Nätsäkerhetsavdelningen

Justitiedepartementet
103 33 Stockholm

Yttrande avseende betänkandet ”Datalagring och integritet” (SOU 2015:31)

Post- och telestyrelsen (PTS) har enligt 1 § förordningen (2007:951) med instruktion för Post- och telestyrelsen ett samlat ansvar inom postområdet och området för elektronisk kommunikation. Enligt 2 § förordningen (2003:396) om elektronisk kommunikation är PTS tillsynsmyndighet enligt lagen (2003:389) om elektronisk kommunikation (LEK). Enligt 2 § postförordningen (2010:1049) är PTS tillsynsmyndighet enligt postlagen (2010:1045). PTS har med utgångspunkt från myndighetens verksamhetsområden följande synpunkter.

Sammanfattning

PTS välkomnar att regeringen har låtit utreda förändringar i regleringen för att stärka skyddet för den personliga integriteten och ser i huvudsak positivt på de förslag utredningen lämnar. Det finns i många avseenden en välgrundad nytta för brottsbekämpningen med lagring av vissa trafikuppgifter. Myndigheten anser dock att det finns anledning att överväga fler åtgärder än de utredningen föreslår, för att ytterligare stärka skyddet för den personliga integriteten.

PTS anser att det finns behov av en samlad översyn av regelverket rörande integritetsskydd, lagring respektive inhämtning av uppgifter om elektronisk kommunikation. Regleringen är idag svårtillämpad och behäftad med risker för gränsdragnings- och tolkningsproblem.

Vad gäller lagringsskyldighetens omfattning menar PTS att utredningen skulle behöva kompletteras med en mer empirisk utredning avseende den faktiska nytta som de olika typerna av uppgifter har för brottsbekämpningen.

Post- och telestyrelsen

Postadress:
Box 5398
102 49 Stockholm

Besöksadress:
Valhallavägen 117A
www.pts.se

Telefon: 08-678 55 00
Telefax: 08-678 55 05
pts@pts.se

PTS anser också att eventuella krav på att lagringen av uppgifter ska ske inom EU bör utredas vidare. PTS menar att myndighetens möjligheter till effektiv tillsyn kan begränsas om lagringen förläggs till utlandet samt att en sådan lagring även skulle vara förknippad med risker för nationell säkerhet. Utredningens slutsats att en reglering som inte tillåter lagring utanför EU inte är förenlig med EU-rätten kan, enligt PTS mening, ifrågasättas.

Den föreslagna regleringen av beslut om inhämtning av abonnemangsuppgifter bör kompletteras med regler som tydliggör vilket ansvar tillhandahållare av elektroniska kommunikationstjänster (fortsättningsvis kallade ”tillhandahållare”) har att kontrollera varje begäran om att uppgifter ska lämnas ut. PTS menar också att abonnemangsuppgifter många gånger är integritetskänsliga och att risken för felaktig rättstillämpning vid inhämtning av sådana uppgifter är tillräcklig för att motivera en särskild tillsynsuppgift avseende inhämtningen.

Inledning

Rättsordningen har sedan länge erkänt den enskildes intresse av personlig integritet och rätten att kunna kommunicera förtroligt, utan ingrepp från vare sig staten eller andra enskilda. Dessa grundlagsstadgade rättigheter kompletteras av såväl straffrättslig reglering som en strikt marknadsreglering, med särskilda regler om bland annat informationssäkerhet och tystnadsplikt för den information som kommuniceras, liksom andra uppgifter som beskriver kommunikationen.

PTS kan konstatera att det under de senaste åren har genomförts ett antal förändringar i svensk rätt som på olika sätt har medfört begränsningar i rätten till förtrolig kommunikation. Målen med förändringarna har varit att uppnå stärkt förmåga inom till exempel brottsbekämpning eller upprätthållande av nationell säkerhet. PTS har dock i tidigare remissyttranden pekat på brister i avvägningen mellan de mål som ska uppnås med regleringen och rätten till skydd för den personliga integriteten.[1]

PTS välkomnar därför att regeringen nu har låtit utreda lämpliga förändringar i reglerna om lagring av uppgifter om elektronisk kommunikation för brottsbekämpande ändamål för att stärka skyddet för den personliga integriteten. Myndigheten ser i huvudsak också positivt på de förslag till förändringar i regelverket som utredningen lämnar. PTS anser emellertid, vilket

[1] Se bl.a. PTS yttrande (dnr 05-9849) avseende departementsskrivelsen *En anpassad försvarsunderrättelseverksamhet* (Ds 2005:30), PTS yttrande (dnr 05-11036) avseende betänkandet *Tillgång till elektronisk kommunikation i brottsutredningar m.m.* (SOU 2005:38), PTS yttrande (dnr 08-2806) avseende betänkandet *Skyddet för den personliga integriteten - Bedömningar och förslag* (SOU 2008:3) samt PTS yttrande (dnr 09-1210) avseende betänkandet *En mer rättssäker inhämtning av elektronisk kommunikation i brottsbekämpningen* (SOU 2009:1).

utvecklas i det följande, att det finns anledning att överväga ytterligare åtgärder för att stärka skyddet för den personliga integriteten.

Utredningens författningsförslag

PTS instämmer i utredningens förslag till reglering av beslut om inhämtning av uppgifter enligt 6 kap. 22 § första stycket 2 LEK. PTS anser dock att bestämmelsen inte bör placeras i förordningen (2003:396) om elektronisk kommunikation (FEK) eftersom bestämmelsen riktar sig till de brottsbekämpande myndigheterna medan FEK primärt reglerar PTS verksamhet och tillhandahållande av elektroniska kommunikationsnät och kommunikationstjänster.

PTS har inga synpunkter på utredningens övriga författningsförslag.

Överväganden i övrigt

En samlad översyn av regelverket behövs

För brottsbekämpande ändamål finns regler om lagring och inhämtning av uppgifter om elektronisk kommunikation. Reglerna om lagring respektive om inhämtning av uppgifter, innebär var för sig undantag från de grundläggande reglerna om integritetsskydd i LEK. Som utgångspunkt tillåter reglerna i LEK vare sig lagring eller utlämnande av uppgifter, annat än för ett fåtal specifika ändamål.

Reglerna om integritetsskydd, och lagring respektive inhämtning av uppgifter, har, var för sig, varit föremål för ett antal utredningar och förändringar under senare år. De olika delarna av regelverket har emellertid inte vid något tillfälle setts över gemensamt, i ett sammanhang, vilket PTS anser är olyckligt.

PTS har i tidigare remissyttranden påpekat att det saknas en gemensam systematik för reglerna om integritetsskydd, och lagring respektive inhämtning av uppgifter.[2] Till exempel saknas en konsekvent terminologi för och kategorisering av de uppgifter som berörs av regleringen. I dagens bestämmelser används en rad olika begrepp, som har sitt ursprung i såväl äldre telelagstiftning som EU-reglering och processrättsliga regler. Reglerna finns även utspridda i ett antal olika lagar och förordningar. Tillämpning och tillsyn över reglerna vilar på flera olika myndigheter med överprövning i olika domstolar. Bristerna i systematiken gör sammantaget regelverket svårtillämpat och ökar risken för gränsdragnings- och tolkningsproblem.

[2] Se t.ex. PTS yttrande (dnr 07-13540) avseende betänkandet *Lagring av trafikuppgifter för brottsbekämpning* (SOU 2007:76), s 5.

Det finns således ett behov av att genomföra en samlad analys och översyn av reglerna rörande integritetsskydd, lagring respektive inhämtning av uppgifter om elektronisk kommunikation för brottsbekämpande ändamål. En sådan översyn bör även ta sikte på en systematisk renodling av regelverket och en sammanhållen reglering av tillsyn och kontroll av regelverkets tillämpning, samt en samlad avvägning mellan individens rätt till skydd av den personliga integriteten och de brottsbekämpande verksamheternas intressen av lagring och inhämtning av uppgifter.

Vilka uppgiftskategorier som ska lagras

Utredningen gör bedömningen att det inte bör göras några förändringar i fråga om vilka uppgifter som ska lagras enligt datalagringsreglerna. Enligt utredningens uppfattning står det klart att lagringsskyldigheten inte omfattar annat än vad som är strikt nödvändigt för att uppnås syftet med regleringen.[3]

Det finns i många avseenden en välgrundad nytta för brottsbekämpningen med lagring av vissa trafikuppgifter och PTS ifrågasätter inte att denna nytta många gånger kan vara proportionerlig i förhållande till det integritetsintrång lagringen innebär. PTS har inte någon uppfattning om vilka uppgifter som faktiskt är strikt nödvändiga för att uppnå syftet med regleringen. Det är emellertid PTS uppfattning att utredningen skulle behöva kompletteras med ett erfarenhetsbaserat underlag, för att stärka bedömningen av vilka uppgifter som är nödvändiga och proportionerliga att lagra.

Krav på lagring inom EU

Utredningen gör bedömningen att det inte bör införas något uttryckligt förbud mot lagring av uppgifter i ett tredje land. Till stöd för denna bedömning framför utredningen dels att de befogenheter PTS har får anses vara tillräckliga för att myndigheten ska kunna utöva en aktiv och ändamålsenlig tillsynsverksamhet, dels att en reglering som inte tillåter lagring utanför EU skulle stå i strid med EU-rätten och Sveriges åtaganden enligt dataskyddskonventionen.

PTS möjligheter till effektiv tillsyn i utlandet kan vara begränsade

När det gäller PTS tillsynsmöjligheter instämmer PTS i att dessa, rent principiellt, inte påverkas av var uppgifterna lagras. Den som tillhandahåller tjänster som är anmälningspliktiga enligt LEK, ansvarar för att lagring sker i enlighet med reglerna i lagen. PTS tillsyn torde som regel riktas mot tillhandahållaren och inte mot eventuella underleverantörer, oavsett om underleverantörerna finns inom rikets gränser eller inte.

[3] SOU 2015:31 s. 168.

Det torde också åligga den svenska tillhandahållaren att i avtal med sådana underleverantörer reglera hur de får hantera de lagrade uppgifterna. I ett sådant avtal kan även ingå en rätt för tillhandahållaren att genomföra revisioner på plats hos underleverantören, för att säkerställa att avtalet efterlevs. PTS kan i sin tillsyn granska sådana avtal, liksom tillhandahållarens rutiner för revisioner och uppföljning av avtalen.

PTS saknar däremot möjligheter att rent faktiskt kontrollera att lagring av uppgifter i utlandet sker i enlighet med de svenska reglerna. Enligt LEK har PTS rätt att för sin tillsyn få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, där verksamhet som omfattas av lagen bedrivs. I praktiken gäller detta dock endast på svenskt territorium. Vid lagring av uppgifter utomlands saknar således PTS möjlighet att genom inspektion på plats kontrollera att reglerna i LEK, och i synnerhet de särskilda informations-säkerhetsbestämmelser som gäller för lagrade uppgifter, efterlevs.

I nuläget finns det inte heller, enligt PTS mening, förutsättningar för samverkan med myndigheter i andra länder, vare sig inom eller utom EU, avseende enskilda tillsynsärenden. Sedan datalagringsdirektivet upphävdes finns det inte längre några harmoniserade regler om vare sig själva lagringen av uppgifter eller om informationssäkerheten för sådana uppgifter. Inte heller när det gäller tillsyn enligt de regler om integritetsskydd och behandling av uppgifter som är harmoniserade, finns det något etablerat system för att erhålla bistånd av myndighet i en annan medlemsstat.

Det kan finnas EU-rättsliga möjligheter att reglera var lagring får ske

Utredningen menar att ett förbud mot lagring av uppgifter i tredjeland inte skulle stå i överensstämmelse med EU-rätten. Utredningen framför att det förefaller mindre sannolikt att det varit EU-domstolens avsikt att förändra förutsättningarna för tillämpningen av kommissionens beslut om så kallad adekvat skyddsnivå, samt att kommissionen rimligtvis i sådana fall borde ha tagit initiativ till att se över dessa beslut.[4]

EU-domstolen anger emellertid i punkt 68 i domen att datalagringsdirektivet ”inte kräver att uppgifterna ska lagras inom unionen, vilket innebär att den i artikel 8.3 i stadgan uttryckligen föreskrivna oberoende myndighetskontrollen av att de i de båda föregående punkterna behandlade skydds- och säkerhetskraven följs, inte fullt ut kan anses vara garanterad”. Det kan således enligt PTS bedömning inte hållas för osannolikt att domstolen, som är den slutliga uttolkaren av EU-rätten, menade att kommissionens beslut om adekvat

[4] SOU 2015:31 s. 181.

skyddsnivå inte är tillräckliga för den känsliga behandling av uppgifter som trafikdatalagringen innebär.

Att kommissionen inte har tagit initiativ till att se över besluten om adekvat skyddsnivå, måste enligt PTS mening, ses i ljuset av att kommissionen överhuvudtaget inte har vidtagit några åtgärder till följd av den aktuella domen.

Kommissionens beslut om adekvat skyddsnivå tar sikte på en nivå av skydd som motsvarar vad som gäller generellt för behandling av personuppgifter inom EU. Det bör därför också påpekas att den svenska lagstiftaren har gjort bedömningen att vare sig dessa generella säkerhetskrav eller de mer specifika säkerhetskrav som gäller för elektroniska kommunikationstjänster, är tillräckliga för att skydda de uppgifter som lagras för brottsbekämpande ändamål.[5] Tillsammans med kravet på lagring av uppgifter infördes därför särskilda säkerhetskrav i 6 kap. 3 a § LEK. Vid riksdagsbehandlingen av lagförslaget framfördes att stor vikt fästes vid skyddet mot spridning av de uppgifter som lagras och riksdagen beslutade därför att regeringens eventuella föreskrifter om skyddsåtgärder snarast skulle underställas riksdagen för prövning.[6] Sådana föreskrifter om skyddsåtgärder har därefter meddelats och återfinns i 37 § FEK. Kraven har preciserats ytterligare av PTS genom föreskrifter och allmänna råd (PTSFS 2012:4).

Slutligen noterar PTS att det i andra medlemsstater förekommer nationella krav på att datalagringen ska ske inom landets gränser. Det gäller till exempel Grekland.[7]

Lagring i utlandet har betydelse för nationell säkerhet

Det har inte ingått i Datalagringsutredningens uppdrag att göra säkerhetspolitiska bedömningar. PTS vill ändå i anledning av frågan om lagring i utlandet, påpeka att det i de flesta länder förekommer hemlig inhämtning av uppgifter. Sådan inhämtning skulle kunna omfatta uppgifter om elektronisk kommunikation som finns lagrade i utlandet för en svensk tillhandahållares räkning.

---

[5] Se prop. 2010/11:46 s. 53f.
[6] Se justitieutskottets betänkande, 2011/12:JuU28, s 50.
[7] Artikel 6 i Lag 3917/2011 Lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät, med hjälp av övervakningssystem för att ta emot eller spela in ljud eller video på offentliga platser och därmed sammanhängande bestämmelser. (*ΝΟΜΟΣ ΥΠ' ΑΡΙΘ. 3917 Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις.*)

Det kan inte uteslutas att sådan inhämtning av uppgifter skulle kunna verkställas som ett led i landets underrättelseverksamhet mot Sverige eller svenska intressen. Det är vidare rimligt att anta att den som hanterar lagringen av uppgifter i det aktuella landet normalt saknar rättsliga möjligheter att lämna upplysningar om att sådan inhämtning sker, vare sig till sin svenska uppdragsgivare eller till svenska myndigheter. Eftersom reglerna om lagring av trafikuppgifter omfattar även trafik som är hänförlig till nyckelpersoner inom såväl statsväsendet som svenskt näringsliv, menar PTS att lagring i utlandet skulle kunna medföra betydande risker för nationell säkerhet.

Mot bakgrund av ovanstående omständigheter anser PTS att frågan om reglering av var lagring av uppgifter om elektronisk kommunikation får ske bör utredas vidare.

Inhämtning av abonnemangsuppgifter

Utredningen föreslår att det ska regleras vem som får fatta beslut om inhämtning av abonnemangsuppgifter och hur sådana beslut ska dokumenteras. PTS instämmer i detta förslag men anser att regleringen bör förstärkas ytterligare för att säkerställa att sådan inhämtning sker på ett korrekt sätt och i enlighet med gällande regler.

Abonnemangsuppgifter kan vara integritetskänsliga

Utredningen framför att abonnemangsuppgifter inte har ansetts särskilt integritetskänsliga. PTS menar dock att den värderingen härrör från en tid när abonnemangsuppgifter i stort sett endast avsåg namn och telefonnummer för fasta telefonabonnemang. Det var då fråga om uppgifter som i stor utsträckning publicerades i telefonkataloger, tillgängliga för var och en. Endast i begränsad utsträckning, vid inhämtning av så kallade hemliga nummer som inte var publicerade, kunde något större integritetsintrång anses uppkomma. Även reglerna om tystnadsplikt avseende abonnemangsuppgifter härrör från denna tid och har i stort sett oförändrade överförts från den tidens reglering.

Begreppet abonnemangsuppgift har emellertid kommit att förändras i takt med utvecklingen inom området elektronisk kommunikation. En mängd olika tekniker och tjänster för kommunikation har tillkommit, och med dem en rad nya uppgifter som kan anses utgöra abonnemangsuppgifter. Gränsdragningen mellan abonnemangsuppgifter och andra slags uppgifter, såsom trafikuppgifter, har med tiden blivit allt svårare.

PTS vill särskilt framhålla behandlingen av ip-adresser, som numera är nödvändig vid i stort sett all elektronisk kommunikation. Det ansågs länge oklart hur ip-adresserna skulle kategoriseras, men med tiden har uppfattningen att ip-adresser utgör abonnemangsuppgifter kommit att bli den etablerade. Till

skillnad från telefonnummer har det dock aldrig funnits några offentliga register över vem som innehar en viss ip-adress (undantaget större organisationer som kan ha ip-adresser tilldelade direkt från en så kallad Internet Registry). Det är alltså i normalfallet inte möjligt för envar att ta reda på vem som innehar en viss ip-adress. Vid kommunikation över internet presenteras dock alltid ip-adressen för den andra parten i kommunikationen, och det är mycket vanligt förekommande att användarnas ip-adresser registreras i en logg hos de som tillhandahåller tjänster över internet. Kännedom om vem som innehar en viss ip-adress skulle således kunna möjliggöra kartläggning av dennes internetanvändning, till exempel vilka webbsidor som individen har besökt.

Det är mot denna bakgrund PTS uppfattning att abonnemangsuppgifter som utgångspunkt bör anses vara känsliga ur integritetssynpunkt.

Det finns risk för felaktig rättstillämpning vid inhämtning av abonnemangsuppgifter

Utredningen framför också att det är svårt att se att inhämtning av abonnemangsuppgifter skulle vara förknippade med några direkta risker för felaktig rättstillämpning. PTS menar dock att den ovan beskrivna utvecklingen, med allt mer komplicerade gränsdragningar mellan olika kategorier av uppgifter, medför ökade risker för att uppgifter begärs utlämnade från tillhandahållarna på felaktiga grunder. Tillhandahållarna har själva uppgett att så är fallet och gränsdragningsfrågor har vid ett antal tillfällen blivit föremål för bedömning av PTS. I enstaka fall har frågan även blivit föremål för domstolsprövning.[8]

Det finns stora skillnader i kriterierna för inhämtning mellan abonnemangsuppgifter och andra uppgifter om elektronisk kommunikation. Det kan därför ofta vara avgörande för en brottsbekämpande myndighets möjligheter att inhämta uppgifter, huruvida de efterfrågade uppgifterna kan kategoriseras som abonnemangsuppgifter.

Utredningens bedömning att risken för felaktig rättstillämpning är låg, grundas bland annat på att det finns relativt få förutsättningar, såsom krav på viss allvarlighet i den aktuella brottsligheten, för inhämtningen av abonnemangsuppgifter. PTS vill dock framhålla att även om det finns få lagstadgade kriterier för inhämtningen, torde den brottsbekämpande myndigheten vara skyldig att göra en individuell bedömning av proportionaliteten mellan å ena sidan nyttan för myndigheten i det enskilda

[8] Se till exempel PTS beslut i ärendena med dnr 01-88, dnr 06-1426, dnr 06-12813 och dnr 08-10820, samt Kammarrätten i Stockholms dom den 19 januari 2010, mål nr 3138-09. Besluten härrör från tiden före den 1 juli 2012, när inhämtning av andra uppgifter än abonnemangsuppgifter för brottsbekämpande ändamål utgick ur LEK. PTS har sedan lagändringen inte möjlighet att i samma utsträckning pröva gränsdragningsfrågor inom ramen för myndighetens tillsyn.

fallet och å andra sidan det intrång i den personliga integriteten som inhämtningen skulle medföra, inför varje enskilt beslut om inhämtning av abonnemangsuppgifter.

Det bör regleras vilka upplysningar som ska lämnas vid inhämtning av abonnemangsuppgifter

Utredningen har föreslagit en reglering av beslutsordningen för inhämtning av abonnemangsuppgifter. PTS föreslår att det uttryckligen regleras även vilka upplysningar rörande ett beslut om inhämtning som ska lämnas tillhandahållare i samband med inhämtningen. Bakgrunden är att tillhandahållarnas tystnadsplikt för uppgifter om elektronisk kommunikation innebär att de är, under straffansvar, förhindrade att obehörigen lämna ut sådana uppgifter. I praktiken medför reglerna att tillhandahållarna antingen är skyldiga eller förbjudna att lämna ut uppgifterna. Endast undantagsvis kan en situation uppkomma där tillhandahållarna har rätt men inte skyldighet att lämna ut uppgifter, vilket innebär att tillhandahållarna måste försäkra sig om att de verkligen är skyldiga att verkställa ett utlämnande, innan så sker. Det är därför viktigt att de myndigheter som hämtar in uppgifter tydliggör för tillhandahållarna att inhämtningen sker i enlighet med gällande regler. Det förekommer i dagsläget, såvitt PTS erfarit, viss osäkerhet om vilka upplysningar en tillhandahållare behöver erhålla av myndigheten, för att kunna exculpera sig i förhållande till tystnadspliktsreglerna.

PTS anser därför att det bör regleras vilka upplysningar den brottsbekämpande myndigheten ska lämna tillhandahållaren. Enligt PTS uppfattning bör tillhandahållaren åtminstone upplysas om vilken myndighet som begär ut uppgifterna, liksom namn, befattning och kontaktuppgifter till den som handlägger ärendet för myndighetens räkning, samt grunden för inhämtning av uppgifter (aktuellt lagrum samt referens till beslut om inhämtning).

Det föreligger behov av en särskild tillsynsuppgift för inhämtningen

Utredningens samlade bedömning är att behovet av en tillsynsfunktion som specifikt tar sikte på att granska inhämtningen av abonnemangsuppgifter inte är särskilt stort. PTS kan inte instämma i den slutsatsen. Enligt PTS uppfattning är, som redovisats ovan, risken för felaktig rättstillämpning och därmed otillåtna intrång i grundläggande mänskliga rättigheter, tillräckligt hög för att motivera en ändamålsenligt utformad tillsyn över de brottsbekämpande myndigheternas inhämtning även av abonnemangsuppgifter.

Inhämtning av abonnemangsuppgifter sker, i likhet med vad som gäller för hemliga tvångsmedel, i hemlighet och utan att den enskilda individen informeras om detta. Beslut om sådan inhämtning kan, såvitt PTS känner till, inte heller överklagas, vare sig av den enskilda individen, av tillhandahållaren eller någon annan part.

Polisorganisationskommittén konstaterade i sitt betänkande *Tillsyn över polisen* (SOU 2013:42) att en avsaknad av möjligheter till överprövning av vissa polisiära beslut, i viss mån, kan vägas upp av en möjlighet till kontroll och granskning av polisens verksamhet i efterhand. Vidare framfördes i betänkandet att det är en nödvändig förutsättning för att det ska finnas förtroende för polisens verksamhet, att verksamheten bedrivs i enlighet med lagar och andra bindande föreskrifter och även i övrigt utförs på ett korrekt och konsekvent sätt. Kommittén menade också att en granskning av polisens agerande i efterhand är ett sätt att bidra till medborgarnas förtroende.[9] PTS instämmer i den bedömningen och anser att inhämtning av abonnemangsuppgifter är just en sådan ingripande åtgärd som bör vara föremål för granskning.

Datalagringsutredningen framför att inhämtningen av abonnemangsuppgifter redan är föremål för den tillsyn som utövas av JO och JK. PTS menar dock att den extraordinära tillsyn som utövas av JO och JK aldrig kan ersätta reguljär heltäckande tillsyn i de fall ett tydligt behov av sådan tillsyn kan identifieras. Såväl JO som Polisorganisationskommittén har tidigare, i närliggande sammanhang, framfört liknande uppfattningar rörande förhållandet mellan den extraordinära tillsynen och en löpande och kontinuerlig ordinarie tillsyn.[10]

I dagsläget är det i praktiken tillhandahållarna som utövar den enda löpande, oberoende kontrollen över de brottsbekämpande myndigheternas inhämtning av abonnemangsuppgifter. Tillhandahållarna ser sig med nuvarande system tvungna att granska varje begäran om utlämnande av uppgifter för att undgå att bryta mot tystnadsplikten i 6 kap. 20 § LEK. PTS menar att det inte kan vara en lämplig ordning att låta kommersiella företag utgöra den enda oberoende garanten för individens rättssäkerhet vid brottsbekämpande myndigheters inhämtning av abonnemangsuppgifter. PTS förordar således att tillsyn, på samma sätt som är fallet vad gäller inhämtning av uppgifter enligt inhämtandelagen (2012:278), utövas av ett oberoende statligt tillsynsorgan.

Den myndighet som idag har den mest närliggande verksamheten torde vara Säkerhets- och integritetsskyddsnämnden (SIN), som bland annat granskar användningen av hemliga tvångsmedel. Datalagringsutredningen framför dock ett antal argument emot att SIN tilldelas rollen som tillsynsmyndighet även för inhämtning av abonnemangsuppgifter. PTS noterar samtidigt att Polisorganisationskommittén nyligen föreslog att en fristående myndighet ska

[9] SOU 2013:42 s. 121 f.
[10] Se SOU 2007:22 s. 225 f. samt SOU 2013:42 s. 122 f.

tillskapas, med ansvar för tillsyn över Polismyndigheten, Säkerhetspolisen och Kriminalvården.[11]

PTS har ingen bestämd uppfattning om vilket tillsynsorgan som är bäst lämpat att ansvara för en ordinarie tillsyn över inhämtningen av abonnemangsuppgifter. Enligt PTS är det dock viktigt att tillsynen utövas av en myndighet som kan upprätthålla kompetens avseende såväl den brottsbekämpande verksamheten som de tekniska och organisatoriska förutsättningarna för tillhandahållare.

Utöver en sådan reguljär tillsyn anser PTS, som beskrivits ovan, att kontrollsystemet rörande inhämtning av abonnemangsuppgifter, för att vara komplett, även bör innefatta tydligare reglering av hur inhämtningen av uppgifter från tillhandahållare ska gå till.

Göran Marby
Generaldirektör

Yttrandet har beslutats av generaldirektören Göran Marby. I ärendets slutliga handläggning har även divisionschefen Catarina Wretman, avdelningschefen Annica Bergman, chefsjuristen Karolina Asp och juristen Staffan Lindmark (föredragande) deltagit.

[11] SOU 2015:57.