Kommittédirektiv

Datalagring vid brottsbekämpning – ytterligare åtgärder för en modern och ändamålsenlig reglering

Beslut vid regeringssammanträde den 5 augusti 2021

Sammanfattning

En särskild utredare ska se över den lagstiftning som medför en skyldighet för tillhandahållare av elektroniska kommunikationstjänster att lagra uppgifter om elektronisk kommunikation för brottsbekämpande syften, samt vissa anknytande frågor om myndigheternas tillgång till sådana uppgifter. Uppdraget syftar till att säkerställa att de brottsbekämpande myndigheternas tillgång till information förbättras och upprätthålls över tid i takt med teknikutvecklingen och förändrade kommunikationsvanor, samtidigt som respekten för mänskliga rättigheter säkerställs.

Utredaren ska bl.a.

- analysera förutsättningarna för att leverantörer av s.k. OTT-tjänster ska kunna omfattas av skyldigheten att lagra och ge tillgång till uppgifter om elektronisk kommunikation samt ta ställning till om en sådan skyldighet bör införas,
- analysera och föreslå moderniseringar av regleringen när det gäller tjänsteleverantörers skyldighet att anpassa sin verksamhet så att hemliga tvångsmedel kan verkställas på ett effektivt sätt,
- analysera och utvärdera nuvarande reglering om lagring av och tillgång till uppgifter om elektronisk kommunikation i förhållande till bl.a. ny praxis från EU-domstolen och ta ställning till om regelverket behöver förändras, och
- analysera vissa frågor om jurisdiktion, inklusive folkrättsliga överväganden, i förhållande till elektronisk information som finns eller kan finnas utanför Sverige och ta ställning till om det bör införas en särskild lagreglering för exekutiv jurisdiktion.

Utredaren ska föreslå de författningsändringar och andra åtgärder som behövs.

Uppdraget ska redovisas senast den 6 februari 2023.

Behovet av åtgärder

Teknikutvecklingen och nya kommunikationsvanor leder till en förändrad spelplan

De brottsbekämpande myndigheterna behöver ha tillgång till ändamålsenliga och verkningsfulla verktyg för att kunna förhindra, upptäcka, utreda och lagföra brott. Brottsligheten är i förändring, liksom kriminellas handlingssätt och hur de kommunicerar. Detta har medfört att de brottsbekämpande myndigheternas behov av att kunna använda hemliga tvångsmedel har ökat. Brott som begås inom ramen för kriminella nätverk är ofta svåra att utreda eftersom brottsoffer och vittnen av olika anledningar kan vara obenägna att lämna information till de brottsbekämpande myndigheterna. Tillgång till information och bevisning från elektroniska kommunikationer är ofta av stor betydelse i utredningar av allvarlig brottslighet. Också brottslighet som begås över internet är till sin natur sådan att uppgifter om elektroniska kommunikationer i regel är avgörande för utredningens framgång.

Den tekniska utvecklingen och nya kommunikationsmönster har gjort att mycket av den information som tidigare varit tillgänglig för brottsbekämpande myndigheter inte längre går att komma åt. Det blir allt vanligare att kommunikation sker genom tjänster som inte omfattas av någon rättslig skyldighet att lagra och tillhandahålla uppgifter, nämligen via tjänster som tillhandahålls av andra än de traditionella teleoperatörerna. Sådana tjänster kallas OTT-tjänster (over the top) eller nummeroberoende interpersonella kommunikationstjänster. Exempel på OTT-tjänster är Apple Imessage och Facetime, Facebook Messenger och Whatsapp.

Användningen av de tjänster som direkt tillhandahålls av teleoperatörerna – främst telefonsamtal och sms – har minskat till förmån för kommunikation genom tjänster som tillhandahålls av andra än operatörerna, men vars information överförs genom bland annat teleoperatörernas nät. Enligt statistik från Post- och telestyrelsen ökade användningen av sms till och med 2010, då det genomsnittliga antalet sms som skickades från mobiltelefon per samtalsabonnemang och månad var 139, för att därefter minska. År 2020 uppgick det genomsnittliga antalet till 44. Enligt en rapport från en arbetsgrupp vid Europaparlamentet förväntades OTT-tjänster stå för närmare 90 procent av alla elektroniska kommunikationsmeddelanden 2020 (Directorate-General for Internal Policies, Over-the-Top players [OTTs], Study for the IMCO Committee, 2015, s. 43).

Det pågår även en utveckling av de tjänster som tillhandahålls av teleoperatörerna, som kan komma att påverka de brottsbekämpande myndigheternas verktyg. Införandet av 5G kan till exempel medföra tillämpning av krypterings- och autentiseringsprocesser som

riskerar att väsentligt försvåra möjligheterna att verkställa hemliga tvångsmedel. Den standard för roaming som kan bli aktuell riskerar också att försvåra eller omöjliggöra verkställande av hemlig avlyssning och hemlig övervakning av utländska abonnemang i Sverige.

Information lagras allt oftare på andra platser än hos användaren och inte sällan utomlands. Informationen kan ständigt förflyttas eller finnas på flera platser samtidigt, vilket gör det omöjligt att bestämma en specifik plats där informationen finns. Den traditionella tolkningen av territorialitetsprincipen har inneburit att informationens fysiska belägenhet är avgörande för om brottsbekämpande myndigheter har jurisdiktion att hämta in den. Tolkningen gjordes innan informationssamhället antog sin nuvarande form och är alltså inte anpassad för dagens tekniska verklighet. Internationellt går fler länder mot att andra anknytningsmoment får betydelse för jurisdiktionen, såsom den misstänktes hemvist, platsen där brottet begåtts eller hemvistet för den som förfogar över användarkontot. För en effektiv brottsbekämpning är det viktigt att reglerna om tillgång till elektronisk kommunikation och annan elektronisk bevisning också kan tillämpas i praktiken, även när informationen finns utanför Sverige eller det är okänt var den finns. Det finns därför skäl att överväga om det, med beaktande av folkrättsliga aspekter, bör lagstiftas om exekutiv jurisdiktion som baseras på andra anknytningsfaktorer än den plats där informationen lagras.

Regleringen behöver anpassas efter de brottsbekämpande myndigheternas behov i den nya tekniska verkligheten

De hemliga tvångsmedlen utgörs bl.a. av hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation. De båda tvångsmedlen får användas såväl under en förundersökning som innan en förundersökning har inletts, dvs. i underrättelseverksamhet. Dessa tvångsmedel regleras i rättegångsbalken (RB), lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen) och lagen (1991:572) om särskild utlänningskontroll (LSU). Även lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen) har regler om inhämtning av uppgifter om elektronisk kommunikation i underrättelseverksamhet. Hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation kan också aktualiseras inom ramen för Sveriges internationella samarbete enligt lagen (2017:1000) om en europeisk utredningsorder och lagen (2000:562) om internationell rättslig hjälp i brottmål.

Bestämmelserna om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation i rättegångsbalken är i sig teknikneutrala och således inte begränsade till en viss typ av teknik för att befordra meddelanden. Enligt

reglerna får meddelanden avlyssnas eller övervakas om de överförs eller har överförts i ett elektroniskt kommunikationsnät till eller från ett telefonnummer eller annan adress. Huruvida det är fråga om fast telefoni, mobiltelefoni eller kommunikation över internet har alltså ingen betydelse för frågan om meddelandet som sådant faller under tvångsmedelsregleringen.

Det svenska regelverket för elektronisk kommunikation finns huvudsakligen i lagen (2003:389) om elektronisk kommunikation (LEK). De tjänsteleverantörer som i dag omfattas av regelverket är framför allt traditionella teleoperatörer. I lagen om elektronisk kommunikation finns bl.a. bestämmelser om hur tjänsteleverantörerna ska lagra viss information samt anpassa sin verksamhet så att hemliga tvångsmedel kan verkställas. Tjänsteleverantörerna har också en skyldighet att lämna ut vissa s.k. abonnemangsuppgifter till olika myndigheter för vissa ändamål, t.ex. till brotts-bekämpande myndigheter vid misstanke om brott.

Genom propositionen Datalagring vid brottsbekämpning – anpassningar till EU-rätten (prop. 2018/19:86) trädde den 1 oktober 2019 nya regler om datalagring i kraft. Ändringarna innebär bl.a. att lagringens omfattning har begränsats och att lagringstiderna har differentierats. I förarbetena uttalade regeringen att det senast inom fyra år efter ikraftträdandet kunde finnas anledning att se över de föreslagna ändringarna, bl.a. mot bakgrund av den tekniska utvecklingen, ändrade kommunikationsvanor och nya mål om datalagring i EU-domstolen (samma prop. s. 38 och 108). Som beskrivits inledningsvis har teknikutvecklingen och kommunikationsvanorna förändrat de brottsbekämpande myndigheternas förutsättningar påtagligt. I oktober 2020 kom också EU-domstolen med nya avgöranden på området. Mot denna bakgrund finns det skäl att redan nu inleda den aviserade översynen av regelverket.

Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation (e-kodexdirektivet) ska genomföras i Sverige. Genom e-kodexdirektivet inrättas ett harmoniserat ramverk för bl.a. elektroniska kommunikationsnät och tjänster. En nyhet är att definitionen av elektroniska kommunikationstjänster utvidgas till att även omfatta OTT-tjänster. För att genomföra direktivet pågår ett arbete med att ta fram ett förslag till en ny lag som ska ersätta den nuvarande lagen om elektronisk kommunikation. Promemorian Genomförande av direktivet om inrättande av en kodex för elektronisk kommunikation har tagits fram inom Regeringskansliet och remitterats. Promemorians lagförslag omfattar, liksom e-kodexdirektivet, i vissa delar OTT-tjänster. Frågorna om lagrings-skyldighet, anpassningsskyldighet och skyldighet att lämna ut uppgifter behandlas dock inte i e-kodexdirektivet. Lagförslaget innebär därför inte någon skyldighet för de som tillhandahåller OTT-tjänster att lagra eller ge tillgång till uppgifter om elektronisk kommunikation för brottsbekämpande syften. Det finns därför anledning att se över regelverket för att förbättra de brottsbekämpande myndigheternas möjligheter att utföra

sina uppdrag. Med hänsyn till den snabba tekniska utvecklingen är det angeläget att regleringen, så långt det är möjligt, är teknikneutral för att kunna stå sig över tid.

Utredaren bör överväga hur brottsbekämpningens behov kan mötas på ett sätt som säkerställer mänskliga rättigheter och rättssäkerheten

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 och rättssäkerhet i förhållande till staten.

Regeringsformen (RF) garanterar den enskilde ett skydd i förhållande till det allmänna mot bl.a. husrannsakan och liknande intrång, hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande. Skyddet omfattar även betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden (2 kap. 6 § RF). Dessa grundläggande fri- och rättigheter får begränsas endast genom lag och endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Begränsningarna får aldrig gå utöver vad som är nödvändigt eller utgöra ett hot mot den fria åsiktsbildningen (2 kap. 20 och 21 §§ RF).

Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) är inkorporerad i svensk lag. Enligt artikel 8.1 i Europakonventionen har var och en rätt till skydd för sitt privat- och familjeliv, sitt hem och sin korrespondens, vilket bl.a. omfattar skydd mot övervakning i olika former. Tvångsmedel som innefattar ingrepp i området som artikel 8 skyddar kan enligt konventionen endast godtas om de har stöd i lag och omfattas av de undantag som anges i artikel 8.2. Undantagen avser t.ex. åtgärder som i ett demokratiskt samhälle är nödvändiga för att upprätthålla den allmänna säkerheten och för att förebygga brott. Artikel 8 innebär också att staten har ett ansvar för att skydda enskildas privatliv och personliga integritet mot intrång som begås av andra enskilda. En förutsättning för att staten ska kunna leva upp till kravet på att upprätthålla rättstryggheten för enskilda är att det finns en väl fungerande och effektiv brottsbekämpning.

EU:s stadga om de grundläggande rättigheterna gäller när unionsrätten utformas och tillämpas. Enligt artikel 7 i stadgan har var och en rätt till respekt för sitt privatliv och familjeliv, sin bostad och sina kommunikationer. Vidare anges i artikel 8 att var och en har rätt till skydd av de personuppgifter som rör honom eller henne. I det sammanhanget kan tekniska skyddslösningar såsom kryptering vara en viktig faktor för att säkerställa skyddet av mänskliga rättigheter.

FN:s konvention om barnets rättigheter (barnkonventionen) är inkorporerad i svensk lag. Enligt artikel 16 får inget barn utsättas för godtyckliga eller olagliga ingripanden i sitt privat- och familjeliv, sitt hem eller sin korrespondens och inte heller för olagliga angrepp

på sin heder och sitt anseende. Vidare framgår av artikel 3 i barnkonventionen att vid samtliga åtgärder och beslut som rör barn ska i första hand beaktas vad som bedöms vara barnets bästa. Enligt artikel 19 ska barn skyddas från alla former av fysiskt eller psykiskt våld, inklusive misshandel, utnyttjande och sexuella övergrepp. Det ska finnas effektiva medel för bl.a. förebyggande, identifiering, undersökning och uppföljning samt förfaranden för rättsligt ingripande om barn farit illa.

För all tvångsmedelsanvändning gäller ändamålsprincipen, behovsprincipen och proportionalitetsprincipen. Ändamålsprincipen innebär att en myndighets befogenhet att använda ett tvångsmedel ska vara bundet till det ändamål för vilket tvångsmedlet har beslutats. Enligt behovsprincipen får en myndighet använda ett tvångsmedel bara när det finns ett påtagligt behov av det och en mindre ingripande åtgärd inte är tillräcklig. Proportionalitetsprincipen innebär att ett tvångsmedel får användas endast om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den misstänkte eller något annat motstående intresse.

Regelverket om hemliga tvångsmedel innehåller även 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 utöver vad som är nödvändigt. Förutom den föregående prövningen av domstol finns olika former av tillsyn som genomförs av Säkerhets- och integritetsskyddsnämnden, Justitiekanslern, Riksdagens ombudsmän och Integritetsskyddsmyndigheten.

De brottsbekämpande myndigheternas befogenheter att med stöd av hemliga tvångsmedel bereda sig tillgång till information om en enskild innebär ett ingrepp i den enskildes personliga integritet.

Utredaren ska därför

- noga väga behovet av en effektiv brottsbekämpning mot den enskildes rätt till skydd för sin personliga integritet,
- analysera förslagens påverkan på skyddet för mänskliga rättigheter, inklusive rätten till respekt för privatlivet,
- ta ställning till om skyddet för privat- och familjelivet respektive den personliga integriteten bör stärkas, och
- se till att de förslag som lämnas uppfyller högt ställda krav på rättssäkerhet.

Uppdraget att modernisera förutsättningarna för datalagring och åtkomst till data från OTT-tjänster

Hemlig övervakning av elektronisk kommunikation och datalagringens praktiska betydelse

Med stöd av bl.a. 27 kap. 19 § RB kan hemlig övervakning av elektronisk kommunikation tillåtas under vissa förutsättningar. Genom hemlig övervakning av elektronisk kommunikation kan brottsbekämpande myndigheter inom ramen för en förundersökning få tillgång till bl.a. information om meddelanden (annat än innehållet), vilka elektroniska kommunikationsutrustningar som varit i ett visst område vid ett visst tillfälle och i vilket område en viss elektronisk kommunikationsutrustning finns eller har funnits. Också lagen om särskild utlänningskontroll och preventivlagen medger användning av hemlig övervakning av elektronisk kommunikation genom hänvisningar till rättegångsbalkens bestämmelser.

Utöver tvångsmedelsregleringen i rättegångsbalken finns det i inhämtningslagen bestämmelser som ger Polismyndigheten, Säkerhetspolisen eller Tullverket möjlighet att i underrättelseverksamhet hämta in uppgifter från den som enligt lagen om elektronisk kommunikation tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst. Det gäller bl.a. uppgifter om meddelanden som i ett elektroniskt kommunikationsnät har överförts till eller från ett telefonnummer eller annan adress.

Myndigheternas faktiska möjligheter att komma framåt med sitt arbete för att förhindra, upptäcka, utreda och lagföra brottslighet med hjälp av bl.a. hemlig övervakning av elektronisk kommunikation är beroende av att uppgifterna som behövs finns lagrade hos en aktör som går att nå med hjälp av tvångsmedlet. Av denna anledning finns det regler som innebär en skyldighet för teleoperatörer att lagra uppgifter om elektronisk kommunikation, s.k. datalagring.

Enligt 6 kap. 16 a § LEK ska den som bedriver ett allmänt kommunikationsnät av sådant slag som vanligen tillhandahålls mot ersättning eller en allmänt tillgänglig elektronisk kommunikationstjänst lagra uppgifter som behövs för brottsbekämpande verksamhet. Skyldigheten omfattar uppgifter som är nödvändiga för att spåra och identifiera kommunikationskällan, slutmålet för kommunikationen, datum, tidpunkt och varaktighet för kommunikationen, typ av kommunikation, kommunikationsutrustning samt lokalisering av mobil kommunikationsutrustning vid kommunikationens början och slut. Någon skyldighet att lagra innehållet i en kommunikation finns inte.

OTT-tjänster omfattas för närvarande inte av begreppet elektronisk kommunikationstjänst och att tillhandahålla en OTT-tjänst är inte heller att betrakta som bedrivande av ett allmänt kommunikationsnät. Sådana tjänsteleverantörer har således inte någon lagringsskyldighet enligt gällande rätt.

I 6 kap. 20 § första stycket 1 LEK föreskrivs tystnadsplikt för den som i samband med tillhandahållande av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst har fått del av eller tillgång till s.k. abonnemangsuppgifter. Med abonnemangsuppgifter avses t.ex. uppgifter om abonnentens nummer, namn, titel och adress (prop. 1992/93:200 s. 164). Vidare har det ansetts innefatta ip-adresser och IMSI-nummer, vilket är ett nummer som är kopplat till abonnentens simkort och därmed telefonnummer (se t.ex. prop. 2011/12:55 s. 101 och Kammarrätten i Stockholms dom den 19 januari 2010 i RK 2010:1). Post- och telestyrelsen har inom ramen för sin tillsyn av skyldigheten att lämna ut uppgifter om IMEI-nummer till brottsbekämpande myndigheter bedömt att uppgifter om IMEI-nummer är att anse som uppgift om abonnemang, när det tydligt framgår av begäran att syftet är att identifiera ett abonnemang eller en abonnent. I 6 kap. 22 § LEK finns bestämmelser som anger under vilka förutsättningar som abonnemangsuppgifter ska lämnas ut till vissa myndigheter och regionala alarmeringscentraler. Utlämnande av abonnemangsuppgifter får exempelvis ske i brottsbekämpande syfte, för att kunna delge personer som håller sig undan eller för att leta efter försvunna personer vars liv eller hälsa är i fara. I det sistnämnda syftet kan även annan uppgift som angår ett särskilt elektroniskt meddelande lämnas ut.

Skyldigheten att lämna ut abonnemangsuppgifter m.m. gäller den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst. Eftersom OTT-tjänster i dag inte omfattas av begreppet elektronisk kommunikationstjänst i lagen om elektronisk kommunikation kan myndigheterna inte, med stöd av den bestämmelsen, få ut information om t.ex. vem som är avsändare av ett meddelande från en sådan tjänsteleverantör.

Utredaren bör se över regelverket i förhållande till OTT-tjänster

Det är angeläget att teknikutvecklingen och ändrade kommunikationsvanor inte innebär försämrade möjligheter för de brottsbekämpande myndigheternas arbete. Som framgått ovan ska, med anledning av genomförandet av e-kodexdirektivet, definitionen av elektronisk kommunikationstjänst enligt det remitterade förslaget till ny lag om elektronisk kommunikation vara vidare än i dag och kommer att omfatta de s.k. OTT-tjänsterna. När det gäller lagringsskyldigheten och skyldigheten att lämna ut abonnemangsuppgifter och annan uppgift som angår ett särskilt elektroniskt meddelande föreslås, på grund av e-kodexdirektivets omfattning, att bestämmelserna ska föras över till den nya lagen utan ändring i sak. Detta innebär att något ställningstagande till frågan om lagring och utlämnande av uppgifter från OTT-tjänsteleverantörer inte görs inom ramen för det lagstiftningsprojektet. Även vad gäller inhämtningslagen föreslås att bestämmelserna ska ha samma tillämpningsområde som hittills. Det innebär att också förutsättningarna att hämta in uppgifter enligt inhämtningslagen kvarstår oförändrade i förhållande till OTT-tjänster. Polismyndigheten, Säkerhetspolisen och Åklagar-myndigheten har, i sina remissvar med anledning av förslaget till ny lag om elektronisk

kommunikation, uppgett att den tekniska utvecklingen och ändrade kommunikationsvanor medför att det är mycket angeläget att frågan utreds och att OTT-tjänster bör omfattas av regleringen. Ekobrottsmyndigheten har framfört liknande synpunkter. Det finns således behov av att modernisera lagstiftningen i syfte att även OTT-tjänsteleverantörer ska omfattas av skyldigheterna att lagra och lämna ut uppgifter om elektroniska kommunikationer. En sådan modernisering skulle innebära att brotts-bekämpande myndigheter kan förbättra möjligheterna att komma åt uppgifter om elektronisk kommunikation som de på grund av teknikutvecklingen och ändrade kommunikationsvanor har förlorat.

Utöver ovannämnda skyldigheter att lagra och lämna ut uppgifter finns flera bestämmelser i lagen om elektronisk kommunikation som kan vara av betydelse för att OTT-tjänster ska omfattas av regelverket på ett konsekvent sätt, såsom krav på säkerhet (6 kap. 3–4 b §§ LEK), tystnadsplikt (6 kap. 20–23 §§), villkor för behandling (6 kap. 5–10 a §§) och föreläggande att bevara elektronisk information (6 kap. 16 g §). I lagen (2020:62) om hemlig dataavläsning finns också bestämmelser om medverkansskyldighet och tystnadsplikt (24 och 32 §§). Utredaren bör även se över hur dessa bestämmelser ska förhålla sig till OTT-tjänsteleverantörer.

Hur vissa EU-rättsliga termer förhåller sig till nationella termer kan även behöva klarläggas. Ett exempel på detta är hur det EU-rättsliga begreppet ”trafikuppgift” förhåller sig till begreppet ”annan uppgift som angår ett särskilt elektroniskt meddelande” som finns i 6 kap. 20 § LEK (som flera andra bestämmelser hänvisar till), samt den närmare omfattningen av begreppet abonnemangsuppgifter i förhållande till exempelvis s.k. NAT-teknik, där många användare kan dela på samma ip-adress.

I kommissionens förslag till en förordning om tillgång till e-bevisning (COM(2018) 225) finns också vissa förslag som har koppling till frågan om tillgång till uppgifter från bl.a. OTT-tjänsteleverantörer. I förordningen föreslås införande av s.k. europeiska utlämnandeordrar som kommer att medföra en möjlighet för en rättslig myndighet i en medlemsstat att utfärda en order om utlämnande av elektronisk bevisning mot en tjänsteleverantör i en annan medlemsstat. I förordningen föreslås ingen skyldighet för tjänsteleverantörer att lagra data. Däremot finns förslag till s.k. europeiska bevarande-ordrar. De innebär att en rättslig myndighet i en medlemsstat kan beordra en tjänste-leverantör i en annan medlemsstat att under en viss tid bevara vissa uppgifter medan en framställan om utlämnande av de aktuella uppgifterna tas fram. Även om förordningen som sådan kommer att vara direkt tillämplig i Sverige kan den medföra behov av en översyn av svensk rätt, innefattande de regler som nu blir föremål för utredning. Det är därför viktigt att utredaren bevakar utvecklingen i dessa förhandlingar och eventuellt kommande lagstiftningsprojekt.

Utredaren ska därför

- analysera förutsättningarna, även ur ett tekniskt perspektiv, för att OTT-tjänsteleverantörer ska kunna omfattas av skyldigheterna att lagra och lämna ut uppgifter om elektroniska kommunikationer, och
- lämna förslag på de författningsändringar och andra åtgärder som bedöms nödvändiga.

Uppdraget att modernisera anpassningsskyldigheten

De tjänsteleverantörer som enligt lagen om elektronisk kommunikation tillhandahåller allmänna kommunikationsnät eller elektroniska kommunikationstjänster spelar en viktig roll när brottsbekämpande myndigheter hämtar in elektronisk kommunikation och uppgifter om sådan. För att underlätta för de brottsbekämpande myndigheterna har tjänsteleverantörerna ålagts vissa skyldigheter. I 6 kap. 19 § LEK föreskrivs den s.k. anpassningsskyldigheten. Enligt denna bestämmelse ska verksamheten bedrivas så att beslut om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation kan verkställas och att det kan ske på ett sådant sätt att verkställandet inte röjs. Innehållet i och uppgifter om avlyssnade eller övervakade meddelanden ska göras tillgängliga så att informationen enkelt kan tas om hand. Bestämmelserna om anpassningsskyldighet är i praktiken ofta en förutsättning för att beslut om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation över huvud taget ska kunna verkställas och att verkställandet kan ske i nära anslutning till tvångsmedelsbeslutet.

Anpassningsskyldigheten gäller i fråga om uppgifter som hämtas in efter beslut om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation med stöd av rättegångsbalken, inhämtningslagen, preventivlagen eller lagen om särskild utlänningskontroll.

Det finns också särskilda regler om anpassning för utlämnande för den som är skyldig att lagra uppgifter enligt 6 kap. 16 a § LEK. Även här gäller att uppgifterna ska göras tillgängliga på ett sådant sätt att informationen enkelt kan tas om hand (se 6 kap. 16 f §). Anpassningsskyldigheten enligt 6 kap. 16 f och 19 §§ gäller emellertid endast för vissa särskilt angivna verksamheter och träffar i huvudsak traditionella telekomleverantörer. De omfattar inte t.ex. OTT-tjänsteleverantörer. Det inbördes förhållandet mellan lagrings- och anpassningsskyldigheten kan också leda till tolkningsproblem. Lagringsskyldigheten omfattar i dag fler tjänsteleverantörer än de som är anpassningsskyldiga enligt 6 kap. 19 § LEK. Detta eftersom lagringsskyldigheten inte, såsom anpassningsskyldigheten, är begränsad vad gäller telefonitjänster till att avse samtal inom en nationell eller internationell nummerplan. Lagringsskyldigheten innehåller inte heller några begränsningar vad gäller tjänster för datakommunikation. Det kan t.ex. innebära att internetleverantörer som inte tillhandahåller telefonitjänster kan omfattas av lagringsskyldigheten enligt 6 kap. 16 a § utan att omfattas av anpassningsskyldigheten i 6 kap. 19 §.

I juni 2020 överlämnades departementspromemorian Registrering av kontantkort, m.m. (Ds 2020:12). I promemorian föreslås, utöver registrering av kontantkort, bl.a. en omarbetning av anpassningsskyldigheten i 6 kap. 19 § andra stycket LEK på så sätt att uppgifter som lämnas ut till brottsbekämpande myndigheter ska ordnas och göras tillgängliga i ett format som gör det möjligt att enkelt ta hand om dem. När det gäller bestämmelserna om anpassningsskyldighetens omfattning i 6 kap. 19 § första stycket LEK konstaterar utredaren att den teknikutveckling som pågått länge och som fortfarande pågår innebär att bestämmelsen blivit oklar och ålderdomlig samt att det vore önskvärt att bestämmelsen förtydligades och formulerades på ett så teknikneutralt sätt som möjligt. Utredaren anser också att det vore lämpligt att utforma bestämmelserna om anpassningsskyldighet i 6 kap. 19 § första stycket och lagringsskyldighet enligt 6 kap. 16 a § så att de träffar samma aktörer, men lämnar inget förslag i denna del. I sina remissvar med anledning av promemorian har Polismyndigheten, Säkerhetspolisen, Tullverket och Post- och telestyrelsen uttalat att det är angeläget att frågan blir föremål för utredning. Promemorian bereds inom Regeringskansliet.

Som framgår ovan ska definitionen av elektronisk kommunikationstjänst enligt det remitterade förslaget till ny lag om elektronisk kommunikation vara vidare än i dag och även omfatta OTT-tjänster. När det gäller anpassningsskyldigheten föreslås att dessa bestämmelser ska föras över till den nya lagen utan ändring i sak. Därför kvarstår de oklarheter som påpekas i promemorian Registrering av kontantkort, m.m.. Det är angeläget att anpassningsskyldighetens omfattning är tydlig, modern och anpassad efter brottsbekämpningens behov. Det bör därför utredas hur anpassningsskyldighetens utformning bör se ut framöver och om OTT-tjänster kan omfattas av denna skyldighet.

Därtill behöver det utredas om introduktionen av 5G medför behov av förändringar av anpassningsskyldigheten. 5G kan exempelvis medföra tillämpningar av flera krypterings- och autentiseringsprocesser som riskerar att väsentligt försvåra möjligheten att verkställa hemliga tvångsmedel. Bland annat har 5G en inbyggd möjlighet till så kallad totalsträckskryptering (eng. end-to-end encryption, E2EE). Totalsträckskryptering skulle väsentligt försvåra för brottsbekämpande myndigheter att få tillgång till elektronisk kommunikation trots domstolsbeslut om tillstånd till hemlig övervakning av elektronisk kommunikation eller hemlig avlyssning av elektronisk kommunikation. Det kommer också vara möjligt att kryptera IMSI-nummer i 5G-nätet. Detta skulle göra det närmast omöjligt för brottsbekämpande myndigheter att identifiera enskilda enheter eller var vissa personer, såsom misstänkta gärningsmän, befinner sig. Kringinformation (metadata) som normalt är tillgänglig via hemlig övervakning av elektronisk kommunikation – såsom plats, datum, tid, samtalslängd, samtal och motpart – skulle därmed kunna gå förlorad för brottsbekämpande myndigheter.

Ytterligare en fråga som kan ha betydelse för anpassningsskyldigheten är hur internationell roaming sker. Internationell roaming kan i såväl 5G-mobilnätet som

befintliga mobilnät ske enligt flera olika standarder. Antingen kan informationen hanteras av operatören i landet som simkortet är uppkopplat mot, eller så kan informationen omedelbart vidarebefordras till simkortets operatör i hemlandet. I det senare fallet, s.k. S8 Home Routing som redan är standard i 4G-näten, behandlas en mycket begränsad mängd information av operatören i det land som simkortet, och därmed användaren, befinner sig i. Beroende på vilken lösning som tillämpas kan information som härrör från utländska simkort som finns i Sverige bli otillgänglig eller svår att få tillgång till för de brottsbekämpande myndigheterna. Frågan har lyfts i internationella sammanhang men hittills har någon lösning inte föreslagits.

Sammanfattningsvis är det angeläget att anpassningsskyldighetens omfattning är tydlig, modern och tillgodoser brottsbekämpningens behov. Samtidigt behöver regleringen vara välavvägd så att teknikutvecklingen främjas, nätsäkerheten bibehålls och företagen inte påförs orimliga bördor. Kryptering är centralt för säkerheten i ett läge där allt större delar av industri, samhälle och stat är sammanlänkade genom elektronisk kommunikation. Föreslagna åtgärder får inte innebära att generella sårbarheter införs i kryptering eller att systematiska bakdörrar introduceras.

Utredaren ska därför

- analysera anpassningsskyldighetens omfattning och ta ställning till hur en reglering kan utformas på ett så tydligt, enhetligt, säkert och teknikneutralt sätt som möjligt,
- analysera behovet av lagstiftning eller andra åtgärder i fråga om anpassnings-skyldigheten så att hemliga tvångsmedel kan verkställas på ett effektivt sätt även i framtiden, och
- lämna förslag på de författningsändringar och andra åtgärder som bedöms nödvändiga.

Uppdraget att se över datalagringsregleringen utifrån bl.a. ny domstolspraxis

Ändrad svensk datalagringslagstiftning och behovet av en uppföljande översyn

EU-rätten sätter upp ramarna för nationell lagstiftning om datalagring för brotts-bekämpande ändamål. Europaparlamentets och rådets direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv 2002/58) anger bl.a. att medlemsstaterna ska säkerställa konfidentialitet vid elektronisk kommunikation och därmed förbundna trafikuppgifter. Uppgifter som inte längre behövs ska enligt direktivet utplånas eller avidentifieras. Medlemsstaterna får dock göra undantag från dessa skyldigheter om det behövs för bl.a. brottsbekämpande verksamhet. Direktivet är genomfört i svensk rätt främst genom bestämmelser i lagen om elektronisk kommunikation. Kommissionen lämnade i januari 2017 ett förslag på en förordning om integritet och elektronisk kommunikation (COM(2017) 10) (eDataskyddsförordning) som ska ersätta direktiv 2002/58. Förslaget förhandlas fortfarande.

I samband med att EU-domstolen i Digital Rights-domen den 8 april 2014 (förenade målen C-293/12 och C-594/12) ogiltigförklarade det s.k. datalagringsdirektivet (Europaparlamentets och rådets direktiv 2006/24/EG om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG) ifrågasattes de svenska datalagringsreglerna. Kammarrätten i Stockholm begärde därför ett förhandsavgörande från EU-domstolen (Kammarrättens mål nr 7380-14). EU-domstolen besvarade begäran genom en dom den 21 december 2016 (förenade målen C-203/15 och C-698/15), den s.k. Tele2-domen. EU-domstolens slutsats var bl.a. att en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter, avseende samtliga abonnenter och registrerade användare och samtliga elektroniska kommunikationsmedel, inte var förenlig med EU-rätten. Domstolen gjorde även vissa uttalanden om förutsättningarna för de brottsbekämpande myndigheternas åtkomst till lagrade uppgifter och om säkerheten för uppgifterna.

Med anledning av Tele2-domen sågs den svenska lagstiftningen över och den 1 oktober 2019 trädde nya regler om datalagring i kraft (prop. 2018/19:86). Som framgått ovan innebär ändringarna bl.a. att lagringens omfattning har begränsats och att lagringstiderna har differentierats (6 kap. 16 a och d §§ LEK samt 39 och 40 §§ förordningen [2003:396] om elektronisk kommunikation). I förarbetena uttalade regeringen att det senast inom fyra år efter ikraftträdandet kunde finnas anledning att se över regleringen, bl.a. mot bakgrund av den tekniska utvecklingen, ändrade kommunikationsvanor och nya mål om datalagring i EU-domstolen (samma prop. s. 38 och 108). Som förutsågs har den tekniska utvecklingen fortsatt i snabb takt och kommunikationsvanorna har förändrats. EU-domstolen har nu även meddelat domar i flera av de mål som nämndes i förarbetena (se vidare nedan). Riksdagen har också tillkännagett för regeringen att den skyndsamt ska återkomma med förslag som dels innebär en mer omfattande skyldighet att lagra uppgifter med koppling till nationell säkerhet, dels innebär en mer omfattande lagringsskyldighet generellt (bet. 2018/19:JuU27 punkt 6, rskr. 2018/19:296). Det finns således flera skäl att se över regleringen och redan nu göra den aviserade översynen av regelverket.

Bör lagstiftningen förändras med anledning av ny domstolspraxis?

Den 6 oktober 2020 meddelade EU-domstolen ytterligare domar om lagring och tillgång till uppgifter om elektronisk kommunikation (målet C-623/17 och förenade målen C-511/18, C-512/18 och C-520/18). I domarna konstaterade domstolen att direktiv 2002/58 är tillämpligt också när det gäller lagring av eller tillgång till uppgifter i elektroniska kommunikationer som syftar till att skydda den nationella säkerheten. Samtidigt konstaterade domstolen att EU-rätten, under vissa förutsättningar, inte hindrar en lagstiftning till skydd för nationell säkerhet som ålägger tjänsteleverantörer en generell och odifferentierad lagringsskyldighet avseende trafik- och lokaliseringsuppgifter i

situationer där den berörda medlemsstaten står inför ett allvarligt hot mot nationell säkerhet som visar sig vara verkligt, aktuellt eller förutsägbart. En sådan lagring kan tillåtas under förutsättning att beslutet kan bli föremål för en effektiv kontroll av en domstol eller av en oberoende myndighet och att den sker under en period som måste vara tidsmässigt begränsad till vad som är strängt nödvändigt, men som kan förlängas om hotet består.

När det gäller datalagring för bekämpning av grov brottslighet och för att förebygga allvarliga hot mot den allmänna säkerheten stod domstolen fast vid sina uttalanden i Tele2-domen om att en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter om samtliga abonnenter och registrerade användare och samtliga elektroniska kommunikationsmedel inte är förenlig med EU-rätten. Samtidigt uttalade domstolen att en generell och odifferentierad lagring av uppgifter om den fysiska identiteten (eng. civil identity) för användare av elektroniska kommunikationsmedel är tillåten utan någon specifik tidsbegränsning. Domstolen öppnade också upp för en generell och odifferentierad lagring av ip-adresser som har tilldelats källan för en internetanslutning i syfte att skydda den nationella säkerheten, bekämpa grov brottslighet och för att förebygga allvarliga hot mot den allmänna säkerheten, om lagringen är tidsmässigt begränsad till vad som är strängt nödvändigt. Domstolen stod vidare fast vid sina tidigare uttalanden om att medlemsstaterna är oförhindrade att föreskriva om en tidsbegränsad riktad lagring vilken, på grundval av objektiva och icke-diskriminerande faktorer, är avgränsad genom de kategorier av personer som berörs eller genom ett geografiskt kriterium. Domstolen uttalade sig också om möjligheterna att genom beslut från en behörig myndighet ålägga tjänsteleverantörer att skyndsamt säkra de trafik- och lokaliseringsuppgifter som de har tillgång till. Domstolen uttalade sig inte specifikt om den begränsade och differentierade lagring som införts i Sverige efter Tele2-domen.

Också vad gäller villkoren och formerna för tillgång till lagrad information har ny praxis kommit från EU-domstolen (se EU-domstolens dom den 2 mars 2021 i mål C-746/18).

Vid EU-domstolen finns ytterligare mål, som ännu inte avgjorts, som gäller datalagring för brottsbekämpande ändamål (bl.a. förenade målen C-793/19 och C-794/19 samt målet C-140/20). Den 25 maj 2021 meddelade den Europeiska domstolen för de mänskliga rättigheterna en dom i ett mål som rör en rad olika frågor om bl.a. avlyssning och inhämtning av s.k. mängddata (eng. bulk interception) i underrättelseverksamhet (Europadomstolens dom den 25 maj 2021 i Big Brother Watch m.fl. mot Förenade Kungariket, mål nr 58170/13, 62322/14 och 24960/15). Målet prövades i stor sammansättning (eng. Grand Chamber).

Mot bakgrund av de nya och kommande domarna finns det skäl att analysera om de ger anledning till anpassningar av den svenska lagstiftningen. Det är angeläget att de brottsbekämpande myndigheternas möjligheter att förhindra, upptäcka, utreda och

lagföra brott upprätthålls och stärks, samtidigt som ett starkt skydd för de grundläggande rättigheterna säkerställs. Som framgått ovan har EU-domstolen i sina avgöranden den 6 oktober 2020 lämnat flera öppningar för datalagring under förutsättning att effektiva skyddsmekanismer finns på plats. Särskilt när det gäller åtgärder till skydd för nationell säkerhet, lagring av ip-adresser och för att ta reda på en användares fysiska identitet anser domstolen att det finns större utrymme för datalagring.

Utredaren ska därför

- analysera hur dagens regler om lagring och tillgång till uppgifter om elektronisk kommunikation förhåller sig till ny praxis på området,
- överväga och ta ställning till vilka möjligheter som finns till förändringar av reglerna om lagring och tillgång till uppgifter om elektronisk kommunikation i syfte att tillgodose de brottsbekämpande myndigheternas möjligheter att upprätthålla och stärka sin förmåga, samtidigt som skyddet för de mänskliga rättigheterna säkerställs, och
- lämna förslag på de författningsändringar och andra åtgärder som bedöms nödvändiga.

Utredaren ska hålla sig informerad om och beakta de pågående EU-förhandlingarna om eDataskyddsförordningen samt eventuella lagstiftningsprojekt som kan följa av förhandlingarna.

Uppdraget att se över vissa frågor om exekutiv jurisdiktion

Rätten för en stat att vidta åtgärder och verkställa beslut som har fattats inom ramen för lagstiftning och rättsskipning kallas exekutiv jurisdiktion. Utgångspunkten i folkrätten är att det råder ett förbud för stater att vidta verkställighetsåtgärder inom andra staters territorier, t.ex. att använda hemliga tvångsmedel där. Detta baseras på den s.k. territorialitetsprincipen som är en grundläggande folkrättslig princip om staters suveränitet.

Elektroniskt lagrade uppgifter kan finnas i flera stater samtidigt eller ständigt förflyttas mellan stater. I många fall är det inte ens för den som tillhandahåller tjänsten möjligt att klargöra var uppgifterna finns i varje givet ögonblick. När detta trots allt är möjligt kan förhållandena ändras på bråkdelen av en sekund. I Sverige har territorialitetsprincipen traditionellt sett tolkats så att svenska brottsbekämpande myndigheter saknar jurisdiktion om uppgifter lagras elektroniskt på annan plats än i Sverige eller om det är okänt var uppgifterna lagras. I det första fallet, dvs. när det är känt att informationen lagras i ett annat land, är det många gånger möjligt att få biträde med att få åtgärden verkställd av myndigheterna i det land där uppgifterna finns. Detta kan ske genom internationell rättslig hjälp eller en europeisk utredningsorder. En sådan process kan dock ta lång tid, särskilt när det rör sig om en framställan till en stat utanför EU. I det andra fallet, när det

råder ovisshet om var informationen finns – s.k. loss of location – kan det inte klarläggas till vilket eller vilka länder ansökan om rättslig hjälp ska skickas. När det framför allt gäller loss of location-fall gör många andra stater en annan tolkning av territorialitets-principen än som traditionellt gjorts i Sverige och anser tvärtom att myndigheterna har befogenhet att vidta åtgärder.

Utredningen om hemlig dataavläsning och Beslagsutredningen har i sina betänkanden uppmärksammat frågan och bedömt att det finns skäl att ändra tolkningen av territorialitetsprincipen (SOU 2017:89 s. 479-485 och SOU 2017:100 s. 374-375). De båda utredningarna uttalade att frågan borde prövas i rättstillämpningen. I remissyttranden med anledning av Utredningen om hemlig dataavläsning anförde Svea hovrätt, Göteborgs tingsrätt, Polismyndigheten och Skatteverket att frågan borde lösas genom lagstiftning. Uppsala universitet (juridiska fakultetsnämnden) ansåg att det framstår som mindre lämpligt att utan vidare överlämna frågan åt rättstillämpningen. Säkerhets- och integritetsskyddsnämnden anförde att ett överlämnande till rättstillämpningen inte kan godtas. Det framkom även i remissyttrandena med anledning av Beslagsutredningen att flera remissinstanser ansåg att frågan borde lösas genom lagstiftning. Polismyndigheten uttalade i sitt yttrande att det var önskvärt att regeringen i varje fall uttalade vilka omständigheter som bör iakttas vid bedömningen.

I propositionen Hemlig dataavläsning konstaterade regeringen att det inte inom ramen för det lagstiftningsprojektet var möjligt att omhänderta denna fråga samt att frågan bäst tas om hand inom ramen för det internationella samarbetet eller på annat lämpligt sätt (prop. 2019/20:64 s. 203). Beslagsutredningen bereds för närvarande inom Regeringskansliet.

Den fortsatta teknikutvecklingen gör att frågan blir av allt större betydelse för de brottsbekämpande myndigheterna. Frågan om tillgång till elektroniska uppgifter ses för närvarande över i olika internationella forum. Som nämnts ovan pågår det inom EU förhandlingar om förslag till en förordning om tillgång till e-bevisning och ett direktiv om utseende av företrädare för insamling av e-bevisning (COM(2018) 225 och COM(2018) 226). Kommissionen har föreslagit att en myndighet i en medlemsstat ska kunna beordra en tjänsteleverantör i en annan medlemsstat att bevara eller lämna ut uppgifter. Om tjänsteleverantören inte skulle följa en sådan order får den utfärdande myndigheten begära hjälp från myndigheterna i den verkställande staten. Kommissionen har också fått mandat att förhandla fram ett avtal med USA som rör tillgång till elektronisk bevisning. Inom Europarådet pågår förhandlingar om ett andra tilläggsprotokoll till Europarådets konvention om it-relaterad brottslighet, den s.k. Budapestkonventionen. Beroende på utfallet från de pågående förhandlingarna skulle vissa delar av jurisdiktionsproblematiken kunna lösas. Det står dock klart att frågan om s.k. loss of location inte kommer att få en lösning i förhandlingarna.

Någon lösning inom ramen för det internationella samarbetet har ännu inte kommit till stånd. Det har hittills inte heller kommit någon vägledande praxis från de inhemska prejudikatsinstanserna som löser jurisdiktionsfrågan för svensk del. För en effektiv brottsbekämpning är det viktigt att reglerna om tillgång till elektronisk kommunikation och annan elektronisk bevisning också kan tillämpas i praktiken, även när informationen finns utanför Sverige eller när det är okänt var den finns. Det finns därför skäl att se över förutsättningarna, inklusive de folkrättsliga aspekterna, för att införa en särskild lagreglering för territorialitetsprincipen vid exekutiv jurisdiktion i förhållande till elektronisk information som finns utanför Sverige.

Utredaren ska därför

- analysera de folkrättsliga frågorna om exekutiv jurisdiktion i förhållande till elektroniska uppgifter utanför Sverige, och i denna analys även göra en jämförelse med rättsläget i andra relevanta länder,
- ta ställning till om det bör införas en särskild lagreglering för territorialitetsprincipen vid exekutiv jurisdiktion som också tar hänsyn till andra anknytningsfaktorer än var data lagras, och
- vid behov lämna förslag på de författningsändringar och andra åtgärder som bedöms nödvändiga.

Utredaren ska hålla sig informerad om och beakta det arbete som pågår inom ramen för ovan nämnda EU-förhandlingar, pågående förhandlingar med USA samt inom Europarådet. Utredaren ska också hålla sig informerad om eventuella lagstiftningsprojekt som kan följa av de ovan nämnda förhandlingarna.

Konsekvensbeskrivningar

Utredaren ska bedöma och redogöra för förslagens ekonomiska konsekvenser och konsekvenser i övrigt för enskilda, företag och det allmänna samt redogöra för förslagens samhällsekonomiska effekter. Utredaren ska särskilt beskriva vilka konsekvenser de förslag som lämnas har för det nationella och internationella skyddet för mänskliga rättigheter, inklusive den personliga integriteten, och för möjligheterna att kommunicera på ett säkert sätt. De offentligfinansiella effekterna av förslagen ska beräknas, och om förslagen kan förväntas leda till offentligfinansiella kostnader ska utredaren föreslå hur dessa ska finansieras.

Kontakter, genomförande 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, It- och telekomföretagen, teleoperatörer, ISOC-SE och OTT-tjänsteleverantörer, 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 säkerställa att en välfungerande systematik i regelverket kring hemliga tvångsmedel upprätthålls. Det innebär att utredaren även ska bedöma behovet av följdändringar i rättegångsbalken, inhämtningslagen, preventivlagen, lagen om särskild utlänningskontroll, lagen om hemlig dataavläsning och lagen om elektronisk kommunikation. Utredaren ska även bedöma behovet av följdändringar i lagen om internationell rättslig hjälp i brottmål och lagen om en europeisk utredningsorder. När det finns behov av det ska utredaren lämna förslag på författningsändringar. Utredaren har även möjlighet att ta upp andra frågor som har samband med de frågeställningar som ska utredas under förutsättning att uppdraget kan redovisas i tid.

Uppdraget ska redovisas senast den 6 februari 2023.

(Justitiedepartementet)