nummer eller det fysiska informationssystem från vilket ett visst telefonnummer används. En sådan angivelse får vanligtvis anses tillräckligt specificerat för att identifiera själva informationssystemet och kopplingen till den berörde. Vid en första hemlig dataavläsning kan det framkomma mer specifika uppgifter om t.ex. olika användarnamn och konton eller tjänster som finns tillgängliga från själva mobiltelefonen. Därefter kan i ett andra steg den nya ansökan och det nya tillståndet avse den specifika molntjänsten, exempelvis ”Facebookkontot XX”. Avgörande är att tillståndet avgränsas

på ett rättssäkert sätt. Även andra identifieringsfaktorer än t.ex. ett specificerat användarnamn eller konto bör därför kunna användas. Exempelvis bör ”det eller de Facebook-konton som används från den aktuella utrustningen, om det inte är uppenbart att de tillhör en annan person än den misstänkte” utgöra en tillräckligt rättssäker och specifik avgränsning. Det är oaktat typ av molntjänst eller teknisk utrustning angeläget att tillståndet inte lämnar utrymme för missförstånd. Exempelvis kan kortfattade hänvisningar till enbart en längre siffer- eller teckenkombination (som ibland används för att unikt identifiera ett användarkonto) leda till att tillståndet inte går att verkställa om det t.ex. har förekommit ett skrivfel under ärendets behandling. Åtgärdens omfattning, som bör framgå redan av ansökan, måste uttryckligen framgå av tillståndet. Avgörande är att domstolen i det enskilda fallet kan ta ställning till den konkreta åtgärd som avses.

8.4.7 Särskilt om kravet att i tillståndet ange vem som är skäligen misstänkt

Förslag: I ett tillstånd till hemlig dataavläsning ska anges vem som är skäligen misstänkt för brottet eller brotten, om sådan uppgift finns.

Skälen för vårt förslag

I ett tillstånd till hemlig dataavläsning ska det enligt 18 § första stycket 5 lagen om hemlig dataavläsning anges vem som är skäligen misstänkt för brottet eller brotten, vid åtgärd som gäller rumsavlyssningsuppgifter. Bestämmelsen är utformad på detta sätt med 27 kap. 21 § femte stycket rättegångsbalken som förebild. Där stadgas att det i ett beslut att tillåta hemlig rumsavlyssning ska anges vem som är skäligen misstänkt för brottet eller brotten. Bestämmelserna framstår som något svårlästa. De ska inte läsas motsatsvis så att det i övriga fall *inte behövs* någon uppgift om vem som är skäligen misstänkt. Det som åsyftas i bestämmelserna är att uppgiften *inte ska anges i tillståndet* annat än vid hemlig rumsavlyssning respektive hemlig dataavläsning avseende rumsavlyssningsuppgifter.

Skälet till att regleringen ser ut på detta sätt är att bestämmelserna om hemliga tvångsmedel har tillkommit vid olika tidsperioder. Bestämmelsen i 27 kap. 21 § femte stycket rättegångsbalken har oförändrad flyttats över från den tidigare lagen om hemlig rumsavlyssning till den allmänna bestämmelsen om domstolsprövning och hemliga tvångsmedelsbeslut i rättegångsbalken. Varken kravet i lagen om hemlig rumsavlyssning på att ange vem som är skälig misstänkt i beslutet eller avsaknaden av motsvarande krav på övriga tvångsmedelsbeslut har motiverats närmare i förarbetena.

Vi bedömer dock att övervägande skäl talar för att det i alla tillstånd till hemlig dataavläsning bör anges vem som är skäligen misstänkt, om sådan uppgift finns. Uppgiften behövs under alla omständigheter för att domstolen, eller i förekommande fall åklagaren, ska kunna pröva saken. Vi återkommer i avsnitt 8.5.5 till frågor om dokumentation. Där föreslår vi att alla beslut och åtgärder som rör hemlig dataavläsning ska *dokumenteras*, vilket självklart innefattar uppgift om vem som är skäligen misstänkt för visst brott eller viss brottslighet. Att det samtidigt endast vid hemlig dataavläsning beträffande rumsavlyssningsuppgifter finns ett krav på att uppgiften *anges i tillståndet* framstår som svårförklarligt och riskerar att skapa otydligheter och tolkningssvårigheter. Härtill kommer att det i 18 § tredje stycket lagen om hemlig dataavläsning nyligen har införts en ytterligare särbestämmelse som stadgar att om beslutet med stöd av 4 a § fjärde stycket eller 6 § fjärde stycket avser den skäligen misstänkte ska det anges i beslutet.

Vi bedömer sammantaget att en ordning där det i ett tillstånd till hemlig dataavläsning alltid ska anges vem som är skäligen misstänkt, förutsatt att sådan uppgift finns, skulle vara tydligare och bättre bidra till att uppfylla de rättssäkerhetskrav som ställs på lagstiftningen. Vi föreslår därför att lydelsen i nuvarande 18 § första stycket 5 ska ändras på föreslaget sätt. Den nuvarande bestämmelsen i 18 § tredje stycket blir därmed överflödig och ska utgå.

8.5 Rättssäkerhetsgarantier vid verkställighet

8.5.1 Genomförande av hemlig dataavläsning

Bedömning: Kraven på hur hemlig dataavläsning ska genomföras uppfyller de rättssäkerhetskrav och krav på informationssäkerhet som ställs på lagstiftningen.

Detsamma gäller de bestämmelser om sekretess, tystnadsplikt, partsinsyn och behandling av personuppgifter som gäller för hemlig dataavläsning.

Skälen för vår bedömning

Nuvarande bestämmelser om genomförandet av hemlig dataavläsning

I 22–26 §§ lagen om hemlig dataavläsning finns ett antal verkställighetsbestämmelser som reglerar själva genomförandet av hemlig dataavläsning. Här finns bestämmelser om verkställighetsteknik, otillåten tilläggsinformation, medverkansskyldighet och särskilda aktsamhetskrav. Vi har närmare redogjort för dessa bestämmelser i avsnitt 3.2.12. I detta avsnitt behandlar vi även frågor om informationssäkerhet. Hemlig dataavläsning innebär som tidigare konstaterats en förhöjd risk för informationssäkerheten, se avsnitt 5.9. Detta beror framför allt på att verkställighet av hemlig dataavläsning tillåter utnyttjande av tekniska sårbarheter. De risker som åsyftas är framför allt risken att information sprids till obehöriga från det informationssystem som åtgärden avser, risken för minskad säkerhet i andra informationssystem än det som tillståndet avser och risken för att sårbarheter blir kända utanför kretsen av personer som ska vara betrodda med informationen (se prop. 2019/20:64 s. 164). Förenklat handlar informationssäkerhet alltså om rätt typ av information, till rätt person och vid rätt tillfälle. Detta ställer höga krav på rättssäkerheten i regelverket. Rättssäkerhetsgarantierna för hemlig dataavläsning är därför i vissa avseenden förstärkta i förhållande till bakomliggande tvångsmedel. Gränsen för vilken verkställighetsmetod som får användas avgörs av bestämmelserna om verkställighetsteknik i 22–23 §§, aktsamhets- och kvalifikationskraven i 25–26 §§ och rättens tillståndsbeslut inklusive eventuella villkor enligt 18 § första stycket 4. Härutöver har den verkställande myndigheten möjlighet att begära assistans av de operatörer

som bedriver verksamhet enligt lagen om elektronisk kommunikation, se 24 §. Vi återkommer till denna bestämmelse i nästa avsnitt.

Av betydelse för såväl rättssäkerheten som informationssäkerheten vid genomförandet av hemlig dataavläsning är vilka personer som tillåts ta del av uppgifterna. I detta avsnitt berör vi därför även kort de bestämmelser om sekretess, tystnadsplikt, partsinsyn och behandling av personuppgifter som gäller för hemlig dataavläsning. I avsnitt 3.2.12 och 3.3.1 har vi närmare utvecklat vilka bestämmelser som är tillämpliga i dessa avseenden. Utöver de regler om partsinsyn som framgår av rättegångsbalken och offentlighets- och sekretesslagen har det nyligen införts en rätt för den misstänkte och försvararen att efter väckt åtal och på begäran få en sammanställning över förundersökningens sidomaterial, se 23 kap. 21 a § andra stycket rättegångsbalken. Med sidomaterial avses sådant material som inte ingår i förundersökningsprotokollet eller anteckningarna från förundersökningen. Syftet med den nya bestämmelsen är att tydliggöra och tillförsäkra den misstänktes rätt till en rättvis rättegång (se prop. 2022/23:126 s. 185 ff. och 202).

Rättssäkerhetsgarantierna för genomförandet av hemlig dataavläsning är tillräckliga

När det gäller hur rättssäkerheten och informationssäkerheten upprätthålls i praktiken bör det framhållas att hemlig dataavläsning enligt 26 § lagen om hemlig dataavläsning verkställs av särskilt kvalificerade personer. Polismyndigheten har en särskild HDA-funktion på sin nationella operativa avdelning som hanterar alla frågor om och verkställighet av hemlig dataavläsning. Även vid Säkerhetspolisen sker verkställigheten av hemlig dataavläsning på en särskild enhet. På samma sätt har Tullverket en särskild enhet, ITC, som arbetar med hemliga tvångsmedel inklusive hemlig dataavläsning. Enheterna hanterar alla frågor om och verkställighet av hemlig dataavläsning. Företrädare för dessa myndigheter har till utredningen redogjort för verksamheten och de särskilt upprättade rutiner som finns för hemlig dataavläsning, där riskbedömningar beträffande informationssäkerheten görs i flera led. Företrädare för Polismyndigheten har särskilt redogjort för sina rutiner enligt följande.

Inför verkställighet

Inför inköp eller framtagande av ny teknik kontrolleras den tekniska lösningens infrastruktur och funktioner noggrant utifrån krav på informationssäkerhet. Informationssäkerhetsaspekter finns alltid med i kravställningen vid anskaffning av nya system och systemen är föremål för omfattande testning innan de tas i bruk. Rättsavdelningen gör rättsutredningar, konsekvensbedömningar och skyddsvärdeanalyser inklusive säkerhetsanalys beträffande nya system. I samband med detta bedömer man uppgifter om inre och yttre infrastruktur, säkerhetsfunktioner, loggning, krav på personal etc. Sammantaget påverkar alla dessa aspekter informationssäkerheten. Inför en ansökan om hemlig dataavläsning ska HDA-funktionen alltid kontaktas. Kontakten syftar till att det ska kunna göra en kartläggning och bedömning avseende det avläsningsbara informationssystemet. Genom testutrustning genomförs kontroller av tekniken och metoderna för att informationssäkerheten ska kunna säkerställas under verkställigheten.

Under verkställighet

HDA-funktionen har upprättade rutiner beträffande de olika arbetsmomenten vid verkställighet av hemlig dataavläsning, i syfte att säkerställa att användningen utförs korrekt och mot rätt person. Det finns bl.a. kontrollfunktioner för att exempelvis tillse att den som berörs inte har bytt telefon mellan kartläggningen och verkställighetsperioden. Hemlig dataavläsning verkställs endast av särskilt utbildad personal med den kompetens och erfarenhet som krävs för uppdraget. Alla de åtgärder som genomförs loggas och all användaraktivitet kan kontrolleras i efterhand.

Efter verkställighet

Inhämtade uppgifter exporteras endast till behörig personal. Det innebär att informationen lagras beständigt och tillgängliggörs för granskning (se figur 7.1 i avsnitt 7.2). Det är beställaren, dvs. åklagaren eller Säkerhetspolisen, som ansvarar för granskning och analys av materialet. I praktiken är det företrädare för den brottsbekämpande myndigheten som, efter delegation av åklagare, utför själva gransk-

ningen. Med hjälp av forensiska verktyg genomförs med jämna mellanrum särskilda kontroller av informationssäkerheten. Under dessa tester kontrolleras att informationssäkerheten är på minst samma nivå som tidigare, dvs. att inga nya sårbarheter eller liknade har kunnat identifierats efter det att verktygen har tagits bort från en enhet. Man följer också upp behörighetstilldelning och logganvändning för att säkerställa att endast behörig personal har tillgång till systemen och att inga otillåtna åtgärder vidtas.

De tekniska och andra anpassningar som har gjorts framstår sammantaget som tillräckliga för att uppfylla de rättssäkerhetskrav som ställs och begränsa riskerna för informationssäkerheten. SIN har inte gjort någon renodlad granskning av verkställigheten av hemlig dataavläsning. Av den allmänna efterhandskontroll som sker i form av SIN:s tillsynsverksamhet har dock annat inte framkommit än att bestämmelserna om genomförande av hemlig dataavläsning uppfyller de krav på rättssäkerhet och informationssäkerhet som ställs.

När det gäller risken för oönskad spridning av de uppgifter som hämtas in genom hemlig dataavläsning är det inte bara tekniken, utan även de personer som tillåts ta del av uppgifterna som har betydelse för riskbedömningen. Kretsen av personer som får ta del av uppgifter som hämtas in med stöd av hemlig dataavläsning är begränsad till företrädare för de brottsbekämpande myndigheterna och berörda parter samt i förekommande fall andra behöriga myndigheter. Nuvarande regler om sekretess, tystnadsplikt, partsinsyn och behandling av personuppgifter bedöms ge adekvat skydd för dessa uppgifter (jfr SOU 2018:61 s. 242 ff. och prop. 2019/20:64 s. 180 ff.).

Det ska i sammanhanget anmärkas att hemlig dataavläsning även kan användas vid internationellt informationsutbyte, exempelvis efter en begäran om internationell rättslig hjälp i brottmål eller en europeisk utredningsorder. Vi återkommer närmare till denna reglering i kapitel 10. Av tabell 6.3 i kapitel 6 framgår att det hittills endast förekommit ett fåtal tillstånd till hemlig dataavläsning vid internationellt informationsutbyte. Några mer långtgående slutsatser om de risker för informationssäkerheten och den personliga integriteten som hemlig dataavläsning har inneburit i detta avseende är därför inte möjliga att dra. Rent allmänt kan dock konstateras att det vid internationellt informationsutbyte finns risk för en förlorad kontroll över information och flödet av personuppgifter och att den nationella lagstiftningen inte kan säkerställa ett skydd för informationen. Informationen kan

t.ex. komma att användas för andra syften eller få en större spridning än vad som varit avsett. All användning av hemliga tvångsmedel vid internationellt informationsutbyte kan därför generellt sett anses innebära en ökad risk för informationssäkerheten och därmed även för den personliga integriteten (jfr *Hur står det till med den personliga integriteten? – En kartläggning av Integritetskommittén*, SOU 2016:41, s. 104). Samtidigt kan det konstateras att det finns särskilda bestämmelser i dataskyddslagstiftningen som reglerar överföringen av personuppgifter till tredje land och internationella organisationer (se 8 kap. brottsdatalagen [2018:1177] och 9 kap. lagen [2019:1182] om Säkerhetspolisens behandling av personuppgifter). Dessa bestämmelser syftar bland annat till att ge ett tillräckligt skydd för personuppgifterna vid sådana överföringar. Bestämmelserna innebär bland annat att uppgifterna endast får överföras när en viss skyddsnivå är säkerställd hos mottagaren. När det gäller överföring till EU-medlemsstater kan det konstateras att mottagarna är bundna av brottsdatadirektivet och därför har lagstiftning som motsvarar brottsdatalagen. De eventuella risker för informationssäkerheten och den personliga integriteten som hemlig dataavläsning kan innebära i detta avseende får enligt vår bedömning anses försvarliga för att kunna ge de brottsbekämpande myndigheterna mer effektiva verktyg i bekämpandet av den internationella brottsligheten.

Sammantaget uppfyller såväl bestämmelserna som reglerar själva genomförandet av hemlig dataavläsning som den hittillsvarande tillämpningen de krav på rättssäkerhet och informationssäkerhet som ställs på lagstiftningen. Vår bedömning innefattar även de bestämmelser om sekretess, tystnadsplikt, partsinsyn och behandling av personuppgifter som gäller för hemlig dataavläsning.

8.5.2 Särskilt om medverkansskyldigheten

Bedömning: Systemet med en skyldighet för vissa operatörer att medverka vid verkställighet uppfyller de rättssäkerhetskrav som ställs på lagstiftningen.

Skälen för vår bedömning

Den nuvarande medverkansbestämmelsen

I 24 § lagen om hemlig dataavläsning finns en särskild bestämmelse om skyldighet för operatörer som bedriver verksamhet enligt lagen (2022:482) om elektronisk kommunikation (LEK) att medverka vid verkställighet av hemlig dataavläsning. I betänkandet *Hemlig dataavläsning* SOU 2017:89 föreslog utredningen att det endast skulle införas en *möjlighet* för operatörerna att medverka vid verkställighet. Ställningstagandet byggde bl.a. på att operatörerna har ett samhällsansvar att bistå de brottsbekämpande myndigheterna och att det med de regler om personlig integritet och informationssäkerhet som föreslogs saknades skäl för operatörerna att avstå från att medverka. Utredningen ansåg vidare att en skyldighet att medverka skulle utgöra ett alltför stort intrång i operatörernas verksamhet. Förslaget mötte remisskritik, varvid det gjordes både principiella och praktiska invändningar mot förslaget. Regeringen delade de tveksamheter som många remissinstanser gav uttryck för inför en frivillig medverkan. En medverkansskyldighet bedömdes enligt regeringen dessutom som väl förenlig med det samhällsansvar som följer med den bedrivna verksamheten. I propositionen föreslogs därför en *skyldighet* för operatörer att medverka vid verkställighet. Regeringen framhöll samtidigt att de ingrepp som de brottsbekämpande myndigheterna vidtar hos den enskilde operatören ska vara proportionerliga och att tekniken ska vara anpassad efter vilka slags uppgifter som ska inhämtas. Med hänsyn till det begränsade antal fall av hemlig dataavläsning som det förväntades bli fråga om bedömdes det inte föreligga något behov av att införa en anpassningsskyldighet för operatörerna (jfr 19 § LEK). Förarbetena till medverkansbestämmelsen i 24 § lagen om hemlig dataavläsning finns i a. SOU s. 426 ff. samt prop. 2019/20:64 s. 176 ff. och 237 f.

I 3 § förordningen (2020:172) om hemlig dataavläsning finns närmare bestämmelser om vad som omfattas av medverkansskyldigheten. Enligt denna bestämmelse kan medverkan omfatta att operatören

1. tillhandahåller tillgänglig teknisk information om det avläsningsbara informationssystem som omfattas av beslutet om hemlig dataavläsning,

2. tillhandahåller tillgängliga upplysningar om vilka förbindelser som används av det avläsningsbara informationssystem som omfattas av beslutet om hemlig dataavläsning,
3. använder tillgängliga tekniska metoder enligt 22 § lagen om hemlig dataavläsning eller tillhandahåller möjlighet att använda sådana metoder, eller
4. tillhandahåller andra liknande tillgängliga åtgärder som kan användas för att möjliggöra verkställighet av hemlig dataavläsning.

Bestämmelsen är således inte uttömmande. Vilka specifika uppgifter en operatör ska bistå den verkställande myndigheten med beror på hur myndigheten formulerar sin begäran. Det kan t.ex. röra sig om att en operatör identifierar vilka tjänster en specifik användare har och vilka förbindelser den använder, ger råd avseende vilka tekniska hjälpmedel som kan användas, tillhandahåller möjlighet att installera tekniska hjälpmedel i operatörens nät för verkställighet eller bistår med andra liknande stödåtgärder (se a. prop. s. 237 f.). Den som medverkar har rätt till ersättning för de kostnader som uppstår vid sådan medverkan. Ersättning ska betalas av den verkställande myndigheten, se 24 § andra stycket lagen om hemlig dataavläsning. Post- och telestyrelsen (PTS) är tillsynsmyndighet enligt lagen om elektronisk kommunikation. PTS har tagit fram föreskrifter om ersättning vid medverkan i samband med verkställighet av hemlig dataavläsning (PTSFS 2021:6).

Rättssäkerhetsgarantierna för medverkansskyldigheten är tillräckliga

Företrädare för de största operatörerna har bekräftat att i de fall som hemlig dataavläsning krävt åtgärd från operatörerna har verkställigheten fungerat väl.

Företrädare för PTS har i kontakter med utredningen inte haft några särskilda synpunkter på den nuvarande lagstiftningen eller den hittillsvarande tillämpningen. I diskussioner med företrädare för operatörerna har främst frågor om omfattningen av medverkansskyldigheten samt risker för nät- och informationssäkerheten aktualiserats. Även formerna för dialogen mellan operatörerna och de brottsbekämpande myndigheterna har tagits upp. Det senare är en fråga som enligt vår bedömning inte kan behandlas inom ramen för detta betänkande. Vad gäller övriga frågeställningar har det inte framkommit något som

enligt vår bedömning tyder på att det finns behov av förändringar i regelverket i aktuellt avseende. Bestämmelserna i lagen om hemlig dataavläsning, t.ex. avseende proportionalitet och aktsamhet, gäller även i förhållande till operatörerna. För operatörerna gäller härutöver en särskild bestämmelse om tystnadsplikt i 32 § lagen om hemlig dataavläsning. Någon mer detaljerad omfattning av medverkansskyldigheten än den som redan är reglerad och exemplifierad i förordningsform framstår inte som ändamålsenlig eller lämplig att göra. De risker för nät- och informationssäkerheten som kan uppstå är enligt vår bedömning redan noggrant balanserade i lagen om hemlig dataavläsning. Det har inte framkommit något som tyder på att lagstiftningen är otillräcklig i detta avseende (se avsnitt 8.5.1). Det är därför vår samlade bedömning att de rättssäkerhetsgarantier som omgärdar medverkansskyldigheten är tillräckliga.

8.5.3 Användning av överskottsinformation

Förslag: Åklagare ska, utan några särskilt stadgade begränsningar och i likhet med vad som sedan den 1 oktober 2023 gäller för de bakomliggande tvångsmedlen, få besluta att uppgifter som har kommit fram vid användning av hemlig dataavläsning under förundersökning och i preventivlagsfallen får användas för ett annat ändamål än det som har legat till grund för åtgärden.

För det fall att bestämmelsen om överskottsinformation i inhämtningslagen ändras i enlighet med förslaget i SOU 2023:60, ska det, som en följd av ändringen, införas en motsvarande reglering om användning av överskottsinformation i inhämtningslagsfallen.

Bedömning: De bestämmelser om överskottsinformation som gäller vid särskild utlänningskontroll uppfyller de rättssäkerhetskrav som ställs på lagstiftningen.

Skälen för våra förslag och vår bedömning

Nuvarande bestämmelser om överskottsinformation

Överskottsinformation är uppgifter som kommer fram vid användning av hemliga tvångsmedel och som handlar om något annat än det brott eller den brottslighet som legat till grund för själva åtgärden. Frågan om användningen av överskottsinformation är därför av central betydelse ur ett rättssäkerhetsperspektiv.

Överskottsinformation från användningen av hemlig dataavläsning under förundersökning regleras i 28 § lagen om hemlig dataavläsning som hänvisar till 27 kap. 23 a § rättegångsbalken i dess lydelse före den 1 oktober 2023. Motsvarande bestämmelse i preventivlagsfallen regleras i 29 § lagen om hemlig dataavläsning som hänvisar till 12 § preventivlagen i dess lydelse före den 1 oktober 2023. Vid hemlig dataavläsning vid särskild utlänningskontroll och i inhämtningslagsfallen motsvarar reglerna om överskottsinformation de regler som gäller för bakomliggande tvångsmedel, se 30 och 31 §§ lagen om hemlig dataavläsning.

Gemensamt för bestämmelserna i 28–31 §§ är att överskottsinformation från hemlig dataavläsning alltid får användas för att förhindra förestående brott. Bestämmelserna i 28 och 29 §§ begränsar dock på olika sätt, bl.a. genom strafftrösklar, när förundersökning får inledas och brott får utredas på grund av överskottsinformation. Motsvarande begränsningar finns inte vid hemlig dataavläsning vid särskild utlänningskontroll och i inhämtningslagsfallen. Vid hemlig dataavläsning vid särskild utlänningskontroll får Säkerhetspolisen, om det inte finns hinder enligt andra bestämmelser, besluta att uppgifter som har kommit fram vid hemlig dataavläsning får användas för ett annat ändamål än det som har legat till grund för åtgärden. Detta framgår av 30 § lagen om hemlig dataavläsning som hänvisar till 5 kap. 23 § lagen om särskild kontroll av vissa utlänningar. Vid hemlig dataavläsning i inhämtningslagsfallen får uppgifter som kommit fram användas i en förundersökning endast efter tillstånd till hemlig övervakning av elektronisk kommunikation. Utan ett sådant tillstånd får dock inhämtade uppgifter ligga till grund för beslut om att inleda en förundersökning. Detta framgår av 31 § lagen om hemlig dataavläsning som hänvisar till alternativt återger vad som föreskrivs i 6–8 §§ inhämtningslagen.

De bestämmelser som det hänvisas till i 28 och 29 §§ lagen om hemlig dataavläsning, dvs. 27 kap. 23 a § rättegångsbalken respektive 12 § preventivlagen i dess lydelser före den 1 oktober 2023, har kritiserats för att vara otydliga, oförutsebara och alltför begränsande i förhållande till i vilken utsträckning överskottsinformation får användas. Det har även ansetts oförenligt med såväl kraven i regeringsformen som Europakonventionen att bestämmelserna saknar uttryckligt lagstöd för viss av lagstiftaren avsedd användning av överskottsinformation, t.ex. underrättelseverksamhet och andra ändamål än det som har legat till grund för åtgärden. Därtill har vissa av begränsningarna i enskilda fall ansetts kunna leda till att Sverige inte uppfyller Europakonventionens krav på att förhindra och utreda brott som begås mot enskildas privatliv. De närmare analyserna av bestämmelserna framgår av betänkandet *Rättssäkerhetsgarantier och hemliga tvångsmedel*, SOU 2018:61 s. 167 ff. I betänkandet föreslogs en revidering av bestämmelserna om överskottsinformation i rättegångsbalken och preventivlagen, i syfte att stärka rättssäkerheten och bättre uppfylla kraven på tydlighet och förutsebarhet samt för att stärka möjligheterna att utöva efterhandskontroll. Lagförslagen godtogs i det fortsatta lagstiftningsarbetet och trädde i kraft den 1 oktober 2023. Lagändringarna innebär att användningen av överskottsinformation enligt rättegångsbalken och preventivlagen inte längre begränsas av några s.k. straffrösklar och att överskottsinformation får användas även för andra ändamål än det som legat till grund för tillståndet, om det inte finns hinder enligt andra bestämmelser eller är oproportionerligt. Användningen av överskottsinformation kräver beslut från åklagare, se prop. 2022/23:126 s. 171 ff., 221 f. och 232 f.

Vidare föreslår utredningen om preventiva tvångsmedel i slutbetänkandet *Utökade möjligheter att använda preventiva tvångsmedel 2*, SOU 2023:60, att även användningsområdet för överskottsinformation i inhämtningslagen ska utvidgas. Förslaget innebär att överskottsinformation som har kommit fram vid inhämtning av uppgifter ska få användas utan särskilda begränsningar för ett annat ändamål än det som har legat till grund för tillståndet. Förslaget motsvarar vad som gäller för överskottsinformation enligt rättegångsbalken och preventivlagen, med den skillnaden att det inte är åklagare utan den verkställande myndigheten som ska besluta om användning av överskottsinformation. Förslaget är för närvarande under beredning.

Ändringarna i 27 kap. 23 a § rättegångsbalken och 12 § preventivlagen omfattar inte hemlig dataavläsning eftersom lagen om hemlig dataavläsning trädde i kraft efter att Utredningen om rättssäkerhetsgarantier vid användningen av vissa hemliga tvångsmedel redovisat sitt uppdrag (se prop. 2022/23:126 s. 179 f.). Inte heller lagförslaget avseende inhämtningslagen omfattar hemlig dataavläsning (se a. SOU s. 272 och 590 f.). Frågan om det behövs förändringar i bestämmelserna om överskottsinformation omfattas av vårt uppdrag (jfr a. prop. s. 180).

Användningsområdet för överskottsinformation ska ändras

Ändringarna av bestämmelserna om överskottsinformation i rättegångsbalken och preventivlagen samt motsvarande ändringsförslag i inhämtningslagen väcker frågan om det är ändamålsenligt och tillfredsställande ur ett rättssäkerhetsperspektiv att hantera överskottsinformation från hemlig dataavläsning annorlunda än överskottsinformation från bakomliggande hemliga tvångsmedel.

Med hänsyn till det strukturella sambandet mellan regelverken talar systematiska skäl för att användningsområdet för överskottsinformation från hemlig dataavläsning bör ändras på samma sätt som för de bakomliggande tvångsmedlen. Vid införandet av den nya lagen om hemlig dataavläsning ansågs att reglerna om överskottsinformation för hemlig dataavläsning ska följa de regler som gäller för överskottsinformation som kommit fram genom användandet av bakomliggande hemliga tvångsmedel (se prop. 2019/20:64 s. 168). Det som främst talar emot att ändra användningsområdet för överskottsinformation från hemlig dataavläsning är att hemlig dataavläsning kan ge upphov till en stor mängd överskottsinformation. I avsnitt 8.4.5 föreslår vi att ett tillstånd till hemlig dataavläsning ska förenas med villkor om vilka inhämtade uppgifter som inte får granskas. Vidare föreslår vi i avsnitt 8.5.6 nedan att inhämtade uppgifter som inte får granskas enligt villkoren för tillståndet, ska förstöras så snart det står klart att sådana uppgifter inhämtats. Våra förslag i avsnitt 8.4.5 och 8.5.6 innebär således att en stor del av den information som hämtas in genom hemlig dataavläsning kommer att förstöras. Denna information kommer med andra ord inte att omfattas av bestämmelserna om överskottsinformation. Härtill kommer att en helt grundläggande

princip för tvångsmedelsanvändning är att sådana åtgärder inte får användas i syfte att få fram överskottsinformation. Integritetsriskerna med ett ändrat användningsområde för överskottsinformation från hemlig dataavläsning ska därför inte överdrivas.

Ur integritetssynpunkt ska även beaktas att överskottsinformation handlar om information som myndigheterna redan har tillgång till. Att använda informationen en gång till får anses innebära ett marginellt ytterligare intrång i förhållande till det intrång som den ursprungliga inhämtningen och bearbetningen har inneburit. Samtidigt innebär användning av överskottsinformation för andra ändamål än det ursprungliga att informationen sprids, vilket i sin tur får anses en ökad risk för den personliga integriteten. En annan fråga som diskuterades i förarbetena bakom lagändringarna om överskottsinformation är risken för att hemliga tvångsmedel missbrukas för att komma åt överskottsinformation. Det skulle kunna argumenteras för att risken för missbruk är större avseende hemlig dataavläsning eftersom åtgärden möjliggör inhämtning av stora mängder lagrad information. Med hänsyn till de höga krav som ställs för åtgärdens användande och de starka rättssäkerhetsgarantier och andra kontrollmekanismer som omgärdar regelverket bedömer vi dock att ett ändrat användningsområde för överskottsinformation från hemlig dataavläsning inte innebär någon egentlig risk för missbruk. Härutöver bedömer vi att de analyser och noggranna intresseavvägningar som har gjorts i det tidigare lagstiftningsarbetet gör sig gällande även beträffande hemlig dataavläsning (se prop. 2022/23:126 s. 171 ff., 221 f. och 232 f. samt SOU 2023:60 s. 263 ff. och 579 ff.). Inom ramen för vårt uppdrag har vi inte funnit anledning att ifrågasätta dessa tidigare analyser och intresseavvägningar. Följande förtjänar dock att särskilt framhållas. Nuvarande reglering innebär som ovan konstaterats otillfredsställande begränsningar beträffande användningen av överskottsinformation i brottsbekämpningen. Som redogjorts för i det föregående får alla förestående brott förhindras, men när ett brott har påbörjats medger reglerna inte alltid användning av överskottsinformation för att avbryta brottet. Sådana begränsningar överensstämmer inte med det processrättsliga regelverket som genomsyras av principerna om fri bevisprövning och fri bevisföring. Behovet av att inte onödigtvis begränsa användningen av överskottsinformation får anses påtagligt. Överskottsinformation kan innehålla uppgifter som är viktiga för att utreda allvarlig brottslighet. Samtidigt får behovet av att förhindra

brott anses lika påtagligt som behovet av att utreda brott, oavsett brottets dignitet. Det finns vidare ett påtagligt behov av användning av överskottsinformation för andra ändamål, t.ex. användning av uppgifter om att barn far illa och som bör föranleda ett ingripande av socialnämnden eller uppgifter som av olika skäl är mycket viktiga för landets försvar (jfr *Överskottsinformation vid användning av hemliga tvångsmedel m.m.*, prop. 2004/05:143 s. 46). Ett utvidgat användningsområde är av vikt inte bara för en effektiv brottsbekämpning, utan även för enskilda brottsoffers befogade rätt till upprättelse. En förutsättning är att tillämpningen kan avgränsas på ett rättssäkert sätt. Vid all tvångsmedelsanvändning, liksom vid användningen av överskottsinformation från hemlig dataavläsning, gäller allmänna principer som bl.a. proportionalitetsprincipen. Denna princip har tidigare bedömts utgöra en fullgod avgränsning för användning av överskottsinformation. Det saknas anledning att i detta avseende göra någon annan bedömning. Proportionalitetsbedömningen innebär, tillsammans med de begränsningar som följer av bl.a. dataskydds- och sekretessregler, att regleringen blir tydlig och väl avvägd. Genom att införa ett krav på att det är åklagaren som beslutar om användningen av överskottsinformation ges därtill en god garanti för att integritetsintressena noggrant övervägs (se prop. 2022/23:126 s. 178 f.).

Sammantaget har det inte framkommit skäl att göra någon annan bedömning avseende användningen av överskottsinformation från hemlig dataavläsning under en förundersökning, i preventivlagsfallen och i inhämtningslagsfallen än vad som har gjorts beträffande användningen av överskottsinformation enligt rättegångsbalken, preventivlagen och inhämtningslagen. Vi föreslår därför att reglerna för användning av överskottsinformation från hemlig dataavläsning ändras på motsvarande sätt som för bakomliggande hemliga tvångsmedel enligt rättegångsbalken, preventivlagen och inhämtningslagen. De nuvarande begränsningarna i 28–29 §§ lagen om hemlig dataavläsning, genom hänvisningar till tidigare lydelser i 27 kap. 23 a § rättegångsbalken och 12 § preventivlagen, ska därför tas bort. Som en följd härav ska även hänvisningen till 13 § preventivlagen i dess tidigare lydelse tas bort (jfr prop. 2022/23:126 s. 233). På motsvarande sätt föreslår vi att de nya regler om användning av överskottsinformation som föreslås gälla enligt inhämtningslagen ska bli gällande även för hemlig dataavläsning i inhämtningsfallen. Förslagen bidrar till att säkerställa en välfungerande systematik i regelverket om hemliga tvångsmedel. För-

slaget innebär också en mer effektiv brottsbekämpning och en förstärkt rättssäkerhetsgaranti för enskilda, genom att regelverket blir tydligare.

När det gäller de bestämmelser om överskottsinformation som gäller för hemlig dataavläsning vid särskild utlänningskontroll överensstämmer dessa som konstaterat med bakomliggande tvångsmedel. Vi bedömer att dessa bestämmelser är tillräckligt tydliga och förutsebara. Bestämmelserna bedöms inte heller sätta några med Europakonventionen oförenliga gränser för när förundersökning får inledas och brott får utredas på grund av överskottsinformation. Bestämmelsen om överskottsinformation i 30 § lagen om hemlig dataavläsning bedöms därför uppfylla de rättssäkerhetskrav som ställs på lagstiftningen (jfr a. prop. s. 179 f.).

8.5.4 Granskning, bevarande och förstöring

Förslag: Upptagningar och uppteckningar från hemlig dataavläsning under en förundersökning ska bevaras i enlighet med de regler som infördes för de bakomliggande tvångsmedlen den 1 oktober 2023. Det innebär att allt material som huvudregel ska bevaras.

Om den misstänkte medger det ska upptagningar och uppteckningar få förstöras innan förundersökningen har lagts ned eller avslutats eller, om åtal har beslutats, målet har avgjorts slutligt.

För det fall att bestämmelsen om bevarande och förstöring i inhämtningslagen ändras i enlighet med förslaget i SOU 2023:60, ska det, som en följd av ändringen, införas en motsvarande reglering om bevarande och förstöring i inhämtningslagsfallen.

Bedömning: För det fall att bestämmelsen om bevarande och förstöring i preventivlagen ändras redaktionellt i enlighet med förslaget i SOU 2023:60, bör det, som en följd av ändringen, införas en motsvarande redaktionell ändring i 29 § lagen om hemlig dataavläsning.

I övrigt uppfyller bestämmelserna om granskning, bevarande och förstöring de rättssäkerhetskrav som ställs på lagstiftningen.

Skälen för våra förslag och våra bedömningar

Nuvarande bestämmelser om granskning, bevarande och förstöring

Bestämmelser om granskning, bevarande och förstöring av upptagningar och uppteckningar från användningen av hemlig dataavläsning regleras i 28–31 §§ lagen om hemlig dataavläsning. Med upptagningar och uppteckningar avses det material som är resultatet av den hemliga dataavläsningen (jfr SOU 2018:61 s. 207 f. med där gjorda hänvisningar). Bestämmelserna i 28–31 §§ lagen om hemlig dataavläsning motsvarar i princip de regler som gäller för bakomliggande tvångsmedel utom såvitt avser hemlig dataavläsning under en förundersökning.

I de delar upptagningar och uppteckningar från användningen av hemlig dataavläsning under en förundersökning är av betydelse ur brottsutredningssynpunkt ska de bevaras till dess förundersökningen har lagts ned eller avslutats eller, om åtal har beslutats, målet har avgjorts slutligt. De ska därefter förstöras. Detta framgår av 28 § lagen om hemlig dataavläsning som hänvisar till 27 kap. 24 § rättegångsbalken i dess lydelse före den 1 oktober 2023. Regeln om bevarande gäller både sådant material som är av betydelse för utredningen av det brott som legat till grund för beslutet om hemliga tvångsmedel och, i förekommande fall, vid användning av överskottsinformation (prop. 2004/05:143 s. 52). I de delar som upptagningarna och uppteckningarna är av betydelse för att förhindra förestående brott ska de bevaras så länge det behövs för att förhindra brott. När materialet inte längre behövs för detta ändamål ska det förstöras. Den tidigare utformningen av bestämmelsen om bevarande och förstöring i 27 kap. 24 § rättegångsbalken har kritiserats för att vara otydlig och ge uttryck för att det som bedöms sakna intresse från utredningssynpunkt inte ska bevaras. Eftersom det under pågående utredning kan vara svårt att göra en bedömning av vilket material som har betydelse kan en felaktig bedömning leda till att den misstänktes rätt till en rättvis rättegång åsidosätts. De närmare analyserna av bestämmelsen framgår av betänkandet *Rättssäkerhetsgarantier och hemliga tvångsmedel*, SOU 2018:61 s. 200 ff. I betänkandet föreslogs därför att begränsningen i bestämmelsen, dvs. att upptagningarna och uppteckningarna ska vara av betydelse från brottsutredningssynpunkt för att bevaras, skulle tas bort. Syftet med förslaget var att förenkla tillämpningen och få en bättre överensstämmelse med Europadomstolens praxis och det sätt som regleringen tillämpats i praktiken. Lagförslaget godtogs i det fortsatta

lagstiftningsarbetet och trädde i kraft den 1 oktober 2023. Lagändringen innebär att alla upptagningar och uppteckningar från hemliga tvångsmedel, undantaget hemlig dataavläsning, under en förundersökning ska bevaras till dess förundersökningen läggs ned eller, om åtal väcks, till dess målet avgjorts slutligt. Genom ändringen tydliggörs att också material som används i en annan förundersökning alltjämt ska bevaras. Den bortre tidsgränsen för bevarandet knyts numera till den tidpunkt då förfarandet avslutas, vilket innebär att bevarandetiden anpassas efter förloppet i det enskilda fallet. Endast om den misstänkte medger det ska upptagningarna och uppteckningarna få förstöras innan dess. Förarbetena bakom lagändringen finns i prop. 2022/23:126 s. 182 ff. och 222.

I preventivlagsfallen avviker bestämmelserna om bevarande och förstöring något från vad som gäller för det bakomliggande tvångsmedlet, eftersom 29 § lagen om hemlig dataavläsning hänvisar till 13 § preventivlagen i dess lydelse före den 1 oktober 2023. Bestämmelsen i 13 § preventivlagen justerades något den 1 oktober 2023, som en följd av att strafftrösklarna i 12 § preventivlagen togs bort (se avsnitt 8.5.3 ovan). Vårt förslag i avsnitt 8.5.3 om att ta bort hänvisningen till 13 § preventivlagen i dess tidigare lydelse innebär dock att bestämmelserna om bevarande och förstöring i preventivlagsfallen åter kommer att överensstämma med vad som gäller för bakomliggande tvångsmedel. Det ska i sammanhanget noteras att Utredningen om preventiva tvångsmedel i sitt slutbetänkande föreslår en redaktionell ändring i preventivlagen, innebärandes att bestämmelserna om bevarande och förstöring oförändrade ska flyttas från 13 § till 14 § preventivlagen (se *Utökade möjligheter att använda preventiva tvångsmedel 2*, SOU 2023:60 s. 436 ff. och 570 f.). Förslaget är för närvarande under beredning. Någon motsvarande ändring i 29 § lagen om hemlig dataavläsning föreslås inte. Detta innebär att om både vårt lagförslag om att ta bort hänvisningen till 13 § preventivlagen i dess tidigare lydelse och den redaktionella ändringen i preventivlagen genomförs, kommer 29 § lagen om hemlig dataavläsning att sakna en hänvisning till preventivlagens bestämmelser om bevarande och förstöring. Vi återkommer nedan till att detta är något som måste tas i beaktande under beredningen av vårt förslag om att ta bort hänvisningen till 13 § preventivlagen i dess tidigare lydelse.

Vidare föreslår Utredningen om preventiva tvångsmedel i samma slutbetänkande, SOU 2023:60, att det, för det fall att reglerna om

överskottsinformation ändras i enlighet med deras förslag som redogjorts för ovan i avsnitt 8.5.3, ska införas en bestämmelse i inhämtningslagen om att i de delar uppteckningar innehåller sådana uppgifter om brott som får användas för att utreda brott ska de bevaras till dess att förundersökningen har lagts ned eller avslutats eller, om åtal har väckts, målet avgjorts slutligt. Förslaget är för närvarande under beredning.

Ändringarna i rättegångsbalken och preventivlagen omfattar inte hemlig dataavläsning eftersom lagen om hemlig dataavläsning trädde i kraft efter att Utredningen om rättssäkerhetsgarantier vid användningen av vissa hemliga tvångsmedel redovisat sitt uppdrag. Inte heller lagförslaget avseende inhämtningslagen omfattar hemlig dataavläsning (se SOU 2023:60 s. 272 och 590 f.). Frågan om det behövs förändringar i bestämmelserna om granskning, bevarande och förstöring omfattas av vårt uppdrag (jfr a. prop. s. 185).

Innebörden av granskningsbestämmelserna

Gemensamt för bestämmelserna i 28–31 §§ lagen om hemlig dataavläsning är att när hemlig dataavläsning har använts ska de upptagningar eller uppteckningar som gjorts granskas snarast möjligt. Granskningsbestämmelserna innebär också att kretsen av dem som får granska inhämtad information från hemlig dataavläsning är begränsad. Bestämmelserna syftar i denna del till att avgränsa den skara personer som får ta del av material från hemlig dataavläsning. Ur ett integritetsperspektiv är det angeläget att inte fler personer än nödvändigt tar del av uppgifterna. Skyndsamhetskravet återknyter till de grundläggande brottsbekämpande ändamålen med hemlig dataavläsning; att driva en brottsutredning framåt alternativt att förebygga, förhindra eller upptäcka viss allvarlig brottslighet (jfr *om vissa tvångsmedelsfrågor*, prop. 1988/89:124 s. 69 som hänvisar till SOU 1989:1). Med hänsyn till lagstiftarens avsikter med bestämmelsen och hur metoden för hemlig dataavläsning fungerar ska skyndsamhetskravet inte läsas som att alla uppgifter som inhämtas från ett informationssystem måste granskas. Det är inte heller så som bestämmelsen tillämpas i praktiken. Den inledande bearbetning som sker av inhämtade uppgifter syftar till att skilja ut den information som bedöms ha relevans för syftet med åtgärden, dvs. de uppgifter som enligt tillståndet till den

hemliga dataavläsningen ska tillgängliggöras för granskning (se figur 7.1 i avsnitt 7.2). Hemlig dataavläsning kan generera enorma mängder information. Långt ifrån all denna information har relevans för det brottsbekämpande ändamålet med åtgärden. Det är således inte nödvändigtvis möjligt eller ändamålsenligt att i detalj bearbeta allt det material som inhämtas. Det sagda innebär också att det inte heller nödvändigtvis är möjligt eller ändamålsenligt att bearbetningen omfattar ett krav på eftersökning av uppgifter som kan falla under förbudsbestämmelserna eller utanför villkoren för tillståndet. Först om det under bearbetningen påträffas otillåtna uppgifter ska dessa sorteras bort och förstöras (se avsnitt 8.5.6 nedan). Granskningsbestämmelserna ska alltså inte förväxlas med bevarande- och förstöringsbestämmelserna. Vi återkommer till dessa bestämmelser i det följande.

Med hänsyn till hur den praktiska tillämpningen av granskningsbestämmelserna fungerar, kan det övervägas att i 28–31 §§ ta bort hänvisningarna till skyndsamhetskravet, men att låta hänvisningarna till den personkrets som får granska inhämtade uppgifter kvarstå. Övervägande skäl talar dock mot en sådan lösning. Även om verkställighet av hemlig dataavläsning i många fall innebär inhämtning av omfattande informationsmängder, förekommer också ärenden som genererar mindre mängder information. Skyndsamhetskravet är lagfäst i övrig lagstiftning om hemliga tvångsmedel och återknyter till de grundläggande ändamålen med åtgärderna. Ett borttagande av skyndsamhetskravet i lagen om hemlig dataavläsning skulle därmed framstå som en både omotiverad och otydlig avvikelse från systematiken i tvångsmedelslagstiftningen. Vi bedömer sammantaget att såväl regelverket kring granskningen som den praktiska tillämpningen av granskningsbestämmelserna i lagen om hemlig dataavläsning får anses förenliga med kraven i regeringsformen och Europakonventionen (jfr bl.a. SOU 2018:61 s. 200 ff.). Bestämmelserna om granskning uppfyller därmed de rättssäkerhetskrav som ställs på lagstiftningen.

Tydligare bestämmelser om bevarande och förstöring

Ändringen av bestämmelsen i 27 kap. 24 § rättegångsbalken om bevarande och förstöring väcker dock frågan om det är ändamålsenligt och tillfredsställande ur ett rättssäkerhetsperspektiv att uppgifter som hämtas in genom hemlig dataavläsning under förundersökning ska

hanteras annorlunda än uppgifter som hämtas in med bakomliggande tvångsmedel.

Nuvarande reglering innebär som ovan konstaterats otillfredsställande otydligheter som riskerar att komma i konflikt med den enskildes rätt till en rättvis rättegång enligt Europakonventionen. De argument som framhållits för att revidera den tidigare bevarande- och förstörandebestämmelsen i rättegångsbalken gör sig gällande även beträffande hemlig dataavläsning. Inom ramen för vårt uppdrag har vi inte funnit anledning att ifrågasätta dessa tidigare analyser och intresseavvägningar. Vi stannar därför vid att hänvisa till dessa, se prop. 2022/23:126 s. 182 ff. och 222. Eftersom metoden för hemlig dataavläsning skiljer sig från övriga hemliga tvångsmedel är det dock nödvändigt att härutöver göra några särskilda överväganden beträffande hemlig dataavläsning.

Enligt företrädare för de brottsbekämpande myndigheterna bevaras redan i dag i princip alla uppgifter som hämtas in genom hemlig dataavläsning under förundersökning till dess förundersökningen har lagts ned eller avslutats eller, om åtal väckts, målet har avgjorts slutligt. Skälet till att nästan inget material från hemlig dataavläsning förstörs på förhand är att den nuvarande bestämmelsen om bevarande och förstöring anses svårtolkad, samt att det får anses följa av Europadomstolens praxis att det finns ett begränsat utrymme för att förstöra material i ett tidigt skede. Att låta den nya bestämmelsen i 27 kap. 24 § rättegångsbalken om bevarande och förstöring omfatta även uppgifter från hemlig dataavläsning under förundersökning skulle därför närmast innebära en anpassning till hur reglerna redan tillämpas.

Det som främst talar emot att införa en motsvarande bestämmelse är de stora mängder information som hemlig dataavläsning kan generera. I förhållande till övriga hemliga tvångsmedel innebär hemlig dataavläsning generellt sett inhämtning av en mycket större mängd information. Det är framför allt hemlig dataavläsning med stöd av 2 § första stycket 6 lagen om hemlig dataavläsning som genererar stora mängder lagrad information. Metoden för hemlig dataavläsning kan förenklat jämföras med en husrannsakan av ett elektroniskt informationssystem. Med hänsyn till hur metoden fungerar är det ofta inte möjligt att redan i inhämtningsfasen begränsa inhämtningen av all information (se avsnitt 6.2.5 och 7.3.2). Däremot är det ofta direkt efter inhämtningen möjligt att göra en snävare filtrering av informationen.

Det kan därför övervägas om det bör införas en ventil för bevarandet av uppgifter som kan anses vara uppenbart utan betydelse för utredningen.

En ordning där uppgifter som är uppenbart utan betydelse för utredningen måste bevaras framstår inte som ändamålsenlig med tanke på syftet med hemlig dataavläsning. Kravet på bevarande av sådana uppgifter kan även i vissa fall framstå som svårmotiverat ur ett integritetsperspektiv (jfr SIN:s remissyttrande över SOU 2018:61 av den 14 november 2018, dnr 108-2018). En möjlighet att förstöra uppgifter som uppenbart saknar betydelse för utredningen skulle också stå i bättre överensstämmelse med den dataskyddsrättsliga principen om uppgiftsminimering. Härutöver kan det principiellt ifrågasättas om det är rimligt att ålägga de brottsbekämpande myndigheterna en ovillkorlig skyldighet att använda stora serverutrymmen för att bevara lagrade uppgifter från hemlig dataavläsning. I praktiken handlar det ju oftast om bevarande av kopior på uppgifter som den berörde redan har lagrade.

Ett alternativ skulle därför vara att, tillsammans med införandet av en ny bestämmelse som motsvarar den nyligen införda i rättegångsbalken, införa en ventil som möjliggör omedelbar förstöring av uppgifter som uppenbart saknar betydelse för utredningen. Detta var något som SIN förordade under lagstiftningsarbetet avseende ändringen av 27 kap. 24 § rättegångsbalken. I propositionen bakom lagändringen ansåg regeringen dock att en möjlighet till förstöring av material som är uppenbart utan betydelse skulle kunna innebära att reglerna inte är förenliga med Europadomstolens praxis.

Den praxis som åsyftades var de avgöranden där Europadomstolen har fällt Finland för att material från hemliga tvångsmedel förstörts under utredningsstadiet. Se Europadomstolens domar den 8 december 2009 i målet Janatuinen mot Finland, nr 28552/05, och den 30 juni 2009 i målet Natunen mot Finland, nr 21022/04. Båda målen avsåg hemlig avlyssning av telefontrafik (motsvarande hemlig avlyssning av elektronisk kommunikation). I båda målen hade åklagaren åberopat ett urval av de inspelningar av telefonsamtal som hade avlyssnats av polisen, till styrkande av att den tilltalade i respektive mål hade gjort sig skyldig till viss narkotikabrottslighet. Såväl Janatuinen som Natunen begärde att få tillgång till inspelningar av andra avlyssnade samtal än de som lades fram i målet. Dessa samtal skulle enligt de tilltalade visa att det var annat än narkotika som samtalen rörde. Polisen hade dock förstört alla inspelningar som inte åberopats som bevisning. Skälet

till detta var att inspelningarna hade bedömts sakna betydelse i målet respektive bedömts inte handla om någon brottslig verksamhet. Sådana inspelningar var inte heller tillåtna att behålla enligt den nationella lagstiftningen. Europadomstolen fann i båda fallen att agerandet hade inneburit en kränkning av de misstänktas rätt till en rättvis rättegång, eftersom besluten att förstöra materialet hade medfört att varken domstolen eller den misstänkte fått möjlighet att bedöma om materialet varit relevant eller inte. I sammanhanget finns anledning att särskilt framhålla punkt 47 i målet Nantunen mot Finland:

> Even though the police and the prosecutor were obliged by law to take into consideration both the facts for and against the suspect, a procedure whereby the investigating authority itself, even when cooperating with the prosecution, attempts to assess what may or may not be relevant to the case, cannot comply with the requirements of Article 6 § 1.
>
> Moreover, it is not clear to what extent the prosecutor was, in fact, involved in the decision to destroy those recordings which were not included in the case file. In this case, the destruction of certain material obtained through telephone surveillance made it impossible for the defence to verify its assumptions as to its relevance and to prove their correctness before the trial courts.

En felaktig bedömning kan alltså gå ut över både möjligheterna att utreda och lagföra brottet och den misstänktes möjlighet att förbereda sitt försvar. Det kan i sin tur leda till att den misstänktes rätt till en rättvis rättegång enligt artikel 6 i Europakonventionen åsidosätts. Vidare ansåg regeringen att de svårigheter som är förenade med en sådan bedömning i ett tidigt skede, även med ett uppenbarhetsrekvisit, talar emot införandet av en sådan möjlighet (se prop. 2022/23:126 s. 184).

Det kan konstateras att Europadomstolens praxis på området avser information som har hämtats in genom hemlig avlyssning av elektronisk kommunikation, s.k. HAK-uppgifter. HAK-uppgifter utgör information som den berörde inte själv har tillgång till, annat än om denne t.ex. har spelat in sina egna samtal. HAK-uppgifter innehåller också generellt sett stora mängder information om innehållet i olika typer av samtal och meddelanden. Det skulle därmed kunna argumenteras för att Europadomstolens praxis inte tar sikte på lagrade uppgifter som har hämtats in med stöd av 2 § första stycket 1–3 eller 6 lagen om hemlig dataavläsning. Sådana uppgifter utgör ju information som den berörde själv har tillgång till eftersom den hemliga dataavläsningen bara utgör en spegling av uppgifterna. Ett uppenbar-

hetsrekvisit innebär emellertid ett krav på att inget som kan antas vara av intresse för den misstänktes försvar får förstöras i förtid. Råder det minsta tvekan om uppgifternas betydelse bör de bevaras, såvida inte åklagaren tillsammans med den misstänkte eller dennes försvarare gör en annan bedömning. Några generella exempel på uppgifter som uppenbart saknar betydelse för utredningen har inte kunnat konkretiseras. Användningsområdet för och behovet av en ventil framstår mot sammantaget som mycket begränsat. Även om det kan bedömas förenligt med Europadomstolens praxis att införa en ventil för att omedelbart förstöra uppgifter som uppenbart saknar betydelse för utredningen, framstår inte behovet härav som tillräckligt starkt. Slutsatsen är med andra ord att sådan information som bedöms irrelevant alltjämt ska bevaras, såvida informationen inte ska förstöras med stöd av bestämmelserna i 23 eller 27 §§, se avsnitt 8.5.6 nedan. Det ska i sammanhanget framhållas att uppgifter som inte får inhämtas eller granskas i enlighet med villkor i 18 § första stycket 4 lagen om hemlig dataavläsning ska hanteras vid sidan av bestämmelserna om förstörande och bevarande. I avsnitt 8.5.6 nedan föreslår vi bl.a. att det ska införas ett krav som innebär att sådana otillåtna uppgifter ska förstöras så snart det är möjligt. Vi bedömer sammantaget att det inte finns behov av att införa en möjlighet att omedelbart förstöra uppgifter som uppenbart saknar betydelse för utredningen.

Övervägande skäl talar därmed för att hantera upptagningar och uppteckningar från hemlig dataavläsning under förundersökning och i inhämtningslagsfallen på samma sätt som upptagningar och uppteckningar från bakomliggande tvångsmedel hanteras. Vi föreslår därför att hänvisningen i 28 § lagen om hemlig dataavläsning till den tidigare lydelsen i 27 kap. 24 § rättegångsbalken tas bort och ersätts med en ordinarie hänvisning till aktuell lydelse. Vidare föreslår vi att hänvisningen i 31 § lagen om hemlig dataavläsning till nuvarande 8 § inhämtningslagen tas bort och ersätts med en hänvisning till 7 § inhämtningslagen i den lydelse som utredningen om preventiva tvångsmedel föreslår (se SOU 2023:60 s. 60). Förslagen innebär i detta avseende en tydligare reglering för tillämparen och en anpassning till hur reglerna redan tillämpas. Förslaget bidrar också till att säkerställa att en välfungerande systematik i regelverket om hemliga tvångsmedel upprätthålls. Förslagen bedöms innebära en mer effektiv brottsbekämpning och en förstärkt rättssäkerhetsgaranti för enskilda.

När det gäller bestämmelserna om bevarande och förstöring i preventivlagsfallen gör vi följande principiella bedömning. Dessa bestämmelser bör även fortsättningsvis överensstämma med bakomliggande tvångsmedel (jfr prop. 2019/20:64 s. 171 f.). Detta blir också en indirekt följd av vårt förslag i avsnitt 8.5.3 om att hänvisningen i 29 § lagen om hemlig dataavläsning till 13 § preventivlagen i dess tidigare lydelse ska tas bort. Under beredningen av vårt förslag härom måste hänsyn tas till de redaktionella förslag på ändringar i preventivlagen som för närvarande är under beredning. För det fall att bestämmelsen om bevarande och förstöring i preventivlagen ändras redaktionellt i enlighet med förslaget i SOU 2023:60, bör det, som en följd, införas en motsvarande ändring i 29 § lagen om hemlig dataavläsning. Med andra ord; om bevarande- och förstörandebestämmelserna i 13 § preventivlagen flyttas till 14 § samma lag, bör hänvisningen i 29 § lagen om hemlig dataavläsning utvidgas till att omfatta även 14 § preventivlagen. Behovet av en sådan följdändring är som framgår beroende av utfallet av olika lagförslag. Vi lämnar därför inte något lagförslag härom. Under alla omständigheter bör det säkerställas att bestämmelserna om bevarande och förstöring i preventivlagsfallen även fortsättningsvis överensstämmer med bakomliggande tvångsmedel. Det kan därför förväntas att det under beredningen av vårt lagförslag görs ett ställningstagande i fråga om hänvisningen i 29 § lagen om hemlig dataavläsning, utifrån då gällande bestämmelser i preventivlagen.

I övrigt bedöms bestämmelserna om granskning, bevarande och förstöring av materialet förenliga med kraven i regeringsformen och Europakonventionen (jfr SOU 2018:61 s. 200 ff. och prop. 2022/23:126 s. 185).

8.5.5 Dokumentation

Förslag: Beslut och åtgärder som rör hemlig dataavläsning ska dokumenteras.

Skälen för vårt förslag

Det saknas en lagstadgad dokumentationsskyldighet

I dag finns ingen lagstadgad skyldighet att dokumentera användningen av hemlig dataavläsning. Den 1 oktober 2023 infördes en lagstadgad skyldighet att dokumentera beslut och åtgärder som rör hemliga tvångsmedel enligt rättegångsbalken och preventivlagen. Detta framgår av 27 kap. 35 § rättegångsbalken och 19 § preventivlagen. Det nya dokumentationskravet är tillämpligt även vid användning av hemliga tvångsmedel enligt 5 kap. 5 och 6 §§ lagen om särskild kontroll av vissa utlänningar. I dessa bestämmelser, som inte särskilt reglerar frågan om dokumentation, anges att reglerna i 27 kap. rättegångsbalken ska tillämpas i övrigt. I övrigt berörs inte användningen av hemlig dataavläsning av lagändringarna.

Bakgrunden till att det infördes en dokumentationsplikt var att Utredningen om rättssäkerhetsgarantier vid användningen av vissa hemliga tvångsmedel (SOU 2018:61) vid sin översyn fann brister i dokumentationen om användningen av hemliga tvångsmedel, både under och utanför en förundersökning. Att dokumentationen inte i samtliga fall har varit fullgod framgår också av SIN:s uttalanden om hemliga tvångsmedel (se bl.a. nämndens uttalanden av den 16 november 2022, dnr 58-2020 och den 14 december 2022, dnr 106-2022). Av nämndens uttalanden framgår att en avsaknad av dokumentation är bekymmersam, eftersom förutsättningarna för granskning i efterhand försämras. Som utredningen anger försvårar en bristfällig dokumentation också den enskildes möjlighet till efterhandskontroll. I syfte att stärka den enskildes möjlighet till efterhandskontroll samt förutsättningarna för tillsynen infördes därför ett krav i lag på att beslut och åtgärder som rör hemliga tvångsmedel ska dokumenteras. Förarbetena bakom lagändringen finns i prop. 2022/23:126 s. 180 ff. och 224 f.

Utredningen om preventiva tvångsmedel har i sitt slutbetänkande föreslagit att det även i inhämtningslagen ska införas ett lagstadgat dokumentationskrav, med bestämmelserna i rättegångsbalken och

preventivlagen som förebild (se *Utökade möjligheter att använda preventiva tvångsmedel 2*, SOU 2023:60). Förslaget är för närvarande under beredning.

Det ska införas ett dokumentationskrav för hemlig dataavläsning

Med hänsyn till det strukturella sambandet mellan regelverken bör ett motsvarande dokumentationskrav införas även beträffande hemlig dataavläsning. SIN har redan i samband med ikraftträdandet av lagen om hemlig dataavläsning framhållit behovet av ett lagstadgat dokumentationskrav (se nämndens remissyttrande över SOU 2017:89 av den 20 februari 2018, dnr 193-2017). De argument som framhållits för att införa ett dokumentationskrav i rättegångsbalken, preventivlagen och inhämtningslagen gör sig gällande även beträffande lagen om hemlig dataavläsning. Det saknas anledning att göra någon annan bedömning för hemlig dataavläsning än för bakomliggande tvångsmedel. Inom ramen för vårt uppdrag har vi inte funnit anledning att ifrågasätta eller vidareutveckla de analyser och intresseavvägningar som gjorts i det tidigare lagstiftningsärendet. Vi stannar därför vid att hänvisa till dessa, se prop. 2022/23:126 s. 180 ff. och 224 f. Som framhållits i det tidigare lagstiftningsarbetet är det inte ändamålsenligt med en dokumentationsskyldighet som är för detaljerad. Ytterligare riktlinjer om dokumentationsskyldigheten kan t.ex. utfärdas av Åklagarmyndigheten (jfr prop. 2022/23:126 s. 182).

Vi föreslår därför att det ska införas en lagstadgad skyldighet att dokumentera beslut och åtgärder som rör hemlig dataavläsning. Förslaget om ett dokumentationskrav för hemlig dataavläsning bidrar både till att säkerställa att en välfungerande systematik i regelverket om hemliga tvångsmedel upprätthålls och till att bättre uppfylla rättssäkerhetskraven i form av efterhandskontroll.

8.5.6 Särskilt om inhämtning av uppgifter i strid mot lagen om hemlig dataavläsning m.m.

Förslag: Vid verkställighet av hemlig dataavläsning ska teknik och tillvägagångssätt anpassas efter tillståndet. Kravet på att tekniken inte får göra det möjligt att hämta in någon annan typ av uppgift än vad som anges i tillståndet tas bort.

Om någon annan uppgiftstyp än vad som anges i tillståndet har hämtats in ska upptagningar och uppteckningar av dessa uppgifter omedelbart förstöras och Säkerhets- och integritetsskyddsnämnden underrättas. Upptagningar och uppteckningar av uppgifter som inte får inhämtas eller granskas enligt villkor meddelade med stöd av 18 § första stycket 4 ska förstöras i de delar de innehåller sådana uppgifter så snart det står klart att sådana uppgifter har inhämtats eller granskats.

Om det under eller efter verkställigheten kommer fram uppgifter som omfattas av förbudsbestämmelsen i 27 § ska granskningen av dessa uppgifter omedelbart avbrytas. Upptagningar och uppteckningar ska omedelbart förstöras i de delar som de omfattas av förbudet.

Bedömning: I övrigt uppfyller bestämmelserna i 23 och 27 §§ de rättssäkerhetskrav som ställs på lagstiftningen.

Skälen för våra förslag och våra bedömningar

Inhämtning som strider mot lagen om hemlig dataavläsning

Inledningsvis finns skäl att göra skillnad på de olika typer av informationsinhämtning som strider mot lagen om hemlig dataavläsning samt vad som gäller om sådan informationsinhämtning ändå äger rum. Vid sidan om bestämmelserna om överskottsinformation och bevarandeskyldigheten finns i 23 och 27 §§ lagen om hemlig dataavläsning en bestämmelse om teknikanpassning och s.k. otillåten tilläggsinformation respektive en särskild förbudsbestämmelse. Bestämmelsen i 23 § handlar bl.a. om inhämtning av *uppgiftstyper* som inte omfattas av tillståndet, medan 27 § handlar om inhämtning av vissa *uppgifter* som omfattas av beslagsförbudet och avlyssningsförbudet i rättegångsbalken. Vi redogör närmare för dessa särskilda bestämmelser nedan.

Det ska i sammanhanget framhållas att också *uppgifter* som inhämtats i strid med villkor enligt 18 § första stycket 4 lagen om hemlig dataavläsning är att hantera vid sidan av bestämmelserna om överskottsinformation och bevarandeskyldigheten (se vidare avsnitt 8.4.5 och 8.5.3 ovan). Uppgifter som har hämtats in i strid med villkor utgör per definition uppgifter som omedelbart ska förstöras även om detta inte i dag framgår uttryckligen av lagtext. Närmare bestämmelser om åklagarnas hantering och förstöring av inhämtade uppgifter regleras i Åklagarmyndighetens rättsliga vägledning (jfr RÄV 2022:25).

Bestämmelsen i 23 § ska förtydligas

Bestämmelsen i 23 § lagen om hemlig dataavläsning saknar motsvarighet bland övriga hemliga tvångsmedel. Bestämmelsen ställer inledningsvis krav på att den teknik som används i samband med hemlig dataavläsning ska anpassas efter det tillstånd som beviljats. I bestämmelsen anges också att ”Tekniken får inte göra det möjligt att läsa av eller ta upp någon annan typ av uppgift än vad som anges i tillståndet”. Det innebär enligt författningskommentaren till bestämmelsen att om tillståndet exempelvis tillåter hemlig dataavläsning för att läsa av eller ta upp kommunikationsavlyssningsuppgifter ska det inte vara möjligt att med den teknik som används läsa av eller ta upp kameraövervakningsuppgifter. Om ett tekniskt hjälpmedel är konstruerat på så sätt att det i och för sig är möjligt att använda det för att läsa av eller ta upp olika uppgiftstyper krävs att hjälpmedlet är inställt på ett sådant sätt att det inte är möjligt att utan ändringar av inställningarna i hjälpmedlet komma åt andra uppgiftstyper än de som tillståndet avser (se prop. 2019/20:64 s. 236 f.). Bestämmelsen framstår dock som missvisande eftersom det i inhämtningsfasen i princip alltid är tekniskt möjligt att hämta in andra uppgiftstyper än de som anges i tillståndet. Bestämmelsen ger också intrycket av att det är enkelt att dela upp information, något som inte överensstämmer med den praktiska tillämpningen. Att särskilja kommunikationsavlyssningsuppgifter från kameraövervakningsuppgifter är knappast problematiskt. Däremot kan det konstateras att uppgiftstyperna i 2 § första stycket 1–3 respektive 6 sällan kan särskiljas före inhämtningen. Vi har därför i avsnitt 7.3 föreslagit en förtydligande huvudregel som innebär att ett typiskt tillstånd till hemlig dataavläsning omfattar alla

dessa uppgiftstyper. Införandet av en sådan huvudregel balanseras av att vi samtidigt föreslår tydligare bestämmelser om tillståndet (se avsnitt 8.4). Verkställigheten, som ska anpassas efter hur tillståndet i det enskilda fallet är utformat, omfattar inte bara inhämtning av uppgifter utan också viss inledande bearbetning i form av förädling, sortering och filtrering av inhämtade uppgifter (se figur 7.1 i avsnitt 7.2). För att kraven på ett tillstånd ska kunna uppfyllas i praktiken behöver inte bara verkställighetstekniken anpassas, utan också de instruktioner som ges i samband med verkställighet måste anpassas särskilt. Det är verkställande myndighet som ansvarar för att dessa anpassningskrav är uppfyllda (se avsnitt 8.5.1). Eftersom verkställighet av hemlig dataavläsning i praktiken inte bara handlar om teknikanpassning, utan också om det tillvägagångssätt som används i samband med verkställighet bör detta framgå uttryckligen av lagtext.

Vi föreslår därför att bestämmelsen i 23 § lagen om hemlig dataavläsning förtydligas enligt följande. Vid verkställighet av hemlig dataavläsning ska teknik och tillvägagångssätt anpassas efter tillståndet. Vi föreslår samtidigt, med hänsyn till hur hemlig dataavläsning går till i praktiken, att kravet på att tekniken inte får göra det möjligt att läsa av eller ta upp någon annan typ av uppgift än vad som anges i tillståndet ska tas bort. Någon eftergift av de rättssäkerhetsgarantier som omgärdar verkställighet av hemlig dataavläsning är dock inte avsedd. Vi bedömer att det redan av kravet på att teknik och tillvägagångssätt ska anpassas efter tillståndet följer att verkställighet av hemlig dataavläsning ska ske inom de ramar som uppställts för det enskilda tillståndet. Vidare föreslår vi att det i lagtext förtydligas att om en annan uppgiftstyp än som anges i tillståndet har hämtats in så utgör den uppgiften otillåten tilläggsinformation. Sådana uppgifter ska omedelbart förstöras och får inte användas till nackdel för någon i en brottsutredning. Våra förslag innebär en tydligare och mer förutsebar lagstiftning som undanröjer oavsiktliga begränsningar i nuvarande bestämmelse. Våra förtydliganden bedöms därför, tillsammans med våra förslag om tydligare bestämmelser om vad ett tillstånd till hemlig dataavläsning ska innehålla, kunna undanröja nuvarande verkställighetsproblem och de osäkerheter som i dag kan finnas kring ett tillstånds omfattning. Denna bedömning omfattar även det förtydligande tillägg som vi i det följande föreslår ska införas i samma bestämmelse.

Vi föreslår följande förtydligande tillägg. Upptagningar och uppteckningar av uppgifter som inte får inhämtas eller granskas enligt

villkor meddelade med stöd av 18 § första stycket 4 ska förstöras i de delar de innehåller sådana uppgifter så snart det står klart att sådana uppgifter har inhämtats eller granskats.

Förslaget i denna del innebär ett förtydligande av att inte bara inhämtade *uppgiftstyper* utan också inhämtade *uppgifter* kan utgöra otillåten tilläggsinformation. Vårt förslag innebär att det införs en uttrycklig bestämmelse om att uppgifter som har hämtats in i strid med villkor för inhämtningen ska förstöras så snart det står klart att sådana uppgifter inhämtats eller granskats. Exempelvis kan ett tillstånd ha förenats med villkor om att endast meddelanden som har skickats eller tagits emot efter en viss tidpunkt får inhämtas. Om den verkställande myndigheten, trots villkoret, har hämtat in meddelanden som har skickats eller tagits emot före angiven tidpunkt, utgör dessa meddelanden otillåten tilläggsinformation. Som vi tidigare har framhållit utgör sådana uppgifter per definition uppgifter som ska förstöras. Förslaget i denna del innebär därför närmast en kodifiering av vad som redan gäller. Vårt förslag innebär därutöver att uppgifter som enligt villkoren för tillståndet får inhämtas men inte granskas ska förstöras så snart det står klart att sådana uppgifter har inhämtats eller granskats. Förslaget i denna del innebär i praktiken att de uppgifter som enligt villkoren får inhämtas men inte granskas ska förstöras, efter att de sorterats och filtrerats bort i en initial bearbetningsfas. Det kan exempelvis handla om ett tillstånd som omfattar inhämtning av ett helt mejlkonto, men där endast mejl från ett visst datum och mellan vissa personer får granskas. Mejl som inte omfattas av granskningsvillkoren utgör otillåten tilläggsinformation som omedelbart ska förstöras i samband med bearbetningen av det inhämtade mejlkontot. Genom vårt förslag i denna del tydliggörs att hemlig dataavläsning innebär inhämtning av information i syfte att möjliggöra efterföljande bearbetning och granskning, se avsnitt 7.2 och figur 7.1. Som vi tidigare har framhållit går det många gånger inte att på förhand begränsa själva inhämtningen. Det sker därför en efterföljande sortering och filtrering av det inhämtade materialet för att skilja ut de uppgifter som den hemliga dataavläsningen syftar till att tillgängliggöra (jfr våra samverkande förslag i avsnitt 7.3.2, 8.4.4 och 8.4.5). Om förfarandet vid verkställighet hade möjliggjort en initial sortering och filtrering redan i inledningsskedet hade informationen alltså aldrig hämtats in. Av integritetsskäl bör det undvikas att information som aldrig har efterfrågats bevaras. Det skulle sam-

tidigt kunna argumenteras för att den personliga integriteten kränks om myndigheter kan hämta in information utan att denna bevaras så att inhämtningen kan kontrolleras i efterhand. Eftersom det är fråga om information som myndigheterna om det varit möjligt, hade underlåtit att hämta in och som aldrig blivit föremål för granskning gör sig detta skäl emellertid inte gällande. I stället bör sådan information förstöras enligt samma regelverk som när information har hämtats in av misstag. Som redogjorts för ovan har Europadomstolen funnit att beslut att förstöra HAK-uppgifter inneburit en kränkning av de misstänktas rätt till en rättvis rättegång, eftersom besluten medfört att varken domstolen eller den misstänkte fått möjlighet att bedöma om materialet varit relevant eller inte. Vårt förslag innebär emellertid att de uppgifter som kommer att förstöras är lagrade uppgifter som den berörde själv, till skillnad från inspelade telefonsamtal, bör ha tillgång till. Vidare är det fråga om information som har sorterats bort i ett tidigt skede och som således aldrig har granskats eller ens varit avsedd att användas. Förslaget bör mot denna bakgrund vara väl förenligt med Europadomstolens praxis på området. Förslaget är också väl förenligt med den dataskyddsrättsliga principen om uppgiftsminimering (jfr avsnitt 8.5.4). Övervägande skäl talar därmed för att införa en bestämmelse om förstöring av viss information i enlighet med vårt förslag. Förslaget bedöms innebära en förstärkt rättssäkerhetsgaranti för enskilda, i synnerhet i förhållande till våra förslag i avsnitt 7.3.2, 8.4.4 och 8.4.5. SIN:s tillsyn utgör en viktig kontrollmekanism för efterlevnaden av de villkor som ett tillstånd till hemlig dataavläsning förenas med. Vi bedömer att den allmänna underrättelseskyldighet som följer av 21 § tillförsäkrar att nämnden får underlag som kan läggas till grund för att bedöma om ett tillsynsärende bör initieras i detta avseende. Den bedömningen är inte beroende av om informationen finns kvar eller inte (jfr prop. 2019/20:64 s. 163). Någon ytterligare underrättelseskyldighet utöver den som följer av 21 § bedöms därmed inte nödvändig att införa. Vi återkommer i avsnitt 8.7 närmare till frågan om underrättelseskyldigheten till SIN.

Att uppgifterna ska förstöras överensstämmer med vad som gäller för uppgifter som omfattas av de s.k. beslagsförbuden och frågeförbuden i rättegångsbalken, se 27 kap. 2 § och 36 kap. 5 § rättegångsbalken. Regleringen om att uppgifterna inte får användas till nackdel för någon har inte någon lagfäst motsvarighet i någon annan författning. Med hänsyn till lagens ingripande karaktär har det dock ansetts

nödvändigt med tydliga och uttryckliga bestämmelser till skydd för rättssäkerheten (se prop. 2019/20:64 s. 163). I övrigt får bestämmelsen i 23 § därför anses uppfylla de rättssäkerhetskrav som ställs på lagstiftningen.

Förbudsbestämmelsen i 27 § ska förtydligas

Förbudet i 27 § lagen om hemlig dataavläsning om att inhämta vissa uppgifter motsvarar det beslagsförbud och det avlyssningsförbud som finns i rättegångsbalken, se 27 kap. 2 och 22 §§ rättegångsbalken. Enligt bestämmelsen ska uppgifter som omfattas av beslags- eller avlyssningsförbudet omedelbart förstöras. Förutom principen om lex specialis, måste det anses uppenbart att bestämmelserna om överskottsinformation och bevarandeskyldigheten inte gäller för uppgifter som omfattas av 23 och 27 §§ lagen om hemlig dataavläsning (jfr SOU 2018:61 s. 217). Något uttryckligt undantag från bevarandeskyldigheten behöver därför inte införas beträffande sådan information som enligt lagen om hemlig dataavläsning ska förstöras omedelbart. Däremot ska det framhållas att alla beslut och åtgärder som rör hemlig dataavläsning, även förstöring, omfattas av det nu föreslagna dokumentationskravet, se avsnitt 8.5.5.

Av bestämmelsens tredje stycke framgår att om det under verkställigheten kommer fram uppgifter som omfattas av första eller andra styckena ska verkställigheten omedelbart avbrytas och upptagningar och uppteckningar omedelbart förstöras i de delar som de omfattas av förbudet. Bestämmelsen har sin motsvarighet i 27 kap. 22 § tredje stycket rättegångsbalken. Med hänsyn till hur metoden för hemlig dataavläsning skiljer sig från bakomliggande tvångsmedel finns emellertid skäl att förtydliga bestämmelsen i 27 § tredje stycket lagen om hemlig dataavläsning för att bättre möta lagstiftarens avsikter. Bestämmelsen ger nämligen intrycket av att det under själva inhämtningen är enkelt att upptäcka uppgifter som omfattas av förbudsbestämmelsen och därvid avbryta pågående verkställighet. Detta är i själva verket möjligt endast när det är fråga om hemlig dataavläsning i realtid. Vid inhämtning av lagrade uppgifter är det svårt och ofta omöjligt att under pågående verkställighet göra en sådan bedömning. Detta gäller i synnerhet uppgifter som omfattas av det s.k. avlyssningsförbudet. Företrädare för de brottsbekämpande myndigheterna har framhållit att

sådana uppgifter i princip bara är möjliga att upptäcka först vid själva granskningen av de inhämtade uppgifterna. Vidare saknas det skäl att avbryta *verkställigheten* eftersom denna närmast kan jämföras med en husrannsakan och inte med HAK, som betraktas som den närmaste förebilden i rättegångsbalken. Bestämmelsen bör bättre möta lagstiftarens avsikt som är att förbudet ska gälla mot att ta del av uppgifter som omfattas av bestämmelsen. Bestämmelsen i 27 § tredje stycket bör därför förses med följande förtydligande. Om det under *eller efter* verkställigheten kommer fram uppgifter som omfattas av förbudsbestämmelsen, ska *granskningen av dessa uppgifter* omedelbart avbrytas. Upptagningar och uppteckningar ska omedelbart förstöras i de delar som de omfattas av förbudet. Ett sådant förslag innebär en tydligare och mer förutsebar lagstiftning som bättre överensstämmer med lagstiftarens avsikter. Någon ändring i sak är inte avsedd.

Beslags- och avlyssningsförbuden har tidigare funnits överensstämma med de krav som ställs på lagstiftningen (jfr SOU 2018:61 s. 160 ff.). Rättssäkerhetsgarantierna för att motverka avläsning och användning av otillåten tilläggsinformation vid hemlig dataavläsning är som redogjorts för högt ställda. Även denna bestämmelse får därför i övrigt anses uppfylla de rättssäkerhetskrav som ställs på lagstiftningen.

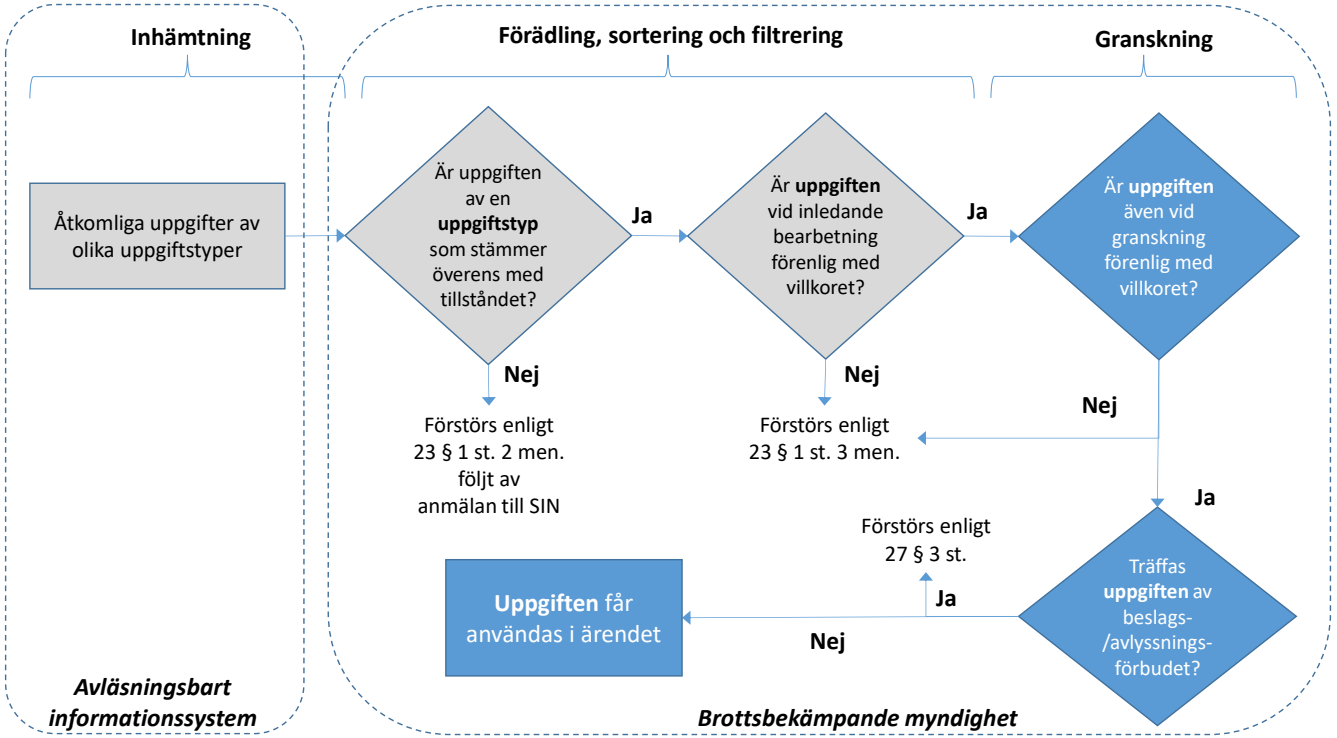
En tydligare reglering om förstöring av otillåten information

Våra förslag innebär tillsammans en tydligare reglering om förstöring av otillåten information. Bestämmelserna utgör undantag från huvudregeln om att allt material från hemlig dataavläsning ska bevaras (se avsnitt 8.5.3 ovan). Huvudregeln gäller alltså även sådant material som bedöms vara utan intresse för utredningen. Förutom den situation där den misstänkte medger förstöring av viss information innebär våra förslag att det finns ytterligare fyra undantagssituationer där olika delmängder inhämtad information ska förstöras så snart det är möjligt. Undantaget från huvudregeln om bevarande gäller om upptagningar eller uppteckningar av följande otillåtna uppgifter påträffas:

1. Uppgiftstyper som inte får inhämtas enligt tillståndet (2 §) ska förstöras enligt nu föreslagna 23 § första stycket andra meningen.
2. Uppgifter som inte får inhämtas enligt villkor för tillståndet (18 § första stycket 4) ska förstöras enligt nu föreslagna 23 § första stycket tredje meningen.
3. Uppgifter som inte får granskas enligt villkor för tillståndet (18 § första stycket 4) ska förstöras enligt nu föreslagna 23 § första stycket tredje meningen.
4. Uppgifter som omfattas av beslags- eller avlyssningsförbudet ska förstöras enligt nu föreslagna 27 § tredje stycket.

Förstöring av otillåtna uppgifter med stöd av 23 och 27 §§ kan illustreras med det flödesschema som framgår av figur 8.1.

Figur 8.1 Förstöring av vissa uppgifter med stöd av 23 och 27§§ lagen om hemlig dataavläsning



Det ska i sammanhanget framhållas att bevarande- och förstörandebestämmelserna inte ska förväxlas med granskningsbestämmelserna. Kravet i 28–31 §§ på att inhämtade uppgifter ska granskas snarast möjligt innefattar inte ett krav på att granska alla inhämtade uppgifter eller att leta efter uppgifter som faller utanför villkoren för tillståndet (se närmare härom i avsnitt 8.5.4 ovan). Förstörandeskyldigheten enligt 23 och 27 §§ blir således endast aktuell om det under eller efter inhämtningen påträffas uppgifter som omfattas av dessa bestämmelser. I enstaka fall kan det förekomma att de otillåtna uppgifterna aldrig gås igenom i detalj och därför heller aldrig identifieras. I dessa fall kommer de otillåtna uppgifterna att förstöras i enlighet med huvudregeln om bevarande och förstörande som framgår av 28–31 §§, dvs. om uppgifterna inte identifieras som otillåtna innan dess.

8.6 Underrättelse i efterhand till enskilda

Bedömning: Systemet med underrättelser till enskilda som berörts av hemlig dataavläsning uppfyller de rättssäkerhetskrav som ställs på lagstiftningen.

Skälen för vår bedömning

Nuvarande bestämmelser om underrättelse till enskilda

Syftet med underrättelseskyldigheten är bland annat att den enskilde ska få möjlighet att bedöma vilket integritetsintrång som åtgärden har inneburit och kunna reagera mot vad han eller hon kan anse ha varit en rättsstridig åtgärd. En skyldighet att lämna en sådan underrättelse har även ansetts kunna ha en återhållande verkan på användningen av hemliga tvångsmedel och bidra till att prövningen inför ett beslut sker på ett än mer noggrant sätt. Detta framgår av *Ytterligare rättssäkerhetsgarantier vid användandet av hemliga tvångsmedel, m.m.*, prop. 2006/07:133 s. 30.

Bestämmelser om underrättelse till enskilda vid hemlig dataavläsning under förundersökning och i preventivlagsfallen finns i 28–29 §§ lagen om hemlig dataavläsning. Genom hänvisningar i dessa bestämmelser gäller motsvarande regler om underrättelse till enskilda som gäller för bakomliggande tvångsmedel. Det som i bakomliggande be-

stämmelser anges om telefonnummer, annan adress eller en viss elektronisk kommunikationsutrustning gäller för ett avläsningsbart informationssystem.

Huvudregeln vid hemlig dataavläsning under förundersökning är att den som är eller har varit misstänkt för ett brott och även vissa innehavare av platser som berörts av verkställigheten ska underrättats om tvångsmedelsanvändningen i efterhand. Flera undantag finns från underrättelseskyldigheten. Exempelvis undantas fall där uppgifterna omfattas av utrikessekretess, försvarssekretess, förundersökningssekretess eller sekretess i underrättelseverksamhet. Har det på grund av sekretess inte kunnat lämnas någon underrättelse inom ett år från det att förundersökningen avslutades behöver det inte lämnas någon underrättelse. Enligt 14 b § förundersökningskungörelsen ska dock SIN underrättas härom. Förundersökningar angående ett antal brott som normalt handläggs av Säkerhetspolisen undantas också helt från underrättelseskyldighet.

För hemlig dataavläsning i preventivlagsfallen kan motsatt huvudregel sägas gälla, nämligen att underrättelse inte ska ske. Detta beror på att de brott som undantas från underrättelseskyldigheten är brott som faller inom Säkerhetspolisens verksamhetsområde, dvs. de flesta brott som kan föranleda hemlig dataavläsning i preventivlagsfallen. När det är fråga om brott som faller inom Polismyndighetens verksamhetsområde motsvarar däremot bestämmelserna om underrättelseskyldighet i allt väsentligt reglerna enligt rättegångsbalken.

När det gäller hemlig dataavläsning vid särskild utlänningskontroll och i inhämtningslagsfallen finns inte någon underrättelseskyldighet till enskild (se prop. 2019/20:64 s. 167 ff. och 241 ff.). Detta har motiverats av att det inte bör finnas någon sådan skyldighet i de brottsbekämpande myndigheternas underrättelseverksamhet (se prop. 2011/12:55 s. 105 ff.). Vidare angår lagen om särskild kontroll av vissa utlänningar terroristbrottslighet. Samma skäl gör sig därför gällande för att undanta tvångsmedelsanvändningen enligt denna lag från underrättelseskyldigheten som motiverat att sådana brott bör undantas från underrättelseskyldigheten vid förundersökningar i brottmål (jfr prop. 2006/07:133 s. 52).

Rättssäkerhetsgarantierna för underrättelse till enskilda är tillräckliga

De regler som enligt rättegångsbalken och preventivlagen gäller för underrättelse till enskilda har tidigare ansetts väl avvägda och förenliga med kraven i regeringsformen och Europakonventionen (se prop. 2006/07:133 och SOU 2018:61 s. 223 ff.). Det saknas skäl att beträffande hemlig dataavläsning vid särskild utlänningskontroll eller i inhämtningslagsfallen avvika från bakomliggande reglering. Den tillsyn som SIN utövar över hemlig dataavläsning bedöms tillsammans med andra rättssäkerhetsgarantier för åtgärderna uppfylla Europakonventionens krav på tillgång till ett effektivt rättsmedel (jfr prop. 2011/ 12:55 s. 107 f. och SOU 2017:89 s. 420 f.).

När det gäller hur systemet med underrättelse till enskilda i praktiken lever upp till de krav som ställs har det inte framkommit annat än att systemet beträffande hemlig dataavläsning fungerar tillfredsställande. Däremot har SIN under år 2021 inkommit med en framställning till regeringen angående åtgärder för att förbättra enskildas rättssäkerhet i fråga om underrättelser om användning av hemliga tvångsmedel (se Ju2021/01982). I framställningen anges bl.a. att det finns brister i dagens reglering som bör åtgärdas. Mot bakgrund av SIN:s framställning har Utredningen om utökade möjligheter att använda hemliga tvångsmedel haft i uppdrag att bedöma om det finns ett behov av att ändra reglerna om underrättelse till enskild om användning av hemliga tvångsmedel. Utredningen föreslår i sitt slutbetänkande *Bättre möjligheter att verkställa frihetsberövanden*, SOU 2022:50, ett antal ändringar i reglerna om underrättelse till en enskild vid användning av hemliga tvångsmedel under förundersökning för att åtgärda de problem som SIN lyft fram. Utredningens förslag innebär i korthet att grundregeln om underrättelse behålls men förtydligas och att slutpunkten för när man får avstå från underrättelse ändras. Utredningen föreslår att den tidsfrist efter vilken åklagaren får avstå från underrättelse till enskild inte längre ska utgå från förundersökningens avslutande, utan i stället ska löpa under ett år och sex månader från det att tvångsmedelsanvändningen avslutades. Oavsett om förundersökningen vid denna tidpunkt har avslutats eller fortfarande pågår föreslår Utredningen om utökade möjligheter att använda hemliga tvångsmedel att åklagaren slutligt ska pröva underrättelsefrågan och då få fatta ett beslut om att avstå från att underrätta enskilda, om det på grund av men för utredningen eller sekretess inte har kunnat läm-

nas någon underrättelse. I ett sådant fall ska den enskildes rättssäkerhetsintresse tas om hand genom att SIN informeras om beslutet. Förslaget omfattar även underrättelse till enskilda vid hemlig dataavläsning under förundersökning, se 28 § andra stycket lagen om hemlig dataavläsning som hänvisar till 27 kap. 31–33 §§ rättegångsbalken. Utredningens överväganden och förslag framgår av SOU 2022:50 s. 129 ff. och 166 f. Betänkandet är för närvarande under beredning.

Sammantaget har annat inte framkommit än att systemet med underrättelser till enskilda som berörts av hemlig dataavläsning är förenligt med de rättssäkerhetskrav som ställs. Som framgår av det lagförslag som för närvarande är under beredning kan det trots detta kan finnas skäl att förstärka enskildas rättssäkerhet i fråga om underrättelser om användning av hemliga tvångsmedel, inklusive hemlig dataavläsning, under förundersökning. Inom ramen för vårt uppdrag har vi inte funnit anledning att ifrågasätta eller vidareutveckla dessa överväganden. Eftersom förslaget för närvarande är under beredning finns det inte någon anledning för oss att lämna ett eget förslag i frågan.

8.7 Tillsyn och annan efterhandskontroll

Bedömning: Systemet med tillsyn och annan efterhandskontroll uppfyller de rättssäkerhetskrav som ställs på lagstiftningen.

Skälen för vår bedömning

Efterhandskontrollen av hemlig dataavläsning

En effektiv efterhandskontroll är nödvändig för att säkerställa en rättssäker användning av hemlig dataavläsning. De brottsbekämpande myndigheternas användning av hemlig dataavläsning står inte bara under särskild tillsyn av Säkerhets- och integritetsskyddsnämnden (SIN). Även Riksdagens ombudsmän (JO) och Justitiekanslern (JK) utövar tillsyn över de statliga myndigheternas verksamhet. Inom ramen för denna tillsyn, som omfattar även domstolarnas verksamhet, kan såväl JO som JK uttala sig i frågor gällande användningen av hemlig dataavläsning. Integritetsskyddsmyndigheten (IMY) är tillsynsmyndighet för viss behandling av personuppgifter. SIN och IMY har delvis överlappande tillsynsansvar när det gäller t.ex. Polismyndig-

hetens och Säkerhetspolisens behandling av personuppgifter. Härtill kommer den parlamentariska kontroll som riksdagen utövar över tillämpningen av hemlig dataavläsning. Kontrollen utövas på grundval av en årlig skrivelse från regeringen. I skrivelsen redovisas användningen av hemliga tvångsmedel, innefattandes hemlig dataavläsning, under föregående år till riksdagen (se avsnitt 3.2.13). Den parlamentariska kontrollen fyller en viktig funktion och bidrar till allmänhetens insyn i myndigheternas tvångsmedelsanvändning. Genom den parlamentariska kontrollen säkerställs också att hemlig dataavläsning endast får användas så länge åtgärden kan anses vara ett ändamålsenligt och nödvändigt instrument i brottsbekämpningen. Genom att tillämpningen av hemlig dataavläsning omfattas av såväl tillsyn som annan efterhandskontroll sker alltså fortlöpande avvägningar kring nytta, behov och integritetsintrång.

SIN:s verksamhet har vid olika utvärderingar ansetts utgöra en väl fungerande kontrollmekanism för de brottsbekämpande myndigheternas användning av hemliga tvångsmedel (se t.ex. Riksrevisionen rapport *En granskning av Säkerhets- och integritetsskyddsnämnden*, RiR 2016:2 s. 8 och 10 f., samt SOU 2012:44 s. 667). Vidare har utredningen om rättssäkerhetsgarantier vid användningen av vissa hemliga tvångsmedel ansett att systemet med tillsyn av bland annat SIN, JK och JO samt regeringens skrivelse till riksdagen uppfyller de krav som ställs på efterhandskontroll i regeringsformen och Europakonventionen (se SOU 2018:61 s. 230 ff.). Det har inte framkommit något under vårt utredningsarbete som ger anledning att göra någon annan bedömning i detta avseende. Däremot behöver vi analysera hur SIN:s tillsyn mer specifikt över användningen av hemlig dataavläsning har fungerat i praktiken och om det bör göras några ändringar i regelverket i detta avseende.

Särskilt om Säkerhets- och integritetsskyddsnämndens tillsyn

SIN är en myndighet under regeringen som bl.a. har till uppgift att utöva tillsyn över de brottsbekämpande myndigheternas användning av hemliga tvångsmedel, Säkerhetspolisens användning av hemliga tvångsmedel vid särskild kontroll av vissa utlänningar och viss personuppgiftsbehandling. Användningen av hemlig dataavläsning omfattas av nämndens tillsyn.

Nämndens verksamhet är reglerad i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet och i förordningen (2007:1141) med instruktion för Säkerhets- och integritetsskyddsnämnden. Enligt nämnda lag ska SIN utöva tillsyn genom inspektioner och andra undersökningar. Tillsynen ska särskilt syfta till att säkerställa att de brottsbekämpande myndigheternas användning av hemliga tvångsmedel varit författningsenlig. Nämnden får efter granskningen uttala sig om vad den kommit fram till och om vad som bör ändras i den granskade myndighetens verksamhet. Nämnden kan även uppmärksamma regeringen på behovet av förändringar i lag eller annan författning. Nämnden är skyldig att på begäran av en enskild kontrollera om denne har utsatts för hemliga tvångsmedel eller varit föremål för viss personuppgiftsbehandling. Det finns inget krav på att den enskilde ska ha skäl för sin begäran eller att det ska finnas en konkret misstanke om att personen är föremål för en hemlig tvångsåtgärd eller personuppgiftsbehandling. Nämnden ska kontrollera om den eventuella användningen har utförts i enlighet med lag eller annan författning samt underrätta den enskilde om att kontrollen har utförts. Om nämnden vid kontrollen bedömer att det förekommit felaktigheter som kan medföra skadeståndsansvar för staten gentemot den enskilde ska det anmälas till JK. Om nämnden bedömer att det förekommit felaktigheter som innefattar misstanke om brott ska ärendet anmälas till Åklagarmyndigheten eller annan behörig myndighet. Vidare ska nämnden i vissa fall anmäla brister i personuppgiftsbehandlingen till IMY.

Enligt 21 § lagen om hemlig dataavläsning ska rätten, när den har beslutat i frågor om hemlig dataavläsning, skyndsamt underrätta nämnden om beslutet. Underrättelseskyldigheten gäller oavsett om tillstånd till tvångsmedlet beviljas eller avslås och omfattar även t.ex. beslut om tillträdestillstånd (se prop. 2019/20:64 s. 175 och 235). Nämnden ska också underrättas om otillåten tilläggsinformation har lästs av eller tagits upp, se 23 § lagen om hemlig dataavläsning. Detta gäller oberoende av om informationen har hunnit förstöras eller inte (jfr a. prop. s. 162). Utformningen av underrättelseskyldigheten innebär att SIN har möjlighet att påbörja tillsyn redan under pågående verkställighet. I 2 § förordningen (2020:172) om hemlig dataavläsning finns närmare bestämmelser om vilken information som ska lämnas. Nuvarande ordning innebär en omfattande underrättelseskyldighet i förhållande till den som gäller vid användande av permanenta tvångs-

medel enligt rättegångsbalken, jfr 14 b § förundersökningskungörelsen. Ordningen för hemlig dataavläsning har motiverats med att en omfattande underrättelseskyldighet ger ett bättre underlag för en effektiv tillsyn (se a. prop. s. 175).

Nämndens tillsynsfunktion utgör en viktig rättssäkerhetsgaranti och underrättelseskyldigheten enligt 21 och 23 §§ bör kvarstå

Det kan konstateras att SIN:s tillsynsfunktion utgör en viktig rättssäkerhetsgaranti för säkerställandet av att användningen av hemlig dataavläsning bedrivs lagenligt. Under lagstiftningsarbetet med den nya lagen om hemlig dataavläsning framhöll Lagrådet särskilt vikten av nämndens roll beträffande tillsyn och efterhandskontroll av lagens efterlevnad (se prop. 2019/20:64 s. 316 f.). Det är därför nödvändigt att ramverket för hemlig dataavläsning även i praktiken möjliggör en effektiv efterhandskontroll.

Nämndens olika granskningar av användningen av hemlig dataavläsning, t.ex. användningen av villkor för att värna den enskildes integritet och olika aspekter av verkställigheten, har vi redogjort för löpande i våra överväganden. När det gäller underrättelseskyldigheten enligt 21 och 23 §§ lagen om hemlig dataavläsning framgår av SIN:s årsredovisningar att nämnden under 2022 mottog 604 underrättelser enligt 21 § (636 under 2021 och 305 under 2020). Siffran är inte jämförbar med antalet redovisade tillstånd enligt de brottsbekämpande myndigheternas officiella redovisningar eftersom ett beslut kan innefatta flera tillstånd. Vidare inräknas inte antalet avslagsbeslut i den officiella statistiken (se avsnitt 6.3). Annat har dock inte framkommit än att underrättelseskyldigheten enligt 21 § i allt väsentligt har uppfyllt sitt syfte. De underrättelser som tagits emot har också granskats löpande. Under åren 2020–2022 mottogs inga underrättelser enligt 23 §. SIN inledde under 2022 en särskild granskning gällande bl.a. underrättelser och otillåten tilläggsinformation. Granskningen är för närvarande pågående och väntas vara slutförd före utgången av 2023.

Vi delar tidigare bedömningar om att hemlig dataavläsning förutsätter en mer aktiv tillsyn än vad som är fallet avseende övriga hemliga tvångsmedel och att formerna för denna tillsyn är väl avvägda (jfr a. prop. s. 175). En omfattande underrättelseskyldighet, i kombination med förtydliganden om vad ett tillstånd ska innehålla och

ett lagstadgat dokumentationskrav, bedöms därför ändamålsenlig för att tillsynsmyndigheten ska kunna utöva en rättssäker efterhandskontroll. Vi har även i samband med vårt förslag i avsnitt 8.5.6. framhållit att den underrättelseskyldighet som följer av 21 § utgör ett viktigt led i efterhandskontrollen. Företrädare för SIN har också till utredningen bekräftat att underrättelseskyldigheten enligt 21 § har fungerat väl och fyllt en viktig funktion i nämndens tillsyn. Underrättelseskyldigheten enligt 21 § bör därför kvarstå. När det gäller underrättelseskyldigheten enligt 23 § kan det mot bakgrund av den hittillsvarande tillämpningen ifrågasättas om en sådan reglering är ändamålsenlig. Även om bestämmelsen ännu inte har kommit till användning syftar den till att tillförsäkra att nämnden får underlag som kan läggas till grund för att bedöma om ett tillsynsärende bör initieras (se a. prop. s. 162). Att bestämmelsen inte har tillämpats i praktiken skulle kunna bero på att bestämmelsen inte har tillämpats korrekt. Det kan också bero på att verkställighet av hemlig dataavläsning har skett med den omsorg som krävs och att någon otillåten tilläggsinformation därmed inte tagits upp. Våra analyser av genomförandet av hemlig dataavläsning talar för det senare. De rättssäkerhetsgarantier som omgärdar verkställigheten av hemlig dataavläsning är så starka att risken för att verkställande myndighet läser av eller tar upp otillåten tilläggsinformation i samband med verkställighet bedöms vara mycket liten. Risken är dock inte obefintlig. Nuvarande underrättelseskyldighet enligt 23 § innebär således en förstärkt rättssäkerhetsgaranti för den enskilde som bör finnas kvar.

Underrättelseskyldigheten enligt 21 § bör även i framtiden gälla domstolen

När det gäller frågan om vilken aktör som ska åläggas den underrättelseskyldighet som följer av 21 § lagen om hemlig dataavläsning gör vi följande överväganden. Företrädare för SIN har framhållit att det bör vara åklagaren och inte domstolen som ska underrätta nämnden eftersom nämndens tillsyn inte omfattar domstolarnas verksamhet. Varför man valde att ålägga just rätten en underrättelseskyldighet motiverades inte närmare i förarbetena till lagen om hemlig dataavläsning (se prop. 2019/20:64 s. 175). Det framstår dock som naturligt att domstolen i samband med den expediering av beslut om hemlig dataavläsning som sker till berörda aktörer även expedierar en

underrättelse till SIN. Det kan också rent allmänt vara en fördel med ett system där underrättelseskyldigheten åligger någon annan än den som ska granskas. Vid en samlad bedömning anser vi därför att övervägande skäl talar för att den underrättelseskyldighet som följer av 21 § ska gälla för domstolen även fortsättningsvis.

8.8 Kontrollmekanismerna och rättssäkerhetsgarantierna är tillräckliga

Bedömning: De kontrollmekanismer och andra rättssäkerhetsgarantier som omgärdar regelverket för hemlig dataavläsning innebär att de krav som regeringsformen och Europakonventionen ställer på lagstiftningen i huvudsak uppfylls.

Våra förslag i detta kapitel leder till en förstärkning av de rättssäkerhetsgarantier som redan gäller för hemlig dataavläsning. Bestämmelserna i lagen om hemlig dataavläsning uppfyller därmed de högt ställda krav som ska gälla vid användning av hemlig dataavläsning.

Skälen för vår bedömning

De nuvarande och nu föreslagna bestämmelserna om ett utökat tillämpningsområde för hemlig dataavläsning innebär en ökad risk för enskildas personliga integritet. Regelverket för hemlig dataavläsning måste därför omgärdas av kontrollmekanismer och andra rättssäkerhetsgarantier för att leva upp till högt ställda krav på rättssäkerhet och informationssäkerhet. Intrånget i den personliga integriteten får aldrig bli större än vad som kan tillåtas enligt regeringsformen och Europakonventionen.

Det kan konstateras att de kontrollmekanismer och andra rättssäkerhetsgarantier som omgärdar regelverket för hemlig dataavläsning är sådana att regelverket i stor utsträckning lever upp till de krav som regeringsformen och Europakonventionen ställer på lagstiftningen, även med beaktande av de ändringar som nyligen har trätt i kraft och som nu föreslås i kapitel 6 och 7. Tillsammans med dessa lagändringar och lagförslag bör dock vissa förändringar i regelverket ske i syfte att ytterligare stärka rättssäkerhetsgarantierna. Vi har där-

för i detta kapitel föreslagit en tydligare reglering av vad ett tillstånd till hemlig dataavläsning ska innehålla, tydligare regler för användning och hantering av information från hemlig dataavläsning och stärkta förutsättningar för tillsyn. Genom våra förslag blir det mer förutsebart både för rättstillämparen och för den enskilde när och hur hemlig dataavläsning får användas. Förslagen innebär också ett förstärkt skydd mot otillåtna och obefogade integritetsintrång, eftersom de skapar bättre förutsättningar för efterhandskontroll. Vi bedömer därmed att våra förslag i detta kapitel leder till en förstärkning av de rättssäkerhetsgarantier som redan gäller för hemlig dataavläsning. Bestämmelserna bedöms även i övrigt vara förenliga med Sveriges åtaganden avseende mänskliga rättigheter samt uppfylla de höga krav på rättssäkerhet och informationssäkerhet som ställs. Sammantaget bedöms nuvarande och nu föreslagna bestämmelser om hemlig dataavläsning ge uttryck för en ändamålsenlig avvägning mellan behovet av en effektiv brottsbekämpning och den enskildes rätt till skydd för sin personliga integritet.

9 Lagstiftningens struktur och placering

9.1 Uppdraget

Enligt utredningsuppdraget ska utredaren säkerställa att en välfungerande systematik i regelverket kring såväl hemliga som öppna tvångsmedel upprätthålls. Vi har i kapitel 7–8 bl.a. behandlat frågan om hur den materiella regleringen bör harmoniseras med övriga tvångsmedel. Vi övergår nu till frågan om en harmonisering av lagstiftningens struktur.

Inför den nya lagens införande lämnade Lagrådet följande anmärkningar på valet att reglera hemlig dataavläsning i en egen lag (se prop. 2019/20:64 s. 317).

> Den valda lagstiftningstekniken, att reglera hemlig dataavläsning i en egen lag, innebär dels att många av de föreslagna bestämmelserna i stora delar är likalydande med bestämmelser i gällande tvångsmedelslagstiftning, dels att hänvisningar görs till flera andra lagar. Regelverket blir därmed mer svåröverskådligt än om bestämmelserna om hemlig dataavläsning hade arbetats in i den befintliga lagstiftningen; detta särskilt eftersom hemlig dataavläsning i stor utsträckning utgör en ny verkställighetsform av redan existerande hemliga tvångsmedel.
>
> Lagstiftningstekniken ställer stora krav på tillämparen och ökar riskerna för misstag. Eftersom det är fråga om en tillfällig lagstiftning får emellertid den valda metoden accepteras. För det fall det blir fråga om att förlänga eller permanenta hemlig dataavläsning bör dock lagstiftningstekniken övervägas på nytt.

I utredningsuppdraget ligger alltså frågan om hemlig dataavläsning ska integreras i rättegångsbalken och speciallagstiftning eller om bestämmelserna fortsatt ska regleras i en egen lag.

9.2 Bestämmelserna om hemlig dataavläsning bör fortsatt regleras i egen lag

Förslag: Bestämmelserna om hemlig dataavläsning bör i vart fall för närvarande fortsatt regleras i en särskild lag (lagen om hemlig dataavläsning).

Bedömning: Det bör göras en samlad översyn över området för tvångsmedel.

Skälen för vårt förslag och vår bedömning

Uppdraget att säkerställa en välfungerande systematik i regelverket kompliceras av att det inte finns någon sammanhållen reglering på området, varken för hemliga eller öppna tvångsmedel. Balansen mellan tvångsmedel och integritet har pendlat fram och tillbaka genom tiderna. Den materiella regleringen har tillkommit vid olika tidpunkter och är därför inte alltid helt konsekvent. Vidare är lagstiftningsområdet för straffprocessuella tvångsmedel under pågående förändring. Ny lagstiftning på området har nyligen trätt i kraft och flera lagförslag är för närvarande under beredning. Vi har redogjort mer ingående för detta i avsnitt 3.3.3 och 5.3.4.

Utöver hemlig dataavläsning finns sex stycken tvångsåtgärder som räknas till de hemliga tvångsmedlen. Bestämmelser om hemliga tvångsmedel finns både i 27 kap. rättegångsbalken och i vissa speciallagar (se avsnitt 4.1.2). Redan i dag upplever många professionella aktörer som arbetar med hemliga tvångsmedel att 27 kap. rättegångsbalken är svårnavigerat. Exempelvis innehåller kapitlet hänvisningar i flera led. Speciallagarna hänvisar i sin tur till 27 kap. rättegångsbalken. I de lagförslag som bereds föreslås bl.a. en utökning av tillämpningsområdet för vissa hemliga tvångsmedel, däribland hemlig dataavläsning. Vidare föreslås ytterligare en speciallag som i sin tur innehåller hänvisningar till både 27 kap. rättegångsbalken och till lagen om hemlig dataavläsning (*Bättre möjligheter att verkställa frihetsberövanden*, SOU 2022:50, se avsnitt 3.3.3).

Samtidigt finns en mängd öppna tvångsmedel, reglerade i bl.a. rättegångsbalken och polislagen men även oreglerade utredningsmetoder, som ibland utförs av de brottsbekämpande myndigheterna utan den

enskildes kännedom och som kan utgöra ett betydande intrång i den enskildes personliga integritet. Några exempel på detta är spaning mot en person och infiltratörsverksamhet. Husrannsakan, beslag och genomsökning på distans som sker utan föregående underrättelse är andra exempel på öppna åtgärder som kan innebära intrång i den enskildes personliga integritet i olika omfattning. Flera av dessa bestämmelser har införts nyligen och i samband därmed kritiserats för att göra tvångsmedelsregleringen i rättegångsbalken än mer svåröverskådlig. Enbart de nya bestämmelserna om genomsökning på distans omfattar nio nya paragrafer, reglerade i 28 kap. 10 a–i §§ rättegångsbalken. Flera av dessa paragrafer innehåller i sin tur hänvisningar till bl.a. 27 kap. rättegångsbalken. Överskådligheten kompliceras ytterligare av att genomsökning på distans föreslås få användas även för att förhindra allvarlig brottslighet (se slutbetänkandet *Utökade möjligheter att använda preventiva tvångsmedel 2*, SOU 2023:60).

De öppna tvångsmedlen kan alltså innebära stora integritetsintrång, men omfattas trots detta inte av samma rättssäkerhetsgarantier och kontrollmekanismer som de hemliga tvångsmedlen. I doktrin har därför argumenterats för att fler öppna åtgärder och metoder borde anses vara hemliga tvångsmedel. Det faktum att det saknas en sammanhållen reglering för hemliga tvångsmedel talar starkt för att en samlad översyn av tvångsmedelsområdet bör göras (jfr Heuman och Gatenheim, Några problematiserande aspekter på hemliga tvångsmedel, *Juridisk Tidskrift* nr 2 2018/19, s. 261). Vi delar uppfattningen att det vore önskvärt att reglerna om tvångsmedelsanvändning blev föremål för en fullständig översyn i syfte att förenkla och harmonisera reglerna.

För närvarande måste vi dock förhålla oss till hur regelverket ser ut i dag. Bestämmelserna om hemlig dataavläsning gäller både under förundersökning och i underrättelseverksamhet. Redan av detta skäl skulle många bestämmelser behöva upprepas för att integrera dem i såväl rättegångsbalken som i speciallagstiftning. Som redogjorts för är regelverken på tvångsmedelsområdet svåröverskådliga och dessutom i pågående förändring, vilket bedöms ytterligare försvåra överblicken och förutsebarheten.

Vid en sammantagen bedömning framstår det för närvarande som ett sämre och mer svåröverskådligt alternativ att arbeta in bestämmelserna om hemlig dataavläsning i befintlig lagstiftning än att fortsatt låta bestämmelserna regleras i en egen lag. Vi anser att kraven på systematik, tydlighet och förutsebarhet för närvarande tillgodoses bättre om hemlig dataavläsning fortsatt, och i avvaktan på att det görs en samlad översyn, regleras i en egen lag.

10 Hemlig dataavläsning och internationella förhållanden

10.1 Uppdraget

Den allvarliga brottslighet som kan föranleda hemlig dataavläsning är inte sällan av gränsöverskridande natur. Såväl personerna bakom brottsligheten som de informationssystem som används i kriminella syften kan finnas utspridda i olika länder. Brottsutredningar om grov narkotikabrottslighet, terroristbrott och internetrelaterade sexuella övergrepp mot barn är bara några exempel på utredningar om allvarlig brottslighet där det är vanligt med rättsligt samarbete över nationsgränserna. I våra direktiv understryks också vikten av att de brottsbekämpande myndigheterna både nationellt och i det internationella samarbetet har tillgång till ändamålsenliga och verkningsfulla verktyg för att effektivt kunna utreda, förebygga och förhindra allvarlig brottslighet. Vidare ingår i vårt uppdrag att se till att en välfungerande systematik upprätthålls i regelverket om hemliga tvångsmedel. Det innebär att vi i ett internationellt perspektiv måste överväga behovet av förändringar eller följdändringar i lagen (2000:562) om internationell rättslig hjälp i brottmål (LIRB) och lagen (2017:1000) om en europeisk utredningsorder. I detta kapitel behandlar vi frågor om exekutiv jurisdiktion och hemlig dataavläsning i det internationella rättsliga samarbetet.

Av intresse i sammanhanget är hur den motsvarande lagstiftningen om hemlig dataavläsning ser ut utanför Sveriges gränser. Avslutningsvis gör vi därför en kort internationell utblick för att titta på hur möjligheterna till hemlig dataavläsning och motsvarigheter till åtgärden ser ut utomlands.

10.2 Exekutiv jurisdiktion i förhållande till elektroniskt lagrade uppgifter

Bedömning: Svensk exekutiv jurisdiktion föreligger vid hemlig dataavläsning även om de eftersökta uppgifterna lagras elektroniskt på annan plats än i Sverige eller om det är okänt var uppgifterna lagras, under förutsättning att

- de brottsbekämpande myndigheterna utan bistånd kan skaffa sig tillgång till uppgifterna,
- inhämtningen inte bedöms innebära mer än ett obetydligt intrång i en annan stats suveränitet, och
- inhämtningen inte bedöms kunna orsaka någon skada på det avläsningsbara informationssystem som tvångsmedlet avser.

10.2.1 Inledning

Med exekutiv jurisdiktion avses rätten att vidta åtgärder och verkställa beslut som har fattats inom ramen för lagstiftning och rättsskipning. Utgångspunkten i folkrätten är att det råder ett förbud för stater att vidta verkställighetsåtgärder inom andra staters territorier, t.ex. att använda hemlig dataavläsning där. Detta är ett utflöde av den s.k. territorialitetsprincipen. Att begränsningen av svensk verkställande jurisdiktion till svenskt territorium ska beaktas följer av 2 kap. 12 § brottsbalken eller av grunderna för den bestämmelsen.

Förutsättningarna för exekutiv jurisdiktion har vuxit fram i den traditionellt fysiska världen, där det oftast är enkelt att konstatera var olika ting, exempelvis fysiska handlingar, förvaras. I den digitala it-miljön ser förutsättningarna annorlunda ut. Elektroniskt lagrade uppgifter kan finnas i flera stater samtidigt eller ständigt vara på väg mellan olika stater. I många fall är det inte ens för den som tillhandahåller en internettjänst möjligt att klargöra var uppgifterna finns i varje givet ögonblick. När detta trots allt är möjligt kan förhållandena ändras på bråkdelen av en sekund. I Sverige har de folkrättsliga principerna traditionellt tolkats så att svenska brottsbekämpande myndigheter saknar jurisdiktion om uppgifter lagras elektroniskt på annan plats än i Sverige eller om det är okänt var uppgifterna lagras, s.k. *loss of location*. Det innebär exempelvis att det tidigare inte har ansetts

tillåtet för svenska brottsbekämpande myndigheter att under en förundersökning, där man känner till den misstänktes inloggningsuppgifter, logga in på dennes internetbaserade kommunikations- eller lagringstjänster om tjänsteföretagets servrar kan finnas utanför Sverige. De senaste åren har det emellertid ifrågasatts om just lagringsplatsen är den mest relevanta grunden för jurisdiktion i dessa fall (se SOU 2017:89 s. 444 och prop. 2019/20:64 s. 202).

Vid verkställighet av hemlig dataavläsning kan de svenska brottsbekämpande myndigheterna komma att påträffa elektroniska handlingar som finns lagrade i utlandet eller på okänd plats. Det handlar framför allt om elektronisk information som finns på immateriella informationssystem, exempelvis genom ett konto vars uppgifter finns på en server i en annan stat. När det gäller åtkomst till uppgifter som finns lokalt lagrade på fysiska informationssystem, exempelvis en mobiltelefon, uppstår inte samma problematik. För det fall mobiltelefonen finns i en annan stat är de brottsbekämpande myndigheterna primärt hänvisade till att begära rättslig hjälp från den stat där mobiltelefonen finns alternativt underrätta den staten i enlighet med lagen om en europeisk utredningsorder (se avsnitt 10.3).

Frågan om det finns några hinder mot att de brottsbekämpande myndigheterna inhämtar information som är eller kan vara lagrad utanför Sveriges gränser diskuterades under lagstiftningsarbetet med lagen om hemlig dataavläsning. Utredningen om hemlig dataavläsning bedömde att det fanns starka skäl att nyansera den dittillsvarande svenska hållningen avseende vad territorialitetsprincipen vid exekutiv jurisdiktion innebär för elektroniskt lagrade uppgifter. Utredningen ansåg att detta gjorde sig gällande särskilt i de fall då det inte är känt och inte kan klarläggas i vilket eller vilka länder som de elektroniska uppgifterna lagras. Bestämmelserna om hemlig dataavläsning är därför enligt sin ordalydelse inte begränsade till eftersökning av information som är lagrad i Sverige. Utredningen fann dock inte lämpligt att lagstiftningsvägen, inom ramen för utredningen, ändra den svenska hållningen. Utredningen bedömde att frågan i stället borde ses över i särskild ordning eller prövas i rättstillämpningen. Utredningen framhöll samtidigt att frågan om en ändrad hållning kan prövas av domstol i samband med tillståndsprövning för hemlig dataavläsning när åtgärden avser användarkonton till internetbaserade tjänster (se a. SOU s. 479 ff.). Inte heller regeringen ansåg sig ha underlag för att i sammanhanget kunna överväga frågan. Regeringen uttalade

att frågan om hur territorialitetsprincipen vid exekutiv jurisdiktion bör tolkas bäst tas om hand inom ramen för det internationella samarbetet eller på annat lämpligt sätt (se a. prop. s. 201 ff.).

Det ska i sammanhanget framhållas att frågan om exekutiv jurisdiktion i förhållande till elektronisk information som är eller kan vara lagrad utanför Sveriges gränser aktualiseras även vid genomsökning på distans. I motiven till bestämmelserna om detta tvångsmedel kom man till motsvarande slutsatser som Utredningen om hemlig dataavläsning. Man uttalade bl.a. att en tolkning av territorialitetsprincipen som enbart tar sikte på den plats där elektronisk information finns lagrad inte är anpassad till it-miljön. Utredningen landade dock i slutsatsen att detta inte bör bli en fråga för lagstiftning utan får överlämnas till rättspraxis. Regeringen hänvisade i det lagstiftningsärendet till 2021 års datalagringsutredning som vid tidpunkten nyligen hade tillsatts. Regeringen framhöll därvid att en del av den särskilda utredarens uppdrag var att ta ställning till om det bör införas en särskild lagreglering för territorialitetsprincipen vid exekutiv jurisdiktion som också tar hänsyn till andra anknytningsfaktorer än var data lagras (se SOU 2017:100 s. 374 f. och prop. 2021/22:119 s. 85 f.).

Förutsättningarna för exekutiv jurisdiktion i förhållande till elektroniskt lagrade uppgifter som finns utanför Sverige, inklusive de folkrättsliga aspekterna, har helt nyligen behandlats både av Högsta domstolen och av 2021 års datalagringsutredning.

10.2.2 Rättsfallet ”Den okända lagringsplatsen”

I rättsfallet ”Den okända lagringsplatsen” prövade Högsta domstolen frågan om genomsökning på distans får beslutas även när den information som genomsökningen avser kan vara lagrad i utlandet, se domstolens beslut den 30 mars 2023 i mål Ö 5686-22.

Bakgrunden i målet var att åklagaren i en förundersökning om grovt penningtvättsbrott och grovt bokföringsbrott hade begärt att tingsrätten skulle besluta om genomsökning på distans. Åtgärden syftade till att söka efter handlingar som kunde vara av betydelse för utredningen av brotten. Enligt åklagaren fanns handlingarna lagrade i avläsningsbara informationssystem som var tillgängliga i mobiltelefoner och datorer som hade tagits i beslag hos den misstänkte. Åkla-

garen angav att det var oklart på vilken molntjänst och var i världen som den eftersökta informationen fanns lagrad. Tingsrätten, som kom fram till att förutsättningarna för att besluta om genomsökning på distans var uppfyllda, beviljade åklagarens begäran. Beslutet överklagades till hovrätten som fastställde tingsrättens beslut. Högsta domstolen beviljade därefter prövningstillstånd i frågan om det är möjligt att besluta om genomsökning på distans, trots att genomsökningen avsåg information som kan vara lagrad i utlandet.

I målet konstaterade Högsta domstolen inledningsvis att rättegångsbalkens bestämmelser om genomsökning på distans är utformade så att de medger eftersökning av information som finns lagrad utanför Sverige. Högsta domstolen fann inte heller några folkrättsliga hinder mot sådan eftersökning. Högsta domstolen konstaterade samtidigt att genomsökningen måste ske inom ramen för en svensk brottsutredning, att den måste vidtas med användning av utrustning som finns i Sverige och att genomsökningen ska ske på ett sådant sätt att den eftersökta informationen inte raderas eller på annat sätt påverkas till sitt innehåll.

10.2.3 2021 års datalagringsutredning

Regeringen gav i augusti 2021 en särskild utredare i uppdrag att se över den lagstiftning som medför en skyldighet för tillhandahållare av elektroniska kommunikationstjänster att lagra uppgifter om elektronisk kommunikation för brottsbekämpande syften, samt vissa anknytande frågor om myndigheternas tillgång till sådana uppgifter. I uppdraget ingick bl.a. att se över vissa frågor om svenska myndigheters tillgång till elektroniska uppgifter, när de finns utanför Sveriges gränser (exekutiv jurisdiktion). Utredningen antog namnet 2021 års datalagringsutredning. Uppdraget redovisades den 30 maj 2023, i betänkandet *Datalagring och åtkomst till elektronisk information*, SOU 2023:22.

I betänkandet framgår att utredningen har sett över förutsättningarna, inklusive de folkrättsliga aspekterna, för att införa en särskild lagreglering för exekutiv jurisdiktion i förhållande till elektronisk information som finns utanför Sverige vid användning av straffprocessuella tvångsmedel (se a. SOU s. 431 ff. och 511 ff.).

Utredningen konstaterade inledningsvis att den snabba tekniska utvecklingen av elektroniska kommunikations- och lagringstjänster

och internationaliseringen av dessa har medfört att de brottsbekämpande myndigheterna har ett påtagligt behov av att kunna få tillgång till elektronisk information även när den är lagrad utanför Sverige. Vidare konstaterade utredningen i sina analyser att folkrätten, under vissa närmare angivna förutsättningar, inte hindrar att brottsbekämpande myndigheter inhämtar elektronisk information som är eller kan vara lagrad utanför Sverige. Utredningen framhöll att det i praktiken huvudsakligen handlar om information som finns lagrad på immateriella informationssystem, vanligen en server, t.ex. på användarkonton till olika molntjänster. Utredningen bedömde att omfattningen av jurisdiktionen bör klargöras genom att förutsättningarna framgår av lag. Utredningen framhöll att det för närvarande endast är hemlig dataavläsning och genomsökning på distans som är av relevans i sammanhanget. Detta med hänsyn till att det i dag inte finns några andra tvångsmedel som i praktiken medger att myndigheterna på egen hand bereder sig tillgång till information i ett annat land. Utredningen framhöll samtidigt vikten av en lagreglering av mer principiellt slag, som tar höjd för såväl ändringar i tvångsmedelslagstiftningen som nya tekniska lösningar. Den föreslagna regleringen är därför inte begränsad till vissa tvångsmedel eller till inhämtning från immateriella lagringsplatser. Utredningen bedömde att den föreslagna regleringen inte nämnvärt bör öka risken för intrång i den personliga integriteten och att de rättssäkerhetsgarantier som gäller enligt respektive tvångsmedelsreglering är tillräckliga.

I slutskedet av utredningsarbetet meddelade Högsta domstolen det nämnda avgörandet där det tydliggjordes att genomsökning på distans får ske även om den eftersökta informationen kan vara lagrad i utlandet, se föregående avsnitt. Utredningen gjorde då den bedömningen att de tidigare analyserna och förslaget i betänkandet beträffande exekutiv jurisdiktion skulle kvarstå, bl.a. därför att utredningens ansats var något bredare än Högsta domstolens.

Mot den bakgrunden föreslog utredningen en lagreglering som ska förtydliga vad som gäller för viss inhämtning av elektronisk information som lagras utanför Sverige. Datalagringsutredningens förslag till en ny lag, benämnd lag om inhämtning av elektronisk information som är lagrad utanför Sverige vid användning av straffprocessuella tvångsmedel, ser ut enligt följande:

1 § Med de begränsningar som följer av 2 och 3 §§ denna lag får brottsbekämpande myndigheter genom straffprocessuella tvångsmedel inhämta elektronisk information som är lagrad utanför Sverige.

2 § Inhämtning enligt 1 § får avse endast sådan information som de brottsbekämpande myndigheterna utan bistånd kan skaffa sig tillgång till i det informationssystem som tvångsmedlet avser.

3 § Inhämtning enligt 1 § får inte innebära mer än ett obetydligt intrång i en annan stats suveränitet. Information får inte inhämtas, om inhämtningen bedöms kunna orsaka någon skada på det informationssystem som tvångsmedlet avser.

Att informationen är lagrad utanför Sverige innebär enligt motiven att den finns eller är sparad utomlands. Lagen ska gälla även om det är oklart var informationen lagras. Vidare ska lagen gälla såväl inom som utom förundersökningar beträffande brott som svensk domstol är behörig att döma över eller brottslig verksamhet som innefattar brott som svensk domstol är behörig att döma över, dvs. sådana brott eller sådan brottslig verksamhet som svenska myndigheter får bekämpa. Med att ”utan bistånd skaffa sig tillgång” avses att den brottsbekämpande myndigheten kan bereda sig tillgång till de aktuella uppgifterna utan hjälp från utomstående, t.ex. tillhandahållaren av en lagringstjänst eller någon annan stat. Regleringen förutsätter vidare att inhämtningen görs från en plats där den brottsbekämpande myndigheten är behörig att verka, i praktiken Sverige. I motiven anges också att hemlig dataavläsning, med de begränsningar som följer av den föreslagna lagen, och genomsökning på distans normalt inte bör innebära några beaktansvärda risker för informationssäkerheten, eftersom informationen fortfarande är tillgänglig på användarkontot och inga ändringar får göras i informationen. Tillgång till uppgifter på ett användarkonto genom inloggning på kontot eller i övrigt normal åtkomst till tjänsten bör som huvudregel anses vara ett obetydligt intrång i andra staters suveränitet. Bestämmelsen i 3 § sträcker sig längre än aktsamhetsbestämmelsen i 25 § lagen om hemlig dataavläsning, vilket ger uttryck för den försiktighetsprincip som ska tillämpas när information som är eller kan vara lagrad utanför Sverige inhämtas av svenska brottsbekämpande myndigheter.

Förslaget föreslås träda i kraft den 1 juli 2024 och bereds för närvarande i Regeringskansliet. Inom ramen för vårt uppdrag har vi inte funnit anledning att ifrågasätta eller vidareutveckla Datalagringsutred-

ningens överväganden och förslag. Eftersom förslaget för närvarande är under beredning finns det inte någon anledning för oss att lämna ett eget förslag i frågan.

10.2.4 Hemlig dataavläsning och exekutiv jurisdiktion

För en effektiv brottsbekämpning är det angeläget att bestämmelserna om hemlig dataavläsning kan tillämpas, även när informationen är lagrad utanför Sverige eller när det är okänt var den finns. I annat fall kan själva syftet med bestämmelserna komma att motverkas.

Det är som ovan konstaterats en principiell fråga om när elektroniskt lagrad information ska få inhämtas från svenskt territorium. Rättsfallet ”Den okända lagringsplatsen” gällde visserligen genomsökning på distans, men får enligt vår bedömning genomslag även för hemlig dataavläsning. Vid båda dessa tvångsmedel handlar det om inhämtning av elektronisk information som finns i ett avläsningsbart informationssystem. Båda dessa tvångsmedel medger att svenska myndigheter på egen hand bereder sig tillgång till elektronisk information i ett annat land. De principiella överväganden och slutsatser som aktualiseras i Högsta domstolens beslut avseende genomsökning på distans får mot denna bakgrund anses likaledes applicerbara på hemlig dataavläsning.

Vidare delar vi Datalagringsutredningens bedömningar om förutsättningarna för exekutiv jurisdiktion vid hemlig dataavläsning. Vi hänvisar därför till deras analyser och förslag i betänkandet SOU 2023:22 s. 431 ff. och 511 ff.

Sammantaget bedömer vi mot bakgrund av såväl Högsta domstolens beslut och Datalagringsutredningens analyser att det föreligger svensk exekutiv jurisdiktion vid hemlig dataavläsning även om de eftersökta uppgifterna lagras elektroniskt på annan plats än i Sverige eller om det är okänt var uppgifterna lagras, under förutsättning att:

- de brottsbekämpande myndigheterna utan bistånd kan skaffa sig tillgång till uppgifterna,
- inhämtningen inte bedöms innebära mer än ett obetydligt intrång i en annan stats suveränitet, och
- inhämtningen inte bedöms kunna orsaka någon skada på det avläsningsbara informationssystem som tvångsmedlet avser.

Vår bedömning är att detta följer redan av allmänna folkrättsliga principer. Det bör således gälla oavsett om Datalagringsutredningens förslag om en ny lag på området genomförs eller inte.

10.3 Det internationella rättsliga samarbetet

Bedömning: Nuvarande regler om hemlig dataavläsning i lagen om internationell rättslig hjälp i brottmål och i lagen om en europeisk utredningsorder är ändamålsenligt och proportionerligt utformade. Några författningsändringar är inte nödvändiga i detta avseende.

Skälen för vår bedömning

En självklar utgångspunkt är att de utredningsåtgärder som är möjliga att vidta i Sverige ska kunna vidtas i en annan stat på begäran av svenska åklagare. På samma sätt ska utländska åklagare kunna begära att en motsvarande åtgärd vidtas i Sverige. Samtidigt som lagen om hemlig dataavläsning trädde i kraft infördes därför särskilda bestämmelser om hemlig dataavläsning i de lagar som reglerar det internationella rättsliga samarbetet. Bestämmelserna tidsbegränsades inte. De lagar som är aktuella i sammanhanget är lagen (2000:562) om internationell rättslig hjälp i brottmål (LIRB) och lagen (2017:1000) om en europeisk utredningsorder (LEUO). I Datalagringsutredningens betänkande *Datalagring och åtkomst till elektronisk information* har nyligen mer ingående redogjorts för syftet med och innehållet i dessa lagar (se SOU 2023:22 s. 130 ff. och 435 ff.). Något kort om bestämmelserna ska nämnas även här.

LEUO gäller gentemot alla medlemsstater i EU förutom Danmark och Irland. Med en europeisk utredningsorder avses i korthet ett beslut i Sverige eller i en annan medlemsstat i EU som innebär att en utredningsåtgärd ska vidtas i en annan medlemsstat i syfte att inhämta bevisning. Hemlig dataavläsning ingår sedan den 1 mars 2020 i den katalog över utredningsåtgärder som kan vidtas med stöd av lagen, se 1 kap. 4 § 6 LEUO. Kraven för utfärdande, erkännande och verkställande av en europeisk utredningsorder avseende hemlig dataavläsning motsvarar huvudsakligen de krav som gäller för övriga hem-

liga tvångsmedel enligt lagen. Detta innebär t.ex. att en utredningsorder för hemlig dataavläsning i Sverige eller i en annan medlemsstat än den stat till vilken ordern översänds endast får avse kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter. I övriga fall av hemlig dataavläsning gäller att åtgärden endast får ske i den medlemsstat dit utredningsordern har sänts.

I förhållande till övriga stater tillämpas LIRB. Den 1 mars 2020 fördes hemlig dataavläsning, tekniskt bistånd med hemlig dataavläsning och tillstånd till gränsöverskridande hemlig dataavläsning till förteckningen över de åtgärder som rättslig hjälp enligt LIRB omfattar, se 1 kap. 2 § 10–12 LIRB. Rättslig hjälp avseende hemlig dataavläsning lämnas under de förutsättningar som gäller för motsvarande åtgärd i en svensk förundersökning. Tekniskt bistånd och tillstånd till gränsöverskridande hemlig dataavläsning avser enbart hemlig dataavläsning för kommunikationsavlyssnings- och kommunikationsövervakningsuppgifter. Vidare ställs det upp ett krav på dubbel straffbarhet. De allmänna förfaranderegler som stadgas i 2 kap. är tillämpliga även beträffande hemlig dataavläsning. I 2 kap. 4 § LIRB finns en särskild bestämmelse om vad en ansökan om rättslig hjälp i Sverige till hemlig dataavläsning ska innehålla. I 4 kap. 28 c–h §§ LIRB återfinns särskilda bestämmelser om hemlig dataavläsning. Bestämmelserna motsvarar i allt väsentligt vad som gäller för rättslig hjälp med andra hemliga tvångsmedel enligt LIRB.

Förarbetena bakom bestämmelserna om hemlig dataavläsning i LIRB och LEUO återfinns i prop. 2019/20:64 s. 188 ff. och 246 ff. respektive 196 ff. och 295 ff. Vi har inte haft anledning att ifrågasätta eller vidareutveckla dessa tidigare analyser och överväganden. Det hittillsvarande tillämpningen visar inte heller annat än att lagstiftningen i dessa avseenden är ändamålsenligt och proportionerligt utformad (se avsnitt 6.3 och 8.5.1).

De utökningar av tillämpningsområdet för hemlig dataavläsning som redan har skett bedöms, tillsammans med de andra ändringar i regelverket för hemlig dataavläsning som nu föreslås, få genomslag i det internationella samarbetet även utan följdändringar. Detta med hänsyn till hur lagstiftningen i dessa avseenden är uppbyggd med hänvisningar till andra bestämmelser i bl.a. lagen om hemlig dataavläsning. Exempelvis innebär hänvisningen i 2 kap. 5 § första stycket 3 LEUO respektive i 4 kap. 28 c § LIRB till 17 § lagen om hemlig dataavläsning att den nya möjligheten till interimistiska beslut om hemlig

dataavläsning avseende rumsavlyssningsuppgifter har fått genomslag även vid internationella förhållanden. Vidare är bestämmelserna om hemlig dataavläsning i det internationella straffrättsliga samarbetet, till skillnad från bestämmelserna lagen om hemlig dataavläsning, inte begränsade i tiden.

Reglerna om hemlig dataavläsning i LIRB och LEUO bedöms sammantaget som ändamålsenligt och proportionerligt utformade. Vi bedömer därmed att det inte finns något behov av författningsändringar detta avseende.

I sammanhanget kan det nämnas att frågan om en mer effektiv gränsöverskridande åtkomst till elektroniska bevis för brottsbekämpande myndigheter för närvarande är under utredning (se regeringens kommittédirektiv 2023:84). Utredningen har tillsatts mot bakgrund av bl.a. förordning (EU) 2023/1543[1]. Den övergripande frågan som utredningen ska se över är hur EU:s medlemsstater i straffrättsliga förfaranden snabbare och effektivare ska kunna säkra och inhämta elektroniska bevis som lagras av leverantörer i en annan medlemsstat, samtidigt som skyddet för enskildas grundläggande fri- och rättigheter följs. Uppdraget ska redovisas senast den 13 december 2024.

10.4 Internationell utblick

10.4.1 Inledning

Som inledningsvis konstaterats är sådan allvarlig brottslighet som kan föranleda hemlig dataavläsning ofta gränsöverskridande. Den svenska tvångsmedelslagstiftningen måste därför hålla jämna steg inte bara med teknik- och samhällsutvecklingen i stort utan även med rättsutvecklingen i omvärlden. Risken är annars att Sverige inte kan biträda andra länder i deras utredningar av allvarlig brottslighet, eller att Sverige blir ett land där det är attraktivt att placera digital infrastruktur som används för illegala syften (se närmare härom avsnitt 7.4.4).

I det följande redovisar vi kortfattat hur några andra länders lagstiftning om hemlig dataavläsning är uppbyggd. I vår utblick utgår vi från en nederländsk jämförande rättsstudie om hemlig dataavläsning

[1] Europaparlamentets och rådets förordning (EU) 2023/1543 av den 12 juli 2023 om europeiska utlämnandeorder och europeiska bevarandeorder för elektroniska bevis i straffrättsliga förfaranden och för verkställighet av fängelsestraff eller annan frihetsberövande åtgärd till följd av straffrättsliga förfaranden.

som publicerades digitalt den 31 augusti 2023, i rapporten *De hackbevoegdheid in het Buitenland*, *cahier 2023-12*[2]. Rättsstudien är utförd av WODC (*Wetenschappelijk Onderzoek- en Documentatiecentrum*), ett nederländskt oberoende forsknings- och kunskapsorgan, på uppdrag av det nederländska Justitie- och säkerhetsministeriet (*Ministerie van Justitie en Veiligheid*). Studien finns allmänt tillgänglig även i engelsk översättning, i rapporten *Police Hacking regulation abroad – A comparative law study into legal regulations and safeguards regarding the quality of data*[3]. Rapporten kompletterar tidigare utvärderingar av den nederländska lagstiftningen om hemlig dataavläsning som trädde i kraft den 1 mars 2019. I de tidigare utvärderingar som gjorts har konstaterats att den nederländska lagstiftningen om användningen av tekniska verktyg och inspektionen av dessa ännu inte tillämpats som avsetts. Den nederländska lagstiftningen om hemlig dataavläsning utgör utgångspunkt för nämnda rapport som även innehåller fördjupade jämförande studier med motsvarande reglering i Sverige, Belgien, Tyskland, Frankrike och Schweiz.

10.4.2 Lagstiftning om hemlig dataavläsning utanför Sveriges gränser

Den nederländska rapporten visar att i princip alla EU-länder samt USA, Kanada och Australien har lagstiftning som möjliggör hemlig dataavläsning eller en motsvarighet till åtgärden. De EU-länder där det saknas lagstadgade möjligheter att använda en sådan åtgärd är enligt rapporten Lettland, Österrike, Slovenien, Bulgarien och Grekland (a. rapport s. 25 ff.).

Av den översiktliga jämförelse som gjorts mellan de länder som har lagstadgade möjligheter till hemlig dataavläsning framgår att de flesta länders regleringar är uppbyggda på liknande sätt, utifrån de grundläggande principer som även i Sverige gäller vid all tvångsmedelsanvändning. De särskilda kvalifikationskrav och rättssäkerhetsgarantier som omgärdar regelverken innefattar i de flesta länder särskilda krav på brottets allvar och andra särskilda villkor för åtgärdens användande, krav på dokumentation, särskilda bestämmelser om underrättelse till enskild samt särskilda krav på överföring och lagring av inhämtad information.

[2] http://hdl.handle.net/20.500.12832/3282, läst den 31 augusti 2023.
[3] https://repository.wodc.nl/handle/20.500.12832/3303, läst den 12 oktober 2023.

Av den fördjupade jämförande studien som omfattar lagstiftningarna i Nederländerna, Sverige, Belgien, Tyskland, Frankrike och Schweiz framgår att den svenska lagen om hemlig dataavläsning skiljer sig från lagstiftningen i de övriga länder som ingår i studien på flera sätt.

Inledningsvis kan det konstateras att Sverige som, i likhet med t.ex. Australien, Danmark, Norge, och Storbritannien, har ett särskilt oberoende organ (SIN) som utövar tillsyn över användningen av hemlig dataavläsning, är ensamt om denna ordning. Den nederländska Justitie- och säkerhetsinspektionen (*Inspectie Justitie en Veiligheid)*, som är en del av det nederländska Justitie- och säkerhetsministeriet (*Ministerie van Justitie en Veiligheid*), utövar emellertid också viss tillsyn. Denna tillsyn är dock begränsad till polisens verkställighet av hemlig dataavläsning och innefattar bl.a. krav på anställda, processer, rutiner och tekniska verktyg.

Vidare framgår att de övriga fem länderna har någon form av lagstadgat inspektions- och testförfarande för de tekniska verktyg som ska användas. Den nederländska lagstiftningen är den mest långtgående i detta avseende. I Nederländerna får hemlig dataavläsning som huvudregel endast verkställas med hjälp av ett tekniskt verktyg som på förhand har inspekterats och godkänts av en oberoende inspektionsenhet. I övriga fyra länder utförs inspektions- och testförfarandena inte av några oberoende kontrollorgan, utan huvudsakligen av samma myndighet som verkställer den hemliga dataavläsningen. I Belgien och Schweiz är detta polismyndigheten i respektive land och i Frankrike det statliga organet STNCJ (*Le Sérvice technique national de captation judiciaire*). När det gäller Tyskland står det inte helt klart vilket organ som utför tester och kontroller av tekniska verktyg. Det framgår inte heller av studien hur de olika test- och inspektionsförfarandena går till i de olika länderna. I Sverige är det de verkställande myndigheterna som är skyldiga att se till att de tekniska anpassningar som har gjorts är tillräckliga för att uppfylla de lagkrav som ställs. Dessa myndigheter, dvs. Polismyndigheten, Säkerhetspolisen och Tullverket, har särskilt upprättade interna riktlinjer om tester och inspektion av de tekniska verktyg som används vid hemlig dataavläsning. Dessa riktlinjer är, med hänsyn till åtgärdens natur, inte officiella. Säkerhets- och integritetsskyddsnämnden (SIN) utövar i sin tur tillsyn över användningen av hemlig dataavläsning. SIN har således befogenhet att utöva tillsyn över myndigheternas riktlinjer och de tekniska hjälpmedel som används vid hemlig dataavläs-

ning. SIN:s hittillsvarande granskningar har också innefattat myndigheternas riktlinjer om hemlig dataavläsning (se t.ex. nämndens uttalande med beslut av den 12 december 2021, dnr 92-2020, s. 4). Någon renodlad teknisk granskning av de verktyg som används har dock inte genomförts. Av den allmänna efterhandskontroll som sker i form av SIN:s tillsynsverksamhet har emellertid annat inte framkommit än att bestämmelserna om genomförande av hemlig dataavläsning uppfyller de krav på rättssäkerhet och informationssäkerhet som ställs (se avsnitt 8.5.1).

Slutligen framgår att Sverige är det enda av de studerade länderna som inte har några lagstadgade krav på dokumentation, rapportering eller säker överföring och lagring av inhämtad information. Övriga fem länders lagstiftningar innehåller uttryckliga krav på dokumentation samt särskilda krav på säker överföring och lagring av information. Belgiens och Frankrikes lagstiftningar innehåller dessutom krav på rapportering om hur åtgärden framskrider. Rapporteringskravet innebär att ett tillstånd till hemlig dataavläsning kan återkallas av domstolen under pågående verkställighet, baserat på de statusuppdateringar om verkställigheten som polis eller åklagare i dessa länder enligt lag är skyldig att lämna till domstolen. Den schweiziska lagstiftningen utmärker sig genom att källkoden för den tekniska enheten ska kunna kontrolleras i efterhand om domstolen begär det. I Sverige finns allmänna verkställighetsbestämmelser i 22–26 §§ lagen om hemlig dataavläsning. Själva verkställighetstekniken ingår dock inte i domstolsprövningen. Detta har varken ansetts lämpligt eller ändamålsenligt (jfr prop. 2019/20:64 s. 154 ff. och 158 ff.). I stället har verkställande myndigheter internt upprättade riktlinjer för verkställandet av hemlig dataavläsning. Dessa riktlinjer är, med hänsyn till åtgärdens natur och i likhet med riktlinjerna för tester och inspektion av de tekniska verktygen, inte officiella. SIN har utöver vad som nämnts ovan även en möjlighet att utöva tillsyn under pågående verkställighet. När det gäller frågan om dokumentation föreslår vi i avsnitt 8.5.5 att det ska införas en lagstadgad dokumentationsskyldighet för beslut och åtgärder som rör hemlig dataavläsning.

Sammantaget finner vi att redan förekomsten av lagreglerade möjligheter till hemlig dataavläsning i praktiskt taget alla EU-länder, samt USA, Kanada och Australien, innebär att åtgärden i vart fall i dessa länder bedömts vara tillräckligt effektiv och ge tillräcklig nytta för att motivera en sådan lagstiftning. Även tidigare internationella ut-

blickar visar att hemlig dataavläsning medför effektivitet och nytta i brottsbekämpningen i flera länder utanför Sveriges gränser (se t.ex. SOU 2017:89 s. 150 ff.). Det finns under alla omständigheter ett påtagligt behov av ändamålsenliga och effektiva verktyg i det internationella samarbete som syftar till att bekämpa den gränsöverskridande allvarliga brottsligheten. Vi bedömer därför att våra förslag i kapitel 6–8 medför bättre förutsättningar även för det internationella rättsliga samarbetet på området.

11 Ikraftträdande- och övergångsbestämmelser

Förslag: Lagändringarna ska träda i kraft den 1 mars 2025.

Äldre bestämmelser om möjligheter att använda överskottsinformation i rättegångsbalken och i preventivlagen ska gälla för uppgifter från tvångsåtgärder som verkställts före ikraftträdandet.

Äldre föreskrifter ska fortfarande gälla för tillstånd som har beviljats före ikraftträdandet.

Skälen för våra förslag

Våra förslag bör träda i kraft så snart som möjligt. Några behov av speciella informationsinsatser bedöms inte föreligga. Med hänsyn till sedvanlig tid för remissbehandling och beredning inom Regeringskansliet bedöms våra förslag kunna träda i kraft tidigast den 1 mars 2025.

Utgångspunkten när det gäller processrättslig lagstiftning är att nya regler ska tillämpas på varje processuell företeelse som inträffar efter det att regleringen har trätt i kraft. Förslagen i avsnitt 8.5.3 innebär att möjligheterna att använda överskottsinformation från hemlig dataavläsning under förundersökning och i preventivt syfte utökas. Av rättssäkerhetsskäl bör det inte vara tillåtet att använda sådan information i större utsträckning än vad som var tillåtet vid den tidpunkt då informationen samlades in. Med hänsyn till detta bör det föreskrivas att äldre bestämmelser ska tillämpas i fråga om överskottsinformation som samlats in före de nya reglernas ikraftträdande. När det gäller sådana tillstånd som har beslutats före ikraftträdandet, men som ännu inte har löpt ut, ska äldre föreskrifter fortfarande gälla. I övrigt behövs inte några övergångsbestämmelser.

12 Konsekvenser

12.1 Inledning

De krav som ställs på redovisningen av vilka konsekvenser som förslagen i ett betänkande kan få framgår huvudsakligen av 14–16 §§ kommittéförordningen (1998:1474). Av dessa bestämmelser framgår bl.a. följande. Om förslagen i betänkandet påverkar kostnaderna eller intäkterna för staten, kommuner, regioner, företag eller andra enskilda, ska en beräkning av dessa konsekvenser redovisas. Om förslagen innebär samhällsekonomiska konsekvenser i övrigt, ska även dessa redovisas. När det gäller kostnadsökningar och intäktsminskningar för staten, kommuner eller regioner, ska även en finansiering föreslås. Om förslagen i ett betänkande har betydelse för det kommunala självstyret, ska konsekvenserna i det avseendet anges i betänkandet. Detsamma gäller när ett förslag har betydelse 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. Härutöver följer av våra direktiv att vi särskilt ska beskriva vilka konsekvenser de förslag som lämnas har för det nationella och internationella skyddet för grundläggande fri- och rättigheter, såsom den personliga integriteten.

Problembeskrivningar, analyser av behov och nytta samt integritets- och proportionalitetsbedömningar i förhållande till alternativa lösningar framgår av våra övervägandekapitel. Där redovisar vi också våra bedömningar av hur förslagen förhåller sig till EU-rätten och Sveriges åtaganden när det gäller mänskliga rättigheter. I det här avsnittet fokuserar vi huvudsakligen på de samhällsekonomiska konsekvenserna av våra förslag samt på hur de kostnadsökningar som våra förslag bedöms innebära kan finansieras.

12.2 Våra förslag

Vi föreslår i avsnitt 6.5 att den tillfälliga lagen om hemlig dataavläsning ska permanentas. Åtgärden bedöms helt nödvändig med hänsyn till intresset av att bekämpa den allvarliga brottsligheten och för att upprätthålla enskildas rättstrygghet och rätt till skydd mot kränkningar från andra enskilda. Våra förslag i kapitel 7 och 8 beträffande de materiella bestämmelserna i lagen om hemlig dataavläsning innebär till övervägande del förtydliganden av lagstiftningen. Dessa syftar till att förenkla ansöknings- och beslutsprocessen samt undanröja den osäkerhet som i dag kan finnas angående ett tillstånds omfattning. Vi har i alla våra överväganden strävat efter att upprätthålla en välfungerande systematik i regelverket kring såväl hemliga som öppna tvångsmedel. De viktigaste konsekvenserna av våra förslag i kapitel 7 och 8 är att det blir tydligare under vilka förutsättningar som hemlig dataavläsning får användas, hur det inhämtade materialet ska hanteras och vilka skyldigheter som åligger tillämparen. Vi bedömer att våra förslag om en tydligare och mer förutsebar lagstiftning medför att lagen om hemlig dataavläsning kommer att stå i bättre överensstämmelse med de högt ställda krav på rättssäkerhet, informationssäkerhet och de krav på skydd för enskildas personliga integritet som följer av regeringsformen, Europakonventionen och EU-rätten. Några av våra förslag innebär även en viss utvidgning av tillämpningsområdet för hemlig dataavläsning och att de brottsbekämpande myndigheterna får mer effektiva verktyg i arbetet med att utreda samt förebygga, förhindra och upptäcka viss allvarlig brottslighet. Vi bedömer att det utökade tillämpningsområdet är avgränsat på ett tydligt och ändamålsenligt sätt. Vidare är våra förslag utformade med särskilda kvalifikationskrav och rättssäkerhetsgarantier för att balansera den ökade risken för intrång i den personliga integriteten som förslagen kan innebära. Våra förslag på ändringar i lagen om hemlig dataavläsning kan sammanfattas enligt följande.

- Bestämmelsen om innebörden av hemlig dataavläsning förtydligas, liksom vissa materiella bestämmelser i lagen (se avsnitt 7.2, 8.4.4, 8.4.5, 8.4.7 och 8.5.6).
- Bestämmelsen om vilka uppgiftstyper ett tillstånd till hemlig dataavläsning får omfatta förtydligas, samtidigt som det införs en huvudregel som tydliggör att ett typiskt tillstånd till hemlig dataavläs-

ning omfattar alla uppgiftstyper utom kameraövervaknings- och rumsavlyssningsuppgifter (se avsnitt 7.3.2).

- Det införs utökade möjligheter att utreda vem som skäligen kan misstänkas för visst brott eller delaktighet i viss brottslighet (se avsnitt 7.4.4).
- Bestämmelserna om ett tillstånds varaktighet och vilka villkor som ska anges i tillståndet ändras och förtydligas. Åklagaren, eller i förekommande fall Säkerhetspolisen, ska föreslå sådana villkor som ett tillstånd bör förenas med. Det införs också en ventil för situationer där det framstår som obehövligt att förena ett tillstånd till hemlig dataavläsning med villkor (se avsnitt 8.4.4 och 8.4.5).
- Användningsområdet för överskottsinformation från hemlig dataavläsning förtydligas (se avsnitt 8.5.3).
- Bestämmelserna om bevarande och förstöring av uppgifter från hemlig dataavläsning förtydligas (se avsnitt 8.5.4). Vidare förtydligas och utvecklas bestämmelsen om teknikanpassning och otillåten tilläggsinformation. Vi föreslår en bestämmelse som innebär att om otillåtna uppgifter påträffas så ska dessa uppgifter förstöras så snart det är möjligt (se avsnitt 8.5.6).
- Det införs ett lagstadgat dokumentationskrav för beslut och åtgärder som rör hemlig dataavläsning (se avsnitt 8.5.5).

12.3 Konsekvenser för det brottsbekämpande arbetet och för enskilda

Bedömning: Våra förslag innebär en ökad risk för den personliga integriteten men bidrar samtidigt till att förbättra möjligheterna för de brottsbekämpande myndigheterna att förebygga, förhindra, upptäcka och utreda allvarlig brottslighet, som innebär intrång i bl.a. brottsoffers personliga integritet. Därmed innebär förslagen en ökad rättstrygghet för enskilda. Vissa förslag leder också till en förbättrad rättssäkerhet. Förslagen ger sammantaget uttryck för en rimlig avvägning mellan behovet av en effektiv brottsbekämpning och den enskildes rätt till skydd för sin personliga integritet.

Skälen för våra bedömningar

Konsekvenser för det brottsbekämpande arbetet

Vårt förslag om att lagen om hemlig dataavläsning ska permanentas är en nödvändig anpassning till de senaste årens brotts-, teknik- och samhällsutveckling. Förslaget innebär att de brottsbekämpande myndigheterna kan fortsätta att bekämpa den allvarliga brottsligheten samt upprätthålla enskildas rättstrygghet och rätt till skydd mot kränkningar från andra enskilda. I kapitel 6 har vi mer utförligt redogjort för våra överväganden beträffande behovet och nyttan av hemlig dataavläsning, för åtgärdens olika konsekvenser för den personliga integriteten samt för våra proportionalitetsavvägningar.

Våra förslag får konsekvenser för det brottsbekämpande arbetet både under och utanför en förundersökning. Även förslag som direkt berör hemlig dataavläsning under förundersökning kan få indirekta konsekvenser för underrättelsearbetet. Våra förslag innebär förbättrade möjligheter för de brottsbekämpande myndigheterna att hämta in sådan information som inte är åtkomlig genom andra hemliga tvångsmedel. Förslagen innebär därmed bättre möjligheter att hämta in viktig information i ett tidigt skede av utredningen.

Våra egna förslag i den materiella lagstiftningen utgörs huvudsakligen av olika förtydliganden av nuvarande lagstiftning. Dessa förtydliganden syftar bl.a. till att förbättra de nuvarande möjligheterna för de brottsbekämpande myndigheterna att förebygga, förhindra, upptäcka och utreda allvarlig brottslighet.

Tillämpningsområdet för hemlig dataavläsning har nyligen utökats och ytterligare förslag om utökningar är för närvarande under beredning. Härutöver föreslår vi för egen del vissa utökningar av tillämpningsområdet för hemlig dataavläsning. Förslagen i avsnitt 7.4.4 innebär utökade möjligheter att använda hemlig dataavläsning under förundersökning för att identifiera en misstänkt gärningsman. Detta är information som på grund av anonymisering och kryptering inte går att få fram genom andra tvångsmedel. Som exempel på brottslighet där den föreslagna åtgärden skulle kunna användas med framgång kan nämnas terrorbrott, spionerі, narkotikahandel under alias på Darknet, grova dataintrång eller barnpornografibrott. I sådana utredningar är det många gånger omöjligt att genom traditionella tvångsmedel utreda vem eller vilka som ligger bakom den i övrigt fullt synliga brotts-

ligheten. Våra förslag kan därför innebära ett genombrott för brottsbekämpningen i detta avseende.

Förslaget i avsnitt 8.5.3 om att förtydliga bestämmelsen om användning av överskottsinformation från hemlig dataavläsning kan generellt sett förväntas leda till att fler allvarliga brott kan förhindras, utredas och lagföras.

Våra förslag om förbättrade möjligheter i utredningsarbetet kan sammantaget också förväntas leda till en ökad uppklarning av allvarliga brott. Förbättrade utredningsmöjligheter innebär generellt sett en ökad upptäcktsrisk och bättre förutsättningar att förhindra allvarlig brottslighet. På sikt kan våra förslag därför ha brottsförebyggande effekter och leda till att färre brott begås. Om fler personer lagförs för brott och döms till en frihetsberövande påföljd, kan det i sig leda till minskad brottslighet.

Våra förslag får indirekt genomslag även för det internationella straffrättsligt samarbetet (se kapitel 10). Bättre förutsättningar för internationellt rättsligt samarbete får i sin tur särskilt stor betydelse vid gränsöverskridande brottslighet som t.ex. internetrelaterade sexuella övergrepp mot barn samt narkotika- eller cyberbrottslighet.

Konsekvenser för enskilda

Bestämmelserna om hemlig dataavläsning utgör lagreglerade inskränkningar i det grundläggande skydd för privatlivet och den personliga integriteten som tillförsäkras enskilda i bl.a. regeringsformen, Europakonventionen och EU:s rättighetsstadga (se avsnitt 5.4). Vidare innebär hemlig dataavläsning i förhållande till andra hemliga tvångsmedel en ökad risk för intrång i den personliga integriteten (se kapitel 6).

Vårt förslag om att permanenta den hittills tillfälliga lagen om hemlig dataavläsning och flera av våra förslag på förändringar i regelverket innebär en viss ökad risk för den personliga integriteten. I våra övervägandekapitel har vi närmare redogjort för i vilka avseenden som våra förslag innebär ökade risker för den personliga integriteten och varför vi i våra avvägningar kommit till slutsatsen att våra förslag är försvarliga ur integritetssynpunkt. Vi har härvid framhållit att hemlig dataavläsning i flera avseenden också innebär ett förstärkt skydd för enskildas personliga integritet och en ökad rättstrygghet för enskilda. Detta framför allt med hänsyn till statens positiva förpliktel-

ser som innebär en skyldighet att skydda enskilda mot ingrepp i privatlivet från andra. Vi har i våra överväganden tagit hänsyn till att en kombination av olika mindre integritetsrisker kan ge anledning att beakta den samlade risken högre. Även vid en samlad proportionalitetsbedömning av hela det utökade tillämpningsområdet för hemlig dataavläsning har vi dock kommit till slutsatsen att lagstiftningen är ändamålsenligt och proportionerligt avgränsad. De risker som våra förslag innebär balanseras med höga krav för åtgärdens användande samt gedigna kontrollmekanismer och andra rättssäkerhetsgarantier. Våra förslag på ändringar i den materiella lagstiftningen är utformade på ett sätt som gör att det kommer att vara tydligare och mer förutsebart när och hur hemlig dataavläsning får användas (se särskilt avsnitt 7.2, 7.3.2, 8.4.4, 8.4.5, 8.4.7 och 8.5.3–8.5.6). Flera av förslagen skapar också bättre förutsättningar för efterhandskontroll (se särskilt avsnitt 8.4.5 och 8.5.5). Förslagen innebär i dessa delar ett förbättrat skydd mot otillåtna och obefogade integritetsintrång. Våra förslag bedöms mot denna bakgrund även innebära en förstärkt rättssäkerhet för den enskilde.

Även med beaktande av det samlade integritetsintrång som våra förslag och de nyligen ikraftträdda ändringarna innebär är det vår bedömning att regelverket för hemlig dataavläsning ger uttryck för en rimlig avvägning mellan behovet av en effektiv brottsbekämpning och den enskildes rätt till skydd för sin personliga integritet (se särskilt avsnitt 7.6 och 8.8).

12.4 Ekonomiska konsekvenser

Bedömning: Förslagen innebär att de brottsbekämpande myndigheterna får effektivare verktyg i kampen mot den allvarliga brottsligheten. Förslagen kan därför medföra betydande samhällsekonomiska besparingar inom ett flertal områden.

Det är av olika skäl förenat med svårigheter att uppskatta de ekonomiska konsekvenserna av våra förslag. De besparingseffekter som kan uppstå med anledning av förslagen kan inte uppskattas till något bestämt belopp.

Vårt förslag om att permanenta lagstiftningen om hemlig dataavläsning innebär att resursbehovet för berörda myndigheter i detta avseende permanentas. Våra förslag medför också en viss ökning av antalet tillstånd till hemlig dataavläsning och högre andel verkställbara beslut jämfört med i dag.

Säkerhetspolisen och Tullverket har uppskattat att myndigheternas resursbehov kommer att öka om våra förslag genomförs. De ökade kostnaderna avser huvudsakligen teknikkostnader och personalkostnader för att bibehålla och utveckla egen nödvändig teknisk förmåga på området. Säkerhets- och integritetsskyddsnämnden (SIN) har bedömt att nämndens tillsynsuppdrag, som en följd av våra förslag, kommer att öka i en sådan omfattning att nämnden bör tillföras ytterligare medel för att kunna utföra en effektiv och rättssäker tillsyn. De resursbehov som uppkommer för dessa myndigheter föreslås huvudsakligen finansieras genom att medel tillförs från andra utgiftsområden. Även Polismyndigheten och Sveriges Domstolar, inklusive anslaget för rättsliga biträden, kommer att få vissa ökade kostnader med anledning av våra förslag, men dessa kostnader bedöms rymmas inom befintliga anslag. Detsamma gäller de ökade kostnader som våra förslag kan komma att medföra för Skatteverket, Finansinspektionen och Kriminalvården. Beträffande övriga berörda aktörer – Åklagarmyndigheten, Ekobrottsmyndigheten och företag som medverkar vid verkställighet – bedöms genomförandet av våra förslag inte medföra några ökade kostnader.

Skälen för våra bedömningar

Utgångspunkter och antaganden

Att bedöma de ekonomiska konsekvenserna av våra förslag är förenat med flera svårigheter. I våra prognoser utgår vi från antagandet om att våra förslag inte leder till någon stor ökning av användningen av hemlig dataavläsning jämfört med i dag, räknat i antal meddelade tillstånd. Vi antar även att andelen verkställbara beslut komma att öka något. Eftersom det i dag inte förs någon statistik över antalet verkställbara beslut kan vi inte göra någon närmare prognos än att det handlar om en viss ökning av andelen verkställbara beslut. Som kommer att framgå i det följande är dessa antaganden förenade med flera osäkerhetsmoment.

Till ledning för våra beräkningar av kommande resursbehov har vi, baserat på våra antaganden, utgått från tidigare prognoser jämfört med den hittillsvarande resursåtgången. Det ska redan här framhållas att våra beräkningar som redovisas nedan utgör grova uppskattningar av kommande resursbehov.

Det står vidare klart att våra förslag också medför betydande samhällsekonomiska besparingar inom ett flertal områden. Hur stora dessa besparingar kan komma att bli, räknat i kronor, kan dock inte uppskattas till något bestämt belopp.

För att slutligen kunna ta ställning till hur de uppskattade kostnadsökningarna bör finansieras redogör vi i det följande också för hur anslagen för berörda myndigheter har sett ut i de tidigare budgetpropositionerna.

En viss ökning av antalet tillstånd och en högre andel verkställbara beslut

Enligt de brottsbekämpande myndigheternas årliga redovisningar meddelas i dag cirka 300–600 tillstånd till hemlig dataavläsning per år. Siffran kan jämföras med antalet tillstånd till hemlig avlyssning av elektronisk kommunikation som de senaste åren har varierat mellan cirka 3 900–5 100 tillstånd/år (se avsnitt 6.3.1). Som vi har redogjort för i våra övervägandekapitel har olika oklarheter och otydligheter i lagstiftningen om hemlig dataavläsning lett till att verkställigheten av vissa tillstånd har varit förenad med svårigheter. Någon statistik

över antalet verkställbara beslut finns inte att tillgå. Det kan dock konstateras att motsvarande svårigheter inte finns vid verkställighet av hemlig avlyssning av elektronisk kommunikation. Särskilt förslaget om ett förtydligande av bestämmelsen om de olika uppgiftstyperna (se avsnitt 7.3.2) bedöms, tillsammans med förslagen om en tydligare verkställighets- och villkorsreglering (se avsnitt 8.4.4 och 8.4.5), leda till fler verkställbara beslut om hemlig dataavläsning jämfört med i dag.

Tillämpningsområdet för hemlig dataavläsning har nyligen utökats och vi föreslår i detta betänkande vissa ytterligare utökningar. Vidare innebär våra förslag om ett tydligare och mer förutsebart regelverk att både tillståndsförfarandet och verkställigheten av hemlig dataavläsning kommer att effektiviseras. Våra förslag på förbättrade rättsliga förutsättningar bedöms sammantaget kunna leda till en ökad användning av hemlig dataavläsning. Därtill kommer att antalet redovisade tillstånd till hemlig dataavläsning har ökat varje år sedan lagens ikraftträdande (se avsnitt 6.3.1 och 6.3.3). Mycket talar därför för att ett permanentande av den hittills tillfälliga lagen kommer att medföra en fortsatt ökning av antalet tillstånd de närmsta åren. Hur stor ökningen kan komma att bli beror på flera samverkande faktorer. Hemlig dataavläsning är ett relativt nytt hemligt tvångsmedel som ställer höga krav på verkställighetstekniken. Utöver tekniska och rättsliga förutsättningar är det flera andra omständigheter som påverkar användningen av hemlig dataavläsning. Förutsättningarna och omfattningen av tillämpningen är som vi tidigare har redogjort för beroende av ett flertal faktorer som inte styrs av regelverket som sådant. Hit hör exempelvis brottsutvecklingen, hur den brottsbekämpande verksamheten organiseras och hur resurser utnyttjats. Det är redan mot denna bakgrund svårt att fullt ut överblicka hur stor ökningen, räknat i antalet meddelade tillstånd, kommer att bli. Det nya tvångsmedlet genomsökning på distans överlappar till viss del hemlig dataavläsning och kommer därför troligen att ersätta vissa av tillstånden till hemlig dataavläsning under förundersökning. På motsvarande sätt kan förslaget om genomsökning på distans utanför förundersökning komma att ersätta vissa av tillstånden till hemlig dataavläsning utanför förundersökning (se avsnitt 4.3.4). Vidare, om Datalagringsutredningens förslag om att ålägga tillhandahållare av s.k. Noik-tjänster en anpassningsskyldighet för HAK genomförs, kan även beslut om HAK till viss del komma att ersätta beslut om hemlig dataavläsning (se av-

snitt 4.2.3). Som inledningsvis redogjorts för har hemlig dataavläsning hittills endast använts i ett begränsat antal fall, både i absoluta tal och jämfört med andra hemliga tvångsmedel. Vår samlade bedömning är att våra förslag inte leder till någon stor ökning av hemlig dataavläsning, räknat i antal meddelade tillstånd. Flertalet av dessa tillstånd bedöms i sin tur bli verkställbara.

Prognoser och ökade anslag inför införandet av hemlig dataavläsning

Inför införandet om lagen om hemlig dataavläsning bedömde Utredningen om hemlig dataavläsning att hemlig dataavläsning skulle medföra ökade kostnader för de brottsbekämpande myndigheterna. Kostnaderna beräknades av utredningen uppgå till cirka 100 miljoner kronor årligen. I kostnadsberäkningen innefattades nyrekrytering, utbildning, kompetensutveckling, anskaffning av teknisk utrustning, drift och underhåll samt kostnader för medverkande operatörer. Däremot innefattades inte kostnader för sådana resurser som krävs för kartläggning inför hemlig dataavläsning eller sådana resurser som krävs för bearbetning av det inhämtade materialet. Sådana kostnader bedömdes rymmas inom befintliga anslag efter omdispositioner. Utredningen konstaterade att den enskilt största posten som skulle tillkomma med hemlig dataavläsning avsåg inköp av nödvändig teknisk utrustning. Kostnaden för (Polismyndighetens) investering i teknisk utrustning (anläggningstillgångar) bedömdes därför kunna finansieras genom ianspråktagande av låneramar. Detta innebar att kostnaden för utrustningen bedömdes komma att belasta myndighetens resultat genom årliga avskrivningar. Övriga verkställande myndigheter antogs komma att bidra till finansieringen genom licensavgifter eller liknande till Polismyndigheten. Vidare bedömde utredningen att hemlig dataavläsning skulle medföra ökade kostnader för Säkerhets- och integritetsskyddsnämnden med 1,5 miljoner kronor årligen. De mindre kostnadsökningar som hemlig dataavläsning förväntades medföra för Sveriges Domstolar, offentliga ombud och Åklagarmyndigheten bedömdes rymmas inom befintliga anslag. Härutöver bedömdes förslagen om hemlig dataavläsning inte medföra några ökade kostnader.

Utifrån de uppgifter som utredningen redovisade, samt de remissvar som inkom, bedömde regeringen sedan att hemlig dataavläsning

skulle leda till ökade löpande kostnader för Polismyndigheten med 65 miljoner kronor/år, för Säkerhetspolisen med 35 miljoner kronor/år och för Tullverket med 12,5 miljoner kronor/år. Ekobrottsmyndighetens ökade resursbehov uppskattades inte till något exakt belopp. I budgetpropositionen för 2020 höjdes anslagen för Polismyndigheten och Säkerhetspolisen för att finansiera uppskattade kostnadsökningar med anledning av den nya lagen om hemlig dataavläsning. Tullverket erhöll inte något utökat anslag kopplat till införandet av den nya lagen. Regeringen bedömde att Ekobrottsmyndighetens förmåga att hantera hemlig dataavläsning kunde hanteras inom det ökade anslag om 19 miljoner kronor/år (35 miljoner kronor/år fr.o.m. år 2021) avseende resurskrävande ärenden som samtidigt avsattes till myndigheten. Regeringen bedömde att de ökade kostnaderna för Sveriges Domstolar, offentliga ombud och Åklagarmyndigheten kunde rymmas inom befintliga anslag. Regeringen bedömde att inga ökade kostnader för Säkerhets- och integritetsskyddsnämnden skulle uppstå med anledning av förslagen, dvs. att nämnden skulle kunna utföra de nya uppgifterna inom tilldelade ramar. Regeringen instämde slutligen i utredningens bedömning att hemlig dataavläsning inte skulle medföra några ekonomiska konsekvenser i övrigt (se prop. 2019/20:64 s. 205 ff.).

Ökade anslag i budgetpropositionen för 2023

I budgetpropositionen för 2023 tillfördes Polismyndigheten, Åklagarmyndigheten, Tullverket, Ekobrottsmyndigheten, Säkerhets- och integritetsskyddsnämnden (SIN), Skatteverket och Sveriges Domstolar ökade medel från och med 2024. Syftet var att finansiera de ökade kostnader som de utökade möjligheterna att använda hemliga och preventiva tvångsmedel, hemlig dataavläsning inkluderat, bedömdes medföra. De utökningar som åsyftades var de lagändringar som trädde i kraft den 1 oktober 2023 (se prop. 2022/23:126 samt kapitel 7 och 8). De ökade anslagen framgår av prop. 2022/23:1, utgiftsområde 3 och 4, och fördelar sig på följande sätt:

- Polismyndigheten 130 miljoner kronor/år.
- Åklagarmyndigheten 30 miljoner kronor/år.
- Ekobrottsmyndigheten 20 miljoner kronor/år.
- Sveriges Domstolar 10 miljoner kronor/år.
- SIN 4,2 miljoner kronor/år.
- Skatteverket 8 miljoner kronor/år.
- Tullverket 65 miljoner kronor/år.

Som framgår av redogörelsen tilldelades inte Säkerhetspolisen några ytterligare medel med anledning av de lagändringar som trädde i kraft den 1 oktober 2023. Skälet var att lagändringarna, till skillnad från de förslag som vi nu lägger fram, inte bedömdes påverka myndigheten ekonomiskt i någon större utsträckning (jfr prop. 2022/23:126 s. 197 ff.). Resursfördelningen i 2023 års budgetproposition påverkar de olika myndigheternas ytterligare resursbehov med anledning våra förslag i detta betänkande, se vidare nedan.

Våra förslag medför betydande samhällsekonomiska besparingar

Mer effektiva verktyg för att förebygga, förhindra, upptäcka och utreda allvarlig brottslighet bedöms få stora positiva samhällsekonomiska konsekvenser. Förbättrade möjligheter att förhindra och klara upp brott besparar inte bara rättsväsendet kostnader. Även personligt lidande för brottsoffer, potentiella brottsoffer och anhöriga minskar. Förslagen kan medföra betydande samhällsekonomiska besparingar kopplade till exempelvis sjukvården, sociala myndigheter, Skatteverket och Försäkringskassan. De samhällsekonomiska kostnader som den allvarliga brottsligheten medför är avsevärda. Kostnaderna är svåra att beräkna men knappast obetydliga ens för ett enskilt fall. De besparingar som kan uppstå med anledning av förslagen kan därför inte heller inte uppskattas till något bestämt belopp. Det kan dock konstateras att det rör sig om betydande besparingseffekter.

Våra förslag medför ökade kostnader

Användningen av hemlig dataavläsning är som tidigare framhållits mycket resurskrävande för de brottsbekämpande myndigheterna. Hemlig dataavläsning påverkar kostnaderna även för andra aktörer, däribland Säkerhets- och integritetsskyddsnämnden (SIN) och Sveriges Domstolar.

De ekonomiska prognoser som gjordes inför ikraftträdandet av lagen om hemlig dataavläsning byggde på olika antaganden och uppskattningar. I vissa delar har prognoserna huvudsakligen överensstämt med utfallet. Detta gäller med undantag för den resursåtgång som beräknades för SIN, Polismyndigheten, Säkerhetspolisen och Tullverket. Utfallet beror både på att hemlig dataavläsning har använts i större utsträckning än förväntat och att det har visat sig dyrare än beräknat att bedriva HDA-verksamheten, se vidare nedan.

Vårt förslag om att permanenta lagstiftningen om hemlig dataavläsning innebär att resursbehovet för berörda myndigheter i detta avseende permanentas. Våra förslag om ändringar i den materiella lagstiftningen bedöms sammantaget innebära en viss ökning av antalet tillstånd till hemlig dataavläsning samt en högre andel verkställbara beslut. Detta kan i sin tur innebära ytterligare ökade kostnader för berörda myndigheter.

De beräkningar som presenteras i det följande utgår huvudsakligen från underlag som företrädare för SIN och de olika brottsbekämpande myndigheterna har sammanställt på förfrågan av utredningen.

Polismyndigheten

Företrädare för Polismyndigheten har uppgett att hemlig dataavläsning har använts i större utsträckning än vad som uppskattades vid lagens införande. Våra föreslag innebär att lagstiftningen ska permanentas och till viss del utvidgas. Detta kommer enligt företrädare för Polismyndigheten att leda till ett ökat behov av teknisk utrustning och personal, vilket innebär ökade kostnader för Polismyndigheten. Den preliminära bedömningen är dock att myndigheten kommer att kunna hantera dessa ökade kostnader inom befintliga anslag.

Säkerhetspolisen

Företrädare för Säkerhetspolisen har konstaterat att HDA-verksamheten har varit dyrare att bedriva än de 35 miljoner kronor/år som ursprungligen uppskattades. Enligt myndighetens egna beräkningar uppgår Säkerhetspolisens kostnader för verkställande av hemlig dataavläsning under 2023 till cirka 55 miljoner kronor. De överskjutande kostnaderna om 20 miljoner kronor har finansierats genom omfördelningar inom myndighetens ram, vilket har inneburit att andra delar av Säkerhetspolisens verksamhet fått stå tillbaka.

I den årliga kostnaden för hemlig dataavläsning inryms personalkostnader, kostnader för anskaffade produkter, kostnader för infrastruktur, livscykelkostnader för diverse hårdvaror samt inköp av testutrustning. Företrädare för Säkerhetspolisen har till utvecklande av vilka kostnader som hemlig dataavläsning (HDA) har inneburit och kommer att innebära för myndigheten framhållit följande.

Verkställande av HDA kräver att omfattande arbete gjorts i förväg i syfte att – till att börja med – hitta sårbarheter i det avläsningsbara informationssystemet i fråga och – i nästa steg – utveckla förmåga att exploatera dessa sårbarheter på ett sätt som fungerar på det avsedda målsystemet. Av flera skäl är det också nödvändigt att se till att verkställandet löper minimal risk att upptäckas, vilket ställer extra höga krav på förmåga och tillvägagångssätt. Personal med rätt slags kompetens för att framgångsrikt bedriva detta slags arbete är svår att hitta, och de personer som innehar nödvändiga fördjupade kunskaper och färdigheter är vanligtvis mycket eftertraktade på arbetsmarknaden, inte minst av it-säkerhetsföretagen.

I vissa fall är det möjligt att köpa förmåga att bedriva HDA från externa leverantörer. Sådan anskaffning kan avse enstaka komponenter som kan komplettera den egna utvecklingen, eller färdiga systemlösningar som inte kräver något kompletterande eget utvecklingsarbete. I båda dessa fall är det fråga om mycket dyra produkter, vilket förklaras av att leverantörernas forsknings- och utvecklingsarbete är omfattande, samtidigt som marknaden, i form av antalet tänkta köpare av sådana produkter, är begränsad. Användning av lösningar från externa leverantörer löper av olika skäl större risk att upptäckas av målen själva, eller av andra aktörer ”längs vägen”, t.ex. tjänsteleverantörer, jämfört med egenutvecklade lösningar, förutsatt att de sistnämnda håller hög kvalitet. För de typer av brott och brottslig

verksamhet som utgör Säkerhetspolisens ansvarsområde är användning av externa lösningar av olika skäl ofta riskabel. Säkerhetspolisen har därför ett stort behov av att bedriva egen förmågeutveckling på området.

Den tekniska utvecklingen är i ständig rörelse. Nya typer och versioner av de avläsningsbara informationssystemen, och de programvaror dessa nyttjar, släpps ständigt på marknaden. De företag som tillhandahåller datorer, telefoner, operativsystem och andra programvaror lägger stora resurser på att upptäcka och täppa till sårbarheter och andra säkerhetsluckor, varför specifik HDA-förmåga mot en viss typ av avläsningsbart informationssystem ofta är kortlivad. Detta gör att anskaffning av HDA-förmåga inte tar sig formen av en engångskostnad, utan HDA är ett instrument som är förenat med stora kostnader varje år, eftersom arbetet med att upptäcka och exploatera nya sårbarheter aldrig upphör, oavsett om detta arbete bedrivs av externa leverantörer eller av egen personal.

Hittillsvarande erfarenheter har påvisat ett tydligt verksamhetsbehov för Säkerhetspolisen att ytterligare utöka den egna HDA-förmågan. Andelen ärenden där HDA inte går att verkställa är fortfarande besvärande hög, och det ska poängteras att Säkerhetspolisen inte begär tillstånd för HDA i sådana fall där myndigheten redan på förhand kan bedöma att utsikterna till ett framgångsrikt verkställande är obefintliga, t.ex. för att man för stunden inte har någon förmåga mot en viss typ av avläsningsbart informationssystem. Det är besvärande ur rättssäkerhetssynpunkt att möjligheterna att utreda ett brott eller att avbryta förestående brottslig verksamhet är avhängig exempelvis vilka modeller av de avläsningsbara informationssystemen som används av de individer som är föremål för hemliga tvångsmedel. Ytterligare satsningar på HDA-förmåga är därför nödvändiga.

Satsningar på utökad egenutvecklad HDA-förmåga är långsiktiga, eftersom nyrekryterad utvecklingspersonal på detta område ofta behöver en relativt lång upplärningsperiod. Den tekniska utvecklingen avstannar inte och säkerhetsfunktionerna i de avläsningsbara informationssystemen uppdateras ständigt, vilket innebär att arbetet med förmågeutveckling blir långsiktigt och löpande till sin natur. Om HDA-lagstiftningen permanentas blir det motiverat för Säkerhetspolisen att genomföra nödvändiga ökade satsningar på egen förmågeutveckling, vilka hittills fått stå tillbaka med hänsyn till att lagstiftningen varit tillfällig.

Säkerhetspolisen ser därför, utöver de 55 miljoner kronor/år som myndigheten i dag avsätter för kostnader för HDA, ett behov av ytterligare 28 miljoner kronor årligen, för att bibehålla och utveckla nödvändig egen förmåga på området. Totalt handlar det alltså om 28 miljoner kronor/år som inte bedöms rymmas inom befintlig anslagsram. Dessa ytterligare medel avser i huvudsak personalkostnader, men även årliga kostnader för verktyg som behövs i det egna utvecklingsarbetet. Eftersom den personal som krävs är svårrekryterad, kan de dessa ytterligare 28 miljoner kronor med fördel fördelas successivt, lämpligen i jämna steg under en fyraårsperiod, dvs:

- 2025: 7 miljoner kronor.
- 2026: 14 miljoner kronor.
- 2027: 21 miljoner kronor.
- 2028 och framåt: 28 miljoner kronor/år.

Som tidigare nämnts har 2021 års datalagringsutredning (SOU 2023:22) föreslagit att samtliga leverantörer av interpersonella kommunikationstjänster, dvs. inte bara de tjänster som baseras på användning av traditionella telefonnummer, ska åläggas samma anpassningsskyldighet för HAK och HÖK. Om Datalagringsutredningens förslag genomförs bedömer Säkerhetspolisen att antalet ärenden där användning av HDA är nödvändigt kommer att minska. Exakt hur de årliga kostnaderna för HDA skulle påverkas beror på hur den föreslagna anpassningsskyldigheten utformas, vilka leverantörer och tjänster som undantas och på vilket sätt de leverantörer som träffas uppfyller sina skyldigheter. Men eftersom HDA-lagstiftningen till stor del kan ses som en kompensatorisk åtgärd för avsaknaden av en sådan anpassningsskyldighet, bedöms kostnaderna för HDA markant kunna reduceras om förslagen i Datalagringsutredningen genomförs.

Tullverket

Företrädare för Tullverket har konstaterat att kostnaderna för hemlig dataavläsning (HDA) har varit större än de 12,5 miljoner kronor/år som uppskattades vid införandet. Tullverket uppskattar att myndighetens kostnader för HDA hittills har uppgått till 16,5 miljoner kronor/år, varav 12,5 miljoner kronor avser teknikkostnader och 4 mil-

joner kronor personalkostnader. Tullverket erhöll inte något utökat anslag kopplat till införandet av HDA. Kostnaderna för HDA har således hittills finansierats genom omfördelningar inom myndighetens ram. Företrädare för Tullverket har till utvecklande av vilka kostnader som HDA har inneburit och kommer att innebära för myndigheten framhållit följande.

Det finns ett tydligt och påtagligt behov av att utöka den egna förmågan avseende HDA framöver. Behovet av att utöka förmågan är långsiktigt, vilket i sin tur innebär att om lagstiftningen permanentas finns det motiverande skäl för Tullverket att genomföra de inköp/uppgraderingar av teknik- och personalsatsningar som Tullverket har sett ett nödvändigt behov av.

Det är svårt att på förhand göra en beräkning av vad teknikkostnaderna för Tullverket kommer att vara framöver då dessa är osäkra. De kostnadsberäkningar som lämnas utgörs därmed av uppskattningar. Det som påverkar är bland annat kostnaden för den teknik som inhandlas, livslängden på tekniken och hur fördelningsmodellen mellan Tullverket och andra berörda myndigheter av kostnader (för bland annat system avseende verkställande av HDA) kommer att se ut. Tullverkets uppskattning är att det minst vart tredje år kommer att krävas kompletterande tekniska system för att Tullverket ska kunna upprätthålla sin förmåga avseende verkställandet av HDA. Teknikkostnaden kommer enligt Tullverkets uppskattning från och med år 2024 att öka från 12,5 miljoner kronor/år till 16 miljoner kronor/år för myndigheten. Dessutom, som ett led i att utöka den egna förmågan om lagstiftningen permanentas, behöver Tullverket köpa in system för bearbetning av den informationen som generas från inhämtningen vid HDA. Behovet av att omhänderta informationen är densamma för Tullverket som för andra brottsbekämpande myndigheter. Kostnaderna för system för bearbetning uppskattar Tullverket till dels ett engångsbelopp om 10 miljoner kronor avseende hårdvaruinköp, dels ett belopp om 20 miljoner kronor/år avseende licenskostnader samt, efter första året, en årlig kostnad på 2 miljoner kronor avseende återinvestering av hårdvara. Systemet är nödvändigt att köpa in för Tullverket. För det fall Tullverket inte skulle få ett ökat anslag för systemet skulle Tullverket behöva prioritera om, så att andra delar av Tullverkets verksamhet får stå tillbaka, eller prioritera ner sin förmåga avseende HDA.

Därtill tillkommer kostnader för personal. Tullverkets uppfattning är att personalkostnaderna kommer att öka med motsvarande fyra årsarbetskrafter, uppgående till totalt cirka 3,4 miljoner kronor/år. Detta innebär att personalkostnaderna för myndigheten kommer att öka från 4 miljoner kronor/år till 7,4 miljoner kronor/år. De ökade kostnaderna kan till viss del härledas från de förslag som föreslås i utredningen om en något utvidgad möjlighet att använda HDA, en ökad möjlighet att använda överskottsinformation samt den skyldighet som föreslås för bland annat Tullverket att förstöra uppgifter som inte får granskas eller inhämtas. Den övervägande delen beror dock på att det krävs mer personal för att arbeta med HDA än vad Tullverket beräknade initialt när lagen trädde i kraft. Detta med hänsyn till att det krävs en bemanning på dygnets alla timmar och att det bedöms nödvändigt som en del av Tullverkets satsning att öka sin förmåga avseende HDA.

Sammanfattningsvis är det Tullverkets uppskattning att utredningens förslag medför följande ytterligare kostnader för myndigheten, dvs. kostnader som inte ryms inom befintlig anslagsram:

- Engångskostnad: 10 miljoner kronor, avseende hårdvaruinköp.
- 2025: 43,4 miljoner kronor, varav 7,4 miljoner kronor avser personalkostnader och 36 miljoner kronor teknikkostnader.
- 2026 och framåt: 45,4 miljoner kronor/år, varav 7,4 miljoner kronor avser personalkostnader, 36 miljoner kronor teknikkostnader och 2 miljoner kronor återinvestering av hårdvara.

Åklagarmyndigheten

Våra förslag om utökade möjligheter att använda hemlig dataavläsning för att identifiera en skäligen misstänkt och de ökade möjligheterna att använda sig av överskottsinformation kan komma att innebära fler ärenden för Åklagarmyndigheten. Företrädare för Åklagarmyndigheten har härutöver framhållit att man generellt sett räknar med att antalet ärenden där hemlig dataavläsning används kommer att fortsätta att öka ett antal år framåt. Först därefter förväntar man sig en sådan stabilisering av antalet ärenden från år till år som man kan se avseende övriga hemliga tvångsmedel. Enligt Åklagarmyndigheten hänger det förhållandet inte samman med de förslag som förs fram i utred-

ningen, utan snarare med att hemlig dataavläsning fortfarande är ett relativt nytt hemligt tvångsmedel. Åklagarmyndigheten har sammantaget bedömt att den förväntade förändringen för myndigheten kommer att vara marginell. De förslag som läggs fram av utredningen förväntas därför inte innebära något ökat resursbehov för myndigheten.

Ekobrottsmyndigheten

Företrädare för Ekobrottsmyndigheten har anslutit sig till vad Åklagarmyndigheten har anfört beträffande förväntade konsekvenser av förslagen och sammantaget bedömt att utredningens förslag inte medför något ökat resursbehov för Ekobrottsmyndigheten.

Säkerhets- och integritetsskyddsnämnden

Eftersom hemlig dataavläsning innebär en ökad risk för integritetsintrång jämfört med övriga hemliga tvångsmedel är det nödvändigt att denna risk vägs upp av en effektiv tillsyn. Våra förslag innebär inte bara att hemlig dataavläsning permanentas utan även att möjligheten att använda tvångsmedlet utvidgas. Mot denna bakgrund krävs enligt Säkerhets- och integritetsskyddsnämnden (SIN) en förstärkt tillsyn över området.

SIN har konstaterat att den bedömning av konsekvenserna för tillsynen som gjordes i samband med att lagen om hemlig dataavläsning infördes visat sig vara otillräcklig. Det beror enligt SIN till stor del på att hemlig dataavläsning använts i betydligt större utsträckning än förväntat. Tvångsmedlet ställer också, genom sin tekniskt komplicerade struktur, delvis andra krav på tillsynen än övriga tvångsmedel. SIN har framhållit att man inte haft möjlighet att fullt ut fördjupa tillsynen på området på ett ändamålsenligt sätt. Dessutom har utredningen konstaterat att antalet tillstånd till hemlig dataavläsning i viss mån kommer att öka till följd av de nu framlagda förslagen. För att SIN ska fungera som den rättssäkerhetsgaranti som utredningen betonar krävs enligt nämnden extra resurser för tillsyn över hemlig dataavläsning.

De framlagda förslagen innebär i delar att brottsbekämpande myndigheter kommer få använda hemlig dataavläsning på sätt som tidigare inte varit möjligt. Därutöver föreslås ändringar beträffande hur

ansökan om och tillstånd till hemlig dataavläsning ska utformas, vilket enligt SIN har direkt effekt på rättssäkerheten och integriteten. SIN menar att förslagen i dessa delar innebär att det finns behov av ytterligare resurser för att upparbeta nya metoder och former för tillsyn på området. SIN bedömer att förslagen motiverar att anslaget till myndigheten utökas med cirka 3 miljoner kronor/år för att täcka nödvändiga kostnader för personal, it-stöd och lokaler. Kostnaden bedöms inte rymmas inom befintlig anslagsram.

Sveriges Domstolar och anslaget Rättsliga biträden m.m.

Alla frågor om hemlig dataavläsning ska prövas av allmän domstol och i alla ärenden om hemlig dataavläsning ska ett offentligt ombud utses. Mot bakgrund av våra inledande antaganden kan det uppskattningsvis bli fråga om en ökning av antalet ärenden i domstolarna med cirka 10–20 procent jämfört med i dag. Det förs dock inte någon statistik över antal ärenden, antal sammanträden, tidsåtgång etc. när det gäller domstolsärenden om hemlig dataavläsning eller andra hemliga tvångsmedel för den delen. Det förs inte heller någon särskild statistik över kostnaderna för offentliga ombud i tvångsmedelsärenden. Det saknas därför underlag för att närmare kunna bedöma hur stor resursökning våra förslag kommer att innebära. Det står dock klart att våra förslag innebär ökade kostnader för de allmänna domstolarna, vilka sorterar under anslaget för Sveriges Domstolar. Sveriges Domstolar tilldelades i budgetpropositionen för 2023 ett ökat anslag fr.o.m. 2024, för kostnader med anledning av utökade möjligheter att använda hemliga tvångsmedel. Vi bedömer att våra förslag inte påverkar resursbehovet för Sveriges Domstolar i större omfattning än att ökningen bedöms rymmas inom den befintliga anslagsramen.

Vidare innebär våra förslag även att offentliga ombud kommer att behövas i fler ärenden än i dag. Som ovan konstateras är det svårt att i kronor mäta detta ökade resursbehov. Med utgångspunkt från vårt antagande om en ökning av antalet ärenden med cirka 10–20 procent bedömer vi att våra förslag inte medför någon betydande kostnadsökning för anslaget för Rättsliga biträden m.m. Vi bedömer därför att de ökade kostnader som våra förslag medför inte är större än att de kan hanteras inom ramen för befintligt anslag.

Skatteverket, Finansinspektionen och Kriminalvården

Skatteverket biträder Ekobrottsmyndigheten i många utredningar om allvarlig brottslighet. Det förekommer även att Finansinspektionen biträder Ekobrottsmyndigheten i sådana utredningar. Även med beaktande av att våra förslag inte bedöms medföra några kostnadsökningar för Ekobrottsmyndigheten kan förslagen komma att innebära vissa kostnadsökningar för Skatteverket och Finansinspektionen.

Vidare bedöms våra förslag leda till en ökad lagföring när det gäller allvarlig brottslighet. Detta kommer att innebära en ökad belastning för Kriminalvården.

Det är inte möjligt att göra några bedömningar av vilka resursökningar som kan bli aktuella i dessa avseenden. De ökade kostnader som våra förslag kan komma att innebära för Skatteverket, Finansinspektionen och Kriminalvården får under angivna förutsättningar anses rymmas inom befintliga anslag.

Företag som medverkar vid verkställighet

De företag som bedriver verksamhet enligt lagen (2022:482) om elektronisk kommunikation är skyldiga att medverka i samband med verkställighet av hemlig dataavläsning. I praktiken handlar det om vissa operatörer av mobiltelefoni och internet. Dessa operatörer har rätt till ersättning för kostnader som uppstår vid sådan medverkan, Medverkansskyldigheten och rätten till ersättning framgår av 24 § lagen om hemlig dataavläsning jämte 3–4 §§ förordningen (2020:172) om hemlig dataavläsning.

Företrädare för en av de större operatörerna har till utredningen framfört att det förekommer ärenden som stannar vid rena förfrågningar till operatören och som således aldrig leder till någon verkställighet av hemlig dataavläsning. Även i dessa ärenden kan det uppstå kostnader för operatören i form av t.ex. utredningskostnader. Det har dock inte begärts ersättning för sådana kostnader eftersom man bedömt dessa som icke ersättningsgilla.

Det framgår av förarbetena till 24 § lagen om hemlig dataavläsning att omfattningen av medverkansskyldigheten beror på hur den verkställande myndigheten formulerar sin begäran. Det kan t.ex. handla om att operatören ger råd eller bistår med olika stödåtgärder (se prop. 2019/20:64 s. 237). Vidare utgör uppräkningen i 3 § för-

ordningen om hemlig dataavläsning endast en exemplifiering av vad en medverkan kan omfatta. Bestämmelsen i 24 § lagen om hemlig dataavläsning är avsedd att vara kostnadsneutral för företagen. Som bestämmelsen är utformad är medverkansskyldigheten också direkt kopplad till rätten att få ersättning för kostnader. Vår bedömning är därmed att lagstiftningen även i praktiken är kostnadsneutral och således inte ska medföra några kostnader för de operatörer som medverkar vid verkställighet. Med hänsyn till den osäkerhet som har uppstått i praktiken kan dock finnas anledning till att se över formerna för dialogen mellan operatörerna och de brottsbekämpande myndigheterna. Denna fråga är emellertid inte möjlig att behandla inom ramen för detta betänkande (se vidare i avsnitt 8.5.2).

Ersättning för medverkan ska enligt 24 § lagen om hemlig dataavläsning betalas av den verkställande myndigheten. De kostnader för medverkan som uppstår för de brottsbekämpande myndigheterna omfattas av de bedömningar som har gjorts för respektive myndighet i avsnitten ovan. Hittills har hemlig dataavläsning inte krävt åtgärd från operatörerna vid verkställighet i någon större utsträckning. De kostnader som kan komma att uppstå för verkställande myndighet med anledning av medverkansskyldigheten framstår därför närmast som försumbara i sammanhanget.

Finansiering

De ökade resursbehov som våra förslag medför sammanfaller till viss del med tidigare ökade resursbehov och ökade anslag med anledning av de lagändringar om hemliga tvångsmedel som trädde i kraft den 1 oktober 2023. De ökade kostnader som genomförandet av våra förslag medför för Polismyndigheten och Sveriges Domstolar, inklusive anslaget Rättsliga biträden m.m., bedöms rymmas inom befintliga anslag. Detsamma gäller de ökade kostnader som kan komma att uppstå för Skatteverket, Finansinspektionen och Kriminalvården. De ytterligare kostnader som våra förslag medför för Säkerhetspolisen, Tullverket och SIN, dvs. kostnader som inte bedöms rymmas inom befintliga ramar, bör huvudsakligen finansieras genom att medel tillförs från andra utgiftsområden. Finansiering bör även ske genom verksamhetsutveckling och prioriteringar samt, i den utsträckning det är möjligt, genom fördelning av kostnadsökningar mellan myndigheterna.

12.5 Övriga konsekvenser

Bedömning: Våra förslag kommer huvudsakligen att beröra samma personer som riskerar att bli föremål för andra hemliga tvångsmedel.

Män kommer att beröras av våra förslag i större utsträckning än kvinnor.

Våra förslag får konsekvenser även för barn.

Förslagen är förenliga med de krav som följer av EU-rätten och Sveriges övriga internationella åtaganden när det gäller mänskliga rättigheter.

Förslagen medför inte i övrigt några konsekvenser som utredningen ska redovisa enligt kommittéförordningen eller kommittédirektiven.

Skälen för våra bedömningar

Vilka personer som berörs

I det ovanstående har vi bedömt att våra förslag kommer att medföra en viss ökning av antalet tillstånd till hemlig dataavläsning samt en högre andel verkställbara beslut. Detta innebär i sin tur att något fler personer än i dag kan komma att bli föremål för hemlig dataavläsning. Relativt sett handlar det om ett begränsat antal personer som kan förväntas beröras av våra förslag. Av de brottsbekämpande myndigheternas årliga redovisningar kan utläsas att hemlig dataavläsning årligen riktas mot upp till 170–310 personer. Siffran kan jämföras med hemlig avlyssning av elektronisk kommunikation som de senaste åren har riktats mot cirka 1 400–1 700 personer/år (se avsnitt 6.3.1). Med ledning av hur vi har bedömt att användningen av hemlig dataavläsning kommer att utvecklas, kan hemlig dataavläsning komma att riktas mot något fler personer än i dag. Det kan konstateras att det rör sig om en förhållandevis liten ökning. Av våra resonemang i avsnitt 7.6 framgår att dessa personer i sin tur huvudsakligen bedöms vara samma personer som riskerar att bli föremål för andra hemliga tvångsmedel. I detta avsnitt har vi också utvecklat i vilken utsträckning som tredje man kan komma att beröras av våra förslag.

Konsekvenser för jämställdheten

Den reglering vi föreslår är könsneutral. Detta utesluter inte att olika grupper kan komma att påverkas olika av bestämmelserna om hemlig dataavläsning. Enligt kriminalstatistiken lagförs fler män än kvinnor för allvarlig brottslighet. Detta innebär att fler män än kvinnor kommer att beröras av våra förslag (jfr t.ex. *Skärpta straff för brott i kriminella nätverk*, prop. 2022/23:53 s. 137).

Konsekvenser för barn

Även barn berörs av hemlig dataavläsning, varför deras rättigheter enligt FN:s konvention om barnets rättigheter (barnkonventionen) måste beaktas särskilt. De rättigheter som barn tillförsäkras enligt barnkonventionen är en del av de mänskliga rättigheter som under lång tid fastställts i olika internationella överenskommelser. Sedan den 1 januari 2020 har barnkonventionen ställning som svensk lag. I samband med inkorporeringen framhölls vikten av att barnets rättigheter uppmärksammas och fångas upp på ett tidigt stadium i lagstiftningsprocessen (se *Inkorporering av FN:s konvention om barnets rättigheter*, prop. 2017/18:186, s. 74 och 95).

Bestämmelserna om hemlig dataavläsning berör barn på sätt att hemlig dataavläsning kan komma att riktas mot barn under 18 år. Barn ingår också i den krets av ovidkommande som kan komma att drabbas av åtgärden (se avsnitt 7.6). Vi har tidigare redogjort för vår bedömning att regelverket för hemlig dataavläsning ger uttryck för en rimlig avvägning mellan behovet av en effektiv brottsbekämpning och den enskildes rätt till skydd för sin personliga integritet. Det finns ingen anledning att göra någon annan bedömning i fråga om barn som kan bli föremål för hemlig dataavläsning. Det ska i sammanhanget framhållas att det vid användning av hemlig dataavläsning mot straffmyndiga barn kan finnas skäl att vara återhållsam. Förutom den proportionalitetsbedömning som ska göras i varje enskilt fall ska även barnets bästa beaktas, se artikel 3 i barnkonventionen.

Hemlig dataavläsning bedöms samtidigt på flera sätt innebära en förstärkt rättstrygghet för barn. Möjligheten att använda hemlig dataavläsning kan antas få stor betydelse vid t.ex. utredningar om sexualbrott mot barn, särskilt i de fall brottsligheten begås på nätet eller annars med hjälp av elektronisk kommunikation (se prop. 2022/23:126

s. 197). Vårt förslag att permanenta lagen om hemlig dataavläsning medför därför förbättrade möjligheter för de brottsbekämpande myndigheterna att upptäcka, förhindra och utreda sådan allvarlig brottslighet. I förlängningen kan förslaget också väntas leda till en ökad lagföring på området.

Konsekvenser för det nationella och internationella skyddet för de grundläggande fri-och rättigheterna

Av våra överväganden i tidigare kapitel framgår att vi bedömer de förslag som vi nu lämnar som väl förenliga med de krav som följer av Sveriges nationella och internationella åtaganden när det gäller de grundläggande fri- och rättigheterna. Detta innefattar de skyldigheter som följer av Sveriges anslutning till Europeiska unionen. Se särskilt avsnitt 5.4.1 och kapitel 8.

Ytterligare konsekvenser enligt kommittéförordningen eller direktiven

Vi bedömer i övrigt att våra förslag inte får några ytterligare konsekvenser av det slag som avses i kommittéförordningen eller kommittédirektiven, exempelvis för företagen eller det allmänna.

13 Författningskommentar

13.1 Förslaget till lag om ändring i lagen (2020:62) om hemlig dataavläsning

1 §

Hemlig dataavläsning innebär att uppgifter, som är avsedda för automatiserad behandling *och som är åtkomliga* i ett avläsningsbart informationssystem, *inhämtas* i hemlighet och med ett tekniskt hjälpmedel.

I lagen avses med

avläsningsbart informationssystem: en elektronisk kommunikationsutrustning eller ett användarkonto till, eller en på motsvarande sätt avgränsad del av, en kommunikationstjänst, lagringstjänst eller liknande tjänst,

kommunikationsavlyssningsuppgifter: uppgifter om innehåll i meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller *en* annan adress,

kommunikationsövervakningsuppgifter: uppgifter om meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller *en* annan adress,

platsuppgifter: uppgifter om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits,

kameraövervakningsuppgifter: uppgifter som framkommer genom optisk personövervakning,

rumsavlyssningsuppgifter: uppgifter som avser tal i enrum, samtal mellan andra eller förhandlingar vid sammanträden eller andra sammankomster som allmänheten inte har tillträde till.

Paragrafen, som behandlas i avsnitt 7.2, innehåller en definition av hemlig dataavläsning och definitioner av andra begrepp i lagen. Tidigare överväganden finns i prop. 2019/20:64 s. 101 ff. och 209 ff.

I första stycket görs en språklig ändring som innebär att definitionen av hemlig dataavläsning förtydligas. I bestämmelsen anges att hemlig dataavläsning innebär att uppgifter, som är avsedda för automatiserad behandling och som är åtkomliga i ett avläsningsbart informationssystem, inhämtas i hemlighet och med ett tekniskt hjälpmedel.

Genom ändringen ersätts uttrycket ”läses av eller tas upp” med ”inhämtas”. Ändringen innebär att legaldefinitionen av hemlig dataavläsning begränsas till själva inhämtningen av uppgifter. Med uttrycket ”inhämtas” avses att på ett teknikneutralt sätt tydliggöra att hemlig dataavläsning innebär både *avläsning* och *överföring* av information till de brottsbekämpande myndigheterna. Med avläsning avses den initiala process som sker i ett avläsningsbart informationssystem med hjälp av ett tekniskt hjälpmedel. Eftersom hemlig dataavläsning kan användas för att inhämta olika typer av uppgifter kan avläsningen innebära en rad olika tillvägagångssätt, t.ex. avlyssning, upptagning eller övervakning. Efter avläsningen överförs uppgifterna från det avläsningsbara informationssystemet till den brottsbekämpande myndigheten. I anslutning till inhämtningen sker viss sortering och filtrering av uppgifterna. Det förekommer också att rådata förädlas i form av t.ex. uppackning, avkodning eller dekryptering för att informationen ska bli läsbar. Även dessa moment, som syftar till att tillgängliggöra uppgifter som överensstämmer med tillståndet för granskning, omfattas av verkställigheten. Bearbetningen av inhämtade uppgifter ingår dock inte i legaldefinitionen av begreppet hemlig dataavläsning. Det framgår i stället av andra bestämmelser i lagen att ett tillstånd till hemlig dataavläsning också innebär att inhämtade uppgifter, under de i lagen angivna förutsättningarna, får bearbetas och granskas. Även de allmänna ändamålen med hemlig dataavläsning – att förebygga, förhindra, upptäcka eller utreda viss allvarlig brottslighet – kommer till uttryck genom andra bestämmelser i lagen. Med uttrycket ”åtkomliga” avses att på ett teknikneutralt sätt tydliggöra att hemlig dataavläsning kan användas för att hämta in alla de uppgifter som under verkställighetstiden går att komma åt i det avläsningsbara informationssystem som tillståndet avser. Uttrycket återknyter till definitionen av uppgiftstypen i 2 § första stycket 6, se kommentaren till den bestämmelsen. Någon ändring i sak är inte avsedd. Ändringen av definitionen innebär alltså endast ett tydliggörande av att hemlig dataavläsning innebär inhämtning av uppgifter i syfte att möjliggöra en efterföljande bearbetning och granskning.

Ändringarna i *andra stycket* är endast språkliga.

Uppgiftstyper som får *hämtas in*

2 §

Tillstånd till hemlig dataavläsning får *avse*
1. kommunikationsavlyssningsuppgifter,
2. kommunikationsövervakningsuppgifter,
3. platsuppgifter,
4. kameraövervakningsuppgifter,
5. rumsavlyssningsuppgifter *eller*
6. uppgifter som *är åtkomliga* i ett avläsningsbart informationssystem men som inte avses i 1–5.

Vid hemlig dataavläsning som gäller kommunikationsavlyssnings- eller kommunikationsövervakningsuppgifter får meddelanden som överförs eller har överförts i ett elektroniskt kommunikationsnät även hindras från att nå fram.

Ett tillstånd enligt första stycket omfattar uppgiftstyperna i första stycket 1–3 och 6, om inget annat särskilt beslutas eller framgår av andra bestämmelser.

Paragrafen, som behandlas i avsnitt 7.3, anger vilka uppgiftstyper som får hämtas in med hemlig dataavläsning och att meddelanden i vissa fall får hindras från att nå fram. Tidigare överväganden finns i prop. 2019/20:64 s. 105 ff. och 212 ff.

I rubriken görs språkliga ändringar. Ändringen till uttrycket ”uppgiftstyper” avser att tydliggöra att en *uppgiftstyp* kan innefatta en mängd olika *uppgifter*, se vidare härom i kommentarerna till 18 § första stycket 3 och 4 samt 23 §. Angående uttrycket ”hämtas in”, se kommentaren till 1 §. Någon ändring i sak är inte avsedd.

I *första stycket* tas uppgiftstyperna i punkterna 6 och 7 bort och ersätts med en *ny punkt 6* som avser uppgifter som är åtkomliga i ett avläsningsbart informationssystem men som inte avses i 1–5. Det innebär att den nya punkten 6 är sekundär i förhållande till punkterna 1–5. Om de uppgifter som ska hämtas in faller under punkterna 1–5 får tillståndet alltså inte avse punkt 6 utan någon annan punkt som täcker in uppgifterna. Rent lagtekniskt innebär ändringen att de tidigare punkterna 6 och 7 slås ihop till en ny punkt 6. I den nya punkten görs inte längre någon skillnad på om uppgifterna är lagrade eller om de utgör realtidsuppgifter. Uttrycket ”är åtkomliga” är avsett att på ett teknikneutralt sätt markera att all information som under verkställighetstiden går att komma åt i det avläsningsbara informationssystemet och som inte går att hänföra till punkt 1–5 är att sortera under punkten 6. Som framgår av 1 § andra stycket kan det

avläsningsbara informationssystemet vara fysiskt, t.ex. en mobiltelefon, eller immateriellt, t.ex. en molntjänst. Såväl fysiska som immateriella informationssystem måste specificeras i tillståndet för att omfattas av detsamma, se 18 § första stycket 2. Det räcker således inte med att endast ange vilken mobiltelefon som tillståndet avser om tillståndet även ska omfatta inhämtning av uppgifter i molntjänster som används från den aktuella mobiltelefonen.

Andra stycket är oförändrat.

Genom *tredje stycket,* som är nytt, införs en förtydligande huvudregel. Bestämmelsen tydliggör att ett typiskt tillstånd till hemlig dataavläsning ofta behöver omfatta såväl uppgiftstyperna i punkt 1–3 som den nya punkten 6 för att motsvara de brottsbekämpande myndigheternas behov av informationsinhämtning. Ett tillstånd till hemlig dataavläsning ska dock differentieras i varje enskilt fall, se 18 § första stycket 3. Huvudregeln utesluter alltså inte att det i ett enskilt fall finns behov av eller skäl att meddela tillstånd avseende endast en av de sex uppgiftstyperna eller avseende en annan kombination av punkter än punkt 1–3 och 6. Uttrycket ”om inget annat särskilt beslutas” syftar på just denna differentiering som alltid ska ske. Uttrycket ”eller framgår av andra bestämmelser” syftar på den begränsning av vilka uppgiftstyper som kan komma i fråga som i vissa fall följer redan av lagtext, se t.ex. 4 a–5 och 8–10 §§. I de fall det inte är möjligt eller ändamålsenligt att vid tillståndsgivningen begränsa vilka *uppgiftstyper* som får inhämtas talar detta för att tillståndet, för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan, bör begränsas genom villkor enligt 18 § första stycket 4. Villkor kan avse såväl inhämtningen av *uppgifter* som granskningen av desamma, se kommentaren till 18 § första stycket 4.

4 a §

Ett tillstånd enligt 4 § får endast avse ett avläsningsbart informationssystem som används, eller som det finns särskild anledning att anta har använts eller kommer att användas, av den misstänkte.

Ett tillstånd enligt 4 § som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter får även avse ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att den misstänkte har kontaktat eller kommer att kontakta.

Ett tillstånd enligt 4 § som gäller kameraövervakningsuppgifter får endast avse en plats där den misstänkte kan antas komma att uppehålla sig. En sådan plats får dock inte vara någons stadigvarande bostad.

Trots tredje stycket får ett tillstånd enligt 4 § som gäller kameraövervakningsuppgifter avse den skäligen misstänkte i stället för en viss plats, om det finns särskilda skäl för det. Den hemliga dataavläsningen får då endast användas på en plats där den misstänkte kan antas komma att uppehålla sig. En sådan plats får dock inte vara någons stadigvarande bostad.

I paragrafens *andra stycke* görs en språklig ändring som är föranledd av ändringen i 18 § tredje stycket, se kommentaren till den bestämmelsen. Någon ändring i sak är inte avsedd. I övrigt är paragrafen oförändrad.

4 b §

Ett tillstånd till hemlig dataavläsning som gäller *uppgiftstyperna i 2 § första stycket 1–4 eller 6* får, om åtgärden är av synnerlig vikt för utredningen, även beviljas för att utreda vem som skäligen kan misstänkas för brottet eller brotten vid en förundersökning om brott som avses i 27 kap. 18 b § andra stycket rättegångsbalken.

Hemlig dataavläsning enligt första stycket får endast avse ett avläsningsbart informationssystem som

1. det finns särskild anledning att anta att gärningsmannen eller någon annan som har medverkat till brottet eller brotten har använt eller kommer att använda, eller,

2. *om tillståndet gäller uppgiftstyperna i 2 § första stycket 1–3 eller 6*, det finns synnerlig anledning att anta att gärningsmannen eller någon annan som har medverkat till brottet eller brotten har kontaktat eller kommer att kontakta.

Ett tillstånd enligt första stycket som gäller kameraövervakningsuppgifter får inte verkställas på en plats som är någons stadigvarande bostad.

Trots tredje stycket får tillståndet verkställas på en sådan plats, om det finns synnerliga skäl att anta att den som åtgärden riktar sig mot uppehåller sig i direkt anslutning till det avläsningsbara informationssystem som tillståndet avser.

Paragrafen, som behandlas i avsnitt 7.4.4, innehåller bestämmelser om användning av hemlig dataavläsning i syfte att utreda vem som skäligen kan misstänkas för brott. Tidigare överväganden finns i prop. 2022/ 23:126 s. 117 ff. och 240 f.

I *första stycket* införs utökade möjligheter att använda hemlig dataavläsning för att utreda vem som skäligen kan misstänkas för brott som avses i 27 kap. 18 b § andra stycket rättegångsbalken. Tillstånd till en sådan åtgärd får beviljas inte bara avseende kommunikationsavlyss-

ningsuppgifter, utan enligt ändringen också avseende uppgiftstyperna i 2 § första stycket 2–4 eller 6. När det gäller uppgiftstyperna i 2 § första stycket 2 och 3 kan ett tillstånd till hemlig dataavläsning för att utreda vem som skäligen kan misstänkas för brott beviljas även med stöd av 5 §, se kommentaren till den paragrafen i prop. 2019/20:64 s. 218 f. Syftet med den hemliga dataavläsningen ska vara att kunna identifiera en misstänkt gärningsman. Om det finns en skäligen misstänkt person kan hemlig dataavläsning användas i syfte att identifiera ytterligare personer som skälig misstanke kan riktas mot. När det gäller tillämpningsområdet och kravet på att åtgärden ska vara av synnerlig vikt för utredningen, se kommentaren till 27 kap. 18 b § rättegångsbalken i prop. 2022/23:126 s. 207 ff. De utökade möjligheterna bör tillämpas med restriktivitet, t.ex. i situationer när graden av integritetsintrång är att bedöma som låg och när åtgärden kan begränsas genom tydliga villkor för tillståndet enligt 18 § första stycket 4. Ett exempel på en situation där graden av integritetsintrång är att bedöma som låg är när åtgärden riktas mot en avgränsad del av Darknet, en anonymiserad och krypterad del av internet. Ett annat exempel är när åtgärden riktas mot en s.k. proxyserver, där den ende användaren är den person som utför det aktuella brottet och som utnyttjar proxyservern i syfte att minimera sina digitala avtryck. Villkoren för åtgärdens användande måste anpassas efter det enskilda fallet. Det bör för rätten tydligt anges hur det aktuella informationssystemet har ringats in och hur det kan undvikas att ovidkommande personer drabbas av åtgärden, t.ex. i ett skriftligt underlag som bifogas ansökan. Detta innebär att det ställs höga krav på ansökan vilket syftar till att försäkra att tillståndet utformas tydligt och med erforderliga begränsande villkor. För exempel på villkor, se kommentaren till 18 § första stycket 4.

I *andra stycket andra punkten* görs ett tillägg som innebär att ett tillstånd enligt första stycket som gäller kameraövervakningsuppgifter endast får avse ett informationssystem som det finns särskild anledning att anta att gärningsmannen eller någon annan som har medverkat till brottet eller brotten har använt eller kommer att använda. Vidare görs i samma punkt, precis som i *första punkten,* en språklig ändring som är föranledd av ändringen i 18 § tredje stycket, se kommentaren till den bestämmelsen. Någon ändring i sak är inte avsedd.

I *tredje stycket*, som är nytt, anges att ett tillstånd enligt första stycket som gäller kameraövervakningsuppgifter inte får verkställas

på en plats som är någons stadigvarande bostad. Ett sådant förbud motsvarar vad som i allmänhet gäller för hemlig dataavläsning avseende kameraövervakningsuppgifter under en förundersökning, jfr 4 a § tredje och fjärde styckena. Kravet ska beaktas vid verkställigheten och inte vid tillståndsprövningen. Det framgår vidare av 6 a § att hemlig dataavläsning som gäller kameraövervakningsuppgifter aldrig får användas på en plats dit tillträdestillstånd enligt 13 § inte får beviljas.

I *fjärde stycket*, som är nytt, görs ett undantag från huvudregeln i tredje stycket. En grundläggande förutsättning för tillämpning av denna undantagsbestämmelse är att andra mindre ingripande metoder och tvångsmedel har uttömts. Syftet med åtgärden – att utreda vem som skäligen kan misstänkas – ska i princip inte vara möjligt att uppnå på något annat sätt än genom inhämtning av kameraövervakningsuppgifter. Detta framgår redan av kravet i första stycket på att åtgärden ska vara av synnerlig vikt för utredningen och av proportionalitetsprincipen som är lagfäst i 3 §. Kravet på att det ska finnas synnerliga skäl att anta att den person som åtgärden riktar sig mot uppehåller sig i direkt anslutning till det avläsningsbara informationssystem som tillståndet avser är högt ställt. Kravet innebär att det på grund av tillförlitliga uppgifter ska vara så gott som säkert att så är fallet, exempelvis om det i verkställighetsögonblicket kan säkerställas att den som åtgärden riktas mot använder informationssystemet i fråga. Kravet ska således beaktas vid verkställigheten och inte vid tillståndsprövningen.

8 §

Hemlig dataavläsning enligt 7 § får avse ett avläsningsbart informationssystem som används, eller som det finns särskild anledning att anta har använts eller kommer att användas, av en person som anges i den bestämmelsen.

Hemlig dataavläsning som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter får även avse ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att en person som anges i 7 § har kontaktat eller kommer att kontakta.

I paragrafens *andra stycke* görs en språklig ändring som är föranledd av ändringen i 18 § tredje stycket, se kommentaren till den bestämmelsen. Någon ändring i sak är inte avsedd. I övrigt är paragrafen oförändrad.

9 §

Ett tillstånd till hemlig dataavläsning får beviljas för att *inhämta* uppgifter i ett avläsningsbart informationssystem som används, eller som det finns särskild anledning att anta har använts eller kommer att användas, av en utlänning som omfattas av

1. ett utvisningsbeslut enligt 2 kap. 1 § lagen (2022:700) om särskild kontroll av vissa utlänningar, eller

2. ett avvisnings- eller utvisningsbeslut enligt 8 kap. eller 8 a kap. utlänningslagen (2005:716) om det finns sådana omständigheter i fråga om utlänningen som avses i 2 kap. 1 § lagen om särskild kontroll av vissa utlänningar.

Ett tillstånd till hemlig dataavläsning som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter får också beviljas för att *hämta in* uppgifter i ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att utlänningen har kontaktat eller kommer att kontakta.

Tillståndet får beviljas endast om Migrationsverket, regeringen eller en domstol har beslutat att 5 kap. 5 och 6 §§ lagen om särskild kontroll av vissa utlänningar samt denna lag ska tillämpas på utlänningen. Det förfarande och de förutsättningar som gäller för ett beslut om att 5 kap. 5 och 6 §§ lagen om särskild kontroll av vissa utlänningar ska tillämpas i fråga om utlänningen gäller också för ett beslut i fråga om hemlig dataavläsning.

Ett tillstånd får beviljas endast om det finns synnerliga skäl och det är av betydelse för att klarlägga om

1. utlänningen tillhör eller verkar för en organisation eller grupp som planlägger eller förbereder brott enligt terroristbrottslagen (2022:666) eller om det finns en risk för att utlänningen kan komma att engagera sig i en sådan organisation eller grupp,

2. det finns risk för att utlänningen själv planlägger eller förbereder brott som avses i 1, eller

3. det finns risk för att utlänningen själv eller tillsammans med andra medverkar i eller på annat sätt främjar ett allvarligt brott som rör Sveriges säkerhet.

Ett tillstånd får inte avse rumsavlyssningsuppgifter.

I paragrafens *första* och *andra stycke* görs språkliga ändringar, se kommentarerna till 1 § respektive 18 § tredje stycket. Några ändringar i sak är inte avsedda. I övrigt är paragrafen oförändrad.

14 §

Frågor om hemlig dataavläsning prövas av rätten på ansökan av åklagaren. En ansökan om hemlig dataavläsning enligt 9 § ska dock göras av Säkerhetspolisen.

Åklagaren, *eller i förekommande fall Säkerhetspolisen,* ska i samband med ansökan föreslå sådana villkor som avses i 18 § första stycket 4, *om sådana villkor inte framstår som obehövliga.*

I paragrafen, som behandlas i avsnitt 8.4.5, anges att rätten prövar ansökan om hemlig dataavläsning och vem som ska göra ansökan. Tidigare överväganden finns i prop. 2019/20:64 s. 147 ff. och 228 f. samt prop. 2022/23:126 s. 153 ff. och 243 f.

Första stycket är oförändrat.

Ändringen i *andra stycket* innebär att åklagaren, eller i förekommande fall Säkerhetspolisen, åläggs att i samband med en ansökan om hemlig dataavläsning också föreslå de villkor som tillståndet enligt 18 § första stycket 4 ska förenas med. Åläggandet gäller vid alla ansökningar om hemlig dataavläsning, utom i de fall där villkor framstår som obehövliga. För exempel på situationer där det kan framstå som obehövligt med villkor, se kommentaren till 18 § första stycket 4. Förslaget på villkor bör tas in i redan i den ansökan eller i det tillhörande underlag som ges in till rätten. Om åklagaren, eller i förekommande fall Säkerhetspolisen, anser det obehövligt att förena ett tillstånd med villkor bör detta och skälen härtill anges i samband med ansökan.

17 §

Om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen eller för möjligheterna att förebygga, förhindra eller upptäcka den brottsliga verksamheten att inhämta rättens *beslut* i en fråga om hemlig dataavläsning, får tillstånd ges av åklagaren i avvaktan på rättens beslut. Ett sådant tillstånd får dock aldrig avse hemlig dataavläsning vid särskild utlänningskontroll enligt 9 §.

Om åklagaren har gett ett tillstånd enligt första stycket, ska åklagaren snarast möjligt skriftligt anmäla beslutet till rätten. I anmälan ska skälen för åtgärden anges. Rätten ska skyndsamt pröva ärendet. Om rätten finner att det inte finns skäl för åtgärden, ska den upphäva beslutet.

Om åklagarens beslut har verkställts innan rätten gjort en prövning som avses i andra stycket, ska rätten pröva om det funnits skäl för åtgärden. Om rätten finner att det saknats sådana skäl, får de uppgifter som *hämtats in*

inte användas i en brottsutredning till nackdel för den som har omfattats av åtgärden, eller för någon annan som uppgifterna avser.

I paragrafens *första* och *tredje stycke* görs språkliga ändringar. Beträffande ändringen i tredje stycket, se kommentaren till 1 §. Några ändringar i sak är inte avsedda. I övrigt är paragrafen oförändrad.

18 §

I ett tillstånd till hemlig dataavläsning ska följande anges:

1. *under* vilken tid *som verkställighet får ske*,
2. vilket avläsningsbart informationssystem tillståndet avser,
3. vilken *uppgiftstyp* enligt 2 § första stycket som får *inhämtas*,
4. *vilka uppgifter som inte får granskas och övriga* villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan, *om det inte framstår som obehövligt,* och
5. vem som är skäligen misstänkt för brottet eller brotten, *om sådan uppgift finns*.

Om tillståndet avser en plats enligt 4 a § tredje stycket, 6 § tredje stycket eller 7 § tredje stycket ska även platsen anges i tillståndet. Om tillståndet är förenat med ett tillträdestillstånd enligt 12 §, ska det anges i beslutet.

Tiden för *verkställighet* får inte bestämmas längre än nödvändigt *och* får inte överstiga en månad från dagen för beslutet.

Paragrafen, som behandlas i avsnitten 8.4.4–8.4.7, reglerar vad ett beslut om tillstånd till hemlig dataavläsning ska innehålla. Tidigare överväganden finns i prop. 2019/20:64 s. 154 ff. och 232 ff. samt prop. 2022/23:126 s. 66 ff., 155 och 245.

I *första stycket* anges vad som ska framgå av ett beslut om hemlig dataavläsning.

Första punkten ändras på sätt att det i ett tillstånd ska anges under vilken tid som verkställighet får ske. Enligt den tidigare lydelsen skulle det anges vilken tid tillståndet avsåg. Ändringen innebär delvis ett förtydligande av vad som redan gäller. Vid bestämmande av tid måste begränsningen i tredje stycket, som motsvarar det hittillsvarande fjärde stycket, beaktas. Av denna begränsning följer att tiden för verkställighet inte får bestämmas längre än vad som är nödvändigt i det enskilda fallet. Om det finns behov av hemlig dataavläsning under en längre period än en månad så krävs ett nytt beslut. Som utgångspunkt finns det inte något hinder mot att verkställighet äger rum flera gånger under verkställighetsperioden. Det sagda gäller under förutsättning

att tillståndet inte har förenats med särskilda villkor angående t.ex. en kortare verkställighetstid. När det gäller inhämtning av uppgifter som är åtkomliga i informationssystemet under verkställighetstiden finns inte någon lagstadgad bortre tidsgräns för hur gamla uppgifter som får inhämtas. Ändringen innebär därmed ett förtydligande som klargör att alla uppgifter som omfattas av tillståndet och som under verkställighetstiden är åtkomliga i informationssystemet får hämtas in, om inte annat framgår av tillståndets villkor enligt fjärde punkten. Genom ändringen tas kravet på att ange ”vilken tid tillståndet avser” bort. Detta innebär i sin tur att inhämtningen inte längre behöver begränsas till information som lagrats under en viss tid, om det inte är möjligt eller ändamålsenligt med en sådan begränsning. I dessa fall är i stället tidsmässiga villkor som avser själva granskningen av inhämtade uppgifter av central betydelse, se kommentaren till fjärde punkten.

I *tredje punkten* görs språkliga ändringar. Uttrycket ”uppgiftstyper” avser tydliggöra skillnaden från fjärde punkten eftersom en *uppgiftstyp* kan innefatta en mängd olika *uppgifter*, se vidare härom i kommentarerna till fjärde punkten och 23 §. Angående uttrycket ”hämtas in”, se kommentaren till 1 §. Några ändringar i sak är inte avsedda.

Fjärde punkten ändras på sätt att det i ett tillstånd till hemlig dataavläsning ska anges vilka *uppgifter* som inte får granskas och övriga villkor för att tillgodose intresset av att enskildas integritet inte kränks i onödan. Ändringen återknyter till bestämmelserna i 1 och 2 §§ och innebär att kravet på villkor får en annan praktisk betydelse än tidigare. I 1 § tydliggörs att själva inhämtningen av uppgifter är att skilja från den efterföljande granskningen av desamma. Av 2 § tredje stycket framgår vidare att ett typiskt tillstånd till hemlig dataavläsning omfattar inhämtning av alla uppgiftstyper i 2 § första stycket förutom kameraövervaknings- och rumsavlyssningsuppgifter. Som utgångspunkt kan såväl lagrade uppgifter som realtidsuppgifter hämtas in med stöd av ett sådant tillstånd. När det gäller lagrade uppgifter enligt 2 § första stycket 1–3 eller 6 är det ofta svårt att ställa upp villkor som begränsar själva inhämtningen av uppgifter. Däremot är sådana filtreringar möjliga att göra i en inledande bearbetning av uppgifterna, dvs. i anslutning till själva inhämtningen. Denna inledande bearbetning syftar endast till att tillgängliggöra uppgifter, inom ramen för tillståndet, för granskning. För bestämmelsens tillämpning saknas därför betydelse om den inledande bearbetningen är maskinell eller manuell. Med villkor som avser ”vilka uppgifter som inte får granskas” avses

alltså villkor som avgränsar vilka inhämtade uppgifter som får gås igenom av behöriga personer i en granskningsfas, efter verkställighet (dvs. efter inhämtning samt förädling, sortering och filtrering av inhämtade uppgifter). Det förhållandet att det i villkoren ska anges vilka uppgifter som *inte* får granskas hindrar inte att villkoren formuleras som att endast vissa angivna uppgifter *får* granskas. Avgörande är att villkoren ur ett integritets- och rättssäkerhetsperspektiv är tydligt utformade. Villkoren bör om möjligt och ändamålsenligt ta sikte på tidsmässiga avgränsningar, men kan också avse andra begränsningar. I 23 § första stycket regleras hur uppgifter som enligt villkoren för tillståndet inte får granskas ska hanteras. Exempel på villkor som avser vilka uppgifter som får/inte får granskas:

> Efter att uppgifterna hämtats in får endast uppgifter [från ett visst datum/ som avser kommunikation med NN/vissa uppgifter] granskas.
>
> Vid analys av de inhämtade uppgifterna får inte uppgifter [före ett visst datum] granskas.
>
> Efter att uppgifterna hämtats in får inte uppgifter, såsom kommunikation från mejlkonton eller andra användarkonton, tillhörande [familjemedlemmar till NN] granskas.

Med ”övriga villkor” för tillståndet avses att tydliggöra att villkor för tillståndet kan ta sikte även på andra omständigheter och således inte bara själva granskningen. I de fall som det är möjligt och ändamålsenligt att uppställa villkor som avser själva inhämtningen bör denna begränsas genom villkor för att åtgärden ska framstå som proportionerlig. I de fall som det är möjligt och ändamålsenligt att göra en åtskillnad mellan lagrade uppgifter och realtidsuppgifter redan i inhämtningsfasen bör detta göras. Om åtgärden exempelvis endast avser ett visst samtal eller möte som man misstänker kommer att äga rum föreligger endast behov av att hämta in realtidsuppgifter. Det saknas då anledning att låta tillståndet omfatta inhämtning av uppgifter som har tillkommit före verkställighetsperioden. Villkoret för tillståndet skulle i ett sådant fall kunna utformas på exempelvis följande sätt:

> Inhämtning får inte omfatta kommunikationsavlyssnings- eller platsuppgifter som har tillkommit före verkställighetsperioden.

Vid hemlig dataavläsning avseende kameraövervaknings- eller rumsavlyssningsuppgifter bör villkor som begränsar redan själva inhämtningen av uppgifter vara tämligen enkla att ställa upp, exempelvis:

> Verkställighet av kameraövervaknings- eller rumsavlyssningsuppgifter får endast ske när det genom spaning eller på annat sätt bekräftats att NN möter upp XX och i nära anslutning till mötet.
>
> Verkställighet av kameraövervaknings- eller rumsavlyssningsuppgifter får inte ske när NN befinner sig på [viss plats etc.]. De uppgifter som behövs för att bedöma om NN befinner sig på [platsen] får dock tas upp.
>
> Verkställighet av kameraövervakning- eller rumsavlyssningsuppgifter får inte ske under [viss tid/på viss plats etc.].

Villkor ska syfta till att gagna skyddet för den personliga integriteten. Vid exempelvis hemlig dataavläsning enligt 4 b eller 5 §§ för att identifiera en skäligen misstänkt kan det finnas särskilda skäl att förena tillståndet med villkor för att minimera riskerna för att tredje man utsätts för hemlig dataavläsning. Det kan t.ex. vid hemlig dataavläsning enligt 4 b § avseende kameraövervakningsuppgifter många gånger vara nödvändigt med villkor om olika åtgärder i samband med verkställighet. Exempelvis kan det ställas villkor på spaning för att kunna säkerställa att integritetsintrånget för den enskilde och risken för att utomstående drabbas minimeras. Det införs i samma punkt också en ventil för tillfällen då det är obehövligt att bestämma villkor. Såväl villkor om vilka uppgifter som inte får granskas som övriga villkor för tillståndet kan i ett enskilt fall framstå som obehövliga för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan. I ett sådant fall krävs inte att tillståndet förenas med några villkor. Typexemplet på situationer där det framstår som obehövligt med villkor är när man på förhand känner till att det inte finns något legalt användningsområde av informationssystemet i fråga. Det kan t.ex. handla om hemlig dataavläsning av vissa chattkonton som man känner till används för kommunikation mellan kriminella eller s.k. brottstelefoner (”burner-telefoner”) som har använts endast under en begränsad tidsperiod. Det kan också förekomma situationer där villkor om vilka uppgifter som inte får granskas framstår som obehövliga, t.ex. om det genom övriga villkor är möjligt att göra en snäv begränsning av vilka uppgifter som får inhämtas. Situationen kan också vara sådan att övriga villkor inte behöver anges eftersom en nödvändig begränsning redan har gjorts genom villkor om vilka uppgif-

ter som inte får granskas. Möjligheten att helt eller delvis låta bli att förena ett tillstånd med villkor bör under alla omständigheter användas med viss restriktivitet. Om det finns anledning att tro att villkor kan vara av betydelse bör tillståndet förenas med villkor. En bedömning måste alltid göras i det enskilda fallet.

I *femte punkten* införs ett krav på att det i ett tillstånd till hemlig dataavläsning alltid ska anges vem som är skäligen misstänkt, förutsatt att sådan uppgift finns. Hittillsvarande tredje stycket utgår som en följd av ändringen.

Tredje stycket, som motsvarar det hittillsvarande fjärde stycket, ändras på det sättet att tiden för verkställighet inte får bestämmas längre än nödvändigt. Verkställighetstiden får inte överstiga en månad från dagen för beslutet. Ändringen innebär ett förtydligande av att ett tillstånd till hemlig dataavläsning ska verkställas inom en viss tid som inte får överstiga en månad, medan det inte alltid i beslutet behöver anges hur gamla uppgifter som får hämtas in. Ändringen ska inte förstås som att fler uppgifter än nödvändigt får inhämtas och granskas. Det är fortfarande grundläggande principer, såsom ändamåls- och proportionalitetsprinciperna, som styr hur ett tillstånd till hemlig dataavläsning ska utformas. Ändringen innebär därmed att villkor som anger under vilken tid som inhämtningen får verkställas eller vilka inhämtade uppgifter (avgränsat till en viss tidsperiod) som inte får granskas, kommer att bli mer framträdande. Ett tillstånd till hemlig dataavläsning bör i många fall kunna avgränsas i tiden genom villkor beträffande vilka uppgifter som får inhämtas eller granskas för att åtgärden ska kunna anses proportionerlig. För exempel på tidsmässiga villkor för tillståndet, se kommentaren till första stycket fjärde punkten. Ändringen i tredje stycket föranleder en justering av de bestämmelser i lagen som ställer krav på viss koppling mellan den enskilde och ett informationssystem, närmare bestämt 4 a § andra stycket, 4 b § andra stycket, 8 § andra stycket och 9 § andra stycket. Någon ändring i sak är inte avsedd. Kravet på koppling mellan den enskilde och ett informationssystem ska alltså fortsatt gälla.

23 §

Vid verkställighet av hemlig dataavläsning ska teknik *och tillvägagångssätt* anpassas efter *tillståndet*. Om *någon annan uppgiftstyp än vad som anges i tillståndet har hämtats in* ska upptagningar och uppteckningar av dessa upp-

gifter omedelbart förstöras och Säkerhets- och integritetsskyddsnämnden underrättas. *Upptagningar och uppteckningar av uppgifter som inte får inhämtas eller granskas enligt villkor meddelade med stöd av 18 § första stycket 4 ska förstöras i de delar de innehåller sådana uppgifter så snart det står klart att sådana uppgifter har inhämtats eller granskats.*

Uppgifter som anges i första stycket får inte användas i en brottsutredning till nackdel för den som har omfattats av åtgärden eller för någon annan som uppgifterna avser.

I paragrafen, som behandlas i avsnitt 8.5.6, finns bestämmelser om verkställighet av hemlig dataavläsning. Tidigare överväganden finns i prop. 2019/20:64 s. 162 f. och 236 f.

Ändringarna i *första stycket* innebär ett förtydligande av att såväl teknik som tillvägagångssätt vid verkställighet ska anpassas efter tillståndet i det enskilda fallet. Med tillvägagångssätt avses bl.a. de särskilda instruktioner eller riktlinjer om arbetssätt vid verkställighet som måste följas för att kraven på ett tillstånd till hemlig dataavläsning ska kunna uppfyllas. Det är verkställande myndighet som ansvarar för att upprätta instruktioner och riktlinjer till den särskilt utsedda personal som ska verkställa den hemliga dataavläsningen. Genom ändringen tas det tidigare förbudet mot att tekniken inte får göra det möjligt att läsa av eller ta upp någon annan uppgiftstyp än vad som anges i tillståndet bort. Ändringen förtydligar hur verkställighet av hemlig dataavläsning går till i praktiken och återknyter till bestämmelserna i 1, 2 och 18 §§. Någon eftergift av de rättssäkerhetsgarantier som omgärdar verkställighet av hemlig dataavläsning är inte avsedd. Redan av kravet på att teknik och tillvägagångssätt ska anpassas efter tillståndet följer att verkställighet av hemlig dataavläsning ska ske inom de ramar som uppställts för det enskilda tillståndet. Vidare införs i tredje meningen ett förtydligande tillägg om att inte bara inhämtade *uppgiftstyper* utan också inhämtade *uppgifter* kan utgöra otillåten tilläggsinformation. Om upptagningar och uppteckningar av uppgifter som inte får inhämtas eller granskas enligt villkor meddelade med stöd av 18 § första stycket 4 ändå har inhämtats eller granskats, ska dessa förstöras i de delar de innehåller sådana uppgifter så snart det står klart att sådana uppgifter har inhämtats eller granskats. Tillägget innebär att uppgifter som har hämtats in i strid med villkor för inhämtningen utgör otillåtna uppgifter som ska förstöras. Detsamma gäller för uppgifter som enligt villkoren för tillståndet får inhämtas men inte granskas. De otillåtna uppgifterna ska förstöras ”så snart det står klart att sådana uppgifter har inhämtats eller grans-

kats”. Detta innebär i praktiken ett krav på förstöring snart sådana uppgifter *påträffas*, dvs. i regel direkt efter att de har sorterats och filtrerats bort i en initial bearbetningsfas. Med hänsyn till att alla inhämtade uppgifter inte är möjliga att gå igenom i detalj, förekommer att vissa otillåtna uppgifter påträffas först vid själva granskningen. Förstöring av de otillåtna uppgifterna kan då ske först i samband med granskningen. Med hänsyn till mängden information som kan hämtas in med stöd av hemlig dataavläsning kan det också förekomma att de otillåtna uppgifterna aldrig gås igenom i detalj och därför heller aldrig identifieras. I dessa fall kommer de otillåtna uppgifterna att förstöras i enlighet med huvudregeln om bevarande och förstörande som framgår av 28–31 §§, dvs. om uppgifterna inte identifieras som otillåtna innan dess. Till skillnad från vad som gäller för inhämtning av otillåtna uppgiftstyper ska Säkerhets- och integritetsskyddsnämnden inte underrättas särskilt vid inhämtning av otillåtna uppgifter. Den allmänna underrättelseskyldighet som följer av 21 § har ansetts tillräcklig.

Andra stycket är oförändrat.

Förbud att *hämta in* vissa uppgifter

27 §

Hemlig dataavläsning enligt 2 § första stycket 6 får inte avse uppgifter som enligt 27 kap. 2 § rättegångsbalken hindrar beslag.

Hemlig dataavläsning som gäller kommunikationsavlyssnings- eller rumsavlyssningsuppgifter får inte avse uppgifter i telefonsamtal, samtal eller andra meddelanden eller tal där någon som yttrar sig, på grund av bestämmelserna i 36 kap. 5 § andra–sjätte styckena rättegångsbalken, inte skulle ha kunnat höras som vittne om det som har sagts eller på annat sätt kommit fram.

Om det under *eller efter* verkställigheten kommer fram uppgifter som omfattas av första eller andra stycket ska *granskningen av dessa uppgifter* omedelbart avbrytas. Upptagningar och uppteckningar *ska* omedelbart förstöras i de delar som de omfattas av förbudet.

I rubriken till paragrafen görs en språklig ändring, se kommentaren till 1 §. I paragrafen, som behandlas i avsnitt 8.5.6, regleras förbud mot att i vissa fall hämta in vissa uppgifter. Tidigare överväganden finns i prop. 2019/20:64 s. 139 ff. och 240 f. samt prop. 2022/23:126 s. 245 f.

I *första stycket* görs en ändring i hänvisningen till 2 § första stycket som en följd av att punkterna 6 och 7 i nämnda bestämmelse tas bort och ersätts med en ny punkt 6.

I *tredje stycket* införs ett förtydligande tillägg som innebär att om det under eller efter verkställigheten kommer fram uppgifter som omfattas av förbudsbestämmelsen ska granskningen av dessa uppgifter omedelbart avbrytas. Upptagningar och uppteckningar ska omedelbart förstöras i de delar som de omfattas av förbudet. Ändringen innebär endast ett förtydligande av bestämmelsen och vad som redan gäller. Någon ändring i sak är inte avsedd.

I övrigt är paragrafen oförändrad.

28 §

När hemlig dataavläsning används eller har använts under en förundersökning ska det som gäller för hemlig avlyssning av elektronisk kommunikation enligt 27 kap. 23 a och 24 §§ rättegångsbalken tillämpas för åtgärden. Det som gäller för hemlig rumsavlyssning ska dock tillämpas för hemlig dataavläsning som gäller rumsavlyssningsuppgifter.

För underrättelse till en enskild vid hemlig dataavläsning under förundersökning gäller 27 kap. 31–33 §§ rättegångsbalken. Det som anges där om

– hemlig kameraövervakning ska tillämpas för hemlig dataavläsning som gäller kameraövervakningsuppgifter

– hemlig rumsavlyssning ska tillämpas för hemlig dataavläsning som gäller rumsavlyssningsuppgifter

– hemlig avlyssning av elektronisk kommunikation ska tillämpas för hemlig dataavläsning i övrigt

– telefonnummer, annan adress eller en viss elektronisk kommunikationsutrustning ska avse avläsningsbart informationssystem.

I paragrafen, som behandlas i avsnitt 8.5.3 och 8.5.4, anges vad som gäller bl.a. beträffande hur överskottsinformation får användas vid hemlig dataavläsning under en förundersökning. Tidigare överväganden finns i prop. 2019/20:64 s. 167 ff. och 241 f. samt prop. 2022/23:126 s. 171 ff. och 246.

Genom ändringen i *första stycket* tas hänvisningen till rättegångsbalkens bestämmelser i dess lydelser före den 1 oktober 2023 bort. Ändringen innebär att användning av överskottsinformation samt bevarande och förstöring av uppteckningar och upptagningar från hemlig dataavläsning under förundersökning regleras på samma sätt som för hemliga tvångsmedel enligt rättegångsbalken. Se vidare kommentarerna till 27 kap. 23 a och 24 §§ rättegångsbalken i prop. 2022/23:126 s. 221 f.

Andra stycket är oförändrat.

29 §

När hemlig dataavläsning används eller har använts i fall som anges i 7 § ska 12 och 13 §§ lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott tillämpas.

För underrättelse till en enskild vid hemlig dataavläsning i fall som anges i 7 § gäller 16–18 §§ lagen om åtgärder för att förhindra vissa särskilt allvarliga brott. Det som anges där om

– hemlig kameraövervakning ska tillämpas för hemlig dataavläsning som gäller kameraövervakningsuppgifter

– hemlig avlyssning av elektronisk kommunikation ska tillämpas för hemlig dataavläsning i övrigt

– telefonnummer, annan adress eller en viss elektronisk kommunikationsutrustning ska avse avläsningsbart informationssystem.

I paragrafen, som behandlas i avsnitt 8.5.3, anges vad som ska gälla bl.a. beträffande hur överskottsinformation får användas vid hemlig dataavläsning i preventivlagsfallen. Tidigare överväganden finns i prop. 2019/20:64 s. 167 ff. och 242 samt prop. 2022/23:126 s. 171 ff. och 246 f.

Genom ändringen i *första stycket* tas att hänvisningen till preventivlagens bestämmelser i dess lydelser före den 1 oktober 2023 bort. Ändringen innebär att användning av överskottsinformation samt bevarande och förstöring av uppteckningar och upptagningar från hemlig dataavläsning i preventivlagsfallen regleras på samma sätt som för hemliga tvångsmedel enligt preventivlagen. Se vidare kommentaren till 12 och 13 §§ lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen) i prop. 2022/23:126 s. 232 f.

Andra stycket är oförändrat.

31 §

När hemlig dataavläsning används eller har använts i fall som anges i 10 § ska 6 och 7 §§ lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet tillämpas. Det som anges där om inhämtning av uppgifter ska tillämpas för hemlig dataavläsning.

I paragrafen, som behandlas i avsnitt 8.5.3 och 8.5.4, anges vad som ska gälla för bl.a. överskottsinformation när hemlig dataavläsning används i inhämtningslagsfallen. Tidigare överväganden finns i prop. 2019/20:64 s. 167 ff. och 243.

I paragrafen kvarstår den nuvarande hänvisningen till 6 § inhämtningslagen, vilket innebär att 6 § inhämtningslagen i den lydelse som i SOU 2023:60 föreslås träda i kraft den 1 januari 2025 blir gällande även för hemlig dataavläsning i inhämtningslagsfallen. Vidare ändras den nuvarande hänvisningen till nuvarande 7 § inhämtningslagen till 8 § inhämtningslagen i den lydelse som i SOU 2023:60 föreslås träda i kraft den 1 januari 2025. Ändringen innebär att de nya regler om användning av överskottsinformation samt granskning, bevarande och förstöring som föreslås gälla enligt inhämtningslagen blir gällande även för hemlig dataavläsning i inhämtningsfallen. Det hittillsvarande andra stycket utgår som en följd av ändringen.

Dokumentation

34 §

Beslut och åtgärder som rör hemlig dataavläsning ska dokumenteras.

Genom paragrafen, som i likhet med rubriken är ny, införs en dokumentationsskyldighet. Övervägandena finns i avsnitt 8.5.5. Bestämmelsen har utformats med bestämmelsen i 27 kap. 35 § rättegångsbalken som förebild.

Av paragrafen framgår att det finns en skyldighet att dokumentera beslut och åtgärder som rör hemlig dataavläsning. Uppgifterna ska dokumenteras på ett sådant sätt att det är möjligt att på ett överskådligt sätt följa beslut och andra åtgärder avseende tvångsmedelsanvändningen. Exempel på uppgifter som bör dokumenteras är uppgifter om tillståndet, såsom när det beviljats och om det har ändrats eller upphävts. Även datum och tidpunkt för verkställigheten samt vilken adress, kommunikationsutrustning eller plats som verkställigheten avsett eller skett på bör dokumenteras. Om det funnits tillträdestillstånd eller samtycke från innehavaren av en plats som omfattats av verkställigheten bör det också dokumenteras. Dokumentationsskyldigheten omfattar även frågor om förstöring av upptagningar och uppteckningar, liksom om förbudsbestämmelserna i 23 eller 27 §§ har aktualiserats. Även en uppgift som har betydelse för förstöringstidpunkten bör dokumenteras, t.ex. en uppgift om när förundersökningen avslutades. Därutöver bör åtgärder som gäller användning av överskottsinformation och en uppgift om en underrättelse till en en-

skild dokumenteras, detta gäller särskilt om underrättelsen lämnats muntligen, exempelvis vid ett förhör (jfr prop. 2022/23:126 s. 225).

Ikraftträdande- och övergångsbestämmelser

1. Denna lag träder i kraft den 1 mars 2025.
2. Äldre föreskrifter gäller fortfarande för tillstånd som har beviljats före ikraftträdandet.
3. För uppgifter från hemlig dataavläsning som har verkställts före ikraftträdandet gäller 28, 29 och 31 §§ i den äldre lydelsen.

Punkterna behandlas i kapitel 11. Enligt *första punkten* träder lagen i kraft den 1 mars 2025. Det innebär att lagen från och med detta datum fortsätter gälla utan begränsning till viss tid. Av *andra punkten* framgår den processrättsliga principen om att nya regler ska tillämpas på varje processuell företeelse som inträffar efter det att regleringen har trätt i kraft. Övergångsbestämmelsen träffar sådana tillstånd till hemlig dataavläsning som har beslutats före ikraftträdandet, men som ännu inte löpt ut. Bestämmelsen kompletteras av *tredje punkten*. Där anges att 28, 29 och 31 §§ gäller i den äldre lydelsen för uppgifter från hemlig dataavläsning som har verkställts före ikraftträdandet. Det innebär att det inte är tillåtet att använda överskottsinformation i större utsträckning än vad som var tillåtet vid den tidpunkt då informationen samlades in.

Kommittédirektiv 2022:82

Utvärdering av hemlig dataavläsning

Beslut vid regeringssammanträde den 22 juni 2022

Sammanfattning

En särskild utredare ska utvärdera lagen (2020:62) om hemlig dataavläsning inför ett ställningstagande till om den bör permanentas och om den i så fall bör ändras i något avseende. Genom lagen, som trädde i kraft den 1 april 2020, infördes ett nytt hemligt tvångsmedel som de brottsbekämpande myndigheterna kan använda vid misstankar om allvarlig brottslighet. Lagen är tidsbegränsad till utgången av mars 2025.

Utredaren ska bland annat

- analysera nyttan och behovet av hemlig dataavläsning,
- ta ställning till om lagstiftningen bör permanentas och föreslå de åtgärder som behövs för ett permanentande,
- analysera om lagstiftningen har fått en ändamålsenlig och proportionerlig utformning eller om det behövs förändringar i regelverket, och
- lämna förslag på de författningsändringar och andra åtgärder som bedöms nödvändiga.

Uppdraget ska redovisas senast den 1 december 2023.

Hemlig dataavläsning – ett efterfrågat verktyg i kampen mot allvarlig brottslighet

Den 1 april 2020 fick de brottsbekämpande myndigheterna ett nytt verktyg, hemlig dataavläsning. Verktyget ger utökade möjligheter att komma åt information som tidigare inte har varit tillgänglig, till exempel på grund av kryptering. I praktiken handlar hemlig dataavläsning om att de brottsbekämpande myndigheterna med hjälp av tekniska hjälpmedel i hemlighet får samla in uppgifter från en dator, en mobiltelefon, ett användarkonto på internet eller något annat informationssystem. Tvångsmedlet får – under vissa förutsättningar – användas under en förundersökning, i underrättelseverksamhet och vid särskild utlänningskontroll, liksom i det internationella straffrättsliga samarbetet.

Vid införandet av hemlig dataavläsning konstaterades att det finns ett påtagligt behov av bättre metoder för att i hemlighet komma åt uppgifter som redan får hämtas in med befintliga tvångsmedel, men också för att kunna komma åt uppgifter som inte är möjliga att tillgå med befintliga verktyg. Det anmärktes att teknikutvecklingen, med bland annat ökad användning av kryptering och automatiska funktioner för radering av data, gjort det väsentligt svårare för de brottsbekämpande myndigheterna att komma åt elektronisk information. Förväntningarna var att hemlig dataavläsning skulle leda till betydligt bättre tillgång till information än befintliga verktyg. (Hemlig dataavläsning, prop. 2019/20:64 s. 69–83.)

Hemlig dataavläsning får endast användas vid misstankar om allvarlig brottslighet. Som huvudregel krävs att det är fråga om ett brott som har ett minimistraff om fängelse i två år. Som exempel på brott som uppfyller dessa krav kan nämnas grovt narkotikabrott, grovt vapenbrott, våldtäkt och mord. Tvångsmedlet får som huvudregel användas mot en utrustning eller ett användarkonto som kan knytas till en person med koppling till de misstankar som avses.

Regleringen av hemliga tvångsmedel har utformats efter en avvägning mellan å ena sidan samhällets behov av en effektiv brottsbekämpning till skydd för medborgarna och å andra sidan den enskildes rätt till privatliv, skydd för sin personliga integritet och rättssäkerhet i förhållande till staten. Liksom andra hemliga tvångsmedel innebär hemlig dataavläsning risker för enskildas personliga integritet och regelverket innehåller därför flera rättssäkerhetsgarantier. Förhandsprövning av

domstol är en sådan. Huvudregeln är att domstol prövar frågor om hemliga tvångsmedel innan de får användas och domstolen har dessutom möjlighet att ange närmare villkor för tvångsmedelsanvändningen i syfte att säkerställa att enskildas personliga integritet inte kränks i onödan.

Förutom den föregående prövningen av domstol finns olika former av tillsyn av både tvångsmedelsanvändningen och myndigheternas övriga verksamhet som utförs av Säkerhets- och integritetsskyddsnämnden, Justitiekanslern, Riksdagens ombudsmän och Integritetsskyddsmyndigheten. En annan viktig grundsten är systemet med offentliga ombud, vilka har till uppgift att bevaka enskildas integritetsintressen. I likhet med vad som gäller för övriga hemliga tvångsmedel redovisas myndigheternas användning av hemlig dataavläsning årligen till riksdagen. Den parlamentariska kontrollen fyller en viktig funktion och bidrar till allmänhetens insyn i myndigheternas tvångsmedelsanvändning.

Reglerna om hemlig dataavläsning är införda i en särskild lag, lagen (2020:62) om hemlig dataavläsning. Eftersom det rör sig om en ny utredningsmetod, som förvisso förväntades vara effektiv men som också ansågs innebära vissa risker för den personliga integriteten, begränsades lagen till att gälla under fem år. En senare utvärdering av den tidsbegränsade lagen ansågs minimera risken för att lagen görs permanent utan ett fullgott underlag (prop. 2019/20:64 s. 99–101).

Uppdraget att utreda frågan om permanentande av hemlig dataavläsning

Brottsligheten har utvecklats och blivit mer samhällshotande. Även kriminellas handlingssätt och hur de kommunicerar är i förändring. Uppgifter om elektronisk kommunikation är många gånger helt avgörande för en framgångsrik brottsbekämpning. Samtidigt innebär den tekniska utvecklingen, liksom brotts- och samhällsutvecklingen i övrigt, att de brottsbekämpande myndigheterna inte längre kan ta del av många av de uppgifter som man tidigare fick del av genom användande av straffprocessuella tvångsmedel.

Sedan möjligheten till hemlig dataavläsning infördes har betydelsen av effektiv tillgång till elektronisk bevisning blivit än tydligare. Det visar inte minst framgångarna tack vare materialet från de krypterade kommunikationstjänsterna Encrochat, Sky ECC och Anom.

Samtidigt innebär den fortsatta teknik- och kommunikationsutvecklingen att det praktiska användningsområdet för hemlig avlyssning och hemlig övervakning av elektronisk kommunikation begränsas. Exempelvis kan införandet av den femte generationens mobilnät (5G) medföra tillämpning av krypterings- och autentiseringsprocesser som syftar till att höja säkerheten men samtidigt riskerar att väsentligt försvåra möjligheterna att verkställa hemliga tvångsmedel. Också förändrade tekniska förfaranden vid roaming riskerar att göra att enbart en mycket begränsad mängd information kan avläsas av operatören i det land som simkortet, och därmed användaren, befinner sig i, med följd att information som härrör från utländska simkort som används i Sverige blir otillgänglig för de brottsbekämpande myndigheterna. Inte bara kommunikationen i sig är föremål för kryptering, utan det sker också en utveckling av möjligheterna att kryptera innehållet i kommunikationsutrustning och lagringsmedier.

De brottsbekämpande myndigheterna har nu haft möjlighet att använda hemlig dataavläsning i drygt två år. Åklagarmyndigheten har, tillsammans med Ekobrottsmyndigheten, Polismyndigheten, Tullverket och Säkerhetspolisen, redovisat användningen av tvångsmedlet under 2020 och 2021. Av redovisningen kan slutsatsen dras att hemlig dataavläsning har kommit till användning i väsentligt större omfattning än vad som förutsetts. Åklagarmyndigheten har för 2020 redovisat att hemlig dataavläsning användes i 60 ärenden från och med 1 april då lagen trädde i kraft, vilket över ett helt år skulle motsvara 80 ärenden. För 2021 var motsvarande siffra 145. Vid lagens införande förväntades antalet verkställigheter, ej inräknat Säkerhetspolisens verksamhet, bli åtminstone 50 per år (Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet, SOU 2017:89 s. 283 f.). De brottsbekämpande myndigheternas erfarenheter av hemlig dataavläsning hittills har varit mycket goda. Polisen har även gett uttryck för att de skulle vilja använda verktyget i större omfattning.

Säkerhets- och integritetsskyddsnämnden granskar de brottsbekämpande myndigheternas användning av bland annat hemlig dataavläsning. I december 2021 lämnade nämnden sin första granskningsrapport om hemlig dataavläsning. Nämnden konstaterade att de grundläggande förutsättningarna för tvångsmedlet genomgående var uppfyllda i de granskade ärendena, liksom att det överlag var god ordning i den granskade tvångsmedelshanteringen. Nämnden anmärkte att det fanns ett par frågor som det fanns anledning att återkomma till,

såsom att tillstånden till hemlig dataavläsning i vissa fall innefattat långa tidsperioder och att det fanns tillstånd som inte förenats med villkor enligt 18 § 4 lagen om hemlig dataavläsning. Vidare ansåg nämnden att det inte är klart huruvida 2 § 7 lagen om hemlig dataavläsning medger inhämtning enbart av realtidsuppgifter eller också historiska uppgifter.

Mot denna bakgrund, och med hänsyn till lagens begränsade giltighetstid, bör en utredare nu utvärdera lagen om hemlig dataavläsning inför ett ställningstagande till om verktyget bör göras permanent och om det i så fall bör förändras i något avseende. Utvärderingen bör innefatta en noga avvägning av de olika intressen som berörs. Det är angeläget att de brottsbekämpande myndigheterna både nationellt och i det internationella samarbetet har tillgång till ändamålsenliga och verkningsfulla verktyg för att effektivt kunna utreda, förebygga och förhindra allvarlig brottslighet. Samtidigt innebär de brottsbekämpande myndigheternas användning av hemliga tvångsmedel ett ingrepp i den berördes personliga integritet i det enskilda fallet. Det är viktigt att förslag inom området kringgärdas av starka rättssäkerhetsgarantier och innehåller tydliga och strikta ramar som tillämparen har att hålla sig inom.

Utredaren ska därför

- analysera nyttan och behovet av hemlig dataavläsning,
- ta ställning till om bestämmelserna i lagen om hemlig dataavläsning bör göras permanenta,
- oavsett vilket ställningstagande som görs, analysera vilka åtgärder som behövs för ett permanentande och lämna förslag på dessa,
- analysera om lagstiftningen har fått en ändamålsenlig och proportionerlig utformning samt om kontrollmekanismerna och övriga rättssäkerhetsgarantier är tillräckliga,
- ta ställning till om det bör göras förändringar i regelverket i syfte att uppnå en mer effektiv brottsbekämpning samtidigt som respekten för grundläggande fri- och rättigheter, såsom rätten till respekt för privatlivet, liksom kraven på rättssäkerhet, säkerställs, och
- lämna förslag på nödvändiga författningsändringar och andra åtgärder.

Utredaren ska bedöma behovet av följdändringar och säkerställa att en välfungerande systematik i regelverket kring såväl hemliga som öppna tvångsmedel upprätthålls. Utredaren har även möjlighet att överväga andra frågor som har samband med de frågeställningar som ska utredas. I och med att lagen gäller till utgången av mars 2025 behöver eventuella åtgärder för ett permanentande kunna genomföras dessförinnan.

Konsekvensbeskrivningar

Utredaren ska bedöma och redogöra för förslagens ekonomiska konsekvenser och konsekvenser i övrigt för enskilda, företag och det allmänna samt redogöra för förslagens samhällsekonomiska effekter. Utredaren ska särskilt beskriva vilka konsekvenser de förslag som lämnas har för det nationella och internationella skyddet för grundläggande fri- och rättigheter, såsom den personliga integriteten. De offentligfinansiella effekterna av förslagen ska beräknas, och om förslagen kan förväntas leda till offentligfinansiella kostnader ska utredaren föreslå hur dessa ska finansieras.

Kontakter och redovisning av uppdraget

Utredaren ska föra dialog med och inhämta upplysningar från Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Säkerhets- och integritetsskyddsnämnden, Integritetsskyddsmyndigheten, Post- och telestyrelsen och Sveriges advokatsamfund, men även med andra myndigheter och berörda aktörer, såsom civilsamhället, i den utsträckning som utredaren finner det lämpligt.

Utredaren ska också hålla sig informerad om och beakta relevant arbete som pågår inom Regeringskansliet och inom utredningsväsendet. Utredaren ska beakta utvecklingen vid såväl EU:s lagstiftande institutioner som EU-domstolen, Europadomstolen och Europarådet.

Utredaren ska påbörja sitt arbete den 1 september 2022. Uppdraget ska redovisas senast den 1 december 2023.

(Justitiedepartementet)

Statens offentliga utredningar 2023

Kronologisk förteckning

1. Skärpta straff för flerfaldig brottslighet. Ju.
2. En inre marknad för digitala tjänster – ansvarsfördelning mellan myndigheter. Fi.
3. Nya regler om nödlidande kreditavtal och inkassoverksamhet. Ju.
4. Posttjänst för hela slanten. Finansieringsmodeller för framtidens samhällsomfattande posttjänst. Fi.
5. Från delar till helhet. Tvångsvården som en del av en sammanhållen och personcentrerad vårdkedja. S.
6. En lag om tilläggsskatt för företag i stora koncerner. Fi.
7. På egna ben. Utvecklad samverkan för individers etablering på arbetsmarknaden. A.
8. Arbetslivskriminalitet – arbetet i Sverige, en bedömning av omfattningen, lärdomar från Danmark och Finland. A.
9. Ett statligt huvudmannaskap för personlig assistans. Ökad likvärdighet, långsiktighet och kvalitet. S.
10. Tandvårdens stöd till våldsutsatta patienter. S.
11. Tillfälligt miljötillstånd för samhällsviktig verksamhet – för ökad försörjningsberedskap. KN.
12. Förstärkt skydd för demokratin och domstolarnas oberoende. Ju.
13. Patientöversikter inom EES och Sverige. S.
14. Organisera för hållbar utveckling. KN.
15. Förnybart i tanken. Ett styrmedelsförslag för en stärkt bioekonomi. LI.
16. Staten och betalningarna. Del 1 och 2. Fi.
17. En tydligare bestämmelse om hets mot folkgrupp. Ju.
18. Värdet av vinden. Kompensation, incitament och planering för en hållbar fortsatt utbyggnad av vindkraften. Del 1 och 2. KN.
19. Statlig forskningsfinansiering. Underlagsrapporter. U.
20. Förbud mot bottentrålning i marina skyddade områden. LI.
21. Informationsförsörjning på skolområdet. Skolverkets ansvar. U.
22. Datalagring och åtkomst till elektronisk information. Ju.
23. Ett modernare socialförsäkringsskydd för gravida. S.
24. Etablering för fler – jämställda möjligheter till integration. A.
25. Kunskapskrav för permanent uppehållstillstånd. Ju.
26. Översyn av entreprenörsansvaret. A.
27. Kamerabevakning för ett bättre djurskydd. LI.
28. Samhället mot skolattacker. U.
29. Varje rörelse räknas – hur skapar vi ett samhälle som främjar fysisk aktivitet? S.
30. Ett trygghetssystem för alla. Nytt regelverk för sjukpenninggrundande inkomst. S.
31. Framtidens yrkeshögskola – stabil, effektiv och hållbar. U.
32. Biometri – för en effektivare brottsbekämpning. Ju.
33. Ett förbättrat resegarantisystem. Fi.
34. Bolag och brott – några åtgärder mot oseriösa företag. Ju.
35. Nya regler om hållbarhetsredovisning. Ju.
36. Genomförande av minimilönedirektivet. A.

37. Förstärkt skydd för den personliga integriteten. Behovet av åtgärder mot oskuldskontroller, oskuldsintyg och oskuldsingrepp samt omvändelseförsök. Ju.
38. Ett förstärkt konsumentskydd mot riskfylld kreditgivning och överskuldsättning. Fi.
39. En inre marknad för digitala tjänster – kompletteringar och ändringar i svensk rätt. Fi.
40. Förbättrade möjligheter för barn att utkräva sina rättigheter enligt barnkonventionen. S.
41. Förutsättningarna för en ny kollektivavtalad arbetslöshetsförsäkring. A.
42. Ett modernare regelverk för legaliseringar, apostille och andra former av intyganden. UD.
43. En samordnad registerkontroll för upphandlande myndigheter och enheter. Fi.
44. En översyn av regleringen om frihetsberövande påföljder för unga. Ju.
45. Övergångsrestriktioner – ökat förtroende för offentlig verksamhet. Fi.
46. Jakt och fiske i renbetesland. LI.
47. En utvecklad arbetsgivardeklaration – åtgärder mot missbruk av välfärdssystemen. Fi.
48. Rätt förutsättningar för sjukskrivning. S.
49. Skyddet för EU:s finansiella intressen. Ändringar och kompletteringar i svensk rätt. Fi.
50. En modell för svensk försörjningsberedskap. Fö.
51. Signalspaning i försvarsunderrättelseverksamhet – frågor med anledning av Europadomstolens dom. Fö.
52. Ett stärkt och samlat skydd av välfärdssystemen. S.
53. En ändamålsenlig arbetsskadeförsäkring – för bättre ekonomisk trygghet, kunskap och rättssäkerhet. Volym 1 och 2. S.
54. Centraliseringen av administrativa tjänster till Statens servicecenter – en utvärdering. Fi.
55. Vem äger fastigheten. Ju.
56. Några smittskyddsfrågor inom socialtjänsten och socialförsäkringen. S.
57. Åtgärder för tryggare bostadsområden. Ju.
58. Kultursamhället – utvecklad samverkan mellan stat, region och kommun. Ku.
59. Ny myndighetsstruktur för finansiering av forskning och innovation. U.
60. Utökade möjligheter att använda preventiva tvångsmedel 2. Ju.
61. En säker och tillgänglig statlig e-legitimation. Fi.
62. Vi kan bättre! Kunskapsbaserad narkotikapolitik med liv och hälsa i fokus. S.
63. Sveriges säkerhet i etern. Ku.
64. Ett förändrat regelverk för framtidens el- och gasnät. KN.
65. Bättre information om hyresbostäder. Kartläggning av andrahandsmarknaden och ett förbättrat lägenhetsregister. LI.
66. För barn och unga i samhällsvård. S.
67. Anonyma vittnen. Ju.
68. Som om vi aldrig funnits – exkludering och assimilering av tornedalingar, kväner och lantalaiset. Aivan ko meitä ei olis ollukhaan – eksklyteerinki ja assimileerinki tornionlaaksolaisista, kväänistä ja lantalaisista. *Slutbetänkande*. Som om vi aldrig funnits. Vår sanning och verklighet. Aivan ko meitä ei olis ollukhaan. Meän tottuus ja toelisuus. *Intervjuberättelser*. Som om vi aldrig funnits. Tolv tematiska forskarrapporter. Aivan ko meitä ei olis ollukhaan. Kakstoista temattista tutkintoraporttia. *Forskarrapporter*. Ku.
69. Ökat informationsflöde till brottsbekämpningen. En ny huvudregel. Ju.

70. Ordning och reda – förstärkt och tillförlitlig byggkontroll. LI.
71. Speciallivsmedel till barn inom öppen hälso- och sjukvård. S.
72. En enklare hantering av vattenfrågor vid planläggning och byggande. LI.
73. Genomförandet av vaccineringen mot sjukdomen covid-19 – en utvärdering. S.
74. Förenklade förutsättningar för ett hållbart vattenbruk. LI.
75. Stärkt konstitutionell beredskap. Ju.
76. Vidareanvändning av hälsodata för vård och klinisk forskning. S.
77. Behörig myndighet enligt EU:s avskogningsförordning. LI.
78. Hemlig dataavläsning – utvärdering och permanent lagstiftning. Ju.

Statens offentliga utredningar 2023

Systematisk förteckning

Vem äger fastigheten. [55]

Åtgärder för tryggare bostadsområden. [57]

Utökade möjligheter att använda preventiva tvångsmedel 2. [60]

Anonyma vittnen. [67]

Ökat informationsflöde till brottsbekämpningen. En ny huvudregel. [69]

Stärkt konstitutionell beredskap. [75]

Hemlig dataavläsning – utvärdering och permanent lagstiftning. [78]

Klimat- och näringslivsdepartementet

Tillfälligt miljötillstånd för samhällsviktig verksamhet – för ökad försörjningsberedskap. [11]

Organisera för hållbar utveckling. [14]

Värdet av vinden. Kompensation, incitament och planering för en hållbar fortsatt utbyggnad av vindkraften. Del 1 och 2. [18]

Ett förändrat regelverk för framtidens el- och gasnät. [64]

Kulturdepartementet

Kultursamhället – utvecklad samverkan mellan stat, region och kommun. [58]

Sveriges säkerhet i etern. [63]

Som om vi aldrig funnits – exkludering och assimilering av tornedalingar, kväner och lantalaiset. Aivan ko meitä ei olis ollukhaan – eksklyteerinki ja assimileerinki tornionlaaksolaisista, kväänistä ja lantalaisista. *Slutbetänkande.* Som om vi aldrig funnits. Vår sanning och verklighet. Aivan ko meitä ei olis ollukhaan. Meän tottuus ja toelisuus. *Intervjuberättelser.* Som om vi aldrig funnits. Tolv tematiska forskarrapporter. Aivan ko meitä ei olis ollukhaan. Kakstoista temattista tutkintoraporttia. *Forskarrapporter.* [68]

Landsbygds- och infrastrukturdepartementet

Förnybart i tanken. Ett styrmedelsförslag för en stärkt bioekonomi. [15]

Förbud mot bottentrålning i marina skyddade områden. [20]

Kamerabevakning för ett bättre djurskydd. [27]

Jakt och fiske i renbetesland. [46]

Bättre information om hyresbostäder. Kartläggning av andrahandsmarknaden och ett förbättrat lägenhetsregister. [65]

Ordning och reda – förstärkt och tillförlitlig byggkontroll. [70]

En enklare hantering av vattenfrågor vid planläggning och byggande. [72]

Förenklade förutsättningar för ett hållbart vattenbruk. [74]

Behörig myndighet enligt EU:s avskogningsförordning. [77]

Socialdepartementet

Från delar till helhet. Tvångsvården som en del av en sammanhållen och personcentrerad vårdkedja. [5]

Ett statligt huvudmannaskap för personlig assistans. Ökad likvärdighet, långsiktighet och kvalitet. [9]

Tandvårdens stöd till våldsutsatta patienter. [10]

Patientöversikter inom EES och Sverige. [13]

Ett modernare socialförsäkringsskydd för gravida. [23]

Varje rörelse räknas – hur skapar vi ett samhälle som främjar fysisk aktivitet? [29]

Ett trygghetssystem för alla. Nytt regelverk för sjukpenninggrundande inkomst. [30]

Förbättrade möjligheter för barn att utkräva sina rättigheter enligt barnkonventionen. [40]

Rätt förutsättningar för sjukskrivning. [48]

Ett stärkt och samlat skydd av välfärdssystemen. [52]

En ändamålsenlig arbetsskadeförsäkring – för bättre ekonomisk trygghet, kunskap och rättssäkerhet. Volym 1 och 2. [53]

Några smittskyddsfrågor inom socialtjänsten och socialförsäkringen. [56]

Vi kan bättre! Kunskapsbaserad narkotikapolitik med liv och hälsa i fokus. [62]

För barn och unga i samhällsvård. [66]

Speciallivsmedel till barn inom öppen hälso- och sjukvård. [71]

Genomförandet av vaccineringen mot sjukdomen covid-19 – en utvärdering. [73]

Vidareanvändning av hälsodata för vård och klinisk forskning. [76]

Utbildningsdepartementet

Statlig forskningsfinansiering. Underlagsrapporter. [19]

Informationsförsörjning på skolområdet. Skolverkets ansvar. [21]

Samhället mot skolattacker. [28]

Framtidens yrkeshögskola – stabil, effektiv och hållbar. [31]

Ny myndighetsstruktur för finansiering av forskning och innovation. [59]

Utrikesdepartementet

Ett modernare regelverk för legaliseringar, apostille och andra former av intygan-den. [42]