Sisäministeriö Perusmuistio EU/199/2024-SM-2

Simonen Katariina 23.4.2024

Oikeus- ja lainvalvontaviranomaisten lainmukainen tietoon pääsy digitaalisessa ympäristössä eli ns. Going Dark –aloite

Käsittelyvaihe ja jatkokäsittelyn aikataulu

Tammikuussa 2023 epävirallinen oikeus- ja sisäministerikokous antoi tukensa tuolloisen puheenjohtajamaa Ruotsin esitykselle perustaa uusi foorumi, jossa jäsenvaltiot yhdessä eri intressitahojen kanssa selvittävät keinoja taata oikeus- ja lainvalvontaviranomaisten tietoon pääsy digitaalisessa ympäristössä olevaan tietoon (Going Dark –aloite). Taustalla on rikollisuuden siirtyminen yhä enemmän tietoverkkojen ja tietojärjestelmien avulla tehtäväksi, minkä vuoksi myös rikosten torjuminen ja selvittäminen vaativat mahdollisuutta seurata digitaalisia rikosjälkiä. Aloitetta eteenpäin viemään perustettiin keväällä 2023 korkean tason asiantuntijaryhmä (High-Level Group, jäljempänä HLG).

HLG on komission ja puheenjohtajavaltion yhdessä vetämä työryhmä, jossa edustettuina ovat jäsenvaltiot sekä useita EU:n virastoja: EU:n lainvalvontayhteistyövirasto (Europol), EU:n rikosoikeudellisen yhteistyön virasto (Eurojust), EU:n lainvalvontakoulutusvirasto (CEPOL), EU:n kyberturvallisuusvirasto (ENISA), Euroopan unionin perusoikeusvirasto (FRA), EU:n terrorismintorjunnan koordinaattori ja neuvoston sihteeristö. Euroopan tietosuojavaltuutettu (EDPS) sekä Euroopan tietosuojaneuvosto (EDPB) osallistuvat työhön tarkkailijoina ja asiantuntijoina. HLG:n alle on perustettu kolme teknisen tason asiantuntijatyöryhmää. Suomi osallistuu HLG:n ja sen alaisten asiantuntijatyöryhmien työhön. Työhön osallistutaan sisäministeriön johdolla, ja mukana ovat myös oikeusministeriö ja liikenne- ja viestintäministeriö.

HLG:n tavoitteena on valmistella asiakirja, jossa esitetään mahdolliset ratkaisuehdotukset oikeus- ja lainvalvontaviranomaisten tietoon pääsyn turvaamiseksi, ja pyrkiä vaikuttamaan tulevan komission työohjelmaan. HLG:n on määrä saada työnsä valmiiksi kesällä 2024.

Tämän E-kirjeen tarkoituksena on linjata Suomen kantoja oikeus- ja lainvalvontaviranomaisten tietoon pääsyyn digitaalisessa maailmassa sekä HLG:ssä ja sen alaisissa työryhmissä tehtävä työ huomioiden. Lisäksi E-kirjeen tavoitteena on muodostaa aihepiiristä alustavia kantoja tulevan komission työohjelmaan vaikuttamiseksi.

Suomen kanta

Pääministeri Petteri Orpon hallitusohjelman mukaisesti hallitus on sitoutunut vahvistamaan digitalisaatiota sekä rikostutkinnassa että –torjunnassa. Suomi katsoo, että yhä vahvemmin kansainvälistyvän ja tietoverkoissa tapahtuvan tai sähköisiä palveluja hyväksi käyttävän rikollisuuden tutkimiseksi ja torjumiseksi on tarpeen hakea myös kattavia EU-tason ratkaisuja.

Suomi tukee HLG:n työtä ja työn lähtökohtia. Suomi katsoo, että oikeus- ja lainvalvontaviranomaisten lainmukaista tietoon pääsyä digitaalisessa ympäristössä on tarpeellista selvittää EU-tasolla laajassa ja avoimessa yhteistyössä, läpinäkyvästi ja eri näkökulmia käsitellen.

Suomi pitää tärkeänä, että EU-tasolla selvitetään, mitä konkreettisia käytännön haasteita ja teknisiä haasteita oikeus- ja lainvalvontaviranomaiset kohtaavat pääsyssä digitaalisessa ympäristössä olevaan tietoon, ja liittyykö tietoon pääsyyn EU-lainsäädännöstä johtuvia teknisiä tai muita esteitä tai rajoituksia. Suomi pitää tärkeänä, että tunnistettaviin ongelmiin on tärkeä etsiä EU-tason ratkaisuja sen tietoon pääsemiseksi tarkkaan rajatuissa tapauksissa. Ratkaisujen tavoitteena tulisi olla rikosten ennalta estäminen, paljastaminen ja selvittäminen sekä syyteharkintaan saattaminen ja yleisen turvallisuuden vahvistaminen, ja niissä on huomioitava täysimääräisesti EU:n perusoikeuskirjasta, tietosuojalainsäädännöstä ja EU:n tuomioistuimen oikeuskäytännöstä johtuvat velvoitteet. Keskeistä on se, että ratkaisuilla varmistetaan oikeasuhtaisesti kaikkien perusoikeuksien toteutuminen. Suomi pitää myös tärkeänä, että tarkoituksenmukaisuuden tarkastelua täydennetään asianmukaisilla oikeudellisilla ja muilla vaikutusarvioilla, mukaan lukien perusoikeusvaikutusten arviointi, jotta toimien tehokkuutta, oikeasuhteisuutta ja välttämättömyyttä pystytään arvioimaan.

Suomi pitää tärkeänä, että EU-tasolla kehitetään sellainen tasapainoinen, teknologianeutraali ja oikeasuhtainen lähestymistapa tietoon pääsyyn parantamiseksi, joka samanaikaisesti huomioi tarpeen turvata vahva salaus sekä viranomaisten laissa tarkkarajaisesti määritelty mahdollisuus yksittäistapauksissa päästä salattuihin tietoihin ja sähköiseen aineistoon.

Mahdollisten ratkaisuehdotusten ei tulisi sisältää toimenpiteitä, jotka vaarantaisivat kyberturvallisuutta heikentämällä viestintä- ja tietojärjestelmien turvallisuutta. Suomi pitää tärkeänä, ettei esitetä toimenpiteitä, joilla palveluntarjoajia edellytetään heikentämään päästä päähän salausta tai luopumaan sen käytöstä. Heikentämisellä ei kuitenkaan tarkoiteta tek-

nologisen kehityksen tai muiden järjestelyjen mahdollistamaa tuomioistuimen luvalla yksittäistapauksissa tapahtuvaa lainvalvontaviranomaisten pääsyä salattuun tietoon. Suomi kiinnittää huomiota siihen, että yleisellä velvoitteella purkaa viestinnän salausta olisi laajakantoisia ja periaatteellisia vaikutuksia luottamuksellisen viestin salaisuuden suojaan sekä muiden perusoikeuksien toteutumiseen verkossa. Suomi pitää tärkeänä selvittää, mitä mahdollisuuksia edellä mainitut reunaehdot antavat viranomaisen pääsylle reaaliaikaiseen tietoon. Selvityksessä on tarpeellista käsitellä niin viranomaisten omien kyvykkyyksien kehittämistä kuin palveluntarjoajille asetettavia velvoitteita.

Suunniteltavilla toimenpiteillä ei tulisi heikentää tai kohtuuttomasti vaikeuttaa digitaalisen liiketoiminnan edellytyksiä vaan vahvistaa sisämarkkinoiden yhtenäisyyttä. Kaikille toimijoille taatut samat oikeudet ja asetetut velvoitteet takaavat tasapuolisen kilpailun edellytykset. Lisäksi työssä tulisi varmistaa riittävä tulevaisuuskestävyys ja pyrkiä tunnistamaan uusien teknologioiden tuomat lisätarpeet viranomaisille. Toimenpiteiden tulisi olla kustannustehokkaita, erityisesti ottaen huomioon viestintä- ja tietojärjestelmien kehittämiseen ja uudelleen suunnitteluun liittyvät kustannukset.

Suomi pitää tärkeänä lainvalvontaviranomaisten osallistumista standardointikomiteoiden ja työryhmien työhön, jotta lainvalvontaviranomaisten tarpeet tulevat huomioitua tuotekehittelyssä ja suunnittelussa etukäteisesti. Tässä yhteydessä Suomi pitää tärkeänä selvittää mahdollisia teknisiä ratkaisuja ja juridisia velvoitteita palvelujen kehittämiseksi siten, että ne mahdollistavat viranomaisen reaaliaikaiseen tietoon pääsyä.

Suomi katsoo, että oikeus- ja lainvalvontaviranomaisten tietoon pääsy tulee turvata sekä EU-alueelle sijoittautuneiden yritysten, että EU-alueella palveluita tarjoavien, mutta EU:n ulkopuolelle sijoittautuneiden yritysten hallussa olevan tiedon osalta.

Pääasiallinen sisältö

Going Dark – aloite ja sen tausta

Ruotsin puheenjohtajuuskaudella keväällä 2023 käynnistetyn Going Dark -aloitteen taustalla vaikuttavat oikeus- ja lainvalvontaviranomaisten entistä suuremmat vaikeudet saada digitaalisessa ympäristössä tehokkaasti tietoa rikollisuuden torjumiseksi. Komission mukaan rikolliset ja terroristit käyttävät verkkomaailman mahdollisuuksia tehokkaasti hyödykseen. Myös perinteisten rikosten (kuten huumausaine- ja petosrikollisuus) tekeminen on viimeisen vuoksikymmenen aikana siirtynyt enenevässä määrin ainakin osittain tietoverkkojen ja tietojärjestelmien avulla tehtäväksi, minkä seurauksena rikoksista jää aikaisempaa enemmän digitaalisia tietoja ja sen vuoksi myös rikosten torjuminen ja selvittäminen vaativat mahdollisuutta seurata digitaalisia rikosjälkiä.

Sisäisen turvallisuuden pysyvä komitea (COSI) on edistänyt Ruotsin puheenjohtajuuskauden aloitetta. Komitean mukaan oikeus- ja lainvalvontaviranomaisten on entistä vaikeampi pysyä digitaalisen kehityksen mukana ja toteuttaa tehokkaita lainvalvontatoimia EU:ssa. Haasteet vaikuttavat yleisen järjestyksen turvaamiseen, rikosten ennaltaehkäisemiseen, havaitsemiseen, selvittämiseen ja tuomioistuimeen saattamiseen sekä uhrien legitiimien oikeusturva- ja korvausvaateisiin vastaamiseen. COSI arvioi, että mikäli oikeus- ja lainvalvontaviranomaisten kokemia ongelmia ei ratkaista asianmukaisesti, on olemassa merkittävä riski siitä, että digitaalisessa maailmassa tapahtuvat kehityskulut mahdollistavat rikollisuuden jäämisen lainvalvontaviranomaisten ulottumattomiin tietoverkossa syntyvien,

anonymiteetin takaamien turvasatamien myötä. COSI:n näkemyksen mukaan tämä muodostaa merkittävän riskin yksilön ja yhteiskunnan turvallisuuden kannalta ja voi myös estää valtion kyvyn turvata oikeusvaltio ja demokraattinen yhteiskunta.

Korkean tason asiantuntijaryhmän HLG:n työn tarkoituksena on kannustaa keskeisiä intressitahoja etsimään yhdessä EU-tason kattavia ratkaisuja niistä edellytyksistä ja keinoista, joilla digitaalisessa ajassa voidaan taata usea intressi: sisäinen turvallisuus, kyberturvallisuus, viestintäpalveluiden ja –järjestelmien turvallisuus ja perusoikeuksien, kuten palveluita käyttävien yksityisyyden suojan toteutuminen verkossa. HLG perehtyy oikeus- ja lainvalvontaviranomaisten rikokseen liittyvään tietoon pääsyn turvaamiseen kolmessa eri tilanteessa: tiedon ollessa käyttäjän laitteella, tiedon ollessa palveluntarjoajan laitteella tai tiedon ollessa välitettävänä.

Työssä tunnistetut tietoon pääsyn suurimmat ongelmat liittyvät viranomaisten puutteellisiin mahdollisuuksiin toimia teknologian kehityksen johdosta, anonyymeihin viestintäpalveluihin, ml. VPN ja verkon pimeät kauppapaikat, tiedon säilyttämistä koskeviin edellytyksiin, OTT (over-the-top) –toimijoilla olevaan dataan sekä tietojen salaukseen.

HLG:n työssä on keskeistä se, että digitaalisessa maailmassa viestinnän salaus on keskeistä, sillä se turvaa toisaalta digitaalisia järjestelmiä ja toisaalta yksityisyyden suojaa ja henkilökohtaisia tietoja. Vahva salaus on merkityksellinen perusoikeuksien, kuten sananvapauden, yksityisyyden suojan ja tietosuojan, suojaamisessa. Digitaalisella aikakaudella tekniset ratkaisut sähköisen viestinnän yksityisyyden turvaamiseksi ja suojaamiseksi, mukaan lukien salaustoimenpiteet, osaltaan varmistavat muiden perusoikeuksien, kuten sananvapauden, toteutumisen. Salaus lisäksi auttaa kansalaisia ja yrityksiä puolustautumaan tietotekniikan väärinkäytöksiä, kuten hakkerointia, identiteetti- ja henkilötietojen varkauksia, petoksia ja luottamuksellisten tietojen epäasianmukaista paljastamista vastaan. Tämä on otettava asianmukaisesti huomioon arvioitaessa toimenpiteitä, jotka voivat heikentää salausta. (Podchasov v. Venäjä, 2024, §§ 76) Salauksen heikentäminen heikentää aina palvelun tietoturvaa. Digitaalista teknologiaa ja välineitä, ml. ne, joilla turvataan yhteiskunnan kyberturvallisuus, tietosuoja, yksityisyyden suoja ja muut perusoikeudet, voidaan myös käyttää rikollisiin tarkoituksiin. Eräs viranomaisten kohtaama haaste on, että rikolliset käyttävät salaustekniikkaa ja peittävät siten tehokkaasti jälkensä.

Tietoon pääsy tarkoittaa sitä, että data on oikeus- ja lainvalvontaviranomaisten käytettävissä tietyin erikseen määritellyin edellytyksin hankittavissa, luettavassa muodossa ja reaaliaikaisesti, jotta rikosten selvittäminen, ennalta estäminen ja paljastaminen olisi mahdollista. Lainvalvontaviranomaisten kokemat tietoon pääsyn haasteet liittyvät erityisesti päästä- päähän salatun viestinnän telekuunteluun eli välitettävänä olevaan viestintään, joka ei ole saatavissa palvelun tarjoajan tai käyttäjän laitteilta. Kun kansallisesti tällä hetkellä tuomioistuimen myöntämällä telepakkokeinoluvalla kohdistetaan telekuuntelua tällaiseen salattuun viestintään, telekuuntelua suorittavalle viranomaiselle palautuu selkokielistä viestintää lähinnä teleyrityksen itse tarjoaman tai palveluun yhdistämänsä palvelun osalta. Viranomaisen telekuuntelulla hankkimassa materiaalissa muiden toimijoiden salattu liikenne, mukaan lukien päästä päähän salattujen viestintäohjelmistojen liikenne, ei ole selkokielistä. Mikäli operaattori yhdistää esim. Googlen RCS-ominaisuuden (Rich Communication Services, moderni viestintästandardi) televerkkoonsa, syntyy siitä operaattorin itse tarjoama palvelu, jonka osalta operaattorilla on velvollisuus huolehtia tämän kautta kulkevan viestinnän toimittamisesta viranomaiselle selkokielisenä, sopimalla siitä ominaisuuden toimittajan kanssa, tässä tapauksessa Googlen. Pikaviestinohjelmiston liikenne,

kuten esimerkiksi Signalin, ei ole operaattorin hallinnassa oleva palvelu ja sen toimittamiseen ei operaattorilla ole velvollisuuksia eikä mahdollisuuksia.

Poliisin mukaan selkokieliseen viestintään liittyvät haasteet voivat merkittävällä tavalla haitata, hidastaa ja pahimmassa tapauksessa jopa estää poliisia tutkimasta käsillä olevaa vakavaa rikosta. Tiedon toimittaminen selkokielisessä muodossa on yksi erittäin keskeinen elementti poliisin viestinnälle asettamissa laatuvaatimuksissa. Ratkaisujen löytäminen tähän viestintään pääsyyn selkokielisessä muodossa yksittäistapauksissa ja tuomioistuimen luvalla ei kuitenkaan tarkoita salauksen eikä tietoturvan heikentämistä yleisesti. Tarkoituksenmukaisten ja oikeasuhtaisten ratkaisujen kehittäminen on keskeistä.

Päästä päähän –salausta koskevien laatuvaatimusten osalta on arvioitu, ettei tällä hetkellä ole tiedossa teknistä ratkaisua, jolla laatuvaatimuksia koskevat pyynnöt voitaisiin toteuttaa siten, että niiden voisi katsoa olevan rinnastettavissa perinteisten viestimien televalvontaan ja -kuunteluun tekniseltä ja oikeudelliselta kannalta. Päästä päähän -salaus turvaa tehokkaasti viestinnän luottamuksellisuutta, ja viestinnän salauksella suojataan niin yksityishenkilöiden, yritysten kuin valtioidenkin etuja, koska sillä estetään viestinnän sisällön oikeudetonta muokkausta ja sen päätymistä vääriin käsiin. Salauksen heikentäminen huonontaa palvelujen turvallisuutta yleisesti ja mahdollistaa siten myös pahantahtoisille toimijoille aiempaa helpommin erilaiset väärinkäytökset. Esimerkiksi mahdolliset takaportit voisivat olla myös ulkopuolisten valtiollisten toimijoiden ja rikollisten tahojen hyödynnettävissä. Turvallisia päästä päähän -salaustekniikoita ei voida muuttaa suunnittelematta palveluita täysin uudelleen. Toisaalta palveluiden uutta suunnittelua ja sopimista ovat aikanaan edellyttäneet myös perinteisillä teleoperaattoreilla nykyisin käytössään olevat, muutaman valmistajan toteuttamat yhteisiin teknisiin määrityksiin perustuvat ratkaisut. Kuitenkaan nykyisin käytössä olevia ratkaisuja ei voida siirtää OTT-viestintäpalveluissa sovellettavaksi. Ratkaisuja, joilla salattu viestintä voitaisiin yksittäistapauksessa ja tuomioistuimen luvalla luovuttaa selkokielisessä muodossa ja joka ei johda yleiseen salauksen tai tietoturvan heikentämiseen, selvitetään.

Erityisen tapauksen muodostavat OTT-toimijat. OTT-toimijat ovat teleyrityksistä riippumattomia toimijoita internetissä, kuten WhatsApp ja Skype. Nämä uuden ajan teleyritykset toimivat samalla toimialueella kuin perinteiset teleyrityksetkin, mutta ne eivät omista verkkoon pääsyn mahdollistavaa infrastruktuuria vaan ne hyödyntävät muiden järjestämää pääsyä hyväkseen tarjotakseen samoja palveluita, ilman perinteiselle teleyritykselle asetettuja velvollisuuksia telekuuntelun ja valvonnan toteuttamisesta. Viestinnälle asetettavat laatuvaatimukset ja muut velvoitteet eivät kohdistu tällä hetkellä OTT-palveluihin, minkä vuoksi päästä-päähän salaus luo haasteen rikostorjunnalle. OTT-viestintäpalvelujen tarjoajilla on käytössään keskenään hyvin erilaisia teknisiä ratkaisuja ja yhteisiä standardeja on vähän. HLG:n työssä tarkastellaan mm. ratkaisuja OTT-toimijoiden hallussa olevaan tietoon pääsemiseksi. Tässä tarkastelussa on kyse esimerkiksi siitä, voitaisiinko OTT-toimijoiden kanssa toimia samalla tavalla kuin perinteisten teleoperaattoreiden kanssa telekuuntelua käytettäessä. Tämä tarkoittaisi sopimista televalvonnan ja –kuuntelun käytännöistä ja niiden toteuttamisesta. Tässä yhteydessä arvioidaan myös tarvetta EU-tason lainsäädännölle.

Toinen HLG:n työssä laajalti tunnistettu oikeus- ja lainvalvontaviranomaisten kohtaama haaste tietoon pääsyssä liittyy fragmentoituneeseen viestinnän välitystietojen säilytysvelvollisuuden sääntelyyn. Viranomaiset ovat tuoneet esiin haasteen, joka johtuu siitä, että kansalliset käytännöt tietojen säilytysvelvollisuuden ja erityisesti säilytysaikojen suhteen

eroavat merkittävästi eri jäsenvaltioissa. Toisiin jäsenmaihin tai EU:n ulkopuolelle sijoittuneille yrityksille osoitetut tietopyynnöt eivät välttämättä tuota haluttua lopputulosta. Myös teleyritysten näkökulmasta fragmentoitunut sääntely on haaste. EU-tason lainsäädäntö datan säilytysaikojen harmonisoimiseksi on saanut kannatusta HLG:ssä.

Mahdollisen yhtenäisen datan säilytysaikoja koskevan lainsäädäntökehikon lisäksi ennakollinen vaikuttaminen, ns. lawful access by design, on nostettu HLG:n työssä esille keinona edistää lainvalvontaviranomaisten pääsyä dataan. Kysymyksessä on lainvalvontaviranomaisten osallistuminen standardointikomiteoiden ja työryhmien työhön, jotta lainvalvontaviranomaisten tarpeet tulisivat huomioitua etukäteisesti tuotekehittelyssä ja suunnittelussa. Tällaisia toimijoita ovat ETSI:n (European Telecommunications Standards Institute) alainen TC LI –alakomitea (Technical Committee Lawful Interception) sekä 3GPP –ryhmät (3rd Generation Partnership Project). Yhtiöt ovat myös edustettuina tässä työssä. HLG:ssä tehdyn arvioinnin mukaan EU-tasolla lainvalvontaviranomaisten osallistumismahdollisuutta ei ole maksimaalisesti hyödynnetty tähän mennessä.

Aloitteeseen liittyvät Suomen lainsäädännön asettamat edellytykset

Perustuslain 10 §

Perustuslain 10 § säädetään yksityiselämän suojasta, joka sisältää kirjeen puhelun tai muun luottamuksellisen viestin salaisuuden loukkaamattomuuden. Lailla voidaan säätää välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa.

Poliisioikeudelliset periaatteet

Kaikkea poliisivaltuuksien käyttöä ja poliisitehtävien hoitoa ohjaavat niin sanotut poliisioikeudelliset periaatteet.

Poliisilain (872/2011) 1 luvussa säädetään kyseessä olevista poliisioikeudellisista periaatteista, perusoikeuksien ja ihmisoikeuksien kunnioittamisesta (2 §), suhteellisuusperiaatteesta (3 §), vähimmän haitan periaatteesta (4 §) ja tarkoitussidonnaisuusperiaatteesta (5 §) sekä mahdollisuudesta luopua tehtävästä tai siirtää sitä (9 §). Nämä periaatteet ovat yleisesti sovellettavia, ja seuraavat monelta osin myös perustuslain perusoikeussäännöksistä ja kansainvälisistä perus- ja ihmisoikeusvelvoitteista, ja ne ilmenevät välillisesti uudelleen myös useiden muiden poliisilakiin sisältyvien yksittäisten säännösten sanamuodosta. Korostetun tärkeätä näiden periaatteiden noudattaminen on voimakeinojen käytön yhteydessä ja salaisten tiedonhankintakeinojen yhteydessä sekä yleensäkin puututtaessa poliisitoimenpiteiden yhteydessä muutoin olennaisin tavoin kansalaisten oikeuspiiriin.

Perusoikeuksien ja ihmisoikeuksien kunnioittamista koskevan poliisilain 1 luvun 2 §:n mukaan poliisin on valtaansa käyttäessään valittava ajateltavissa olevista vaihtoehdoista se, joka parhaiten ja vähimmällä haitalla edistää näiden oikeuksien toteutumista.

Suhteellisuusperiaatteella tarkoitetaan sitä, että käytettävien keinojen ja niiden aiheuttamien haittojen tulee olla järkevässä suhteessa tavoiteltuun päämäärään. Suhteellisuusperiaatteen ilmaiseva poliisilain 1 luvun 3 § kuuluu seuraavasti: ”Poliisin toimenpiteiden on oltava puolustettavia suhteessa tehtävän tärkeyteen, vaarallisuuteen ja kiireellisyyteen, tavoiteltavaan päämäärään, toimenpiteen kohteena olevan henkilön käyttäytymiseen, ikään,

terveyteen ja muihin vastaaviin häneen liittyviin seikkoihin sekä muihin tilanteen kokonaisarviointiin vaikuttaviin seikkoihin”.

Suhteellisuusperiaatteen ajatuksen ilmentävä erityissäännös on lisäksi poliisilain 1 luvun 9 §:ssä otsikolla ”Toimenpiteestä luopuminen ja sen siirtäminen”. Säännöksen mukaan poliisilla on oikeus luopua toimenpiteestä, jos sen loppuunsaattaminen voisi johtaa tavoiteltavaan tulokseen nähden kohtuuttomiin seurauksiin. Säännöksellä pyritään estämään sellaisten tilanteiden syntyminen, joissa poliisivaltuuksien käyttö saattaisi aiheuttaa asianosaiselle tai sivulliselle henkilölle suurempaa haittaa kuin torjuttava oikeudenloukkaus tai häiriö.

Vähimmän haitan periaate korostaa perusoikeutta rajoittavan toimenpiteen välttämättömyyden vaatimusta. Poliisin toimenpiteet on suoritettava puuttumatta kenenkään oikeuksiin enempää tai aiheuttamatta suurempaa vahinkoa tai haittaa kuin on välttämätöntä tehtävän suorittamiseksi. Poliisi saa arvioida toimenpiteen välttämättömyyttä lähtökohtaisesti vain poliisille kuuluvien päämäärien saavuttamiseen nähden. Poliisitehtäviä suoritettaessa ei ole siten toimivaltajärjestelmän soveltamiseen nähden mahdollista pitää silmällä yhteiskunnan ”yleistä hyvää”.

Poliisityössä ei saa käyttää voimakeinoja tai muita toimivaltuuksia enempää kuin tilanne välttämättä vaatii. Poliisitehtävän yhteydessä on usein mahdollista harkita erilaisia toimenpiteitä tilanteen ratkaisemiseksi. Valintaa ohjaa välttämättömyyden vaatimus. Keinovalikoimasta tulee ottaa käyttöön se, josta aiheutuva haitta jää pienimmäksi. Tämä voi käytännössä merkitä sitä, ettei poliisi voi valita sille itselleen parhaiten sopivaa, kätevintä ja halvinta toimintatapaa. Periaatteen käytännön merkitys ilmenee ehkä selvimmin niissä tilanteissa, joissa poliisi joutuu harkitsemaan erityyppisten voimakeinojen tai salaisten tiedonhankintakeinojen käyttöä.

Välttämättömyyden vaatimus ilmenee myös siten, että vain sellaisen toimivaltuuden käyttäminen on oikeutettua, joka on omiaan johtamaan poliisin tavoittelemaan tulokseen. Henkilöön ei esimerkiksi saa kohdistaa telekuuntelua, vaikka telekuuntelun edellytykset näennäisesti olisivatkin olemassa, mikäli tilanteen osalta tiedetään, että telekuuntelulla ei todellista tavoitetta kuitenkaan tulla saavuttamaan. Välttämättömyyden periaatteen unohtaminen merkitsisi silloin poliisitoimenpiteen muuttumista perusteettomaksi puuttumiseksi perus- ja ihmisoikeuksiin.

Poliisitoiminnassa saatetaan joutua puuttumaan voimakkaasti ja sangen konkreettisestikin toimen kohteena olevan henkilön oikeusasemaan. Tämä korostaa ehdotonta lainmukaisuuden vaatimusta kaikissa poliisitehtävissä. Poliisilain 1 luvun 5 §:n mukaan poliisi saa käyttää toimivaltuuttaan vain säädettyyn tarkoitukseen.

Salaiset pakkokeinot ja tiedonhankintakeinot

Suomessa poliisin nykyiset toimivaltuudet mahdollistavat telekuuntelun, tietojen hankkimisen telekuuntelun sijasta, televalvonnan ja muut keinot (esim. tekninen kuuntelu ja tekninen laitetarkkailu) myös päästä päähän salattujen viestien kuuntelussa, kunhan salaisen tiedonhankintakeinon käytön edellytykset täyttyvät. Näistä edellytyksistä säädetään kattavasti pakkokeinolain (PKL) 10 luvussa ja poliisilain 5 luvussa. Arvion salaisen pakkokeinon tai tiedonhankintakeinon käytöstä tekee aina tuomioistuin. Viestin salauksen tasolla ei pakkokeinon tai tiedonhankintakeinon edellytysarvioinnissa ole merkitystä. Poliisin lisäksi Tullilla, Rajavartiolaitoksella ja Puolustusvoimilla on oikeus salaisten pakkokeinojen

ja tiedonhankintakeinojen käyttöön ja niistä säädetään kyseisten organisaatioiden rikostorjuntaa koskevassa kansallisessa lainsäädännössä.

Salaisten pakkokeinojen ja tiedonhankintakeinojen käyttö on tiukasti säänneltyä. Salaisten pakkokeinojen ja tiedonhankintakeinojen käytön yleisenä edellytyksenä on, että käytöllä voidaan olettaa saatavan rikoksen selvittämiseksi tarvittavia tietoja. Jokaisen salaisen pakkokeinojen käytön erityisistä edellytyksistä säädetään jokaista pakkokeinoa koskevassa pykälässä erikseen. Tämän lisäksi telekuuntelua, tietojen hankkimista telekuuntelun sijasta, suunnitelmallista tarkkailua, teknistä kuuntelua, teknistä katselua, henkilön teknistä seurantaa, teknistä laitetarkkailua, peitetoimintaa, valeostoa, tietolähteen ohjattua käyttöä ja valvottua läpilaskua saadaan käyttää vain, jos niillä voidaan olettaa olevan erittäin tärkeä merkitys rikoksen selvittämiselle. Salaisen pakkokeinon käyttö on lopetettava ennen päätöksessä mainitun määräajan päättymistä, jos käytön tarkoitus on saavutettu tai sen edellytyksiä ei enää ole.

Salaisten pakkokeinojen käyttöperusteille yhteinen piirre on se, että ne on määritelty henkilö- ja rikoslähtöisesti. Henkilölähtöisyys tarkoittaa sitä, että salaisen pakkokeinon käyttö tapahtuu aina yksittäistapauksessa tietyn henkilön osalta. Ja rikoslähtöisyys tarkoittaa sitä, että pakkokeinon myöntäminen on mahdollista vain tutkittaessa pakkokeinoa koskevassa pykälässä säädettyjä tiettyjä rikoksia.

Salaisten pakkokeinojen ja tiedonhankintakeinojen valvonta

Poliisin suorittamien salaisten pakkokeinojen ja tiedonhankintakeinojen valvontaa säädellään pakkokeinolaissa ja poliisilaissa. Pakkokeinolain 10 luvun 65 §:n mukaan poliisin salaisten pakkokeinojen käyttöä valvovat niitä käyttävien yksiköiden päälliköt ja Poliisihallitus alaistensa yksiköiden osalta. Sisäministeriön on annettava eduskunnan oikeusasiamiehelle vuosittain kertomus salaisten pakkokeinojen ja niiden suojaamisen käytöstä ja valvonnasta sekä salaisten tiedonhankintakeinojen ja niiden suojaamisen käytöstä ja valvonnasta. Esitutkintaviranomaiset suorittavat telekuuntelua virkavastuulla. Poliisilain 5 luvun 63 §:n mukaan salaista tiedonhankintaa valvovat salaisia tiedonhankintakeinoja käyttävien yksiköiden päälliköt sekä sisäministeriö suojelupoliisin osalta ja Poliisihallitus alaistensa yksiköiden osalta. Sisäministeriön on annettava eduskunnan oikeusasiamiehelle vuosittain kertomus salaisten tiedonhankintakeinojen ja niiden suojaamisen käytöstä ja valvonnasta. Oikeusasiamiehelle annettavista rikoksen selvittämiseksi käytettyjä salaisia pakkokeinoja koskevista kertomuksista säädetään pakkokeinolaissa.

EU:n oikeuden mukainen oikeusperusta/päätöksentekomenettely

Käsittely Euroopan parlamentissa

Kansallinen valmistelu

Oikeus- ja sisäasioiden EU 7-jaoston ja EU 19 -viestintäjaoston kirjallinen menettely 16.2-27.2.2024

Eduskuntakäsittely

Kansallinen lainsäädäntö, ml. Ahvenanmaan asema

Teleoperaattoreihin kohdistuu voimassa olevassa lainsäädännössä teknisiä laatuvaatimuksia, joiden mukaisesti teleoperaattoreiden on rakennettava tarjoamansa viestintäpalvelu siten, että televalvonta sekä muut viranomaisten tiedonsaantioikeuksia koskevat pyynnöt voidaan toteuttaa laissa säädetyn mukaisesti. Sähköisen viestinnän palveluista annetun lain (917/2014) 245 §:n mukaan telekuuntelua tai televalvontaa suorittavan viranomaisen on toimitettava Liikenne- ja viestintävirastolle (Traficom) esitys niistä toiminnallisista laatuvaatimuksista, jotka viestintäverkon ja viestintäpalvelun on täytettävä. Traficom päättää yksittäistapauksessa telekuuntelussa tai televalvonnassa käytettävälle apuvälineelle tai ominaisuudelle asetettavista teknistä vaatimuksista kuultuaan teleyritystä ja viranomaista, joka on tehnyt sille esityksen edellä mainituista toiminnallisista laatuvaatimuksista.

Viestinnän välittäjän avustusvelvollisuudesta säädetään myös pakkokeinolain (2011/806) 10 luvun 63 §:ssä, jossa teleoperaattoreille on asetettu velvollisuus tehdä telekuuntelun ja valvonnan edellyttämät kytkennät ja annettava esitutkintaviranomaisen käyttöön tarpeelliset tiedot, välineet ja henkilöstön, josta on johdettavissa laatuvaatimusten kautta, että se saattaa vaatia muutoksia näiden uuden ajan teleoperaattoreiden ohjelmistoihin tai laitteistoihin.

Taloudelliset vaikutukset

Mahdollisia taloudellisia vaikutuksia voisi koitua esimerkiksi liittyen järjestelmäkehitykseen tai tulevaisuudessa tarvittaviin koulutuksiin. Mahdolliset lisäresurssitarpeet käsitellään talousarviomenettelyssä ja julkisen talouden suunnitelman valmistelussa.

Muut asian käsittelyyn vaikuttavat tekijät

Kansallisesti on parhaillaan käynnissä hanke sähköisen viestinnän eräiden välitystietojen säilytysvelvollisuutta koskevan lainsäädännön täsmentämiseksi (LVM040:00/2023). HLG:n työllä ja erityisesti sitä seuraavilla toimenpidealoitteilla saattaa olla vaikutusta myös kansalliseen hankkeeseen.

Euroopan ihmisoikeustuomioistuimen oikeuskäytäntö: sallittu puuttuminen EIS 8(1) artiklan mukaisiin oikeuksiin

Siitä, että sekä viestinnän sisältö että viestinnän tunnistamistiedot nauttivat EIS 8 artiklan mukaista suojaa, ei seuraa, että viranomaiset eivät niihin voisi puuttua. Yksityiselämään puuttuminen voi olla verrattain laajamittaistakin, kunhan se tapahtuu EIS 8(2) artiklan edellyttämissä puitteissa. EIS 8(2) artikla asettaa kolme ehtoa sille, että artiklan takaamiin oikeuksiin voidaan viranomaistoiminnassa puuttua: 1) puuttumisen on oltava kansallisen lain sallimaa, 2) sen on tapahduttava tiettyjen artiklassa erikseen lueteltujen etujen turvaksi ja 3) puuttumisen on oltava demokraattisessa yhteiskunnassa välttämätön.

Yksityiselämän ja siten myös luottamuksellisen viestinnän suojaan puuttumisen mahdollistavia etuja ovat muun muassa yleinen turvallisuus ja rikollisuuden estäminen.

EU-tuomioistuimen oikeuskäytäntö

Viranomaisten tiedonsaantioikeuksiin ja erityisesti niiden laajentamiseen digitaalisessa ympäristössä liittyy keskeisesti perus- ja ihmisoikeusherkkyyksiä, sillä niillä usein puututaan käyttäjien perusoikeuksiin, erityisesti yksityisyydensuojaan ja henkilötietojen suojaan. Unionin tuomioistuin on käsitellyt viimeisten vuosien aikana useissa eri ennakkoratkaisuissaan yksityisyydensuojan yhteensovittamista rikollisuuden torjunnan ja kansallisen turvallisuuden tavoitteiden varmistamisen kanssa (ks. erityisesti ratkaisut asioissa C-362/14, C-311/18 ja C-817/19 sekä yhdistetyissä asioissa C-511/18, C-512/18 ja C-520/18 sekä C-203/15 ja C-698/15). Erityisesti HLG:n työn kannalta on merkityksellistä unionin tuomioistuimen sähköisen viestinnän luottamuksellisuutta koskeva oikeuskäytäntö. Yksityisyyden suoja ja henkilötietojen suoja eivät ole ehdottomia oikeuksia, vaan ne on suhteutettava siihen tehtävään, joka niillä on yhteiskunnassa (La Quadrature du Net ym., C-511/18, C-512/18 ja C-520/18, EU:C:2020:791, 120 kohta oikeuskäytäntöviittauksineen).

EUT:n ja EIT:n vakiintuneen oikeuskäytännön mukaan jo pelkästään yksityiselämään liittyvien tietojen säilyttäminen merkitsee puuttumista 8 artiklan mukaiseen yksityiselämän suojaan. Euroopan ihmisoikeussopimuksen 8 artiklan 2 kohdassa säädetään tilanteista, joissa puuttuminen 8 artiklan mukaisiin oikeuksiin on mahdollista, esimerkiksi rikollisuuden estämiseksi. Suojatoimien tarve on suurempi silloin, kun kyse on automatisoidusta henkilötietojen käsittelystä. Kun EU:n tuomioistuin on arvioinut liikenne- ja paikkatietojen kohdennettua säilyttämisestä vakavan rikollisuuden torjumiseksi, se on edellyttänyt, että toimi on objektiivisten ja syrjimättömien seikkojen perusteella rajattu asianomaisten henkilöiden ryhmien mukaan tai maantieteellisen kriteerin avulla ajanjaksoksi, joka on rajoitettu täysin välttämättömään (La Quadrature du Net ym., C-511/18, C-512/18 ja C-520/18, EU:C:2020:791, 168 kohta) tai ainakin välillistä yhteyttä vakavien rikosten ja henkilöiden, joiden tiedot säilytetään, välillä (SpaceNet AG, C-793/19 ja C-794/19, 112 kohta). EU-tuomioistuin on edellyttänyt, että lainsäädännön on täytettävä objektiiviset kriteerit, joilla luodaan yhteys säilytettävien tietojen ja tavoitellun päämäärän välille. Näiden edellytysten on erityisesti oltava käytännössä sellaisia, että niissä rajataan tehokkaasti toimenpiteen laajuus ja tätä kautta asianomainen yleisö (Tele2 ja Watson –ratkaisu, yhdistetyt asiat C-203/15 ja C-698/15, kohta 110).

Asiakirjat

Laatijan ja muiden käsittelijöiden yhteystiedot

Katariina Simonen, neuvotteleva virkamies, SM PO KEY, + 358 295 488 212, katariina.simonen@gov.fi

Hannele Taavila, poliisijohtaja, SM PO KEY, + 358 295 488 568, hannele.taavila@gov.fi

VAHVA-tunnus
EU/199/2024

Liitteet ei ole

Viite ei ole