

Datum
2019-12-02

Diarienummer
2019-20953-2

Mottagare
Infrastrukturdepartementet
103 33 Stockholm

Er referens
I2019/02319/D

Promemorian Genomförande av direktivet om inrättande av en kodex för elektronisk kommunikation

Säkerhetspolisen lämnar följande synpunkter på promemorian.

Sammanfattning

- Alla olika typer av begäran om tillträde bör kunna avslås om det finns en risk för skada för allmän säkerhet, totalförsvaret eller Sveriges säkerhet i övrigt.
- Förslaget innebär att det i vissa fall kommer att finnas en rapporteringsskyldighet för incidenter både enligt säkerhetsskyddstiftningen och lagen om elektronisk kommunikation. Post- och telestyrelsen behöver vidta åtgärder för att säkerställa att incidentrapportering även sker i enlighet med säkerhetsskyddslagstiftningen.
- Kraven på lagring bör vara desamma för alla som tillhandahåller elektroniska kommunikationstjänster. Det är en mycket stor brist att frågan om lagringsskyldighet för nummeroberoende interpersonella kommunikationstjänster inte övervägts inom ramen för det aktuella lagstiftningsarbetet. Det är mycket angeläget att frågan omedelbart utreds.
- Genom förslagen införs anpassningsskyldighet och uppgiftsskyldighet för nummeroberoende interpersonella kommunikationstjänster utan att detta har analyserats närmare i promemorian. Sådana skyldigheter är välkomna men den föreslagna regleringen ger upphov till tolknings- och tillämpningsfrågor som inte har behandlats i promemorian.

Datum

2019-12-02

Diarienummer

2019-20953-2

6. Lagens syfte

Säkerhetspolisen tillstyrker förslaget att det införs en portalparagraf om att elektroniska kommunikationers betydelse för bland annat Sveriges säkerhet ska beaktas vid tillämpningen av lagen.

13.3 Tillträde till fysisk infrastruktur för att montera trådlösa accesspunkter med kort räckvidd

Säkerhetspolisen tillstyrker förslaget att vissa myndigheter ska vara helt undantagna från skyldigheten att medge tillträde. Det föreslås i promemorian att regeringen i förordning bör bestämma vilka myndigheter som ska omfattas av undantaget. Vid bedömningen av vilka myndigheter som ska vara undantagna bör tillämpningsområdet för säkerhetsskyddslagen (2018:585) tjäna som vägledning.

15.9 Tillträde

En operatör som har identifierats som ett företag med betydande inflytande på en marknad bör anses bedriva säkerhetskänslig verksamhet enligt 1 kap. 1 § säkerhetsskyddslagen. Det kan uppstå situationer där sådana operatörer behöver neka tillträde till specificerade nätdelar och tillhörande faciliteter, informationssystem m.m. för att upprätthålla kravet på säkerhetsskydd. Det är därför viktigt att Post- och telestyrelsen kan avslå en begäran på den grunden att ett tillträde kan medföra en risk för skada för allmän säkerhet, totalförsvaret eller Sveriges säkerhet i övrigt. Detta bör uttryckligen anges i den aktuella bestämmelsen.

15.12 Tillträde till infrastruktur för anläggning av nät

Enligt samma resonemang som anförts angående förslaget i avsnitt 15.9 så bör Post- och telestyrelsen ha en möjlighet att avslå en begäran då ett tillträde till infrastruktur för anläggning av nät kan medföra en risk för skada för allmän säkerhet, totalförsvaret eller Sveriges säkerhet i övrigt. Detta bör uttryckligen anges i den aktuella bestämmelsen.

15.19 Tillträde till nät närmast slutanvändaren

Enligt samma resonemang som anförts angående förslaget i avsnitt 15.9 så bör Post- och telestyrelsen ha en möjlighet att avslå en begäran då ett tillträde till nät närmast slutanvändaren kan medföra en risk för skada för allmän säkerhet, totalförsvaret eller Sveriges säkerhet i övrigt. Detta bör uttryckligen anges i den aktuella bestämmelsen.

17.13 Tjänsters tillgänglighet vid extraordinära händelser i fredstid

Säkerhetspolisen vill påtala att förslaget såvitt avser att tillhandahållare ska se till att tjänsten uppfyller rimliga krav på tillgänglighet vid extraordinära händelser i fredstid inte synes motsvara direktivets krav. Av direktivet framgår att medlemsstaterna ska vidta alla nödvändiga åtgärder för att säkerställa största möjliga tillgång vilket måste anses utgöra ett starkare krav än vad som föreslås i nationell rätt.

18.4 Incidentrapportering

Förslaget innebär att det i vissa fall kommer att finnas en rapporteringsskyldighet för incidenter både enligt säkerhetsskyddslagstiftningen och lagen om elektronisk kommunikation. Det finns en risk att så inte sker utan att rapportering endast görs till Post- och telestyrelsen, som då måste ha rutiner för att säkerställa att informationen även kommer Säkerhetspolisen till del. Vid incidenter som rör säkerhetskänslig verksamhet kommer innehållet i rapporterna att innehålla säkerhetsskyddsklassificerade uppgifter. Post- och telestyrelsen måste därför säkerställa att informationen kan tas emot och lämnas till Säkerhetspolisen på ett sätt som uppfyller säkerhetsskyddslagstiftningens krav på informationssäkerhet.

18.5.2 Lagring och annan behandling av trafikuppgifter för brottsbekämpande ändamål

Kraven på lagring bör vara desamma för alla som tillhandahåller elektroniska kommunikationstjänster

I promemorian konstateras att användningen av traditionella kommunikationstjänster minskar till förmån för nya nummeroberoende interpersonella kommunikationstjänster. Så är även fallet bland personer som är verksamma inom organiserad brottslighet och terrorism. Det är därför mycket olyckligt att det inom ramen för det aktuella lagstiftningsarbetet inte närmare har utretts vilka krav som bör ställas på sådana tjänster angående lagring utan att frågan föreslås skjutas på framtiden.

Nyttan och behovet av tillgången till lagrade uppgifter är desamma för de brottsbekämpande myndigheterna oavsett vilken typ av interpersonell kommunikationstjänst som använts. I promemorian presenteras inte några argument för varför nummeroberoende interpersonella kommunikationstjänster ska vara undantagna från lagringsskyldigheten. Tvärtom tycks det innebära en snedvridning av konkurrensen mellan till synes likvärdiga tjänster. Att även i fortsättningen undanta nummeroberoende interpersonella tjänster från lagringsskyldigheten riskerar

Datum

2019-12-02

Diarienummer

2019-20953-2

att i än högre grad än idag påtagligt försvåra möjligheterna att förebygga och bekämpa grov brottslighet.

I sammanhanget bör även uppmärksammas att flera av de stora tillhandahållarna av nummeroberoende interpersonella kommunikationstjänster såsom Apple, Google, Facebook, Microsoft och WhatsApp sedan en tid tillbaka deltar i det internationella arbetet med att ta fram standarder för att underlätta överföring av uppgifter till de brottsbekämpande myndigheterna. Säkerhetspolisen uppfattar att anledningen till detta är att EU antog direktivet om inrättande av en europeisk kodex för elektronisk kommunikation och att tillhandahållarna bygger upp en beredskap för att kunna leverera uppgifter till brottsbekämpande myndigheter i de länder där de åläggs sådana skyldigheter till följd av direktivet. De brottsbekämpande myndigheterna i Sverige riskerar alltså att halka efter i en europeisk jämförelse om nummeroberoende interpersonella kommunikationstjänster undantas från lagringsskyldigheten.

Med anledning av vad som anförts ovan är det mycket angeläget att lagringsskyldighet för nummeroberoende interpersonella kommunikationstjänster omedelbart utreds.

Förslagen i promemorian bygger på en felaktig utgångspunkt

I promemorian anges att nummeroberoende interpersonella kommunikationstjänster inte omfattas av reglerna om hemliga tvångsmedel. Detta påstående är felaktigt.

Bestämmelserna om hemliga tvångsmedel är teknikneutrala och helt oberoende av exempelvis reglerna om lagring. I 27 kap. 18 och 19 §§ rättegångsbalken anges *telefonnummer eller annan adress* som den identifikator som kan avlyssnas respektive övervakas. Adress har i detta sammanhang samma betydelse som teleadress hade i tidigare reglering.¹ När begreppet teleadress infördes (och ersatte teleanläggning) angav regeringen att en teleadress kan vara ett abonnemang, en enskild anknytning, adressen för elektronisk post, en kod eller någon annan motsvarande tillförlitlig identifieringsmetod.²

Regeringen angav vidare att genom att man inte uttömmande anger vilka identifieringsmöjligheter som får användas kan tvångsmedlet tillämpas oberoende av om det är fråga om en traditionell fysisk avgränsning, t.ex. en viss ledning till en viss byggnad med en viss telefonapparat, eller om IT-användningen har skapat nya möjligheter till identifiering av vissa telemeddelanden. En sådan reglering gör det alltså möjligt att anpassa tillståndsprovningen till nya förutsättningar på teleområdet och

¹ Prop. 2011/12:55 s.62.

² Prop. 1994/95:227 s. 21.

Datum

2019-12-02

Diarienummer

2019-20953-2

komplexa resonemang om vilka tekniska åtgärder som aktualiseras kan delvis undvikas.³

Det finns med andra ord inget som hindrar att ett tillståndsbeslut kopplas till ett specifikt konto på en nummeroberoende interpersonell kommunikationstjänst. Att så inte sker i dagsläget beror i stället på att tillhandahållare av sådana tjänster enligt nu gällande rätt saknar en anpassningsskyldighet.

18.5.3 Andra bestämmelser om behandling av uppgifter

Förslaget innebär att en anpassningsskyldighet införs för nummeroberoende interpersonella kommunikationstjänster

I promemorian föreslås att bestämmelsen om den s.k. anpassningsskyldigheten i 6 kap. 19 § lagen (2003:389) om elektronisk kommunikation ska föras över till den nya lagen. Då den nya definitionen av elektroniska kommunikationstjänster omfattar nummeroberoende interpersonella kommunikationstjänster kommer tillhandahållare av sådana tjänster få en skyldighet att bedriva verksamheten så att beslut om hemlig avlyssning och hemlig övervakning av elektronisk kommunikation kan verkställas.

Detta är välkommet och kan innebära nya möjligheter för de brottsbekämpande myndigheterna att ta del av meddelanden som överförs med en nummeroberoende interpersonell kommunikationstjänst i klartext. När sådan kommunikation i dagsläget inhämtas från en operatör är den i regel krypterad.

Frågan berörs dock överhuvudtaget inte i promemorian, vilket riskerar att ge upphov till tolknings- och tillämpningsfrågor när det gäller omfattningen av anpassningsskyldigheten. Detta särskilt eftersom en verkställighet av hemlig avlyssning hos en sådan tillhandahållare skulle behöva ske på ett annat sätt än hos en operatör.

Förslaget innebär att en uppgiftsskyldighet införs för nummeroberoende interpersonella kommunikationstjänster

I promemorian föreslås att uppgiftsskyldigheten i 6 kap. 22 § lagen om elektronisk kommunikation föras över till den nya lagen. Då den nya definitionen av elektroniska kommunikationstjänster omfattar nummeroberoende interpersonella kommunikationstjänster kommer även tillhandahållare av sådana tjänster att få en uppgiftsskyldighet.

Möjligheten att begära ut uppgifter hos tillhandahållare av elektroniska kommunikationstjänster är ett mycket viktigt verktyg i Säkerhetspolisens brottsbekämpande arbete. Att även nummeroberoende interpersonella

³ A.a.

Datum

2019-12-02

Diarienummer

2019-20953-2

kommunikationstjänster föreslås omfattas av uppgiftsskyldigheten är därför oerhört positivt.

Frågan berörs dock överhuvudtaget inte i promemorian, vilket riskerar att ge upphov till tolknings- och tillämpningsfrågor när det gäller omfattningen av uppgiftsskyldigheten. Detta särskilt eftersom tillhandahållare av nummeroberoende interpersonella kommunikationstjänster föreslås undantas från anmälningsskyldigheten och de flesta sådana dessutom är utländska företag.

20.6 Lösning av tvister

Tvister om tillträde för att sätta upp trådlösa accesspunkter med kort räckvidd eller för att ansluta sådana accesspunkter till ett stamnät

I promemorian föreslås att tillsynsmyndigheten ska höra Försvarmakten och Myndigheten för samhällsskydd och beredskap i frågor som rör totalförsvaret och Säkerhetspolisen när det gäller frågor om Sveriges säkerhet i övrigt. Säkerhetspolisen bedömer att det inte är möjligt att på detta mycket förenklade sätt göra denna gränsdragning mellan totalförsvaret och Sveriges säkerhet i övrigt. Säkerhetspolisen har en betydande roll inom totalförsvaret och utgör i andra sammanhang samrådsmyndighet i frågor som rör totalförsvaret, se t.ex. förordning (2016:320) om skydd för geografisk information och Förbättrad skydd för totalförsvaret (SOU 2019:34). Regleringen för detta förfarande bör utformas på motsvarande sätt som regleringen för det samrådsförfarande som tillsynsmyndigheten ska ha med Säkerhetspolisen och Försvarmakten i tillståndsärenden (jfr. prop. 2019/20:15 s. 35).

I det fortsatta arbetet behöver även noggranna sekretessöverväganden göras i fråga om sådana uppgifter som samrådsmyndigheterna kommer att behöva lämna till tillsynsmyndigheten inom ramen för det aktuella förfarandet.

I händelse av att tillsynsmyndigheten fattar beslut som går emot en samrådsmyndighets uppfattning bör samrådsmyndigheten ha möjlighet att överklaga ett sådant beslut (jfr. prop. 2019/20:15 s. 39).

Överhuvudtaget är det viktigt att de förändringar i lagen om elektronisk kommunikation som föreslås i prop. 2019/20:15 förs över till den nya lagen och beaktas i det fortsatta arbetet.

21.4 Sanktionsavgift ska tas ut för vissa överträdelser

Säkerhetspolisen välkomnar förslaget att tillsynsmyndigheten ska ta ut en sanktionsavgift av den som inte uppfyller kraven i den nya lagen och i föreskrifter som har meddelats med stöd av lagen, t.ex. vad gäller att bedriva

Datum

2019-12-02

Diarienummer

2019-20953-2

sin verksamhet så att beslut om hemlig avlyssning och hemlig övervakning av elektronisk kommunikation kan ske.

28. Konsekvenser

I avsnitt 20.6 föreslås att tillsynsmyndigheten vid vissa tvistelösningsärenden ska höra Säkerhetspolisen. De ekonomiska konsekvenserna för Säkerhetspolisen med anledning av detta har inte övervägts i promemorian.

På senare tid har det i flera sammanhang föreslagits att Säkerhetspolisen ska vara samrådsinstans och utföra liknande arbetsuppgifter med hänsyn till Sveriges säkerhet. Säkerhetspolisen har konsekvent pekat på att sådana ytterligare arbetsuppgifter inte ryms inom det befintliga anslaget utan att medel behöver tillskjutas.

I Säkerhetspolisens remissvar till betänkandet Kompletteringar till den nya säkerhetsskyddslagen (SOU 2018:82) framfördes att det förändrade uppdraget, som bl.a. innefattar att vara samrådsinstans, uppskattningsvis kommer att kräva ett fyrtiotal ytterligare årsarbetskrafter.

I remissvaret till betänkandet Förbättrat skydd för totalförsvaret (SOU 2019:34) uppskattades det tillkommande resursbehovet till tio årsarbetskrafter.

I remissvaret till betänkandet Frekvenser i samhällets tjänst (SOU 2019:92) framfördes att myndigheten inte i dag har möjlighet att fullgöra de uppgifter som föreslås utan att göra avkall på annan verksamhet och att det därför är nödvändigt att Säkerhetspolisen tillförs ytterligare anslagsmedel.

Även det nu föreslagna samrådsförfarandet kommer att innebära ett ytterligare behov av årsarbetskrafter.
