

Kommittédirektiv

Utvärdering av hemlig dataavläsning

Beslut vid regeringssammanträde den 22 juni 2022

Sammanfattning

En särskild utredare ska utvärdera lagen (2020:62) om hemlig dataavläsning inför ett ställningstagande till om den bör permanentas och om den i så fall bör ändras i något avseende. Genom lagen, som trädde i kraft den 1 april 2020, infördes ett nytt hemligt tvångsmedel som de brottsbekämpande myndigheterna kan använda vid misstankar om allvarlig brottslighet. Lagen är tidsbegränsad till utgången av mars 2025.

Utredaren ska bland annat

- analysera nyttan och behovet av hemlig dataavläsning,
- ta ställning till om lagstiftningen bör permanentas och föreslå de åtgärder som behövs för ett permanentande,
- analysera om lagstiftningen har fått en ändamålsenlig och proportionerlig utformning eller om det behövs förändringar i regelverket, och
- lämna förslag på de författningsändringar och andra åtgärder som bedöms nödvändiga.

Uppdraget ska redovisas senast den 1 december 2023.

Hemlig dataavläsning – ett efterfrågat verktyg i kampen mot allvarlig brottslighet

Den 1 april 2020 fick de brottsbekämpande myndigheterna ett nytt verktyg, hemlig dataavläsning. Verktöget ger utökade möjligheter att komma åt information som tidigare inte har varit tillgänglig, till exempel på grund av kryptering. I praktiken handlar hemlig dataavläsning om att de brottsbekämpande myndigheterna med hjälp av tekniska hjälpmedel i hemlighet får samla in uppgifter från en dator, en mobiltelefon, ett användarkonto på internet eller något annat informationssystem. Tvångsmedlet får – under vissa förutsättningar – användas under en förundersökning, i underrättelseverksamhet och vid särskild utlänningskontroll, liksom i det internationella straffrättsliga samarbetet.

Vid införandet av hemlig dataavläsning konstaterades att det finns ett påtagligt behov av bättre metoder för att i hemlighet komma åt uppgifter som redan får hämtas in med befintliga tvångsmedel, men också för att kunna komma åt uppgifter som inte är möjliga att tillgå med befintliga verktyg. Det anmärktes att teknikutvecklingen, med bland annat ökad användning av kryptering och automatiska funktioner för radering av data, gjort det väsentligt svårare för de brottsbekämpande myndigheterna att komma åt elektronisk information. Förväntningarna var att hemlig dataavläsning skulle leda till betydligt bättre tillgång till information än befintliga verktyg. (Hemlig dataavläsning, prop. 2019/20:64 s. 69–83.)

Hemlig dataavläsning får endast användas vid misstankar om allvarlig brottslighet. Som huvudregel krävs att det är fråga om ett brott som har ett minimistraff om fängelse i två år. Som exempel på brott som uppfyller dessa krav kan nämnas grovt narkotikabrott, grovt vapenbrott, våldtäkt och mord. Tvångsmedlet får som huvudregel användas mot en utrustning eller ett användarkonto som kan knytas till en person med koppling till de misstankar som avses.

Regleringen av hemliga tvångsmedel har utformats efter en avvägning mellan å ena sidan samhällets behov av en effektiv brottsbekämpning till skydd för medborgarna och å andra sidan den enskildes rätt till privatliv, skydd för sin personliga integritet och rättssäkerhet i förhållande till staten. Liksom andra hemliga tvångsmedel innebär hemlig dataavläsning risker för enskildas personliga integritet och regelverket innehåller därför flera rättssäkerhetsgarantier. Förhandsprövning av domstol är en sådan. Huvudregeln är att

domstol prövar frågor om hemliga tvångsmedel innan de får användas och domstolen har dessutom möjlighet att ange närmare villkor för tvångsmedelsanvändningen i syfte att säkerställa att enskildas personliga integritet inte kränks i onödan.

Förutom den föregående prövningen av domstol finns olika former av tillsyn av både tvångsmedelsanvändningen och myndigheternas övriga verksamhet som utförs av Säkerhets- och integritetsskyddsämnden, Justitiekanslern, Riksdagens ombudsmän och Integritetsskyddsmyndigheten. En annan viktig grundsten är systemet med offentliga ombud, vilka har till uppgift att bevaka enskildas integritetsintressen. I likhet med vad som gäller för övriga hemliga tvångsmedel redovisas myndigheternas användning av hemlig dataavläsning årligen till riksdagen. Den parlamentariska kontrollen fyller en viktig funktion och bidrar till allmänhetens insyn i myndigheternas tvångsmedelsanvändning.

Reglerna om hemlig dataavläsning är införda i en särskild lag, lagen (2020:62) om hemlig dataavläsning. Eftersom det rör sig om en ny utredningsmetod, som förvisso förväntades vara effektiv men som också ansågs innebära vissa risker för den personliga integriteten, begränsades lagen till att gälla under fem år. En senare utvärdering av den tidsbegränsade lagen ansågs minimera risken för att lagen görs permanent utan ett fullgott underlag (prop. 2019/20:64 s. 99–101).

Uppdraget att utreda frågan om permanentande av hemlig dataavläsning

Brottsligheten har utvecklats och blivit mer samhällshotande. Även kriminellas handlingsätt och hur de kommunicerar är i förändring. Uppgifter om elektronisk kommunikation är många gånger helt avgörande för en framgångsrik brottsbekämpning. Samtidigt innebär den tekniska utvecklingen, liksom brotts- och samhällsutvecklingen i övrigt, att de brottsbekämpande myndigheterna inte längre kan ta del av många av de uppgifter som man tidigare fick del av genom användande av straffprocessuella tvångsmedel.

Sedan möjligheten till hemlig dataavläsning infördes har betydelsen av effektiv tillgång till elektronisk bevisning blivit än tydligare. Det visar inte minst framgångarna tack vare materialet från de krypterade kommunikationstjänsterna Encrochat, Sky ECC och Anom. Samtidigt innebär den

fortsatta teknik- och kommunikationsutvecklingen att det praktiska användningsområdet för hemlig avlyssning och hemlig övervakning av elektronisk kommunikation begränsas. Exempelvis kan införandet av den femte generationens mobilnät (5G) medföra tillämpning av krypterings- och autentiseringsprocesser som syftar till att höja säkerheten men samtidigt riskerar att väsentligt försvåra möjligheterna att verkställa hemliga tvångsmedel. Också förändrade tekniska förfaranden vid roaming riskerar att göra att enbart en mycket begränsad mängd information kan avläsas av operatören i det land som simkortet, och därmed användaren, befinner sig i, med följd att information som härrör från utländska simkort som används i Sverige blir otillgänglig för de brottsbekämpande myndigheterna. Inte bara kommunikationen i sig är föremål för kryptering, utan det sker också en utveckling av möjligheterna att kryptera innehållet i kommunikationsutrustning och lagringsmedier.

De brottsbekämpande myndigheterna har nu haft möjlighet att använda hemlig dataavläsning i drygt två år. Åklagarmyndigheten har, tillsammans med Ekobrottsmyndigheten, Polismyndigheten, Tullverket och Säkerhetspolisen, redovisat användningen av tvångsmedlet under 2020 och 2021. Av redovisningen kan slutsatsen dras att hemlig dataavläsning har kommit till användning i väsentligt större omfattning än vad som förutsetts. Åklagarmyndigheten har för 2020 redovisat att hemlig dataavläsning användes i 60 ärenden från och med 1 april då lagen trädde i kraft, vilket över ett helt år skulle motsvara 80 ärenden. För 2021 var motsvarande siffra 145. Vid lagens införande förväntades antalet verkställigheter, ej inräknat Säkerhetspolisens verksamhet, bli åtminstone 50 per år (Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet, SOU 2017:89 s. 283 f.). De brottsbekämpande myndigheternas erfarenheter av hemlig dataavläsning hittills har varit mycket goda. Polisen har även gett uttryck för att de skulle vilja använda verktyget i större omfattning.

Säkerhets- och integritetsskyddsnämnden granskar de brottsbekämpande myndigheternas användning av bland annat hemlig dataavläsning. I december 2021 lämnade nämnden sin första granskningsrapport om hemlig dataavläsning. Nämnden konstaterade att de grundläggande förutsättningarna för tvångsmedlet genomgående var uppfyllda i de granskade ärendena, liksom att det överlag var god ordning i den granskade tvångsmedelshanteringen. Nämnden anmärkte att det fanns ett par frågor som det fanns anledning att återkomma till, såsom att tillstånden till hemlig data-

avläsning i vissa fall innefattat långa tidsperioder och att det fanns tillstånd som inte förenats med villkor enligt 18 § 4 lagen om hemlig dataavläsning. Vidare ansåg nämnden att det inte är klart huruvida 2 § 7 lagen om hemlig dataavläsning medger inhämtning enbart av realtidsuppgifter eller också historiska uppgifter.

Mot denna bakgrund, och med hänsyn till lagens begränsade giltighetstid, bör en utredare nu utvärdera lagen om hemlig dataavläsning inför ett ställningstagande till om verktyget bör göras permanent och om det i så fall bör förändras i något avseende. Utvärderingen bör innefatta en noga avvägning av de olika intressen som berörs. Det är angeläget att de brottsbekämpande myndigheterna både nationellt och i det internationella samarbetet har tillgång till ändamålsenliga och verkningsfulla verktyg för att effektivt kunna utreda, förebygga och förhindra allvarlig brottslighet. Samtidigt innebär de brottsbekämpande myndigheternas användning av hemliga tvångsmedel ett ingrepp i den berördes personliga integritet i det enskilda fallet. Det är viktigt att förslag inom området kringgärdas av starka rättssäkerhetsgarantier och innehåller tydliga och strikta ramar som tillämparen har att hålla sig inom.

Utredaren ska därför

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

Utredaren ska bedöma behovet av följdändringar och säkerställa att en välfungerande systematik i regelverket kring såväl hemliga som öppna tvångsmedel upprätthålls. Utredaren har även möjlighet att överväga andra frågor som har samband med de frågeställningar som ska utredas.

I och med att lagen gäller till utgången av mars 2025 behöver eventuella åtgärder för ett permanentande kunna genomföras dessförinnan.

Konsekvensbeskrivningar

Utredaren ska bedöma och redogöra för förslagets ekonomiska konsekvenser och konsekvenser i övrigt för enskilda, företag och det allmänna samt redogöra för förslagets samhällsekonomiska effekter. Utredaren ska särskilt beskriva vilka konsekvenser de förslag som lämnas har för det nationella och internationella skyddet för grundläggande fri- och rättigheter, såsom den personliga integriteten. De offentligfinansiella effekterna av förslagen ska beräknas, och om förslagen kan förväntas leda till offentligfinansiella kostnader ska utredaren föreslå hur dessa ska finansieras.

Kontakter och redovisning av uppdraget

Utredaren ska föra dialog med och inhämta upplysningar från Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Säkerhets- och integritetsskyddsnämnden, Integritetsskyddsmyndigheten, Post- och telestyrelsen och Sveriges advokatsamfund, men även med andra myndigheter och berörda aktörer, såsom civilsamhället, i den utsträckning som utredaren finner det lämpligt.

Utredaren ska också hålla sig informerad om och beakta relevant arbete som pågår inom Regeringskansliet och inom utredningsväsendet. Utredaren ska beakta utvecklingen vid såväl EU:s lagstiftande institutioner som EU-domstolen, Europadomstolen och Europarådet.

Utredaren ska påbörja sitt arbete den 1 september 2022. Uppdraget ska redovisas senast den 1 december 2023.

(Justitiedepartementet)