Sisäministeriö
Inrikesministeriet

Lausunto

6.5.2024

EU/199/2024
EU/199/2024-SM-4

Jakelussa mainituille

Sisäministeriön lausunto hallintovaliokunnalle (Going Dark)

Hallintovaliokunta on pyytänyt sisäministeriön lausuntoa E-kirjeestä, joka koskee oikeus- ja lainvalvontaviranomaisten lainmukaista tietoon pääsyä digitaalisessa ympäristössä (ns. Going Dark –aloite).

E-kirjeen tausta

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).

Hankkeen 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). Kysymyksessä on komission ja puheenjohtajavaltion yhdessä vetämä työryhmä. Edustettuina ovat jäsenvaltiot sekä useita EU:n virastoja. Suomi osallistuu HLG:n ja sen alaisten asiantuntijatyöryhmien työhön sisäministeriön johdolla, ja mukana ovat myös oikeusministeriö ja liikenne- ja viestintäministeriö.

Rikostorjunnan digitaalisen ympäristön haasteet

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.

Haasteen muodostaa se, että oikeus- ja lainvalvontaviranomaisten on entistä vaikeampi pysyä digitaalisen kehityksen mukana ja toteuttaa tehokkaita lainvalvontatoimia. Haasteet vaikuttavat yleisen järjestyksen turvaamiseen, rikosten ennaltaehkäisemiseen, havaitsemiseen, selvittämiseen ja tuomioistuimeen saattamiseen sekä uhrien legitiimien oikeusturva- ja korvausvaateisiin vastaamiseen.

Postiosoite **Postadress** **Postal Address**	**Käyntiosoite** **Besöksadress** **Office**	**Puhelin** **Telefon** **Telephone**	**Faksi** **Fax** **Fax**	**s-posti, internet** **e-post, internet** **e-mail, internet**
Sisäministeriö				
PL 26 00023 Valtioneuvosto	Kirkkokatu 12 Helsinki	0295 480 171 +358 295 480 171	09 160 44635 +358 9 160 44635	kirjaamo.sm@gov.fi www.intermin.fi

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.

Lainvalvontaviranomaisten 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.

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.

Erityisen haasteen muodostavat OTT-toimijat. OTT-toimijat ovat teleyrityksistä riippumattomia toimijoita internetissä, kuten WhatsApp ja Skype. Nämä 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.

Tietoon pääsy tarkoittaa sitä, että data on oikeus- ja lainvalvontaviranomaisten hankittavissa, yksittäistapauksissa ja tuomioistuimen luvalla, luettavassa muodossa ja reaaliaikaisesti, jotta rikosten selvittäminen, ennalta estäminen ja paljastaminen olisi mahdollista.

On tärkeä korostaa, että ratkaisujen löytäminen tähän viestintään pääsyyn selkokielisessä muodossa yksittäistapauksissa ja tuomioistuimen luvalla ei kuitenkaan tarkoita salauksen eikä tietoturvan heikentämistä yleisesti, eikä tällaista nyt käsillä olevassa E-kirjeessä esitetä. Heikentämisellä ei siten tarkoiteta teknologisen kehityksen tai muiden järjestelyjen mahdollistamaa tuomioistuimen luvalla yksittäistapauksissa tapahtuvaa lainvalvontaviranomaisten pääsyä salattuun tietoon.

Oikeus- ja lainvalvontaviranomaisten intressit on kyettävä turvaamaan tulevaisuudessakin. Sen vuoksi tarkoituksenmukaisten ja oikeasuhtaisten ratkaisujen kehittäminen on keskeisintä. Tämä on tehtävä tulevaisuusorientoituneesti, tutkimukseen ja kehitykseen painottaen, ratkaisuhakuisesti ja yhdessä kaikkien intressitahojen kesken.

HLG – Korkean tason asiantuntijaryhmä

HLG:n tavoitteena on valmistella asiakirja, jossa esitetään mahdollisia ratkaisuehdotuksia oikeus- ja lainvalvontaviranomaisten tietoon pääsyn turvaamiseksi. HLG:n työllä pyritään myös vaikuttamaan tulevan komission työohjelmaan. HLG:n on määrä saada työnsä valmiiksi kesällä 2024. 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.

HLG:n työn oikeudelliset puitteet muodostaa EU:n perusoikeuskirja, tietosuojalainsäädäntö, EU:n ja EIT:n (Euroopan ihmisoikeustuomioistuimen) oikeuskäytäntö sekä Suomen kansallinen lainsäädäntö.

HLG:n työssä on tähän mennessä noussut esiin kysymys OTT-toimijoiden hallussa olevaan tietoon pääsemiseksi sopimalla televalvonnan ja –kuuntelun käytännöistä ja toteuttamisesta ja EU-tason lainsäädännön tarve tältä osin. Toiseksi HLG:n työssä on laajalti tunnistettu tietoon pääsyn haasteet, jotka liittyvät sirpaloituneeseen viestinnän välitystietojen säilytysvelvollisuuden (ns. *data retention*, DR) sääntelyyn. Vastaavasti EU-tason lainsäädännön tarve datan säilytysaikojen harmonisoimiseksi on ollut työssä esillä. Kolmas kokonaisuus on koskenut ennakollista vaikuttamista, ns. *lawful access by design*. Kyse on lainvalvontaviranomaisten osallistuminen standardointityöryhmiin, jotta lainvalvontaviranomaisten tarpeet tulisivat huomioitua etukäteisesti tuotekehittelyssä ja suunnittelussa.

Suomen kanta

Suomi tukee HLG:n työtä ja työn lähtökohtia.

Suomi pitää tärkeänä, että tunnistettaviin ongelmiin etsitään EU-tason ratkaisuja tietoon pääsemiseksi tarkkaan rajatuissa tapauksissa. Ratkaisujen tavoitteena tulisi olla rikosten ennalta estäminen, paljastaminen ja selvittäminen sekä syyteharkintaan saattaminen ja yleisen turvallisuuden vahvistaminen. Ratkaisuissa on huomioitava täysimääräisesti EU:n ja kansallisen lainsäädännön asettamat edellytykset.

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

Mahdollisten ratkaisuehdotusten ei tulisi sisältää toimenpiteitä, jotka vaarantaisivat kyberturvallisuutta heikentämällä viestintä- ja tietojärjestelmien turvallisuutta. Heikentämisellä ei kuitenkaan tarkoiteta teknologisen kehityksen tai muiden järjestelyjen mahdollistamaa tuomioistuimen luvalla yksittäistapauksissa tapahtuvaa lainvalvontaviranomaisten pääsyä salattuun tietoon.

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.

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.

Neuvotteleva virkamies Katariina Simonen

Liitteet ei ole

Jakelu Eduskunnan hallintovaliokunta

Tiedoksi Eduskunta, Minna-Liisa Rinne
SM Sisäministeriö, Mari Rantanen
SM Sisäministeriö, Timo Kerttula
SM Sisäministeriö, Antti Salminen
SM PO Poliisiosasto, Hannele Taavila
SM Kansliapäällikkö, Anu Alvesalo
SM KP Esikunnan tukipalvelut, Katarine Lindstedt

EU/199/2024-SM-4

Seuraavat henkilöt ovat allekirjoittaneet tämän asiakirjan sähköisesti /

Följande personer har undertecknat denna handling elektroniskt /

This document has been signed electronically by the following persons:

Simonen Katariina 913016085

2024-05-06