Hallintovaliokunta

Poliisihallituksen asiantuntijalausunto asiassa: E 26/2024 vp Valtioneuvoston selvitys: Oikeus- ja lainvalvontaviranomaisten lainmukainen tietoon pääsy digitaalisessa ympäristössä eli ns. Going Dark –aloite

1 Yleistä

Going dark -ongelmista eli lainvalvonta- ja oikeusviranomaisten pääsystä digitaaliseen tietoon on käyty keskustelua jo vuosia ja Going dark -termiä on käytetty ensimmäisen kerran jo vuonna 2015 Yhdysvaltojen liittovaltion lainvalvontaviranomaisen FBI:n ja Euroopan lainvalvontaviraston Europolin julkisissa puheenvuoroissa. Teknologian nopea kehittyminen on asettanut rikosten ennalta estämiselle, paljastamiselle ja selvittämiselle jo pitkään haasteita ja lainsäädäntö tietoon pääsemiseksi ei ole kaikilta osin seurannut teknologian kehittymistä. Euroopan unionissa on tunnistettu lainvalvonta- ja oikeusviranomaisten tarve saada pääsy laissa säädetyissä tapauksissa digitaaliseen tietoon ja Euroopan unionissa on säädetty asetus ja direktiivi sähköiseen todistusaineistoon pääsystä eli ns. E-evidence asetus ja direktiivi (EU) 2023/1543 ja (EU) 2023/1544. Asetukseen liittyvä kansallisen toimeenpanon lainsäädäntö on tällä hetkellä oikeusministeriön johdolla valmisteltavana. Vaikka kyseisen lainsäädännön tavoitteena on ollut nopeuttaa ja varmistaa lainvalvonta- ja oikeusviranomaisten tiedonsaanti, siinä ei kuitenkaan säädetä esimerkiksi velvollisuuksista toimittaa tietoa luettavassa muodossa eli tieto voi olla siten salattua, etteivät tietoon pääsyyn oikeutetut viranomaiset voi tietoa avata luettavaan muotoon.

Euroopan poliisiylijohtajat ovat kiinnittäneet Going dark ongelmaan useana vuonna huomiota ja 18.4.2024 pidetyn Euroopan poliisiylijohtajien kokouksen julkilausumassa pyydetään lainsäätäjiä kiinnittämään huomiota siihen, että lainsäädäntö mahdollistaisi riittävän tiedon saamisen, jotta lainvalvontaviranomaiset voisivat turvata kansalaisia. Samalla kiinnitetään huomiota myös siihen, että teknologiateollisuus suunnittelisi palvelunsa siten, että se mahdollistaisi lainvastaisen toiminnan tunnistamisen ja siitä ilmoittamisen lainvalvontaviranomaisille. Poliisiylijohtajat kiinnittävät huomiota myös siihen, että viestinnän luottamuksellisuus ja kyberturvallisuus ovat tärkeitä innovaatioita, mutta em. seikkojen ja turvallisuuden osalta ei tule tehdä absoluuttisia valintoja vaan etsiä kaikkia palvelevia ratkaisuja.

POLIISIHALLITUS
Vuorimiehentie 3, PL 1000, 02151 ESPOO
kirjaamo.poliisihallitus@poliisi.fi
Puh. +358 295 480 181, Faksi +358 295 411 780

On huomattava, että Going dark -haasteet eivät koske vain tietoverkoissa tapahtuvaa rikollisuutta, vaan kysymys on rikostorjunnan kokonaisuuteen vaikuttavista asioista. Esimerkiksi henkirikosta selvitettäessä voi selvitä, että rikoksesta epäillyn käyttämästä viestiliikenteestä ei voida saada sisältöä selville, koska tieto on siten salattu, ettei sitä voida avata.

Suomessa kuten muissakin EU-jäsenvaltioissa lainsäätäjät ovat säätäneet lainvalvontaviranomaisille oikeuden saada tuomioistuimen päätöksellä tietoa viestinnän sisällöstä. Lainsäätäjän tahto on ollut sillä tavalla selvä, että riittävien vakavien rikosten estämiseksi, paljastamiseksi tai selvittämiseksi voidaan tuomioistuimen erikseen myöntämällä luvalla poiketa perustuslain (731/1999) 10 §:ssä säädetystä kirjeen, puhelun tai muun viestinsalaisuuden loukkaamattomuudesta. Vaikka Suomessa mm. pakkokeinolaissa ja poliisilaissa säädetään telekuuntelusta, ei näissä laeissa säädettyjen toimivaltuuksien toteuttaminen ole kuitenkaan teknologian kehittymisen johdosta enää kaikissa tapauksissa mahdollista toimivaltaisille viranomaisille.

Perusmuistiossa mainittu oikeus- ja sisäministerien aloitteesta perustettu korkean tason asiantuntijaryhmä HLG on tervetullut aloite sille, että selvitetään teknisiä ja lainsäädännöllisiä mahdollisuuksia Going dark -ongelman ratkaisemiseksi.

2 Suomen kanta

Kuten perusmuistiossa todetaan, pääministeri Petteri Orpon hallitusohjelmaan on kirjattu digitalisaation vahvistamista rikostutkinnassa ja -torjunnassa ja tässä tapauksessa ratkaisujen hakeminen tulee tapahtua EU-tasoisesti. Valtaosassa lainvalvontaviranomaisten tutkimista rikoksista on saatavilla myös sähköistä todistusaineistoa ja usein todistusaineisto sijaitsee Suomen rajojen ulkopuolella esimerkiksi jollain sosiaalisen median palveluita tai pikaviestintää tarjoavalla yhtiöllä. Vaikka tieto saataisiinkin, niin tietoa ei voida hyödyntää rikosten tutkinnassa, mikäli se on salattua. Tieto, jota ei saada luettavaan muotoon voi olla rikosprosessin kannalta merkittävää joko syyllisyyden tai syyttömyyden osoittamiseksi.

Edellä mainitun HLG asiantuntijaryhmän tavoitteena on ollut perusmuistiosta ilmenevällä tavalla nimenomaan selvittää laajassa, avoimessa yhteistyössä ja läpinäkyvästi ongelman ydintä sekä mahdollisia ratkaisuesityksiä. On erittäin tärkeää, että ratkaisut, joita esitetään, ovat EU-tasolla toteutettavia varsinkin niissä tapauksissa, joissa sillä olisi vaikutusta sähköisiä palveluita tarjoavien yritysten toimintaan. Kansalliset lainsäädännön ratkaisut eivät ole riittäviä, koska internetin suuret palveluntarjoajat sijaitsevat ulkomailla ja todennäköisesti vain Euroopan kokoisen markkina-alueen oikeudellisella sääntelyllä olisi toivottu vaikutus palveluiden tuottamiseen.

Mahdolliset esitettävät ratkaisut Going dark ongelmaan tulee olla sellaisia, että niissä huomioidaan riittävällä tavalla kansalaisten turvallisuus ja koskemattomuus suhteessa viestinnän luottamuksellisuuteen ja kyberturvallisuuteen. Ei voida vain todeta, ettei ongelmaan ole tarjolla ratkaisua, koska

kaikki nyt tiedossa olevat ratkaisut ovat sellaisia, joiden arvioidaan olevan haitallisia kyberturvallisuudelle tai viestinnän luottamuksellisuuden suojalle ja samaan aikaan sivuutetaan yhteiskunnan korkea intressi esimerkiksi estää ennalta ja selvittää vakavia rikoksia ja terrorismia. Oikeasuhtaista perusoikeuksien toteutumista voidaan tulkita monella tavalla, mutta olennaista on, ettei muita kansalaisten turvallisuuteen ja vapauteen liittyviä perusoikeuksia sivuuteta muilla perusoikeuksilla. Perusmuistiossa Suomen kannassa esitetyt oikeudelliset ja muut vaikutusarviot ovat kannatettavia silloin kuin niissä huomioidaan riittävän kattavasti myös kansalaisten turvallisuus.

Salauksen käyttö viestinnässä on osa tunnistettua Going dark-ongelmaa. Kuten perusmuistiossa on todettu, olisi tärkeää kehittää EU-tasolla tapa, jossa yksittäistapauksissa laissa säädetyin edellytyksin lainvalvontaviranomaisilla olisi pääsy tietoon samaan tapaan kuin tällä hetkellä kansallinen lainsäädäntö mahdollistaa tuomioistuimen luvalla telekuuntelun. Olennaista on, että näissäkin tapauksissa lainsäädännössä on säädetty selvä prosessi tietoon pääsylle ja siihen kohdistuu tuomioistuimen ennakkovalvonnan lisäksi myös jälkikäteistä valvontaa mm. eduskunnan oikeusasiamiehen toimesta. Telekuuntelussa pääsystä tietoon vastaa teleoperaattori, jolla on tieto siitä mikä viranomainen suorittaa telepakkokeinoja ja teleoperaattorit myös vastaavat hallussaan olevasta tiedosta. Tällaisen käytössä olevan ratkaisun soveltuvuutta muidenkin viestinnän palveluita toimittavien tahojen kanssa olisi selvitettävä. Teleoperaattoreiden velvoitteiden täyttäminen ei ole edellyttänyt takaovien rakentamista järjestelmiin, vaan prosessit ovat läpinäkyviä.

Suomen kannassa esitetään, ettei *ratkaisuehdotusten 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.* Tätä täsmennetään perusmuistion muistion seuraavassa virkkeessä. Tässä yhteydessä parempi tapa olisi ilmaista asia siten, ettei salaustapoja ole tarpeen muuttaa, mikäli näin voidaan toimia yksittäisten käyttäjien osalta laissa säädetyissä tapauksissa, jotta viranomaiset pääsevät tietoon salaamattomassa muodossa.

Salauksen heikentämistä, vahvuutta tai hyväksyttyjä salaustapoja ole määritelty lainsäädännössä. Vuonna 2023 voimaan tulleessa kyberturvallisuuteen liittyvistä toimenpiteistä säätävän EU:n NIS2 direktiivin (EU) 2022/2555 resitaalissa 98 on käsitelty päästä päähän salausta ja siinä yhteydessä on todettu, että "*Päästä päähän -salauksen käyttö olisi sovitettava jäsenvaltioiden toimivaltaan varmistaa keskeisten turvallisuusetujensa ja yleisen turvallisuuden suojelu ja mahdollistaa rikosten ennalta estäminen, tutkiminen, paljastaminen ja rikoksiin liittyvät syytetoimet unionin oikeuden mukaisesti.*" Kuten edeltä selviää, niin lainsäätäjä on tunnistanut päästä päähän salaukseen liittyvän riskin esimerkiksi rikosten estämisen, paljastamisen ja selvittämisen osalta ja antaa kansallisesti mahdollisuuden

puuttua sen käyttöön. Tämän tulisi näkyä myös Suomen kannassa sekä tulevissa ratkaisuehdotuksissa.

Perusmuistiossa kirjattua virkettä "*Suomi pitää tärkeänä selvittää, mitä mahdollisuuksia edellä mainitut reunaehdot antavat viranomaisen pääsylle reaaliaikaiseen tietoon*" voisi harkita muutettavaksi siten, että kyse ei välttämättä ole kaikissa tapauksissa reaaliaikaisesta tiedosta, kun päästä päähän salattuun tietoon on tarpeen päästä yksittäisissä tapauksissa.

Tasapuolisen kilpailun osalta on todettava, että pikaviestinpalveluita toimittavat yritykset eivät ole heille asetettavien velvollisuuksien osalta samassa asemassa kuin esimerkiksi teleoperaattorit, joita velvoittaa kansallinen lainsäädäntö viranomaisten avustamisessa.

Internetin ja viestinnän teknologioiden standardoinnissa ja niitä koskevassa EU-lainsäädännössä tulisi huomioida nykyistä paremmin lainvalvonta- ja oikeusviranomaisten tarpeet vakavien rikosten torjumiseksi ja Suomen kannassa tätä koskeva kirjaus on kannatettava.

Poliisitarkastaja Toni Sjöblom

Asiakirja on sähköisesti allekirjoitettu asianhallintajärjestelmässä. Poliisi 06.05.2024 klo 23:07. Allekirjoituksen oikeellisuuden voi todentaa kirjaamosta.