Eduskunnan lakivaliokunta
Viite: U33/2018 vp

U 33/2018 vp Valtioneuvoston kirjelmä eduskunnalle ehdotuksista Euroopan parlamentin ja neuvoston asetukseksi ja direktiiviksi (lainvalvontaviranomaisten rajat ylittävä pääsy sähköiseen todistusaineistoon)

Eduskunnan lakivaliokunta on pyytänyt Keskusrikospoliisin kirjallista asiantuntijalausuntoa asiassa Valtioneuvoston kirjelmä (U 33/2018 vp) eduskunnalle ehdotuksista Euroopan parlamentin ja neuvoston asetukseksi ja direktiiviksi (lainvalvontaviranomaisten rajat ylittävä pääsy sähköiseen todistusaineistoon).

Keskusrikospoliisi lausuu kantanaan seuraavaa:

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

Yleistä

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 assistace-menettely) siihen maahan, johon palveluntarjoaja on sijoittautunut tai missä data sijaitsee. Tällöin oleellisen todistusaineiston saaminen voi kohtuuttomasti pitkittää esitutkintaprosessia johtuen oikeusapumenettelyjen pitkäkestoisuudesta (usein useita kuukausia tai jopa vuosia). 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 edellä mainitun 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.

Sähköistä todistusaineistoa tarvitaan lainvalvontaviranomaisten käyttöön riippumatta jutun laadusta, joten Keskusrikospoliisi pitää tärkeänä, ettei tehtyä esitystä ole lähtökohtaisesti rajattu esimerkiksi vain terrorismirikoksiin. 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 käytännössä 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 tulisi kytkeä jonkin tasoinen 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 pitää kannatettavana kansainvälistä säädöskehitystä, joka on tällä hetkellä käynnissä Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimuksen (SopS 60/2007; jäljempänä "Budapestin sopimus") 2. lisäpöytäkirjan laatimiseen liit-

tyvässä 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 pitää kannatettavana, että suoraa pääsyä koskevan sääntelyn sisällyttämistä asetuksen soveltamisalaan harkitaan, mikäli oikeusperusta sen mahdollistaa. Toisaalta Keskusrikospoliisi pitää tärkeänä, että EU-tasolla pystyttäisiin pikaisesti luomaan tehokkaat säännöt todistusaineiston hankkimiseksi suoraan palveluntarjoajilta EU-valtioiden rajat ylittävissä tilanteissa. On olemassa riski, että sääntelyalan laajentaminen koskettamaan suoraan pääsyyn liittyviä tilanteita sekä mahdollisesti myös reaaliaikaista tiedonhankintaa aiheuttaisi merkittäviä hidasteita sääntelyn kehittymiseen liittyen.

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.

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.

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. Tältä osin tulisi tarvittaessa tarkastella kansallisiin lakeihin sisältyviä esitutkintaviranomaisten tiedonsaantisäännöksiä. Kansallisesta lainsäädännöstä puuttuu tällä hetkellä ainakin mahdollisuudet asettaa lainvalvontaviranomaisten palveluntarjoajille osoittamien tietopyyntöjen tehosteiksi sakkoja.

Määritelmät (Artikla 2)

(3) Palveluntarjoaja

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 sähköisen

viestinnän palveluista annetun lain (917/2014) 1 luvun 3 §:n 10-kohdassa. Lisäarvopalvelun tarjoajalla tarkoitetaan tietoyhteiskuntakaaressa palvelua, joka perustuu välitystietojen ja sijaintitietojen käsittelyyn muuta tarkoitusta kuin viestin välittämistä varten. Myös tällaisilla palveluntarjoajilla saattaa olla rikosten tutkinnan kannalta merkityksellistä tietoa, joten ko. palveluntarjoajat tulisi myös saada esittämis- ja säilyttämismääräyksen soveltamisalan piiriin.

(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.

(8) Access data eli pääsytiedot

Keskusrikospoliisi haluaa aluksi kiinnittää huomion asetuksen käännökseen tältä osin. **Acces data** on käännetty asetuksen suomenkielisessä versiossa **verkkoyhteystiedoksi,** joka antanee ehkä vähän väärän kuvan tietoluokasta. Mitään vakiintunutta termiä access datalle suomenkielessä ei ole, mutta usein käytetty termi 'pääsytiedot/palveluun kirjautumistiedot' kuvaisivat Keskusrikospoliisin näkemyksen mukaan tuota tietoluokkaa hieman paremmin.

Keskusrikospoliisi katsoo, että tässä yhteydessä on syytä käsitellä tarkemmin pääsytietoa ja sen merkitystä rikostutkinnan kannalta. Pääsytiedon voidaan katsoa olevan epäilemättä viestintään liittyvää henkilötietoa. Pääsytiedoilla/palveluun kirjautumistiedoilla on usein etenkin esitutkinnan alkuvaiheessa keskeinen merkitys tutkinnan kohdentamisessa ja esimerkiksi rikoksesta epäiltyjen yksilöinnissä. Pääsytietoja on kansallisessa lainsäädäntökehyksessä pidetty henkilötietoina, joista palveluntarjoaja on oikeutettu sähköisen viestinnän palveluista annetun lain (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.[1]

Sähköisen viestinnän palveluista annetun lain 136 §:ää koskevassa 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 lain esitöiden mukaan kuitenkaan aina huomioitu sitä, että tilanteessa toimitaan usein viestinnän toisena osapuolena.[2]

Pääsytiedoissa eli palveluun kirjautumistiedoissa on katsottava olevan lähtökohtaisesti kyse IP-osoitetiedoista aikaleimoineen. Tiettyyn sähköiseen palveluun kirjautumisvaiheessa palveluntuottaja on tällaisen viestintätapahtuman toinen osapuoli, joka hyväksyy tai hylkää kirjautumisen. Sähköisen viestinnän palveluista annetun lain 136 §:ää koskevassa hallituksen esityksessä on nimenomaisesti katsottu, että henkilön kirjautuminen

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

esimerkiksi internetissä tarjottavaan viestintäpalveluun on osapuolten välistä viestintää. ***Varsinaisessa palveluun kirjautumisessa viestinnän osapuolia ovat kirjautuva henkilö 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 221/2013 vp 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 sähköiseen palveluun kirjautumisen osalta on kyse viestinnästä palveluntarjoajan ja palveluun kirjautuvan henkilön välillä, on palveluntarjoajalla Keskusrikospoliisin näkemyksen mukaan oikeus käsitellä näitä tietoja tietoyhteiskuntakaaren 136 §:n mukaisesti edellä esitetyllä tavalla.*** Palveluun kirjautumistiedot tulee siten olla saatavissa rikosten selvittämistä varten poliisilain 4 luvun 3 §:n 1 momentin perusteella.

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.

Keskusrikospoliisi pitää ensiarvoisen tärkeänä, että suora yhteydenpito lainvalvontaviranomaisen ja toiseen valtioon sijoittautuneen palveluntarjoajan välillä mahdollistettaisiin asetuksella tilaajatietojen lisäksi ainakin edellä käsiteltyjen pääsytietojen 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 rikosoikeudellisiin menettelyihin (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 esimerkiksi 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)

Keskusrikospoliisi pitää tärkeänä, että ainakin tilaaja- ja pääsytietojen osalta esitutkintaviranomainen olisi oikeutettu tekemään esittämis- ja säilyttämismääräyksen itsenäisesti ilman asetuksen kuvaamaa oikeusviranomaisen vahvistamismenettelyä. Tehokkaan rikosprosessin turvaamiseksi olisi ensiarvoisen tärkeää, ettei palveluntarjoajille osoitettavaa esittämis- ja säilyttämismääräystä alisteta vastaavanlaiseen oikeusviranomaisen (Suomessa syyttäjän) vahvistamismenettelyyn kuin EIO -prosessissa. 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. Määräyksen antamiseen liittyvän prosessin pitää olla joustava ja nopea.

Suomessa esitutkintaviranomaisella on sellaista laajahkoakin itsenäistä päätäntävaltaa, mikä rinnastuu muiden maiden syyttäjäviranomaisten toimivaltaan, minkä vuoksi tällainen ratkaisu olisi perusteltua.

Eurooppalaisen esittämismääräyksen antamisedellytykset (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 taikka tiettyihin rikosnimikkeisiin. 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. Takavarikkosäännösten perusteella kansallisesti saatavien tietojen (transaktio- ja sisältötiedot) osalta vaadittaisiin jatkossa asetusehdotuksen 5 artiklan 4-kohdan mukaisia lisäedellytyksiä, mikäli tietoja halutaan pyytää eurooppalaista esittämismääräystä käyttäen toiseen EU-maahan sijoittautuneelta palveluntarjoajalta. Tällaista rajoitusta ei sisälly oikeusapumenettelyyn.

Artiklan 5 kohdassa 7 jätetään esittämismääräyksen antavalle valtiolle harkintavaltaa (*'syytä olettaa'*) suhteessa siihen, että onko pyydetyt tiedot (liikenne- tai sisältötiedot) suojattu täytäntöönpanovaltion erioikeuksilla ja vapauksilla taikka voiko tietojen luovuttaminen vaikuttaa täytäntöönpanovaltion olennaisiin etuihin (esim. kansallinen turvallisuus ja puolustus). Keskusrikospoliisin näkemyksen mukaan täytäntöönpanovaltion etua pystyisi tältä osin turvaamaan paremmin täytäntöönpanovaltion lainvalvontaviranomaiselle tehtävällä notifikaatiolla. Notifikaatiomenettely, joka asetuksesta puuttuu tällä hetkellä täysin, mahdollistaisi täytäntöönpanovaltion reagoinnin tarvittaessa artiklassa kuva-

tuissa tilanteissa. Notifikaatiomenettelystä on huomioita myös jäljempänä artiklojen 9 ja 14 yhteydessä.

Eurooppalaisen esittämismääräyksen ja eurooppalaisen säilyttämismääräyksen vastaanottaja (Artikla 7)

Asetusehdotuksen 7 artiklan 1 kohdan mukaan määräys tulee osoittaa suoraan palveluntarjoajan lailliselle edustajalle. Asetuksessa laillista edustajaa ja sen määritelmää ei ole kuitenkaan kytketty direktiivin vaatimuksiin laillisen edustajan asettamisesta. Palveluntarjoajalla voisi artiklan nykymuotoilun perusteella ilmeisesti olla laillisia edustajia useammassakin maassa taikka vaihtoehtoisesti palveluntarjoaja voisi jättää nimeämättä laillisen edustajan. Keskusrikospoliisin näkemyksen mukaan 7 artiklan 1 kohdassa tulisi olla selvyyden vuoksi maininta siitä, että laillisen edustajan tulee olla sijoittautunut johonkin jäsenvaltioon, ja se tulee asettaa noudattaen direktiivissä (2017/0107 (COD)) asetettuja vaatimuksia.

Keskusrikospoliisi nostaa esiin seuraavat kysymykset liittyen 7 artiklan 2 kohtaan:

- mahdollistaako artiklan 2 kohta sen, että eurooppalainen esittämismääräys tai säilyttämismääräys 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 jäsenvaltiosta.

Eurooppalaisen esittämis- ja säilyttämismääräyksen vahvistava todistus (artikla 8)

Keskusrikospoliisi haluaa kiinnittää huomiota siihen, että säilyttämismääräykset tulisi 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-todistuksen toimeenpano (artikla 9)

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

Seuraamukset (artikla 13)

Kansallisessa lainsäädännössä ei ole tällä hetkellä olemassa sanktiointimekanismia, jos palveluntarjoaja kieltäytyy täytäntöön panemasta lainvalvontaviranomaisten tietopyyntö-

jä. 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 takavarikoimis- ja jäljentämiskieltotilanteesta.

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 katsoo, että kansalliseen lakiin mahdollisesti tehtävät muutokset tulisi tarkastella säädöshankkeen yhteydessä.

Täytäntöönpanoprosessi (Artikla 14)

Keskusrikospoliisi katsoo, että 14 artiklassa kuvatun täytäntööpanomenettelyn voisi osittain korvata määräysten antamisprosessiin luotava täytäntöönpanovaltion notifikaatiomenettely, jolloin täytäntöönpanovaltion viranomainen voisi arvioida tiedon luovuttamisen vaikutuksia suhteessa erioikeuksiin tai vapauksiin taikka kansalliseen turvallisuuteen tai puolustukseen jo heti ensivaiheessa sekä tarvittaessa näillä perusteilla kieltää esittämismääräyksen täytäntöönpanon.

Keskusrikospoliisi katsoo, että määräyksissä käytettävän kielen tulisi olla englanti.

Uudelleentarkastelumenettely ristiriitaisten velvoitteiden tapauksessa perusoikeuksien tai kolmannen maan olennaisten etujen perusteella (artikla 15) sekä uudelleentarkastusmenettely ristiriitaisten velvoitteiden tapauksessa muilla perusteilla (artikla 16)

Keskusrikospoliisin näkemyksen mukaan tällainen uudelleentarkastusmenettely ei vaikuta tehokkaalta menettelyltä ja siten artikloihin sisältyvistä määräajoista huolimatta sillä voisi olla prosessin kokonaisaikaa huomattavasti pidentävä vaikutus.

Keskusrikospoliisi kiinnittää huomiota siihen, ettei palveluntarjoajilla ole myöskään välttämättä riittävää osaamista arvioida artiklan 15 kohdan 1 mukaista konfliktitilannetta suhteessa kolmannen maan kansalaisten perusoikeuksiin sekä kolmannen maan kansalliseen turvallisuuteen ja puolustukseen. Myöskään tuomioistuimilla ei välttämättä ole sellaista osaamista arvioida esittämismääräyksen suhdetta kolmannen maan lainsäädäntöön ja mahdollisia konfliktitilanteita siten kuin 15 artiklan 3 - 5 kohdassa ja 16 artiklan 4-5 kohdassa on edellytetty.

Artiklojen 15 ja 16 nykyinen muotoilu sisältää myös riskin siitä, että palveluntarjoajat vetoaisivat tähän konfliktiperusteeseen ilman todellista uhkaa kolmannen maan etujen kanssa ja välttyisivät siten esittämismääräyksen täytäntöönpanolta.

Direktiiviehdotus yhtenäisistä säännöistä koskien laillisten edustajien nimittämistä sähköisen todistusaineiston keräämiseksi

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

Yleistä

Keskusrikospoliisi pitää kannatettavana direktiivin tavoitetta luoda säännöt, joilla asetuksen mukaiset Eurooppalainen esittämis- ja säilyttämismääräys voidaan osoittaa oikealle palveluntarjoajalle EU:n sisällä. Sääntely on tältä osin toistaiseksi perustunut jäsenvaltioiden sääntelyyn ja se on ollut kovin pirstaleista. Yhtenäinen sääntelypohja parantaisi myös palveluntarjoajien mahdollisuuksia täyttää tietopyyntöjä ja niihin liittyviä määräyksiä. Yhtenäistä sääntelypohjaa voidaan pitää lähtökohtaisesti kannatettavana.

Keskusrikospoliisi esittää seuraavia huomioita asetusehdotukseen sisällytettyjen artiklojen osalta:

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 eurooppalainen esittämis- ja/tai säilyttämismääräys osoitetaan?
- miten voidaan varmistua siitä, että palveluntarjoajalla on edustaja ainakin yhdessä jäsenvaltiossa direktiivin edellyttämällä tavalla? Kuka valvoo tätä?

Keskusrikospoliisin
apulaispäällikkö Björn Weckström

Rikostarkastaja Heidi Björk