Oikeusministeriö

Oikeusministeriön lausuntopyyntö 20.4.2018 komission lainsäädäntöehdotuksista liittyen lainvalvontaviranomaisten rajat ylittävään pääsyyn sähköiseen todistusaineistoon rikosasioissa, OM 4/481/2018

KESKUSRIKOSPOLIISIN LAUSUNTO

Asian tausta ja lausuntopyyntö

Oikeusministeriö on pyytänyt Keskusrikospoliisilta lausuntoa komission 17.4.2018 antamasta ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi sähköistä todistusaineistoa rikosasioissa koskevista eurooppalaisesta esittämismääräyksestä ja säilyttämismääräyksestä (COM(2018) 225 final) sekä direktiiviehdotuksesta yhtenäisistä säännöistä koskien laillisten edustajien nimittämistä sähköisen todistusaineiston keräämiseksi rikosasioissa (COM(2018) 226 final). Ehdotus on osa komission samana päivänä hyväksymiä toimenpiteitä, joiden tarkoituksena on toteuttaa toimia terroristien ja muiden rikollisten toimintatapojen ja -tilan rajoittamiseksi. Lausuntopyyntö on pyydetty toimittamaan oikeusministeriölle viimeistään 9.5.2018. Keskusrikospoliisi sai pyynnöstä lisäaikaa lausunnon toimittamiselle 14.5.2018 saakka.

Asetusehdotus sähköistä todistusaineistoa rikosasioissa koskevista eurooppalaisesta esittämismääräyksestä ja säilyttämismääräyksestä (COM (2018) 225 final)

Yleistä

Nyt lausunnolla olevassa asetusehdotuksessa säännellään siitä, miten ja millä edellytyksillä jäsenvaltion lainvalvontaviranomainen voi velvoittaa Euroopan unionin alueella palveluita tarjoavan palveluntarjoajan toimittamaan tai säilyttämään tietyn palveluntarjoajan hallussa olevan sähköisessä muodossa olevan tiedon käytettäväksi todistusaineistona käynnissä olevassa rikosoikeudellisessa menettelyssä. Kysymys voisi olla esimerkiksi sähköpostia koskevista sisältö- tai lähetystiedoista. Ehdotuksella ei ole tarkoitettu vaikutettavan jäsenvaltioiden sisäisiin menettelyihin, joissa on kysymys lainvalvontaviranomaisen oikeuksista velvoittaa samassa jäsenvaltiossa toimivaa palveluntarjoajaa luovuttamaan tietoja.

Keskusrikospoliisi toteaa, että tehty esitys on lähtökohtaisesti kannatettava, sillä tavoitteena on nimenomaan tehostaa lainvalvontaviranomaisten toimintaa virtaviivaistamalla sähköisen todistusaineiston hankkimiseen liittyvää prosessia jäsenvaltioiden rajat ylittävissä tilanteissa. Rikostutkinnassa käytettävä todistusaineisto on yhä enenevässä määrin sähköisessä muodossa johtuen toimintaympäristöjen digitalisoitumisesta. Lisäksi sähköinen todistusaineisto on usein johonkin toiseen valtioon sijoittautuneen palveluntarjoajan hallussa. Sähköisen todistusaineiston hankkimiseksi rikostutkintaa varten joudutaankin nykyisellään lähtökohtaisesti kohdistamaan oikeusapupyyntö (mutual legal asssistace-menettely) siihen maahan, johon palveluntarjoaja on sijoittautunut tai missä data sijaitsee. Tällöin oleellisen todistusaineiston saaminen voi kohtuuttomasti pitkittää esitut-

kintaprosessia johtuen oikeusapumenettelyjen pitkäkestoisuudesta (usein useita kuukausia tai jopa vuosia). Kuluva aika ei aina ole edes pyytäjän vaikutuspiirissä, vaikka pyyntöjä kiirehtisi. Käytännössä oikeusapumenettelyiden kestoissa on suuriakin eroja.

Esitetyllä muutoksella voidaan katsoa olevan esitutkintaprosessin kokonaisaikaa lyhentävä vaikutus. Palveluntarjoajilta pyydettävät tiedot voivat olla myös esitutkintaa suuntaavia (esim. rikoksesta epäillyn henkilöllisyys tai osoitetiedot). Tällöin on tärkeää, että tiedot saadaan esitutkintaviranomaisten käyttöön mahdollisimman aikaisessa vaiheessa rikosprosessia ja samalla mahdollisimman nopeasti.

Asetuksen tavoitteena em. tehostamistavoitteen lisäksi yhdenmukaistaa palveluntarjoajilta saatavan tiedon prosessia EU:ssa. Tällä hetkellä tiedonsaantiprosessi voi vaihdella merkittävästi riippuen siitä, mihin maahan ja mille palveluntarjoajalle tietopyyntö osoitetaan. Nykysääntely on pirstaleista ja monimutkaista, mikä aiheuttaa myös monimutkaisia tietopyyntöprosesseja lainvalvontaviranomaisten kesken. Kokonaisuuteen liittyy myös paljon erilaisia maakohtaisia käytäntöjä. Näin ollen Keskusrikospoliisi pitää lähtökohtaa yhdenmukaisesta prosessista erittäin perusteltuna.

Esityksen mukaan toisen EU-maan lainvalvontaviranomainen voisi tehdä dataa koskevan esittämis- ja säilyttämismääräyksen suoraan toiseen EU-maahan sijoittautuneelle palveluntarjoajalle. Keskusrikospoliisi katsoo, että esityksellä on tältä osin myös täytäntöönpanovaltion lainvalvontaviranomaisten resursseihin kohdistuva positiivinen vaikutus. Kohdistettaessa eurooppalainen esittämis- ja/tai säilyttämismääräys suoraan palveluntarjoajalle ilman täytäntöönpanovaltion aktiivista myötävaikutusta vapautuu täytäntöönpanovaltion lainvalvontaviranomaisten resurssit muun muassa varsinaisten oikeusapupyyntöjen täytäntöön panemiseen.

Tällä hetkellä Suomen ulkopuolelta osoitetut tietopyynnöt Suomeen sijoittautuneille palveluntarjoajille toimitetaan täytäntöön pantavaksi Keskusrikospoliisiin, joka toimii poliisille osoitettujen tiedustelu- ja oikeusapupyyntöjen osalta kansallisena keskusvirastona / keskuksena. Johtuen sähköisen todistusaineiston kasvavasta merkityksestä rikostutkinnoissa sekä tiettyjen keskeisten sähköisten palvelujen tarjoajien sijoittautumisesta Suomeen, voidaan sanoa, että palveluntarjoajille tehdyt tietopyynnöt työllistävät tällä hetkellä Keskusrikospoliisia merkittävästi. Siten asetusehdotuksella tavoiteltua muutosta voidaan pitää poliisin näkökulmasta kustannustehokkuutta lisäävänä ratkaisuna. Myöhemmin tehtävien käytännön toiminnallisten ratkaisujen pitää olla sellaisia, että ne mahdollistavat esityksen kokonaistavoitteen saavuttamisen. Käytännön menettelyt eivät saa olla liian formaalisia ja niiden pitää tarvittaessa olla joustavia. Tutkinnalliset tavoitteet pitää pystyä toteuttamaan aikaperiaatteella 24/7.

Sähköistä todistusaineistoa tarvitaan lainvalvontaviranomaisten käyttöön riippumatta jutun laadusta, joten Keskusrikospoliisi pitää tärkeänä, ettei tehtyä esitystä ole lähtökohtaisesti rajattu esimerkiksi vain terrorismirikoksiin. Esityksen tavoitteena on torjua terrorismirikoksia, mikä on sinällään perusteltua. Esityksessä on tehty tiettyjen tietoluokkien osalta rangaistusmaksimiin sekä rikosnimikkeisiin liittyviä rajauksia, joihin liittyviä huomioita esitetään tarkemmin jäljempänä.

Aiemmin datan sijaintipaikalla on ollut ratkaisevaa merkitystä myös palveluntarjoajille tehtävien tietopyyntöjen osalta. Tämä on voinut merkitä sitä, että todistusaineiston hankkimiseksi tehty oikeusapupyyntö on jouduttukin tekemään datan sijaintipaikan valtioon. Nyt käsillä olevassa ehdotuksessa luovutaan datan sijaintipaikan merkityksestä tässä mielessä. Tätä kehitystä Keskusrikospoliisi pitää kannatettava johtuen ensinnäkin siitä, että datan sijaintipaikan määrittäminen voi olla lainvalvontaviranomaisille usein käytän-

nössä jopa mahdotonta. Sähköisen todistusaineiston tallennuspaikka saattaa lisäksi vaihtaa myös paikkaa nopeasti, joten käytännössä datan sijaintipaikkaan nojautuva menettely asettaa isoja haasteita lainvalvontaviranomaisille.

Jotta täytäntöönpanovaltiolla olisi kuitenkin käsitys siitä, millaisia esittämis- ja säilyttämismääräyksiä sen alueelle sijoittautuneille palveluntarjoajille tehdään, niin Keskusrikospoliisi katsoo, että asetukseen tulee kytkeä notifikaatiomenettely ainakin esittämismääräyksen osalta. Tällaisella menettelyllä pystyttäisiin turvaamaan myös se, että täytäntöönpanovaltio voisi kieltää tietyissä tilanteissa (esim. oma rikostutkinnallinen syy) esittämismääräyksen täytäntöönpanon. Notifikaatiomenettelyllä turvattaisiin merkittävissä määrin lisäksi valtioiden suvereniteettia. Lisäksi voitaisiin luoda paremmat takeet sen osalta, ettei esittämismääräyksellä loukattaisi kansallista turvallisuutta ja puolustusta siten kuin esimerkiksi artiklan 5 kohdassa 7 tarkoitetaan.

Keskusrikospoliisi toteaa, että asian hoitamiseksi välttämättömät pakkokeinot tulee suorittaa edelleen kansallisten viranomaisten kautta. Pakkokeinojen käyttöön liittyy usein myös velvollisuus ilmoittaa jälkikäteen pakkokeinon käytöstä kohteelle. Tämän vuoksi ehdotuksessa tulisi ottaa selkeästi kantaa siihen, kenen velvollisuuksiin ilmoittaminen kuuluu, ja minkä valtion lakia asiassa noudatetaan.

Tietojen rajat ylittävä suora pääsy on rajattu nyt kokonaisuudessaan esityksen ulkopuolelle. Vuonna 2017 käydyissä asiantuntijakokouksissa suora yhteydenpito oli vielä mukana omana elementtinään. Ehdotuksessaan komissio toteaa, että vaikutusten arvioinnissa päädyttiin malliin D, joka mahdollistaisi myös suoran pääsyn dataan. (s. 9) Tämä elementti jätettiin lopullisesta ehdotuksesta pois.

Keskusrikospoliisi pitää kannatettavana kansainvälistä säädöskehitystä, joka on tällä hetkellä käynnissä Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimuksen (SopS 60/2007; jäljempänä "Budapestin sopimus") 2. lisäpöytäkirjan laatimiseen liittyvässä sääntelytyössä. Tuossa Neuvoston instrumentissa on tavoitteena luoda säännökset siitä, miten tietoa voitaisiin hankkia myös suoraan lainvalvontaviranomaisten käytössä olevalta laitteelta ns. loss of knowledge of location-tilanteissa sekä äärimmäisissä kiiretilanteissa. Loss of knowledge of location -tilanteilla tarkoitetaan tilannetta, joissa tiedon sijaintipaikka on tuntematon tai tieto on jatkuvasti liikkeessä taikka ei ole muista syistä tiedossa tahoa, johon tiedonsaantipyynnön voisi kohdistaa. Tuo kehitystyö on vasta alkuvaiheessa ja tavoitteena on saada 2. lisäpöytäkirja valmiiksi vuoden 2019 loppuun mennessä. Keskusrikospoliisi pitääkin tästä syystä järkevänä, että suora yhteydenpito on jätetty nyt lausuttavana olevan komission esityksen ulkopuolelle tässä vaiheessa. Ei olisi tarkoituksenmukaista luoda Budapestin sopimuksen kanssa kilpailevaa tai jopa ristiriitaista instrumenttia liittyen rajat ylittävään suoraan pääsyyn.

Komission toimesta on pyritty tehostamaan myös käytännön toimenpiteitä liittyen rajat ylittävän tiedonsaannin edistämiseksi, mm. turvallisen sähköisen alustan luomiseen tietopyyntöjen välittämistä varten. Tällaiset käytännön toimenpiteet ovat tärkeitä, mutta eivät riittäviä, minkä vuoksi Keskusrikospoliisi pitää nyt lausuttavana olevaa säädösehdotusta lähtökohtaisesti kannatettava.

Lainsäädäntöperusta

Lainsäädäntöperustaksi on esitetty Euroopan unionista tehdyn sopimuksen ja Euroopan unionin toiminnasta tehdyn sopimuksen konsolidoidut toisinnot (2016/C 202/01) V osaston 4 luvun (oikeudellinen yhteistyö rikosoikeuden alalla) 82 artiklaa:

1. Oikeudellinen yhteistyö unionissa rikosoikeuden alalla perustuu tuomioistuinten tuomioiden **ja oikeusviranomaisten päätösten vastavuoroisen tunnustamisen** periaatteeseen, ja siihen kuuluu jäsenvaltioiden lakien ja asetusten lähentäminen 2 kohdassa ja 83 artiklassa tarkoitetuilla aloilla.

Euroopan parlamentti ja neuvosto säätävät tavallista lainsäätämisjärjestystä noudattaen toimenpiteistä, joiden tarkoituksena on:

a) laatia sääntöjä ja menettelyjä **kaikenmuotoisten tuomioiden ja oikeusviranomaisten päätösten tunnustamisen** varmistamiseksi koko unionissa;

b) ehkäistä ja ratkaista jäsenvaltioiden välisiä tuomioistuimen toimivaltaa koskevia ristiriitoja;

c) tukea tuomareiden ja oikeuslaitoksen henkilöstön koulutusta;

d) helpottaa jäsenvaltioiden oikeusviranomaisten tai vastaavien viranomaisten yhteistyötä rikosasioiden käsittelyn ja päätösten täytäntöönpanon yhteydessä.

2. Euroopan parlamentti ja neuvosto voivat tavallista lainsäätämisjärjestystä noudattaen annetuilla direktiiveillä säätää vähimmäissäännöistä sikäli kuin se on tarpeen tuomioiden ja oikeusviranomaisten päätösten vastavuoroisen tunnustamisen sekä poliisiyhteistyön ja **oikeudellisen yhteistyön helpottamiseksi rajat ylittävissä rikosasioissa**. Näissä vähimmäissäännöissä otetaan huomioon jäsenvaltioiden oikeusperinteiden ja -järjestelmien erot.

Vähimmäissäännöt koskevat seuraavia asioita:

a) todisteiden vastavuoroinen hyväksyttävyys jäsenvaltioissa;

b) yksilön oikeudet rikosasioiden käsittelyssä;

c) rikosten uhrien oikeudet;

d) muut rikosasioiden käsittelyn erityiset osatekijät, jotka neuvosto on ennalta määrittänyt päätöksellä. Neuvosto tekee tällaisen päätöksen yksimielisesti Euroopan parlamentin hyväksynnän saatuaan.

Tässä kohdassa tarkoitettujen vähimmäissääntöjen hyväksyminen ei estä jäsenvaltioita pitämästä yllä tai ottamasta käyttöön niitä korkeatasoisempaa yksilön suojelua.

3. Jos neuvoston jäsen katsoo, että ehdotus 2 kohdassa tarkoitetuksi direktiiviksi vaikuttaisi jäsenen rikosoikeusjärjestelmän perusteisiin, se voi pyytää asian saattamista Eurooppa-neuvoston käsiteltäväksi. Tässä tapauksessa tavallisen lainsäätämisjärjestyksen mukainen menettely keskeytetään. Kun asiaa on käsitelty ja jos on päästy yhteisymmärrykseen, Eurooppa-neuvosto palauttaa ehdotuksen neljän kuukauden kuluessa keskeyttämisestä neuvostolle, mikä lopettaa tavallisen lainsäätämisjärjestyksen mukaisen menettelyn keskeyttämisen.

Jos asiasta ei päästä yhteisymmärrykseen ja jos vähintään yhdeksän jäsenvaltiota haluaa aloittaa tiiviimmän yhteistyön kyseisen direktiiviehdotuksen pohjalta, niiden on saman määräajan kuluessa ilmoitettava asiasta Euroopan parlamentille, neuvostolle ja komissiolle. Tällöin lupa aloittaa Euroopan unionista tehdyn sopimuksen 20 artiklan 2 kohdassa ja tämän sopimuksen 329 artiklan 1 kohdassa tarkoitettu tiiviimpi yhteistyö katsotaan annetuksi ja määräyksiä

Keskusrikospoliisilla ei ole riittävää kompetenssia arvioida asetusehdotuksen lainsäädäntöperustan oikeellisuutta. Valinta nostettiin kuitenkin asiaa koskevassa Neuvoston kokouksessa 27.4.2018 useiden jäsenvaltioiden toimesta esille. Tältä osin pyydettiin jopa konsultaatiota Neuvoston oikeuspalvelulta (NOP). Keskusrikospoliisin näkemyksen mukaan asia tulisi tutkia tältä osin hankkeen aikana perusteellisesti.

Keskusrikospoliisi esittää seuraavia huomioita asetusehdotukseen sisällytettyjen artiklojen osalta:

Asiasisältö (Artikla 1)

Palveluntarjoajan, johon esittämis- tai säilyttämismääräys kohdistetaan, tulee tarjota palvelujaan EU:n alueella. Sen sijaan pyydettävän datan sijaintipaikalla ei ole esityksen mukaan merkitystä ratkaistaessa sitä, voidaanko asetusta soveltaa. Tämä mainitaan nimenomaisesti artiklan 1.kohdassa. Valittu malli noudattelee kansainvälistä kehitystä tältä osin, sillä datan sijaintipaikalle ei ole annettu viime aikoina enää niin määräävää asemaa kuin aikaisemmin. Tämä johtuu luonnollisesti siitä tosiseikasta, että datan sijaintipaikan tarkka määrittäminen voi olla lainvalvontaviranomaisille vaikea tai jopa mahdoton tehtävä. Tältä osin lähtökohtaa, jossa datan sijaintipaikalla ei ole enää määräävää vaikutusta, voidaan pitää onnistuneena. Malli seuraa toimintaympäristökehitystä.

Keskusrikospoliisi kiinnittää huomiota artiklassa 1 käytettyyn termiin 'authority'. Selitysmuistiossa on käytetty vastaavassa yhteydessä termiä 'judicial authority'. Jälkimmäinen viittaa oikeusviranomaiseen. Oikeusviranomaista ei ole kuitenkaan sen tarkemmin määritelty asetuksessa. Sen sijaan myöhemmin asetuksen artiklassa 4 määritellään ne viranomaiset, joiden toimesta Eurooppalainen esittämis- ja säilyttämismääräys voidaan antaa. Tältä osin esitetään huomiot artiklan 4 yhteydessä.

Asetuksessa todetaan nimenomaisesti, että se ei saa vaikuttaa kansallisiin olemassa oleviin menettelyihin. Keskusrikospoliisi pyytää huomioimaan, ettei sääntelyn myötä pääse muodostumaan tilanteita, jossa toisen EU-maan lainvalvontaviranomainen voi saada tietyn asetuksen kattaman tiedon palveluntarjoajalta tehokkaammin kuin vastaavassa tilanteessa kansallinen viranomainen. Ainakin tältä osin tulisi myös tarkastella kansallisiin lakeihin sisältyviä esitutkintaviranomaisten tiedonsaantisäännöksiä. Kansallisesta lainsäädännöstä puuttuu tällä hetkellä ainakin mahdollisuudet asettaa lainvalvontaviranomaisten palveluntarjoajille osoittamien tietopyyntöjen tehosteiksi sakkoja. Tällä hetkellä puuttumiskeinona on lupaedellytyksiin liittyvä arviointi tilanteissa, joissa palveluntarjoaja ei noudata viranomaistoiminnan tiedonsaantisäännöksiä.

Määritelmät (Artikla 2)

(3) Palveluntarjoaja

Palveluntarjoajien määritelmän osalta viitataan artiklan 2 kohdassa 3 palveluntarjoajiin, jotka tarjoavat yhtä tai useampaa seuraavista palveluista:

> a) sähköisiä yhteyspalveluja siten kuin ne on määritelty direktiivissä (Directive establishing the European Electronic Communication Code)[1]
> b) tietoyhteiskunnan palveluja siten kuin ne on määritelty direktiivin (EU) 2015/1535 artiklasn 1(1) b-kohdassa ja joille datan säilöminen (storage of data) on määräävä komponentti käyttäjälle tarjottavan palvelun osalta ml. sosiaaliset networkit, online markkinapaikat, jotka mahdollistavat siirrot käyttäjien ja niiden hosting-palveluiden välillä
> c) internetin domain nimi ja IP-numeropalvelut kuten IP-osoitepalveluntarjoajat ja niihin kytkeytyvät yksityisyys ja proxy-palvelut.

Keskusrikospoliisi pitää tärkeänä, että asetukseen sisällytettävä palveluntarjoajien määritelmä on mahdollisimman laaja. On erityisen tärkeää, että myös lisäarvopalvelun tarjoajat kuuluvat soveltamisalan piiriin. Lisäarvopalvelun tarjoajat on määritelty kansallisen tietoyhteiskuntakaaren (917/2014; Laki sähköisen viestinnän palveluista 1.6.2018 lukien) 1 luvun 3 §:n 10-kohdassa. Listauksen pitää olla kattava. Lisäarvopalvelun tarjoajalla tarkoitetaan tietoyhteiskuntakaaressa palvelua, joka perustuu välitystietojen ja sijaintitietojen käsittelyyn muuta tarkoitusta kuin viestin välittämistä varten. Keskusrikospoliisi esittää, että c-kohtaan lisättäisiin VPN -palveluntarjoajat, sillä muutoin ne näyttävät jäävän soveltamisalan ulkopuolelle.

(4) Palveluiden tarjoaminen EU-alueella

Keskusrikospoliisi katsoo, että asetukseen sisällytetty määritelmä ei ole riittävän tarkkarajainen. Tältä osin tulisi täsmentää, mitä tarkoitetaan b-kohdan mukaisella 'olennainen/huomattava liityntä' (substantial connection) määritelmällä tässä yhteydessä.

[1] COM/2016/0590 final- 2016/0288 (COD)

(8) Access data eli pääsytiedot

Access datana pidetään asetuksessa tietoja, jotka on määritelty artiklan 2 kohdassa 8. Määritelmän osalta viitataan osittain vielä hyväksymättömän e-privacy direktiiviehdotuksen artiklaan 4(3) kohtaan g. Ilmeisesti tässä on kuitenkin tarkoitettu artiklan kohtaa c 'sähköisen viestinnän metadata'. Sähköisen viestinnän metadatalla tarkoitetaan direktiiviehdotuksessa:

> *Tietoja, jotka käsitellään sähköisessä viestintäverkossa sähköisen viestinnän sisällön siirtoa, jakelua tai vaihtoa varten, mukaan lukien viestinnän lähteen ja määränpään jäljittämiseksi ja tunnistamiseksi käytettävät tiedot, sähköisen viestintäpalvelujen tarjoamisen yhteydessä tuotetut laitteen sijaintitiedot sekä viestinnän päivämäärä, ajankohta, kesto ja tyyppi.*

Keskusrikospoliisi katsoo, että tässä yhteydessä olisi syytä käsitellä tarkemmin pääsytietoa ja sen merkitystä rikostutkinnan kannalta. Pääsytiedon voidaan katsoa olevan epäilemättä viestintään liittyvää henkilötietoa. Pääsytietoja on kansallisessa lainsäädäntökehyksessä pidetty henkilötietoina, joista palveluntarjoaja on oikeutettu tietoyhteiskuntakaaren (917/2014) 136 §:n 1 momentin perusteella antamaan tiedon silloin, kun palveluntarjoajaa voidaan pitää viestinnän toisena osapuolena. Kyseisen lainkohdan mukaan viestinnän osapuoli voi käsitellä omia sähköisiä viestejään ja niihin liittyviä välitystietoja, jollei laissa toisin säädetä. Viestinnän osapuolella tarkoitetaan ko. lainkohdassa viestin lähettäjää ja sitä, jolle viesti on tarkoitettu. Osapuoli voi olla joko luonnollinen henkilö tai oikeushenkilö. Osapuolia voivat siten olla esimerkiksi luonnolliset henkilöt, yritykset, työnantajat ja internetsivustojen sekä muiden verkkopalvelujen ylläpitäjät.[2]

TYK 136 § voidaan pitää informatiivisena säännöksenä siitä, kenellä on oikeus ja missä tilanteessa käsitellä viestejä ja niiden välitystietoja. Hallituksen esityksessä arvioitiin, että merkittävä osa sähköistä viestintää koskevista tulkintaepäselvyyksistä johtuu käytettävissä olevien käsittelyoikeuksien virheellisestä arvioinnista. Tulkintaepäselvyyksien taustalla on hallituksen esityksen mukaan ollut usein se, että sähköisen viestinnän tietosuojalaissa määriteltyjä tunnistamistietojen (välitystietojen) käsittelyperusteita on pidetty tarpeettoman tiukkoina välttämättömien toimenpiteiden suorittamiseksi. Arvioinnissa ei ole kuitenkaan aina huomioitu sitä, että tilanteessa toimitaan usein viestinnän toisena osapuolena.

Pääsytiedoissa eli palveluun kirjautumistiedoissa on lähtökohtaisesti kyse IP-osoitetiedoista aikaleimoineen. Tiettyyn sähköiseen palveluun kirjautumisvaiheessa palveluntuottaja on tällaisen viestintätapahtuman toinen osapuoli, joka hyväksyy tai hylkää kirjautumisen. Kirjautumistiedoissa ei siten ole kyse samalla tavalla luottamuksellisen viestin suojan alaisista tiedoista kuin esim. viestiä koskevilla tunnistamistiedoilla. Verkkopalveluun kirjautumista ei ole pidettävä sellaisena viestin lähettämisenä, jota pakkokeinolain telekuuntelua ja valvontaa koskevissa säännöksissä tarkoitetaan. Kirjautumistiedoilla ei ole myöskään viestille keskeisiä ominaisuuksia (sisältöä tai ulkopuolista määränpäätä). Palveluun kirjautumistiedoilla on etenkin esitutkinnan alkuvaiheessa keskeinen merkitys tutkinnan kohdentamisessa ja esimerkiksi rikoksesta epäiltyjen yksilöinnissä.

Hallituksen esityksessä on nimenomaisesti katsottu, että henkilön kirjautuminen esimerkiksi internetissä tarjottavaan viestintäpalveluun on osapuolten välistä viestintää. ***Varsinaisessa palveluun kirjautumisessa viestinnän osapuolia ovat kirjautuva henkilö***

[2] HE 221/2013 vp, s.152.

ja palveluntarjoaja. Sen sijaan, jos palveluntarjoaja tarjoaa viestien välittämistä palvelussaan, on palveluntarjoaja viestinnän välittäjän eli kolmannen osapuolen roolissa palvelun sisällä tapahtuvaan, kirjautumisen jälkeen palvelua hyödyntäen lähetettyihin viesteihin nähden. Kirjautumisen jälkeen tapahtuvaa muiden osapuolten välistä viestintää voidaan käsitellä ainoastaan laissa yksilöidyillä perusteilla.[3]

Käyttäjän näkökulmasta tarkasteltuna viestintätapahtuma saattaa siten sisältää useita erillisiä viestintätapahtumia ja osapuolia. Tietoyhteiskuntakaarta koskevassa hallituksen esityksessä todettiin, että kysymys nousee usein esiin arvioitaessa esimerkiksi keskustelupalstalle lähetettyyn viestiin liittyvien välitystietojen käsittelyperustetta. Teknisessä mielessä tarkasteltuna keskustelupalstalle lähetettyä viestiä voidaan pitää samankaltaisena tilanteena kuin silloin kun sanomalehtien yleisönosastoille lähetetään kirjeitä julkaistavaksi. Tällöin sanomalehti, jolle kirje on tarkoitettu, on viestinnän osapuoli. Viestinnän osapuolena kerättyjen tietojen käsittelyä säännellään palvelua koskevassa sopimuksessa, henkilötietolaissa ja mahdollisesti muussa lainsäädännössä.[4] ***Koska palveluun kirjautumisen osalta on kyse viestinnästä palveluntarjoajan ja palveluun kirjautuvan henkilön välillä, on palveluntarjoajalla Keskusrikospoliisin näkemyksen mukaan oikeus käsitellä niitä tietoyhteiskuntakaaren 136 §:n mukaisesti edellä esitetyllä tavalla.***

Nyt lausuttavana olevassa asetusehdotuksessa tällaiset pääsytiedot on nostettu omaksi tietoluokakseen suhteessa sisältö- ja liikennetietoihin, mutta rinnastetaan muun muassa edellytysten osalta tilaajatietoihin. Keskusrikospoliisi pitää asetuksessa esitettyä jakoa tietoluokista onnistuneena. Tosin asetuksessa käytettyä pääsytietoa koskevaa määritelmää tulisi vielä huolellisesti tarkastella huomioiden erityisesti edellä mainittu. Mahdollisesti asetusehdotuksen mukainen pääsytietoa koskeva määritelmä on hieman laajempi kuin, mihin viestinnän osapuoli on oikeutettu 136 §:n perusteella.

Keskusrikospoliisi pitää ensiarvoisen tärkeänä, että suora yhteydenpito lainvalvontaviranomaisen ja toiseen valtioon sijoittautuneen palveluntarjoajan välillä mahdollistettaisiin asetuksella tilaajatietojen lisäksi ainakin edellä käsiteltyjen pääsytietojen (palveluun kirjautumistietojen) osalta.

Ulottuvuus / laajuus (artikla 3)

Keskusrikospoliisi pitää kannatettavana sitä, että asetuksen ulottuvuus suhteessa palveluntarjoajiin on mahdollisimman laaja kattaen myös palveluntarjoajat, joita ei ole perustettu Euroopan Unionissa, mutta jotka tarjoavat palveluitaan täällä.

Asetuksen käyttöala on esityksessä rajoitettu vain rikosprosessiin (criminal proceedings). Tällä tarkoitetaan prosessia esitutkinnasta aina tuomioon saakka. Keskusrikospoliisi haluaa tältä osin nostaa esille, että vastaava menettely tulisi tarvittaessa ulottaa ainakin tilaaja- ja pääsytietojen osalta myös ns. tiedusteluvaiheeseen kattaen rikosten estämisen ja paljastamisen. Rikosten paljastaminen ja estäminen on usein käytännössä mahdotonta, elleivät lainvalvontaviranomaiset voi saada käyttöönsä esim. tietyn IP-osoitteen rekisteröintitietoja. Tiedusteluvaiheessa tietojen nopea saaminen lainvalvontaviranomaisten käyttöön voi olla jopa tärkeämpää, kuin rikosten selvittämisvaiheessa. Tällöin on vielä mahdollista estää uusien rikosten tekeminen ja mahdollisten lisävahinkojen syntyminen. Preventiivinen toiminta on kustannustehokkuus huomioiden tehokkaampaa ja vaikuttavampaa kuin jälkikäteinen jo tapahtuneen rikoksen selvittäminen.

---

[3] HE 221/2013 vp, s. 152-153.
[4] HE 221/2013 vp, s. 152-153.

Määräyksen antava viranomainen (Artikla 4)

Asetusehdotuksen 4 artiklan mukaan esittämismääräyksen voi antaa a-kohdan mukaiset oikeusviranomaiset tai ko. jutun syyttäjä taikka b-kohdan mukaisesti muu toimivaltainen viranomainen, joka on oikeutettu päättämään todisteiden keräämisestä käynnissä olevassa rikosprosessissa.

Keskusrikospoliisi pitää ehdottoman tärkeänä, että esittämis- ja säilyttämismääräys voitaisiin antaa esitutkintaviranomaisen toimesta ainakin tilaaja- pääsytietojen osalta. Tehokkaan rikosprosessin turvaamiseksi olisi ensiarvoisen tärkeää, ettei palveluntarjoajille osoitettavaa esittämis- ja säilyttämismääräystä alisteta vastaavanlaiseen oikeusviranomaisen (Suomessa käytännössä syyttäjän) vahvistamismenettelyyn kuin EIO - prosessissa.

Asetusehdotus sisältää nyt ehdotuksen tällaisen vahvistamismenettelystä. Menettelyn pitää olla joustavaa ja nopeaa. Tältä osin Keskusrikospoliisi viittaa vielä aiemmin tässä asiassa lausumaansa. Keskusrikospoliisi pitää tärkeänä, että ainakin tilaaja- ja pääsytietojen osalta esitutkintaviranomainen olisi oikeutettu tekemään esittämis- ja säilyttämismääräyksen itsenäisesti ilman asetuksen kuvaamaa oikeusviranomaisen vahvistamismenettelyä. Suomessa esitutkintaviranomaisella on sellaista laajahkoakin itsenäistä päätäntävaltaa, mikä rinnastuu muiden maiden syyttäjäviranomaisten toimivaltaan, minkä vuoksi tällainen ratkaisu olisi perusteltua. Toimi- ja harkintavaltavertailussa määräyksen antajana voisi hyvinkin olla esitutkintaviranomainen. EIO -asetus on ollut voimassa vajaan vuoden. Jo nyt on Keskusrikospoliisin tutkimissa asioissa ollut havaittavissa vahvistamismenettelyn aiheuttamat hidasteet tehokkaalle rikosprosessille. Käytännön menettely on kankeahkoa. Keskusrikospoliisi kiinnitti menettelyä hidastaviin seikkoihin huomiotaan jo EIO:n soveltamislain lausumisvaiheessa.

Edellytykset / olosuhteet Eurooppalaiselle esittämismääräykselle (Artikla 5)

Keskusrikospoliisi pitää kannatettavana sitä, ettei asetuksessa ole asetettu rikosten rangaistusmaksimiin perustuvia edellytyksiä tilaaja- ja pääsytietojen osalta. Valittu linja on kansallisen lainsäädäntömme mukainen. Tilaaja-, ja pääsytiedot ovat tällä hetkellä saatavissa poliisilain 4 luvun 3 §:n mukaisella tiedonsaantioikeudella. Viestiin liittyvien liikenne- ja sisältötietojen osalta edellytysten kytkeminen lähtökohtaisesti rangaistusmaksimiin ja tiettyihin rikosnimikkeisiin voidaan pitää perusteltuna, sillä näihin tietoluokkiin kytkeytyvällä tiedonsaantioikeudella puututaan merkittävämmin perusoikeutena suojattuun luottamuksellisen viestinnän suojaan.

Keskusrikospoliisi huomauttaa kuitenkin, että koska asetus koskee vain tallennettua tietoa ja telepakkokeinoilla hankittu tieto on rajattu esityksen ulkopuolelle, voidaan 3 vuoden rangaistusmaksimia pitää tältä osin kohtuuttoman korkeana.

Kansallisessa pakkokeinolaissa takavarikoimisen edellytyksiä ei ole kytketty rangaistusmaksimiin. Tämä on perusteltua huomioiden takavarikkosäännöksen tarkoituksen. Pakkokeinolain 7 luvun 1 §:n mukaan tieto tai asiakirja voidaan takavarikoida, jos on syytä olettaa, että sitä voidaan käyttää todisteena rikosasiassa, se on rikokselta viety tai se voidaan tuomita menetetyksi. Keskusrikospoliisi katsoo, että esittämismääräyksen 5 artiklan 4-kohdan edellytyksiä tulisi tältä osin tarkastella huolellisesti uudelleen. Tietojen, jotka ovat saatavissa kansallisen lainsäädännön mukaan takavarikon edellytyksillä (pl. teleyritykset; ks. PKL 7:4), osalta vaadittaisiin jatkossa asetusehdotuksen mukaisia lisä-

edellytyksiä, mikäli tietoja halutaan pyytää eurooppalaista esittämismääräystä käyttäen. Tällaista rajoitusta ei sisälly oikeusapumenettelyyn.

Artiklan 5 kohdassa 7 jätetään esittämismääräyksen antavalle valtiolle harkintavalta suhteessa siihen, että voiko liikenne- tai sisältötietoa koskeva pyyntö loukata täytäntöönpanovaltion perusoikeuksia (immuniteettia ja perusoikeuksia) taikka kansallista turvallisuutta ja puolustusta. Keskusrikospoliisin näkemyksen mukaan asian pystyisi turvaamaan paremmin täytäntöönpanovaltion lainvalvontaviranomaiselle tehtävä notifikaatio. Notifikaatiomenttely, joka asetuksesta puuttuu tällä hetkellä täysin, mahdollistaisi täytäntöönpanovaltion reagoinnin tarvittaessa. Notifikaatiomenettelystä on huomioita myös jäljempänä artiklojen 9 ja 14 yhteydessä.

Esittämismääräyksen ja säilyttämismääräyksen vastaanottaja (Artikla 7)

Asetusehdotuksen 7 artiklan 1 kohdan mukaan määräys tulee osoittaa suoraan palveluntarjoajan lailliselle edustajalle. Laillista edustajaa ja sen määritelmää ei ole kuitenkaan kytketty direktiivin vaatimuksiin laillisen edustajan osoittamisesta. Palveluntarjoajalla voisi artiklan nykymuotoilun perusteella ilmeisesti olla laillisia edustajia useammassakin maassa. Keskusrikospoliisin näkemyksen mukaan 7 artiklan 1 kohdassa tulisi olla maininta siitä, että laillisen edustajan tulee olla sijoittautunut johonkin jäsenvaltioon, ja se tulee asettaa noudattaen direktiivissä (2017/0107 (COD)) asetettuja vaatimuksia. Keskusrikospoliisi kiinnittää huomioita siihen, ettei asetuksella voida antaa määräyksiä yli EU:n lainsäädäntövallan suhteessa kolmansiin maihin, minkä vuoksi artiklassa tulee tältä osin löytyä kytkös jäsenvaltioon sijoitettavasta laillisesta edustajasta.

Keskusrikospoliisi nostaa esiin seuraavat kysymykset liittyen 7 artiklan 2 kohtaan:

- mahdollistaako artiklan 2 kohta sen, että Eurooppalainen esittämismääräys toimitettaisiin samassa maassa (pyytävä maa) olevan palveluntarjoajan toimipaikkaan? (vastaavalla tavalla myös artiklan 3 - 4 kohta)
- Vaatisiko tällainen tulkinta muutoksia määritelmiin artiklassa 2? Määritelmät esittämismääräyksestä ja säilyttämismääräyksestä on sidottu siihen, että palveluntarjoaja on edustettuna / toimii toisesta maasta.

Esittämismääräystä ja säilyttämismääräystä koskeva sertifikaatti / EPOC ja EPOC-CR (artikla 8)

Keskusrikospoliisi kiinnittää huomiota siihen, että säilyttämismääräykset tulee lähettää turvallisella ja luotettavalla tavalla palveluntarjoajalle. Tällä tavoin estetään esitutkintaa koskevien tietojen päätyminen ulkopuolisten käyttöön. Näin menetellen palveluntarjoaja voi lisäksi riittävällä tavalla varmistua siitä, että tiedot tulevat esittämis- tai säilyttämismääräykseen oikeutetulta 4 artiklan mukaiselta viranomaiselta. Keskusrikospoliisi korostaa tämän kohdan merkitystä. Toiminnan luotettavuuden kannalta on erittäin tärkeää varmistaa, ettei rikollinen taho pääse viranomaisena esiintyen pyytämään tietoja palveluntarjoajalta.

Keskusrikospoliisi katsoo, että EPOC:ssa ja EPOC-CR:ssä käytettävän kielen tulisi olla englanti. Tällöin vältytään turhilta käännöksiltä, tiedot ovat nopeasti käytettävissä sekä määräykset täytäntöön pantavissa. Lisäksi mahdollisten väärinymmärrysten määrä vähenee, kun käännökset omalle kielelle tehdään englannista. Esimerkiksi Suomessa voi toisinaan olla vaikeaa löytää joitakin harvinaisempien eurooppalaisten kielten tulkkeja.

EPOC:in täytäntöönpano (Artikla 9)

Keskusrikospoliisi kiinnittää huomiota siihen, että artiklan 9 kohdissa 3 - 5 selvitettyjen tilanteiden suhde 14 artiklan mukaisiin kieltäytymisperusteisiin on epäselvä.

Lisäksi Keskusrikospoliisi pitää haastavana palveluntarjoajalle asetettua 9 artiklan 5 kohdan mukaista velvollisuutta arvioida esittämismääräyksen suhdetta Euroopan unionin perusoikeuskirjaan. Keskusrikospoliisin näkemyksen mukaan tämä voitaisiin turvata täytäntöönpanovaltion lainvalvontaviranomaiselle tehtävällä notifikaatiomenettelyllä.

EPOC-PR:n täytäntöönpano (Artikla 10)

Keskusrikospoliisi kiinnittää huomiota siihen, että artiklan 10 kohdissa 4 - 5 selvitettyjen tilanteiden suhde 14 artiklan mukaisiin kieltäytymisperusteisiin on epäselvä.

Sanktiot (Artikla 13)

Kansallisessa lainsäädännössä (poliisilaki tai muussa laissa) ei ole tällä hetkellä sanktiointimekanismia, jos palveluntarjoaja kieltäytyy täytäntöön panemasta lainvalvontaviranomaisten tietopyyntöjä. Lainvalvontaviranomaisten on kieltäytymistapauksissa mahdollista suorittaa esitutkintalain 7 luvun 9 §:n mukainen palveluntarjoajan edustajan kuulustelu tuomioistuimessa, jossa voidaan tutkia kieltäytymisen peruste. Lisäksi tietojen turvaamiseksi on mahdollista suorittaa pakkokeinolain (PKL) 7 luvun 1 §:n mukainen tietojen takavarikointi, mikäli kyse ei ole PKL 7:4 mukaisesta teleyrityksestä tai yhteisötilaajasta. Lisäksi takavarikoitava asiakirja tai data ei saa sisältää tämän lain 10 luvun 3 §:n 1 momentissa tarkoitettuun viestiin liittyviä tietoja taikka mainitun luvun 6 §:n 1 momentissa tarkoitettuja tunnistamistietoja tai 10 §:n 1 momentissa tarkoitettuja tukiasematietoja.

Tietoyhteiskuntakaaren 332 § mukaan on mahdollista asettaa uhkasakko (myös keskeyttämisuhka ja teettämisuhka) lain 330 tai 331 §:n mukaisen velvoitteen tehosteeksi. Keskusrikospoliisin tulkinnan mukaan uhkasakko ei ole kuitenkaan käytettävissä poliisilain 4 luvun mukaisen tiedonsaantipyynnöstä kieltäytymisen tehosteena.

Keskusrikospoliisi pitää asetukseen sisällytettyä mahdollisuutta tehostaa tietopyyntöjen käsittelyä hallinnollisilla sakoilla lähtökohtaisesti kannatettavana. Palveluntarjoajien velvollisuudet tulee kuitenkin määritellä riittävän selkeästi, jotta viranomainen voi arvioida kieltäytymisen ilman tulkintavaikeuksia. Keskusrikospoliisi esittää, että kansalliseen lakiin (poliisilaki) mahdollisesti tehtävät muutokset tulisi tarkastella säädöshankkeen yhteydessä.

Täytäntöönpanoprosessi (Artikla 14)

Keskusrikospoliisi katsoo, että 14 artiklassa kuvatun menettelyn voisi osittain korvata määräysten antamisprosessiin luotava täytäntöönpanovaltion notifikaatio. Palveluntarjoajalla ei ole välttämättä riittävää kykyä arvioida artiklan mukaisia kieltäytymisperusteita. Lisäksi 14 artiklan suhdetta artiklaan 9 tulisi selkeyttää.

Keskusrikospoliisi katsoo, että määräyksissä käytettävän kielen tulisi olla englanti.

Prosessi liittyen konflikteihin kolmannen maan perusoikeuksia ja kansalliseen turvallisuuteen ja puolustukseen liittyvien intressien kanssa (Artikla 15)

Keskusrikospoliisi kiinnittää huomiota siihen, ettei palveluntarjoajilla ole välttämättä riittävää osaamista arvioida artiklan 15 kohdan 1 mukaista konfliktitilannetta suhteessa kol-

mannen maan kansalaisten perusoikeuksiin sekä kolmannen maan kansalliseen turvallisuuteen ja puolustukseen. Keskusrikospoliisin näkemyksen mukaan asetukseen luotava mahdollinen notifikaatiomenettely suhteessa täytäntöönpanovaltion lainvalvontaviranomaiseen voisi luoda paremmat edellytykset em. konfliktitilanteiden arvioimiseksi.

Artiklan nykyinen muotoilu sisältää myös riskin siitä, että palveluntarjoajat vetoavat tähän konfliktiperusteeseen ilman todellista uhkaa kolmannen maan etujen kanssa ja välttyisivät siten esittämismääräyksen täytäntöönpanolta. Myöskään tuomioistuimilla ei välttämättä ole sellaista osaamista arvioida esittämismääräyksen suhdetta kolmannen maan lainsäädäntöön ja mahdollisia konfliktitilanteita siten kuin 15 artiklan 3 - 5 kohdassa on edellytetty.

Prosessi liittyen muihin konflikteihin (16 artikla)

Samat huomiot kuin edellä artikla 15 kohdalla.

Direktiiviehdotus yhtenäisistä säännöistä koskien laillisten edustajien nimittämistä sähköisen todistusaineiston keräämiseksi

Direktiiviehdotuksessa säännellään palveluntarjoajien laillisten edustajien nimittämistä sähköisen todistusaineiston keräämisen helpottamiseksi rikosasioissa.

Yleistä

Direktiiviehdotuksessa säännellään palveluntarjoajien laillisten edustajien nimittämisestä Unionin alueelle liittyen sähköisen todistusaineiston keräämiseen rikosasioissa. Direktiivin tavoitteena on nimenomaan luoda säännöt, joilla asetuksen mukaiset Eurooppalainen esittämis- ja säilyttämismääräys voidaan osoittaa oikealle palveluntarjoajalle EU:n sisällä. Ehdotus kattaa palveluntarjoajat, jotka tarjoavat palveluja EU:ssa riippumatta siitä, missä ne on perustettu (EU:ssa tai EU:n ulkopuolella).

Sääntely on tältä osin toistaiseksi perustunut jäsenvaltioiden sääntelyyn ja se on ollut kovin pirstaleista. Yhtenäinen sääntelypohja parantaa myös palveluntarjoajien mahdollisuuksia täyttää tietopyyntöjä ja niihin liittyviä määräyksiä. Yhtenäistä sääntelypohjaa voidaan pitää lähtökohtaisesti kannatettavana.

Keskusrikospoliisi esittää seuraavia huomioita asetusehdotukseen sisällytettyjen artiklojen osalta:

Soveltamisala ja laajuus (Artikla 1)

Keskusrikospoliisi kiinnittää huomiota siihen, tulisiko direktiivin soveltamisala olla nimenomaisesti kytketty asetuksen mukaisiin määräyksiin (eurooppalainen esittämis- ja säilyttämismääräys). Vai onko direktiivin tarkoituksena asettaa yleinen velvollisuus laillinen edustaja asettamiseksi liittyen todisteiden keräämiseen rikosprosessissa?

Määritelmät (Artikla 2)

Keskusrikospoliisi esittää palveluntarjoajan määritelmän (2-kohta) sekä palveluiden tarjoamisen määritelmän (3-kohta) osalta samat huomioit kuin edellä asetuksen yhteydessä.

Laillinen edustaja (3 artikla)

Artiklan sanamuoto näyttäisi mahdollistavan sen, että palveluntarjoaja asettaa useita laillisia edustajia EU:hun. Tällainen tilanne, jossa palveluntarjoajalla voi olla useita laillisia edustajia herättää seuraavia kysymyksiä:

- minne ja mille edustajalle esittämis- ja säilyttämismääräykset osoitetaan?
- mikäli pyytävässä maassa on laillinen edustaja, niin voidaanko asetusta enää tällöin soveltaa, koska kyse ei tällöin ole asetuksen tarkoittamassa mielessä rajat ylittävästä tilanteesta?
- miten voidaan varmistua siitä, että palveluntarjoajalla on edustaja ainakin yhdessä jäsenvaltiossa direktiivin edellyttämällä tavalla? Kuka valvoo tätä?

Keskusrikospoliisin päällikkö
Poliisineuvos — Robin Lardot

Poliisilakimies — Tommi Reen