27.2.2024

Eduskunnan hallintovaliokunta
HaV@eduskunta.fi

Viite: Eduskunnan hallintovaliokunnan lausuntopyyntö 20.2.2024

Asia: E 58/2023 vp Valtioneuvoston selvitys: Suomen avaintavoitteet EU-vaalikaudelle 2024-2029 https://www.eduskunta.fi/pdf/E+58/2023

1 Lausuntopyyntö

Eduskunnan hallintovaliokunta on pyytänyt Keskusrikospoliisilta kirjallista lausuntoa ja kutsunut Keskusrikospoliisin edustajan asiantuntijakuulemiseen otsikon asiassa, Suomen avaintavoitteet EU:n strategiseen agendaan ja tulevan komission ohjelmaan vaikuttamiseksi. Asiasta on laadittu perusmuistio EU/41/2024-VNK-1.

2 Asiantuntijalausunto

Keskusrikospoliisi lähestyy lausunnossaan asiaa perusmuistion otsikoiden teemoista: puhdas ja digitaalinen siirtymä, kokonaisturvallisuus ja vahvempi Eurooppa, sekä muuttoliikkeiden hallinta. Keskusrikospoliisi lausuu näkemyksensä, niiden alle sijoittuvista osa-alueista. Keskusrikospoliisi toteaa yleisesti, että perusmuistiossa nostetut teemat ovat tärkeitä, keskeisiä ja hyvin kannatettavia.

Puhdas ja digitaalinen siirtymä

Kyberturvallisuus
Kyberturvallisuus linkittyy kyberrikollisuuteen, eli tietoverkkoja hyväksikäyttävään tai tietoverkkoavusteiseen rikollisuuteen, joka aiheuttaa merkittäviä taloudellisia haittoja valtioille ja organisaatioille. Kyberrikollisuus on vahvasti järjestäytynyttä, sekä valtioiden tai valtiollisten toimijoiden tekemää rikollisuutta. Se on myös rikoslajineutraalia, koska siihen sisältyy esimerkiksi kiristystä, vakoilua tai muita rikosnimikkeitä. Kyberrikollisuuden luonteesta johtuen, sen torjunnassa ja ennaltaehkäisemisessä korostuu kansainvälinen yhteistyö ja tiedonvaihto.

Uudet teknologiat päätyvät nopeasti myös rikollisien käyttöön. Tästä syystä on tärkeää varmistaa myös viranomaisten mahdollisuudet hyödyntää samoja teknologioita rikollisuuden torjuntaan ja tehokkaaseen tutkimiseen. Yhteistyötä viranomaisten ja palveluntarjoajien välillä on edelleen tiivistettävä. Hyvällä tilannekuvalla on keskeinen merkitys torjuntatoimien onnistumiselle ja turvallisuuden edistämiselle.

Datan määrän kasvaminen tulee lisäämään tarvetta esimerkiksi tekoälyavusteisien teknologioiden hyödyntämistä osana lainvalvonta- ja turvallisuusviranomaisien toimintaa. Keskusrikospoliisi toteaa, että em. asiaan panostamisella edistetään myös sitä, että kriittistä infrastruktuuria kyetään suojaamaan ja siihen kohdistuvia vaikuttamisyrityksiä havaitsemaan ja niihin reagoimaan.

Tietoverkoista on muodostunut uudenlainen toimintaympäristö sekä kansalaisille, viranomaisille että rikollisillekin. Yhteiskunnan digitalisoituminen ja siihen liittyvä teknologinen kehitys on siirtänyt rikosten tekemisen enenevässä määrin tietoverkkoihin.

Poliisilla lainvalvontaviranomaisena on keskeinen rooli kansallisessa kyberturvallisuudessa. Lainvalvontaviranomaisten näkökulmasta keskeistä on luoda ja ylläpitää kyvykkyyttä ennalta estää, paljastaa ja selvittää kansalaisiin ja yrityksiin kohdistuvia kyberuhkia, jotka usein täyttävät jonkin rikoksen tunnusmerkistön. Tehokkailla ennalta estävillä toimilla luodaan turvallista kybertoimintaympäristöä, mikä myös vähentää rikosoikeudellista puuttumisen tarvetta. Poliisin toimintamahdollisuudet ennalta estää ja paljastaa rikoksia tietoverkoissa ovat kuitenkin tällä hetkellä vajavaiset.

Poliisin tietoon tulee vain murto-osa kansalaisiin ja yrityksiin kohdistuvista tietoverkkorikoksista. Suomessa ei ole velvoitetta ilmoittaa törkeistä tietoverkkorikoksista poliisille, mikä vaikuttaa merkittävällä tavalla tietoverkkorikollisuutta koskevaan rikostilannekuvan täsmällisyyteen esim. kriittiseen infrastruktuuriin kytkeytyvien kyberrikosten osalta.

Kyberrikosten esitutkinta ja tekijöiden rikosvastuuseen saattaminen on hyvin haastavaa. Rikoskokonaisuudet edellyttävät useiden maiden saumatonta yhteistyötä ja samanaikaista toimivaltuuksien käyttämistä eri maissa. Esimerkiksi kiristyshaittaohjelmat voivat pahimmillaan lamaannuttaa yrityksen koko toiminnan ja aiheuttaa merkittäviä taloudellisia vahinkoja. Pahimmillaan tällainen rikos voi vaikuttaa myös yhteiskunnan toimintaan laajasti. Operatiivisella yhteistyöllä, sekä osaamisen jakamisella on saavutettavissa tuloksia erityisesti EU alueella (Europol, JCAT).

Poliisin kyky paljastaa verkossa tapahtuvaa laajamittaista laittomien aineiden, esineiden ja palveluiden kauppaa sekä pimeän verkon kauppapaikkoja tai saada haltuun oman toiminnan tai kansainvälisen lainvalvontayhteistyön kautta järjestäytyneen rikollisuuden toimijoiden välistä - erityisesti rajat ylittävään huumausainekauppaan liittyvää - salattua viestintää tai rikosten toteuttamiseen käytettyjen palvelinten sisältöä, on myös lisääntynyt. Tällaisen vakavaan rikollisuuteen liittyvän tiedon syvällisempi analysointi antaa poliisille myös mahdollisuuden muodostaa lähes ajantasaista tilannekuvaa järjestäytyneen rikollisuuden keskeisistä toimijoista ja heidän välisistä suhteistaan maan sisällä, sekä kansainvälisesti.

Kuvatunlaista tietoa voidaan hyödyntää yhteiskunnalle haitallisimpien rikollistoimijoiden torjuntatoimenpiteiden kohteeksi saattamiseen. Haasteeksi muodostuu se, että tietojen seulonnan yhteydessä voi paljastua jopa tuhansia tavanomaisia vanhoja Suomessa tai ulkomailla tapahtuneiksi epäiltyjä

huume- tai käyttörikoksia, joissa ei ole asianomistajaa. Poliisi on velvollinen käynnistämään esitutkinnan jokaisessa paljastuneessa tapauksessa, joka ylittää rikoksen syytä epäillä kynnyksen, tällä on vaikutusta koko rikosprosessiketjuun.

Keskusrikospoliisi pitää erittäin kannatettavana, että korkean kyberturvallisuuden ylläpitäminen ja siihen liittyvä kyberrikollisuuden torjuminen ovat Suomen avaintavoitteita. Lainvalvontaviranomaisten tulee voida tässä tarkoituksessa hyödyntää teknologista kehitystä.

Kokonaisturvallisuus ja vahvempi Eurooppa

Järjestäytynyt rikollisuus ja vakava rikollisuus
Järjestäytyneet rikollisryhmät (jr-ryhmät) vastaavat Suomessa suurelta osin huumausaineiden kaupasta, johon kytkeytyy myös ampuma-aserikollisuutta ja väkivaltaa. Viime aikoina erityisesti kokaiinin osuus on korostunut huumausainekaupassa. Muita merkittäviä järjestäytyneen rikollisuuden toiminta-alueita ovat mm. ihmiskauppa ja työperäinen hyväksikäyttö, talousrikollisuus ja omaisuusrikollisuus. Yritykset ovat rikollisille tärkeä työkalu sekä rikoksenteossa että laittomasti hankitun varallisuuden menestyksellisessä hallinnassa. Laillisten rakenteiden hyödyntäminen kasvattaa rikollista toimintaa, vahvistaa rikollisten vaikutusvaltaa yhteiskunnassa ja lisää korruption riskejä. Varsinkin kansainvälinen järjestäytynyt rikollisuus hyödyntää yhä enemmän myös tietoverkkoja rikollisessa toiminnassa, minkä myötä petosrikollisuus on noussut merkittäväksi tulonlähteeksi järjestäytyneelle rikollisuudelle. Ruotsin poliisin arvion mukaan petokset ovat ruotsalaiselle järjestäytyneelle rikollisuudelle jo huumausainekauppaa suurempi tulonlähde.

Suomessa on kymmenkunta katujengiksi luokiteltua ryhmää. Katujengeille on leimallista, että ryhmiin liittyvät henkilöt ovat pääasiassa Suomessa tai ulkomailla syntyneitä maahanmuuttajataustaisia nuoria miehiä. Ryhmien välillä on moninaisia rikolliseen toimintaan liittyviä verkostoja ja vuorovaikutussuhteita, joissa on kyse sekä yhteistyösuhteista että joiltakin osin ryhmien välisestä rikollisuudesta. Katujengien toiminta on muuttunut nopeasti ammattimaisemmaksi ja järjestäytyneemmäksi

Osana kansainvälistymistä jr-ryhmät pyrkivät soluttautumaan maahantulopisteisiin, infrastruktuuriin ja logistisiin ketjuihin. Järjestäytyneeseen rikollisuuteen kytkeytyvän väkivallan on syytä ennakoida yleistyvän ja käyvän aggressiivisemmaksi aseellisen varustautumisen, kiristyvän kilpailun sekä väkivallan käyttöön erityisen alttiiden toimijoiden määrän kasvun myötä. Rikollisen toimijakentän muutokset ja laajeneminen voivat näkyä rikollisten madaltuneena kynnyksenä kohdistaa myös poliisiin ja muihin viranomaisiin häirintää, väkivallan uhkaa tai muita vastatoimia.

Keskusrikospoliisi toteaa, että on erittäin tärkeää, että järjestäytynyttä rikollisuutta torjuntaan vahvasti, laajasti ja sen torjunnassa käytetään erilaisia lähestymiskulmia. Tämä edellyttää tehokasta kansallista ja kansainvälistä yhteistyötä.

Tiedonvaihto rikollisuuden torjumiseksi
Tiedonvaihdolle on esteitä ja lainsäädäntö tarvitsee selkeytystä, tulkinnanvaraisuus tulee saada mahdollisimman pieneksi. Kun tiedonvaihto hankaloituu tai ei ole mahdollista, kokonaiskäsitys esimerkiksi väkivallan uhasta sirpaloituu, ja tekojen ennalta estämisen mahdollisuudet vähenevät.

Tietojenvaihdon on oltava soveltajan kannalta selkeää, oikeus vaihtaa ja velvollisuus luovuttaa tietoa viranomaisten kesken niissä tilanteissa, kun rikos on vielä estettävissä, mutta konkretia rikoksen osalta on vähäistä. Interoperabilty ja tiedonvaihtodirektiivi tähtäävät oikeaan suuntaan tehostetun tiedonvaihdon osalta, mutta on tärkeä tehdä tiedonvaihtoon liittyvästä menettelyistä suoraviivaisia, tehokkaita ja nopeita ilman ylimääräistä byrokratiaa.

Erityisesti viranomaiskentän tietojenvaihtosäännösten tulkinnanvaraisuudesta ja puutteista johtuen esimerkiksi järjestäytyneen rikollisuuden hallinnollisen torjunta on keskittynyt viime vuosina poliisin lupahallintoon. Tietojen vaihtoa tulee kehittää ja laajentaa sekä kansallisesti että EU-tasolla.

Kyberturvallisuuteen ja tietoturvaloukkausten ja -uhkien selvittämiseen liittyvät viranomaisvastuut on Suomessa hajautettu eri viranomaisten kesken. Kyberturvallisuuden kannalta on tärkeää, että keskeiset viranomaiset voivat vaihtaa tietoja riittävässä laajuudessa. Tiedonvaihdon sujuvuus korostuu erityisesti vakavissa tietoturvaloukkaustilanteissa, joissa viranomaisten on toimittava nopeasti yhteisymmärryksessä vaikutusten poistamiseksi ja vahinkojen minimoimiseksi. Sisäministeriössä onkin käynnissä keskeinen poliisin tiedonvaihtosääntelyä koskeva lakihanke, jossa tarkastellaan erityisesti poliisilain tiedonvaihtoa koskevan sääntelyn ajantasaistamista. Voimassa oleva sääntely on osoittautunut tulkinnanvaraiseksi esimerkiksi oma-aloitteisen tietojen luovuttamisen osalta.

EU-tasoista ratkaisua kyberympäristön rajat ylittävyyden osalta on haettu E-evidence-asetuksella. Asetuksen soveltaminen alkaa vasta vuonna 2026, joten sääntelyn tuloksellisuutta ei ole mahdollista arvioida tässä vaiheessa. On kuitenkin nähtävissä, että erilaisilla palveluntarjoajilla on merkittävä rooli väärinkäytösten ja rikosten havaitsemisessa, mutta niiden vastuun osalta edessä vaikeasti ratkaistavia kysymyksiä liittyen yksityisyyden suojaan sähköisessä ympäristössä (esim. CSAM). Tiedonvaihdon ja tietoon pääsyn rajat ylittävien esteiden poistaminen myös 3. maiden suuntaan on tärkeää (EU-USA eEvidence neuvottelut), sillä merkittävä osa keskeisistä palveluntarjoajista sijaistee EU-alueen ulkopuolella.

Lisäksi samaan aikaan erilaiset uudet teknologiat haastavat lainvalvontaviranomaisten työtä (tekoäly, deep fakes, E2E salaus, OTT-palvelut). Tällä hetkellä poliisin salaisen tiedonhankinnan esteenä on pidettävä ensisijaisesti sitä, että ns. OTT-viestintäpalvelut (*Internetin päällä tarjottavat ns. Over the Top- palvelut, esimerkiksi WhatsApp)* toteutetaan pääasiassa päästä päähän salattuna (*end to end crypted*). Sisäisen turvallisuuden näkökulmasta olisi tärkeää, että myös ns. OTT-viestintäpalveluihin kohdistettaisiin vastaavia teknisiä ratkaisuja koskevia laatuvaatimuksia kuin perinteisiin teleoperaattoreihin.

Laatuvaatimuksissa tulisi edellyttää sitä, että kohdistettaessa telekuuntelua viestintäpalveluun (perinteinen televiestintä tai OTT-palvelu), tulee kaikki kuuntelun kohteena oleva materiaali toimittaa viranomaiselle selkokielisessä muodossa. EU-tasolla onkin jo aloitettu keskustelu lainvalvontaviranomaisten pääsystä päästä päähän salattuun tietoon (ns. *Going Dark – aloite ja HLEG-työ*). Aloite johtaa mahdollisesti säädöshankkeeseen. On tärkeää, että lainvalvontaviranomaisten pääsy tietoon turvataan myös tulevaisuudessa.

Rikollisuuden ennalta estäminen
Rikosten ennalta estäminen perustuu hyvään tilannekuvaan, jota kautta tunnistetaan ilmiöitä ja siten voidaan kohdentaa laajalla skaalalla erilaisia toimenpiteitä rikollisuuden torjumiseksi.

Suomessa hallinnollisen rikostorjunnan tavoitteeksi on asetettu erityisesti sen varmistaminen, ettei yksittäisillä viranomaispäätöksillä edistetä järjestäytyneen rikollisuuden toimintaedellytyksiä tai mahdollisteta rikollisen toiminnan jatkamista. Käytännössä tämä tarkoittaa sitä, ettei viranomaislupia myönnetä järjestäytyneeseen rikollisuuteen kytkeytyville henkilöille tai yhteisöille, mikäli arvioidaan, että viranomaisluvat parantaisivat järjestäytyneen rikollisuuden toimintaedellytyksiä. Toisaalta lupavalvontaa pyritään kohdistamaan tunnistettuihin järjestäytyneeseen rikollisuuteen kytkeytyviin toimijoihin.

Asetetun tavoitteen mukaisesti hallinnollisen rikostorjunnan keskiössä on poliisin ja muiden viranomaisten lupahallinto, mutta hallinnollisen rikostorjunnan viitekehyksessä on perusteltua pyrkiä tukemaan myös kuntien toimintaa esimerkiksi hankintojen ja maankäytön osalta siten, ettei kuntasektorin toimintakaan millään muotoa tue järjestäytynyttä rikollisuutta.

On havaittu myös, että myös järjestösektorin ja eräiden yritystoiminnan alojen osallistaminen hallinnollisen rikostorjunnan muodossa tapahtuvaan ennalta estävään työhön olisi perusteltua ja kustannustehokasta, esimerkkinä voidaan mainita finanssiala.

On tärkeää, että koko EU:n tasolla pystytään turvaamaan riittävät ja tehokkaat keinot ennalta estää ja selvittää valtion rajat ylittäviä tietoverkkorikoksia. Oleellista on selvittää verkkoympäristössä käytettävien toimivaltuuksien ajantasaistamista sekä pyrkiä löytämään ennakkoluulottomasti uusia keinoja tietoverkkorikosten ennalta ehkäisemiseen. Erityisesti tulisi tutkia mahdollisuutta passiivisten keinojen (nyt lähinnä tiedonhankinta, takavarikko) ohella vaikuttaa rikolliseen infraan rikosten laajenemisen ja rikosvahinkojen estämiseksi. Tällä hetkellä EU-tason yhteistyön ongelmana on erot maiden toimivaltuuksissa sekä mahdollisuuksissa puuttua rikolliseen toimintaan verkkoympäristössä.

Erinomaisen ennalta estävän toiminnan mallina on todettu mm. nuoriin kohdistuva Cybercrime-exit hanke, joka huomioi hyvin muuttuvaa ja muuttunutta toimintaympäristöä. Cybercrime Exit -hanke on ennalta estävää erityistoimintaa, jolla estetään nuorten vakavaa tietoverkkorikollisuutta ja siitä aiheutuvaa inhimillistä kärsimystä ja vahinkoa yksilön, organisaatioiden ja yhteiskunnan näkökulmasta. Toiminnan kohderyhmänä ovat noin 12-25

vuotiaat, jotka ovat tehneet tietoverkkorikoksen tai ovat vaarassa syyllistyä vakaviin tietoverkkorikoksiin. Tämän tyyppisiä hankkeita on edistettävä kansallisella ja EU tasolla.

Yhteistyötä palveluntarjoajien kanssa on tehostettava tietoverkkoavusteisen rikollisuuden torjumiseksi. Suomessa on yhteistyöllä aikaan satu hyviä tuloksia. Tietosuojasääntely ei saa estää tehokasta vakavan rikollisuuden torjuntaa.

Hybridiuhat ja kriittinen infra
Suomi korostaa tarvetta vahvistaa unionin kriisinsietokykyä eli kokonaisvaltaista ja laaja-alaista varautumista mahdollisiin tuleviin kriiseihin ja hybridiuhkiin. Keskusrikospoliisin näkemyksen mukaan EU:n tasolla tulee varmistaa (tarvittaessa luoda) mekanismi yhtenäisen ja ajantasaisen tilannekuvan tuottaminen hybridivaikuttamisesta ja hybridiuhkista kansallisten viranomaisten välillä (niin EU-tason intressit kuin kansalliset torjunta- ja tutkintavastuut huomioiden). Yhtenäisen tilannekuvan ja torjuntasuunnitelman luominen kansallisella tasolla on keskeistä hybridiuhkien tehokkaaksi torjumiseksi, sillä hybridiuhat ovat luonteeltaan tarkoituksellisen moniulotteisia ja niiden vaikutukset ja torjuntavastuut ulottuvat usean kansallisen viranomaisen vastuulle. Samalla uhkien monimuotoisuus, vastapuolen tavoitteiden kokonaisvaltainen hahmottaminen ja toimintamallien kehittyminen ovat seikkoja, joiden osalla EU-maiden välinen tiedonjako tukisi jokaisen valtion kansallisia pyrkimyksiä ennakoida ja torjua uhkia. Lisäksi erityisesti EU:hun kohdistuvien uhkien tehokas torjunta edellyttää jäsenmaiden havaintojen, kantojen ja torjuntatoimien koordinointia.

Poliisi on ensivasteen sisäisen turvallisuuden viranomainen normaalioloissa sekä myös tilanteissa, joissa ollaan vielä niin sanotulla harmaalla vyöhykkeellä (valmiuslakia ei ole otettu käyttöön, ei julistettu sotatilaa). Mikäli yhteiskuntaan kohdistuu esimerkiksi vihamielistä hybridi- tai kybervaikuttamista, joka poikkeuksetta täyttää jonkin rikoksen tunnusmerkistön, tai yleinen järjestys ja turvallisuus on uhattuna, Keskusrikospoliisilla on osana Suomen poliisia merkittävä rooli tämän kaltaisen rikollisuuden tunnistamisessa, torjumisessa ja tutkimisessa. Kriittiseen infrastruktuuriin kohdistuvan tiedustelun ja vaikuttamisen uhka on kohonnut sekä fyysisessä että kyberympäristössä. Muun muassa näihin haasteisiin vastaamiseksi poliisitoiminnalla ja rikostorjunnalla on sisäisen turvallisuuden osalta poliisilla keskeinen rooli. Yhteistyö ja tiedonvaihto ja toimintamallit tulee olla selkeitä sekä kansallisella että kansainvälisellä tasolla. Keskusrikospoliisin kokemuksen mukaan esitutkinta on eriomainen keino hybridi-ilmiötä ja sen osatekoja selvitettäessä.

Korruption torjunta
Ajankohtaisena asiana perusmuistiossa nostetaan esille mm. korruption ehkäiseminen. Suomessa poliisi on vuoden 2023 aikana laatinut korruptionvastaisen toimintapolitiikkansa, joka koostuu sitä koskevan päätöksen mukaisista linjauksista. Poliisihallitus laatii erillisen toimeenpano- ja viestintäsuunnitelman toimintapolitiikan täytäntöönpanon tukemiseksi.

Keskusrikospoliisi kannattaa kirjausta siitä, että unionin budjetista jaettavien varojen väärinkäytön ehkäisemiseen ja korruption torjuntaan kiinnitetään erityistä huomiota EU:ssa. Keskusrikospoliisi jatkaa tiivistä yhteistyötä Euroopan syyttäjänviraston (EPPO) kanssa EU:n varoihin kohdistuvien petosten ja muiden EU:n taloudellisia etuja vahingoittavien rikosten tutkimiseksi. Korruptio on merkittävä este taloudelliselle kehitykselle ja se pahentaa taloudellisen ja sosiaalisen epätasa-arvon seurauksia sekä heikentää myös ihmisoikeuksien toteutumista. Korruptio on riski myös ulko- ja turvallisuuspolitiikalle. Kannatettavaa on, että korruption ja korruptiorikosten torjunnassa pyritään tehokkuuteen kaikkialla EU:ssa, sillä nämä rikokset tai niiden vaikutukset ovat usein rajat ylittäviä. Keskusrikospoliisin korruptiotoiminto ylläpitää korruptiorikollisuuden valtakunnallista tilannekuvaa ja kehittää korruption tunnistamisen, paljastamisen ja tutkinnan menetelmiä. Keskusrikospoliisi osaltaan suorittaa korruptiorikosten paljastamiseen ja syyteharkintaan saattamiseen liittyvää rikostiedustelua ja -tutkintaa osana talousrikollisuuden ja harmaan talouden torjuntaa.

Muuttoliikkeiden hallinta

Välineellistetty maahantulo, laiton maahanmuutto ja Ihmissalakuljetus
Suomen muuttoliikkeen hallinnan avaintavoitteissa tuodaan ilmi, että tehokas ulkorajavalvonta on hallitun muuttoliikepolitiikan keskeinen osa-alue. Keskusrikospoliisi toteaa, että ulkorajojen EU-jäsenmaat ovat keskeisessä roolissa, kun pyritään torjumaan ulkorajoilta EU:hun kohdistuvaa järjestäytynyttä ihmissalakuljetusta sekä myös EU:n sisäistä, jolla ulkorajalla olevien valtioiden kautta laittomasti maahan saapuneita salakuljetetaan edelleen muihin EU-maihin. EU-alueelle suuntautuvaan ihmissalakuljetukseen järjestelmällinen puuttuminen edellyttää kansallisia toimia, jotka ovat EU-tasolla yhteneviä ja vaikuttavia. Kuten Europol on arvioissaan tuonut ilmi, EU:hun suuntautuvan ihmissalakuljetuksen muodostamat rikollisen toiminnan muodot tuottavat huomattavaa rikollista hyötyä. Koska Ihmissalakuljetus tapahtuu keskeisesti kolmansien maiden kautta, joissa toimivien, EU:n alueelle suuntautuvan ihmissalakuljetukseen järjestäytyneiden organisaatioiden henkilöitä on tällä hetkellä erittäin vaikeaa, jos ei mahdotonta saada teoistaan rikosvastuuseen, on tärkeää etsiä ja edistää EU-tason toimia. Rikosvastuun toteutumattomuus pitää yllä järjestäytyneiden ihmissalakuljetusorganisaatioiden toimintaa, ja on lähtömaiden tilanteiden kanssa yksi keskeinen osa-alue, joka vaikuttaa EU:hun suuntautuvaan laittomaan maahantuloon ja muuttoon.

Keskusrikospoliisi katsoo kansallisen ja sisäisen turvallisuuden kannalta keskeiseksi, että EU:n ulkorajavaltioilla, Suomi mukaan lukien, on tosiallisia ja tehokkaita keinoja estää kolmansien maiden kansalaisten laitonta maahan saapumista. EU-tasoisen ja kansallisen lainsäädännön mahdollistamat keinot torjua laajamittaista laittoman tai välineellistetyn maahanmuuton tilannetta ovat rajoittuneita, eikä nopealla käsittelyllä tai tehokkailla käännytyksillä pystytä vaikuttamaan kolmannen maan kansalaisia välineellistävän maan toimintaan. Riippuen toiminnan muodoista välineellistämisellä voi olla merkittäviä vaikutuksia kansalliseen ja sisäiseen turvallisuuteen. Keskusrikospoliisin näkemyksen mukaan EU-tasolla tulisi pohtia ja edistää yhteneviä, lainmukaisia ratkaisuita, jolla voidaan vaikuttaa kolmansien maiden EU:hun suuntaamaan vaikuttamiseen.

Keskusrikospoliisi pitää keskeisenä, että Suomen ja EU:n maiden viranomaisilla on riittävät lainsäädännön mahdollistamat keinot niin laittomasti kuin laillisesti maahan saapuvien joukosta tosiallisesti ja tehokkaasti tunnistaa kansallista tai sisäistä turvallisuutta mahdollisesti uhkaavia toimijoita. Ihmissalakuljetusorganisaatioiden ja sisäistä turvallisuutta mahdollisesti uhkaavien henkilöiden paljastaminen edellyttää usein laajoja rekisteritarkastuksia, tiedonhankintaa ja tiedonvälitystä. Tämä edellyttää mahdollisuutta riittävän matalalla kynnyksellä käsitellä ja verrata ristiin tietoja paitsi viranomaisten välillä myös salakuljetettujen uhrien tietoja, jotta voidaan selvittää kontaktitietoja keskeisten rikollisten toimijoiden ja toimintatapojen tunnistamiseksi. Myös biometristen tunnisteiden järjestelmällinen käyttöönotto EU:n ulkorajoilla on olennaista. Valvontaviranomaisten näkökulmasta kerättyjä tunnisteita tulee voida hyödyntää kolmannen maiden kansalaisten tunnistamiseksi vapaan liikkuvuuden alueella sekä rikosten tutkinnassa.

Avaintavoitteissa esille tuodusti Keskusrikospoliisi pitää tärkeänä, että palautuspolitiikkaa kehitetään ja vahvistetaan EU-tasolla. Tällä hetkellä Suomi ei pysty palauttamaan useisiin kolmansiin maihin käännyttämispäätöksen saaneita henkilöitä. Tosiallisten maasta poistamisen mahdollisuuksien puuttuminen saattaa vaarantaa Suomen kansallista tai sisäistä turvallisuutta, minkä vuoksi on tärkeää, että poliisi kykenee tosiallisesti poistamaan maasta lainvoimaisen käännytyspäätöksen saaneet kolmannen maan kansalaiset.

Poliisin näkökulmasta on keskeistä luoda selkeät ja yhdenmukaiset prosessit, sekä edistää tunnistamista mahdollistavia järjestelmällisiä ratkaisuja. Keskeistä on, että maahan tulevista tunnistetaan sisäistä turvallisuutta vaarantavat henkilöt mahdollisimman kattavasti aikaisessa vaiheessa.

Keskusrikospoliisin päällikkö Robin Lardot

Rikotarkastaja Arto Tuomela

Automaattisesti päivittyvä allekirjoitusfraasi. Älä poista tätä kenttää, jos allekirjoitat asiakirjan sähköisesti.

Jakelu Eduskunnan hallintovaliokunta, HaV@eduskunta.fi

Tiedoksi