Eduskunnan tulevaisuusvaliokunta

Keskusrikospoliisin lausunto

Asia

Eduskunnan tulevaisuusvaliokunta on pyytänyt Keskusrikospoliisilta lausuntoa asiassa O 9/2023 vp Tulevaisuusvaliokunnan selvityshankkeet 2023 – 2027 teemassa: Lasten, nuorten ja perheiden tulevaisuus.

Keskusrikospoliisille on esitetty kysymys: "Tulevaisuusvaliokunta tarkastelee tiettyjä tulevaisuuskysymyksiä edustajavetoisissa ohjausryhmissä. Lasten, nuorten ja perheiden hyvinvointiin liittyvä ohjausryhmä pyytää KRP:n kirjallista lausuntoa aiheesta ”internetin ja sosiaalisen median riskit ja vaarat lasten, nuorten ja perheiden kannalta”. Ohjausryhmää kiinnostaa myös, onko internetillä ja sosiaalisella medialla havaittavia positiivisia vaikutuksia tässä kontekstissa."

Yleistä toimintaympäristön muutoksista

Digitalisoituneessa maailmassa internet ja erilaisilla tietoverkkoalustoilla toimiminen kuuluvat kiinteästi lasten ja nuorten arkeen. Erilaiset viestintä- ja sosiaalisen median sovellukset sekä pelialustat ovat saaneet yhä nuorempia käyttäjiä. Lapset ja nuoret oppivat usein ymmärtämään tietoverkkoja ja niiden tarjoamia palveluita nopeasti, mutta koska tukea vastuullisen verkkokäyttäytymisen opetteluun ei välttämättä ole tarjolla, nuoret opettelevat palveluiden käyttöä usein itsenäisesti. Jopa 72 prosenttia lapsista ja nuorista on kohdannut jonkin tyyppistä häirintää tai uhkia verkkoalustoilla. Myös kiusaamista ja vihapuhetta esiintyy verkossa runsaasti, ja mahdollisuus toimia nimettömästi voi madaltaa kynnystä kiusaamiseen. Teknisiltä taidoiltaan lapset ja nuoret ovat erittäin osaavia, mutta heidän kypsyytensä ja ymmärryksensä eivät usein riitä verkkomaailman uhkien hahmottamiseen. Sosiaalisten medioiden ja verkon algoritmit myös hämärtävät kokemusta sovelluksien ja verkon sisällöistä, ja kokemukset näistä ovat subjektiivisia.

Digipelialustat ovat nykyään yhä selkeämpi osa tietoverkkoja siinä missä muutkin digitaaliset alustat. Vaikka digipelialustojen käyttö on nuorten keskuudessa yleistä, osa-alueeseen on kiinnitetty vähemmän huomiota kuin esimerkiksi sosiaalisen median alustoihin. Digipelialustoilla on paljon lapsia ja nuoria, jotka kohtaavat alustoilla rikollisen toimintakulttuurin normalisoimista. Kuten muillakin verkkoalustoilla, myös digipelialustoilla tapahtuu erilaista houkuttelua rikollisiin toimiin. Lapsia ja nuoria voidaan pelialustoilla

rekrytoida esimerkiksi ääriliikkeiden toimintaan, verkkorikosten tekemiseen tai hyväksikäyttötarkoituksiin.

Syvä verkko (*deep web)* muodostuu julkisen eli avoimen internetin ulkopuolelle jäävästä internetin osasta, jonka arvioidaan muodostavan suuren osan kaikista verkkosivustoista. Pimeä verkko (*dark web*) on osa syvää verkkoa. Kyse on joukosta piilotettuja internetsivustoja tai -palveluita, jotka ovat käytettävissä vain tähän tarkoitukseen tehdyllä verkkoselaimella. Pimeässä verkossa tapahtuvaan rikolliseen toimintaan liittyvät olennaisesti erilaiset kauppapaikat ja keskustelufoorumit, jotka toimivat rikollisia palveluita tai hyödykkeitä tarjoavien toimijoiden ja asiakkaiden kohtauspaikkoina sekä rikollisten yhteisöinä. Tyypillisesti keskeisillä kauppapaikoilla myydään huumausaineita. Pimeässä verkossa on myös mahdollista ostaa ja myydä hakkerointityökaluja ja varastettuja henkilötietoja, pankkitunnuksia tai laittomia ohjelmistoja, joita voidaan hyödyntää muissa rikoksissa.

Lapsiin kohdistuva seksuaalirikollisuus verkossa

Lapsiin kohdistuvien seksuaalirikosten määrä verkossa on kasvanut viime vuosina. Kasvu selittyy osittain ilmoitusaktiivisuuden lisääntymisellä, mutta on todennäköistä, että rikoksia myös tapahtuu aiempaa enemmän, sillä verkon välityksellä uhrien tavoittaminen on aiempaa helpompaa. Viime vuosina on paljastunut poikkeuksellisen suuria rikoskokonaisuuksia, joissa yhdellä rikoksentekijällä on ollut uhreina useita satoja lapsia. Rikoksentekijät käyttävät alustoja, jotka koetaan helppokäyttöiseksi ja jotka antavat tunteen anonymiteetista.

Lapsiin kohdistuvia yleisimpiä seksuaalirikoksia ovat tapaukset, joissa lapsia lähestytään sosiaalisen median välityksellä. Tyypillisesti tekijä keskustelee lapsen kanssa seksuaalissisältöisiä asioita, lähettää kuvan sukupuolielimestään, pyrkii saamaan lapsen lähettämään alastonkuvia ja -videoita tai pyrkii tapaamaan lapsen fyysisesti aikeinaan kohdistaa häneen seksuaalisia tekoja. Uhrit ovat eri ikäisiä, sillä käytännössä riittää, että lapsella on pääsy internetiin ja sosiaaliseen mediaan. Tekijät ovat tyypillisesti aikuisia, mutta toisinaan he voivat olla myös itse nuoria.

Toinen tyypillinen ilmiö ovat rikokset, jotka liittyvät lasta seksuaalisesti esittävään kuvamateriaaliin. Kuvamateriaalia kerätään ja hallitaan, jaetaan toisille vastineetta tai vaihdetaan uuteen kuvamateriaaliin sekä myydään. Poliisin tietoon tulleissa tapauksissa tällaisissa teoissa tekijät ovat pääosin aikuisia, mutta ilmiötä esiintyy myös nuorten ja lasten keskuudessa. Kuvamateriaalia voidaan jakaa esimerkiksi sosiaalisen median viestominaisuuksilla tai pimeän verkon foorumeilla.

Viime vuosina on myös yleistynyt ilmiö, jossa alastonkuvilla kiristetään rahaa lapsilta (ns. *sextortion*). Tapauksissa tekijä esiintyy yleensä nuorena naisena ja pyrkii saamaan lapsen, yleensä 13–17 -vuotiaan pojan, lähettämään itsestään alastonkuvia. Tämän jälkeen tekijä uhkaa levittää kuvia esimerkiksi lapsen sosiaalisen median yhteyksille tai lähipiirille, ellei lapsi maksa tekijälle. Tekijät ovat pääsääntöisesti aikuisia ja toimivat ulkomailta käsin.

Yksi jo osittain realisoitunut uhkakuva on tekoälyn käyttö lapsiin kohdistuvissa seksuaalirikoksissa. Tekoälyä voidaan hyödyntää lähes kaikissa lapsiin kohdistuvissa seksuaalirikoksissa muun muassa helpottamaan rikoksen toteuttamista tai peittelemään tekijän henkilöllisyyttä. Olisikin tärkeää, että myös viranomaiset pystyvät hyödyntämään tekoälyä työssään entistä laajemmin.

Alaikäisiin liittyvä hyväksikäyttö ja taloudellinen rikollisuus

Alaikäisten seksuaalista ja taloudellista hyväksikäyttöä on havaittu erilaisilla verkkosivustoilla ja alustoilla (esim. OnlyFans, ns. Sugar Dating -palvelut). Nuoret voivat myydä näissä seksuaalisia palveluja ja/tai seksuaalista kuvamateriaalia. Materiaalin jakamiseen voi liittyä myös rahan tai seksuaalisten palvelujen antamiseen liittyvää kiristämistä ja uhkailua ulkopuolisten taholta. Osassa tapauksia rikosten uhrit ovat olleet erityisen haavoittuvassa asemassa, kodin ulkopuolelle sijoitettuja lastensuojelun asiakkaita. Poliisin tietoon on tullut myös joitakin tapauksia, joissa on viitteitä parituksesta. Tällöin täysi-ikäinen henkilö on järjestellyt alaikäiselle kontakteja erilaisten sivustojen tai alustojen kautta. Poliisin tiedossa on myös joitakin yksittäisiä tapauksia, joihin liittyy alaikäisten tyttöjen pakkoavioliittoon saattamista tai kunniaan liittyvää väkivaltaa verkon välityksellä.

Erilaisten tietoverkon avulla tehtyjen huijausten eli tietoverkkoavusteisten petosten nousu yhdeksi keskeisimmistä yksityishenkilöihin kohdistuvista rikoksista on vahvistunut viime vuosien aikana myös Suomessa. Tietoverkkoavusteisissa petoksissa (esim. erilaiset huijaukset, tietojen kalastelu) alaikäisiä uhreja on poliisin havaintojen mukaan vielä vähän. Rikollisten keskeinen motiivi on tähän asti ollut asianomistajan tilivarojen tai pankkitunnusten anastaminen eikä lapsilla pääsääntöisesti ole aktiivisia pankkitunnuksia tai tilivaroja, joita merkittävässä määrin menettää. Varallisuuden lisäksi vaarana on luovuttaa rikolliselle taholle kirjautumistunnuksia, joilla on mahdollista saada haltuunsa erityisen arkoja henkilötietoja kuten terveystietoja.

Taloudellisiin väärinkäytöksiin liittyen poliisin tietoon tulee säännöllisesti tapauksia, joissa alaikäisten tai heidän pankkitilinsä kytkeytyy epäilyttävään rahaliikenteeseen. Rikolliset voivat rekrytoida alaikäisiä sosiaalisen median kanavilla tai pimeän verkon kauppapaikoilla vastaanottamaan ja välittämään rikollisia varoja tai nostamaan käteistä rikollisille. Alaikäiset ovat myös itse osallistuneet pankin palveluhäiriöitä hyödyntävään rikolliseen toimintaan muun muassa mobiilimaksamista hyödyntäen.

Yhtenä huolenaiheena on maksuhäiriöasiakkaiden ottamat pikavipit alaikäisten lasten nimiin, minkä laki mahdollistaa. Pikavippiyhtiöitä ei toistaiseksi kosketa velvollisuus kieltäytyä lainan myöntämisestä, vaikka olisikin ilmeistä, että laina on tosiasiassa otettu luottotiedottoman ja/tai päihdeongelmaisen vanhemman toimesta. Lainsäädännössä velkaantumiselle ei ole myöskään asetettu mitään ikärajaa, eikä mikään estä pikaluottoja myöntäviä yhtiöitä myöntämästä kyseisiä korkean koron luottoja. Seuraukset voivat olla alaikäiselle lapselle kohtalokkaita.

Verkkoympäristö nuorten väkivaltarikollisuuden näkökulmasta

Nuorisorikollisuuteen liittyen sosiaalisen median merkitystä on korostettu väkivallan ihannoinnin ja normalisoinnin näkökulmasta. Sosiaalisen median palveluissa ja pikaviestimissä on havaittu nuorten toisiinsa kohdistamaa halventavaa ja väkivaltaista materiaalia, kuten nöyryytys- ja väkivaltavideoita, joiden avulla pyritään saavuttamaan vertaisten keskuudessa mainetta ja ihailua. Usein videoissa useampi henkilö nöyryyttää uhria ja kohdistaa tähän väkivaltaa. Joissakin tapauksissa uhrilta on lisäksi ryöstetty omaisuutta, kuten vaatteita tai elektroniikkaa. Rikosten lisääntyvä esiintyminen sosiaalisessa mediassa voi saada aikaan harhan niiden normalisoitumisesta. Materiaalia on helppo jakaa uudelleen eri muodoissa ja erilaisissa palveluissa. Väkivalta- ja vihamateriaalia levittävät toimijat keksivät jatkuvasti keinoja alustojen moderoinnin ja/tai sisältöä kontrolloivien algoritmien kiertämiseen.

Nuorten välillä tapahtuneiden ryöstöjen ja pahoinpitelyiden lisäksi myös muunlaista väkivaltamateriaalia jaetaan verkossa. Suomessakin esiintyvässä niin sanotussa "Pedohunt"-ilmiössä nuoret luovat sosiaaliseen mediaan alaikäisten nimissä valeprofiileja, tai käyttävät olemassa olevia profiileja sopiakseen treffejä pääasiassa täysi-ikäisten miesten kanssa. Tarkoituksena on videoida kohtaaminen verkossa jaettavaksi ja mahdollisesti pahoinpidellä väitetty pedofiili. Tapaamistilanteista kuvataan usein verkossa jaettavaksi tarkoitettua väkivaltamateriaalia, jonka tavoitteena on pedofiiliksi väitetyn henkilön häpäisy. Ilmiöön liittyy myös ryöstöjä ja kiristämistä. Alaikäiset törmäävät ilmiöön ja vastaaviin tekoihin erilaisilla alustoilla (esim. TikTok ja YouTube). Tällaisen materiaalin toistuva näkeminen saattaa inspiroida kokeilemaan itse vastaavanlaista toimintaa. Vaikka tapaamisiin kutsutaan pääsääntöisesti vanhempia miehiä, myös alaikäisiä on joutunut tekaistujen raiskaussyytösten ja pahoinpitelyn uhriksi. Niin sanottuun pedofiilinmetsästykseen osallistuvat nuoret saattavat myös itse joutua tapaamisissa väkivallan kohteiksi.

Verkkoympäristöä hyödynnetään myös erilaisten laittomien asioiden ja aineiden kaupassa, etenkin huumausainekaupassa. Suomalainen verkkohuumekauppa on toiminut yli kymmenen vuotta. Pimeän verkon tai pikaviestimien avulla etsitään myös henkilöitä osallisiksi ja avuksi rikolliseen toimintaan. Alle 15-vuotiaita on poliisin havaintojen mukaan ollut mukana rikoksissa esimerkiksi postipalveluiden tuottajina huumausainemyyjille. Tämän lisäksi nuoret pääsevät itsekin käsiksi eri alustojen laajaan huumausainekauppaan. Laittomien aineiden helppo saatavuus saattaa vähentää kynnystä ostaa verkon alustoilta ja samalla kynnys toimia rikollisessa ympäristössä laskee. Poliisin tietoon on tullut myös tapauksia, jossa esimerkiksi lääke-, huumausaineiden tai sähkötupakan (vape) myynnistä on sovittu etukäteen verkossa. Kauppatilanteet voivat johtaa väkivaltaisiin ryöstöihin, joissa joko tilanteeseen ostamaan tulleelta henkilöltä ryöstetään rahat tai vastaavasti myymään tulleelta osapuolelta viedään myytävä tuote sitä maksamatta.

Internetiä ja sosiaalista mediaa käytetään myös koulu-uhkauksien esittämiseen. Poliisin tietojen perusteella kaikista uhkatapauksista noin 40 prosenttia on verkkovälitteisesti kirjallisesti tai audiovisuaalisesti eri alustoilla esitettyjä. Vaikka koulu-uhkausten määrä tyypillisesti lisääntyy julkisuudessa olleiden kouluiskujen jälkeen, uhkaukset ovat kuitenkin

osittain kouluiskuista erillinen ilmiö. Uhkauksiin liittyy monen ikäisiä henkilöitä, mutta useimmiten uhkaaja on 14-vuotias. Noin 90 prosentissa tapauksia uhkauksen esittäjän henkilöllisyys kyetään selvittämään poliisissa. Myös erinäiset somehaasteet ja painostus-/yllytystoimet ovat aiheuttaneet suuren määrän koulu-uhkauksia. Tällöin sosiaalisessa mediassa (esim. TikTok, Jodel) levinnyt haaste koulu-uhkauksen esittämiseen omassa koulussa on aikaansaanut lyhyessä ajassa suuren määrän samankaltaisia uhkatapauksia eri puolilla Suomea. Alaikäiset ovat saattaneet myös esittää koulu-uhkauksia saadakseen poliisit saapumaan koululle ja videoidakseen tilanteesta paljon näkyvyyttä tuovaa materiaalia omiin sosiaalisen median kanaviinsa.

Alaikäisten radikalisoituminen ja rekrytointi verkossa

Niin Suomessa kuin muissakin länsimaissa havaitaan yhä nuorempien henkilöiden radikalisoitumista ja jopa ekstremistiseen ja/tai terroristiseen toimintaan osallistumista. Eri ekstremististen ryhmittymien ja ideologioiden piirissä (erityisesti äärioikeistolainen konkteksti ja radikaali-islamismi) on havaittu alaikäisiä radikalisoituneita, verkkoyhteisöissä aktiivisia henkilöitä. Mikäli alaikäiset osallistuvat verkostoissaan iskujen suunnitteluun tai niiden toteuttamiseen, alaikäisisten toiminnasta voi aiheutua vaaraa sisäiselle turvallisuudelle. Osassa ekstremistisiä ja terroristisia ryhmittymiä tavoitteena on yhteiskunnan romahduttamisen kiihdyttäminen, johon yhtenä keinona nähdään nuoren sukupolven tarkoituksellinen ”pilaaminen” mm. itsemurhaan yllyttämällä tai seksuaalisella hyväksikäytöllä. Tällaisessa toiminnassa yhteydenpito alaikäisiin tapahtuu myös verkon välityksellä.

Internetin rooli alaikäisten radikalisoitumisprosesseissa on merkittävä: se mahdollistaa nopeasti etenevän ns. itseradikalisoitumisen, propagandamateriaalille altistamisen ja alaikäisiin kohdistetut aktiiviset radikalisointi- ja rekrytointitoimet. Lisäksi alaikäiset saattavat myös tiedostamattaan jakaa verkossa eteenpäin ekstremististä materiaalia. Verkosta on saatavilla lisäksi erilaisia manuaaleja esimerkiksi 3D-tulostettavien aseiden rakentamiseen ja räjähteiden valmistamiseen, vaikka mahdollisuudet rakentaa näiden perusteella todellisuudessa toimivia aseita tai räjähteitä on vähintään epävarmaa.

Verkossa alaikäisten keskuudessa on havaittu ekstremististen ja terroristisen toimijoiden syvää ihailua. Lisäksi verkko mahdollistaa esimerkiksi yhteydenottoyritykset ekstremistisessä toiminnassa jo mukana oleville henkilöille, jopa tuomituille terroristeille. Visuaalisesti vahvan verkkoympäristön myötä ekstremistinen ja terroristinen sisältö on nuorten saatavilla houkuttelevassa ja helpossa muodossa ilman, että henkilön tulisi lukea esimerkiksi laajoja ideologisia kirjoituksia.

Alaikäiset näyttäytyvät useille toimijoille mahdollisina rekrytoinnin ja propagoinnin kohteina. Verkkoympäristöissä rekrytoijien strategiana on usein ensin houkutella lapsi tai nuori tutustumaan humoristisen materiaalin avulla ekstremistisen ideologian keskiössä oleviin teemoihin. Tällöin esimerkiksi ideologian mukaiseen "viholliskuvaan" lukeutuvia ihmisryhmiä saatetaan huumorin ja meemien varjolla epäinhimillistää samalla, kun luodaan hiljalleen kuvaa siitä, kuinka tähän "viholliskuvaan" lukeutuvat ihmiset ovat syyllisiä kaikkiin keskeisiin vääryydenkokemuksiin. Materiaalin esittelyn jälkeen saatetaan siirtyä

keskustelemaan aiheista chatteihin, jonka jälkeen henkilöitä johdatellaan yhä radikaalimman materiaalin pariin suljetummille keskustelualustoille ja -foorumeille.

Alaikäiset ovat rekrytoijille usein tarkoituksellinen kohde, sillä elämänkokemuksen puute, kehittymässä oleva identiteetti, toisinaan helposti mustavalkoisia näkemyksiä omaksuva mieli sekä kriittisten ajattelutaitojen puute luovat alttiutta, jota rekrytoijat ja propagandamateriaalin levittäjät osaavat käyttää hyväkseen. Lisääntyvä tekoälyn ja erilaisten syväväärennösten (*deep fake*) käyttö propagandamateriaalin tuottamisessa ja erehdyttämiseen pyrkivän viestinnän toteuttamisessa voi haastaa alaikäisten lisäksi myös muita ilmiön tunnistamiseen harjaantumattomia, kuten lasten ja nuorten vanhempia.

Propagandamateriaalille altistumisen sekä aktiivisten rekrytointipyrkimysten estämisessä keskeistä olisi paitsi alaikäisten ja heidän parissaan työskentelevien ammattilaisten tietoisuuden ja ymmärryksen lisääminen, myös esimerkiksi aiempaa laajempi ja tiukempi sosiaalisen median alustojen moderointi ja sääntely. Haitallista materiaalia tietoverkoissa voidaan jaotella karkeasti terroristiseen/ekstremistiseen materiaaliin ja muuhun haitalliseen materiaaliin. Nuoret käyttävät yhä enemmän sosiaalisen median palveluita ja altistuvat väistämättä edellä mainituille materiaaleille jossain vaiheessa. EU-alueella toimivia sisältöpalveluntarjoajia velvoittaa TCO-lainsäädäntö, joka edellyttää palveluntarjoajia muun muassa ilmoittamaan viranomaisille terroristisesta henkeä ja terveyttä uhkaavasta materiaalista sekä omatoimisesti kehittämään palvelun kykyä torjua kyseistä sisältöä.

Lapset ja nuoret tietoverkkosidonnaisten rikosten tekijöinä

Tietoverkkoihin ja tietojärjestelmiin kohdistuviin rikoksiin eli tietoverkkosidonnaisiin rikoksiin syyllistyvät henkilöt ovat keskimäärin hyvin nuoria. Kansainvälisesti tarkasteltuna ensikertalainen tällaisessa rikoksessa oli vuonna 2021 keskimäärin 19-vuotias, kun vuonna 2024 keskimääräinen ikä oli 15 vuotta. Eurooppalaisten tutkimusten mukaan lähes 70 prosenttia nuorista raportoi syyllistyneensä jonkinlaiseen haitantekoon verkossa, ja lähes puolet nuorista kertoi syyllistyneensä tietoverkkosidonnaiseen tekoon vuoden aikana. Tietoverkkosidonnaisiin rikollisiin tekoihin syyllistyy vuosittain alle rikosvastuuikäisiä lapsia, myös Suomessa.

Tyypillisiä nuorten henkilöiden tekemiä tietoverkkosidonnaisia rikoksia ovat esimerkiksi erilaiset tietomurrot, palvelunestohyökkäykset ja viestintäsalaisuuden loukkaukset. Nuoret, jotka ovat usein teknologisesti taitavampia kuin aikuiset, ovat eturintamassa uusien teknologioiden hyödyntämisessä myös rikolliseen toimintaan. Tällaisia rikostyyppejä ovat esimerkiksi tekoälyn ja automatisoitujen työkalujen avulla suoritetut laajamittaiset palvelunesto- ja muut verkkohyökkäykset.

Pimeästä verkosta on saatavilla hakkerointityökaluja, ohjeita ja muita työkaluja myös verkkorikosten tekemiseen. Pimeän verkon lisäksi ohjeita löytyy myös yleisten hakukoneiden kautta sekä erilaisilta keskustelufoorumeilta ja kanavilta (esim. Discord tai Youtube). Myös automatisoidut rikoksentekovälineet eli niin sanotut *crime-as-a-service* -pal-

velut ovat verkossa helposti lasten ja nuorten löydettävissä. Palveluiden helppo saatavuus ja käytettävyys voi madaltaa kynnystä tietoverkkorikoksen tekemiselle, eikä työkaluja välttämättä tunnisteta laittomiksi. Automatisoituja työkaluja käyttäessään nuori ei välttämättä voi ennakoida hyökkäyksen todellista laajuutta ja seurauksia.

Poliisin havaintojen perusteella nuoret eivät yleensä ole tienneet toiminnan laittomuudesta tai hahmottaneet rikosten seurauksia. Myös nuorten huoltajat ovat yllättyneitä lastensa rikollisesta toiminnasta tietoverkoissa. Vaikka osa nuorten tekemistä tietoverkkorikoksista on lievempiä, nuoret syyllistyvät myös vakaviin, mittavaa vahinkoa aiheuttaviin tekoihin. Vakavampi rikoskierre alkaa usein lievemmillä teoilla, ja myöhemmässä vaiheessa esiin nousee tyypillisesti myös taloudellisia motiiveja. Tietämättömyys, rikoksiin houkuttelu, ja verkkorikollisen kulttuurin ihannointi vaikuttavat osaltaan nuorten tietoverkkorikollisuuteen ilmiönä.

Verkkoympäristö katujengien näkökulmasta

Sosiaalisella medialla ja internetillä on keskeinen merkitys myös katujengirikollisuudessa. Poliisin määritelmän mukaan katujengillä tarkoitetaan useasta henkilöstä muodostuvaa pysyväisluonteista ryhmää, johon kuuluvat henkilöt harjoittavat yhdessä ja toistuvasti rikollista toimintaa, jolla on olennaisia vaikutuksia erityisesti yleisten paikkojen järjestykseen ja turvallisuuteen. Useat katujengit niin Suomessa kuin ulkomailla käyttävät sosiaalista mediaa edistääkseen mainettaan ja osoittaakseen identiteettiään. Tämä tapahtuu esimerkiksi julkaisemalla video-, kuva- tai äänisisältöä, jossa esitellään jengitunnuksia, -symboliikkaa tai rikoksella saatua hyötyä. On myös tavanomaista, että jengien väliset konfliktit syntyvät, eskaloituvat tai niitä ylläpidetään virtuaalisesti. Sosiaalisella medialla tarkoitetaan tässä laajasti erilaisia avoimia ja suljetumpia alustoja (esim. Snapchat, TikTok, Instagram, Telegram, Youtube) sekä laajemmassa merkityksessä myös musiikin suoratoistopalveluita (esim. Spotify).

Eri tutkimuksissa ja raporteissa on tarkasteltu sosiaalisen median ja internetin roolia jengirikollisuuteen liittyvässä rekrytoinnissa. Yleisen tulkinnan mukaan rekrytointi nimenomaan sosiaalisessa mediassa ei yleensä ole aktiivista, vaan pikemminkin voimistaa olemassa olevia, sosiaalisiin suhteisiin perustuvia rekrytointikanavia. Poliisin havaintojen perusteella on todennäköistä, että Suomessa ystävyys- ja sukulaisuussuhteilla sekä paikallisilla instituutioilla kuten kouluilla on toistaiseksi merkittävämpi rooli rekrytointiprosesseissa. Sosiaalisella medialla voi kuitenkin olla keskeinen rooli jengin tunnettavuuden edistämisessä ja valmiiksi jengirikollisuudelle myönteisten yksilöiden verkostoitumisessa.

Viime vuosina useissa Euroopan maissa, erityisesti Ruotsissa, on yleistynyt ilmiö, jossa rikollistoimijat rekrytoivat nuoria tekemään rikoksia jengin lukuun. Vastineeksi nuori voi saada rahaa, muita palkkioita tai mahdollisuuden edetä jengin hierarkiassa. Tyypillisesti rekrytointi tapahtuu sosiaalisessa mediassa tai pikaviestiryhmissä ja toimeksiannon yksityiskohtaisempi ohjeistus suljetummilla alustoilla. Toimeksiantaja tai yllyttäjä toimii usein nimimerkin varjossa ja ohjeistaa toimintaa vähän kerrallaan. Joissakin tapauksissa rekrytoitavan nuoren pitää toimittaa itsestään ja sukulaisistaan tietoja, kuten kuva kasvoista

tai henkilöllisyystodistuksesta. Näitä tietoja voidaan käyttää kiristämiseen tai uhkailuun, jos nuori ei toimi toimeksiantajan ohjeistamalla tavalla; kun nuori on ottanut toimeksiannon vastaan, on siitä vaikeaa enää perääntyä.

Suomessa vastaavasta toimintatavasta ei toistaiseksi ole laajoja havaintoja, joskin rikolliseen toimintaan rekrytointia sinällään tapahtuu erilaisilla sosiaalisen median alustoilla sekä pikaviestinryhmissä. Ei kuitenkaan ole selviä viitteitä siitä, että rekrytointi kohdistuisi erityisesti voimakkaasti juuri nuoriin.

Katujengit hyödyntävät internetiä myös suoraan rikollisessa toiminnassa. Erilaisia palveluja ja alustoja hyödynnetään laajasti ainakin erilaisissa tietoverkkoavusteisissa petoksissa, huumausaineiden kaupassa sekä rahanpesussa. Yleisesti voidaan todeta, että samoin kuin huumausainekauppa yleensä, myös katujengien huumausainekauppa tapahtuu yleisimmillä kaupankäyntialustoilla kuten paikallisissa pikaviestinryhmissä. Myös rikoksiin liittyvä viestintä tapahtuu usein pikaviestimillä, joista osassa tietoliikenne on salattu päätelaitteiden välillä.

Myönteisiä näkökulmia

Riskien ja uhkien lisäksi on tärkeä huomioida, että verkkoalustat, kuten digipelialustat ja erilaiset sosiaalisen median kanavat voivat tarjota nuorelle myös tärkeitä positiivisia kokemuksia. Verkkoalustoilta löytyy vertaiskontakteja, joita ei välttämättä reaalimaailman lähiympäristöstä löydy. Esimerkiksi digipelialustoilla yhteisöllisyys on voimakasta ja voi kasvaa yli tietyn alustan ympäristön ja luoda nuorelle tärkeitä ystävyyssuhteita. Esimerkiksi nuori voi löytää vertaistukea kokemiinsa haasteisiin verkon kautta mistä päin maailmaa tahansa, ja kokea yhteisöllisyyden ja yhteenkuulumisen kokemuksia, jotka ovat keskeisiä teemoja esimerkiksi ekstremismin vastaisessa työssä.

Lisäksi se, että alaikäiset viettävät paljon aikaa verkossa on toisaalta johtanut myös siihen, että alustoilla on tehty paljon niiden omiin moderointiprosesseihin nojaavia ilmiantoja esimerkiksi vihaan tai väkivaltaan lietsovasta materiaalista. Viettäessään paljon aikaa eri alustoilla lapset ja nuoret tekevät huolta aiheuttavasta sisällöstä myös poliisille suunnattuja nettivinkkejä. Nämä ilmoitukset ovat toisinaan johtaneet jopa suunnitteluvaiheessa olevien väkivallantekojen estämiseen.

Viranomaisten ja järjestötoimijoiden aktiivinen läsnäolo eri verkkoalustoilla esimerkiksi pelipoliisitoiminnan tai auttavan chatin muodossa mahdollistaa alaikäisille myös matalan kynnyksen yhteydenoton em. toimijoihin. Pelipoliisitoiminta tuo poliisin lasten ja nuorten lähelle ja lisää vuorovaikutusta sekä positiivisia kokemuksia verkossa toimiville nuorille. Verkossa helposti saatavilla oleva luotettavien toimijoiden tarjoama tuki mahdollistaa avun ja ohjauksen saamisen myös niissä tilanteissa, joissa kynnys kasvokkain tapahtuvalle kontaktin ottamiselle on syystä tai toisesta korkea. Lapset ovat myös usein valmiimpia kertomaan esimerkiksi kokemistaan seksuaalirikoksista sosiaalisessa mediassa toimiville kolmannen sektorin auttaville tahoille, kuin suoraan poliisille tai vanhemmilleen.

Verkkoalustat ovat myös tärkeä informaation lähde nuorille, mikä voi vahvistaa tiedonhakutaitoja, joista on hyötyä tulevaisuudessa. Vaikka objektiivisen tiedon hakeminen verkosta voi olla haastavaa, tiedonhakutaitojen kehittyessä myös luotettavan tiedon löytäminen helpottuu. Verkosta saatavilla hyödyllistä ja erityisesti nuorille suunnattua tietoa rikollisuuteen ja omiin oikeuksiin liittyen.

Robin Lardot, Keskusrikospoliisin päällikkö, Poliisineuvos

Laura Heiskanen, Tutkija

Asiakirja on sähköisesti allekirjoitettu asianhallintajärjestelmässä. Poliisi 18.03.2025 klo 10:31. Allekirjoituksen oikeellisuuden voi todentaa kirjaamosta.

Liitteet

Kirjoita tähän

Jakelu

Eduskunnan tulevaisuusvaliokunta

Tiedoksi

Poliisihallitus