Poliisihallituksen lausunto eduskunnan lakivaliokunnalle U 33/2018 vp: Euroopan parlamentin ja neuvoston asetuksesta ja direktiivistä (lainvalvontaviranomaisen rajat ylittävä pääsy sähköiseen todistusaineistoon)

1 Yleistä

Digitaalinen ts. sähköinen todistusaineisto on luonteeltaan nopeasti syntyvää ja häviävää, jonka vuoksi sähköisen todistusaineiston hankinta rikosten ennalta estämiseksi ja rikostutkinnan tarpeisiin on erittäin aikakriittistä. Rikostorjunnan tarpeisiin hankittava sähköinen todistusaineisto sijaitsee usein toisessa maassa ja todistusaineiston hankinta esitutkintaa varten vaatii useimmiten oikeusapumenettelyn käyttämistä tietojen saamiseksi. Oikeusapuihin perustuva menettely sähköisen todistusaineiston hankkimiseksi ulkomaisilta palveluntarjoajilta on usein hidasta ja pyynnön menestyminen ei ole varmaa. Mikäli pyyntöä sähköisen todistusaineiston saamiseksi ulkomaiselta palveluntarjoajalta ei saada tehtyä riittävän ajoissa, on vaarana, että todistusaineisto on hävitetty ja ei ole enää palautettavissa. Kansainvälisillä sähköisten palveluiden tarjoajilla ei ole usein lainsäädännössä säädettyä velvollisuutta säilyttää sähköistä aineistoa.

Sähköisen todistusaineiston merkitys rikostorjunnassa on kasvanut merkittävästi ja komission arvion mukaan jo noin puolessa rikostutkinnassa olevista tapauksista käytetään sähköistä todistusaineistoa. Digitalisaatio, verkossa asiointi ja erilaisten sähköisten palveluiden käyttö kommunikointiin on lisännyt tarvetta sähköisten todisteiden hankintaan. Esitutkinnan kannalta merkityksellinen sähköinen todistusaineisto Suomessa ilmenneessä rikoksesta sijaitsee entistä useammin Suomen rajojen ulkopuolella ja kansallisella lainsäädännöllä ei voida vaikuttaa ulkomailla toimiviin palveluntarjoajiin todistusaineiston hankkimiseksi ja sen vuoksi komission lainsäädäntöesitykset rikostutkinnan mahdollistamiseksi ja tehostamiseksi ovat oikeansuuntaista kehitystä.

Sähköisen todistusaineiston saannin turvaamiseksi ja nopeuttamiseksi on vireillä useita kansainvälisiä lainsäädäntöön tai sopimuksiin liittyviä aloitteita, joista esitetyn asetuksen sekä direktiivin osalta merkittävin on Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimuksen 2. lisäpöytäkirjan valmistelu.

POLIISIHALLITUS
Asemapäällikönkatu 14, PL 22, 00521 HELSINKI
kirjaamo.poliisihallitus@poliisi.fi
Puh. +358 295 480 181, Faksi +358 295 411 780

2 Asetus- ja direktiiviehdotuksen vaikutus lainvalvontaviranomaisten toimintaan Suomessa

Asetusehdotuksessa on pyritty luomaan jäsenvaltioita ja EU:n alueella sähköisiä palveluita tarjoavia tahoja velvoittavaa lainsäädäntöä sähköisen todistusaineiston säilyttämiseksi ja toimittamiseksi pyytävän jäsenvaltion viranomaiselle. Kysymys on vastavuoroisen tunnustamisen oikeudellisesta instrumentista, jossa pyynnön vastaanottajana toimiva yhteisö velvoitetaan toimittamaan pyytäjävaltion lainvalvonta- tai oikeusviranomaiselle sähköisessä muodossa olevia tietoja rikosprosessissa hyödynnettäväksi.

Toimivaltaisten lainvalvonta- ja oikeusviranomaisten suoraan palveluntarjoajille esittämät sähköisen todistusaineiston säilyttämis- ja esittämismääräykset mahdollistavat oikeusapupyyntöjä nopeamman ja tehokkaamman toiminnan todisteiden hankinnassa. Suorilla palveluntarjoajille esitettävillä pyynnöillä voidaan vähentää lainvalvonta- ja oikeusviranomaisten tarvetta käsitellä rutiininomaisia tietopyyntöjä, tehostaa rikostorjuntaa ja lyhentää esitutkintaan käytettävää aikaa.

Asetusehdotuksessa sähköisen todistusaineiston tietoluokat on jaoteltu neljään osa-alueeseen: tilaajatiedot (subscriber data), kirjautumistiedot (access data), liikennetiedot (transactional data) ja viestin sisältötiedot (content data).

Edellä mainituista tietoluokista tilaajatiedot ovat poliisin toiminnan kannalta merkityksellisimpiä ja tämän tietoluokan osalta olisi varmistettava se, että poliisi voi esittää määräyksen tiedon säilyttämiseksi ja esittämiseksi suoraan ulkomaiselle palveluntarjoajalle samaan tapaan kuin kotimaiselle palveluntarjoajalle esitetty poliisilain (872/2011) 4:3:2 mukainen pyyntö tilaajatietojen saamiseksi.

Kirjautumistietojen (access data) osalta on keskusteltu siitä, mahdollistaako kansallinen lainsäädäntö tiedon pyytämisen poliisilain 4:3 perusteella ja vastaavasti onko tiedon haltijalla mahdollisuus luovuttaa hallussaan oleva kirjautumistieto lain sähköisen viestinnän palveluista 136§ perusteella. Kirjautumistiedoissa on kyse on kansallisen lainsäädännön tulkinnan mukaan henkilötiedoista ja lain sähköisen viestinnän palveluista 136§:n mukaisesti, *viestinnän osapuoli voi käsitellä omia sähköisiä viestejään ja niihin liittyviä välitystietoja, jollei laissa toisin säädetä.* Asetuksessa säädetään kirjautumistiedoista hieman laajemmin kuin kansallisessa lainsäädännössä ja tältä osin kansallista lainsäädäntöä voi olla tarpeen tarkastella ja määrittää tarkemmin.

Kirjautumistiedot ovat tilaajatietojen lisäksi toinen esitutkinnan kannalta tärkeä ja usein palveluntarjoajilta pyydetty tieto ja operatiivisen toiminnan kannalta olisi tarpeellista, että pyynnöt tällaisten tietojen säilyttämiseksi ja esittämiseksi voitaisiin esittää suoraan lainvalvontaviranomaiselta palveluntarjoajalle. Mikäli useimmin käytettyjen tietoluokkien osalta joudutaan käyttämään kansallisia oikeusviranomaisia tiedon säilyttämis- ja esittämismääräysten validointiin, niin asetuksella tavoiteltu toiminnan nopeus ja tehokkuus voivat kärsiä merkittävästi, jolloin asetuksella tavoiteltu hyöty jää saavuttamatta.

Esityksen tavoitteena on ollut siirtyminen oikeusapumenettelystä erilaiseen, kevyempään ja suorempia yhteyksiä koskevaan sääntelyyn. Valtioneuvoston kannassa on esitetty tavoiteltavana, että palveluntarjoajan kotivaltion viranomaisella olisi rooli vieraan valtion viranomaisen määräyksen saavuttua. Jonkinlainen rooli on hyväksyttävissä liikennetietojen ja sisältötietojen osalta, ja silloinkin se tulisi toteuttaa vain kevyen notifikaation tyyppisen menettelyn kautta. Mikäli kaikkien esittämis- ja säilyttämismääräysten osalta ryhdyttäisiin notifikaatiomenettelyyn, niin asetuksella tavoiteltu toiminnan nopeus ja tehokkuus kärsivät merkittävästi, ja asetuksella tavoiteltu hyöty jää saavuttamatta.

Asetusehdotuksen 2. artiklan 3. kohdassa määritelmää palveluntarjoajista on tarpeen tulkita laajasti ja varmistaa, että mm. lisäarvopalveluita tarjoavat yritykset kuuluvat asetuksen soveltamisalan piriin, koska tällaisilla palveluntarjoajilla voi olla rikostutkinnan kannalta merkityksellistä sähköistä todistusaineistoa.

Kansallisessa lainsäädännössä ei ole säädetty palveluntarjoajille seuraamuksia mikäli ne kieltäytyvät lainvalvonta- ja oikeusviranomaisten esittämästä määräyksistä tietojen toimittamiseksi. Asetuksen 13. artiklan mukaiset palveluntarjoajille esitetyt hallinnolliset sanktiot ovat kannatettavia ja asetuksessa esitettyjen sanktioiden lisäksi olisi tarkasteltava tarvetta säätää vastaavat kansalliset sanktiot poliisilain 4 luvun 3§:n mukaisista tietopyynnöistä kieltäytymisille.

3 Resurssivaikutukset

Mikäli asetuksella säädettävien tietojen säilyttämis- ja esittämismääräykset tilaaja- sekä kirjautumistietojen osalta saadaan järjestettyä kansallisesti siten, että poliisi voi esittää määräykset suoraan ulkomailla sijaitseville palveluntarjoajille ja vastaavasti ulkomailta tulevat määräykset toimitetaan Suomessa suoraan palveluntarjoajille, eikä poliisiviranomaisille aseteta tarkastusvelvollisuutta jokaisen saapuvan tiedon säilyttämis- ja esittämismääräyksen osalta, voi tietopyyntöjen käsittelyyn käytettäviä henkilöresursseja poliisissa ohjata muualle tiedonhankintaan ja esitutkintaan.

Tiedon välittäminen lainvalvonta- ja oikeusviranomaisten välillä kansallisesti sekä pyyntöjen ja vastausten välittäminen kansainvälisesti on toteutettava tietoturvallisella tavalla ja tämä aiheuttanee kustannuksia joiden suuruutta ei voida tässä vaiheessa arvioida. Kysymykseen tulisi lähinnä yhdenmukaisen ja salatun viestinnän toteuttaminen eri toimijoiden kesken.

Jakelu Lakivaliokunta