Utkastet
Ärendenummer: VN/25156/2023
Datum: 15.2.2024

Sammandrag av utkastet till bedömningspromemoria:

Skyldighet att lagra förmedlingsuppgifter om elektronisk kommunikation – Bedömningspromemoria om alternativ för att precisera den nationella lagstiftningen

Inledning

Bestämmelser om skyldighet att lagra förmedlingsuppgifter om elektronisk kommunikation för myndigheternas behov finns i 157 § i lagen om tjänster inom elektronisk kommunikation (917/2014, nedan *kommunikationstjänstlagen*). Den skyldighet att lagra förmedlingsuppgifter som det föreskrivs om i paragrafen grundar sig på direktivet om integritet och elektronisk kommunikation[1]. Med stöd av artikel 15.1 i direktivet har medlemsstaterna möjlighet att begränsa omfattningen av vissa rättigheter och skyldigheter som anges i direktivet.

Skyldigheten att lagra uppgifter enligt 157 § i kommunikationstjänstlagen är ett undantag från huvudregeln i direktivet om integritet och elektronisk kommunikation. Utgångspunkten för direktivet är att förmedlingsuppgifter om kommunikation, så kallade trafik- och lokaliseringsuppgifter, bör utplånas eller avidentifieras när de inte längre behövs för förmedling av kommunikation. Bakgrunden till detta är skyddet av de grundläggande fri- och rättigheterna. Det har dock ansetts nödvändigt att göra undantag från utgångspunkten i direktivet för förundersöknings- och underrättelsemyndigheterna till exempel för att utreda flera brott, åtalspröva brott och trygga den nationella säkerheten. Lagringen av uppgifterna uppfyller alltså ett godtagbart mål av allmänt intresse som i sista hand återgår till statens skyldighet att trygga rätten till liv. Utöver ett godtagbart mål ska det säkerställas att begränsningar i de grundläggande fri- och rättigheterna görs på ett sätt som kan anses vara godtagbart med avseende på de grundläggande fri- och rättigheterna överlag. Bedömningen ska göras med tanke på både EU:s stadga om de grundläggande rättigheterna och grundlagen.

Kommunikationsministeriet tillsatte den 26 oktober 2023 en arbetsgrupp som ska stödja preciseringen av lagstiftningen om lagringsskyldighet i fråga om elektronisk kommunikation. I arbetsgruppen deltar utöver kommunikationsministeriet också representanter för justitieministeriet,

[1] Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktivet om integritet och elektronisk kommunikation, även kallat ePrivacy-direktivet)

inrikesministeriet och försvarsministeriet. Arbetsgruppen har till uppgift att ta fram ett kunskapsunderlag till stöd för den kommande ändringen i lagstiftningen. Syftet med arbetsgruppens arbete är att göra en utredning där man bedömer olika alternativ för hur den nationella lagstiftningen om lagring av förmedlingsuppgifter och myndigheternas tillgång till dem ska ordnas för att lagstiftningen ska vara förenlig med Finlands grundlag och EU:s stadga om de grundläggande rättigheterna samt EU-domstolens rättspraxis, vara begränsad till vad som är nödvändigt med tanke på skyddet för privatlivet och samtidigt garantera myndigheterna proportionerlig tillgång till uppgifterna för att säkerställa en effektiv brottsbekämpning. De alternativ för organiseringen av lagringsskyldigheten som granskas i bedömningspromemorian ska utredas närmare genom att ett utkast till regeringsproposition bereds.

Under utarbetandet av bedömningspromemorian har man hört lagringsskyldiga företag, myndigheter som utnyttjar uppgifterna, Transport- och kommunikationsverket Traficom samt finansministeriet.

I denna bedömningspromemoria utvärderas preliminärt olika alternativ för hur lagringen av förmedlingsuppgifter och myndigheternas tillgång till uppgifterna ska ordnas nationellt för att säkerställa bekämpningen av brottsligheten och trygga den allmänna säkerheten och den nationella säkerheten. Bedömningspromemorian fokuserar på skyldigheten att lagra förmedlingsuppgifter och tillgången till dessa uppgifter uttryckligen med avseende på direktivet om integritet och elektronisk kommunikation. I bedömningspromemorian behandlas inte till exempel frågor som hänför sig till upphovsrättsdirektivet eller sådana frågor som behandlats i EU-domstolens avgöranden och som inte direkt hänför sig till lagringsskyldigheten.

I 157 § i lagen om tjänster inom elektronisk kommunikation föreskrivs det om en skyldighet för särskilt utsedda teleföretag att lagra förmedlingsuppgifter om elektronisk kommunikation. Skyddet för förtroliga meddelanden (10 § i grundlagen) gäller också förmedlingsuppgifter om kommunikation. Huvudregeln är att konfidentialitet vid kommunikation garanteras i enlighet med EU:s stadga om de grundläggande rättigheterna (ePrivacy-direktivet) och nationellt genom lagen om tjänster inom elektronisk kommunikation. Förmedlingsuppgifterna om elektronisk kommunikation är dock nödvändiga för förundersöknings- och underrättelsemyndigheterna för skötseln av deras uppgifter, såsom förhindrande och utredning av brott. Lagring och användning av förmedlingsuppgifter om elektronisk kommunikation för myndighetsbehov innebär en betydande begränsning av skyddet för privatlivet och skyddet för personuppgifter. Därför ska det föreskrivas särskilt om detta genom lag.

Förmedlingsuppgifter om kommunikation är uppgifter som lagras hos teleoperatören om förmedling av kommunikation, såsom uppgifter om från vilket nummer det har ringts till ett annat nummer och vid vilken tidpunkt. Teleoperatörerna behöver behandla förmedlingsuppgifter om kommunikation till exempel för att genomföra tjänsten och fakturera för den. Behandling av uppgifterna är tillåten endast i den omfattning som föreskrivs i lag. På behandlingen av uppgifterna tillämpas i huvudsak ePrivacy-direktivet, men till de delar det inte finns några särskilda bestämmelser i direktivet ska EU:s allmänna dataskyddsförordning (EU) 2016/679 tillämpas på behandlingen av uppgifterna.

EU-domstolen har under de senaste åren meddelat flera förhandsavgöranden och behovet att ändra den nationella lagstiftningen till följd av dem har bedömts regelbundet under kommunikationsministeriets ledning (åren 2017, 2021 och 2023). Utifrån bedömningen och

justitiekanslersämbetets utlåtande har man kommit fram att det finns ett behov att precisera den nationella lagstiftningen.

Enligt EU-domstolens rättspraxis bör skyldigheten att lagra uppgifter basera sig på objektiva och icke-diskriminerande kriterier, och i regel har en allmän och odifferentierad lagringsskyldighet i syfte att bekämpa brottslighet enligt EU-domstolen stridit mot unionsrätten. Av denna anledning har flera EU-medlemsländer varit tvungna att ändra sin lagstiftning. EU-domstolens rättspraxis utvecklas fortfarande, eftersom flera sådana begäran om förhandsavgörande fortfarande är under behandling vid domstolen som kan inverka på den nationella lagstiftningen.

En del av EU-medlemsländerna, till exempel Danmark, Irland och Belgien, har ändrat sin nationella lagstiftning i enlighet med de lagringsåtgärder som domstolen bedömt i rättspraxis. Också i Sverige har det utarbetats ett förslag till en motsvarande reglering. En del av medlemsländerna, såsom Nederländerna och Portugal, har ingen gällande reglering om lagringsskyldighet i fråga om förmedlingsuppgifter. Också Tysklands nationella domstol har efter EU-domstolens avgörande upphävt den nationella lagstiftningen.

Utifrån jämförelsen kan det konstateras att medlemsstaterna har infört olika typer av skyldigheter. Medlemsstaterna verkar ha olika åsikter om vad lagringen ska gälla och när den är nödvändig. Detta kan dels bero på den politiska viljan eller den långsamma lagändringsprocessen, dels på medlemsstatsspecifika särdrag i förhållande till vilka till exempel en åtgärds nödvändighet bedöms nationellt.

Nuläge

I lagen om tjänster inom elektronisk kommunikation föreskrivs det om skyldigheten att lagra förmedlingsuppgifter om elektronisk kommunikation. Enligt 157 § i lagen utser inrikesministeriet genom sitt beslut[2] teleföretag (*lagringsskyldiga företag*) som har skyldighet att lagra uppgifter som hänför sig till de telefonitjänster eller textmeddelandetjänster i mobilnät (nedan mobilnätstjänster), internettelefonitjänster och internetaccesstjänster som företaget tillhandahåller.

I 157 § 3 mom. i kommunikationstjänstlagen föreskrivs det närmare om de uppgifter som ska lagras. De uppgifter som ska lagras bestäms per tjänstetyp.[3] I fråga om alla typer av tjänster ska man lagra uppgifter med vilkas hjälp en användare av kommunikationstjänster kan identifieras, uppgifter om abonnentens och den registrerade användarens namn och adress, abonnemangets identifieringsuppgifter samt tidpunkt och varaktighet för transaktionen eller användningen av kommunikationstjänsten. I fråga om mobilnätstjänster och internettelefonitjänster ska man också specificera meddelandets typ och mottagare samt transaktioner. I fråga om mobilnätstjänster ska lagringsskyldiga företag också lagra uppgifter om positionen för den kommunikationsutrustning som använts. I de uppgifter som ska lagras ingår i fråga om internetaccesstjänster abonnemangets installeringsadress samt i fråga om mobilnätstjänster positionen för den utrustning som använts för kommunikationen när transaktionen inleddes. Enligt 5 mom. gäller lagringsskyldigheten inte innehållet i meddelanden eller förmedlingsuppgifter som samlats vid bläddring av webbsidor.

[2] Inrikesministeriets beslut SM1523258, 27.02.2015. SMDno-2014-3051.
[3] Kommunikationsverket kan med stöd av 157 § 8 mom. i kommunikationstjänstlagen meddela preciserande föreskrifter om de uppgifter som ska lagras. Bestämmelser om de uppgifter som ska lagras finns i Kommunikationsverkets föreskrift 53 B/2014 M som meddelats 17.12.2014.

Tiden för skyldigheten att lagra uppgifter är från det att transaktionen inleds i fråga om mobilnätstjänster 12 månader, i fråga om internettelefonitjänster 9 månader och i fråga om internetaccesstjänster 6 månader från det att transaktionen inleds (157 § 4 mom. i kommunikationstjänstlagen).

Enligt 157 § i kommunikationstjänstlagen får uppgifterna endast användas för att utreda och åtalspröva brott som avses i 10 kap. 6 § 2 mom. i tvångsmedelslagen (806/2011). Bestämmelser om rätt att få uppgifter finns däremot annanstans i lag. Förmedlingsuppgifter om elektronisk kommunikation som omfattas av lagringsskyldigheten enligt 157 § i kommunikationstjänstlagen fås inom förundersökning, civil underrättelseinhämtning och militär underrättelseinhämtning med hjälp av teleövervakning (i efterhand). Alla förundersökningsmyndigheter enligt förundersökningslagen (805/2011), det vill säga polisen[4], Tullen, Gränsbevakningsväsendet och försvarsmakten, kan i vissa situationer få uppgifter som ska lagras med stöd av 157 § i kommunikationstjänstlagen för att utreda och åtalspröva brott i förundersökning, eftersom varje förundersökningsmyndighet ansvarar för förundersökningen av åtminstone vissa sådana brott som uppfyller kriterierna i 10 kap. 6 § 2 mom. i tvångsmedelslagen. Dessutom föreskrivs det i myndighetsspecifika lagar om användningen av hemliga metoder för inhämtande av information för att förhindra eller avslöja brott och avvärja fara.

Användningsändamålet för de förmedlingsuppgifter som ska lagras med stöd av 157 § i kommunikationstjänstlagen har genom lagen om civil underrättelseinhämtning avseende datatrafik och lagen om militär underrättelseverksamhet från år 2019 utvidgats att gälla ändamål som avser den nationella säkerheten. Bestämmelser om användning av uppgifter som lagras med avseende på den nationella säkerheten finns i 5 a kap. i polislagen och i lagen om militär underrättelseverksamhet (590/2019).[5] Villkoren för att få uppgifter motsvarar i stora drag bestämmelserna i tvångsmedelslagen.

Villkor enligt EU-lagstiftningen och konstitutionella villkor

När det gäller bestämmelserna i EU:s stadga om de grundläggande rättigheterna bör deras tillämpningsområde beaktas. Enligt artikel 51.1 i stadgan om de grundläggande rättigheterna riktar sig bestämmelserna i stadgan, med beaktande av subsidiaritetsprincipen, till unionens institutioner, organ och byråer samt till medlemsstaterna endast när dessa tillämpar unionsrätten. Därför respekterar de rättigheterna enligt stadgan, följer principerna i den och främjar tillämpningen av dem i enlighet med sin behörighet och inom gränserna för unionens behörighet enligt unionsfördragen.

EU-domstolen har tolkat EU-rättens tillämpningsområde i fråga om lagringsskyldigheten i synnerhet i sitt QdN-avgörande[6]. Enligt domstolen omfattar tillämpningsområdet för direktiv 2002/58 sådan nationell reglering enligt vilken tillhandahållare av elektroniska kommunikationstjänster ska lagra trafikuppgifter och lokaliseringsuppgifter för att skydda den nationella säkerheten och bekämpa brottslighet.

[4] Med undantag för skyddspolisen.
[5] I detta sammanhang bör det beaktas att underrättelseinhämtning som avser datatrafik inte omfattas av begränsningarna i 157 § i kommunikationstjänstlagen, eftersom det inte inom underrättelseinhämtningen ställs lagringskrav som riktas till teleföretagen (se QdN punkterna 101–103).
[6] La Quadrature du Net-domen, de förenade målen C-511/18, C-512/18 och C-520/18.

Bestämmelserna om lagring av förmedlingsuppgifter om elektronisk kommunikation hör till tillämpningsområdet för EU-rätten. Det nationella handlingsutrymmet att föreskriva om skyldigheten att lagra förmedlingsuppgifter baserar sig på artikel 15 i direktivet om integritet och elektronisk kommunikation. Enligt artikeln får medlemsstaterna genom lagstiftning vidta åtgärder för att begränsa omfattningen av de rättigheter och skyldigheter som anges det direktivet när en sådan begränsning i ett demokratiskt samhälle är nödvändig, lämplig och proportionell för att skydda nationell säkerhet (dvs. statens säkerhet), försvaret och allmän säkerhet samt för förebyggande, undersökning, avslöjande av och åtal för brott eller vid obehörig användning av ett elektroniskt kommunikationssystem. Medlemsstaterna får för detta ändamål bland annat vidta lagstiftningsåtgärder som innebär att uppgifter får bevaras under en begränsad period som motiveras av de skäl som fastställs i denna punkt.

Uppräkningen av godtagbara skäl är uttömmande. Tillgång till uppgifterna måste vara faktiskt och strikt begränsad till de fall då tillgången krävs för ett av dessa syften, och syftet med lagstiftningen måste dessutom stå i proportion till hur allvarligt ingrepp i de grundläggande rättigheterna det innebär att ge tillgång till de lagrade uppgifterna. (målet Tele2[7], punkterna 90 och 115) Det saknar betydelse om de uppgifter som avser privatlivet är av känslig art eller ej eller om de berörda har fått utstå eventuella olägenheter på grund av ingreppet. (Ministerio Fiscal[8] punkt 51; Privacy International[9] punkt 70; QdN punkt 115) Det är inte heller relevant huruvida de lagrade uppgifterna därefter används eller inte. (QdN punkt 116)

EU-domstolen har meddelat flera avgöranden om tolkningen av artikel 15 i direktivet jämförd med stadgan om de grundläggande rättigheterna. På basis av detta har domstolen fastställt tillåtna lagringsskyldigheter utifrån en bedömning av hur allvarligt ingrepp i de grundläggande rättigheterna det innebär (se Tele2 punkt 115). Bakom detta ligger tanken att det vid lagring av förmedlingsuppgifter är fråga om ett undantag från huvudregeln som ska tolkas strikt. (Tele2 punkt 89) Lagring av dessa uppgifter får inte bli huvudregeln, eftersom det i stor utsträckning skulle förta verkan av den sistnämnda bestämmelsen (Tele2 punkt 89) och eftersom lagringsskyldigheten kan ha en avhållande inverkan på utövandet av de grundläggande rättigheterna (G.D.[10] punkt 65).

När det föreskrivs om lagringsskyldigheten, ska utöver mål av allmänt intresse också de allmänna förutsättningarna att en begränsning ska vara nödvändig, lämplig och proportionell enligt artikel 15.1 i direktivet om integritet och elektronisk kommunikation iakttas[11]. Dessa förutsättningar har i EU-domstolens praxis ansetts innefatta följande villkor och garantier:

1. Ett mål av allmänt intresse måste vägas mot rättigheterna i fråga. Skyddet för den grundläggande rätten till respekt för privatlivet kräver att undantag från och begränsningar av skyddet för personuppgifter ska inskränkas till vad som är strängt nödvändigt.

    1.1. En begränsning ska bedömas med hänsyn till hur allvarligt det ingrepp är som en sådan begränsning medför och det ska också kontrolleras att betydelsen av det mål av allmänt samhällsintresse som eftersträvas med denna begränsning står i rätt proportion till hur allvarligt ingreppet är. (QdN punkterna 130 och 131)

[7] Tele2-domen, förenade målen C-203/15 och C-698/15.
[8] Ministerio Fiscal-domen, mål C-207/16.
[9] Privacy International-domen, mål C-623/17.
[10] Garda Síochána-domen, mål C-140/20.
[11] Dessutom måste man beakta de allmänna förutsättningarna för begränsning av de grundläggande fri- och rättigheterna, även om de och de krav som presenteras här delvis går in i varandra.

1.2. Det föreligger en hierarki mellan målen av allmänt intresse beroende på deras betydelse. (G. D. punkt 56)

2. När det föreskrivs om lagringsskyldighet, ska bestämmelserna i den nationella lagstiftningen vara klara och precisa bestämmelser om åtgärdens omfattning och tillämpning.

2.1. Regelverket i fråga måste vara rättsligt bindande i nationell rätt. (Tele2 punkt 117)

2.2. I bestämmelserna ska minimikrav slås fast, så att de personer vars personuppgifter det är fråga om har tillräckliga garantier som möjliggör ett effektivt skydd av deras personuppgifter mot riskerna för missbruk. (Tele2 punkt 109)

2.2.1. Bestämmelserna måste särskilt precisera under vilka omständigheter och villkor en sådan åtgärd i fråga om behandling av uppgifter får vidtas. (Tele2 punkt 109)

2.2.2. Behovet av sådana garantier är särskilt stort när personuppgifter är föremål för automatiserad behandling, särskilt när det föreligger en betydande risk för otillåten åtkomst till uppgifterna. Dessa överväganden äger särskild giltighet när det är fråga om skyddet av den särskilda kategori av personuppgifter som utgörs av känsliga uppgifter (QdN punkt 132)

2.3. Lagringen av uppgifterna ska alltid uppfylla objektiva kriterier, som fastställer ett samband mellan de uppgifter som ska lagras och det eftersträvade syftet. (Tele2 punkt 110)

2.3.1. I synnerhet, vad avser bekämpning av allvarlig brottslighet, ska de uppgifter som ska lagras kunna bidra till att bekämpa, utreda eller åtalspröva allvarliga brott. (G. D. punkt 55)

2.4. I synnerhet måste de materiella villkoren vara sådana att de klart avgränsar åtgärdens omfattning och följaktligen den berörda personkretsen. (Tele2 punkt 110)

2.4.1. Den berörda personkretsens verksamhet ska kunna ha ens ett indirekt eller avlägset samband med det eftersträvade målet. (Tele2 punkt 105, QdN punkt 137)

2.4.2. De materiella villkoren kan variera utifrån vilka åtgärder som vidtas för att förebygga, undersöka, utreda och åtalspröva grov brottslighet. (Tele2 punkt 110)

2.5. Riktad lagringsskyldighet får inte vara diskriminerande. (QdN punkt 150)

2.5.1. Dessa överväganden äger särskild giltighet när det är fråga om skyddet av den särskilda kategori av personuppgifter som utgörs av känsliga uppgifter (QdN punkt 132)

3. När det föreskrivs om myndigheternas rätt att få förmedlingsuppgifter, bör det också föreskrivas om materiella och formella villkor för användningen.

3.1. Bestämmelser av detta slag måste vara rättsligt bindande enligt nationell rätt. (Tele2 punkt 117)

3.2. Det räcker inte att det i lagstiftningen krävs att myndigheternas rätt att få uppgifter motsvarar syftet med lagstiftningen i fråga, utan den måste även ange de materiella och

formella villkoren för de behöriga nationella myndigheternas tillgång till de lagrade uppgifterna. (Tele2 punkt 118, Privacy International punkt 77)

3.2.1. Regleringen ska innehålla klara och precisa bestämmelser som anger under vilka omständigheter och på vilka villkor leverantörer av elektroniska kommunikationstjänster måste ge behöriga nationella myndigheter tillgång till uppgifterna. (Tele2 punkt 117)

3.2.2. Regleringen måste vara grundad på objektiva kriterier som avgör under vilka omständigheter och på vilka villkor behöriga nationella myndigheter ska ges tillgång till uppgifterna i fråga (Privacy International punkt 78). Tillgång till förmedlingsuppgifter kan i princip beviljas i samband med syftet bekämpning av brott bara till uppgifter om personer som misstänks planera, begå eller ha begått ett allvarligt brott eller på något sätt vara inblandade i ett sådant brott. I särskilda fall, som när vitala intressen för nationell säkerhet, försvar eller allmän säkerhet hotas av terrorism, skulle dock tillgång kunna ges även till uppgifter om andra personer när det finns objektiva omständigheter som ger skäl att anta att de uppgifterna i ett konkret fall effektivt skulle kunna bidra till att bekämpa sådan verksamhet. (Tele2 punkt 119)

3.2.3. Behovet av sådana garantier är särskilt viktigt när personuppgifter är föremål för automatiserad behandling, särskilt när det föreligger en betydande risk för otillåten åtkomst till uppgifterna. (Privacy International punkt 68)

3.2.4. När det i bakgrunden finns (tillåten) generell och odifferentierad lagring, ska garantierna och villkoren i fråga om utnyttjande (bland annat kartläggning) vara stränga. (QdN punkt 156)

3.3. Ett villkor för tillgången till uppgifter är förhandskontroll av en domstol eller en oberoende förvaltningsmyndighet.[12] (Tele2 punkt 120)

3.3.1. Domstolen meddelar sitt avgörande eller myndigheten fattar sitt beslut efter det att myndigheterna framställt en motiverad ansökan inom ramen för ett förfarande för förebyggande, utredning eller åtalsprövning av brott. (Tele2 punkt 120)

3.3.2. Förhandskontroll innebär bland annat att den domstol eller det oberoende förvaltningsorgan som ska utföra denna kontroll har alla befogenheter och lämnar alla nödvändiga garantier för att kunna göra en vederbörlig avvägning mellan de olika legitima intressen och rättigheter som är i fråga. Vad särskilt gäller en brottsutredning kräver en sådan kontroll att denna domstol eller detta organ kan säkerställa en korrekt balans mellan de legitima intressen som inom ramen för brottsbekämpning gör sig gällande för att svara mot utredningens behov, å ena sidan, och de grundläggande rättigheter avseende respekt för privatlivet och skydd av personuppgifter som tillkommer de personer vars uppgifter kan komma att lämnas ut, å den andra sidan. (Prokuratuur[13] punkt 52)

3.3.3. När denna kontroll inte utförs av en domstol utan av en oberoende förvaltningsmyndighet måste denna myndighet ha en ställning som innebär att den

[12] I brådskande fall är efterhandskontroll tillåten.
[13] Prokuratuur-domen, mål C-746/18.

kan fullgöra sitt uppdrag på ett objektivt och opartiskt sätt, och den måste därför vara fri från all yttre påverkan. Det krav på oberoende som myndigheten med ansvar för förhandskontroll ska uppfylla innebär följaktligen att myndigheten måste vara fristående i förhållande till den som begär tillgång till uppgifterna, så att myndigheten kan utöva sin kontroll på ett objektivt och opartiskt sätt utan yttre påverkan. I synnerhet på det straffrättsliga området innebär kravet på oberoende att den myndighet som ska utföra förhandskontrollen dels inte får vara involverad i den aktuella brottsutredningen, dels ska ha en neutral ställning i förhållande till parterna i det straffrättsliga förfarandet. (Prokuratuur punkterna 53 och 54)[14]

3.3.4. Den nationella lagstiftningen ska uppfylla kraven i artikel 47 i stadgan om de grundläggande rättigheterna, vilket till exempel innebär att domstolens eller en oberoende myndighets beslut ska motiveras. (HYA m.fl.[15] punkterna 43, 44 och 46)

3.4. Tillgång får inte ges utöver vad som är strängt nödvändigt (Tele2 punkt 116) i förhållande till syftet med lagringen, vilket ska säkerställas genom tydliga och exakta bestämmelser i den nationella lagstiftningen. (Spetsializirana prokuratura (Bulgarien)[16] punkt 65) De behöriga nationella myndigheterna har ålagts att i varje enskilt fall säkerställa att både den eller de kategorier av uppgifter som avses och den tidsperiod som ansökan avser, med beaktande av omständigheterna i det enskilda fallet, begränsas till vad som är strängt nödvändigt för den aktuella utredningen. (Prokuratuur punkt 38)

3.5. Det är också viktigt att de behöriga nationella myndigheter som beviljats tillgång till lagrade uppgifter informerar de berörda personerna om detta, enligt tillämpliga nationella förfaranden, så snart en sådan upplysning inte längre riskerar att skada myndigheternas utredningar. (Tele2 punkt 121)

3.5.1. Unionsrätten utgör hinder för sådan nationell lagstiftning där de registrerades rätt till information inte tryggas i enlighet med unionslagstiftningen och utan att de registrerade har en besvärsväg mot lagstridig åtkomst. (Spetsializirana prokuratura (Bulgarien) punkt 76)

3.5.2. Användningen av lagrade uppgifter i brottsutredningar omfattas av tillämpningsområdet för dataskyddsdirektivet[17]. Enligt artikel 13 i direktivet får medlemsstaterna föreskriva om information till den registrerade. EU-domstolen

[14] EU-domstolen har bland annat ansett att en åklagarmyndighet som leder utredningsförfarandet och, i förekommande fall, väcker åtal inte kan anses vara fristående i förhållande till de legitima intressena, eftersom denna uppgift nämligen inte är att helt oavhängigt avgöra en tvist, utan att, i förekommande fall, hänskjuta tvisten till behörig domstol i egenskap av part i målet. Härav följer att en sådan åklagarmyndighet inte kan utföra förhandskontroll av begäran om tillgång till lagrade uppgifter (Prokuratuur punkterna 55 och 57). Unionsrätten utgör också hinder för en nationell lagstiftning enligt vilken en centraliserad handläggning av en begäran om tillgång till lagrade uppgifter, som polisen inkommit med inom ramen för en utredning av och åtal för grova brott, ska utföras av en polistjänsteman som biträds av en enhet inom polismyndigheten med ett visst mått av självständighet när den utför sina uppgifter och vars beslut senare kan bli föremål för en domstolsprövning. (G.D. punkt 114)
[15] HYA m.fl. –domen, mål C-349/21.
[16] Spetsializirana prokuratura –domen, mål C-350/21.
[17] Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF.

konstaterar dock att den bestämmelsen inte möjliggör att rätten till information helt utelämnas. (Spetsializirana prokuratura (Bulgarien) punkterna 68–71)

3.5.3. Bestämmelser om rätten till effektiva rättsmedel ska utfärdas i enlighet med artikel 54 i dataskyddsdirektivet. Utfärdande av närmare bestämmelser omfattas av nationell processuell autonomi, förutsatt att likvärdighets- och effektivitetsprinciperna iakttas. EU-domstolen anser dock att det inte är tillräckligt om det enda rättsmedlet är att domstolen beviljar tillgång till de lagrade uppgifterna enbart på begäran av de behöriga myndigheterna, utan att de berörda personerna har hörts och utan att domstolen har möjlighet att beakta eventuella invändningar från dessa. (Spetsializirana prokuratura (Bulgarien) punkterna 72–75)

3.6. Tillgång till uppgifter får endast beviljas när uppgifterna har lagrats av leverantören på ett sätt som är förenligt med artikel 15.1 i direktivet om integritet och elektronisk kommunikation. (Prokuratuur punkt 29)

4. Ändamålsenligt skydd av uppgifter som ska lagras samt begränsning av lagringen

4.1. För att säkerställa fullständig integritet och konfidentialitet för uppgifterna måste leverantörerna av elektroniska kommunikationstjänster garantera en särskilt hög skydds- och säkerhetsnivå genom lämpliga tekniska och organisatoriska åtgärder. (Tele2 punkt 122)

4.2. Den nationella lagstiftningen måste i synnerhet föreskriva att lagringen sker inom unionen och att uppgifterna oåterkalleligen förstörs när deras lagringstid gått ut. (Tele2 punkt 122)

4.3. Begränsningar som ställs i fråga om tillgången till information kan varken begränsa eller avhjälpa det allvarliga ingrepp som en generell lagring av dessa uppgifter innebär i individens rättigheter. (G. D. punkt 47)

4.3.1. Detta gäller också de garantier som föreskrivs i den nationella lagstiftningen, vilka syftar till att skydda de lagrade uppgifterna mot riskerna för missbruk och otillåten åtkomst. (SpaceNet[18] punkt 91)

4.3.2. Dataskyddsmyndighetens eller ett parlamentariskt organs övervakning av lagringen kan visserligen minska risken för otillåten åtkomst, men eliminerar inte den risk lagringen medför i fråga om individens grundläggande fri- och rättigheter. (Spetsializirana prokuratura (Bulgarien) punkt 59)

5. Medlemsstaterna måste garantera att en oberoende myndighet kontrollerar att den skyddsnivå som säkerställs i unionsrätten iakttas vad gäller skyddet för fysiska personer vid behandlingen av personuppgifter. (Tele2 punkt 123)

6. Direktivet om integritet och elektronisk kommunikation och EU-domstolens rättspraxis i fråga om det bör beaktas också när det annanstans i lagstiftningen föreskrivs om behandling av uppgifter om datakommunikation som innehas av leverantörer av elektroniska kommunikationstjänster. (VD och SR[19] punkterna 79 ja 82)

[18] SpaceNet-domen, de förenade målen C-793/19 och C-794/19.
[19] VD och SR-domen, de förenade målen C-339/20 och C-397/20.

Direktivet om integritet och elektronisk kommunikation preciserar och kompletterar EU:s allmänna dataskyddsförordning.[20] På behandling av personuppgifter tillämpas den allmänna dataskyddsförordningen till den del direktivet om integritet och elektronisk kommunikation inte innehåller särskilda bestämmelser som preciserar förordningen. Å andra sidan ska de särskilda bestämmelserna i direktivet iakttas.

Den gällande lagstiftningen om skyldighet att lagra förmedlingsuppgifter har stiftats med grundlagsutskottets medverkan (GrUU 18/2014 rd). Vid bedömningen av de alternativa åtgärderna finns det skäl att ta hänsyn till å ena sidan den grundlagsskyddade sekretessen för förtroliga meddelanden, och å andra sidan de godtagbara och samhälleligt vägande skäl som anknyter till intresset för att utreda allvarliga brott och det straffrättsliga systemets trovärdighet och som i viss mån talar för en begränsning av de grundlagsskyddade rättigheterna. Strävan att bekämpa allvarlig brottslighet är en grund som talar för bestämmelserna om skyldighet att lagra förmedlingsuppgifter om kommunikation. (GrUU 18/2014 rd, s. 7)

Bestämmelserna om skyldighet att lagra förmedlingsuppgifter är av betydelse med avseende på skyddet för privatlivet, skyddet för personuppgifter och skyddet för hemligheten i fråga om förtroliga meddelanden som tryggas i 10 § i grundlagen. Dessutom bör man beakta grundlagsutskottets praxis i anslutning till ändringen av 10 § 4 mom. i grundlagen. Dessa kan betraktas som utgångspunkt för den konstitutionella tolkningen av lagringsskyldigheten. Utöver innehållet i ett meddelande skyddar bestämmelserna i grundlagen också identifikationsuppgifterna om meddelandets avsändare och mottagare samt övriga uppgifter som kan ha betydelse för att meddelandet ska förbli förtroligt. Enligt grundlagsutskottet ger unionsdomstolens Digital Rights Ireland-dom skäl att i viss mån omvärdera frågan om identifieringsuppgifter för elektroniska meddelanden med avseende på bestämmelserna om förtroliga meddelanden i 10 § i grundlagen. Tidigare hade grundlagsutskottet i sin praxis ansett att identifieringsuppgifter faller utanför kärnområdet i den grundläggande fri- och rättigheten för sekretess i fråga om konfidentiella meddelanden (se t.ex. GrUU 33/2013 rd, s. 3/I, GrUU 6/2012 rd, s. 3/II, GrUU 29/2008 rd, s. 2/II och GrUU 3/2008 rd, s. 2/I). I praktiken kan dock identifieringsuppgifter som ansluter till elektronisk kommunikation samt möjligheten att sammanställa och kombinera dem likväl vara problematiska med hänsyn till skyddet för privatlivet på så sätt att en kategorisk uppdelning av skyddet i ett kärnområde och ett randområde inte alltid är motiverad, utan man måste på ett allmännare plan fästa vikt också vid hur betydelsefulla begränsningarna är (GrUU 18/2014 rd, s. 6/II).

Allmänna frågor för bedömningen av uppgiftslagring

Behörig myndighet för att förelägga uppgiftslagring

I enlighet med 157 § i kommunikationstjänstlagen utser inrikesministeriet särskilt genom sitt beslut lagringsskyldiga företag. Alternativen för att genomföra lagringen av uppgifter förutsätter enligt EU-domstolens rättspraxis i regel ett myndighetsföreläggande innan lagringen inleds. Ett undantag från detta är allmän och odifferentierad lagring av IP-adresser som tilldelats källan för en IP-

[20] Artikel 1.2 i direktivet, se Europeiska dataskyddsstyrelsens utlåtande 5/2019 om växelverkan mellan direktivet om integritet och elektronisk kommunikation och den allmänna dataskyddsförordningen i synnerhet i fråga om dataskyddsmyndigheternas behörighet, uppgifter och befogenheter.

anslutning samt lagring av uppgifter som gäller identiteten hos dem som använder elektroniska kommunikationsmedel.

Med beaktande av hur stor och mångsidig gruppen av potentiella lagringsskyldiga företag är bör behovet av att utse dem genom ett särskilt beslut granskas också i fråga om de lagringsåtgärder som inte till följd av EU-domstolens rättspraxis eller av något annat skäl är förenade med särskild skyldighet att låta lagringen prövas av myndigheterna.

En preventiv domstolstillsyn skulle förbättra rättssäkerheten både för dem som använder kommunikationstjänster och de företag som svarar för verkställigheten av lagringsföreläggandet. Å andra sidan skulle en utökning av domstolens förhandstillsyn till uppgiftslagringsfasen öka den administrativa bördan och sannolikt belasta domstolarna. Då en behörig myndighet utses för föreläggande bör man alltså sträva efter en balans med avseende på en ändamålsenligt ordnad myndighetsverksamhet och dem som svarar för verkställandet av och som är föremål för lagringsskyldigheten.

Lagringsskyldiga företag

I 157 § i kommunikationstjänstlagen finns inga särskilda krav på vilket företag som kan utses till lagringsskyldigt företag, förutom att det är fråga om ett ”teleföretag”. Definitionen av teleföretag är omfattande och täcker många slags tjänsteleverantörer.

Lösningen i den gällande lagen, enligt vilken lagringsskyldiga företag är teleföretag som särskilt utsetts genom beslut av inrikesministeriet, är motiverad bland annat genom att det i enlighet med 299 § i kommunikationstjänstlagen betalas ersättning av statens medel till teleföretagen för den utrustning och programvara som krävs för skyldigheten att lagra förmedlingsuppgifter. Genom beslutet har man alltså i praktiken begränsat lagringsskyldigheten till vissa aktörer.

I samband med utarbetandet av bedömningspromemorian har de myndigheter som utnyttjar uppgifterna lyft fram behovet att i vidare utsträckning ålägga teleföretag att lagra uppgifter. Den gällande lagstiftningen anger dock inga uttryckliga begränsningar på hurudana företag som kan utses till lagringsskyldiga företag och begränsar sålunda inte nämnvärt gruppen möjliga lagringsskyldiga företag.

För att lagringsskyldigheten ska gälla sådana aktörer om vilka det är nödvändigt att få uppgifter i syfte att uppfylla målen med lagringsskyldigheten, är det även i fortsättningen skäl att avgränsa den grupp av företag som skyldigheten ska gälla. Detta kan också i fortsättningen göras genom beslut av inrikesministeriet eller en annan behörig myndighet.

När ett föreläggande om lagring riktas till ett teleföretag ska det lagringsskyldiga företaget anges i föreläggandet. Sålunda ska det bedömas och avgränsas vilka företag som ska lagra uppgifter senast då föreläggandet ges.

Begränsnings av lagringstiden till vad som är nödvändigt

En åtgärd för uppgiftslagring får enligt domstolen genomföras under en tid som är begränsad till vad som är strängt nödvändigt. Även om lagringstiden har betydelse vid bedömning av kränkningar av de grundläggande fri- och rättigheterna, kan inte ens en kort lagringstid på till

exempel mellan fyra och tio veckor förhindra att lagringen leder till en allvarlig begränsning av de grundläggande fri- och rättigheterna.

På basis av statistiken verkar det som om det är motiverat att anse att en strängt nödvändig lagringstid är åtminstone tre månader. Det framgår tydligt att de flesta begäran om information görs i fråga om uppgifter som är högst tre månader gamla. Antalet begäranden om information minskar i regel ju äldre uppgifter det är fråga om. Lagringstiden har direkt samband med för hur lång tid uppgifter finns tillgängliga och alltså för hur lång tid som myndigheterna retroaktivt har tillgång till uppgifterna. På grund av de långa utredningstiderna för allvarliga brott kan det anses att det behövs en längre lagringstid.

EU-domstolen har inte på motsvarande sätt krävt en begränsning av lagringstiden till vad som är nödvändigt när det gäller att skyndsamt säkra de uppgifter som tjänsteleverantören har, dvs. ett Quick freeze-föreläggande, eller allmän och odifferentierad lagring av uppgifter som gäller användarnas identitet.

Vid bedömningen av proportionaliteten i fråga om lagringsskyldighetens varaktighet kan man också beakta hur länge kommunikationstjänsteleverantörerna lagrar uppgifter för egna ändamål, eftersom uppgifterna under denna tid i vilket fall som helst innehas av tjänsteleverantören och sålunda kan lämnas ut till myndigheterna till exempel med stöd av 4 kap. 3 § i polislagen. Enligt den information som arbetsgruppen fått finns det å andra sidan skillnader mellan företagen i fråga om lagringstiderna, och deras lagenlighet har tills vidare inte bedömts.

Specificering av uppgifter som ska lagras

I 157 § i kommunikationstjänstlagen har de kategorier av uppgifter som ska lagras bestämts tjänstespecifikt. För de myndigheter som utnyttjar uppgifterna är de nuvarande uppgiftskategorierna enligt 157 § i kommunikationstjänstlagen fortfarande nödvändiga. Det enda behov som framförts av myndigheterna under utarbetandet av utredningen när det gäller att granska utvidgningen av de uppgiftskategorier som ska lagras gäller lagring av IP-adressuppgifter och portuppgifter.

Tjänster som omfattas av lagringsskyldigheten är specificerade uppgifter som hänför sig till telefonitjänster eller textmeddelandetjänster i mobilnätet, internettelefonitjänster eller internetaccesstjänster. För att bedöma om uppgifterna är nödvändiga kan indelningen i kategorier av tjänster enligt ändamål behöva uppdateras.

Under den fortsatta beredningen bör man mera detaljerat bedöma behovet att även i fortsättningen på motsvarande sätt som i den gällande lagstiftningen föreskriva om de uppgifter som ska lagras enligt tjänstekategori. Alternativt kunde man i den fortsatta beredningen granska möjligheten att slå fast tjänstekategorierna i fråga om lagringsskyldighet i samband med ett särskilt lagringsföreläggande eller genom reglering på lägre nivå än lag. Genom en sådan lösning kan man göra det möjligt att snabbare reagera på förändrade kommunikationssätt. Detta kan dock inte anses vara den primära lösningen, eftersom det på lagnivå bör föreskrivas tillräckligt noggrant om uppgifter som ska lagras med beaktande av de ovan nämnda begränsningarna.

De lagringsskyldiga företagens organisatoriska och tekniska åtgärder för att skydda uppgifter

I sitt Tele2-avgörande fogade domstolen till de lämpliga tekniska och organisatoriska åtgärderna för att garantera en hög skydds- och säkerhetsnivå skyldigheten att uttryckligen föreskriva om lagring av uppgifter inom unionen och deras radering. I 158 § i kommunikationstjänstlagen föreskrivs det om förutsättningar för kostnadseffektiv lagring av uppgifter som omfattas av lagringsskyldigheten samt om krav för lagringsskyldiga företag att sörja för informationssäkerheten. Åtgärderna ska anpassas till hotets allvarlighet, till kostnaderna för åtgärderna samt till de tekniska möjligheter att avvärja hotet som står till buds.

Enligt en utredning som arbetsgruppen fått finns de lagringsskyldiga företagens databaser i Finland. I lagen om tjänster inom elektronisk kommunikation föreskrivs det emellertid inte uttryckligen om utplåning av uppgifter som lagrats med stöd av 157 §, inte heller ställs där ett uttryckligt krav på att uppgifterna ska lagras inom Europeiska unionens territorium. Villkoret att uppgifterna ska lagras inom unionen innebär ett förtydligande genom vilket man entydigt på lagnivå ska säkerställa att uppgifter som lagras med stöd av lagringsskyldigheten inte lagras i tredjeländer.

Genomförandealternativ för skyldigheten att lagra uppgifter

Upphävande av den nationella lagringsskyldigheten

Direktivet om integritet och elektronisk kommunikation möjliggör att lagringsskyldighet införs, men förpliktar inte till det. En möjlighet att anpassa Finlands lagstiftning till EU-rätten kunde vara att upphäva bestämmelserna om lagringsskyldighet.

Denna lösning förbättrar skyddet för privatlivet och personuppgifter och skyddet för förtroliga meddelanden och eliminerar också ingripandet i teleföretagens egendomsskydd.

Då blir dock utredningen av ett stort antal brott beroende av om ett teleföretag fortfarande har uppgifterna i sin besittning för egna syften. Enligt den utredning som arbetsgruppen fått finns det skillnader i lagringstiderna hos olika operatörer. Dessutom lagras en del uppgifter, såsom IP-adresser eller uppgifter om obesvarade samtal, endast en kort tid. Då är tillgången till uppgifter godtycklig och svår att förutse.

Upphävande av lagringsskyldigheten skulle också vara speciellt med beaktande av att lagringsskyldigheten tidigare har bedömts vara nödvändig. Strävan att bekämpa allvarlig brottslighet är en grund som talar för bestämmelserna om lagringsskyldighet.

Upphävande av lagringsskyldigheten verkar alltså inte vara ett primärt alternativ. Det verkar befogat att också i fortsättningen säkerställa tillgången till förmedlingsuppgifter i enlighet med de villkor som följer av EU-domstolens rättspraxis och den nationella grundlagen.

Risker med att bevara den nuvarande lagringsskyldigheten

EU-domstolen har betonat att nationell lagstiftning som föreskriver om allmän och odifferentierad lagring av trafik- och lokaliseringsuppgifter omfattar nästan hela befolkningens elektroniska

kommunikation utan att det görs någon åtskillnad, begränsningar eller undantag på basis av syftet. Sådana bestämmelser gäller på ett allmänt plan alla som använder elektroniska kommunikationstjänster, även om personerna i fråga inte ens indirekt befinner sig i en situation som kan leda till att ett straffrättsligt förfarande inleds.

Om den nuvarande nationella lagstiftningen förblir oförändrad, finns det risk för att den i den nuvarande formen anses strida mot unionsrätten. Då är det risk för att förmedlingsuppgifter inte kan fås med hjälp av retroaktiv teleövervakning eller att utnyttjande av erhållna uppgifter som bevismaterial systematiskt ifrågasätts tills den nationella lagstiftningen ändras.

Ett alternativ som hellre kunde understödjas är att i föregripande syfte rätta till de oklarheter som upptäckts för att säkerställa att myndigheterna har oavbruten tillgång till förmedlingsuppgifter om elektronisk kommunikation på ett sätt som respekterar de grundläggande fri- och rättigheterna även i framtiden. Den nationella lagstiftningen behöver preciseras för att säkerställa att den överensstämmer med Finlands grundlag och EU-domstolens rättspraxis, är begränsad till vad som är nödvändigt med avseende på integritetsskyddet och samtidigt garanterar myndigheterna berättigad och proportionerlig tillgång till uppgifterna för att säkerställa en effektiv brottsbekämpning och trygga den nationella säkerheten.

Precisering av lagringsskyldigheten i enlighet med riktlinjerna i domstolens rättspraxis

Differentiering av lagringsgrunderna och hierarkin mellan mål av allmänt intresse

EU-domstolen har i sin rättspraxis prövat symmetrin mellan lagringsgrunden och syftet med tillgången till uppgifter. Syftena med mål av allmänt intresse, dvs. bekämpning av brott och tryggande av den allmänna säkerheten och den nationella säkerheten, berättigar delvis olika lagringsåtgärder. Den nationella säkerheten kan anses som det viktigaste målet.

För närvarande har användningsändamålen för uppgifterna inte specificerats i 157 § i kommunikationstjänstlagen eller någon annanstans i lag i förhållande till vissa lagringsgrunder. Den nationella lagstiftningen kan behöva preciseras till denna del. Av bestämmelserna om lagringsskyldighet ska det tydligt framgå vilket mål av allmänt intresse som lagringsskyldigheten grundar sig på.

I bestämmelserna ska en behövlig övergångstid garanteras så att differentieringen av grunderna för lagring kan genomföras automatiskt när uppgifter uppkommer och lagras i syfte att minimera mängden manuellt arbete för de lagringsskyldiga företagen. Enligt de uppgifter som arbetsgruppen fått är det tekniskt möjligt att i samband med lagringen av en uppgift fastställa vissa värden för den, på basis av vilka uppgiften lagras, varvid man i samband med tillgången till uppgiften kan vara säker på att tillgång inte beviljas i fråga om en sådan uppgift vars lagringsgrund inte på det sätt som EU-domstolen förutsätter är symmetrisk med uppgiftens användningsändamål.

En differentiering av lagringsgrunderna leder till att tjänsteleverantörerna i fortsättningen när de besvarar begäran om information bör granska både användningsgrunden och överensstämmelsen med lagringsgrunden.

Föreläggande av lagringsskyldighet för att bekämpa brottslighet och garantera den allmänna säkerheten

Riktad lagring enligt ett geografiskt kriterium

För de myndigheter som behöver uppgifterna är detta alternativ en användningsbar åtgärd eftersom den omfattar föregripande lagring av uppgifter och inte är begränsad till endast en eller till en på förhand identifierad person.

En geografiskt riktad lagringsåtgärd kan genomföras antingen mot bakgrund av statistiska uppgifter (platser där det begås många allvarliga brott) eller på basis av risker som hänför sig till en viss plats (platser som är särskilt utsatta i fråga om allvarliga brott, såsom platser och infrastruktur där ett mycket stort antal personer rör sig regelbundet eller strategiska platser).

Ett geografiskt kriterium som baserar sig på antalet brott kräver tillgång till statistiska uppgifter. Vid bedömningen av brottsmängden kan man beakta till exempel områden som förekommer i teleövervakningsinformation. Också Statistikcentralens eventuella roll bör utredas. Som gränsvärde kan man använda antingen ett fast eller ett relativt gränsvärde. Ett fast gränsvärde innebär att lagringsskyldighet riktas till alla områden där en på förhand angiven förekomst av allvarlig brottslighet uppfylls (Sveriges modell). Detta kan leda till geografisk lagring som omfattar en betydande del av eller till och med hela Finland. Ett relativt gränsvärde innebär däremot att lagringsskyldigheten ska omfatta områden som har högre förekomst av brottslighet än andra områden (Danmarks modell). Då är det alltid en del områden som står utanför lagringsskyldigheten.

Det bör regelbundet utvärderas om kriterierna är aktuella, till exempel med 12 månaders mellanrum, så att man säkerställer att åtgärden är effektiv och begränsad till vad som är nödvändigt.

De lagrade uppgifterna kan också användas för att trygga den nationella säkerheten.

Ur teleföretagens synvinkel är det utmanande att genomföra det här alternativet i praktiken och det skulle krävas ändringar i nuvarande praxis. Detaljerna för ett genomförande kommer ännu att utredas och bedömas vid den fortsatta beredningen.

Riktad lagring på basis av en personkrets

Personbaserad lagring förbättrar skyddet för utomståendes privatliv eftersom målgruppen för åtgärden är noggrant avgränsad. Lagring som riktas personbaserat är i synnerhet förenad med en förhandsdimension.

Att rikta en åtgärd till vissa personer till exempel på grund av tidigare brottslig bakgrund är inte oproblematiskt med tanke på oskuldspresumtionen. Åtgärdens godtagbarhet försvagas också av bedömningen att en krets av personer som bildas på basis av tidigare brottslig bakgrund inte kan anses vara en effektiv åtgärd med tanke på brottsbekämpningen.

Lagringen kan vara tekniskt lätt att genomföra. Meddelande till teleoperatörerna om de personer som åtgärden ska omfatta är dock förenat med betydande dataskyddsrisker och förutsätter en särskilt hög nivå på informationssäkerheten (i praktiken innebär det till exempel att förteckna och till företagen förmedla vilka personer som har samband med hot mot den nationella säkerheten).

I situationer som är förenade med brottsmisstanke kan man utnyttja andra metoder, i synnerhet Quick freeze-föreläggande.

Riktad lagring på basis av andra objektiva och icke-diskriminerande kriterier

EU-domstolen har tillåtit den nationella lagstiftaren att utöver kriterier som hänför sig till personer och geografiska kriterier ställa även andra särskiljande objektiva och icke-diskriminerande kriterier för genomförandet av lagringen, om det genom dem kan säkerställas att den riktade lagringsåtgärdens dimension är begränsad till vad som är strängt nödvändigt. Dessutom ska det alltid finnas ett åtminstone indirekt samband mellan allvarliga brott och de personer om vilka uppgifter lagras.

Som ett sådant kriterium har man identifierat stora massevenemang som kan vara förenade med risk för allvarlig brottslighet. Det verkar dock som om ett lagringsföreläggande som genomförs enligt ett geografiskt kriterium kan användas också i en sådan här situation, varvid det inte behöver föreskrivas om en särskild lagringsgrund.

Quick freeze -föreläggande om lagring

I den nationella lagstiftningen får det föreskrivas om möjligheten att genom ett beslut av en behörig myndighet som kan bli föremål för effektiv domstolskontroll ålägga tillhandahållare av elektroniska kommunikationstjänster att skyndsamt säkra att trafik- och lokaliseringsuppgifter som de innehar lagras för en viss tid.

Det kan vara fråga om en åtgärd som stöder geografisk lagring, till exempel i situationer där brottsligheten minskar inom ett visst område så att den geografiska lagringströskeln inte överskrids. Åtgärden möjliggör att lagringstiden i fråga om uppgifter som lagras på basis av ett geografiskt kriterium i enskilda fall förlängs. Enligt bedömningen kan den inte anses effektiv som enda lagringsåtgärd.

Föreläggandet kan riktas geografiskt eller på någon viss person. Föreläggandet hänför sig till ett brott eller ett hot som utreds, och sålunda är föremålet för åtgärden noggrant avgränsat. I regel är denna åtgärd alltså en mera begränsad åtgärd jämfört med föregripande lagringsåtgärder också när det gäller inskränkning av de grundläggande fri- och rättigheterna.

På nationell nivå finns det redan i tvångsmedelslagen bestämmelser om föreläggande att säkra data, genom vilket den som innehar eller har bestämmanderätten över dessa data åläggs att säkra uppgifterna så att de inte ändras.

Lagring av IP-adresser

Enligt EU-domstolen är generell och odifferentierad lagring av IP-adresser som tilldelats källan för en anslutning möjlig. Detta möjliggör föregripande lagring av uppgifter förutsatt att man strikt följer de villkor som EU-domstolen ställt.

IP-adressen kan i fråga om många nätbrott vara den enda undersökningsmetoden för att identifiera gärningsmannen, vilket stöder en omfattande lagring. IP-adressen är enligt domstolen en mindre känslig uppgift än andra trafikuppgifter, varför en mera omfattande lagring är möjlig. Enligt proportionalitetsprincipen bör detta dock begränsas till syftet att bekämpa allvarliga brott och allvarliga hot mot den allmänna säkerheten.

Denna lagringsåtgärd motsvarar i praktiken nuläget.

Lagring av uppgifter om personers identitet (inkl. registreringsskyldighet för prepaid-abonnemang)

I regel ska tjänsteleverantörerna behandla och lagra dessa uppgifter på basis av kundförhållandet, så uppgifterna finns redan tillgängliga. Utgångspunkten är att det inte är fråga om allvarlig kränkning av de grundläggande fri- och rättigheterna. Lagringsskyldigheten kan alltså allmänt tillåtas på grund av målet att bekämpa brott och hot mot den allmänna säkerheten och den är sålunda inte begränsad till endast allvarliga brott eller hot.

Lagringsskyldigheten kan följa direkt av lagen utan något separat föreläggande, men då ska behovet att föreskriva närmare om de lagringsskyldiga företagen granskas. Alternativt kan gruppen av lagringsskyldiga företag begränsas genom ett föreläggande på motsvarande sätt som för närvarande.

Antalet prepaid-abonnemang har varit sjunkande och deras antal i Finland är lågt jämfört med den internationella nivån.

En fördel med prepaid-abonnemang har ansetts vara att de är administrativt enkla. Registreringsskyldigheten kan i synnerhet försvåra möjligheterna för eller beredskapen hos personer som tillfälligt vistas i landet att skaffa telefonabonnemang. För dem som säljer prepaid-abonnemang, såsom olika slags kiosker, uppkommer nya slags skyldigheter i fråga om behandling av uppgifter.

Åtgärden försvårar möjligheten för olika personer (till exempel oliktänkare och förföljda personer) att kommunicera anonymt.

För närvarande finns det inte några elektroniska lösningar för att säkerställa identiteten hos dem som mest använder oregistrerade abonnemang. Detta borde dock bedömas som ett alternativ till fysiska identitetsbevis för identifiering av personer.

En risk med registreringsskyldigheten är att ägaren och innehavaren av ett abonnemang är olika personer (användning av bulvaner).

Tills vidare finns det få uppgifter om nyttan med registreringsskyldigheten ur myndigheternas synvinkel, inklusive möjligheterna att kringgå skyldigheterna vid allvarlig brottslighet.

Införande av lagringsskyldighet för att garantera den nationella säkerheten

Åtgärder som motsvarar de lagringsskyldigheter som ålagts i syfte att bekämpa brottslighet

Alla eventuella lagringsåtgärder som EU-domstolen behandlat är möjliga för att garantera den nationella säkerheten. Sålunda är de åtgärder som presenteras ovan i avsnitt 6.3.3 möjliga också i syfte att garantera den nationella säkerheten.

Enligt domstolen kan uppgifter som lagras på grundval av ett mål av allmänt intresse på lägre nivå användas för att skydda ett viktigare mål. Sålunda kan användning av uppgifter som lagrats i syfte att bekämpa brottslighet tillåtas också för att skydda den nationella säkerheten.

För en tydlig reglering och för att minimera den administrativa börda regleringen medför är det skäl att säkerställa att samma uppgifter inte lagras flera gånger.

Generell och odifferentierad lagring för att garantera den nationella säkerheten

Sådan lagring förutsätter begränsningar och strikta garantier genom vilka man effektivt kan skydda de behöriga personernas personuppgifter mot riskerna för missbruk. Som behövliga skyddsmetoder kan man anse domstolens tillsyn eller annan oberoende tillsyn, tillgodoseende av rättsskyddet vid domstol samt iakttagande av grunderna för dataskyddet.

För att föreläggandet i enlighet med EU-domstolens villkor ska basera sig på tillräckligt konkreta omständigheter utifrån vilka det kan anses att medlemsstatens nationella säkerhet är utsatt för ett allvarligt hot som visar sig vara verkligt och befintligt eller förutsebart, måste föreläggandet basera sig på Skyddspolisens eller Försvarsmaktens förslag och riskbedömning. EU-domstolen har förutsatt att denna lagringsgrund får komma i fråga endast vid verkliga och befintliga/förutsebara hot, vilket innebär att inte heller detta möjliggör ett lagringsföreläggande utan tidsbegränsning. Dessutom får det föreskrivas om skyldighet att höra underrättelsetillsynsombudsmannen.

I EU-domstolens rättspraxis har det inte krävt att domstolen utfört förhandskontroll. Sålunda kan det nationellt föreskrivas för inrikesministeriet om ett sådant föreläggande, såsom det föreskrivs i den gällande lagen (157 § i kommunikationstjänstlagen). Nationellt bör det ännu bedömas närmare om det finns behov att föreläggandet omfattas av domstolens förhandskontroll, med beaktande av också 80 § i grundlagen.

Särskilda frågor som gäller skyldigheten att lagra uppgifter

Utvidgning av lagringsskyldigheten till OTT-kommunikationstjänster

Kommunikationen har i allt högre grad överförts till webben, och i synnerhet användningen och betydelsen av så kallade over-the-top-kommunikationstjänster (OTT) som bygger på internet har ökat. Dessa uppgifter har också fått större betydelse för behoven inom brottsbekämpningen. Med beaktande av riksdagens ställningstaganden kan det vid beredningen vara skäl att utöver nödvändigheten av de nuvarande tjänstekategorierna också granska eventuella nya tjänstekategorier.

OTT-kommunikationstjänsterna verkar i huvudsak falla utanför tjänstekategorierna enligt 157 § i kommunikationstjänstlagen, eftersom så kallade snabbmeddelandetjänster inte hör till de tjänstekategorier som det föreskrivs om.

Under den fortsatta beredningen bör man mer detaljerat bedöma behovet att också i fortsättningen på motsvarande sätt som i den gällande lagstiftningen föreskriva enligt tjänstekategori om de uppgifter som ska lagras samt uppdatera dessa tjänstekategorier så att de motsvarar uppgifter som är nödvändiga med tanke på grunderna för uppgiftslagringen.

En separat fråga är dock att de viktigaste OTT-kommunikationstjänsterna för närvarande är etablerade utanför Finland. Myndigheternas tillgång till uppgifter som innehas av tjänsteleverantörer som är etablerade i en annan EU-medlemsstat eller utanför EU har konstaterats vara en allmän utmaning i hela unionen. Sålunda är det möjligt att problemet inte kan

lösas på ett tillfredsställande sätt genom lösningar enligt Finlands nationella lagstiftning. Däremot kunde det vara fördelaktigt att sträva efter en lösning på detta på EU-nivå.

Utvidgning av skyldigheten att lagra IP-adresser

Myndigheterna har lyft fram behovet att utvidga lagringsskyldigheten till att gälla också mottagarnas IP-adresser och uppgifter om mottagarporten. Om dessa tas med i de uppgifter som ska lagras begränsar det avsevärt antalet uppgifter och kunder som ska uppges för polisen i svar på begäran om information.

En sådan lagring av uppgifter skulle leda till en betydande datamassa, när det i loggen lagras bland annat uppgifter om i vilka alla källor det sökts innehåll som hör till sidan eller gjorts andra webbanrop. Med hjälp av datamassan kan man dra mycket långtgående slutsatser om användarens privatliv.

En mer omfattande lagring av uppgifter skulle vara en betydande förändring jämfört med nuläget. Sådan lagring är inte heller en sådan lagringsåtgärd som behandlas ovan (*lagring av IP-adresser som tilldelats källan*), så en allmän och odifferentierad lagring av dessa uppgifter verkar inte vara förenlig med unionsrätten.

Det förefaller ändamålsenligt att fortsätta bedömningen av skyldigheten att lagra IP-adresser och användningen av dem i EU-domstolen efter att avgörandet av begäran om förhandsavgörande C-470/21 om lagring och myndighetsanvändning av IP-adresser offentliggjorts.

Specificering av begäran om tillgång

EU-domstolen har förutsatt att de behöriga nationella myndigheterna i varje enskilt fall ska säkerställa att både den eller de kategorier av uppgifter som avses och den tidsperiod som ansökan avser, med beaktande av omständigheterna i det enskilda fallet, begränsas till vad som är strängt nödvändigt för den aktuella utredningen. (Prokuratuur punkt 38)

Den nationella lagstiftningen innehåller ingen uttrycklig skyldighet att specificera de kategorier av uppgifter som omfattas av begäran om information eller tidsperioden för dem. Tillstånd söks och ges personbaserat, utom i situationer där den misstänkte inte är känd. (10 kap. 9 § i tvångsmedelslagen)

I lagstiftningen finns det dock ett allmänt krav på nödvändighet som kan anses förutsätta att myndigheten säkerställer att begäran om information begränsas till det nödvändiga också utan ett uttryckligt villkor om att dessa omständigheter ska specificeras.

Den nationella lagstiftningen kan alltså i princip bedömas vara förenlig med unionsrätten.

Myndigheter som får uppgifter och användning av uppgifterna för att förebygga brott

Enligt 322 § i kommunikationstjänstlagen kan endast de myndigheter som enligt lag har rätt att få uppgifter som ska lagras enligt 157 § få sådana uppgifter från de lagringsskyldiga företagen. Bestämmelsen i fråga visar den centrala principen i lagen, enligt vilken det genom den föreslagna

lagen endast föreskrivs om lagring av uppgifter. Myndigheternas rätt att få uppgifter bestäms i enlighet med andra lagar.

I tolkningen av det inbördes förhållandet mellan 157 § och 322 § i kommunikationstjänstlagen har det funnits meningsskiljaktigheter som i synnerhet föranleds av begränsningen av användningen enligt 157 § 1 mom. Uppgifter har dock med stöd av annan lagstiftning, såsom polislagen, använts också får att förebygga brott.

Det verkar skäl att precisera lagstiftningen till denna del. Det kan behövas precisera 157 § i kommunikationstjänstlagen så att lagringsgrunden uttryckligen framgår av den reglering som skapar lagringsskyldigheten. Samtidigt bör man granska det uttryckliga tillåtandet av användning av uppgifter på motsvarande sätt som för närvarande i syfte att förebygga och avslöja brott för att avhjälpa den nuvarande oklarheten i tolkningen.

Det är också skäl att granska myndighetsförteckningen i 322 § i kommunikationstjänstlagen.

Lagring av och tillgång till uppgifter i vissa polisundersökningar

Utöver bestämmelserna om teleövervakning enligt polislagen har polisen rätt att få förmedlingsuppgifter om kommunikation i vissa polisundersökningar, såsom utredning av dödsorsak och vissa slag av brådskande spårning enligt 5 kap. 8 § 3 mom. i polislagen. I 157 § i kommunikationstjänstlagen föreskrivs inte särskilt om lagringsskyldighet i fråga om dessa arbetsuppgifter. Användningen av teleövervakningsuppgifter för att utesluta eller avslöja brott mot liv kan i fråga om allvarlighetsgraden anses vara jämförbar med bekämpning av allvarlig brottslighet.

I fråga om brådskande situationer gäller åtgärden uppgifter som ett teleföretag vanligen ännu lagrar för sina egna behov. Det finns alltså inte nödvändigtvis behov av en separat lagringsskyldighet, men detta kan leda till en situation där uppgifterna inte är tillgängliga om teleföretagens egna lagringsbehov förändras.

Vid den fortsatta beredningen ska behovet att föreskriva om en särskild lagringsgrund eller annan grund för att tillåta användning av lagrade uppgifter för dessa ändamål bedömas med iakttagande av domstolens lära om hierarki mellan mål av allmänt intresse.

Behov av särskilda skyddsmetoder i anslutning till behandling och automatiserad behandling av känsliga uppgifter

I den nationella lagstiftningen föreskrivs det för närvarande inte uttryckligen om automatiserad behandling eller analys av uppgifter. Sådan behandling har inte heller uteslutits särskilt.

Personuppgifter som rör fällande domar i brottmål och brott kan också anses känsliga i konstitutionellt hänseende.

I den gällande lagstiftningen kan det inte anses finnas skrivningar som kräver en noggrannare bedömning av behandlingen av känsliga uppgifter.

Ersättning av kostnader som föranleds av biträdande av myndigheter

Kommunikationsutskottet har i samband med att bestämmelserna om civil underrättelseinhämtning utfärdades förutsatt att nivån på de kostnader som föranleds av biträdande av myndigheter noggrant bevakas och det utan dröjsmål vidtas åtgärder för att ändra ersättningsbestämmelserna i det fall att kostnaderna stiger avsevärt jämfört med nuläget. (KoUU 26/2018 rd)

Bestämmelser om ersättning för kostnader finns i 299 § i kommunikationstjänstlagen. Enligt den paragrafen ersätts också andra kostnader för biträdande av myndigheter än de som föranleds av DR-skyldigheten.

I samband med utarbetandet av utredningen har lagringsskyldiga företag lyft fram att den arbetsinsats som föranletts av myndighetsförfrågningar har ökat betydligt hos operatörerna under de senaste åren.

Enligt teleföretagens bedömningar kommer alla de tekniska ändringar som lagstiftningen förutsätter att kräva manuellt arbete för att säkerställa riktigheten i fråga om svaren på begäran om uppgifter samt processens funktion. I synnerhet i fråga om lagringsskyldighet som baserar sig på ett regionalt kriterium borde man kräva att det satsas på systemutveckling och på hur uppgifter samkörs och raderas. Detta ökar också det manuella arbetet.

Vid bedömning av ersättandet av kostnader är det också skäl att fästa uppmärksamhet vid konsekvenserna av 299 § i kommunikationstjänstlagen i förhållande till annan lagstiftning. Också till exempel en ersättningsmodell enligt regleringen om e-bevisning (e-evidence) iakttar den nationella lagstiftningen.