Polisen

Datum
2015-08-31

Diarienr (åberopas)
A203.603/2015

Saknr
000

Polismyndigheten

Justitiedepartementet

Datalagringsutredningens betänkande Datalagring och integriet (SOU 2015:31)

Allmänt

Myndigheten instämmer i utredningens bedömningar till stor del och välkomnar de förslag som Datalagringsutredningen redovisar i sitt betänkande.

Polismyndigheten har dock följande synpunkter.

1.1 Förslag till lag om ändring i rättegångsbalken

Förstörandeskyldigheten av uppgifter som omfattas av yrkesmässig tystnadsplikt föreslås utökas till att även avse uppgiften att kommunikationen överhuvudtaget ägt rum. Polismyndigheten befarar att förstörandet kan leda till att rättssäkerheten för den misstänkte och utredningen i övrigt kan riskeras lida skada av att detta raderas. Raderingen av metadata kan även leda till att tillsynen av polisens verksamhet i dessa fall riskerar att inte kunna fullgöras på ett tillfredställande sätt. Sådana synpunkter från tillsynsmyndigheterna bör beaktas.

1.2 Förslag till lag om ändring i lagen (2003:389) om elektronisk kommunikation

Polismyndigheten ser positivt på de förslag som förtydligar att uppgifter om abonnemang får, utöver i en förundersökning, hämtas in även i de brottsbekämpande myndigheternas underrättelseverksamhet.

Polismyndigheten föreslår ytterligare tillägg i lagen om elektronisk kommunikation enligt nedan. Skulle förslaget inte anses ligga inom ramen för uppdraget så bör detta tas hand om på annat sätt och utredas.

I nuläget saknas lagstöd för att hämta in uppgifter om abonnemang i syfte att identifiera en okänd person, för att därefter sätta in räddande åtgärder, som via elektronisk kommunikation/sociala media meddelar en avsikt att skada sig själv eller att begå självmord. Problemet har ökat i och med den allmänt ökande användningen av sociala media och hittills har polisen tvingats att använda sig av brottsbalkens regelverk om nöd i sådana fall. Lämpligen bör det i

Postadress
Polismyndigheten
Box 12256
102 26 Stockholm

Besöksadress
Polhemsgatan 30
Stockholm

Telefon
114 14

Webbplats
www.polisen.se

E-post
registrator.kansli@polisen.se

6 kap. 22 § i lagen om elektronisk kommunikation även framgå att de uppgifter som behövs avseende abonnemang ska utlämnas till Polismyndigheten i de fall en okänd person genom meddelande via elektronisk kommunikation lämnar sådana uppgifter att det kan befaras finnas fara för dennes liv eller allvarlig risk för dennes hälsa.

1.6 Förslag till lag om ändring i lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet

Polismyndigheten ser positivt på de förtydliganden och förändringar som föreslås ske i inhämtningslagen. Myndigheten anser dock att förutsättningarna för att få använda lagen bör ses över på en mer övergripande nivå än vad som skett i utredningen. Därvid bör följande beaktas.

Den öppna polisens möjlighet att i dagsläget använda inhämtningslagen är i princip begränsad till misstankar om brottslig verksamhet för brott för vilka inte är föreskrivet lindrigare straff än fängelse i två år. I viss utsträckning kan Polismyndigheten också tillämpa reglerna avseende tillkommande brott.

För att den öppna polisens underrättelseverksamhet fullt ut ska kunna fånga upp signalerna tidigt och förebygga allvarligare brottslighet bör man i inhämtningslagen införa en straffvärdesventil så att lagen kan tillämpas även vid misstankar om brottslig verksamhet rörande t.ex. grova stölder, grova hälerier, grova bokföringsbrott, grova bedrägerier och penningtvätt. Det skulle ge den öppna polisen bättre möjligheter i satsningar mot både grov organiserad brottslighet och mängdbrottssatsningar. Mycket av det som senare avancerar till den nivån av brottslighet som avses i inhämtningslagen börjar mycket tidigare, med mindre allvarliga brott, som dessutom begås med hög frekvens.

Om man gör en jämförelse mellan inhämtningslagen och rättegångsbalkens regler i 27 kap. 18 § om hemlig avlyssning av elektronisk kommunikation (HAK) respektive gränsen för att kunna bryta sjukvårdssekretessen enligt 10 kap. 23§ offentlighet- och sekretesslagen, verkar båda de senare bestämmelserna avse mer integritetskränkande uppgifter än de som polisen får tillgång till via inhämtningslagen. HAK omfattar brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år eller brott där straffvärdet i det enskilda fallet kan anses uppgå till denna nivå. Här öppnar lagstiftaren upp för att besluta om en HAK för t.ex. grova stölder eller grov misshandel utan särskilda syften om straffvärdet kan anses uppgå till två år eller mer. Sjukvårdssekretessen avser brott för vilka inte är föreskrivet lindrigare straff än fängelse i ett år.

10.2 Ekobrottsmyndighetens hemställan

Polismyndigheten ställer sig bakom Ekobrottsmyndighetens hemställan om möjligheter att inhämta uppgifter även för vissa brott i deras brottskatalog.

I den myndighetsgemensamma satsningen mot grov och organiserad brottslighet är det tydligt att ett sådant behov finns. Brott med koppling till näringsverksamhet har identifierats som särskilt allvarlig och samhällshotande då grovt kriminella individer använder företag som brottsverktyg. Brott med koppling till näringsverksamhet betraktas av samverkansrådet som ett av huvudkriterierna för gemensamma brottsbekämpande myndighetsinsatser.

1.7 Förslag till förordning om ändring i förordningen (2003:396) om elektronisk kommunikation

Polismyndigheten befarar att förslaget om en ny bestämmelse (36 b §) i förordningen om elektronisk kommunikation kan innebära att frågor om delegation och dokumentationsskyldighet i framtiden skulle medföra en omfattande beslutsadministration. Utredningarnas handläggningstider skulle bli avsevärt längre och kostnaderna kring dessa kommer att öka betydligt.

Polismyndigheten anser dock, i linje med vad som föreslås i betänkandet, att det är rimligt med krav på dokumentation av inhämtningsbeslut av sådana abonnemangsuppgifter som avses i den förslagna 36 b §, men att en sådan dokumentation och även hanteringen och detaljregleringen av delegation gällande inhämtningsbeslut ska hanteras inom respektive myndighet.

I det fall en åklagare är förundersökningsledare skulle handläggningstiderna ytterligare förlängas i och med att en polisanställd skulle behöva inhämta beslut från åklagaren. Därtill skulle även ett omfattande och dyrbart utvecklingsarbete avseende beslutsadministration mellan polis och åklagare behöva genomföras innan ikraftträdandet. Utvecklingsarbetet skulle enligt Polismyndighetens bedömning behöva hanteras inom ramen för det s.k. RIF-arbetet, *Rättväsendets informationsförsörjning*, då det berör information som behöver skickas mellan Åklagarmyndigheten och brottsutredande myndigheter. Eftersom RIF-arbetet är komplext, då det berör flera av rättskedjans myndigheter, är det inte realistiskt att hinna genomföra erforderligt IT-utvecklingsarbete inom rättskedjans myndigheter innan den 1 juli 2016 då förslaget föreslås träda i kraft.

Angående det föreslagna kravet på dokumentation så skulle det medföra längre handläggningstider och en minskad effektivitet i rättskedjan. Polismyndigheten skulle behöva genomföra utvecklingsarbete avseende flera av sina IT-stöd då behov av sådana abonnemangsuppgifter uppstår såväl vid underrättelseverksamhet som vid förundersökning. Mot denna bakgrund är det inte rimligt att så väsentligt komplicera något som idag är en löpande verksamhet inom såväl polisen som inom de övriga brottsbekämpande myndigheterna, utan att göra en noggrant genomförd konsekvensanalys avseende framförallt kostnader och utökade handläggningstider.

Inhämtning av abonnemangsuppgifter utgör inte hemlig tvångsmedelsanvändning och enligt utredningens uppfattning så råder det inte heller någon tvekan om att abonnemangsuppgifter typiskt sett är klart mindre integritetskänsliga än många andra kategorier av uppgifter, t.ex. trafik- och lokaliseringsuppgifter.[1] Enligt utredningens mening är det dessutom svårt att se att inhämtningen av abonnemangsuppgifter skulle vara förknippad med några direkta risker för felaktig rättstillämpning.[2] Med bakgrund av utredningens resonemang är det för Polismyndigheten svårt att se att dokumentationsskyldigheten, likalydande den som finns i inhämtningslagen är nödvändig.

Synpunkten att placeringen av bestämmelsen inte är idealisk delas av Polismyndigheten och ett förtydligande bör göras om att bestämmelsen vänder sig till de brottsbekämpande myndigheterna och inte till leverantörer av elektronisk kommunikation. När brottsbekämpande myndigheter begär abonnemangsuppgifter ska leverantören bara få veta vilka uppgifter som myndigheten begär tillgång till och att begäran avser ett beslut enligt 6 kap. 22 § första stycket 2 LEK. Själva beslutet ska således inte leverantören som utför verkställigheten kunna begära in från brottsbekämpande myndighet.

10.4 NAT-teknik

Det utrycks i betänkandet att det inte ingår i uppdraget att föreslå åtgärder som innebär att lagringsskyldighetens omfattning utökas och därför har inte frågan avseende NAT-teknik utretts i betänkandet. Polismyndighetens uppfattning är dock att lagringskategorin "identifiera källan och slutmålet" omfattar både publik IP-adress såväl som den NAT:ade adress som används. Detta innebär att problemen som framförts avseende NAT-tekniken gäller den nuvarande lagringsskyldigheten och därför borde ingå i uppdraget.

Regeringen anförde i Lagring av trafikuppgifter för brottsbekämpande ändamål – genomförande av direktiv 2006/24/EG (prop. 2010/11:46) att lagringskravet bör utformas utifrån ändamålen med lagringen, nämligen att spåra och identifiera kommunikationskällan, slutmålet för kommunikationen, datum, tidpunkt och varaktighet för kommunikationen, typen av kommunikation, kommunikationsutrustningen samt lokaliseringen av mobil kommunikationsutrustning (6 kap. 16 a § i LEK.)[3]

Regeringen anförde även i propositionen gällande dynamiska IP-adresser (IP-adresser som byts slumpvis och oregelbundet) att dessa uppgifter begränsas så att endast brottsbekämpande myndigheter kan få tillgång till uppgifterna för att avslöja, utreda och åtala brott. Detta får anses innebära att lagstiftarens mening är att dynamiska IP-adresser ska lagras och lämnas ut till Polisen. Lagringsskyldigheten omfattar således dynamiska IP-adresser. [4] Lagrar operatören endast IP-adressen och inte NAT:ade adressen kan inte källan eller slutmålet identifieras utan kan teoretiskt avse trafik till maximalt 65536 användare.

---

[1] SOU 2015:31 sid. 186
[2] SOU 2015:31 sid. 191
[3] Prop. 2010/11:46 sid 27-28
[4] Prop. 2010/11:46 sid. 24-25

Följden av att användaren av IP- adresser inte kan spåras leder till att utredningar försvåras eller att brott inte kan styrkas. Post- och telestyrelsens skrivelse till Ekobrottsmyndigheten[5] är inte ett beslut och ska därför inte ses som ett slutligt ställningstagande från tillsynsmyndigheten. Polismyndigheten har även inlämnat en anmälan gentemot vissa teleoperatörer till Post- och telestyrelsen som inte lagrat NAT:ade adresser, vilket i skrivande stund inte lett till någon åtgärd.[6]

Med anledning av ovanstående vill Polismyndigheten framföra att ett förtydligande önskas avseende att lagringsskyldigheten även omfattar NAT:ade adresser. Post- och telestyrelsens skrivelse samt utredningens skrivning om detta har lett till att fler ännu teleoperatörer nu inte lagrar NAT:ade adresser. Med tanke på den ökade internetrelaterade brottsligheten är det av yttersta vikt att denna fråga förtydligas och klargörs från lagstiftarens sida så fort som möjligt.

POLISMYNDIGHETEN

Eva Lindeblad
Chef för enheten för rättslig styrning och stöd

Anna Olander Selldén
Jurist, föredragande

Kopia till

Justitiedepartementet, PO
Arbetstagarorganisationerna
Rikspolischefens kansli

[5] Dnr. 15-1185
[6] Dnr A150.918/2015 2015-04-20