LAGRÅDET

Utdrag ur protokoll vid sammanträde 2019-11-18

Närvarande: F.d. justitierådet Ella Nyström samt justitieråden Per Classon och Stefan Johansson

Hemlig dataavläsning

Enligt en lagrådsremiss den 24 oktober 2019 har regeringen (Justitiedepartementet) beslutat inhämta Lagrådets yttrande över förslag till

1. lag om hemlig dataavläsning,
2. lag om ändring i lagen (1988:97) om förfarandet hos kommunerna, förvaltningsdomstolarna 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.

Förslagen har inför Lagrådet föredragits av rättssakkunnige Peter Munck.

Förslagen föranleder följande yttrande.

Allmänna synpunkter

I remissen föreslås lagstiftning som innebär att de brottsbekämpande myndigheterna ska få möjlighet att vid misstanke om allvarlig brottslighet använda ett nytt hemligt tvångsmedel – hemlig dataavläsning. Den särskilda lagen om hemlig dataavläsning föreslås gälla under en begränsad tid om fem år.

Hemlig dataavläsning innebär att den brottsbekämpande myndigheten bereder sig tillgång till teknisk utrustning som kan användas för kommunikation, t.ex. en dator, en surfplatta eller en mobiltelefon, och därefter tar del av de uppgifter som finns i den tekniska utrustningen. Detta innefattar såväl lagrade uppgifter (t.ex. innehållet i e-post och andra meddelanden, besökta webbsidor, lagrade fotografier, dokument och andra filer), som uppgifter i realtid (bl.a. telefonsamtal, videosamtal och pågående kommunikation via textmeddelanden). Vidare ger hemlig dataavläsning den brotts-bekämpande myndigheten möjlighet att bl.a. aktivera den tekniska utrustningens mikrofon och kamera samt att genom GPS-funktionerna fastställa den geografiska platsen för utrustningen.

Det som skiljer hemlig dataavläsning från de hemliga tvångsmedel som de brottsbekämpande myndigheterna nu har tillgång till (hemlig avlyssning och hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning) är att de uppgifter som hemlig dataavläsning är tänkt att komma åt finns i någons tekniska utrustning. Vid hemlig avlyssning eller hemlig

övervakning av elektronisk kommunikation hämtas uppgifterna in på väg till eller från någons tekniska utrustning. Hemlig kamera-övervakning och hemlig rumsavlyssning sker genom utrustning som tillhör och i hemlighet monteras av de brottsbekämpande myndigheterna.

Hemlig dataavläsning innebär att de brottsbekämpande myndigheterna får tillgång till dels en ny form för verkställighet av redan befintliga hemliga tvångsmedel, dels ett nytt hemligt tvångs-medel genom vilket de i hemlighet och i realtid kan komma åt uppgifter som antingen finns lagrade i den tekniska utrustningen eller visar hur den används.

Ett införande av hemlig dataavläsning medför att de brotts-bekämpande myndigheternas möjligheter att i hemlighet samla in uppgifter om och kartlägga enskilda ökar påtagligt och innebär väsentliga intrång i enskilda människors rätt till respekt för sitt privatliv och sin korrespondens. Dessutom kan hemlig dataavläsning medföra risker för informationssäkerheten.

Enligt Lagrådets mening krävs för att förslagen ska kunna godtas att det finns ett så starkt behov av hemlig dataavläsning att det som står att vinna med åtgärden är proportionerligt i förhållande till intrånget i enskildas integritet och riskerna för informationssäkerheten. Det innebär att hemlig dataavläsning endast bör få användas vid allvarlig brottslighet och när andra mindre ingripande tvångsmedel inte är möjliga att använda eller inte är tillräckliga. Vidare måste villkoren för användning av hemlig dataavläsning vara så tydliga att risken för en extensiv tillämpning eller missbruk minimeras. Användningen av tvångsmedlet måste även kringgärdas av betryggande tillstånds- och procedurregler samt rättssäkerhetsgarantier. Därutöver ska det finnas en effektiv tillsyn och efterhandskontroll.

När det gäller behovet är det framför allt den tekniska utvecklingen, särskilt i form av kryptering och anonymisering, samt hur kriminella har anpassat sitt beteende som anförs som skäl för att införa hemlig dataavläsning. Det anges bl.a. att hemlig avlyssning och hemlig övervakning av elektronisk kommunikation i dag är långt ifrån lika effektiva metoder för avlyssning och övervakning som de varit tidigare.

Remissen innehåller en tämligen utförlig analys av behov, tillämpningsområde, förväntad effektivitet samt risker för den personliga integriteteten och för informationssäkerheten. Lagrådet bedömer att det underlag som presenteras är tillräckligt för att motivera att hemlig dataavläsning införs som ett nytt hemligt tvångsmedel. Mot denna bakgrund, och med beaktande av att hemlig dataavläsning alltid ska prövas av domstol som ska underrätta Säkerhets- och integritetsskyddsnämnden om beslutet, anser Lagrådet att förslagen kan läggas till grund för lagstiftning.

I sammanhanget måste emellertid framhållas vikten av att det säkerställs att Säkerhets- och integritetsskyddsnämnden har förutsättningar att på ett effektivt sätt utöva tillsyn och efterhands-kontroll samt att det görs en ingående utvärdering av behovet, nyttan och proportionaliteten innan det fattas beslut om huruvida lagstiftningen ska förlängas eller permanentas.

Förslaget till lag om hemlig dataavläsning

Den valda lagstiftningstekniken, att reglera hemlig dataavläsning i en egen lag, innebär *dels* att många av de föreslagna bestämmelserna i stora delar är likalydande med bestämmelser i gällande tvångs-medelslagstiftning, *dels* att hänvisningar görs till flera andra lagar. Regelverket blir därmed mer svåröverskådligt än om bestäm-

melserna om hemlig dataavläsning hade arbetats in i den befintliga lagstiftningen; detta särskilt eftersom hemlig dataavläsning i stor utsträckning utgör en ny verkställighetsform av redan existerande hemliga tvångsmedel.

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

Beträffande lagförslagets bestämmelser har Lagrådet följande synpunkter.

1 §

I första stycket definieras det nya tvångsmedlet hemlig data-avläsning. Enligt denna definition innebär hemlig dataavläsning att uppgifter, som är avsedda för automatiserad behandling, i hemlighet och med ett tekniskt hjälpmedel läses av eller tas upp i ett avläsningsbart informationssystem.

Enligt remissen och vad som uppgetts vid föredragningen innebär uttrycket ”läses av” att den verkställande myndigheten tar del av uppgifterna i realtid medan uttrycket ” tas upp” innebär att uppgifterna sparas för att granskas i efterhand. Vidare ska uppgifterna läsas av eller tas upp i ett avläsningsbart informationssystem. Det system som avses är det informationssystem, t.ex. en mobiltelefon eller persondator, som är föremål för tvångsmedlet och som används av exempelvis någon som är skäligen misstänkt för ett brott.

Enligt Lagrådets mening framstår definitionen som ofullständig genom att det inte kommer till uttryck att den verkställande myndigheten, efter att uppgifterna tagits upp i ett avläsningsbart informationssystem, hämtar in uppgifterna för att ta del av dem. Definitionen riskerar även att ge upphov till oklarheter och missuppfattningar beträffande vilket avläsningsbart informations-system som avses; det som används av den som är föremål för tvångsmedlet eller myndighetens.

Utformningen av definitionen bör därför övervägas i den fortsatta beredningen.

4 §

Paragrafens andra stycke består av två meningar som innehåller från varandra skilda bestämmelser beträffande förutsättningarna för hemlig dataavläsning under en förundersökning. Lagrådet anser att de olika förutsättningarna framgår tydligare om de delas upp och placeras i ett andra och tredje stycke. Som en konsekvens bör även det förutvarande tredje stycket ändras. Följande lydelse av andra, tredje och fjärde styckena föreslås.

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 och 6 §§

Kopplingen mellan dessa paragrafer och 4 § bör förtydligas genom att det efter de inledande orden ”Ett tillstånd till hemlig dataavläsning” i båda paragraferna tilläggs ”enligt 4 §”. Härigenom framgår att bestämmelserna ska läsas tillsammans med 4 §, där t.ex. kravet på att åtgärden ska vara av synnerlig vikt för utredningen uttrycks (jfr formuleringen i inledningen till 8 § som hänvisar till 7 §).

9 §

I paragrafen regleras vad som gäller för tillståndsgivning till hemlig dataavläsning när det finns förhållanden som kan ligga till grund för beslut om hemliga tvångsmedel enligt lagen om särskild utlännings-kontroll.

I andra stycket anges att ett tillstånd till hemlig dataavläsning får 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.

En motsvarande bestämmelse finns i 8 § andra stycket som ska tillämpas avseende lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen). Enligt den bestäm-melsen får tillstånd i preventivlagsfallen endast beviljas för kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter.

Det har vid föredragningen upplysts att syftet inte är att utvidga möjligheterna till informationsinhämtning avseende situationerna i 9 §

andra stycket till att omfatta de typer av uppgifter som anges i 2 § första stycket 6 och 7.

Det bör därför i 9 § andra stycket, i likhet med i 8 § andra stycket, uttryckligen anges att tillstånd endast får beviljas för kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter.

21 §

I paragrafen föreskrivs en skyldighet för domstolen att underrätta Säkerhets- och integritetsskyddsnämnden vid beslut om hemlig dataavläsning. I författningskommentaren anges att underrättelse bör äga rum i anslutning till beslutstillfället och lämpligen göras samma dag eller följande arbetsdag.

Lagrådet anser att det av lagtexten uttryckligen bör framgå att domstolen inte får dröja med underrättelsen. Detta kan lämpligen ske genom att det i paragrafen anges att rätten ”skyndsamt” ska underrätta Säkerhets- och integritetsskyddsnämnden om beslutet.

31 §

Paragrafen anger vad som ska gälla för bl.a. överskottsinformation i de fall hemlig dataavläsning används enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brotts-bekämpande myndigheternas underrättelseverksamhet (inhämtningslagen).

I paragrafen hänvisas till bl.a. 7 § inhämtningslagen som reglerar hur överskottsinformation får användas enligt den lagen. Av paragrafen följer bl.a. att uppgifter som har kommit fram vid inhämtning enligt

inhämtningslagen får användas i en förundersökning endast efter tillstånd till hemlig övervakning av elektronisk kommunikation.

Lagrådet anser att frågan om behandlingen av överskottsinformation är av så central betydelse att det uttryckligen av lagtexten i 31 § bör framgå vad som gäller för överskottsinformation inom ramen för hemlig dataavläsning.

Förslagen till lag om ändring i lagen om internationell rättslig hjälp i brottmål och lag om ändring i lagen om en europeisk utredningsorder

Den valda lagstiftningsmetoden medför att regelverken blir mycket svårgenomträngliga. Framförallt är det de många hänvisningarna till olika tvångsmedelslagar som komplicerar regelverken.

Eftersom materiella bestämmelser om hemliga tvångsmedel regleras i annan lagstiftning är det i och för sig ofrånkomligt att lagar om internationell rättslig hjälp innehåller förhållandevis många hänvisningar. Förslaget att reglera hemlig dataavläsning i en egen lag som också innehåller hänvisningar till befintlig tvångsmedels-lagstiftning lyfter emellertid upp komplexiteten ytterligare en nivå, vilket är olyckligt. Detta understryker att lagstiftningstekniken bör övervägas på nytt för det fall det blir fråga om att förlänga eller permanenta hemlig dataavläsning.

Vid lagstiftning som innehåller många hänvisningar är utformningen av författningskommentaren av stor betydelse för dem som ska tillämpa regelverket. Lagrådet anser att det finns anledning att i den fortsatta beredningen göra en ordentlig genomarbetning av författningskommentaren till förslagen till ändringar i lagen om internationell rättslig hjälp i brottmål och lagen om en europeisk utredningsorder.

Övriga lagförslag

Lagrådet lämnar förslagen utan erinran.