Justitieutskottets betänkande
2019/20:JuU19

Hemlig dataavläsning

Sammanfattning

Utskottet ställer sig bakom regeringens förslag till lag om hemlig dataavläsning och de följdändringar som föreslås i ett antal andra lagar.

Förslaget innebär att de brottsbekämpande myndigheterna får möjlighet att använda ett nytt hemligt tvångsmedel vid misstankar om allvarlig brottslighet. Det nya tvångsmedlet ska kallas hemlig dataavläsning. Hemlig dataavläsning är en metod för de brottsbekämpande myndigheterna att med någon form av tekniskt hjälpmedel i hemlighet bereda sig tillgång till en dator eller någon annan teknisk utrustning som kan användas för kommunikation och därigenom få besked om hur utrustningen används eller har använts och vilken information som finns i den. Hemlig dataavläsning bedöms leda till bättre och effektivare möjligheter att ta del av information som i dagsläget inte är tillgänglig. Det nya tvångsmedlet ska kunna användas under en förundersökning, i underrättelseverksamhet och vid särskild utlänningskontroll. Möjligheten till hemlig dataavläsning ska enligt förslaget införas genom en särskild tidsbegränsad lag som ska gälla i fem år.

Utskottet föreslår att den nya lagen och lagändringarna ska träda i kraft den 1 april 2020 och att den nya lagen därmed ska upphöra att gälla vid utgången av mars 2025.

Utskottet föreslår även att riksdagen avslår åtta motionsyrkanden.

I betänkandet finns sex reservationer (M, SD, V, KD).

Behandlade förslag

Proposition 2019/20:64 Hemlig dataavläsning.

Åtta yrkanden i följdmotioner.

Innehållsförteckning

Utskottets förslag till riksdagsbeslut

1. Hemlig dataavläsning

Riksdagen antar regeringens förslag till

1. lag om hemlig dataavläsning,
2. lag om ändring i lagen (1988:97) om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m.,
3. lag om ändring i lagen (1991:572) om särskild utlänningskontroll,
4. lag om ändring i lagen (2000:562) om internationell rättslig hjälp i brottmål,
5. lag om ändring i offentlighets- och sekretesslagen (2009:400),
6. lag om ändring i lagen (2017:1000) om en europeisk utredningsorder,

med den ändringen att lagarna ska träda i kraft den 1 april 2020 och att lagen om hemlig dataavläsning ska upphöra att gälla vid utgången av mars 2025.

Därmed bifaller riksdagen proposition 2019/20:64 punkterna 1–6 och avslår motion
2019/20:3451 av Linda Westerlund Snecker m.fl. (V).

Reservation 1 (V)

2. Platskrav

Riksdagen avslår motionerna
2019/20:3471 av Ingemar Kihlström m.fl. (KD) yrkande 2 och
2019/20:3475 av Adam Marttinen m.fl. (SD) yrkande 1.

Reservation 2 (M, SD, KD)

3. Hemlig dataavläsning i inhämtningslagsfallen

Riksdagen avslår motionerna
2019/20:3471 av Ingemar Kihlström m.fl. (KD) yrkande 1 och
2019/20:3475 av Adam Marttinen m.fl. (SD) yrkande 3.

Reservation 3 (M, SD, KD)

4. Förbud mot hemlig dataavläsning i vissa fall

Riksdagen avslår motion
2019/20:3475 av Adam Marttinen m.fl. (SD) yrkande 2.

Reservation 4 (SD)

5. Beslut om tillträdestillstånd

Riksdagen avslår motion
2019/20:3471 av Ingemar Kihlström m.fl. (KD) yrkande 3.

Reservation 5 (KD)

6. Territorialitetsprincipen

Riksdagen avslår motion
2019/20:3475 av Adam Marttinen m.fl. (SD) yrkande 4.

Reservation 6 (SD)

Stockholm den 13 februari 2020

På justitieutskottets vägnar

Fredrik Lundh Sammeli

Följande ledamöter har deltagit i beslutet: Fredrik Lundh Sammeli (S), Ingemar Kihlström (KD), Johan Forssell (M), Petter Löberg (S), Magdalena Schröder (M), Adam Marttinen (SD), Maria Strömkvist (S), Linda Westerlund Snecker (V), Ellen Juntti (M), Katja Nyberg (SD), Joakim Sandell (S), Carina Ödebrink (S), Johan Pehrson (L), Bo Broman (SD), Rasmus Ling (MP), Helena Vilhelmsson (C) och Mattias Ingeson (KD).

Redogörelse för ärendet

I betänkandet behandlar utskottet regeringens proposition 2019/20:64 Hemlig dataavläsning. I propositionen, som överlämnades till riksdagen den 11 december 2019, föreslår regeringen att en ny lag med bestämmelser om hemlig dataavläsning införs. Lagen ska tidsbegränsas till att gälla i fem år efter införandet.

Regeringens förslag till riksdagsbeslut återges i bilaga 1. Regeringens lagförslag finns i bilaga 2.

Tre motioner har väckts med anledning av propositionen. Förslagen i motionerna finns i bilaga 1.

Justitieutskottet beslutade den 23 januari 2020 att ge konstitutionsutskottet tillfälle att yttra sig över propositionen och motionerna i de delar de berör konstitutionsutskottets beredningsområde. Konstitutionsutskottets yttrande finns i bilaga 3.

Utskottets överväganden

Hemlig dataavläsning

Utskottets förslag i korthet

Riksdagen antar regeringens förslag till lag om hemlig dataavläsning och de föreslagna följdändringarna i övriga lagar, med den ändringen att lagarna ska träda i kraft den 1 april 2020 och att lagen om hemlig dataavläsning ska upphöra att gälla vid utgången av mars 2025.

Riksdagen avslår motionsyrkanden om bl.a. avslag på propositionen, platskrav och förbud mot hemlig dataavläsning i vissa fall.

Jämför reservation 1 (V), 2 (M, SD, KD), 3 (M, SD, KD), 4 (SD), 5 (KD) och 6 (SD).

Gällande ordning

Inledning

Enligt 2 kap. 6 § första stycket regeringsformen (RF) gäller att var och en gentemot det allmänna är skyddad mot bl.a. husrannsakan och liknande intrång, undersökning av brev eller annan förtrolig försändelse samt hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande. Det finns också i paragrafens andra stycke en bestämmelse som tillförsäkrar enskilda ett generellt skydd gentemot det allmänna, mot betydande intrång i den personliga integriteten om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Skyddet kan enligt 2 kap. 6 § RF bara begränsas genom lag och endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. En begränsning får inte gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen såsom en av folkstyrelsens grundvalar (2 kap. 20 och 21 §§ RF). För utländska medborgare som är bofasta i riket gäller att särskilda begränsningar i dessa rättigheter får göras genom lag (2 kap. 25 § RF).

Enligt artikel 8 i europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) har var och en rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. En inskränkning i dessa rättigheter får bara göras med stöd av lag och om det är nödvändigt med hänsyn till ändamål som är angivna i artikeln. Europakonventionen gäller som svensk lag. En lag eller en annan föreskrift får inte meddelas i strid med Sveriges åtaganden på grund av konventionen (2 kap. 19 § RF).

En bestämmelse om rätt till respekt för bl.a. privatlivet och korrespondensen finns också i artikel 7 i Europeiska unionens stadga om de grundläggande rättigheterna. I artikel 8 slås därutöver fast en rätt till skydd för personuppgifter som rör någon enskild.

För all användning av tvångsmedel gäller tre allmänna principer, nämligen ändamålsprincipen, behovsprincipen och proportionalitetsprincipen. Enligt ändamålsprincipen får ett tvångsmedel användas endast för det ändamål som framgår av lagstiftningen. Behovsprincipen innebär att ett tvångsmedel får användas endast om det finns ett påtagligt behov och en mindre ingripande åtgärd är otillräcklig. Proportionalitetsprincipen innebär att en tvångsåtgärd i fråga om art, styrka, räckvidd och varaktighet ska stå i rimlig proportion till vad som står att vinna med åtgärden.

Hemliga tvångsmedel enligt rättegångsbalken

Bestämmelser om hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning som tvångsmedel vid utredning av brott finns i 27 kap. rättegångsbalken (RB).

Hemlig avlyssning av elektronisk kommunikation

Hemlig avlyssning av elektronisk kommunikation innebär att meddelanden, som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller annan adress, i hemlighet avlyssnas eller tas upp genom ett tekniskt hjälpmedel för återgivning av innehållet i meddelandet (27 kap. 18 § första stycket RB). Ett elektroniskt kommunikationsnät är ett system för överföring och i tillämpliga fall utrustning för koppling eller dirigering samt passiva nätdelar och andra resurser som medger överföring av signaler, via tråd eller radiovågor, på optisk väg eller via andra elektromagnetiska överföringsmedier oberoende av vilken typ av information som överförs (1 kap. 7 § lagen [2003:389] om elektronisk kommunikation). I begreppet adress ingår olika typer av nummer, t.ex. telefonnummer och andra identifikationsnummer och adresser, såsom e-postadresser (prop. 2011/12:55 s. 62). Tvångsmedlet kan tillämpas på alla former av kommunikation genom elektroniska kommunikationsnät och är tillämpligt på muntlig och skriftlig kommunikation, liksom även på datakommunikation.

Tillstånd till hemlig avlyssning av elektronisk kommunikation får lämnas vid misstanke om brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år, för vissa särskilt uppräknade brott som framför allt Säkerhetspolisen utreder samt om det i ett enskilt fall kan antas att brottets straffvärde överstiger fängelse i två år (27 kap. 18 § andra stycket RB).

Hemlig avlyssning av elektronisk kommunikation får användas när någon är skäligen misstänkt för ett brott och åtgärden är av synnerlig vikt för utredningen (27 kap. 20 § första stycket RB). Avlyssning får avse ett telefonnummer eller annan adress som under den tid som tillståndet avser innehas eller har innehafts av den misstänkte eller annars kan antas ha använts eller

komma att användas av denne. Åtgärden får också avse ett telefonnummer eller annan adress som det finns synnerlig anledning att anta att den misstänkte under den tid som tillståndet avser har kontaktat eller kommer att kontakta.

Hemlig övervakning av elektronisk kommunikation

Hemlig övervakning av elektronisk kommunikation innebär att uppgifter i hemlighet hämtas in om meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller annan adress, vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område eller i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits (27 kap. 19 § första stycket RB). Genom hemlig övervakning av elektronisk kommunikation får meddelanden även hindras från att nå fram (27 kap. 19 § andra stycket RB). Till skillnad från hemlig avlyssning av elektronisk kommunikation ger inte tvångsmedlet tillgång till uppgifter om innehållet i meddelanden. Det som kan hämtas in är i stället trafikuppgifter och uppgifter om lokalisering.

Tillstånd till hemlig övervakning av elektronisk kommunikation kan beviljas vid en förundersökning om brott för vilket det inte är föreskrivet lindrigare straff än fängelse i sex månader, för vissa särskilt uppräknade brott som framför allt Polismyndigheten utreder (t.ex. dataintrång och icke ringa barnpornografibrott) samt för vissa särskilt uppräknade brott som framför allt Säkerhetspolisen utreder (27 kap. 19 § andra stycket RB). Åtgärden får tillåtas dels om någon är skäligen misstänkt för brott och då avse de telefonnummer eller adresser som gäller vid hemlig avlyssning av elektronisk kommunikation, dels i syfte att utreda vem som skäligen kan misstänkas för brottet. I den senare situationen gäller dock att tvångsmedlet får användas endast vid en förundersökning som avser brott som kan leda till hemlig avlyssning av elektronisk kommunikation och att övervakning som innebär att uppgifter hämtas in om meddelanden endast får avse förfluten tid (27 kap. 19 § fjärde stycket och 20 § andra stycket RB).

Hemlig kameraövervakning

Hemlig kameraövervakning innebär att fjärrstyrda tv-kameror, andra optisk-elektroniska instrument eller därmed jämförbar utrustning används för optisk personövervakning vid förundersökning i brottmål utan att upplysning om övervakningen lämnas (27 kap. 20 a § första stycket RB). I förarbetena till lagstiftningen om hemlig kameraövervakning förtydligas att tvångsmedlet inte omfattar ljudupptagning (prop. 1995/96:85 s. 37).

Tillstånd till hemlig kameraövervakning kan lämnas vid förundersökning som rör de brott som kan aktualisera tillstånd till hemlig avlyssning av elektronisk kommunikation (27 kap. 20 a § andra stycket RB). Övervakningen får som huvudregel användas endast om någon är skäligen misstänkt för brottet. Åtgärden får endast avse en plats där den misstänkte kan antas komma att uppehålla sig (27 kap. 20 b § RB). Övervakningen får även omfatta den

plats där ett brott har begåtts eller en nära omgivning till denna plats i syfte att fastställa vem som skäligen kan misstänkas för brottet (27 kap. 20 c § RB).

Hemlig rumsavlyssning

Hemlig rumsavlyssning innebär avlyssning eller upptagning som görs i hemlighet, och med ett tekniskt hjälpmedel som är avsett att återge ljud, och avser tal i enrum, samtal mellan andra eller förhandlingar vid sammanträden eller andra sammankomster som allmänheten inte har tillträde till (27 kap. 20 d § första stycket RB). Rumsavlyssning får endast användas vid förundersökning om brott för vilket det inte är föreskrivet lindrigare straff än fängelse i fyra år, spionerі, brott mot lagen (2018:558) om företagshemligheter som kan antas ha begåtts eller understötts av främmande makt samt för vissa andra särskilt uppräknade brott (t.ex. människohandel, våldtäkt mot barn och grovt övergrepp i rättssak) om det i det enskilda fallet kan antas att brottets straffvärde överstiger fängelse i fyra år. Tvångsmedlet får användas endast när någon är skäligen misstänkt för något av de angivna brotten. Dessutom får åtgärden endast avse en plats där det finns särskild anledning att anta att den misstänkte kommer att uppehålla sig. Om åtgärden avser någon annan stadigvarande bostad än den misstänktes får hemlig rumsavlyssning användas endast om det finns synnerlig anledning att anta att den misstänkte kommer att uppehålla sig där.

Åtgärder för att förhindra vissa särskilt allvarliga brott

Enligt lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen) får tillstånd till hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation eller hemlig kameraövervakning beviljas redan i underrättelseskedet, dvs. innan en förundersökning har inletts. Tillstånd får beviljas om det med hänsyn till omständigheterna finns en påtaglig risk för att en person kommer att utöva brottslig verksamhet som innefattar bl.a. sabotage, spionerі och terroristbrott (1 § första stycket). Sådant tillstånd får också beviljas om det finns en påtaglig risk för att det inom en organisation eller grupp kommer att utövas sådan brottslig verksamhet och det kan befaras att en person som tillhör eller verkar för organisationen eller gruppen medvetet kommer att främja denna verksamhet (1 § andra stycket).

Inhämtning av elektronisk kommunikation i underrättelseverksamhet

Lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen) reglerar förutsättningarna för Polismyndigheten, Säkerhetspolisen och Tullverket att i underrättelseverksamhet hämta in övervakningsuppgifter om elektronisk kommunikation från teleoperatörerna. De uppgifter som kan hämtas in motsvarar de som kan hämtas in genom hemlig övervakning av elektronisk kommunikation när den åtgärden används för att utreda vem som

skäligen kan misstänkas för ett brott (1 §). Uppgifter får hämtas in, om omständigheterna är sådana att åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott vilka har ett straffminimum på fängelse i minst två år eller om det är fråga om brottslig verksamhet som innefattar vissa särskilt angivna samhällsfarliga brott inom Säkerhetspolisens ansvarsområde (2 §).

Särskild utlänningskontroll

Enligt lagen (1991:572) om särskild utlänningskontroll får tillstånd till hemlig avlyssning av elektronisk kommunikation eller, om det är tillräckligt, hemlig övervakning av elektronisk kommunikation beviljas om det är av betydelse för att utreda om en utlänning eller en organisation eller grupp som han eller hon tillhör eller verkar för planlägger eller förbereder terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott och det finns synnerliga skäl (19 och 20 §§).

Förbud mot användning av hemliga tvångsmedel

Vissa yrkeskategorier bedriver verksamhet som omfattas av tystnadsplikt. Tystnadsplikten hindrar i många fall personerna i verksamheten från att vittna i en rättegång om angelägenheter som anförtrotts dem i deras yrkesutövning (36 kap. 5 § RB). Bestämmelserna begränsar möjligheten att inför domstol ställa frågor till ett vittne och brukar därför beskrivas som frågeförbud. Det finns också regler som förbjuder användningen av hemlig rumsavlyssning i lokaler som används för viss verksamhet (27 kap. 20 e § tredje stycket RB). Förbudet mot hemlig rumsavlyssning gäller på följande platser:

1. en plats som stadigvarande används eller är särskilt avsedd att användas för verksamhet som tystnadsplikt gäller för enligt 3 kap. 3 § tryckfrihetsförordningen eller 2 kap. 3 § yttrandefrihetsgrundlagen
2. en plats som stadigvarande används eller är särskilt avsedd att användas för verksamhet som bedrivs av advokater, läkare, tandläkare, barnmorskor, sjuksköterskor, psykologer, psykoterapeuter eller familjerådgivare enligt socialtjänstlagen (2001:453)
3. en plats som stadigvarande används eller är särskilt avsedd att användas av präster inom trossamfund eller av dem som har motsvarande ställning inom sådana samfund, för bikt eller enskild själavård.

Det finns även särskilda regler om avlyssningsförbud för både hemlig avlyssning av elektronisk kommunikation och för rumsavlyssning (27 kap. 22 § RB och 11 § preventivlagen). Bestämmelserna är utformade så att avlyssning inte får avse samtal, annat tal eller meddelanden där någon som yttrar sig är undantagen från vittnesplikt enligt frågeförbudet.

I rättegångsbalken finns också skydd för uppgifter som en befattningshavare eller någon annan som avses i 36 kap. 5 § RB inte får höras som vittne om (27 kap. 2 § första stycket RB). Detta innebär förbud mot att ta en skriftlig

handling i beslag om den kan antas innehålla sådana uppgifter och innehas av antingen en person som avses i 36 kap. 5 § RB eller av den som tystnadsplikten gäller till förmån för. Högsta domstolen har slagit fast att beslagsförbudet är ett informationsskydd som gäller oavsett informationsbärare och således inte enbart för information på ett papper (NJA 2015 s. 631 p. 25 och 26).

Propositionen

Hemlig dataavläsning

Det finns i dag inte någon legaldefinition av hemlig dataavläsning. Följande definition har dock ingått i de direktiv som ligger till grund för övervägandena i delbetänkandet Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet (SOU 2017:89) och för regeringens proposition.

> Hemlig dataavläsning är en metod för de brottsbekämpande myndigheterna att med någon form av tekniskt hjälpmedel i hemlighet bereda sig tillgång till en dator eller annan teknisk utrustning som kan användas för kommunikation och därigenom få besked om hur utrustningen används eller har använts och vilken information som finns i den.

Metoden för hemlig dataavläsning kan alltså sägas inbegripa två delar, dels att den brottsbekämpande myndigheten bereder sig tillgång till teknisk utrustning som kan användas för kommunikation, dels att myndigheten tar del av uppgifter som finns i utrustningen. De uppgifter som hemlig dataavläsning är tänkta att komma åt finns alltså i den tekniska utrustningen, t.ex. i en mobiltelefon eller en dator. Det skiljer sig från vad som är fallet vid hemlig avlyssning eller övervakning av elektronisk kommunikation, där uppgifterna hämtas in på väg till eller från någons tekniska utrustning. Det skiljer sig också från hemlig rumsavlyssning och hemlig kameraövervakning, där uppgifterna hämtas in genom utrustning som tillhör och monteras av de brottsbekämpande myndigheterna.

Redan i dag kan de brottsbekämpande myndigheterna få tillstånd att hämta in många av de uppgifter som skulle kunna hämtas in genom hemlig dataavläsning. I många fall motsvaras emellertid 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 (t.ex. samtal och meddelanden via vanligt förekommande mobiltelefonappar som Whatsapp, Imessage eller Facetime). Meddelanden och samtal som de brottsbekämpande myndigheterna i och för sig har rätt att lyssna av enligt ett tillstånd till hemlig avlyssning av elektronisk kommunikation kan därför inte fångas upp i läsbart eller avlyssningsbart skick.

Behovet av hemlig dataavläsning

Regeringen gör i propositionen bedömningen att det finns ett påtagligt behov av nya och bättre metoder för att i hemlighet komma åt uppgifter som redan i dag får hämtas in med befintliga tvångsmedel men som på grund av den

tekniska utvecklingen och brotts- och samhällsutvecklingen i övrigt inte går att komma åt. Framför allt kryptering och anonymisering har lett till att hemlig avlyssning och hemlig övervakning av elektronisk kommunikation har minskat i effektivitet på senare år. När det gäller hemlig kameraövervakning och hemlig rumsavlyssning finns det visserligen enligt regeringen ingenting som talar för att de åtgärderna i teknisk mening fungerar sämre i dag än de gjort tidigare. Det har däremot framkommit att det i vissa fall inte är möjligt att verkställa åtgärderna på grund av att den verkställande myndigheten inte kan bereda sig tillgång till den plats ett tillstånd avser eller att det inte finns något lämpligt ställe på platsen att montera det tekniska hjälpmedlet på. En generell medvetenhet hos kriminella om under vilka förutsättningar de brottsbekämpande myndigheterna får använda befintliga hemliga tvångsmedel lyfts också fram som skäl för nya metoder.

I propositionen gör regeringen även bedömningen att det finns ett påtagligt behov av att i hemlighet kunna samla in elektroniskt lagrade uppgifter och uppgifter som visar hur ett avläsningsbart informationssystem (t.ex. en dator eller mobiltelefon) används, som inte kan samlas in genom befintliga tvångsmedel. Regeringen konstaterar bl.a. att dagens ordinarie utredningsmetoder oftast inte är tillräckliga för att driva en förundersökning framåt. Beslag av datorer räcker inte för bevissäkring i komplexa ärenden, eftersom kryptering eller lösenordsskydd försvårar eller gör det omöjligt att i efterhand ta fram information från datorn. Förekomsten av raderingsprogram och instruktioner på internet om s.k. antiforensiska metoder talar enligt regeringen för att det finns behov av att kunna samla in uppgifter i hemlighet, löpande och i realtid. För detta talar också de fördelar det skulle innebära för de brottsbekämpande myndigheterna, t.ex. att under pågående tvångsmedelsanvändning kunna identifiera brottsplaner, förhindra att brott fullbordas, avvärja överhängande fara och säkra bevis.

Regeringen framhåller också att det till skillnad från vad som gäller under en förundersökning inte finns några regler som tillåter beslag i den brottsförhindrande verksamheten. Det finns således inte någon möjlighet för de brottsbekämpande myndigheterna att i underrättelseverksamhet komma åt information som finns lagrad i en kommunikationsutrustning, utan det är först när uppgifterna sänds från enheten i t.ex. ett e-brev som de blir åtkomliga genom hemlig avlyssning av elektronisk kommunikation. Regeringen konstaterar att de brottsbekämpande myndigheterna genom hemlig dataavläsning skulle kunna få tillgång till uppgifter som antecknade brottsplaner, fotografier över tänkta brottsplatser och annan lagrad information. Detta skulle redan i ett tidigt skede kunna ge bättre förutsättningar att hindra t.ex. planerade terrordåd.

Hemlig dataavläsning förväntas vara en effektiv åtgärd

Enligt regeringen kommer det att krävas ett omfattande förberedelsearbete och en förmåga att möta tekniska svårigheter vid verkställighet av hemlig dataavläsning. Mot den bakgrunden bedömer regeringen att hemlig dataavläsning endast kommer att vara möjlig att använda i ett begränsat antal fall.

När det gäller kvalitativ effektivitet konstaterar regeringen att en brottsbekämpande myndighet, i de fall den inte har fysisk tillgång till den tekniska utrustningen, måste utnyttja sårbarheter för att komma åt uppgifterna. Sådana sårbarheter kan vara av olika slag och därför i förlängningen ge tillgång till olika delar av en viss teknisk utrustning. Beroende på karaktären på sårbarheten i det enskilda fallet kan det dock finnas begränsningar i vad som går att komma åt. Även andra tekniska faktorer, exempelvis hur säkerheten i form av brandväggar, virusprogram etc. är beskaffad, kan påverka vad som är möjligt att åstadkomma. Sättet att komma över uppgifter kan också variera över tid. Företag som utvecklar hårdvara, programvara eller appar arbetar kontinuerligt för att upptäcka och täppa igen sådana säkerhetsbrister som kan utnyttjas för att komma in i teknisk utrustning. Den kvalitativa effektiviteten av hemlig dataavläsning kan alltså påverkas av olika faktorer. Det får dock enligt regeringen förutsättas att den brottsbekämpande myndighet som ska verkställa åtgärden har gjort en noggrann kartläggning och analys för att säkerställa att verkställighetstekniken i det enskilda fallet ger tillgång till de uppgifter som eftersöks.

I propositionen konstateras även att hemlig dataavläsning är ett mycket resurskrävande tvångsmedel. Regeringen menar dock att detta inte är något som i sig innebär att arbetsmetoden är ineffektiv. De gånger hemlig dataavläsning kan verkställas på ett effektivt sätt får man tillgång till information som man inte hade kunnat skaffa fram på något annat sätt, eftersom en sådan åtgärd ibland är den enda framkomliga vägen i en utredning.

Regeringen konstaterar slutligen att även de kriminellas eget agerande kan påverka hur effektivt det är att använda hemlig dataavläsning, t.ex. genom säkerhetsuppdateringar. Enligt regeringen kan det dock inte förmodas att verkställigheten av hemlig dataavläsning på ett generellt plan skulle bli så lidande att den inte längre skulle kunna vara sakligt motiverad.

Sammanfattningsvis bedömer regeringen att hemlig dataavläsning bör kunna användas som metod för att komma åt uppgifter som de brottsbekämpande myndigheterna har ett påtagligt behov av. Åtgärden kommer dock att kunna genomföras i färre ärenden än där det finns behov av den. När hemlig dataavläsning kan genomföras förväntas åtgärden leda till betydligt bättre tillgång till information än vad dagens metoder ger tillgång till.

Det är proportionerligt att införa regler om hemlig dataavläsning

Regeringen bedömer att hemlig dataavläsning, vid en jämförelse med den nuvarande användningen av hemliga tvångsmedel, innebär att riskerna för

enskildas personliga integritet ökar. Enligt regeringen är det ändå proportionerligt att införa regler om hemlig dataavläsning under förutsättning att dessa balanseras med rättssäkerhetsgarantier och regler för att minska riskerna för informationssäkerheten. Regeringen redovisar i avsnitt 8.6 i propositionen sina bedömningar och de avgränsningar som krävs för att hemlig dataavläsning ska vara en proportionerlig åtgärd. Sammanfattningsvis menar regeringen att de positiva effekter som förslaget får i form av att försvåra de kriminellas verksamhet klart överväger de negativa effekter som förslaget får i form av integritetsinskränkningar för den som blir föremål för åtgärden.

En ny lag om hemlig dataavläsning införs

Regeringen föreslår att en ny lag med bestämmelser om hemlig dataavläsning införs. Lagen ska tidsbegränsas till att gälla i fem år efter införandet. Eftersom nya tvångsmedel ger upphov till risker för otillbörliga integritetsintrång anser regeringen att ett fördjupat underlag kan behövas inför ett ställningstagande till om lagen bör permanentas. Vid en framtida utvärdering och beredning ska nyttan, behovet och proportionaliteten av hemlig dataavläsning återigen analyseras och bedömas.

Genom hemlig dataavläsning ska uppgifter som är avsedda för automatiserad behandling i hemlighet och med ett tekniskt hjälpmedel få läsas av eller tas upp i ett avläsningsbart informationssystem. Med avläsningsbart informationssystem avses antingen en elektronisk kommunikationsutrustning eller ett användarkonto till, eller en på motsvarande sätt avgränsad del av, en kommunikationstjänst, lagringstjänst eller liknande tjänst.

De uppgiftstyper som föreslås ska kunna läsas av eller tas upp efter tillstånd till hemlig dataavläsning är dels uppgifter som får hämtas in enligt de nu gällande reglerna om hemliga tvångsmedel, dels uppgifter som hemliga tvångsmedel tidigare inte gett tillgång till. I den förstnämnda kategorin har hemlig dataavläsning enligt regeringen närmast karaktären av en verkställighetsmetod för befintliga hemliga tvångsmedel. Regeringen föreslår att tillstånd till hemlig dataavläsning ska få beviljas för att läsa av eller ta upp

1. uppgifter om innehåll i meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller någon annan adress (kommunikationsavlyssningsuppgifter)
2. uppgifter om annat än innehåll i meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller någon annan adress (kommunikationsövervakningsuppgifter)
3. uppgifter om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits (platsuppgifter)
4. uppgifter som framkommer genom optisk personövervakning (kameraövervakningsuppgifter)

5. uppgifter som avser tal i enrum, samtal mellan andra eller förhandlingar vid sammanträden eller andra sammankomster som allmänheten inte har tillträde till (rumsavlyssningsuppgifter)
6. uppgifter som finns lagrade 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 (jfr 27 kap. 19 § andra stycket RB).

Eftersom hemlig dataavläsning innebär ett ökat integritetsintrång för den enskilde föreslår regeringen att det i den nya lagen uttryckligen anges att ett tillstånd till hemlig dataavläsning får beviljas endast om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktas mot eller för något annat motstående intresse (proportionalitetsprincipen). En utgångspunkt för proportionalitetsprövningen bör enligt regeringen 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 eller kan förväntas leda till större integritetsintrång.

Hemlig dataavläsning under en förundersökning

Enligt regeringen bör utgångspunkten för vilka krav som ska vara uppfyllda för att hemlig dataavläsning ska få användas för att läsa av eller ta upp uppgifter som får hämtas in med befintliga hemliga tvångsmedel motsvara de som gäller för de bakomliggande tvångsmedlen. Vid hemlig dataavläsning för att läsa av eller ta upp uppgifter som i dag inte är möjliga att hämta in med hemliga tvångsmedel bör kravet för hemlig dataavläsning enligt regeringens bedömning motsvara vad som gäller för hemlig avlyssning av elektronisk kommunikation. Detta medför enligt regeringen att de strafftrösklar som är föreskrivna för dessa tvångsmedel också som utgångspunkt ska tillämpas för hemlig dataavläsning.

Mot den bakgrunden föreslår regeringen att hemlig dataavläsning ska få användas vid förundersökning om sådana brott som kan aktualisera hemlig avlyssning av elektronisk kommunikation. När det gäller hemlig dataavläsning för att läsa av eller ta upp rumsavlyssningsuppgifter ska dock hemlig dataavläsning endast få användas vid förundersökning om sådana brott som kan föranleda hemlig rumsavlyssning. När det gäller avläsning eller upptagning av kommunikationsövervaknings- och platsuppgifter, dvs. uppgiftstyper som i dag får hämtas in genom hemlig övervakning av elektronisk kommunikation, innebär regeringens förslag att kravet för hemlig dataavläsning sätts högre än vad som gäller för inhämtning av uppgifterna enligt nuvarande regler.

Vilka brott som kan föranleda hemlig dataavläsning varierar alltså beroende på vilken åtgärd som tvångsmedlet avser. De straffnivåer som bestämmer när respektive tvångsmedel kan aktualiseras är enligt regeringens mening ändamålsenliga och tar hänsyn till tvångsmedlets ingripande karaktär samtidigt som kraven för användning av det inte ställs för högt. Om lagstiftningen skulle utformas på så sätt att endast Säkerhetspolisen skulle ha möjlighet till hemlig dataavläsning eller att strafftröskeln skulle sättas lika högt som för hemlig rumsavlyssning, som vissa remissinstanser anser, skulle tillämpningsområdet enligt regeringen begränsas på ett sätt som inte stämmer med behovet av tvångsmedlet. Det skulle innebära att det vid mycket allvarliga brott som faller utanför Säkerhetspolisens verksamhetsområde fortfarande skulle saknas möjlighet att läsa av t.ex. krypterad trafik. Det skulle i förlängningen kunna leda till att vissa brott inte kan utredas.

Hemlig dataavläsning ska som utgångspunkt få användas endast om någon är skäligen misstänkt för ett brott. Åtgärden ska vara av synnerlig vikt för utredningen.

Hemlig dataavläsning som används för att läsa av kameraövervakningsuppgifter ska endast få avse en plats där den misstänkte kan antas komma att uppehålla sig. En sådan plats får inte vara någons stadigvarande bostad. Vidare ska hemlig dataavläsning som används för att läsa av rumsavlyssningsuppgifter få användas endast på en plats där det finns särskild anledning att anta att den misstänkte kommer att uppehålla sig. Är platsen någon annan stadigvarande bostad än den misstänktes, ska avläsningen få utföras endast om det finns synnerlig anledning att anta att den misstänkte kommer att uppehålla sig där. Regeringen framhåller att platskravet är viktigt för att kunna bedöma det förväntade integritetsintrånget och hänvisar till den bedömning som gjordes i propositionen Hemlig kameraövervakning (prop. 1995/96:85 s. 29). I den propositionen diskuterade regeringen frågan om tillståndet skulle knytas till person eller plats. Om tillståndet skulle avse en person konstaterade regeringen att ändamålsprincipen, behovsprincipen och proportionalitetsprincipen skulle bli svåra att tillämpa. Som exempel anfördes att det inte skulle gå att tillämpa proportionalitetsprincipen eftersom det på förhand inte är känt vilka eller hur många platser som skulle komma att övervakas. Vid en förundersökning som avser ett visst brott skulle, beroende på omständigheterna, övervakning av en allmän plats kanske anses vara godtagbar medan övervakning av en enskild plats, t.ex. genom att kameran riktades mot ett bostadsfönster, inte skulle kunna komma i fråga. Mot denna bakgrund och av praktiska skäl fann regeringen att tillstånd till hemlig kameraövervakning skulle knytas till plats i stället för till person. Regeringen gör i detta lagstiftningsarbete samma principiella bedömning och föreslår att en verkställighet genom hemlig dataavläsning också ska vara underkastad ett platskrav. Att det kan krävas spaningsarbete eller liknande insatser för att säkerställa platsvillkoret utgör enligt regeringen inte ett tillräckligt skäl att göra någon annan bedömning. Regeringen konstaterar även att ställningstagandet ligger i linje med den slutsats som Utredningen om regeländringar

för vissa hemliga tvångsmedel har kommit fram till i betänkandet Förenklat förfarande vid vissa beslut om hemlig avlyssning, nämligen att det inte finns tillräckliga skäl att knyta ett tvångsmedel till en person, bl.a. eftersom de integritetsintrång som annars kan befaras är för stora (SOU 2018:30 s. 53–59).

Regeringens förslag innebär vidare att hemlig dataavläsning ska få avse ett avläsningsbart informationssystem som används, eller som det finns särskild anledning att anta har använts eller kommer att användas, av någon som är skäligen misstänkt för ett brott. Hemlig dataavläsning som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter ska även få 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. Tillstånd till hemlig dataavläsning som gäller kommunikationsövervaknings- eller platsuppgifter ska även få beviljas för att utreda vem som skäligen kan misstänkas för brottet, om åtgärden är av synnerlig vikt för utredningen. Avläsning eller upptagning av kommunikationsövervakningsuppgifter ska då endast få avse förfluten tid. En sådan åtgärd ska endast få avse 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.

Hemlig dataavläsning utanför en förundersökning

Regler om hemlig tvångsmedelsanvändning utanför en förundersökning finns som framgått ovan i preventivlagen, lagen om särskild utlänningskontroll och i inhämtningslagen. Regeringen gör i propositionen bedömningen att även hemlig dataavläsning bör få användas i underrättelseverksamhet och vid särskild utlänningskontroll. Eftersom införandet av hemlig dataavläsning till stor del syftar till att återställa de brottsbekämpande myndigheternas förmåga att förhindra och utreda brott bör utgångspunkten enligt regeringen vara att kraven som gäller för det hemliga tvångsmedlet enligt respektive lag ska gälla även för hemlig dataavläsning. När det gäller avläsning eller upptagning av lagrade uppgifter och uppgifter som visar hur ett informationssystem används konstaterar regeringen att det saknas befintliga hemliga tvångsmedel som kan bilda utgångspunkt för vilka krav som bör ställas upp. Regeringen gör här, liksom i förundersökningsfallen, bedömningen att sådana uppgifter bör få hämtas in under samma förutsättningar som gäller för hemlig avlyssning av elektronisk kommunikation.

När det gäller inhämtningslagsfallen föreslår regeringen att ett tillstånd till hemlig dataavläsning som gäller kommunikationsövervaknings- eller platsuppgifter ska få beviljas om åtgärden är av synnerlig vikt för att förebygga, förhindra eller upptäcka sådan brottslig verksamhet som anges i inhämtningslagen. Vid sådan hemlig dataavläsning ska meddelanden inte få hindras att nå fram. Ett tillstånd till hemlig dataavläsning för kommunikationsövervakningsuppgifter ska endast få avse uppgifter i förfluten tid.

Uppgifter som får hämtas in enligt inhämtningslagen är samma sorts uppgifter som får hämtas in efter beslut om hemlig övervakning av elektronisk kommunikation under förundersökning för att utreda vem som skäligen kan misstänkas för brottet. Inhämtningslagen uppställer som krav att åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år. Inhämtning får också ske om omständigheterna är sådana att åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar även viss annan samhällsfarlig brottslighet som räknas upp i lagen och vars straffskalor föreskriver lindrigare straff än två års fängelse.

Till skillnad från vad som gäller enligt inhämtningslagen innebär regeringens förslag att åtgärden ska vara av synnerlig vikt för att förebygga, förhindra eller upptäcka den brottsliga verksamheten. Regeringen anser att det är lämpligt att införa detta strängare krav när hemlig dataavläsning ska användas i inhämtningslagsfallen, framför allt med hänsyn till att det kravet föreslås för hemlig dataavläsning i övrigt.

Förbud mot hemlig dataavläsning

Regeringen föreslår att ett tillstånd till hemlig dataavläsning inte ska få avse ett avläsningsbart informationssystem som stadigvarande används eller är särskilt avsett att användas

1. i verksamhet där tystnadsplikt gäller enligt 3 kap. 3 § tryckfrihetsförordningen och 2 kap. 3 § yttrandefrihetsgrundlagen
2. i verksamhet som bedrivs av advokater, läkare, tandläkare, barnmorskor, sjuksköterskor, psykologer, psykoterapeuter eller familjerådgivare
3. av präster inom trossamfund eller av dem som har motsvarande ställning inom sådana samfund, i verksamhet för bikt eller enskild själavård.

Hemlig dataavläsning som gäller rumsavlyssningsuppgifter ska inte få avse en plats som stadigvarande används eller är särskilt avsedd att användas för sådan verksamhet som avses ovan.

Regeringen framhåller att verkställighet av hemlig dataavläsning innebär att man använder tekniker som skulle kunna ge tillgång till alla uppgifter som finns i ett visst avläsningsbart informationssystem. I informationssystem som används av t.ex. advokater, präster, läkare och journalister finns det en mängd känsliga uppgifter som är så skyddsvärda att sekretessen kring dem bör få företräde framför det brottsbekämpande intresset. Det finns behov av ett starkt skydd så att denna information inte kan spridas vidare till obehöriga. Därför bör det enligt regeringen införas ett förbud mot hemlig dataavläsning för informationssystem i sådana verksamheter. Regeringen noterar att detta är ett avsteg från vad som gäller vid hemlig övervakning av elektronisk kommunikation enligt rättegångsbalken. Regeringen bedömer dock, med hänsyn till integritetsintrånget i själva verkställighetstekniken, att det finns skäl att reglera

förbudet mot att läsa av eller ta upp de olika uppgiftstyperna från de aktuella informationssystemen på samma sätt, och därför bör även kommunikationsövervakningsuppgifter omfattas av förbudet. Även proportionalitetsbedömningen kan sätta gränser för om det är tillåtet med hemlig dataavläsning för att läsa av uppgifter när det inte står helt klart att informationssystemet stadigvarande används i vissa skyddade verksamheter. Genom ett krav på att informationssystemet stadigvarande ska användas i den skyddade verksamheten bedömer regeringen att risken för missbruk, t.ex. att kriminella kan anpassa sig efter undantaget i lagstiftningen, minskar.

När det gäller det föreslagna förbudet mot hemlig dataavläsning avseende präster inom trossamfund eller av dem som har motsvarande ställning inom sådana samfund samt i verksamhet för bikt eller enskild själavård skriver regeringen att det är självklart att det bör omfatta informationssystem som används i verksamhet som bedrivs i t.ex. kyrkor, synagogor och moskéer. Regeringen konstaterar att det blir mer komplicerat när en helt vanlig lokal med inga eller mycket få religiösa inslag påstås användas för t.ex. själavård. Det kan t.o.m. vara så att kriminella försöker freda platser från hemlig dataavläsning genom att påstå att de används i verksamhet för själavård. Enligt regeringen bör förbudet mot hemlig dataavläsning inte gälla på en sådan plats. Vidare bör det fredade utrymmet endast vara det begränsade utrymme som är direkt avsett för bikt eller själavård. Det förhållandet att en präst kan hålla ett själavårdande samtal i en kyrkbänk bör inte innebära att platsen är fredad från hemlig dataavläsning. Däremot menar regeringen att ett biktbås eller ett rum som är särskilt inrättat för själavård aldrig bör kunna bli föremål för hemlig dataavläsning. Samtidigt framhåller regeringen att även om en viss plats inte är fredad från hemlig dataavläsning så föreslås en skyldighet att omedelbart avbryta verkställigheten och förstöra upptagningarna om det framkommer uppgifter som är skyddade enligt 27 kap. 2 § första stycket RB, t.ex. uppgifter från bikt eller själavård. Ytterst blir det en fråga vid tillståndsprövningen och verkställigheten att i varje enskilt fall bedöma om hemlig dataavläsning bör utföras på den aktuella platsen eller om den har en skyddad ställning.

Tillträdestillstånd

Av dagens hemliga tvångsmedel är det endast hemlig rumsavlyssning som kan föranleda intrång i annars skyddade utrymmen för att i hemlighet och efter tillstånd installera tekniska hjälpmedel (27 kap. 25 a § RB). Regeringen konstaterar att det vid verkställighet av hemlig dataavläsning i vissa fall kommer att vara nödvändigt för den som ska verkställa åtgärden att komma närmare informationssystemet eller ha det i sin fysiska besittning, t.ex. då hårdvara ska användas vid verkställighet eller när det inte är möjligt att installera programvara på distans. När det står klart var informationssystemet finns behöver den verkställande myndigheten få tillgång till det. Ett sätt att få tillgång till informationssystemet är att tillåta den brottsbekämpande myndigheten att få tillträde till utrymmen som annars är skyddade mot intrång, t.ex.

enligt reglerna i 4 kap. brottsbalken. En möjlighet till tillträdestillstånd för hemlig dataavläsning utgör en utvidgning av möjligheterna till ett sådant tillstånd. Regeringen anser emellertid att en möjlighet till tillträdestillstånd bör införas för att tvångsmedlet ska ha önskad effektivitet.

Vid hemlig dataavläsning ska den verkställande myndigheten således enligt regeringens förslag, efter särskilt tillstånd, i hemlighet få skaffa sig tillträde till och installera tekniska hjälpmedel på en plats som annars skyddas mot intrång. Ett sådant tillstånd ska endast få avse en plats där det finns särskild anledning att anta att det avläsningsbara informationssystemet finns tillgängligt. Om platsen är en bostad som stadigvarande används av någon annan än den misstänkte eller en person som är föremål för hemlig dataavläsning enligt preventivlagen eller lagen om särskild utlänningskontroll, ska tillstånd få beviljas endast om det finns synnerlig anledning att anta att informationssystemet finns där. Tillträdestillstånd ska inte få avse en plats där det bedrivs verksamhet som skyddas av frågeförbudet i 36 kap. 5 § andra–sjätte styckena RB.

Regeringen noterar att Åklagarmyndigheten i sitt remissvar påpekar att det under verkställighet av hemlig dataavläsning kan uppstå en möjlighet till installation på platser som är lämpligare och mindre integritetskänsliga än den misstänktes hem. Dessa tillfällen kan dock vara svåra att förutse vid domstolens tillståndsprövning, och ett särskilt tillträdestillstånd för dessa platser, exempelvis ett skåp i ett omklädningsrum, kanske inte hinner hämtas in innan tillfället går förlorat. Åklagarmyndigheten anser därför att ett beslut om hemlig dataavläsning bör innebära ett generellt tillstånd till tillträde till vissa typer av platser som annars skyddas mot intrång, t.ex. fordon och allmänna förvaringsutrymmen. Den verkställande myndigheten borde därför, enligt Åklagarmyndigheten, ha ett generellt tillstånd att bereda sig tillträde till platser dit allmänheten har tillträde. Alternativt föreslår Åklagarmyndigheten att åklagaren ska kunna besluta om tillträdestillstånd till sådana platser när tillfälle uppkommer.

Regeringen anser, med hänsyn till det allvarliga integritetsintrånget, att kraven för tillträdestillstånd bör vara så högt ställda att det inte bör finnas möjlighet till sådana generella tillstånd som Åklagarmyndigheten föreslår. Däremot föreslår regeringen att åklagare ska ha rätt att under vissa förutsättningar fatta interimistiska beslut (se vidare nedan). Ett sådant beslut ska även kunna avse tillträdestillstånd. Om tillfälle till verkställighet plötsligt uppkommer kommer det alltså enligt förslaget att finnas möjlighet att snabbt få ett interimistiskt tillträdestillstånd.

Tillståndsprövning

Regeringen föreslår att frågor om hemlig dataavläsning ska prövas av domstol på ansökan av åklagare. En ansökan om hemlig dataavläsning vid särskild utlänningskontroll ska dock göras av Säkerhetspolisen eller Polismyndigheten. När en ansökan om hemlig dataavläsning har kommit in till domstolen

ska den så snart som möjligt utse ett offentligt ombud i ärendet och hålla ett sammanträde.

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 domstolens tillstånd i frågor om hemlig dataavläsning, föreslår regeringen att tillstånd ska få ges av åklagaren i avvaktan på domstolens beslut (interimistiskt tillstånd). Ett sådant tillstånd ska dock aldrig få avse rumsavlyssningsuppgifter eller fall som avser särskild utlänningskontroll. Om åklagaren har gett ett interimistiskt tillstånd ska åklagaren enligt förslaget utan dröjsmål skriftligt anmäla beslutet till domstol. I anmälan ska skälen för åtgärden anges. Domstolen ska därefter skyndsamt pröva ärendet. Om domstolen finner att det inte finns skäl för åtgärden ska den upphäva beslutet. Har åklagarens beslut verkställts innan domstolen gjort sin prövning ska domstolen pröva om det funnits skäl för åtgärden. Om den finner att det saknats sådana skäl, ska de uppgifter som lästs av eller tagits upp inte få användas i en brottsutredning till nackdel för den som har omfattats av åtgärden eller för någon annan som uppgifterna avser.

I ett tillstånd till hemlig dataavläsning ska det enligt regeringens förslag anges vilken tid tillståndet avser, vilket avläsningsbart informationssystem det avser, vilken typ av uppgift som får läsas av eller tas upp, villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan och, vid en åtgärd som gäller rumsavlyssningsuppgifter, vem som är skäligen misstänkt för brottet. Om ansökan gäller kameraövervaknings- eller rumsavlyssningsuppgifter ska det även anges vilken plats tillståndet gäller. Om tillståndet är förenat med ett tillträdestillstånd ska det anges i beslutet.

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

Beslut i frågor om hemlig dataavläsning ska få verkställas omedelbart. Om det inte längre finns skäl för ett tillstånd till hemlig dataavläsning, ska den som ansökt om åtgärden eller domstolen omedelbart häva beslutet.

Genomförande av hemlig dataavläsning

När tillstånd till hemlig dataavläsning har lämnats ska de verkställande myndigheterna få använda de tekniska hjälpmedel som behövs för avläsning och upptagning. Med tekniska hjälpmedel avses enligt propositionen både hårdvara och programvara. De tekniska hjälpmedlen kan vara fysiskt placerade i informationssystemet eller, när det är fråga om avläsning av uppgifter i informationssystem som t.ex. ett internetbaserat användarkonto, utgöras av datorer hos den brottsbekämpande myndigheten som utför avläsningen efter inloggning på kontot. Det kan också gälla t.ex. programvara eller funktioner som redan finns i informationssystemet, såsom gps, kamera eller mikrofon för att kunna läsa av eller ta upp plats-, kameraövervaknings- eller rumsavlyssningsuppgifter, eller programvara som den brottsbekämpande myndigheten

placerar i systemet för att hemlig dataavläsning ska kunna genomföras. Om det är nödvändigt ska systemskydd få brytas eller kringgås och tekniska sårbarheter utnyttjas.

Enligt regeringens förslag ska verkställighetstekniken vid hemlig dataavläsning inte ingå i domstolarnas tillståndsprövning. Regeringen konstaterar att reglerna kring de befintliga hemliga tvångsmedlen är utformade på så sätt att domstolen inte särskilt prövar vilka verkställighetsmetoder som ska användas trots att bestämmelserna är teknikneutralt utformade. Domstolen ska däremot pröva om de lagliga förutsättningarna för åtgärderna är uppfyllda, och vid verkställighet är de brottsbekämpande myndigheterna skyldiga att följa grundläggande principer om ändamål, behov och proportionalitet. Regeringen framhåller även att användningen av hemlig dataavläsning kommer att vara föremål för tillsyn. Det finns enligt regeringen inte heller något som hindrar att domstolen ställer frågor om verkställighetsteknik i syfte att kunna utforma eventuella villkor för att tillgodose intresset av att enskildas integritet inte kränks i onödan.

Rättssäkerhetsgarantier

Som redogjorts för ovan måste staten vid användning av hemliga tvångsmedel respektera vissa grundläggande mänskliga rättigheter. Regeringen skriver i propositionen att en viktig komponent i detta är att införa ett integritetsstärkande ramverk kring reglerna om hemliga tvångsmedel som reglerar överskottsinformation, granskning, bevarande och förstörande av upptagningar och uppteckningar samt underrättelse till enskild.

Regeringen anser även att Säkerhets- och integritetsskyddsnämnden bör utses att vara tillsynsmyndighet över användningen av hemlig dataavläsning. Enligt regeringen behövs det inte några författningsändringar för att nämnden ska ha befogenhet att utöva tillsyn eftersom det redan anges i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet att nämnden ska utöva tillsyn över hemlig tvångsmedelsanvändning, vilket begrepp kommer att omfatta hemlig dataavläsning. Däremot föreslår regeringen att det införs en bestämmelse om att den domstol som har beslutat i frågor om hemlig dataavläsning skyndsamt ska underrätta nämnden om beslutet.

Regeringen bedömer också att uppgifter om myndigheternas användning av hemlig dataavläsning bör redovisas i regeringens årliga skrivelse till riksdagen om användningen av hemliga tvångsmedel.

Internationella förhållanden

Regeringen framhåller att den brottslighet som enligt förslagen i propositionen ska omfattas av reglerna om hemlig dataavläsning inte sällan är av gränsöverskridande natur. Vissa brottsutredningar förutsätter mer eller mindre rättsligt samarbete med andra stater, t.ex. vid grov narkotikabrottslighet, människohandel och terroristbrottslighet. Även i utredningar av mer nationell brottslighet kan det enligt regeringen många gånger behövas bistånd utomlands,

t.ex. om bevisningen finns i en annan stat. I detta samarbete används hemliga tvångsmedel vid allvarlig brottslighet. Regeringen betonar att en given utgångspunkt är att all brottslighet – såväl nationell som internationell – ska bekämpas. De utredningsåtgärder som är möjliga att vidta i Sverige vid allvarlig brottslighet ska svenska åklagare kunna begära att de vidtas i en annan stat. På samma sätt ska utländska åklagare kunna begära att en motsvarande åtgärd vidtas i Sverige. Mot den bakgrunden föreslår regeringen att bestämmelser om hemlig dataavläsning ska införas i lagen (2000:562) om internationell rättslig hjälp i brottmål och i lagen (2017:1000) om en europeisk utredningsorder.

I propositionen anges vidare att Utredningen om hemlig dataavläsning har bedömt att det finns starka skäl att nyansera den svenska hållningen när det gäller vad territorialitetsprincipen vid exekutiv jurisdiktion innebär för elektroniskt lagrade uppgifter. Med exekutiv jurisdiktion avses rätten att verkställa åtgärder och förverkliga beslut som fattats inom ramen för lagstiftning och rättsskipning. När det gäller exekutiv jurisdiktion är utgångspunkten i folkrätten att det råder ett förbud för stater att vidta verkställighetsåtgärder på andra staters territorier, t.ex. att använda hemliga tvångsmedel där. Detta är ett utflöde av den s.k. territorialitetsprincipen. Elektroniska uppgifter kan finnas lagrade i flera stater samtidigt eller ständigt vara på väg mellan 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. Den svenska hållningen har hittills varit att om uppgifter lagras elektroniskt på annan plats än i Sverige eller om det är okänt var uppgifterna lagras så saknar svenska brottsbekämpande myndigheter jurisdiktion.

Regeringen konstaterar att frågan om hur man ska hantera åtkomst av uppgifter som lagras utanför den egna jurisdiktionen eller när det inte är känt var uppgifterna lagras har diskuterats inom EU. Anledningen till att frågan diskuteras internationellt är den ökade globaliseringen och att frågan inte anses kunna lösas av enskilda stater var för sig. Regeringen bedömer 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. Regeringen gör sammanfattningsvis bedömningen att frågan om den svenska tolkningen av territorialitetsprincipen vid exekutiv jurisdiktion i förhållande till elektroniskt lagrade uppgifter bör ändras inte kan tas om hand inom ramen för detta lagstiftningsprojekt.

Ikraftträdande

Regeringen föreslår att lagen om hemlig dataavläsning ska träda i kraft den 1 mars 2020 och tidsbegränsas att gälla t.o.m. den 28 februari 2025. Övriga lagändringar föreslås träda i kraft den 1 mars 2020. I propositionen anförs att de brottsbekämpande myndigheterna kommer att behöva viss tid att förbereda

sig för tillämpningen av hemlig dataavläsning. Det är dock enligt regeringen angeläget att reglerna träder i kraft så snart som möjligt.

Motionerna

Avslag på propositionen

I kommittémotion 2019/20:3451 av Linda Westerlund Snecker m.fl. (V) föreslår motionärerna att riksdagen ska avslå regeringens proposition. Motionärerna anser att nyttan av hemlig dataavläsning inte är tillräckligt stor för att motivera ett sådant ingrepp i den personliga integriteten som tvångsmedlet innebär.

Platskrav

Adam Marttinen m.fl. (SD) anser i kommittémotion 2019/20:3475 yrkande 1 att det finns starka skäl att på nytt utreda frågan om platskrav vid avläsning eller upptagning av kameraövervaknings- och rumsavlyssningsuppgifter. Motionärerna hänvisar bl.a. till att regeringens förslag inte tillräckligt beaktar de förutsättningar som det nya tvångsmedlet innebär. Platskravet medför t.ex. vissa problem när hemlig dataavläsning sker genom övervakning eller avlyssning av en mobiltelefon, eftersom den är i rörelse.

Ingemar Kihlström m.fl. (KD) anför i kommittémotion 2019/20:3471 yrkande 2 att det platskrav som regeringen föreslår vid avläsning eller upptagning av kameraövervaknings- och rumsavlyssningsuppgifter kommer att komplicera användningen av hemlig dataavläsning för de rättsvårdande myndigheterna. Motionärerna anser därför att tvångsmedlen bör knytas till en person i stället för en plats.

Hemlig dataavläsning i inhämtningslagsfallen

I kommittémotion 2019/20:3471 av Ingemar Kihlström m.fl. (KD) yrkande 1 föreslås att hemlig dataavläsning ska få beviljas om åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka sådan brottslig verksamhet som anges i inhämtningslagen. Enligt motionärerna behövs det inte ett skarpare krav för hemlig dataavläsning än vad som föreskrivs i den lagen.

Adam Marttinen m.fl. (SD) anser i kommittémotion 2019/20:3475 yrkande 3 att det bör utredas om åtgärden bör vara av synnerlig vikt eller av särskild vikt för att hemlig dataavläsning ska få beviljas i inhämtningslagsfallen.

Förbud mot hemlig dataavläsning i vissa fall

Adam Marttinen m.fl. (SD) föreslår i kommittémotion 2019/20:3475 yrkande 2 att förbudet mot hemlig dataavläsning som avser ett avläsningsbart informationssystem som används av präster inom trossamfund eller av dem som har motsvarande ställning inom sådana samfund i verksamhet för bikt

eller enskild självavård ska tas bort. Det finns enligt motionärerna skäl att anta att det i vissa fall kan finnas behov av hemliga tvångsmedel på sådana platser som omfattas av förbudet.

Beslut om tillträdestillstånd

Ingemar Kihlström m.fl. (KD) anser i kommittémotion 2019/20:3471 yrkande 3 att regeringen bör återkomma till riksdagen med ett förslag som tar hänsyn till de invändningar som bl.a. Åklagarmyndigheten har i fråga om beslut om tillträdestillstånd. Åklagarmyndigheten menar exempelvis att ett beslut om hemlig dataavläsning ska innebära ett generellt tillträde till vissa typer av platser som annars skyddas mot intrång, t.ex. fordon och allmänna förvaringsutrymmen. Alternativt skulle åklagaren kunna fatta beslutet.

Territorialitetsprincipen

Adam Marttinen m.fl. (SD) anser i kommittémotion 2019/20:3475 yrkande 4 att det genom lagstiftning bör klargöras hur territorialitetsprincipen ska tillämpas vid exekutiv jurisdiktion i förhållande till elektroniskt lagrade uppgifter.

Konstitutionsutskottets yttrande

Konstitutionsutskottet har yttrat sig över propositionen. Yttrandet har begränsats till att avse frågor om skyddet för den personliga integriteten. I yttrandet anför konstitutionsutskottet bl.a. följande:

> Utskottet vill inledningsvis betona vikten av att den enskildes personliga integritet värnas. Lagförslag bör föregås av en noggrann analys av förslagets konsekvenser för den personliga integriteten, och en avvägning måste göras mellan integritetsskyddsintresset och det intresse som motiverar lagförslaget. En inskränkning av skyddet för den personliga integriteten får inte gå längre än vad som är nödvändigt med hänsyn till det ändamål som föranlett den.
>
> Syftet med regeringens förslag om hemlig dataavläsning är att ge de brottsbekämpande myndigheterna bättre och effektivare möjligheter att förhindra och utreda allvarlig brottslighet. Detta ska ske genom att berörda myndigheter får ta del av information som i dag inte är tillgänglig. Hemlig dataavläsning innebär att de brottsbekämpande myndigheterna får möjlighet att i hemlighet samla in uppgifter om och kartlägga enskilda. Förslaget innebär därmed enligt utskottets mening ett väsentligt intrång i den enskildes personliga integritet. För att förslaget ska kunna godtas krävs att det finns ett så stort behov av hemlig dataavläsning att fördelarna med tvångsmedlet är proportionerliga i förhållande till detta intrång.
>
> Utskottet konstaterar att regeringen i propositionen utförligt redogör för dels sina överväganden när det gäller förslagets konsekvenser för den personliga integriteten, dels den avvägning som har gjorts mellan integritetsskyddsintresset och intresset av att förbättra möjligheterna att bekämpa och lagföra allvarliga brott med hjälp av hemlig dataavläsning. Härutöver lämnas i propositionen ett antal förslag som är ägnade att så långt som möjligt stärka den enskildes rättssäkerhet och integritetsskydd, såsom att tillstånd till hemlig dataavläsning ska beslutas av domstol, att det

ska råda förbud mot hemlig dataavläsning på vissa platser och för vissa yrkeskategorier samt att Säkerhets- och integritetsskyddsnämndens tillsyn ska omfatta även hemlig dataavläsning. Utskottet noterar också att hemlig dataavläsning enligt förslaget ska införas genom en särskild, tidsbegränsad lag.

I sammanhanget vill utskottet, i likhet med Lagrådet, framhålla vikten av att Säkerhets- och integritetsskyddsnämnden ges förutsättningar för en effektiv tillsyn och av att det görs en ingående utvärdering av behovet, nyttan och proportionaliteten av hemlig dataavläsning innan det fattas beslut om huruvida den tillfälliga lagstiftningen ska förlängas eller permanentas. Härutöver vill utskottet understryka vikten av de bevis- och proportionalitetskrav som syftar till att begränsa intrång i den personliga integriteten för andra personer än den som är misstänkt för allvarlig brottslighet.

Utifrån de utgångspunkter som konstitutionsutskottet har att beakta har utskottet sammantaget inget att invända mot att propositionen bifalls och att motion 2019/20:3451 (V) avslås.

Utskottets ställningstagande

För en effektiv brottsbekämpning är det i vissa fall nödvändigt att myndigheterna har tillgång till hemliga tvångsmedel. Användningen av hemliga tvångsmedel medför emellertid inskränkningar i grundläggande rättigheter som skyddas av regeringsformen och Europakonventionen. Införandet av nya tvångsmedel bör därför föregås av noggranna överväganden där brottsbekämpningens effektivitet vägs mot den personliga integriteten.

Regeringens förslag innebär att de brottsbekämpande myndigheterna får möjlighet att vid misstanke om allvarlig brottslighet använda ett nytt hemligt tvångsmedel – hemlig dataavläsning. Utskottet konstaterar att regeringen har gjort en utförlig analys av behovet av åtgärden, åtgärdens förväntade effektivitet och nytta samt de risker för den personliga integriteteten som förslaget kan förväntas medföra.

Utskottet delar regeringens uppfattning att det finns ett behov av att införa hemlig dataavläsning som ett nytt hemligt tvångsmedel och att åtgärden kan förväntas leda till bättre och effektivare möjligheter att ta del av information som i dagsläget inte är tillgänglig. Vidare delar utskottet regeringens uppfattning att de positiva effekter som förslaget får i form av att försvåra de kriminellas verksamhet klart överväger de negativa effekter som det får i form av integritetsinskränkningar mot den som blir föremål för åtgärden. Mot denna bakgrund, och med beaktande av att hemlig dataavläsning alltid ska prövas av domstol som ska underrätta Säkerhets- och integritetsskyddsnämnden om beslutet, anser utskottet att den föreslagna lagstiftningen är väl avvägd. Konstitutionsutskottet, som har yttrat sig över regeringens lagförslag i fråga om skyddet för den personliga integriteten, har inte heller haft något att invända mot att propositionen bifalls.

Sammantaget anser utskottet att riksdagen bör bifalla regeringens lagförslag och avslå motion 2019/20:3451 (V).

När det gäller kravet på en bestämd plats vid avläsning eller upptagning av kameraövervaknings- eller rumsavlyssningsuppgifter konstaterar utskottet att regeringen i propositionen framhåller att platskravet är viktigt för att kunna bedöma det förväntade integritetsintrånget. Utskottet gör ingen annan bedömning och är därför inte berett att ställa sig bakom ett sådant tillkännagivande som föreslås i motionerna 2019/20:3471 (KD) yrkande 2 och 2019/20:3475 (SD) yrkande 1. Motionsyrkandena avstyrks.

Utskottet delar vidare regeringens uppfattning att det vid hemlig dataavläsning i inhämtningslagsfallen bör krävas att åtgärden är av synnerlig vikt för att förebygga, förhindra eller upptäcka den brottsliga verksamheten. Utskottet avstyrker därför motionerna 2019/20:3471 (KD) yrkande 1 och 2019/20:3475 (SD) yrkande 3.

Även i frågan om förbud mot hemlig dataavläsning som avser vissa avläsningsbara informationssystem och vissa platser anser utskottet att regeringens förslag är väl avvägt. Utskottet är därför inte berett att ställa sig bakom ett sådant tillkännagivande om att ta bort vissa delar av detta förbud som föreslås i motion 2019/20:3475 (SD) yrkande 2. Motionsyrkandet avstyrks.

När det gäller tillträdestillstånd noterar utskottet att åklagare enligt regeringens förslag ska ha rätt att under vissa förutsättningar fatta interimistiska beslut. Om tillfälle till verkställighet plötsligt uppkommer kommer det alltså att finnas möjlighet att snabbt få ett interimistiskt tillträdestillstånd. Mot den bakgrunden ställer sig utskottet även i denna del bakom förslagen i propositionen. Utskottet avstyrker därmed motion 2019/20:3471 (KD) yrkande 3.

Utskottet konstaterar slutligen att frågan om hur territorialitetsprincipen bör tolkas vid exekutiv jurisdiktion har uppmärksammats av regeringen och att det förs internationella diskussioner. Det saknas därför anledning för utskottet att nu ta något initiativ i frågan. Utskottet avstyrker därmed även motion 2019/20:3475 (SD) yrkande 4.

Ikraftträdande m.m.

I propositionen, som överlämnades till riksdagen den 11 december 2019, föreslår regeringen att den nya lagen och lagändringarna ska träda i kraft den 1 mars 2020. Med hänsyn till den korta tid som återstår till dess föreslår utskottet att lagarna i stället ska träda i kraft den 1 april 2020. Till följd därav föreslår utskottet att den nya lagen om hemlig dataavläsning ska upphöra att gälla vid utgången av mars 2025.

Reservationer

1. Hemlig dataavläsning, punkt 1 (V)

av Linda Westerlund Snecker (V).

Förslag till riksdagsbeslut

Jag anser att förslaget till riksdagsbeslut under punkt 1 borde ha följande lydelse:

Riksdagen avslår regeringens förslag.

Därmed bifaller riksdagen motion
2019/20:3451 av Linda Westerlund Snecker m.fl. (V) och
avslår proposition 2019/20:64 punkterna 1–6.

Ställningstagande

Jag ser med stor oro på den utveckling som skett sedan i början av 2000-talet och som i dag lett till att vi börjar närma oss ett övervakningssamhälle. Frågor om personlig integritet och mänskliga rättigheter får gång på gång stå tillbaka. Varje inskränkning har motiverats utifrån skenbart goda syften som effektivare brottsbekämpning och ett generellt ökat skydd för invånarna. Sammantaget framstår dock helheten av snart två decenniers skärpta lagar när det gäller t.ex. kamerabevakning, hemliga tvångsmedel, signalspaning, utlänningskontroll och åtgärder i syfte att hindra terrorism som illavarslande. Varje inskränkning som godtas tenderar att bana väg för ännu fler och mer ingripande skärpningar. Argument i stil med att den som har ett rent samvete inte har något att frukta riskerar att bli urvattnade floskler ju fler inskränkningar av den personliga integriteten som accepteras. Konsekvenserna för samhällsklimatet och demokratin på lång sikt är svåra att överblicka.

Enligt min mening måste samtliga redan genomförda, föreslagna och kommande åtgärder som syftar till att bekämpa terrorism, våldsbejakande extremism och annan grov kriminalitet bedömas som en helhet. Frågan är om dessa åtgärder sammantaget är proportionella i förhållande till syftet och om de är effektiva för att uppnå målet.

Jag gör, i motsats till regeringen, bedömningen att nyttan av hemlig dataavläsning inte är tillräckligt stor för att motivera ett sådant ingrepp i den personliga integriteten som tvångsmedlet innebär. Nedan redovisas några av de viktigaste skälen till det.

Det är tveksamt om hemlig dataavläsning kommer att vara en tillräckligt effektiv metod. Metoden är dyr och innebär i praktiken att staten kommer att installera ett virusliknande program som placeras genom trojaner i människors telefoner och datorer. Tanken är att hemlig dataavläsning ska ge en möjlighet att läsa av information innan den krypteras. Vissa appar kommer dock sannolikt att omöjliggöra detta. Vidare är tillfället då det är möjligt att

installera en trojan i ett kommunikationsmedel näst intill obefintligt. När trojanen väl är placerad är möjligheten att komma åt information i olika appar eller mejl som lagras på servrar eller i ett molnbaserat system högst begränsad. Att läsa av krypterad information kommer även i fortsättningen att vara en stor utmaning eftersom krypteringen sker via nycklar. Regeringen har inte aviserat att staten ska framställa en huvudnyckel för kryptering, vilket skulle vara mycket oroande eftersom mycket av privatpersoners kommunikation i dag sker krypterat. Vidare byter kriminella nätverk självfallet mobiltelefoner ofta, installerar mjukvara för kryptering eller använder olika former av mobiltelefoner med förinställda krypteringsverktyg, allt för att kunna kommunicera utan myndigheternas vetskap. Det finns inget som tyder på att de kriminella nätverken kommer att sluta anpassa sina kommunikationsmetoder efter rådande lagstiftning.

Regeringens förslag innebär att själva verkställighetstekniken inte ska ingå i domstolsprövningen vid tillståndsgivning för hemlig dataavläsning. Detta är en brist, vilket även Säkerhets- och integritetsskyddsnämnden (SIN) påtalar i sitt remissvar. SIN menar att de verkställande myndigheterna genom förslaget får stor frihet att själva avgöra vilka tekniska hjälpmedel som ska användas vid verkställigheten. Detta gör att det är oklart hur rättssäkerheten för enskilda ska garanteras. SIN anser att domstolen måste ha möjlighet att ange villkor för att enskildas personliga integritet inte ska kränkas i onödan. Därför bör verkställighetstekniken ingå i domstolsprövningen. Även Datainspektionen lyfter i sitt remissvar fram att domstolen måste veta vilka tekniska åtgärder som ska genomföras för att kunna göra en fullständig nödvändighets- och proportionalitetsbedömning. Att SIN föreslås utöva tillsyn över de brottsbekämpande myndigheternas användning av hemlig dataavläsning räcker enligt min mening inte för att garantera rättssäkerheten för enskilda vid verkställighet.

Ett stort problem med förslaget är slutligen att regeringen gör bedömningen att utgångspunkten för hemlig dataavläsning bör vara de krav som gäller för det bakomliggande hemliga tvångsmedlet enligt redan gällande lag. I stället för att prova förutsättningarna att använda hemlig dataavläsning för varje enskilt brott för sig utifrån rättsliga principer om proportionalitet, ändamålsenlighet och effektivitet gör regeringen bedömningen att hemlig dataavläsning i huvudsak bara är en ny metod för att komma åt information som det redan är tillåtet att samla in med gällande tvångsmedelslagstiftning. Jag anser att hemlig dataavläsning är så pass integritetskränkande att detta synsätt inte låter sig förenas med gällande rättsliga principer. Enligt min mening skulle det möjligen vara rimligt att använda hemlig dataavläsning vid vissa av de allra grövsta brotten, men eftersom varken utredningen eller regeringen har gjort någon prövning av behovet vid varje brott för sig kan jag inte avgöra om så är fallet. Det är dock positivt att den föreslagna lagen är tidsbegränsad, och jag förväntar mig en noggrann utredning av nyttan, behovet och proportionaliteten i samband med den fortsatta hanteringen.

Jag anser att riksdagen bör avslå regeringens proposition.

2. Platskrav, punkt 2 (M, SD, KD)

av Ingemar Kihlström (KD), Johan Forssell (M), Magdalena Schröder (M), Adam Marttinen (SD), Ellen Juntti (M), Katja Nyberg (SD), Bo Broman (SD) och Mattias Ingeson (KD).

Förslag till riksdagsbeslut

Vi anser att förslaget till riksdagsbeslut under punkt 2 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motionerna
2019/20:3471 av Ingemar Kihlström m.fl. (KD) yrkande 2 och
2019/20:3475 av Adam Marttinen m.fl. (SD) yrkande 1.

Ställningstagande

Det platskrav som regeringen föreslår vid avläsning eller upptagning av kameraövervaknings- och rumsavlyssningsuppgifter kommer att komplicera användningen av hemlig dataavläsning för de rättsvårdande myndigheterna eftersom förslaget inte tillräckligt beaktar de förutsättningar som det nya tvångsmedlet innebär. Platskravet medför t.ex. vissa problem när hemlig dataavläsning sker genom övervakning eller avlyssning av en mobiltelefon, eftersom den är i rörelse. Kriminella nätverk är ofta mycket medvetna om vilka begränsningar som finns för polisens tvångsmedel och utnyttjar dessa begränsningar maximalt. Om de t.ex. byter möteslokal i sista sekund blir det mycket svårt för de rättsvårdande myndigheterna att få till stånd en hemlig kameraövervakning. Sådana problem kan undvikas om tvångsmedlet knyts till en person i stället för en plats.

Med hänsyn till teknikens utveckling och de svårigheter med tillämpningen som de brottsbekämpande myndigheterna påtalar i sina remissvar bör regeringen på nytt utreda frågan om platskrav vid avläsning eller upptagning av kameraövervaknings- och rumsavlyssningsuppgifter.

3. Hemlig dataavläsning i inhämtningslagsfallen, punkt 3 (M, SD, KD)

av Ingemar Kihlström (KD), Johan Forssell (M), Magdalena Schröder (M), Adam Marttinen (SD), Ellen Juntti (M), Katja Nyberg (SD), Bo Broman (SD) och Mattias Ingeson (KD).

Förslag till riksdagsbeslut

Vi anser att förslaget till riksdagsbeslut under punkt 3 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motionerna
2019/20:3471 av Ingemar Kihlström m.fl. (KD) yrkande 1 och
2019/20:3475 av Adam Marttinen m.fl. (SD) yrkande 3.

Ställningstagande

Polismyndigheten och Säkerhetspolisen förordar att hemlig dataavläsning ska få beviljas om åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka sådan brottslig verksamhet som anges i inhämtningslagen. Regeringen gör i stället bedömningen att hemlig dataavläsning endast ska få beviljas om åtgärden är av synnerlig vikt, vilket är ett högre krav än inhämtningslagen ställer upp. Hemlig dataavläsning är en ny metod för att verkställa de hemliga tvångsmedel som det redan i dag finns lagstöd för att besluta om. Därför behövs det inte ett skarpare krav för hemlig dataavläsning än vad som föreskrivs i inhämtningslagen.

Regeringen bör återkomma till riksdagen med ett lagförslag som innebär att hemlig dataavläsning får beviljas om åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka sådan brottslig verksamhet som anges i inhämtningslagen.

4. Förbud mot hemlig dataavläsning i vissa fall, punkt 4 (SD)

av Adam Marttinen (SD), Katja Nyberg (SD) och Bo Broman (SD).

Förslag till riksdagsbeslut

Vi anser att förslaget till riksdagsbeslut under punkt 4 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2019/20:3475 av Adam Marttinen m.fl. (SD) yrkande 2.

Ställningstagande

Regeringen föreslår i propositionen att vissa platser av sin natur bör föranleda ett förbud mot hemlig dataavläsning för informationssystem som stadigvarande används eller är särskilt avsedda att användas där. Säkerhetspolisen har återkommande noterat hot från den våldsbejakande islamistiska miljön, vilket nyligen visade sig vid tillämpningen av lagen om särskild utlänningskontroll gällande flera imamer. Det finns således skäl att anta att det i vissa fall kan finnas behov av hemliga tvångsmedel på sådana platser som omfattas av förbudet. Detta får anses inskränka den personliga integriteten i större utsträckning än på många andra platser men kan i vissa fall vara motiverat utifrån den särskilda hotbilden i det enskilda fallet.

I den mån det kan motiveras av proportionalitetsprincipen bör således förbudet mot hemlig dataavläsning som avser ett avläsningsbart informationssystem som används av präster inom trossamfund eller av dem som har motsvarande ställning inom sådana samfund, i verksamhet för bikt eller enskild själavård tas bort.

5. Beslut om tillträdestillstånd, punkt 5 (KD)

av Ingemar Kihlström (KD) och Mattias Ingeson (KD).

Förslag till riksdagsbeslut

Vi anser att förslaget till riksdagsbeslut under punkt 5 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2019/20:3471 av Ingemar Kihlström m.fl. (KD) yrkande 3.

Ställningstagande

Flera remissinstanser påpekar problemet med att få ett tillträdestillstånd godkänt av domstol i tid i de fall där en misstänkt lämnar ifrån sig exempelvis en mobiltelefon under en begränsad tid eller på en för allmänheten tillgänglig plats, t.ex. ett omklädningsrum. Det kan vara kort om tid för att handla, och tillfället kan därför bli omöjligt att utnyttja om tillstånd ska ges av en domstol. Åklagarmyndigheten menar exempelvis att ett beslut om hemlig dataavläsning ska innebära ett generellt tillträde till vissa typer av platser som annars skyddas mot intrång, t.ex. fordon och allmänna förvaringsutrymmen. Alternativt skulle åklagaren kunna besluta om tillträdestillstånd. Säkerhetspolisen är vidare orolig för att tillträdestillståndet kan få en för snäv tolkning.

Regeringen bör återkomma till riksdagen med ett lagförslag som tar hänsyn till de invändningar som Åklagarmyndigheten, Säkerhetspolisen och Polismyndigheten har i fråga om tillträdestillstånd.

6. Territorialitetsprincipen, punkt 6 (SD)

av Adam Marttinen (SD), Katja Nyberg (SD) och Bo Broman (SD).

Förslag till riksdagsbeslut

Vi anser att förslaget till riksdagsbeslut under punkt 6 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2019/20:3475 av Adam Marttinen m.fl. (SD) yrkande 4.

Ställningstagande

En viss nyansering av tidigare ställningstaganden är nödvändig när tekniken utvecklas, och när det gäller exekutiv jurisdiktion krävs förändringar om det föreslagna hemliga tvångsmedlet ska bli verkningsfullt. Det finns därför skäl att genom lagstiftning klargöra hur territorialitetsprincipen ska tillämpas vid exekutiv jurisdiktion i förhållande till elektroniskt lagrade uppgifter. Den passivitet som uttrycks i propositionen bör inte bli normativ.

BILAGA 1

Förteckning över behandlade förslag

Propositionen

Proposition 2019/20:64 Hemlig dataavläsning:

1. Riksdagen antar regeringens förslag till lag om hemlig dataavläsning.
2. Riksdagen antar regeringens förslag till lag om ändring i lagen (1988:97) om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m.
3. Riksdagen antar regeringens förslag till lag om ändring i lagen (1991:572) om särskild utlänningskontroll.
4. Riksdagen antar regeringens förslag till lag om ändring i lagen (2000:562) om internationell rättslig hjälp i brottmål.
5. Riksdagen antar regeringens förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400).
6. Riksdagen antar regeringens förslag till lag om ändring i lagen (2017:1000) om en europeisk utredningsorder.

Följdmotionerna

2019/20:3451 av Linda Westerlund Snecker m.fl. (V):

Riksdagen avslår proposition 2019/20:64.

2019/20:3471 av Ingemar Kihlström m.fl. (KD):

1. Riksdagen ställer sig bakom det som anförs i motionen om att hemlig dataavläsning ska beviljas om åtgärden är av särskild vikt och tillkännager detta för regeringen.
2. Riksdagen ställer sig bakom det som anförs i motionen om platskrav och tillkännager detta för regeringen.
3. Riksdagen ställer sig bakom det som anförs i motionen om tillträdestillstånd och tillkännager detta för regeringen.

2019/20:3475 av Adam Marttinen m.fl. (SD):

1. Riksdagen ställer sig bakom det som anförs i motionen om platskrav och tillkännager detta för regeringen.
2. Riksdagen ställer sig bakom det som anförs i motionen om undantag för vissa platser och tillkännager detta för regeringen.

3. Riksdagen ställer sig bakom det som anförs i motionen om hemlig dataavläsning i inhämtningslagsfallen och tillkännager detta för regeringen.
4. Riksdagen ställer sig bakom det som anförs i motionen om territorialitetsprincipen och tillkännager detta för regeringen.

BILAGA 2

Regeringens lagförslag

1 Förslag till lag om hemlig dataavläsning

Härigenom föreskrivs följande.

Ord och uttryck i lagen

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.

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 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,

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

2 § Tillstånd till hemlig dataavläsning får beviljas för att läsa av eller ta upp

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.

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.

Grundläggande förutsättning för hemlig dataavläsning

3 § Ett tillstånd till hemlig dataavläsning får beviljas endast om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktas mot eller för något annat motstående intresse.

Hemlig dataavläsning under en förundersökning

4 § Ett tillstånd till hemlig dataavläsning får, om åtgärden är av synnerlig vikt för utredningen och inte annat anges i 6 § första stycket, beviljas vid en förundersökning om

1. brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år,
2. brott som avses i 27 kap. 2 § andra stycket 2–7 rättegångsbalken,
3. försök, förberedelse eller stämpling till brott som avses i 1 eller 2, om en sådan gärning är belagd med straff, eller
4. annat brott om det med hänsyn till omständigheterna kan antas att brottets straffvärde överstiger fängelse i två år.

Ett tillstånd enligt första stycket får, om inte annat anges i 5 §, endast avse ett avläsningsbart informationssystem som används, eller som det finns särskild anledning att anta har använts eller kommer att användas, av någon som är skäligen misstänkt för brottet.

Ett tillstånd enligt första stycket som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter får, om inte annat anges i 5 §, 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 första stycket 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.

5 § Ett tillstånd till hemlig dataavläsning enligt 4 § som gäller kommunikationsövervaknings- eller platsuppgifter får även beviljas för att utreda vem som skäligen kan misstänkas för ett brott som avses i 4 §. Avläsning eller upptagning av kommunikationsövervakningsuppgifter får då endast avse förfluten tid.

Hemlig dataavläsning enligt första stycket får endast avse 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.

6 § Ett tillstånd till hemlig dataavläsning enligt 4 § som gäller rumsavlyssningsuppgifter får endast beviljas vid en förundersökning om brott som avses i 27 kap. 20 d § andra stycket rättegångsbalken.

Hemlig dataavläsning enligt första stycket får användas endast på en plats där det finns särskild anledning att anta att den misstänkte kommer att uppehålla sig. Om platsen är någon annan stadigvarande bostad än den misstänktes, får tillstånd till hemlig dataavläsning beviljas endast om det finns synnerlig anledning att anta att den misstänkte kommer att uppehålla sig där.

Hemlig dataavläsning enligt första stycket får aldrig användas på en plats dit tillträdestillstånd enligt 13 § inte får beviljas.

Hemlig dataavläsning utanför en förundersökning

Förhindrande av vissa särskilt allvarliga brott

7 § Ett tillstånd till hemlig dataavläsning får beviljas om

1. det med hänsyn till omständigheterna finns en påtaglig risk för att en person kommer att utöva brottslig verksamhet som innefattar brott som anges i 1 § lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott, eller

2. det finns en påtaglig risk för att sådan brottslig verksamhet kommer att utövas inom en organisation eller grupp och det kan befaras att en person som tillhör eller verkar för organisationen eller gruppen medvetet kommer att främja denna verksamhet.

Ett tillstånd enligt första stycket får beviljas endast om åtgärden är av synnerlig vikt för att förhindra sådan brottslig verksamhet som anges i det stycket.

Hemlig dataavläsning som gäller kameraövervakningsuppgifter får användas endast på en plats där den person som anges i första stycket kan antas komma att uppehålla sig. En sådan plats får dock inte vara någons stadigvarande bostad.

Ett tillstånd får inte avse rumsavlyssningsuppgifter.

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.

Särskild utlänningskontroll

9 § 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

1. ett utvisningsbeslut enligt 1 § 2 lagen (1991:572) om särskild utlänningskontroll, eller

2. ett avvisnings- eller utvisningsbeslut enligt 8 eller 8 a kap. utlänningslagen (2005:716) eller motsvarande äldre bestämmelser och det finns sådana omständigheter i fråga om utlänningen som avses i 1 § 2 lagen om särskild utlänningskontroll.

Ett tillstånd till hemlig dataavläsning som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- 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.

Tillståndet får beviljas endast om Migrationsverket, regeringen eller en domstol har beslutat att 19–22 §§ lagen om särskild utlänningskontroll samt denna lag ska tillämpas på utlänningen. Det förfarande och de förutsättningar som gäller för ett beslut om att 19–22 §§ lagen om särskild utlänningskontroll 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 utreda om utlänningen eller en organisation eller grupp som han eller hon tillhör eller verkar för planlägger eller förbereder terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott.

Ett tillstånd får inte avse kameraövervaknings- eller rumsavlyssningsuppgifter.

Förebyggande, förhindrande och upptäckande av brottslig verksamhet

10 § Ett tillstånd till hemlig dataavläsning som gäller kommunikationsövervaknings- eller platsuppgifter får beviljas om åtgärden är av synnerlig vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott som anges i 2 § lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

Vid hemlig dataavläsning enligt första stycket får meddelanden inte hindras att nå fram enligt 2 § andra stycket.

Ett tillstånd till hemlig dataavläsning som gäller kommunikationsövervakningsuppgifter får endast avse uppgifter i förfluten tid.

Förbud mot hemlig dataavläsning

11 § Ett tillstånd till hemlig dataavläsning får inte avse ett avläsningsbart informationssystem som stadigvarande används eller är särskilt avsett att användas

1. i verksamhet där tystnadsplikt gäller enligt 3 kap. 3 § tryckfrihetsförordningen eller 2 kap. 3 § yttrandefrihetsgrundlagen,
2. i verksamhet som bedrivs av advokater, läkare, tandläkare, barnmorskor, sjuksköterskor, psykologer, psykoterapeuter eller familjerådgivare enligt socialtjänstlagen (2001:453), eller
3. av präster inom trossamfund eller av dem som har motsvarande ställning inom sådana samfund, i verksamhet för bikt eller enskild själavård.

Tillträdestillstånd

12 § Vid hemlig dataavläsning får den verkställande myndigheten, efter särskilt tillstånd, i hemlighet skaffa sig tillträde till och installera tekniska hjälpmedel på en plats som annars skyddas mot intrång. Ett sådant tillstånd får endast avse en plats där det finns särskild anledning att anta att det avläsningsbara informationssystemet finns tillgängligt. Om platsen är en bostad som stadigvarande används av någon annan än den misstänkte eller en sådan person som anges i 7 § första stycket eller 9 § första stycket, får tillstånd beviljas endast om det finns synnerlig anledning att anta att informationssystemet finns där.

13 § Ett tillträdestillstånd enligt 12 § får inte avse en plats som stadigvarande används eller är särskilt avsedd att användas

1. för verksamhet där tystnadsplikt gäller enligt 3 kap. 3 § tryckfrihetsförordningen eller 2 kap. 3 § yttrandefrihetsgrundlagen,
2. för verksamhet som bedrivs av advokater, läkare, tandläkare, barnmorskor, sjuksköterskor, psykologer, psykoterapeuter eller familjerådgivare enligt socialtjänstlagen (2001:453), eller
3. av präster inom trossamfund eller av dem som har motsvarande ställning inom sådana samfund, för bikt eller enskild själavård.

Tillståndsprövning

14 § Frågor om hemlig dataavläsning prövas av rätten på ansökan av åklagare. En ansökan om hemlig dataavläsning enligt 9 § ska dock göras av Säkerhetspolisen eller Polismyndigheten.

15 § Frågor om hemlig dataavläsning under en förundersökning prövas av den domstol som anges i 19 kap. rättegångsbalken. Om förundersökningen avser brott som anges i 27 kap. 2 § andra stycket 2–8 rättegångsbalken får frågan även prövas av Stockholms tingsrätt.

Frågor om hemlig dataavläsning enligt 7–10 §§ prövas av Stockholms tingsrätt.

16 § När en ansökan eller anmälan om hemlig dataavläsning har kommit in till rätten, ska rätten så snart som möjligt utse ett offentligt ombud i ärendet och hålla ett sammanträde. Vid sammanträdet ska den som gjort ansökan eller anmälan och det offentliga ombudet närvara.

För offentliga ombud i ärenden om hemlig dataavläsning gäller 27 kap. 26 och 27 §§, 28 § andra stycket samt 29 och 30 §§ rättegångsbalken.

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 tillstånd i frågor om hemlig dataavläsning, får tillstånd ges av åklagaren i avvaktan på rättens beslut. Ett sådant tillstånd får dock aldrig avse hemlig dataavläsning som gäller rumsavlyssningsuppgifter eller hemlig dataavläsning vid särskild utlänningskontroll enligt 9 §.

Om åklagaren har gett ett tillstånd enligt första stycket, ska åklagaren utan dröjsmål 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.

18 § I ett tillstånd till hemlig dataavläsning ska följande anges:

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, vid åtgärd som gäller rumsavlyssningsuppgifter.

Om tillståndet avser en plats enligt 4 § fjärde stycket eller 6 § andra stycket ska även platsen anges i tillståndet. Om tillståndet är förenat med ett tillträdestillstånd enligt 12 §, 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.

19 § På förfarandet enligt denna lag tillämpas 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 denna lag. Handläggningen ska ske skyndsamt.

20 § Ett beslut i frågor om hemlig dataavläsning får verkställas omedelbart.

Om det inte längre finns skäl för ett tillstånd till hemlig dataavläsning, ska den som ansökt om åtgärden eller rätten omedelbart upphäva beslutet.

21 § När rätten har beslutat i frågor om hemlig dataavläsning ska den skyndsamt underrätta Säkerhets- och integritetsskyddsnämnden om beslutet.

Genomförande av hemlig dataavläsning

Tillåtna tekniska metoder

22 § När ett tillstånd till hemlig dataavläsning har beviljats får de tekniska hjälpmedel som behövs för avläsningen och upptagningen användas. Om det är nödvändigt får systemskydd brytas eller kringgås och tekniska sårbarheter utnyttjas.

Teknikanpassning och otillåten tilläggsinformation

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 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.

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.

Skyldighet att medverka

24 § Den som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 § lagen (2003:389) om elektronisk kommunikation är på begäran

av den verkställande myndigheten skyldig att medverka i samband med verkställighet av hemlig dataavläsning.

Den som medverkar enligt första stycket har rätt till ersättning för kostnader som uppstår vid sådan medverkan. Ersättningen ska betalas av den verkställande myndigheten.

Aktsamhetskrav

25 § När ett beslut om hemlig dataavläsning verkställs får någon olägenhet eller skada inte förorsakas utöver vad som är absolut nödvändigt. Informationssäkerheten i andra avläsningsbara informationssystem än det tillståndet avser får dock inte åsidosättas, försämras eller skadas till följd av verkställigheten.

När verkställigheten avslutas ska den verkställande myndigheten vidta de åtgärder som behövs för att informationssäkerheten i det avläsningsbara informationssystem som tillståndet avser ska hålla minst samma nivå som vid verkställighetens början.

Ett tekniskt hjälpmedel som har använts ska tas bort, avinstalleras eller annars göras obrukbart så snart det kan ske efter att tiden för tillståndet har gått ut eller tillståndet upphävts.

26 § Den verkställande myndigheten ska utse en eller flera personer som får verkställa hemlig dataavläsning. Sådana personer ska vara särskilt lämpade för uppdraget och ha särskilda kunskaper om informationssäkerhet samt den särskilda kompetens, utbildning och erfarenhet som i övrigt är nödvändig.

Förbud att läsa av eller ta upp vissa uppgifter

27 § Hemlig dataavläsning enligt 2 § första stycket 6 eller 7 får inte avse uppgifter som enligt 27 kap. 2 § första stycket 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 styckena ska verkställigheten omedelbart avbrytas och upptagningar och uppteckningar omedelbart förstöras i de delar som de omfattas av förbudet.

Överskottsinformation, granskning och underrättelse till enskilda

Förundersökning

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.

Förhindrande av vissa särskilt allvarliga brott

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.

Särskild utlänningskontroll

30 § När hemlig dataavläsning används eller har använts i fall som anges i 9 § ska 21 a § och 22 § första och andra styckena lagen (1991:572) om särskild utlänningskontroll tillämpas. Det som anges där om hemlig avlyssning och övervakning av elektronisk kommunikation ska tillämpas för hemlig dataavläsning.

Förebyggande, förhindrande och upptäckande av brottslig verksamhet

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 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.

Tystnadsplikt

32 § Den som i samband med verksamhet som är anmälningspliktig enligt 2 kap. 1 § lagen (2003:389) om elektronisk kommunikation har fått del av eller tillgång till en uppgift som hänför sig till användning av hemlig

dataavläsning, får inte obehörigen föra vidare eller utnyttja det han eller hon fått del av eller tillgång till.

Rätt att meddela föreskrifter

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

1. underrättelser enligt 23 §, och
2. medverkan och ersättning enligt 24 §.

---

1. Denna lag träder i kraft den 1 mars 2020.
2. Lagen upphör att gälla vid utgången av februari 2025.

2 Förslag till lag om ändring i lagen (1988:97) om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m.

Härigenom föreskrivs att 28 § lagen (1988:97) om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m. ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
28 §[1]	
Om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen att inhämta rättens tillstånd till hemlig rumsavlyssning enligt 27 kap. 20 d § rättegångsbalken, får tillstånd till åtgärden ges av åklagaren i avvaktan på rättens beslut.	Om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen att inhämta rättens tillstånd till hemlig rumsavlyssning enligt 27 kap. 20 d § rättegångsbalken *eller hemlig dataavläsning enligt 2 § första stycket 5 lagen (2019:000) om hemlig dataavläsning,* får tillstånd till åtgärden ges av åklagaren i avvaktan på rättens beslut.

Om åklagaren har gett ett sådant tillstånd, ska han eller hon utan dröjsmål 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.

Denna lag träder i kraft den 1 mars 2020.

[1] Senaste lydelse 2014:1426.

3 Förslag till lag om ändring i lagen (1991:572) om särskild utlänningskontroll

Härigenom föreskrivs att 20 § lagen (1991:572) om särskild utlänningskontroll ska ha följande lydelse.

Nuvarande lydelse *Föreslagen lydelse*

20 §[1]

För ett sådant ändamål som avses i 19 § första stycket kan rätten, om det finns synnerliga skäl, meddela Säkerhetspolisen eller Polismyndigheten tillstånd enligt 27 kap. rättegångsbalken till hemlig avlyssning av elektronisk kommunikation eller, om det är tillräckligt, hemlig övervakning av elektronisk kommunikation.

Rätten kan för ett sådant ändamål som avses i 19 § första stycket, om det finns synnerliga skäl, även meddela Säkerhetspolisen eller Polismyndigheten tillstånd att närmare undersöka, öppna eller granska post- eller telegrafförsändelser, brev, andra slutna handlingar eller paket som har ställts till utlänningen eller som avsänts från honom eller henne och som påträffas vid husrannsakan, kroppsvisitation eller kroppsbesiktning eller som finns hos ett befordringsföretag.

I det tillstånd som avses i andra stycket kan rätten förordna att en försändelse som avses i tillståndet och som ankommer till ett befordringsföretag, ska hållas kvar till dess den närmare undersökts, öppnats eller granskats. Förordnandet ska innehålla underrättelse om att meddelande om åtgärden inte får lämnas till avsändaren, mottagaren eller någon annan, utan tillstånd av den som har begärt åtgärden.

I lagen (2019:000) om hemlig dataavläsning finns bestämmelser om att rätten kan meddela Säkerhetspolisen eller Polismyndigheten tillstånd enligt den lagen.

Denna lag träder i kraft den 1 mars 2020.

[1] Senaste lydelse 2014:589.

4 Förslag till lag om ändring i lagen (2000:562) om internationell rättslig hjälp i brottmål

Härigenom föreskrivs i fråga om lagen (2000:562) om internationell rättslig hjälp i brottmål

dels att 1 kap. 2 § och 2 kap. 1, 2 och 4 §§ ska ha följande lydelse,

dels att det ska införas sex nya paragrafer, 4 kap. 28 c–28 h §§, och närmast före 4 kap. 28 c och 28 e–28 h §§ nya rubriker av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 kap.	
2 §[1]	
Rättslig hjälp enligt denna lag omfattar följande åtgärder:	
1. förhör i samband med förundersökning i brottmål,	
2. bevisupptagning vid domstol,	
3. telefonförhör,	
4. förhör genom videokonferens,	
5. kvarstad, beslag samt husrannsakan och andra åtgärder som avses i 28 kap. rättegångsbalken,	
6. hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation,	
7. tekniskt bistånd med hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation,	
8. tillstånd till gränsöverskridande hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation,	
9. hemlig kameraövervakning,	*7. hemlig kameraövervakning,*
10. hemlig rumsavlyssning,	*8. hemlig rumsavlyssning,*
	9. hemlig dataavläsning,
	10. tekniskt bistånd med hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation och hemlig dataavläsning enligt 2 § första stycket 1 och 2 lagen (2019:000) om hemlig dataavläsning,
	11. tillstånd till gränsöverskridande hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation och hemlig dataavläsning enligt 2 § första stycket 1 och 2 lagen om hemlig dataavläsning,

[1] Senaste lydelse 2012:284.

11. överförande av frihetsberövade för förhör m.m., och	*12. överförande av frihetsberövade för förhör m.m., och*
12. rättsmedicinsk undersökning av en avliden person.	*13. rättsmedicinsk undersökning av en avliden person.*

Lagen hindrar inte att hjälp lämnas med någon annan åtgärd än sådan som anges i första stycket om det kan ske utan tvångsmedel eller annan tvångsåtgärd.

I fråga om överlämnande, utlämning och delgivning finns särskilda bestämmelser. Det finns också särskilda bestämmelser om rättslig hjälp i brottmål åt vissa internationella organ.

2 kap.

1 §[2]

Rättslig hjälp som avses i 1 kap. 2 § första stycket *1–6, 9, 10 och 12* ska lämnas under de förutsättningar som gäller för en motsvarande åtgärd under en svensk förundersökning eller rättegång enligt rättegångsbalken eller annan lag eller författning och enligt de särskilda bestämmelserna i denna lag.	Rättslig hjälp som avses i 1 kap. 2 § första stycket *1–9 och 13* ska lämnas under de förutsättningar som gäller för en motsvarande åtgärd under en svensk förundersökning eller rättegång enligt rättegångsbalken eller annan lag eller författning och enligt de särskilda bestämmelserna i denna lag.
Rättslig hjälp som avses i 1 kap. 2 § första stycket *7, 8 och 11* lämnas enligt de särskilda bestämmelserna i denna lag.	Rättslig hjälp som avses i 1 kap. 2 § första stycket *10–12* lämnas enligt de särskilda bestämmelserna i denna lag.

I 5 kap. 2 § finns bestämmelser om att den rättsliga hjälpen får förenas med villkor i vissa fall.

2 §[3]

Rättslig hjälp som avses i 1 kap. 2 § första stycket *1–4, 7 och 11* får lämnas även om den gärning som ansökan avser inte motsvarar ett brott enligt svensk lag. Rättslig hjälp som avses i 1 kap. 2 § första stycket *5, 6, 8–10 och 12* får endast lämnas om den gärning som ansökan avser motsvarar ett brott enligt svensk lag (dubbel straffbarhet), om inte annat följer av 4 kap. 20 § beträffande husrannsakan och beslag.	Rättslig hjälp som avses i 1 kap. 2 § första stycket *1–4, 10 och 12* får lämnas även om den gärning som ansökan avser inte motsvarar ett brott enligt svensk lag. Rättslig hjälp som avses i 1 kap. 2 § första stycket *5–9, 11 och 13* får endast lämnas om den gärning som ansökan avser motsvarar ett brott enligt svensk lag (dubbel straffbarhet), om inte annat följer av 4 kap. 20 § beträffande husrannsakan och beslag.

4 §[4]

En ansökan om rättslig hjälp i Sverige enligt denna lag bör innehålla

[2] Senaste lydelse 2007:982.
[3] Senaste lydelse 2007:982.
[4] Senaste lydelse 2013:836.

– uppgift om den utländska domstol eller myndighet som handlägger ärendet,

– en beskrivning av det rättsliga förfarande som pågår,

– uppgift om den aktuella gärningen *med* tid och plats för *denna*, samt de bestämmelser som är tillämpliga i den ansökande staten,	– uppgift om den aktuella gärningen, tid och plats för *den*, samt *uppgift om* de bestämmelser som är tillämpliga i den ansökande staten,

– uppgift om vilken åtgärd som begärs och, i förekommande fall, i vilken egenskap en person ska höras,

– namn på och adress till de personer som är aktuella i ärendet.

I 4 kap. 8, 11, 14, 24 a, 25, 25 b, 25 c, 26 a, 29 och 29 a §§ finns särskilda bestämmelser om vad en ansökan ytterligare ska innehålla vid vissa slag av åtgärder.	I 4 kap. 8, 11, 14, 24 a, 25, 25 b, 25 c, 26 a, *28 c*, 29 och 29 a §§ finns särskilda bestämmelser om vad en ansökan ytterligare ska innehålla vid vissa slag av åtgärder.
Om ärendet är brådskande eller om *verkställighet* önskas inom viss tidsfrist, ska detta anges och motiveras.	Om ärendet är brådskande eller om *verkställigheten* önskas inom *en* viss tidsfrist, ska detta anges och motiveras.

En ansökan om rättslig hjälp ska göras skriftligen genom post, bud eller telefax. Den får även, efter överenskommelse i det enskilda fallet, översändas på annat sätt.

4 kap.

Hemlig dataavläsning

Rättslig hjälp i Sverige med hemlig dataavläsning

28 c §

En ansökan om hemlig dataavläsning i Sverige handläggs av åklagare. Av ansökan ska det framgå under vilken tid åtgärden önskas och sådana uppgifter som behövs för att åtgärden ska kunna genomföras. Åklagaren ska genast pröva om det finns förutsättningar för åtgärden och i sådant fall ansöka om rättens tillstånd till åtgärden eller, när det får ske enligt 17 § lagen (2019:000) om hemlig dataavläsning, själv besluta om åtgärden.

Upptagningar och uppteckningar behöver inte granskas enligt vad som följer av 28 § första stycket lagen om hemlig dataavläsning.

Om åklagaren har fattat beslut enligt första stycket, ska återredovisning enligt 2 kap. 17 § ske först

sedan rätten fattat beslut om hemlig dataavläsning. Upptagningar och uppteckningar får bevaras efter det att ärendet om rättslig hjälp har avslutats och återredovisning skett enligt 2 kap. 17 § endast om det är tillåtet enligt vad som följer av 28 § första stycket lagen om hemlig dataavläsning.

I fråga om underrättelse till en enskild enligt vad som följer av 28 § andra stycket lagen om hemlig dataavläsning ska bestämmelserna i 25 § tredje stycket tillämpas.

28 d §

Om en ansökan avser hemlig dataavläsning enligt 2 § första stycket 1 och 2 lagen (2019:000) om hemlig dataavläsning får rättens beslut enligt 28 c § att tillåta hemlig dataavläsning verkställas med tillämpning av 25 a §.

Tekniskt bistånd i Sverige med hemlig dataavläsning

28 e §

Tekniskt bistånd med hemlig dataavläsning enligt 2 § första stycket 1 och 2 lagen (2019:000) om hemlig dataavläsning i form av omedelbar överföring av meddelanden eller uppgifter om meddelanden får lämnas i Sverige enligt de förutsättningar som gäller enligt 25 b § andra, tredje och femte styckena. Vid hemlig dataavläsning i en annan stat än den som ansökt om tekniskt bistånd ska ett tillstånd enligt 28 f § ha lämnats.

Ansökan ska prövas av åklagare. För beslutet om tekniskt bistånd tillämpas 1 §, 18 § första stycket 1–3 och tredje stycket och 20 § andra stycket lagen om hemlig dataavläsning.

Tillstånd från Sverige till gränsöverskridande hemlig dataavläsning

28 f §

Om ansökan avser tillstånd till gränsöverskridande hemlig dataavläsning enligt 2 § första stycket 1 och 2 lagen (2019:000) om hemlig dataavläsning tillämpas det som gäller för hemlig avlyssning och hemlig övervakning av elektronisk kommunikation enligt 26 a § första och andra styckena och 26 b §. De förutsättningar som gäller enligt 1–6, 11, 14 och 18 §§ lagen om hemlig dataavläsning tillämpas vid tillståndsprövningen. Rätten ska även tillämpa motsvarande förfarande som anges i 16 § den lagen. Tingsrättens beslut får inte överklagas.

Rättslig hjälp och tekniskt bistånd i utlandet med hemlig dataavläsning

28 g §

Vid rättslig hjälp och tekniskt bistånd med hemlig dataavläsning i en annan stat tillämpas 26 §.

Tekniskt bistånd får endast avse hemlig dataavläsning enligt 2 § första stycket 1 och 2 lagen (2019:000) om hemlig dataavläsning.

Om en underrättelse ska lämnas till en enskild tillämpas 28 § andra stycket lagen om hemlig dataavläsning.

Tillstånd från en annan stat till gränsöverskridande hemlig dataavläsning

28 h §

När ett tillstånd till hemlig dataavläsning enligt 2 § första stycket 1 och 2 lagen (2019:000) om hemlig dataavläsning beslutats i en brottsutredning i Sverige och avläsningen eller upptagningen

kommer att göras i en annan medlemsstat i Europeiska unionen, Island eller Norge utan hjälp från den andra staten, tillämpas 26 c §.

Denna lag träder i kraft den 1 mars 2020.

5 Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400)

Härigenom föreskrivs att 18 kap. 19 § och 44 kap. 5 § offentlighets- och sekretesslagen (2009:400) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
18 kap.	
19 §[1]	
Den tystnadsplikt som följer av 5–8, 9 och 10 §§, 11 § första stycket och 12 och 13 §§ inskränker rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter.	
Den tystnadsplikt som följer av 1–3 §§ inskränker rätten att meddela och offentliggöra uppgifter, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning *eller* hemlig rumsavlyssning på grund av beslut av domstol, undersökningsledare eller åklagare eller inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.	Den tystnadsplikt som följer av 1–3 §§ inskränker rätten att meddela och offentliggöra uppgifter, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning *eller hemlig dataavläsning* på grund av beslut av domstol, undersökningsledare eller åklagare eller inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.
Den tystnadsplikt som följer av 17 § inskränker rätten att meddela och offentliggöra uppgifter, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation *eller* hemlig kameraövervakning på grund av beslut av domstol eller åklagare.	Den tystnadsplikt som följer av 17 § inskränker rätten att meddela och offentliggöra uppgifter, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, *hemlig rumsavlyssning eller hemlig dataavläsning* på grund av beslut av domstol eller åklagare.
Att den tystnadsplikt som följer av 1–3 §§ i vissa fall inskränker rätten att meddela och offentliggöra uppgifter utöver det som anges i andra	

[1] Senaste lydelse 2019:305.

stycket följer av 7 kap. 10 §, 12–18 §§, 20 § 3 och 22 § första stycket 1 och andra stycket tryckfrihetsförordningen samt 5 kap. 1 § och 4 § första stycket 1 och andra stycket yttrandefrihetsgrundlagen.

Lydelse enligt SFS 2019:937	*Föreslagen lydelse*
44 kap.	
5 §	
Rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter inskränks av den tystnadsplikt som följer	
1. av beslut som har meddelats med stöd av 7 § lagen (1999:988) om förhör m.m. hos kommissionen för granskning av de svenska säkerhetstjänsternas författningsskyddande verksamhet,	
2. av 7 kap. 1 § 1 lagen (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap,	
3. av 4 kap. 16 § försäkringsrörelselagen (2010:2043), *och*	3. av 4 kap. 16 § försäkringsrörelselagen (2010:2043),
4. av 5 kap. 15 § lagen (1998:293) om utländska försäkringsgivares och tjänstepensionsinstituts verksamhet i Sverige.	4. av 5 kap. 15 § lagen (1998:293) om utländska försäkringsgivares och tjänstepensionsinstituts verksamhet i Sverige, *och*
	5. av 32 § lagen (2019:000) om hemlig dataavläsning.

Denna lag träder i kraft den 1 mars 2020.

6 Förslag till lag om ändring i lagen (2017:1000) om en europeisk utredningsorder

Härigenom föreskrivs i fråga om lagen (2017:1000) om en europeisk utredningsorder

dels att 1 kap. 4 §, 2 kap. 5 § och 3 kap. 10 § ska ha följande lydelse,

dels att det ska införas fem nya paragrafer, 2 kap. 19 a och 19 b §§, 3 kap. 37 a och 37 b §§ och 4 kap. 16 §, och närmast före 2 kap. 19 a §, 3 kap. 37 a § och 4 kap. 16 § nya rubriker av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 kap.	
4 §	
En utredningsåtgärd enligt denna lag ska avse eller motsvara	
1. förhör under förundersökning,	
2. bevisupptagning vid domstol,	
3. förhör genom ljudöverföring eller ljud- och bildöverföring,	
4. beslag, kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken eller en åtgärd enligt 27 kap. 15 § samma balk,	
5. husrannsakan och andra åtgärder enligt 28 kap. rättegångsbalken,	
6. hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning *och* hemlig rumsavlyssning,	6. hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning *och hemlig dataavläsning*,
7. tillfälligt överförande av en frihetsberövad person,	
8. rättsmedicinsk undersökning av en avliden person,	
9. kontrollerad leverans,	
10. bistånd i en brottsutredning med användning av en skyddsidentitet,	
11. inhämtande av bevis som finns hos en myndighet, eller	
12. andra åtgärder som inte innebär användning av tvångsmedel eller någon annan tvångsåtgärd.	
2 kap.	
5 §	
Innan åklagaren utfärdar en utredningsorder ska åklagaren ansöka om domstolens tillstånd till att utfärda utredningsordern, om utredningsåtgärden avser	
1. kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken,	
2. hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning *eller* hemlig rumsavlyssning, eller	2. hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning *eller hemlig dataavläsning*, eller
3. rättsmedicinsk undersökning enligt 16 § lagen (1995:832) om obduktion m.m.	

I avvaktan på domstolens beslut får åklagaren under de förutsättningar som anges i 27 kap. 9 a och 21 a §§ rättegångsbalken utfärda en utredningsorder för kvarhållande av försändelse, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation *eller* hemlig kameraövervakning. Åklagaren ska utan dröjsmål anmäla till domstolen att en utredningsorder har utfärdats.	I avvaktan på domstolens beslut får åklagaren under de förutsättningar som anges i 27 kap. 9 a och 21 a §§ rättegångsbalken *eller 17 § lagen (2019:000) om hemlig dataavläsning* utfärda en utredningsorder för kvarhållande av försändelse, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation*,* hemlig kameraövervakning *eller hemlig dataavläsning*. Åklagaren ska utan dröjsmål anmäla till domstolen att en utredningsorder har utfärdats.

Innan en utredningsorder för husrannsakan, kroppsvisitation eller kroppsbesiktning utfärdas, får åklagaren enligt 28 kap. 4 § första stycket och 13 § första stycket rättegångsbalken ansöka om domstolens tillstånd till att utfärda utredningsordern.

För domstolens handläggning gäller vad som är föreskrivet i rättegångsbalken eller annan författning för den åtgärd som avses.

Hemlig dataavläsning

19 a §

En utredningsorder får utfärdas för hemlig dataavläsning i Sverige eller i en annan medlemsstat.

En utredningsorder för hemlig dataavläsning i Sverige eller i en annan medlemsstat än den stat till vilken ordern översänds enligt 7 § första stycket får endast avse en åtgärd enligt 2 § första stycket 1–3 lagen (2019:000) om hemlig dataavläsning.

Om dataavläsningen enligt andra stycket ska ske i en annan medlemsstat än den stat till vilken ordern översänds enligt 7 § första stycket ska det av utredningsordern framgå att en underrättelse enligt 4 kap. 12 § har lämnats.

19 b §

När en utredningsorder för hemlig dataavläsning har utfärdats, ska 20 § andra stycket, 27 § och 28 § första stycket lagen (2019:000) om hemlig dataavläs-

	ning tillämpas. I de fall där upptagningen eller uppteckningen görs i Sverige ska 28 § andra stycket lagen om hemlig dataavläsning tillämpas.
3 kap.	
10 §	
I avvaktan på domstolens beslut enligt 9 § första stycket får åklagaren, enligt de förutsättningar som anges i 27 kap. 9 a och 21 a §§ rättegångsbalken, besluta att erkänna och verkställa en utredningsorder för kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken eller för hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation *eller* hemlig kameraövervakning.	I avvaktan på domstolens beslut enligt 9 § första stycket får åklagaren, enligt de förutsättningar som anges i 27 kap. 9 a och 21 a §§ rättegångsbalken *eller 17 § lagen (2019:000) om hemlig dataavläsning*, besluta att erkänna och verkställa en utredningsorder för kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken eller för hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation*,* hemlig kameraövervakning *eller hemlig dataavläsning.*
	Hemlig dataavläsning
	37 a §
	Vid verkställighet av en utredningsorder för hemlig dataavläsning som gäller en åtgärd enligt 2 § första stycket 1 och 2 lagen (2019:000) om hemlig dataavläsning tillämpas 34 §.
	Vid verkställighet enligt 34 § 1 får inte någon upptagning eller uppteckning göras i Sverige, och 28 § andra stycket lagen om hemlig dataavläsning ska inte tillämpas. Vid sådan verkställighet tillämpas 35 § andra stycket.
	37 b §
	Vid verkställighet av en utredningsorder för hemlig dataavläsning som sker med stöd av 34 § 2 eller i andra fall av verkställighet av en utredningsorder för hemlig dataavläsning behöver upptagningar eller uppteckningar inte granskas enligt 28 § första stycket

lagen (2019:000) om hemlig dataavläsning. Upptagningar och uppteckningar, som finns kvar i Sverige efter det att ärendet har avslutats hos åklagaren och bevismaterialet har överlämnats med stöd av 38 eller 40 §, får bevaras endast om detta är tillåtet enligt 28 § första stycket lagen om hemlig dataavläsning.

I fråga om underrättelse till en enskild enligt 28 § andra stycket lagen om hemlig dataavläsning ska bestämmelserna i 36 § andra stycket tillämpas.

4 kap.

Underrättelse om hemlig dataavläsning

16 §

Det som anges om hemlig avlyssning och hemlig övervakning av elektronisk kommunikation i 12–15 §§ tillämpas även för hemlig dataavläsning enligt 2 § första stycket 1–3 lagen (2019:000) om hemlig dataavläsning.

Denna lag träder i kraft den 1 mars 2020.

BILAGA 3

Konstitutionsutskottets yttrande 2019/20:KU5y

Hemlig dataavläsning

Till justitieutskottet

Justitieutskottet beslutade den 23 januari 2020 att ge konstitutionsutskottet tillfälle att yttra sig över regeringens proposition 2019/20:64 Hemlig dataavläsning och följdmotioner, i de delar som berör konstitutionsutskottets beredningsområde.

Konstitutionsutskottet begränsar sitt yttrande till frågor om skyddet för den personliga integriteten.

Utifrån de utgångspunkter som konstitutionsutskottet har att beakta ser utskottet inte något hinder mot att propositionen bifalls och att motion 2019/20:3451 av Linda Westerlund Snecker m.fl. (V) avslås.

Utskottets överväganden

Propositionen

I propositionen föreslår regeringen att de brottsbekämpande myndigheterna får möjlighet att använda ett nytt hemligt tvångsmedel, hemlig dataavläsning, vid misstankar om viss allvarlig brottslighet. Syftet med förslaget är att skapa bättre och effektivare möjligheter för de brottsbekämpande myndigheterna att ta del av information som i dagsläget inte är tillgänglig. Det nya tvångsmedlet ska kunna användas under en förundersökning, i underrättelseverksamhet och vid särskild utlänningskontroll.

I propositionen konstaterar regeringen att de brottsbekämpande myndigheterna för närvarande har flera hemliga tvångsmedel till sitt förfogande men att främst den tekniska utvecklingen har medfört svårigheter att använda dessa tvångsmedel eftersom den information som ska avlyssnas, övervakas eller beslagtas ofta är krypterad. Regeringen föreslår därför att möjligheter till hemlig dataavläsning införs.

Hemlig dataavläsning innebär att de brottsbekämpande myndigheterna bereder sig tillgång till teknisk utrustning som kan användas för kommunikation, såsom en dator eller en mobiltelefon, för att ta del av uppgifter som finns i utrustningen. Det kan röra sig om både uppgifter som finns lagrade och uppgifter från en pågående kommunikation. Hemlig dataavläsning innebär också en möjlighet att aktivera den tekniska utrustningens mikrofon eller kamera och att genom gps-funktionerna fastställa var utrustningen befinner sig. Det som främst skiljer hemlig dataavläsning från befintliga hemliga tvångsmedel är därmed möjligheten att i hemlighet komma åt uppgifter som finns lagrade i någons tekniska utrustning. Med befintliga hemliga tvångsmedel hämtas uppgifter in på väg till eller från någons tekniska utrustning. Hemlig dataavläsning innebär dels en ny form för verkställighet av redan befintliga tvångsmedel, dels ett nytt hemligt tvångsmedel.

Det finns enligt regeringen ett påtagligt behov av nya och bättre metoder för att dels i hemlighet komma åt uppgifter som redan i dag får hämtas in med befintliga tvångsmedel men som på grund av den tekniska utvecklingen inte i praktiken går att ta del av, dels i hemlighet samla in uppgifter som inte kan samlas in med befintliga hemliga tvångsmedel. Hemlig dataavläsning kan enligt regeringen förväntas utgöra en effektiv åtgärd för de brottsbekämpande myndigheterna eftersom metoden kan leda till betydligt bättre tillgång till information än dagens metoder ger tillgång till.

Regeringen konstaterar att hemlig dataavläsning innebär risker för den personliga integriteten. De positiva effekter som åtgärden skulle få i form av försvårande av kriminell verksamhet överväger dock enligt regeringen klart de negativa effekter som åtgärden får i form av integritetsinskränkningar.

För att så långt som möjligt begränsa riskerna för den personliga integriteten lämnar regeringen ett antal förslag som syftar till att stärka

enskildas integritetsskydd och rättssäkerhet. Så ska exempelvis frågor om hemlig dataavläsning prövas av domstol som ska hålla ett sammanträde i ärendet. Offentliga ombud ska förordnas för att tillvarata enskildas integritetsintressen, och ombud ska närvara vid sammanträdena. I likhet med vad som gäller för redan befintliga tvångsmedel ska beslut i ärenden om hemlig dataavläsning få överklagas och ett skyndsamhetskrav ska införas för handläggningen i domstol. Ett beslut om tillstånd för hemlig dataavläsning ska vidare vara detaljerat och ange exempelvis vilket avläsningsbart informationssystem, vilken typ av uppgift och vilka villkor i övrigt som omfattas av tillståndet.

Härutöver föreslås i propositionen bl.a.

- bestämmelser om hanteringen av överskottsinformation
- skydd för vissa yrkesgrupper, såsom journalister, advokater och präster
- underrättelser i efterhand till enskilda om att hemlig dataavläsning har använts
- parlamentarisk insyn och kontroll genom en årlig skrivelse från regeringen till riksdagen där användningen av hemlig dataavläsning redovisas
- underrättelser till och tillsyn av Säkerhets- och integritetsskyddsnämnden
- bestämmelser om tystnadsplikt för uppgifter som hänför sig till hemlig dataavläsning.

Eftersom nya tvångsmedel ger upphov till risker för otillbörliga integritetsintrång kan ett fördjupat underlag enligt regeringen behövas inför ett ställningstagande till om lagen bör permanentas. Möjligheten till hemlig dataavläsning ska därför enligt förslaget införas genom en tidsbegränsad lag. Den nya lagen och övriga lagändringar föreslås träda i kraft den 1 mars 2020.

Lagrådet konstaterar att förslaget innebär väsentliga intrång i enskilda människors rätt till respekt för sitt privatliv och sin korrespondens. Lagrådet menar dock att förslagets underlag i fråga om analys av behov, tillämpningsområde, förväntad effektivitet och proportionalitet i förhållande till riskerna för den personliga integriteten är tillräckligt för att motivera att hemlig dataavläsning införs som ett nytt hemligt tvångsmedel. Lagrådet beaktar i sammanhanget att tillstånd till hemlig dataavläsning alltid ska prövas av domstol, som också ska underrätta Säkerhets- och integritetsskyddsnämnden om ett tillståndsbeslut. Lagrådet framhåller vikten av att det säkerställs att Säkerhets- och integritetsskyddsnämnden har förutsättningar att på ett effektivt sätt utöva tillsyn och efterhandskontroll och att det görs en ingående utvärdering av behovet, nyttan och proportionaliteten innan det fattas beslut om huruvida lagstiftningen ska förlängas eller permanentas.

Motionen

Linda Westerlund Snecker m.fl. (V) yrkar i kommittémotion 2019/20:3451 att riksdagen ska avslå propositionen. Motionärerna anför i huvudsak följande.

Mycket talar för att hemlig dataavläsning inte skulle komma att bli en effektiv åtgärd, eftersom den endast i ett mycket begränsat antal fall i praktiken kommer att ge tillgång till information som de brottsbekämpande myndigheterna inte redan kommer åt i dag. Detta beror enligt motionärerna bl.a. på svårigheter att i hemlighet installera program i någon annans tekniska utrustning och möjligheten för den som utsätts för tvångsmedlet att med hjälp av olika programvaror omöjliggöra en läsning av ett meddelande innan det krypteras. Till detta kommer att tillverkarna av it-system kan komma att åtgärda eventuella säkerhetsbrister och därmed försvåra verkställigheten av hemlig dataavläsning.

Vidare menar motionärerna att förslaget innebär bristande rättssäkerhet för den enskilde eftersom domstolsprövningen inte ska omfatta vilka tekniska hjälpmedel som i det enskilda fallet ska användas för dataavläsningen. För att domstolen ska kunna göra en fullständig nödvändighets- och proportionalitetsbedömning i det enskilda fallet måste den enligt motionärerna veta vilka tekniska åtgärder som ska genomföras. Det är inte tillräckligt att valet av teknik omfattas av den tillsyn som utförs av Säkerhets- och integritetsskyddsnämnden.

Motionärerna anför vidare att förslaget innebär ett sådant betydande intrång i den personliga integriteten att regeringen i propositionen borde ha prövat förutsättningarna för detta nya tvångsmedel för varje brott för sig. I stället har regeringen gjort bedömningen att eftersom hemlig dataavläsning till stora delar är en ny metod att komma åt information som redan är möjlig att samla in med befintliga tvångsmedel bör utgångspunkten vara att de krav som gäller för dessa tvångsmedel ska gälla också för hemlig dataavläsning. Hemlig dataavläsning skulle, menar motionärerna, möjligen kunna vara ett rimligt tvångsmedel för de allra grövsta brotten. Eftersom regeringen inte har gjort någon prövning av behovet av detta tvångsmedel för varje enskilt tänkbart brott saknas det enligt motionärerna dock underlag för sådana överväganden.

Slutligen anför motionärerna att hemlig dataavläsning enligt förslaget bl.a. ska få användas vid en förundersökning om brott för vilket det inte är föreskrivet ett lindrigare straff än fängelse i två år samt vid förundersökningar om andra brott, om det kan antas att brottets straffvärde överstiger fängelse i två år. Motionärerna anför att detta är orimligt ur proportionalitetssynpunkt och jämför med förhållandena i Norge, Danmark och Finland, där ett motsvarande tvångsmedel får användas endast för ett fåtal särskilt allvarliga brott.

Gällande ordning

Regeringsformen, Europakonventionen och rättighetsstadgan

Det allmänna ska enligt 1 kap. 2 § fjärde stycket regeringsformen (RF) verka för att demokratins idéer blir vägledande inom samhällets alla områden och värna den enskildes privatliv och familjeliv.

Var och en är gentemot det allmänna enligt 2 kap. 6 § första stycket RF skyddad mot undersökning av brev eller annan förtrolig försändelse och mot hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande. Var och en är dessutom gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden (2 kap. 6 § andra stycket RF). Begränsningar i detta skydd får göras i lag och endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Begränsningarna får aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett dem och heller inte sträcka sig så långt att de utgör ett hot mot den fria åsiktsbildningen (2 kap. 20 och 21 §§ RF).

Enligt artikel 8 i europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) har var och en rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. En inskränkning i dessa rättigheter får bara göras med stöd av lag och om det är nödvändigt med hänsyn till ändamål som är angivna i artikeln. Sverige har tillträtt Europakonventionen, och den gäller sedan 1995 också som lag i Sverige. Enligt 2 kap. 19 § RF får en lag eller annan föreskrift inte meddelas i strid med Sveriges åtaganden på grund av Europakonventionen.

Artikel 8 i Europeiska unionens stadga om de grundläggande rättigheterna (2010/C 83/02) reglerar skyddet av personuppgifter. Enligt artikeln har var och en rätt till skydd av de personuppgifter som rör honom eller henne. Sådana uppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få dem rättade. En oberoende myndighet ska kontrollera att reglerna efterlevs.

Hemliga tvångsmedel

De befintliga hemliga tvångsmedlen är hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning. Härutöver har inhämtning enligt lagen (2012:278) om inhämtande av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen) och kvarhållande och kontroll av försändelse ansetts utgöra hemliga tvångsmedel. Den senare saknar dock enligt regeringen betydelse för frågan om hemlig dataavläsning.

Regeringen lämnar i propositionen en redogörelse för innebörden av och de grundläggande förutsättningarna för dessa hemliga tvångsmedel.

Utskottets ställningstagande

Utskottet vill inledningsvis betona vikten av att den enskildes personliga integritet värnas. Lagförslag bör föregås av en noggrann analys av förslagets konsekvenser för den personliga integriteten, och en avvägning måste göras mellan integritetsskyddsintresset och det intresse som motiverar lagförslaget. En inskränkning av skyddet för den personliga integriteten får inte gå längre än vad som är nödvändigt med hänsyn till det ändamål som föranlett den.

Syftet med regeringens förslag om hemlig dataavläsning är att ge de brottsbekämpande myndigheterna bättre och effektivare möjligheter att förhindra och utreda allvarlig brottslighet. Detta ska ske genom att berörda myndigheter får ta del av information som i dag inte är tillgänglig. Hemlig dataavläsning innebär att de brottsbekämpande myndigheterna får möjlighet att i hemlighet samla in uppgifter om och kartlägga enskilda. Förslaget innebär därmed enligt utskottets mening ett väsentligt intrång i den enskildes personliga integritet. För att förslaget ska kunna godtas krävs att det finns ett så stort behov av hemlig dataavläsning att fördelarna med tvångsmedlet är proportionerliga i förhållande till detta intrång.

Utskottet konstaterar att regeringen i propositionen utförligt redogör för dels sina överväganden när det gäller förslagets konsekvenser för den personliga integriteten, dels den avvägning som har gjorts mellan integritetsskyddsintresset och intresset av att förbättra möjligheterna att bekämpa och lagföra allvarliga brott med hjälp av hemlig dataavläsning. Härutöver lämnas i propositionen ett antal förslag som är ägnade att så långt som möjligt stärka den enskildes rättssäkerhet och integritetsskydd, såsom att tillstånd till hemlig dataavläsning ska beslutas av domstol, att det ska råda förbud mot hemlig dataavläsning på vissa platser och för vissa yrkeskategorier samt att Säkerhets- och integritetsskyddsnämndens tillsyn ska omfatta även hemlig dataavläsning. Utskottet noterar också att hemlig dataavläsning enligt förslaget ska införas genom en särskild, tidsbegränsad lag.

I sammanhanget vill utskottet, i likhet med Lagrådet, framhålla vikten av att Säkerhets- och integritetsskyddsnämnden ges förutsättningar för en effektiv tillsyn och av att det görs en ingående utvärdering av behovet, nyttan och proportionaliteten av hemlig dataavläsning innan det fattas beslut om huruvida den tillfälliga lagstiftningen ska förlängas eller permanentas. Härutöver vill utskottet understryka vikten av de bevis- och proportionalitetskrav som syftar till att begränsa intrång i den personliga integriteten för andra personer än den som är misstänkt för allvarlig brottslighet.

Utifrån de utgångspunkter som konstitutionsutskottet har att beakta har utskottet sammantaget inget att invända mot att propositionen bifalls och att motion 2019/20:3451 (V) avslås.

Stockholm den 6 februari 2020

På konstitutionsutskottets vägnar

Hans Ekström

Följande ledamöter har deltagit i beslutet: Hans Ekström (S), Ida Karkiainen (S), Marta Obminska (M), Matheus Enholm (SD), Per-Arne Håkansson (S), Linda Modig (C), Mia Sydow Mölleby (V), Ida Drougge (M), Fredrik Lindahl (SD), Tuve Skånberg (KD), Daniel Andersson (S), Tina Acketoft (L), Mikael Strandman (SD), Camilla Hansén (MP), Erik Ottoson (M), Lars Jilmstad (M) och Nermina Mizimovic (S).

Avvikande mening

Hemlig dataavläsning (V)

Mia Sydow Mölleby (V) anför:

De brottsbekämpande myndigheterna måste ges effektiva förutsättningar att bekämpa och utreda brott, bl.a. genom användningen av hemliga tvångsmedel. Sådana tvångsmedel innebär emellertid samtidigt en inskränkning i grundläggande fri- och rättigheter. Införandet av nya hemliga tvångsmedel måste föregås av noggranna överväganden om behov, effektivitet och proportionalitet. Detta gäller inte minst vid inskränkningar av skyddet för den personliga integriteten.

Jag ser med stor oro på de senaste decenniernas utveckling mot en ökad övervakning. Frågor om personlig integritet får gång på gång stå tillbaka i lagstiftningsärenden om exempelvis kamerabevakning, signalspaning, utlänningskontroll och hemliga tvångsmedel. Det finns stora risker med att se olika brottsbekämpande åtgärder för sig: varje enskild åtgärd kan te sig motiverad och befogad, men sammantaget kan ett flertal åtgärder innebära ett oproportionerligt intrång i den personliga integriteten. Dessutom tenderar varje inskränkning i den personliga integriteten att bana väg för ännu fler och mer ingripande åtgärder. Jag menar därför att det krävs en sammantagen proportionalitetsbedömning där både genomförda, föreslagna och kommande åtgärder bedöms utifrån integritetsskyddssynpunkt innan man går vidare med fler lagstiftningsåtgärder.

När det gäller det aktuella förslaget om hemlig dataavläsning anser jag att inskränkningarna i den enskildes personliga integritet är så ingripande att de inte står i proportion till intresset av att bekämpa allvarlig brottslighet. Hemlig dataavläsning skulle möjligen kunna vara en rimlig åtgärd för att förhindra och utreda de allra grövsta brotten, som är fallet i de övriga nordiska länderna, men det underlag som presenteras i propositionen möjliggör inte ett sådant ställningstagande. Regeringen har där inte prövat och redovisat behovet och proportionaliteten av hemlig dataavläsning för varje brott för sig. I stället är regeringens utgångspunkt att i bedömningen av vid vilka brott det ska vara möjligt med hemlig dataavläsning bör motsvarande krav gälla som för de bakomliggande redan befintliga tvångsmedlen. Resultatet blir att förslaget möjliggör ett mycket ingripande hemligt tvångsmedel även för brott som inte är tillräckligt allvarliga.

Det går dessutom att ifrågasätta förslagets effektivitet, bl.a. med hänsyn till svårigheten att i hemlighet installera program i någon annans tekniska utrustning eller att utnyttja säkerhetsbrister i befintliga it-system. Till detta

kommer de rättssäkerhetsbrister som följer av att domstolens tillståndsprövning inte ska omfatta vilka tekniska hjälpmedel som ska användas vid verkställigheten i det enskilda fallet. Säkerhets- och integritetsskyddsnämndens efterhandskontroll utgör enligt min mening inte en tillräcklig garanti för enskildas rättssäkerhet.

Från de utgångspunkter konstitutionsutskottet har att beakta anser jag mot denna bakgrund att justitieutskottet bör föreslå för riksdagen att propositionen avslås och att motion 2019/20:3451 (V) bifalls.

Tryck: Elanders Sverige AB, Vällingby 2020