Kommittédirektiv

Hemlig dataavläsning

Dir. 2016:36

Beslut vid regeringssammanträde den 12 maj 2016

Sammanfattning

En särskild utredare ska undersöka om bestämmelser om hemlig dataavläsning bör införas i svensk rätt för att säkerställa att de brottsbekämpande myndigheterna kan upprätthålla sin förmåga att bekämpa brott.

Utredaren ska bl.a.

- ta reda på vilket behov av hemlig dataavläsning som finns,
- undersöka om hemlig dataavläsning skulle vara en effektiv metod för att bekämpa terrorristbrottslighet och andra allvarliga brott,
- klargöra om intresset av att upprätthålla ett starkt skydd för den personliga integriteten ger utrymme för att tillåta hemlig dataavläsning,
- analysera om det är lämpligt att införa hemlig dataavläsning som ett nytt straffprocessuellt tvångsmedel, och
- lämna fullständiga förslag till författningsändringar eller andra förändringar oavsett vad analysen föranleder.

Uppdraget ska redovisas senast den 13 november 2017.

Förutsättningarna för att bekämpa brott har förändrats

Under senare år har den ökande internationaliseringen i kombination med teknikutvecklingen och en tilltagande internetanvändning inneburit att kriminaliteten delvis har ändrat karaktär. Internet erbjuder lättillgängliga kontaktytor för brottsplanering inom och utom landets gränser och utgör bl.a. en etablerad plattform för våldsbejakande extremism och terrorismpropaganda. Viss typ av kriminalitet, t.ex. barnpornografibrott, har internet som brottsplats. Utvecklingen innebär att även förutsättningarna för att förhindra brott och säkra bevis för begångna brott har förändrats radikalt. Uppgifter om elektronisk kommunikation och andra elektroniska spår är i dag helt nödvändiga för brottsbekämpningen.

Samtidigt har teknik- och kommunikationsutvecklingen under de senaste åren begränsat det praktiska användningsområdet för hemlig avlyssning av elektronisk kommunikation (hemlig avlyssning). Hemlig avlyssning används av brottsbekämpande myndigheter för att komma åt innehållet i kommunikation mellan individer. Nuvarande lagstiftning tillåter hemlig avlyssning av såväl traditionell telefoni som internetbaserad kommunikation, t.ex. ip-telefoni, e-post och sociala medier. Eftersom internetbaserad kommunikation mellan individer allt oftare krypteras när den skickas från avsändare till mottagare får myndigheterna emellertid ofta bara tillgång till krypterad information inom ramen för ett tillstånd till hemlig avlyssning. För leverantörer av internetbaserade tjänster finns det, till skillnad från för leverantörer av traditionell telefoni, inte någon skyldighet att anpassa sina tekniska system så att de kan lämna ut kommunikation som de krypterar i sina nät till brottsbekämpande myndigheter i klartext. De brottsbekämpande myndigheterna har inte någon egen möjlighet att dekryptera kommunikation i realtid. Det är inte heller realistiskt för myndigheterna att bygga upp och underhålla en sådan teknisk förmåga i förhållande till de olika operatörernas system.

Det finns andra tekniska svårigheter med att avlyssna internetbaserad kommunikation inom ramen för ett tillstånd till hemlig avlyssning. Det beror framför allt på att enskilda per-

soner enkelt kan köpa anonymiseringstjänster som skyddar deras identitet, ip-adress, på nätet så att kommunikationen blir helt anonym. Teknikutvecklingen har också medfört att det inte längre är självklart att en viss ip-adress motsvarar en enskild abonnent. Flera abonnenter kan dela på en och samma adress vilket medför att ip-adressen inte är synonym med den misstänktes identitet på nätet. Den stora mängden krypterad information på nätet innebär också att det kan vara svårt för brottsbekämpande myndigheter att identifiera vad som är kommunikation mellan individer i det samlade flödet.

En effektiv brottsbekämpning förutsätter att de brottsbekämpande myndigheterna har ändamålsenliga verktyg för att bekämpa brott. Flera länder tillåter att de brottsbekämpande myndigheterna använder sig av hemlig dataavläsning som metod. I Danmark har hemlig dataavläsning använts sedan 2002. I Finland möjliggör relativt ny lagstiftning hemlig dataavläsning. Också Tyskland använder sig av en sådan metod. De olika länderna har reglerat metoden på olika sätt. Norge arbetar för närvarande med ett lagförslag om hemlig dataavläsning som ska presenteras för Stortinget. Viktiga lärdomar kan dras av hur andra länder till exempel har valt att avgränsa vilka brott som verktyget får användas för och hur överskottsinformation ska hanteras.

Beredningen för rättsväsendets utveckling (BRU) föreslog 2005 att hemlig dataavläsning skulle införas som ett nytt tvångsmedel i svensk rätt (SOU 2005:38). Som bakgrund till förslaget anfördes bl.a. att den organiserade brottsligheten alltmer söker sig till kommunikationsformer som är säkrare än telefoner, utnyttjar modern teknik och använder internet som ett arbetsredskap i verksamheten. Möjligheten att kommunicera på ett relativt anonymt och säkert sätt (främst frågan om kryptering) framhölls vid sidan av globaliseringen och mobiliteten som stora utmaningar som den internetrelaterade brottsligheten ställer upp för rättsväsendet. Beredningen bedömde det helt nödvändigt att de brottsbekämpande myndigheterna skulle ha möjlighet att använda effektiva arbetsmetoder, inte minst med anknytning till internet, för att den kvalificerade brottsligheten med dess struktur, inriktning och tillvägagångssätt skulle kunna

bekämpas (SOU 2005:38, s. 360). Förslaget kritiserades av många remissinstanser och har inte lett till lagstiftning. Den huvudsakliga kritiken gällde att det föreslagna tvångsmedlets effektivitet och integritetseffekter inte ansågs tillräckligt klarlagda. Dessutom ifrågasatte flera remissinstanser om beskrivningen av teknikutvecklingen var rättvisande och därmed om behovet av åtgärder var så tungt vägande att det motiverade ett nytt tvångsmedel.

På motsvarande sätt som BRU redovisade Utredningen om vissa hemliga tvångsmedel några år senare att det vid den kartläggning av tillämpningen av vissa hemliga tvångsmedel som utredningen genomfört hade framkommit att personer inom den organiserade brottsligheten ägnar stor möda åt att anpassa sin kommunikation så att myndigheterna inte ska kunna avlyssna den. Utredningen konstaterade att krypterade telefonitjänster används liksom e-post och att det finns exempel på hur gemensamma mejlkonton utnyttjas för att undgå att meddelanden sänds mellan konton (SOU 2012:44, s. 765).

Det är avgörande att de brottsbekämpande myndigheterna upprätthåller sin förmåga att bekämpa brott. Teknik- och samhällsutvecklingen innebär att det nu finns anledning att på nytt undersöka om hemlig dataavläsning bör införas som ett straffprocessuellt tvångsmedel. Vid en sådan bedömning måste det säkerställas att grundläggande rättigheter respekteras och att intrång i enskildas integritet minimeras.

Uppdraget att undersöka om hemlig dataavläsning bör införas som ett nytt straffprocessuellt tvångsmedel

Det finns inte någon fastställd definition av hemlig dataavläsning. Som utgångspunkt för en analys kan begreppet definieras som 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 används för kommunikation och därigenom få besked om hur utrustningen används i realtid och vilken information som finns i den. Detta kan t.ex. ske genom att en hård- eller mjuk-

vara placeras, antingen fysiskt eller elektroniskt, via en eller flera trojaner, i en användares tekniska utrustning.

Enligt 2 kap. 6 § regeringsformen är var och en gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om intrånget sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Överväganden om att införa regler om hemlig dataavläsning i svensk rätt fordrar en avvägning mellan å ena sidan samhällets behov av en effektiv brottsbekämpning och å andra sidan den enskildes rätt till integritet i förhållande till staten. Bara om hemlig dataavläsning bedöms vara en proportionerlig åtgärd kan den tillåtas. För att det ska vara möjligt att göra den avvägning som behövs måste det inledningsvis fastställas om det finns ett reellt behov av hemlig dataavläsning som metod i brottsbekämpningen eller om den brottsbekämpande förmågan kan upprätthållas med mindre integritetskänsliga metoder. Hur stort behovet av hemlig dataavläsning kan bedömas vara beror bl.a. på hur den moderna brottsligheten ser ut och samhällsutvecklingen i övrigt. Den tekniska utvecklingen och de förändrade förutsättningar för kommunikation som den medfört behöver särskilt uppmärksammas. Endast under förutsättning att behovet är tungt vägande och grundligt redovisat kan det ligga till grund för fortsatta överväganden om att införa metoden.

Nästa fråga blir i vilken utsträckning hemlig dataavläsning kan förväntas vara en effektiv metod för brottsbekämpning i förhållande till behovet. Svaret på den frågan är i stor utsträckning beroende av hur metoden tekniskt kan utformas. Undersökningen ska utgå från de tekniska möjligheter som finns och beakta de svårigheter vid verkställighet som kan förutses. Frågan hur bearbetning av information som inhämtas genom metoden kan förväntas gå till kommer att ha betydelse liksom hur myndigheterna ska skaffa den tekniska förmåga som krävs för att använda metoden. Risken för att de personer som begår brott anpassar sitt beteende för att komma runt de nya övervakningsverktygen och hur det skulle påverka effektiviteten behöver beaktas. Även frågan om vilka resurser metoden förutsätter bör belysas.

Behovet och den förväntade effekten behöver vidare bedömas utifrån olika brott. Hemlig dataavläsning skulle kunna vara en effektiv metod för att bekämpa terroristbrottslighet. Det kan även finnas andra allvarliga brott som hemlig avlyssning av elektronisk kommunikation får användas mot och som är svåra att utreda utan tillgång till hemlig dataavläsning.

Behovet och den förväntade effekten behöver också belysas utifrån olika syften med åtgärden. Straffprocessuella tvångsmedel kan användas både i syfte att förhindra och att utreda brott. Behovet kan skilja sig mellan dessa användningsområden. Exempelvis har behovet av att kunna använda hemlig rumsavlyssning i preventivt syfte bedömts vara mindre än motsvarande behov för andra hemliga tvångsmedel (prop. 2013/14:237 s. 101). Hemlig avlyssning kan användas både för att förhindra och utreda brott medan hemlig rumsavlyssning enbart är tillåtet för att utreda brott inom ramen för en förundersökning. Behovet av den tänkta åtgärden kan också vara olika för olika brott. För effekten av tvångsmedlet är det vidare av betydelse vilka beviskrav som ska ställas på tvångsåtgärdens betydelse för det fastställda ändamålet med åtgärden.

Varje befogenhet för staten att bereda sig tillgång till information om medborgarna leder till ingrepp i den personliga integriteten. Ramarna för intrånget bestäms av hur befogenheten avgränsas och utformas i lag. En behörighet för brottsbekämpande myndigheter att i realtid hemligt läsa information i och från datorer och andra tekniska utrusningar, t.ex. mobiltelefoner, skulle potentiellt kunna innebära ett mycket omfattande intrång i enskildas privatliv. Vid överväganden om hemlig dataavläsning måste därför integritetseffekterna beskrivas noga. Det måste så långt det är möjligt redogöras för hur skyddet för den personliga integritetens kärnområden, dvs. sådant som rör individen och dennes personlighet, skulle påverkas av hemlig dataavläsning, bl.a. risken för att andra personer än den som är föremål för tvångsåtgärden påverkas. Regleringen av bland annat hur överskottsinformation får användas och hur tillsyn ska utföras spelar en viktig roll i denna bedömning. Behovet och den förväntade nyttan av att kunna använda hemlig dataavläsning för de olika syftena där ett behov har identifierats

måste vägas mot det förväntade integritetsintrånget av en sådan användning. Även frågor om hur metoden skulle påverka enskildas egendomsskydd när det gäller tekniska utrustningars lagringsutrymme (eventuella begränsningar i överföring av datamängd och kapacitet) och kostnader för enskilda behöver beaktas.

Oavsett hur avgränsningen mellan integritets- och effektivitetshänsyn utfaller är det ett ovillkorligt krav att de bestämmelser som föreslås uppfyller högt ställda krav på rättssäkerhet. Det finns därför anledning att noga analysera vilka kvalifikationskrav som är nödvändiga för tillämpningen, hur beslutsordningen bör se ut, hur efterhandskontroll och övrig tillsyn bör fungera, hur underrättelseskyldighet till enskilda bör utformas, hur jurisdiktionsreglerna kan upprätthållas och hur användningen av överskottsinformation ska regleras.

Utredaren ska

- ta reda på vilket behov de brottsbekämpande myndigheterna har av att hemligt i realtid bereda sig tillgång till information i datorer och andra tekniska utrustningar för att effektivt kunna fullgöra sin uppgift, bl.a. i förhållande till övriga metoder för att bekämpa brott inklusive övriga (hemliga) tvångsmedel, och vid analysen särredovisa Åklagarmyndighetens, Ekobrottsmyndighetens, Polismyndighetens, Säkerhetspolisens och Tullverkets behov,
- undersöka vilka möjligheter som modern teknik kan ge de brottsbekämpande myndigheterna att i realtid i hemlighet läsa information i datorer och andra tekniska utrustningar och vilka begränsningar som följer av tekniken och av möjligheten att använda motmedel mot en sådan åtgärd,
- kartlägga och med beaktande av eventuell sekretess beskriva hur en sådan metod kan förväntas verkställas och avbrytas eller avslutas inklusive de operativa svårigheterna med detta,
- analysera i vilken utsträckning det kan bidra till en effektiv brottsbekämpning att ge brottsbekämpande myn-

digheter befogenhet att i realtid i hemlighet läsa information i datorer och andra tekniska utrustningar,

- undersöka vilket integritetsintrång detta skulle medföra för enskilda och beskriva vilka avgränsningar som behövs,
- utifrån en avvägning mellan effektivitets- och integritetsskäl ta ställning till om de brottsbekämpande myndigheterna bör ges möjlighet att använda hemlig dataavläsning för att bekämpa terroristbrottslighet och andra allvarliga brott, som i dag ger möjlighet till hemlig avlyssning av elektronisk kommunikation,
- avgöra de närmare förutsättningarna för en sådan användning bl.a. i fråga om syfte, tillämpningsområde och rättssäkerhetsgarantier i enlighet med Europakonventionen och den praxis som Europeiska domstolen för de mänskliga rättigheterna har utvecklat,
- ta ställning till i vilken utsträckning åtgärden ska kunna användas i det internationella rättsliga samarbetet, och
- lämna förslag till författningsändringar eller andra förändringar oavsett vad analysen föranleder.

Vid utarbetandet av lagförslag ska utredaren så långt som det är möjligt välja en teknikneutral reglering. Uppgifter i utredningen ska redovisas med beaktande av eventuell sekretess. Utredaren är fri att lämna sådana närliggande förslag till författningsändringar som bedöms vara nödvändiga.

Ekonomiska konsekvenser

Utredaren ska bedöma de ekonomiska konsekvenserna av förslagen för staten, kommuner och landsting och konsekvenserna i övrigt av förslagen. Om förslagen förväntas leda till kostnadsökningar för staten, kommuner och landsting, ska utredaren föreslå hur dessa ska finansieras. Utredaren ska också redovisa i vilken utsträckning resursutnyttjandet i rättsväsendet kan bli effektivare genom förslagen.

Lagstiftning i andra länder

Utredaren ska redovisa gällande rätt och eventuellt pågående arbete i övriga nordiska länder samt de övriga länder som bedöms vara relevanta för utredningsuppdraget och i övrigt göra de internationella jämförelser som utredaren bedömer befogade.

Samråd och redovisning

Utredaren ska vid genomförande av uppdraget inhämta upplysningar från företrädare för berörda myndigheter och organ, särskilt Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Säkerhets- och integritetsskyddsnämnden, Post- och telestyrelsen och Sveriges advokatsamfund.

Utredaren ska också hålla sig informerad om och beakta sådant arbete inom Regeringskansliet samt inom EU och andra internationella forum som är relevant för uppdraget. Utredaren ska särskilt uppmärksamma det pågående arbetet inom ramen för utredningen om moderna regler om beslag och husrannsakan (dir. 2016:20) och samordna sina bedömningar med den utredningen i den utsträckning det behövs.

Uppdraget ska redovisas senast den 13 november 2017.

(Justitiedepartementet)