23.10.2017
POL-2017-32185

Eduskunnan Lakivaliokunta
Viite: U56/2017vp

Euroopan parlamentin ja neuvoston direktiivi muihin maksuvälineisiin kuin käteisrahaan liittyvien petosten ja väärennysten torjunnasta ja neuvoston puitepäätöksen 2001/413/YOS korvaamisesta

1. Asia

Eduskunnan lakivaliokunta on pyytänyt Keskusrikospoliisin asiantuntijaa kuultavaksi sekä kirjallista asiantuntijalausuntoa asiassa Valtioneuvoston kirjelmä (U56/2017) Eduskunnalle ehdotuksesta Euroopan parlamentin direktiiviksi (maksuvälinepetokset). Pyynnön liitteenä on edellä mainittu U-kirjelmä.

2. Keskusrikospoliisin kanta

Yleistä
Euroopan komissio on 13.9.2017 tehnyt ehdotuksen Euroopan parlamentin ja neuvoston direktiiviksi muihin maksuvälineisiin kuin käteisrahaan liittyvien petosten ja väärennysten torjunnasta ja neuvoston puitepäätöksen 2001/413/YOS korvaamisesta (KOM (2017) 489 lopullinen). Direktiiviehdotuksessa laajennetaan maksuvälinepetosrikosten alaa koskemaan myös sellaisia tekoja, jotka eivät tällä hetkellä ole Suomen rikoslain mukaan rangaistavia ja määritellään rangaistukset ankarammiksi kuin voimassa olevassa rikoslaissa. Erityisesti huomioidaan uuden ja kehittyvän teknologian tarjoamat mahdollisuudet maksuvälinepetosten tekemisessä ja valmistelussa. Direktiivillä pyritään teknologianeutraaliin sääntelyyn.

Direktiiviehdotuksen säännökset ovat pääosin kannatettavia ja toteutuessaan ne tehostaisivat maksuvälinerikosten tutkintaa. Nyt voimassa oleva puitepäätös 2001/413/YOS ei vastaa enää nykypäivän todellisuutta. Tietotekniikan ja siihen liittyvä teknologian kehitys on ollut nopeaa ja tältä osin lainsäädäntö ei kaikilta osiltaan ole kehittynyt mukana. Maksuvälinerikollisuus on tulonlähde järjestäytyneelle rikollisuudelle ja sen avulla rahoitetaan muuta rikollista toimintaa. Muihin kuin käteismaksuihin liittyvät petokset haittaavat lisäksi laillista taloudellista toimintaa. Kaikki toimet maksupalveluiden luotettavuuden turvaamiseksi ja maksuvälipetosten torjumiseksi ovat siten kannatettavia.

Maksuvälineen määritelmä (2 artikla a, d ja e-kohta)
Direktiiviehdotuksen maksuvälineen määritelmä on puitepäätöksen vastaavaa määritelmää laajempi kattaen tietoverkossa tapahtuvat maksut ja digitaalisen vaihdannan välineet. Määritelmä on saman sisältöinen kuin 4. rahanpesun vastaisen

direktiivin muutosehdotuksessa. Maksuvälineen määritelmä kattaisi siten esitetyssä muodossaan myös virtuaalivaluutat. Tältä osin direktiiviehdotus sisältää merkittävän muutoksen Suomen voimassa olevaan lainsäädäntöön. Maksuväline määritellään nykyisellään rikoslain 37 luvun 12 §:ssä. Kyseinen määritelmä on yleinen ja täyttänee direktiiviehdotuksen 2 artiklassa olevan maksuvälineen määritelmän siltä osin kuin se koskee virallisia (keskuspankin liikkeelle laskemia) valuuttoja. Sen sijaan virtuaalivaluutat jäävät kyseisen rikoslakiin sisältyvän määritelmän ulkopuolelle.

Keskusrikospoliisin rahanpesun selvittelykeskuksessa on toteutettu projekti, jossa selvitettiin virtuaalivaluuttojen kytkeytymistä rikostutkintoihin Suomessa. Mainitussa projektissa tehtyjen havaintojen perusteella voidaan sanoa, että virtuaalivaluuttoihin liittyy sellaisia epävarmuustekijöitä, minkä vuoksi virtuaalivaluuttojen suojaamista direktiivissä ehdotetulla tavalla rikosoikeudellisesti on syytä pohtia tarkkaan. Epävarmuustekijät liittyvät ennen kaikkea siihen, että virtuaalivaluuttojen kytkeytyminen rikolliseen toimintaan on kasvanut huomattavasti viimeisten vuosien aikana. Virtuaalivaluutan voidaan sanoa tehdyn selvityksen perusteella liittyvän etenkin petos- ja huumausainerikollisuuteen. Muita epävarmuustekijöitä virtuaalivaluuttaan liittyen ovat sen vahva anonymiteetti, omistajaketjun selvittämisen haasteet, sääntelemätön ja määrittelemätön toimintaympäristö sekä valvonnan puute. Erilaisia virtuaalivaluuttoja on markkinoilla tällä hetkellä yli 1000 kappaletta. Edellä mainituista haasteista johtuen ei ole tiedossa, onko osa virtuaalivaluutoista perustettu pelkästään rikollista tarkoitusta varten. Näiden esitettyjen seikkojen valossa Keskusrikospoliisi haluaa nostaa esille kysymyksen siitä, onko virtuaalivaluutan käyttöä perusteltua suojata vastaavalla tavalla kuin virallista (keskuspankin liikkeelle laskemaa) valuuttaa koskevaa maksuliikennettä. Etenkin kun virtuaalivaluuttaan liittyvä petollinen menettely on Suomessa jo nykyisin laajasti rangaistavaa rikoslain yleisempien säännösten (mm. petos, väärennys, tietoverkkorikokset) nojalla.

Valmistelutyyppiset teot ja yritysteot (3-7 artikla)
Direktiiviehdotus säätää nykyistä laajemmin rangaistavaksi valmistelu- ja yritysteot. Tältä osin ehdotuksen mukaista laaja-alaista sääntelyä puoltaa se, että tietyn tyyppiset verkkorikokset edellyttävät tyypillisesti erityistä valmistelua ja on tärkeää saada tältä osin tekokokonaisuudet kattavasti rangaistavuuden piiriin. Tässä yhteydessä on toki huomattava, että rangaistavien tekojen tulee olla määriteltävissä kuitenkin riittävän täsmällisesti laillisuusperiaatteen mukaisesti.

Rangaistusasteikko (8 artikla)
Direktiiviehdotukseen sisältyvät rangaistusasteikkoja koskevat velvoitteet ovat pääosin ankarammat kuin rikoslaissa. Ongelmana voidaan nähdä yhden rikoslajin rangaistusasteikon ankaroittaminen suhteessa muihin rikoslaissa rangaistaviksi määriteltyihin tekoihin. Ehdotettu rangaistusasteikko (3-5 vuotta) poikkeaa myös Suomessa käytössä olevasta.

Tässä yhteydessä Keskusrikospoliisi haluaa huomauttaa, että Suomen rikoslaissa on kriminalisoitu vain perustekomuotoinen maksuvälinepetoksen valmistelu, josta säädetty ankarin rangaistus on yksi vuosi vankeutta. Törkeää maksuvälinepetoksen valmistelua ei ole kriminalisoitu lainkaan. Esimerkkinä lain ongelmallisuudesta voidaan kuvata seuraavanlainen tilanne: rikoksesta epäillyt on saatu verekseltään kiinni heidän irrottaessaan maksuautomaatista skimmauslaitetta. Laite on ollut kiinni automaatissa jo jonkin aikaa ja sitä ollaan irrottamassa, koska se on jo kopioinut automaatilla käytettyjen maksukorttien tiedot onnistuneesti ja lähettänyt ne ulkomaille. Saatua dataa ei ole kuitenkaan käytetty vielä mihinkään, joten rikosnimikkeeksi tulee maksuvälinepetoksen valmistelu. Päästyään vapaaksi

skimmaajat poistuvat Suomesta ja alkavat käyttää kopioitua korttidataa. Asiasta on nostettu Suomessa jo syyte maksuvälinepetoksen valmisteluna, jolloin kynnys jutun uudestaan avaamiselle ja tutkimiselle on suuri. Kopiointitapauksissa kyseeseen tulee lähes poikkeuksetta suuret rahasummat, jolloin teko onnistuessaan täyttäisi törkeän maksuvälinepetoksen tunnusmerkistön.

Lainkäyttövalta (11 artikla)
Direktiiviehdotuksen 11 artiklan mukaan jäsenvaltioiden tulisi ulottaa lainkäyttövaltansa omalla alueellaan tehtyihin rikoksiin, omien kansalaistensa tekemiin rikoksiin ja rikoksiin, jotka aiheuttavat niiden omalla alueella vahinkoa. Artiklan 2 kohdan mukaan oma alue tulee määritellä sekä henkilön että rikoksen tekemiseen käytetyn tietokoneen tai tietojärjestelmän sijainnin perusteella. Tässä yhteydessä on kuitenkin syytä huomioida, että vaikka direktiivin lainkäyttövaltaa koskevien säännösten perusteella voitaisiinkin ratkaista se, missä valtiossa tietty teko on tutkittava, niin esitutkintaviranomainen joutuu siitä huolimatta seuraavassa kappaleessa kuvattujen käytännön haasteiden eteen hankkiessaan todistusaineistoa maksuvälinerikosta koskevan esitutkinnan aikana. Nyt lausuttavana olevan direktiiviehdotuksen yhtenä keskeisenä eritystavoitteena oli poistaa operatiiviset esteet, jotka vaikeuttavat tutkintaa ja syytteeseenpanoa. Tältä osin tavoite jää osittain toteutumatta, sillä ehdotuksella ei luoda säännöksiä seuraavassa kappaleessa kuvatunkaltaisiin tilanteisiin liittyen.

Keskusrikospoliisi haluaa kiinnittää tässä yhteydessä huomiota niihin haasteisiin, joita liittyy sähköisen todistusaineiston saatavuuteen valtioiden rajat ylittävissä tilanteissa. On yleisesti tiedossa, että maksuvälinepetokset ovat usein valtioiden rajat ylittävää rikollisuutta. Esitutkinnan kannalta relevantti data (usein todistusaineistona käsitettävä tieto) saattaa sijaita täysin eri paikassa ja maantieteellisesti eri valtiossa kuin missä rikoksen tekoon tai valmisteluun käytettävät tietotekniset laitteet tai tietojärjestelmät sijaitsevat. Myös rikoksen seuraukset saattavat ilmetä muualla kuin tietoteknisten laitteitten sijaintimaassa. Lisäksi dataa säilytetään usein pilvipalvelimilla, mutta sillä ei välttämättä ole kiinteää säilytyspaikkaa. Palvelimia voi olla useissa eri maissa ja tiedot saatavat muuttaa sijaintiaan palvelimien välillä. Käsillä voi olla myös ns. loss of knowledge of location -tilanne, jolloin datan sijaintipaikasta ei ole mitään tietoa. Nämä uudenlaiseen toimintaympäristöön (verkkoavaruus) liittyvät erityispiirteet asettavat nykyisellään usein haasteita esitutkinnalle ja etenkin todistusaineiston hankinnalle. Tällöin esitutkinnan aikana joudutaan pohtimaan sitä, A) onko mahdollista takavarikoida pilvipalvelimella olevaa tietoa käyttäen epäillyn henkilön tietoteknistä laitetta, vaikka tieto itsessään sijaitsee jonkin toisen valtion alueella, vai B) onko tiedon saamiseksi turvauduttava oikeusapumenettelyyn (EU:n alueella eurooppalaiseen tutkintamääräykseen). Näitä kuvattuja ongelmia pyritään osittain ratkaisemaan tulevassa komission direktiiviehdotuksessa koskien rajat ylittävän sähköiseen todistusaineistoon pääsyn tehostamista (e-evidence -hanke). Tavoitteena on, että komissio antaa kyseisen ehdotuksen vuoden 2018 alussa.

Direktiiviehdotuksen vaikutukset
Rikosoikeudellisen vastuun laajentaminen ja rangaistusasteikon korottaminen vaikuttavat todennäköisesti esitutkintaviranomaisen tehtävien määrään lisäävästi. Myös tietotekniikan kehitys asettaa esitutkintaviranomaisille uusia vaatimuksia. Tämä tulee huomioida esitutkintaviranomaisten resursoinnissa.

Keskusrikospoliisi kannattaa direktiiviehdotusta edellä mainituin täsmennyksin.

POLIISI
KESKUSRIKOSPOLIISI

Tero Kurenmaa
Apulaispäällikkö

Heidi Björk
Rikostarkastaja