Veeti Katainen

Kyberrikollisuuden torjunnan oikeudelliset perusteet

Poliisin toimivaltuudet oikeudellisessa tarkastelussa

Johtamisen akateeminen yksikkö
Julkisoikeus
Hallintotieteiden kandidaatti

Vaasa 2025

VAASAN YLIOPISTO
Johtamisen akateeminen yksikkö
Tekijä: Veeti Katainen
Tutkielman nimi: Kyberrikollisuuden torjunnan oikeudelliset perusteet: Poliisin toimivaltuudet oikeudellisessa tarkastelussa
Tutkinto: Hallintotieteiden kandidaatti
Koulutusohjelma: Hallintotieteiden kandidaattiohjelma
Opintosuunta: Julkisoikeus
Työn ohjaaja: Laura Perttola
Valmistumisvuosi: 2025 **Sivumäärä:** 34

TIIVISTELMÄ:
Teknologian kehitys ja globalisaatio ovat mahdollistaneet valtavasti uusia asioita ja helpottaneet monen arkea. Teknologian kehityksen ja globalisaation hyötyjä käyttävät hyväkseen myös rikolliset. Teknologian kehitys mahdollistaa yhä tehokkaamman ja laajamittaisemman kyberrikollisuuden, jota viranomaiset pyrkivät torjumaan. Teknologian kehittymisen myötä uudenlainen rikollisuus aiheuttaa sen, että lainsäätäjän on päivitettävä lainsäädäntöä vastaamaan näitä uusia rikoksia. Esimerkiksi tietomurron ja tietoliikenteen häirinnän kriminalisointi on osoittanut sen, että uusia rikosnimikkeitä tulee lisää ja niiden kriminalisointi on tärkeää, jotta poliisin toimivaltuuksia voidaan kohdistaa näiden rikosten ennalta estämiseen, paljastamiseen, selvittämiseen ja syyteharkintaan saattamiseen. Tutkielman lähtökohdat ovat kohtalaisen haastavat, koska oikeustieteellistä tutkimusta kyberrikollisuudesta on niukasti. Lisäksi käsitteiden selkeän määritelmän puuttuminen tuo tutkielmaan haasteita. Nämä haasteet ovat kuitenkin minimoitu tutkielmassa sillä, että kyberrikollisuuden käsitteet on tutkielmassa määritelty ja ne ovat pidetty tarkoituksenmukaisesti melko laaja-alaisena.

Tämä lainopillinen tutkielma tarkastelee poliisin toimivaltuuksia etenkin kyberrikollisuuden torjunnan näkökulmasta. Tutkielmassa perehdytään tarkemmin kyberrikollisuuteen, kyberrikoksiin ja etenkin poliisin toimivaltuuksiin. Tutkielma keskittyy tarkastelemaan poliisin toimivaltuuksia lainsäädännön näkökulmasta. Tutkielma pyrkii vastaamaan siihen, mitä toimivaltuuksia poliisilla on torjua kyberrikollisuutta oikeuden näkökulmasta ja mitä haasteita tähän saattaa liittyä. Erityisesti lainsäädännön kehitys ja sen ajantasaisuus ovat tarkastelun kohteena. Tutkielmassa pyritään selvittämään, millä poliisin toimivaltuuksilla kyberrikollisuutta torjutaan, ja onko lainsäädäntö riittävää. Poliisilain (872/2011) 5 luvun salaiset tiedonhankinta keinot ovat merkittävässä roolissa etenkin kyberrikosten ennalta estämisen kannalta. Tutkielmassa tarkastellaan voimassa olevaa lainsäädäntöä etenkin lainsäädännön, lainvalmisteluaineiston, oikeuskäytännön ja oikeuskirjallisuuden kautta. Tarkastelun avulla tutkielmassa saadaan selville lainsäädännön toimivuus ja mahdolliset haasteet, josta esimerkkinä on korkeimman oikeuden ratkaisu 2022:23.

Tutkielman tuloksena voidaan todeta, että poliisin toimivaltuuksista säätävät lait ovat nykyään suhteellisen hyvin ajan tasalla, mutta lainsäädännön reagointi teknologian kehitykseen on usein liian hidasta. Lainsäädännön uudistukset tulevat hieman jäljessä lainsäädännöllisten puutteiden havaitsemisen jälkeen, etenkin kyberrikollisuuden torjunnan osalta. Esimerkkinä tästä on poliisihallituksen työryhmän loppuraportin havainnot televalvonnan ja telekuuntelun puutteista vuonna 2015. Näihin puutteisiin saatiin muutos vasta vuonna 2022. Toinen suuri haaste kyberrikollisuuden torjunnassa on ilmiön valtionrajat ylittävä luonne. Tämä luo ongelmia kyberrikollisuuden torjuntaan siinä, että poliisin toimivaltuudet eivät ylety valtionrajojen ulkopuolelle.

AVAINSANAT: kyberrikollisuus, kyberrikokset, tietoverkkorikos, poliisi, toimivaltuudet

Sisällys

1 Johdanto 5

2 Kyberrikollisuus oikeudellisena käsitteenä 8

2.1 Kyberrikokset 10

2.1.1 Viestintäsalaisuuden loukkaus 10

2.1.2 Tietoliikenteen häirintä 11

2.1.3 Tietojärjestelmän häirintä 12

2.1.4 Tietomurto 13

2.1.5 Suojauksen purkujärjestelmärikos 14

3 Poliisin toimivaltuuksien oikeudellinen perusta ja haasteet kyberrikollisuuden torjunnassa 15

3.1 Rikostorjunta 16

3.2 Tiedonhankintakeinot kyberrikostorjunnassa 17

3.2.1 Telekuuntelu ja televalvonta 18

3.2.2 Tekninen laitetarkkailu 20

3.2.3 Peitetoiminta 21

3.3 Pakkokeinot 22

3.3.1 Takavarikointi 23

3.3.2 Kotietsintä 24

3.3.3 Laite-etsintä 25

3.3.4 Salaiset pakkokeinot 26

4 Johtopäätökset 28

Lähteet 31

Virallislähteet 33

Oikeustapaukset 34

Ylimpien laillisuusvalvojien ratkaisut 34

Lyhenteet

DDoS	Distributed Denial-of-Service
ETS	European Treaty Series
EU	Euroopan Unioni
HE	Hallituksen esitys eduskunnalle
HO	Hovioikeus
IP	Internet Protocol
ISF	Internal Security Fund
KKO	Korkein oikeus
LaVM	Lakivaliokunnan mietintö
OKV	Oikeuskanslerinvirasto
PeVL	Perustuslakivaliokunnan lausunto
PKL	Pakkokeinolaki (806/2011)
PL	Suomen perustuslaki (731/1999)
PolL	Poliisilaki (872/2011)
RL	Rikoslaki (39/1889)
SopS	Suomen säädöskokoelman sopimussarja
UNODC	United Nations Office on Drugs and Crime
vp	Valtiopäivät
VPN	Virtual Private Network

1 Johdanto

Kyberrikollisuus on lisääntynyt valtavasti viime vuosina[1]. Tämän takia myös viranomaisten on oltava valmiina laajalti erilaisten rikosten torjuntaan. Poliisilain (872/2011) 1 luvun 1 §:n mukaan *poliisin tehtävänä on oikeus- ja yhteiskuntajärjestyksen turvaaminen, kansallisen turvallisuuden suojaaminen, yleisen järjestyksen ja turvallisuuden ylläpitäminen sekä rikosten ennalta estäminen, paljastaminen, selvittäminen ja syyteharkintaan saattaminen*. Tämän takia onkin ajankohtaista pohtia, millä oikeudellisilla perusteilla poliisit pystyvät suorittamaan lain määräämiä tehtäviään. Tässä tutkielmassa tarkastelen poliisin toimivaltuuksia ja sitä, kuinka poliisit pystyvät torjumaan alati muuttuvaa ja teknologisesti kehittynyttä rikollisuutta.

Kyberrikollisuutta pohdittaessa monet saattavat ajatella kansalaisten perusoikeuksien rikkomista sekä pohtia rajaa yksityisyyden suojan ja turvallisuuden välillä. Suomen perustuslain (731/1999) 2 luvun 10 §:n kohta takaa ihmisille perusoikeutena yksityiselämän suojan. Samaisessa perustuslain kohdassa kuitenkin mainitaan sen rajoituksista tiettyjen rikosten selvittämiseksi ja yhteiskunnan turvallisuuden takaamiseksi, mikä on välttämätöntä poliisien toimivaltuuksien kannalta. Kyberrikollisuus voi toisaalta myös saada aikaan pelkoa kansalaisissa, sillä se voi aiheuttaa mittavia taloudellisia vahinkoja, se ei katso valtionrajoja ja se voi aiheuttaa uhreille valtavia henkisiä ongelmia[2]. Kyberrikollisuus onkin ollut mediassa huomattavasti esillä viime vuosina ja aiheuttanut julkista keskustelua, jonka takia onkin mielestäni aiheellista tarkastella asiaa oikeudellisesta näkökulmasta.

Tutkiessani oikeustieteellistä tutkimusta kyberrikollisuudesta huomasin sen olevan vähäistä. Aaltonen ja muut ilmentävät kyberrikollisuuden tutkimusta hyvin siten, että oikeustieteellistä tutkimusta aiheesta on vielä nykyäänkin melko vähän ja että kyberrikollisuuteen liittyvä tutkimus on hyvin pitkälti liittynyt tekniseen puoleen[3]. Eli tutkimus on

---

[1] Aaltonen ja muut, 2021, s. 966; Sisäministeriö, 2017, s. 5.
[2] Murphy, 2024, s. 2.
[3] Aaltonen ja muut, 2021, s. 967; Nevalainen, 2019a, s. 131.

keskittynyt poikkitieteellisesti enemmänkin tekniikkaan, eikä niinkään oikeustieteelliseen näkökulmaan. Toisaalta rikosoikeudesta ja poliisin toimivaltuuksista on paljon tutkimusta ja ennakkotapauksia, joista saa hyvän käsityksen lain nykytilasta ja mahdollisista haasteista.

Tutkielmani tavoitteena on vastata seuraaviin tutkimuskysymyksiin:

1. Mitä toimivaltuuksia poliisilla on torjua kyberrikollisuutta oikeuden näkökulmasta?
2. Mitä oikeudellisia haasteita poliisi kohtaa kyberrikollisuuden torjunnassa?

Tutkielmassa syvennyn tarkemmin viranomaisten toimivaltuuksiin lain, lainvalmisteluaineiston, oikeuskirjallisuuden ja oikeuskäytännön avulla. Tarkastelen tutkielmassa eri kyberrikoksia, niiden oikeudellisia määritelmiä ja mitä haasteita ne tuovat. Tutkielmassani pyrin myös selvittämään, mitä haasteita kyberympäristö tuo rikostorjuntaan ja miten se vaikuttaa oikeuden nykytilaan. Tavoitteena on tarkastella lainsäädäntöä etenkin siitä näkökulmasta, että pystyykö poliisi toteuttamaan lainsäädännöllisiä tehtäviään. Lisäksi tarkastelussa on lainsäädännön ajantasaisuus ja se, että onko poliisilla laista tulevat oikeudet toteuttaa riittäviä menetelmiä rikostentorjuntaan.

Tutkimusmenetelmä on oikeusdogmaattinen eli lainopillinen. Lainopin tarkoituksena on voimassa olevan oikeuden tulkinta ja systematisointi[4]. Tutkimus sijoittuu enimmäkseen virkamies- ja rikosoikeuteen, mutta sillä on yhtymäkohtia myös EU-oikeuteen ja osittain tietosuojaan. Keskeisimpiä säädöksiä ovatkin mm. poliisilaki (872/2011), rikoslaki (39/1889), pakkokeinolaki (806/2011) ja Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus (ETS 185, SopS 59–60/2007). Poliisin toimivaltuuksista säädetään laissa ja etenkin poliisilaissa, pakkokeinolaissa ja esitutkintalaissa.

[4] Määttä, 2016, s. 148.

Tutkielma alkaa johdantoluvulla, jonka tarkoituksena on avata hieman, miksi juuri kyberrikollisuus on merkittävä näkökulma aiheeseen. Tämä jälkeen tarkastelen kyberrikollisuutta ja kyberrikoksia oikeudellisesta näkökulmasta. Määrittelyiden jälkeen onkin tarkoitus syventyä poliisin toimivaltuuksiin ja siihen minkälaisia ns. ”työkaluja” poliisilla on kyberrikollisuutta vastaan. Tarkastelen siis tarkemmin poliisin toimivaltuuksia sekä sitä, millaisia oikeudellisia haasteita kyberrikokset tuovat. Tavoitteena on selvittää, millä lainsäädännöstä tulevilla toimivaltuuksilla poliisit pystyvät torjumaan kyberrikollisuutta, ja pystyykö poliisi torjumaan näillä toimivaltuuksilla teknologisesti kehittynyttä kyberrikollisuutta. Lopuksi vastaan tutkielman tutkimuskysymyksiin vastaan johtopäätökset luvussa ja pohdin sitä, että onko lainsäädäntö ajan tasalla.

2 Kyberrikollisuus oikeudellisena käsitteenä

Kyberrikollisuus tai kyberrikos ei itsessään ole vakiintunut käsite ja se onkin esim. kyberrikollisuuden tutkimisen yksi haasteista[5]. Kyberrikollisuus ei ole myöskään oikeustieteellisesti vakiintunut termi, vaan se on enemmänkin kriminologian tutkimuksessa käytetty yleistermi[6]. Tämä on haastava lähtökohta oikeustieteelliselle tarkastelulle, koska käsitteen varsin laaja ja avoin merkitys ei ole selvästi oikeustieteellisesti määritelty.

Kyber- etuliite käsitteenä sen nykymerkityksessä on tullut käyttöön englannin kielen sanasta ”cyber”, jota käytettiin etenkin Yhdysvalloissa kriittisen infrastruktuurin suojaamiseen liittyvässä kontekstissa ”cyberthreats” -käsitteenä[7]. Kyberrikollisuuden ja kyberrikosten käsite voidaankin täten ajatella tulevan englannin kielen sanasta ”cybercrime”, joka ei sekään ole kuitenkaan vakiintunut käsite edes englannin kielellä[8]. Huomioitavaa on, että se voi tarkoittaa englanniksi sekä kyberrikosta että kyberrikollisuutta riippuen asiayhteydestä[9]. Toisaalta suomalaisessa kirjallisuudessa käytetään myös termiä ”tietoverkkorikollisuus” ja esimerkiksi kääntäessä ”cybercrime” -sanaa englannin kielestä suomen kielelle on osaltaan käytetty käännöstä ”tietoverkkorikollisuus” tai ”tietoverkkorikos”[10]. Oikeustieteessä on usein käytetty termejä tietotekniikkarikos ja tietoverkkorikos[11]. Kyberrikollisuuden käsite kuitenkin korostaa enemmän koko kyberavaruutta, joka sen takia kuvaa nykyhetkeä paremmin kuin aiemmat muut termit[12].

Kyberrikollisuuden tarkastelu oikeudellisena käsitteenä on hyvin haastavaa, koska kyberrikollisuus voidaan nähdä tarkoittavan eri konteksteissa hieman eri asiaa. Esimerkiksi ky-

---

[5] Yar ja Steinmez, 2023, s. 9.
[6] Kaakinen ja Näsi, 2021, s. 124.
[7] Sisäministeriö, 2017, s. 11.
[8] Murphy, 2024, s. 2.
[9] Nevalainen, 2019a, s. 132.
[10] Esim. Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence on suomeksi käännettynä Tietoverkkorikollisuutta koskevan yleissopimuksen toinen lisäpöytäkirja tiiviimmästä yhteistyöstä ja sähköisen todistusaineiston luovuttamisesta.
[11] Lappi-Seppälä ja muut, 2022, s. 1283.
[12] Riekkinen, 2019, s. 161.

berturvallisuuden käsite kuvaa paremmin koko sähköistä toimintaympäristöä kuin tietoturvallisuus, jolla viitataan enemmänkin dataan[13]. Kyberrikokset voidaan jakaa karkeasti kahteen eri kategoriaan. Ne voidaan jakaa *kyberriippuvaisiksi rikoksiksi* (cyber-dependent crime) ja *kybertoimintaympäristön mahdollistamiksi rikoksiksi* (cyber-enabled crime)[14]. Tämä jakolinja on erinomainen jakamaan kyberrikokset etenkin oikeudellisesta tarkastelusta, koska kyberriippuvaiset rikokset ovat näkemäni mukaan enemmänkin rikoslain 38 luvun mukaisia tieto- ja viestintärikoksia. Kyberympäristön mahdollistamat rikokset voivat käytännössä olla minkälainen rikos tahansa, jossa on käytetty verkkoympäristöä. Nykyään etenkin petoksiin käytetään merkittävällä tavalla kyberympäristöä, koska verkkoympäristö mahdollistaa mm. tehokkaasti tietojen laittoman kalastelun. On kuitenkin huomioitava, että kyberrikollisuudesta ei ole yhtä tarkkaa ja luotettavaa määritelmää[15].

Tässä tutkielmassa kyberrikoksilla tarkoitetaan laaja-alaisesti kaikkia niitä lailla kiellettyjä tekoja, joissa on käytetty tai hyödynnetty merkittävästi kyberympäristöä. Kyberrikoksia ja kyberrikollisuutta on tässä tutkielmassa tarkoituksenmukaista pitää laaja-alaisena, jotta tutkielmassa pystytään mahdollisimman laajasti tarkastelemaan kyberrikollisuuden torjuntaa, poliisin toimivaltuuksia ja niiden oikeudellisia piirteitä. Pelkästään kyberrikollisuuden käsitteen haastava määrittely ja rajan veto oikeudellisesti kuvaa jo kyberrikostorjunnan haasteita. On myös tarkoituksenmukaista pitää kyberrikollisuuden käsitettä laaja-alaisena, jotta saadaan ajantasainen ja realistinen käsitys niistä haasteista, joita teknologian kehitys tuo. Teknologian kehittyessä rikolliset pyrkivät löytämään uudesta teknologiasta hyötyjä rikolliseen toimintaan[16]. Kyberrikoksen määrittäminen onkin usein riippuvainen siitä, kuinka sitä käytetään[17]. Tämän takia tutkielmassa kyberrikollisuudella tarkoitetaan edellä mainittuja asioita.

---

[13] Sisäministeriö, 2017, s 11.
[14] Cross ja Hirrle, 2021, s. 10; Nevalainen, 2019a, s. 131; Murphy, 2024, s. 2.
[15] UNODC, 2013, s. 14; Nevalainen, 2019a, s. 135.
[16] Edwards, 2020, s. 24.
[17] UNODC, 2013, s. xvii.

2.1 Kyberrikokset

Kyberrikoksia tarkastellessa oikeuden näkökulmasta on tarpeellista tarkastella osaa rikoslain 38 luvun eri pykälien rikosnimikkeitä ja niiden mahdollisia tunnuspiirteitä, jotta etenkin kyberriippuvaiset rikokset tulevat selkeämmiksi. Pidän selkeimpinä kyberriippuvaisina rikoksina mm. viestintäsalaisuuden loukkausta, tietoliikenteen häirintää, tietojärjestelmän häirintää, tietomurtoa ja suojauksen purkujärjestelmärikosta[18]. Kybertoimintaympäristön mahdollistamat rikokset voivat käytännössä olla kuitenkin minkä tahansa rikosnimikkeen alla, jonka takia näiden tarkempi läpikäynti ei ole realistista tässä tutkielmassa.

2.1.1 Viestintäsalaisuuden loukkaus

Viestintäsalaisuuden loukkauksella tarkoitetaan seuraavaa: *joka oikeudettomasti 1) avaa toiselle osoitetun kirjeen tai muun suljetun viestin taikka suojauksen murtaen hankkii tiedon sähköisesti tai muulla vastaavalla teknisellä keinolla tallennetusta, ulkopuoliselta suojausta viestistä taikka 2) hankkii tiedon televerkossa tai tietojärjestelmässä välitettävänä olevan puhelun, sähkeen, tekstin-, kuvan- tai datasiirron taikka muun vastaavan televiestin sisällöstä taikka tällaisen viestin lähettämisestä tai vastaanottamisesta* (RL 38:3). Tapauksessa rangaistuksena on sakko tai vankeutta enintään kahdeksi vuodeksi.

Viestintäsalaisuuden loukkauksesta on esitetty hallituksen esityksessä (232/2014) siten, että viestintäsalaisuuden loukkaus kattaisi myös tietojärjestelmän sisäisen luottamuksellisen datan siirron, joka vastaisi Euroopan parlamentin ja neuvoston asettamaa tietoverkkorikosdirektiiviä, ja että enimmäisrangaistus korotettaisiin kahteen vuoteen vankeutta[19]. On siis havaittu, että viestintäsalaisuuden loukkauksen riskit ovat kasvaneet, minkä takia on haluttu myös säätää ankarampia rangaistuksia viestintäsalaisuuden loukkauksesta.

---

[18] Tutkimuksessa on usein käsitelty koko rikoslain 38 lukua, mutta tässä tutkimuksessa pidän realistisena käsitellä ainoastaan näitä rikosnimikkeitä.
[19] HE 232/2014 vp, s. 4.

Viestintäsalaisuuden loukkaus on merkittävä säännös kyberrikollisuuden näkökulmasta. Kyberrikoksissa usein kohteena on data[20], jonka varastamisen kriminalisointi on tärkeää kyberrikosten torjunnan kannalta. Toisaalta dataa ja viestejä saatetaan käyttää myös niin sanotuissa lunnashyökkäyksissä, jollainen esimerkiksi Vastaamo-tietomurto oli alun perin[21]. Viestintäsalaisuuden loukkauksella saatua tietoa voidaan kyberrikollisuudessa käyttää mm. kiristyksen välineenä.

2.1.2 Tietoliikenteen häirintä

Tietoliikenteen häirinnästä säädetään rikoslain 38 luvun 5 § kohdassa siten, että se kriminalisoi mm. posti-, tele- ja radioviestinnän tahallisen häiritsemisen. Tietoliikenteen häirinnästä on myös pykälät törkeästä häirinnästä ja lievästä häirinnästä (RL 38:6–7). Rangaistus tietoliikenteen häirinnästä on sakko tai vankeutta enintään kaksi vuotta, mutta törkeästä tietoliikenteen häirinnästä rangaistus on enintään viisi vuotta vankeutta. Huomioitavaa on myös se, että yritys on rangaistavaa (RL 38:5–7).

Tietoliikenteen häirintä voi tapahtua teknisin keinoin, mutta se voi pitää sisällään myös esim. postilaatikoiden rikkomisen[22]. Tietoliikenteen häirintä kattaa siis laajasti eri tekotapoja, jotka pitävät sisällään myös teknisin keinoin tehtyjä tietoliikenteen häirintää. Bottiverkkojen käyttö verkkohyökkäykseen on esimerkiksi yksi törkeän muodon tekotavoista[23].

Kyberrikollisuuden näkökulmasta tietoliikenteen häirintä on nimenomaan usein ns. bottiverkon käyttöä palvelunestohyökkäykseen siten, että se häiritsee tietoliikennettä. Toisaalta palvelunestohyökkäyksiä tietoliikenteen häirinnän tarkoituksessa käyttävät usein

[20] Yar ja Steinmez, 2023, s. 56.
[21] Looi ja muut, 2024, s. 108.
[22] Lappi-Seppälä ja muut, 2022, s. 1298.
[23] Lappi-Seppälä ja muut, 2022, s. 1300.

valtiolliset toimijat tai kyberrikollisjärjestöt, jotka tekevät kyberoperaatioita ns. ostopalveluna valtiollisille toimijoille[24]. Tietoliikenteen häirinnässä ei usein ole suoraan rikoshyötyä, muuta kuin ns. mainetta. Paitsi, jos taustalla on nimenomaan valtiollisen toimijan rahoitus[25].

2.1.3 Tietojärjestelmän häirintä

Tietojärjestelmien häirintä on kyberrikollisuuden kannalta merkittävää, koska se pitää sisällään ns. DDoS-hyökkäykset (Distributed Denial of Service) eli palvelunestohyökkäykset[26]. Palvelunestohyökkäykset tarkoittavat käytännössä halutun tietojärjestelmän tahallista ylikuormittamista, kuten verkkosivuja tai sähköpostipalvelimia[27]. Tietojärjestelmän häirinnässä kyse on järjestelmän toiminnan häirinnästä, kun taas tietoliikenteen häirinnässä kyse on tietoliikenteen ja viestinnän häirinnästä[28]. Näitä on kuitenkin tarkoituksenmukaista usein käsitellä yhdessä, koska tietojärjestelmiin kohdistuva häirintä usein täyttää myös tietoliikenteen häirinnän tunnusmerkit[29].

Tietojärjestelmän häirinnästä säädetään rikoslain 38 luvun 6 §:ssä. Säädös tekee tietojärjestelmän käytön estämisestä tai sen vakavasta häirinnästä laittoman (RL 38:6). Tietojärjestelmän häirinnässä myös yritys on rangaistavaa. Säännöksellä halutaan suojata tietojärjestelmiä virus- ja palvelunestohyökkäyksiltä.[30] Kyberrikollisuuden torjunnan ja koko kansallisen turvallisuuden kannalta tietojärjestelmän ja tietoliikenteen häirintä on merkittävää, koska näillä toimilla rikolliset voivat saada aikaan myös koko kansallista turvallisuutta häiritsevää toimintaa. Etenkin, jos toimet kohdistuvat kriittiseen infrastruktuuriin tai muihin viranomaisten toimintoihin.

---

[24] Valtioneuvoston kanslia, 2024, s. 15–16.
[25] Valtioneuvoston kanslia, 2024, s. 15–16.
[26] HE 153/2006 vp, s. 65.
[27] Aaltonen ja muut, 2021, s. 975.
[28] Nevalainen, 2019a, s. 141.
[29] Lappi-Seppälä ja muut, 2022 s. 1302.
[30] Lappi-Seppälä ja muut, 2022, s. 1302.

2.1.4 Tietomurto

Tietomurrossa on kyse oikeudettomasta tunkeutumisesta tietojärjestelmään tai sen osaan (RL 38:8a)[31]. Tietomurrossa merkittävää on huomioida se, että rikoksen tunnusmerkistö täyttyy heti, kun järjestelmä tai sen turvajärjestelmä on läpäisty[32]. Mikäli koko turvajärjestelyä ei läpäistä, on kyse yrityksestä[33].

> Tapauksessa KKO 2003:36 oli ratkaistavana tietomurron yrityksen tunnusmerkistön täyttyminen. Tapauksessa A oli yrittänyt murtaa Osuuspankkikeskus-OPK:n turvajärjestelyt ja päästä tunkeutumaan heidän tietojärjestelmäänsä. A oli etsinyt haavoittuvuuksia ns. porttiskannauksen avulla niitä kuitenkaan löytämättä, mutta oli kuitenkin kiistatonta, että hän oli tällaista porttiskannausta käyttänyt. KKO viittasi perusteluissaan hallituksen esitykseen HE 94/1993 vp, jossa todetaan, että tietojärjestelmän tunkeutumiselle ei edellytetä mitään erityistä tarkoitusta. Tämä teki A:n puolustuksen tehottomaksi, koska A puolustuksessaan vetosi siihen, että hänellä ei ollut aikomusta edes toteuttaa tietomurtoa, vaan etsi vain haavoittuvuuksia porttiskannauksen avulla. A tuomittiin kuitenkin tietomurron yritykseen, mikä kuvaa hyvin tietomurron yrityksen tunnusmerkistöä, koska tapauksessa oli käytetty teknistä toteutusta ja etsitty aktiivisesti haavoittuvuuksia.[34]

Tietomurron seurauksena rikolliset voivat saada esimerkiksi henkilötietoja, jolloin kyse on myös tietoturvaloukkauksesta[35]. Kyberrikolliset voivat käyttää näitä tietomurron yhteydessä saatuja tietoja kiristykseen, kuten aikaisemmin mainitussa Vastaamo-tietomurrossa, jossa tekijä pyrki kiristämään uhreja nimenomaan arkaluontoisilla henkilötiedoilla[36]. Toisaalta rikolliset käyttävät tietomurroista saatua informaatiota esim. talousrikoksiin, maksupäätepetoksiin ja identiteettivarkauksiin[37]. Tietomurto onkin kyberrikollisuuden kannalta merkittävä tekotapa, jonka torjunnassa poliisilla on paljon tekemistä, koska tietomurron jälkeen data on rikollisten käytettävissä erilaisiin muihin rikoksiin.

---

[31] Aaltonen ja muut, 2021, s. 977.
[32] HE 153/2006 vp, s. 14.
[33] Lappi-Seppälä ja muut, 2022, s. 1305.
[34] KKO:2003:36.
[35] Valtioneuvoston kanslia, 2024, s. 54.
[36] Looi ja muut, 2024, s. 107.
[37] Yar ja Steinmetz, 2023, s. 78.

2.1.5 Suojauksen purkujärjestelmärikos

Suojauksen purkujärjestelmällä tarkoitetaan laitetta, tietokoneohjelmaa tai muuta järjestelmää taikka sen osaa, jonka tarkoituksena on poistaa erityisellä teknisellä järjestelmällä toteutettu suojaus[38]. Suojauksen purkujärjestelmän käyttäminen on kriminalisoitu (RL 38:8b) ja se pitää sisällään mm. suojauksen purkujärjestelmän valmistamisen, maahantuonnin, kaupittelun, vuokraamisen ja levittämisen. Myös suojauksen purkujärjestelmän mainostaminen, asentaminen ja huoltaminen on tuomittavaa[39]. Rangaistus suojauksenpurkujärjestelmärikoksesta on sakko tai vankeutta enintään vuosi (RL 38:8b).

Suojauksen purkujärjestelmärikos on haluttu lisätä rikoslakiin, koska sillä haluttiin kehittää tietoyhteiskunnan palvelujen suojaa[40]. Yleisesti ottaen suojauksen purkujärjestelmärikoksen tunnusmerkistö täyttyy jo, kun teon motiivina on ollut taloudellinen hyöty[41]. Merkittävää rikollisuuden kannalta on myös se, että lainsäätäjä on huomannut myös mahdollisuuden ns. pilkkomiseen. Tavanomaista onkin, että suojauksen purkujärjestelmiä tarjotaan osissa siten, että ne kyetään myöhemmin kokoamaan kokonaisuudeksi, jolla pystytään purkamaan suojaus[42].

Suojauksen purkujärjestelmärikos ei varsinaisesti ole kyberrikollisuuden torjunnan kannalta merkittävä rikosnimike, koska vuosina 2020–2024 viranomaisten tietoon ei tullut yhtäkään suojauksen purkujärjestelmärikosta[43]. Se on kuitenkin rikosnimikkeenä kyberriippuvainen rikos, koska sen suorittaminen vaatii kyberympäristöä tai sellaista teknistä toteutusta, jossa kyberympäristö on vahvasti läsnä.

---

[38] HE 221/2013 vp, s. 194.
[39] HE 146/2000 vp, s. 12.
[40] Lappi-Seppälä ja muut, 2022, s. 1309.
[41] Aaltonen ja muut, 2021, s. 978; Lappi-Seppälä ja muut, 2022, s. 1309; HE 146/2000 vp, s. 12.
[42] HE 146/2000 vp, s. 12.
[43] Tilastokeskus, 2025.

3 Poliisin toimivaltuuksien oikeudellinen perusta ja haasteet kyberrikollisuuden torjunnassa

Kyberrikollisuudella ei ole maantieteellisiä rajoja[44]. Tämä luo erittäin haastavia oikeudellisia pulmia. Monet lait ja säädökset ovat kansallisia tai Suomen tapauksessa EU:n laajuisia, mutta kansainvälisiä säännöksiä kyberrikollisuudesta ei juurikaan ole pl. Budapestin sopimus[45]. Tämä tuo haasteita siihen, kuinka torjua rikollisuutta maissa, joka ylittää omat kansalliset toimivaltuudet[46]. Sisäministeriön julkaisu nostaa esille esimerkkinä rikosten torjunnan haasteista sen, että Suomessa tehdyt nettipetokset usein saadaan selvitettyä, mutta ulkomailla tehtyjen rikosten tutkinta on paljon haastavampaa[47].

Edellä mainittu Budapestin sopimus on Euroopan neuvoston tietoverkkorikollisuutta koskeva sopimus, joka muutti Suomen kansallista lainsäädäntö valtavasti. Budapestin sopimuksen tarkoituksena oli suojella yhteiskuntaa tietotekniikkarikollisuudelta[48]. Budapestin sopimuksen myötä rikoslakiin ja pakkokeinolakiin tuli todella paljon uutta ja merkittävää kyberrikollisuuden kannalta. Merkittäviä uusia ehdotuksia sopimuksen myötä olivat tietoliikenteen ja tietojärjestelmän häirinnän kriminalisointi (RL 38:5 ja RL 38:7) ja Muutokset takavarikoinnin edellytyksiin (PKL 4:1)[49]. Budapestin sopimuksen sisältö päätyi lainvalmisteluaineistoon hallituksen esitykseen (153/2006), jonka tarkoituksena oli nimenomaan saattaa Budapestin sopimuksen sisältö kansallisesti voimaan Suomessa[50]. Budapestin sopimus on siis merkittävä kansainvälinen sopimus kyberrikollisuuden torjunnan kannalta, joka on Suomen kansallisen lainsäädännön taustalla.

---

[44] Murphy, 2024, s. 2.
[45] Sisäministeriö, 2017, s. 19.
[46] Cross ja Hirrle, 2021, s. 15.
[47] Sisäministeriö, 2017, s. 23.
[48] Norrman, 2004, s. 4.
[49] Norrman, 2004, s. 25–30.
[50] HE 154/2006 vp, s. 4.

Ensimmäisessä luvussa mainitut poliisin tehtävät vaativat toteutuakseen monesti lainsäädännöstä tulevia toimivaltuuksia, koska viranomaisen toiminnan on perustuttava tarkoin lakiin (PL 1:2). Poliisihallituksen työryhmän loppuraportissa mainitaan, että poliisi hankkii tietoa myös normaalilla vuorovaikutuksella kansalaisten kanssa, mikä ei vaadi lainsäädännöllistä toimivaltaa. Silloin, kun poliisin tiedonhankinta puuttuu kansalaisten perusoikeuksiin, on toimivaltuuksista säädettävä lailla[51]. Poliisilain toimivaltuudet ovat tarkoitettu rikoksen ennalta estämiseen ja paljastamiseen, kun taas pakkokeinolain mahdollistamat toimivaltuudet perustuvat vahvasti rikosten selvittämiseen[52].

UNODC:n raportissa kyberrikollisuuden torjunnan kriittisiä osia on kolme. Ensimmäinen on tehokas lainsäädäntö, joka on tasapainossa yksilönsuojan ja tutkintavaltuuksien osalta. Toinen on pääsy tutkintavälineisiin ja -tekniikoihin, joka pitää sisällään muun muassa sähköisen todistusaineiston saannin kolmansilta osapuolilta. Viimeinen on riittävä koulutus ja tekninen osaaminen[53]. Suomi on saanut rahallisesti merkittävän panostuksen Euroopan unionin sisäisen turvallisuuden rahastosta muun muassa kyberrikostorjunnan osaamisen kehittämiseen ja nuorten kyberrikollisuuden ehkäisyyn. Suomi on saanut ISF-rahastosta merkittävän rahoituksen Cybercrime Exit 3 -hankkeeseen ja kyberosake -hankkeeseen, joiden tarkoituksena on ehkäistä nuorten kyberrikollisuutta ja kehittää kyberosaamista[54].

3.1 Rikostorjunta

Rikostorjunnalla yleisesti tarkoitetaan rikosten ennalta estämistä, paljastamista ja selvittämistä sekä syyteharkintaan saattamista[55]. Rikostorjunnan käsitteen voidaankin katsoa tulevan suoraan laista, koska poliisin tehtävä on nimenomaan rikosten ennalta estämi-

[51] Poliisihallitus, 2015, s. 13–14.
[52] Poliisihallitus, 2015, s. 5.
[53] UNODC, 2013, s. 118.
[54] Sisäministeriö, 2022.
[55] Helminen ja muut, 2012, s. 229.

nen, paljastaminen, selvittäminen ja syyteharkintaan saattaminen (PolL 1:1). Rikostorjunta kattaa hyvin paljon poliisin tehtäviä. Tässä tutkielmassa perehdyn etenkin rikosten ennalta estämiseen, paljastamiseen ja selvittämiseen.

Kyberrikosten rikostorjunnasta vastaa pääsääntöisesti poliisi[56]. Sisäministeriön julkaisussa poliisin kyberrikostorjunnan tehtävät voidaan jaotella seuraaviin kategorioihin:

1. kybertoimintaympäristön mahdollistamien rikosten ja kyberriippuvaisten rikosten ennalta estäminen, paljastaminen, selvittäminen ja syyteharkintaan saattaminen.
2. Digitaaliforensiikka.
3. Tiedonhankinta.
4. Ennalta estävä toiminta verkossa[57].

Tämä kattaa melko paljon tehtäviä, joita eri poliisilaitokset ja mm. keskusrikospoliisi tekevät päivittäisessä työssä. Digitaaliforensiikalla tarkoitetaan todisteiden esille hakua tietoteknisistä laitteista. Tiedonhankinnalla tarkoitetaan puolestaan ns. rikostiedustelua verkossa[58].

Poliisin toteuttama rikostorjunta pitää sisällään ennalta ehkäisevää toimintaa, joka ei välttämättä vaadi aina lainsäädännöllistä toimivaltaa. Poliisin kenttätoiminnan arvokasta työtä ovat näkyvä valvonta ja kansalaisten informointi. Poliisi toteuttaa myös ns. nettipoliisitoimintaa[59], joka on informointia ja näkyvää valvontaa etenkin sosiaalisessa mediassa.

3.2 Tiedonhankintakeinot kyberrikostorjunnassa

Helminen ja muut mainitsevat, että tiedonhankinta on merkittävässä roolissa rikostorjunnan ja etenkin rikosten ennalta estämisen ja paljastamisen onnistumisen kannalta.

---

[56] Nevalainen, 2019b, s. 884.
[57] Sisäministeriö, 2017, s. 25.
[58] Sisäministeriö, 2017, s. 25.
[59] Sisäministeriö. 2017, s. 32.

Poliisi ei kuitenkaan voi hankkia tietoa, miten tahansa, sillä tiedonhankinta on tarkoin säänneltyä[60]. Yleisesti poliisi suorittaa valvontaa ja tarkkailua, mutta se kohdistuu pitkälti henkilöihin, ajoneuvoihin ja paikkoihin[61]. Tarkkailu on myös mahdollista tietoverkoissa, eikä se käytännössä vaadi toimivaltuussääntelyä [62]. On kuitenkin huomioitava, että tarkkailun tulee olla passiivista, eikä tietoverkossa tapahtuva tarkkailu saa tapahtua nimimerkin takaa, koska silloin kyseessä olisi peitetoiminta[63].

Poliisilla on myös poliisilain 5 luvusta tulevat toimivaltuudet salaisiin tiedonhankintakeinoihin. Kyberrikosten ennalta estämiseen ja paljastamiseen liittyy kuitenkin useita haasteita. Salaisten tiedonhankintakeinojen käyttö voi toisaalta olla ratkaisevassa roolissa, mutta niiden käyttö ulkomailla tehtyjä rikoksia vastaan voi olla tehotonta, koska toisen valtion viranomaisen toimivaltuusalueelle ei voida mennä[64]. Salaisia tiedonhankinta keinoja on useita (PolL 5). Käsittelen tässä tutkielmassa muutamaa salaista tiedonhankintakeinoa, koska tutkielmassa ei ole mahdollista käsitellä kaikkia tiedonhankintakeinoja ja niiden vaikutuksia kyberrikostorjuntaan.

3.2.1 Telekuuntelu ja televalvonta

Telekuuntelusta säädetään poliisilain 5 luvun 5 §:ssä. Telekuuntelu on mahdollistettu rikosten ennalta estämiseksi vuonna 2001 [65]. Telekuuntelua on myös aiemmin kutsuttu ”puhelinkuunteluksi”, mutta termi ei ole enää ajantasainen, koska telekuuntelu kohdistuu nykyään enemmänkin sähköposti- tai tekstiviestintään[66]. Telekuuntelulla tarkoitetaan lyhyesti sanottuna teleosoitteeseen tai telepäätelaitteeseen vastaanotettavan tai siitä lähetetyn viestin kuuntelua, tallentamista ja muuta käsittelyä (PolL 5:5)[67]. Tele-

[60] Helminen ja muut, 2012, s. 387.
[61] Helminen ja muut, 2012, s. 388.
[62] HE 224/2010 vp, s. 34.
[63] HE 224/2010 vp, s. 34; Helminen ja muut, 2012, s. 394.
[64] Sisäministeriö, 2017, s. 42.
[65] Hankilanoja, 2014, s. 78.
[66] Helminen ja muut, 2012, s. 403.
[67] Helminen ja muut, 2012, s. 403.

kuuntelua ei kuitenkaan voida kohdistaa kovin pienin perustein. Telekuuntelua tiedonhankintakeinona voidaan käyttää kyberrikollisuuden torjunnassa hyvin harvoin, koska kyseisen kyberrikoksen tulisi käytännössä olla maanpetos, vakoilu, turvallisuussalaisuuden paljastaminen, luvaton tiedustelutoiminta tai sen pitäisi liittyä terrorismiin (PolL 5:5).

Telekuuntelusta päättää tuomioistuin pidättämiseen oikeutetun poliisimiehen vaatimuksesta aina enintään kuukaudeksi kerrallaan (PolL 5:7). Telekuuntelun käyttö kyberrikollisuuden torjunnassa on haastava useasta syystä. Telekuuntelua ei voida käyttää tiedonhankintaan, vaikka edellytykset käyttöön olisi, mikäli todellista tavoitetta ei tultaisi saavuttamaan[68], mikä on haastavaa valtionrajat ylittävän elementin takia. Tällöin tulisi tarkastella telekuuntelun käytön jälkeen, että oliko todellinen tavoite saavutettavissa, mikäli rikoksentekijä on ulkomailla tai hänellä ei ole minkäänlaisia siteitä Suomeen.

Telekuuntelun edellytyksenä oli aiemmin yksilöity teleosoite tai telepäätelaite, minkä takia telekuuntelu on helppo saada tehottomaksi esimerkiksi usein vaihdetulla prepaid-liittymällä tai puhelinta vaihtamalla[69]. Telekuuntelu- ja televalvontalupa on kuitenkin nykyään muutettu henkilösidonnaiseksi[70]. Tämä kuvastaa toisaalta sitä, että lainsäädäntö kehittyy vastaamaan nykypäivän tarpeita, mutta kehitys saattaa tapahtua hitaasti. Poliisihallitus oli jo vuonna 2015 huomannut tämän epäkohdan, mutta siihen saatiin ratkaisu hallituksen esityksessä vasta vuonna 2022.

Televalvonta on puolesta tunnistamistietojen hankkimista viestistä, sijaintitietojen hankkimista teleosoitteesta tai telepäätelaitteesta tai laitteen tilapäistä estämistä[71]. Televalvonnasta säädetään poliisilain 5 luvun 8 §:ssä. Poliisilla on oikeus kohdistaa televalvontaa, mikäli henkilön lausumien, uhkausten tai käyttäytymisen perusteella tai muuten voidaan perustellusti olettaa hänen syyllistyvän rikokseen, josta säädetty ankarin rangaistus olisi

[68] HE 275/2022 vp, s. 5.
[69] Poliisihallitus, 2015, s. 14.
[70] HE 275/2022 vp, s. 14.
[71] Helminen ja muut, 2012, s. 405.

vähintään neljä vuotta vankeutta (PolL 5:8). Toinen peruste on teleosoitetta tai telepäätelaitetta käyttäen tehty rikos, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta (PolL 5:8). Kolmas on teleosoitetta tai telepäätelaitetta käyttäen tehty, automaattiseen tietojenkäsittelyjärjestelmään kohdistuva luvaton käyttö (PolL 5:8). Muita perusteita ovat seksikaupan kohteena olevan henkilön hyväksikäyttöön, lapsen houkuttelemiseen seksuaalisiin tarkoituksiin tai paritukseen, huumausainerikokset, terrorismiin liittyvät rikokset tai törkeä tulliselvitysrikos (PolL 5:8).

Televalvonnalla yleisesti pyritään selvittämään viestinnän osapuolet[72]. Televalvonta on merkittävä osa kyberrikollisten henkilöllisyyden selvittämisessä. Se, että viestinnän osapuolet saadaan selville voi olla todella arvokasta tietoa myöhemmin rikoksen selvittämisessä, koska kyberrikollisten henkilöllisyyden selvittäminen voi olla hyvin haastavaa[73].

3.2.2 Tekninen laitetarkkailu

Tekninen laitetarkkailu on merkittävä tapa hankkia tietoa rikosten ennalta estämisemiseksi tietoverkoista. Poliisilain 5 luvun 23 §:n mukaan *teknisellä laitetarkkailulla tarkoitetaan tietokoneen tai muun vastaavan teknisen laitteen taikka sen ohjelmiston toiminnan, sisältämien tietojen tai yksilöintitietojen muuta kuin yksinomaan aistinvaraista tarkkailua, tallentamista tai muuta käsittelyä rikoksen estämiselle merkityksellisen seikan tutkimiseksi.* Tekninen laitetarkkailu tarkoittaa siis yleisesti teknisen laitteen tarkkailua ja rikoksesta epäillyn toiminnan seuraamista teknisessä laitteessa[74]. Teknisellä laitetarkkailulla ei kuitenkaan saa hankkia tietoa viestin sisällöstä tai niiden tunnistamistiedoista[75]. Helminen ja muut mainitsevat erääksi teknisen laitetarkkailun muodoksi näp-

[72] Helminen ja muut, 2012, s. 405.
[73] Riekkinen, 2019, s. 186.
[74] Helminen ja muut, 2014, s. 355–356.
[75] HE 275/2022 vp, s. 16.

päimistökuuntelun. Tämän tarkoituksena olisi seurata näppäimistön toimintaa, jotta voidaan saada selville esim. salasanan sisältö[76]. Mikäli näppäimistökuuntelulla saisi selville viestin sisällön tällöin olisi kyse teknisestä kuuntelusta[77].

3.2.3 Peitetoiminta

Peitetoiminnalla tarkoitetaan poliisilain mukaan *tiettyyn henkilöön tai hänen toimintaansa kohdistuvaa suunnitelmallista tiedonhankintaa käyttämällä soluttautumista, jossa tiedonhankinnan edellyttämän luottamuksen hankkimiseksi tai tiedonhankinnan paljastumisen estämiseksi käytetään vääriä, harhauttavia tai peiteltyjä tietoja tai rekisterimerkintöjä taikka valmistetaan tai käytetään vääriä asiakirjoja* (PolL 5:28). Peitetoiminnalla siis salataan henkilöllisyys ja käytetään harhauttavia ja peiteltyjä tietoja, jotta peitetoiminnan kohde ei saisi tietää häneen kohdistetusta peitetoiminnasta.

Poliisilla on oikeus kohdistaa peitetoimintaa tietoverkossa, mikäli voidaan olettaa henkilön syyllistyvän rikokseen, josta ankarin säädetty rangaistus on vähintään kaksi vuotta vankeutta (PolL 5:28)[78]. Peitetoiminta on kyberrikollisuuden torjunnan kannalta merkittävä toimivaltuus ja peitetoimintaa tietoverkoissa voidaankin käyttää vähemmin perustein kuin esim. peiteltyä tiedonhankintaa[79]. Vaikka peitetoiminnan käyttö on yleisesti vähäistä, se on merkittävä kyberrikollisuuden torjunnassa, koska peitetoiminta on lähinnä painottunut tietoverkossa tapahtuvaksi peitetoiminnaksi[80]. Peitetoiminta on näkemäni mukaan tehokkain toimivaltuus salaisista tiedonhankintakeinoista etenkin kyberrikollisuuden ennalta estämiseksi. Lisäksi peitetoimintaa on helpompi toteuttaa tietoverkoissa, koska tietoverkoissa on yleistä toimia nimimerkin takaa[81]. Peitetoiminta on kyberrikollisuuden ennalta estämisessä avainasemassa.

---

[76] Helminen ja muut, 2012, s. 408.
[77] HE 275/2022 vp, s. 17.
[78] HE 105/2023 vp, s. 34.
[79] HE 275/2022 vp, s. 15.
[80] Poliisihallitus, 2023, s. 33.
[81] HE 275/2022 vp, s. 16.

3.3 Pakkokeinot

Poliisin pakkokeinojen käytöstä säädetään lailla. Pakkokeinoja käytetään rikostorjunnassa rikosten estämiseksi tai paljastamiseksi[82]. Pakkokeinojen käyttöä ohjaavat erilaiset periaatteet (PKL 1:2–4). Pakkokeinojen käyttöä ohjaa suhteellisuusperiaate, vähimmän haitan periaate ja hienotunteisuusperiaate. Periaatteiden tarkoituksena on varmistaa, että pakkokeinoja käytetään vain, kun se on välttämätöntä. Eli pakkokeinoilla ei saa puuttua kenenkään oikeuksiin enempää kuin on välttämätöntä ja niillä ei saa aiheuttaa aiheetonta huomiota ja on toimittava hienotunteisesti. Suhteellisuusperiaatteen mukaisesti pakkokeinojen käyttö muutamia poikkeuksia lukuun ottamatta onkin sidottu rikoksen enimmäisrangaistukseen[83].

Kyberrikosten enimmäisrangaistuksia on vuosien varrella kovennettu[84]. Enimmäisrangaistuksia on haluttu nostaa, jotta yhä laajempia pakkokeinoja voidaan kohdistaa rikoksesta epäiltyihin[85]. Pakkokeinojen käyttö edellyttää kuitenkin aina vähintään rikosepäilyä[86], mikä erottaa ne salaisista tiedonhankintakeinoista. Pakkokeinojen käytössä on otettava huomioon se, että mikäli samaa henkilöä epäillään useista rikoksista niin jokainen käsitellään omana kokonaisuutenaan tarkastellessa pakkokeinojen edellytyksiä[87]. Tilanne on merkittävä kyberrikosten torjunnassa ja tutkinnassa, koska kyberrikokset voivat pitää sisällään useita eri rikosnimikkeitä. Pakkokeinoja ei saa kohdistaa epäiltyyn, mikäli kyseinen rikosepäily on jo loppuun käsitelty tuomioistuimessa ja tuomio on lainvoimainen[88].

---

[82] Tolvanen, 2013, s. 1296.
[83] HE 217/2022 vp, s. 9.
[84] LaVM 29/2014 vp, s. 2.
[85] LaVM 29/2014 vp, s. 2.
[86] Fredman ja muut, 2025, s. 687.
[87] Fredman ja muut, 2025, s. 687.
[88] Itä-Suomen HO 25.9.2018/496.

3.3.1 Takavarikointi

Takavarikoinnin edellytyksistä säädetään siten, että esine, omaisuus tai asiakirja voidaan takavarikoida, mikäli sitä voidaan käyttää todisteena rikosasiassa, se on rikoksella joltakulta viety tai se tuomitaan menetetyksi (PKL 7:1)[89]. Takavarikoinnilla on myös tiettyjä reunaehtoja ja osaa koskevat erilaiset takavarikoimis- ja jäljentämiskiellot (PKL 7:3–4). Esimerkiksi salaisista pakkokeinoista määrätään pakkokeinolain 10 luvussa ja tämän vuoksi tiettyjen salaisten pakkokeinojen alle ulottuvia tietoja ei saa takavarikoida (PKL 7:4). Tällä on haluttu estää salaisten pakkokeinojen kiertäminen[90].

Hallituksen esityksessä (153/2006) takavarikoinnin edellytyksiin on lisätty kohta, jossa data olisi myös takavarikoinnin kohteena. Data määritellään samaisessa esityksessä siten, että *data on tietoa, joka on tietokoneessa tai muussa vastaavassa tietojärjestelmässä taikka sen tallennusalustalla*[91]. Esityksessä on muitakin merkittäviä lisäyksiä kyberrikollisuuden torjunnan kannalta, koska esityksen tarkoituksena oli säätää lainsäädäntö vastaamaan Euroopan neuvoston tietoverkkorikollisuutta koskevaa yleissopimusta, eli Budapestin sopimuksen vaatimuksia. Datan lisäys takavarikoinnin kohteeksi oli merkittävä lisäys poliisin kybertoimivaltuuksiin, koska se mahdollistaa todistusaineiston keräämisen tietojärjestelmistä, joka on merkittävä osa useita eri kyberrikoksia.

> Tapauksessa KKO: 2022:23 käsiteltiin takavarikoinnin edellytyksiä juuri pakkokeinolain 7 luvun 1 §:n mukaan. Tapauksessa A Oyj tarjosi VPN (Virtual Private Network) -palvelua, joka salaa käyttäjän todellisen IP-osoitteen ulkopuolisilta. Keskusrikospoliisi oli Saksan keskusrikospoliisin pyynnöstä määrännyt A Oyj:n säilyttämään IP-osoitteeseen liittyvät käyttäjätiedot, rekisteröintitiedot ja lokitiedot. Tämän jälkeen keskusrikospoliisi takavarikoi pakkokeinolain 7 luvun 1 ja 21 §:n nojalla A Oyj:n hallussa olevaa tietoa siitä mihin osoitteeseen IP-osoitteesta oltiin yhteydessä tiettyinä aikoina. Saksan keskusrikospoliisi oli tutkinut epäiltyä törkeää lapsen seksuaalista hyväksikäyttöä koskevaa asiaa.
>
> Tapauksessa ratkaistavana oli se, että olivatko tiedot pakkokeinolain 7 luvun 1 §:n nojalla takavarikoitavissa vai koskeeko näitä tietoja pakkokeinolain 7 luvun 4 §:n

---

[89] Fredman ja muut, 2025, s. 901.
[90] HE 222/2010 vp, s. 276; Helminen ja muut, 2014, s. 287.
[91] HE 153/2006 vp, s. 68.

> mukainen takavarikoimiskielto. Korkein oikeus katsoo tapauksessa, että näitä tietoja koskee takavarikoimiskielto. Korkein oikeus perustelee takavarikoimiskieltoa sillä, että se katsoo A Oyj:n olevan sähköisen viestinnän palveluista annetun lain 3 §:n 36 tarkoittama viestinnän välittäjä. Pakkokeinolain 7 luvun 4 §:n takavarikoimiskielto koskee teleyritysten ja yhteisötilaajien lisäksi myös nimenomaan sähköisen viestinnän palveluista annetun lain 3 §:n 36 tarkoittamia viestinnän välittäjiä.[92]

Kyberrikosten torjunnassa tärkeää on saada poliisin tietoon yksilöitävä IP-osoite tai vastaavanlainen tunniste, jonka avulla voidaan päästä tekijän jäljille[93]. Mielestäni korkeimman oikeuden päätös kuvastaa poliisin kohtaamia haasteita kyberrikollisuuden torjunnassa. Päätös antaa rikollisille vaarallisen esimerkin siitä, että VPN-palvelua käyttämällä pystyy kiertämään takavarikoinnin ja voi jopa olla turvassa rikosoikeudellisesta vastuusta, mikäli rikos ei ylitä pakkokeinolain 10 luvun mukaisia vaatimuksia, koska viranomaisten toimivaltuudet eivät välttämättä riitä muuten todistamaan syyllisyyttä tai he eivät pysty identifioimaan rikoksentekijää.

3.3.2 Kotietsintä

Poliisien toimivaltuuksiin pakkokeinolain mukaan kuuluu myös kotietsintä (PKL 8:2). Yleisellä kotietsinnällä tarkoitetaan yleisesti kotirauhan suojaaman paikan etsintää[94]. Kotirauhan suojaamia paikkoja ovat puolestaan asunnot, loma-asunnot, hotellihuoneet, teltat, asuntovaunut, asuttavat alukset, asuintalojen porraskäytävät, yksityisalueiden pihat, asuntoautot ja rekka-auton nukkumiseen tarkoitetut osat[95]. Erityisellä kotietsinnällä viitataan enemmänkin etsintään, jonka kohteena on tietoa, joka on oikeudenkäynnissä salassa pidettävää tai josta saa kieltäytyä todistamasta[96].

---

[92] KKO:2022:23.
[93] UNODC, 2013, s. 143; Riekkinen, 2019, s. 185–186.
[94] Helminen ja muut, 2014, s. 302; Vuorenpää ja muut, 2021, s. 908.
[95] HE 222/2010 vp, s. 290; Helminen ja muut, 2014, s. 302.
[96] Vuorenperä ja muut, 2021, s. 908.

Yleinen kotietsintä voidaan toteuttaa, mikäli epäillystä rikoksesta ankarin rangaistus olisi vähintään kuusi kuukautta vankeutta tai jos selvitettävänä on yhteisösakon tuomitsemiseen liittyvät seikat (PKL 8:2). Näiden lisäksi edellytyksenä on, että *etsinnässä voidaan olettaa löytyvän tutkittavan olevaan rikokseen liittyvä: 7 luvun 1 §:n 1 tai 2 momentissa tarkoitettu takavarikoitava esine, omaisuus, asiakirja tai tieto; 7 luvun 2 §:n nojalla jäljennettävä asiakirja; vakuutustakavarikkoon määrättävä omaisuus; tai seikka, jolla voi olla merkitys rikoksen selvittämisessä* (PKL 8:2). Kotietsintä voi olla tehokas tapa kerätä todistusaineistoa kyberrikoksesta, mutta haastavaa siitä tekee se, että kyberrikoksissa ei usein ole suoraa rikospaikkaa taikka suoraa rikoksesta epäiltyä[97].

Annan esimerkin, joka kuvaa poliisin kenttätyön teknisiä haasteita ja johon liittyy oikeudellisia tulkintaongelmia. Tapaus, jota Edwards käytti kirjassaan, on tilanne, jossa rikolliset tajusivat pelikonsolien kovalevyjen käytön mahdollisuudeksi kätkeä lasten hyväksikäyttömateriaalia[98]. Tapauksessa rikolliset huomasivat, että materiaalia voidaan piilottaa pelikonsolin kovalevyyn ja se koettiin hyväksi tavaksi piilottaa materiaalia, koska poliisit tarvitsevat etsintäluvan. Vaikka poliisit saisivat etsintäluvan, niin tuolloin poliisit takavarikoisivat kotietsinnän yhteydessä todennäköisesti vain tietokoneen kovalevyn[99]. Voidaan ajatella, että tämä oli jossain vaiheessa tyypillinen tapa vältellä kiinnijäämistä, mutta nyt tällainen toiminta on hyvin poliisin tiedossa ja poliisilla on vastassa taas uusia toimintatapoja, joita rikolliset käyttävät. Esimerkki kuvaa siis sitä verkon kautta nopeasti leviävää rikollista toimintatapaa, jossa rikolliset ovat hiukan poliisien edellä, kunnes jäävät lopulta kiinni.

3.3.3 Laite-etsintä

Laite-etsinnällä tarkoitetaan teknisen laitteen tai tietojärjestelmän tietosisältöön kohdistettavaa etsintää (PKL 8:20). Tietosisällöllä tarkoitetaan laitteessa tai tietojärjestelmässä

---

[97] Riekkinen, 2019, s. 185.
[98] Edwards, 2020, s. 24.
[99] Edwards, 2020, s. 24.

olevaa tietoa tai tietokokonaisuutta[100]. Tietosisältö voi myös koskea tiedostoa, johon voi päästä vain kyseisen etsinnän alaisen laitteen kautta[101]. Laite-etsinnällä ei saa myöskään kiertää salaisia pakkokeinoja, joten laite-etsintää ei saada kohdistaa luottamukselliseen viestiin[102]. Laite-etsintä voidaan suorittaa, mikäli on syytä epäillä rikoksesta, josta voi seurata vähintään kuusi kuukautta vankeutta, tai se voidaan toteuttaa yhteisösakon edellytysten selvittämiseksi (PKL 8:21). Lisäksi tulisi olettaa löytyvän takavarikoitava asiakirja tai tieto (PKL 8:21). Laite-etsinnän yhteyteen voidaan määrätä datan säilyttäminen (PKL 8:25). Tämä tarkoittaa käytännössä sitä, että tietojärjestelmän ylläpitäjä määrätään säilyttämään määrätty data siten, että epäilty tai muu henkilö ei voi sitä poistaa[103].

Laite-etsinnässä, kuten muissa etsinnöissä, tulee haasteeksi kyberrikosten luonne. Kuten aiemmin mainittu, kyberrikosten torjunnan ongelmana on fyysisen rikospaikan ja rikoksesta epäillyn puuttuminen[104]. Lisäksi vielä valtionrajat ylittävä luonne tuo haasteita etenkin etsintään, koska ne oikeastaan etäetsintää lukuun ottamatta ovat fyysisiä etsintöjä. Tällöin etsintää on haastavaa kohdistaa kotiin tai laitteeseen, mikäli fyysistä rikospaikkaa tai tekijää ei ole tiedossa. Etsinnän edellytykset ja vaikutukset kohdistuvat lähinnä Suomesta käsin tehdyille kyberrikoksille.

3.3.4 Salaiset pakkokeinot

Salaiset pakkokeinot ja salaiset tiedonhankintakeinot eivät käytännössä eroa toisistaan. Ero näiden välillä on se, että salaisia tiedonhankintakeinoja käytetään rikosten ennalta estämiseen ja paljastamiseen ja salaisia pakkokeinoja lähinnä selvittämiseen. Salaisten pakkokeinojen käyttö edellyttää myös aina rikosepäilyä[105]. Salaisten pakkokeinojen on kohdistuttava rikoksesta epäiltyyn henkilöön, eikä niitä saa käyttää henkilöön, joka ei ole

[100] HE 222/2010 vp, s. 306.
[101] HE 222/2010 vp, s. 306.
[102] Fredman, 2025, s. 1019.
[103] Vuorenpää ja muut, 2021, s. 911.
[104] Riekkinen, 2019, s. 185.
[105] Fredman ja muut, 2025, s. 687.

pääasiassa rikoksesta epäiltynä[106]. Salaiset pakkokeinot ovat jo aiemmin mainittujen salaisten tiedonhankintakeinojen kanssa teknisesti samanlaisia, mutta niiden vaikutukset ja tarkoitus on hieman erilainen. Tämän takia en tule tässä luvussa käsittelemään yksittäisiä salaisia pakkokeinoja, vaan yleisesti salaisista pakkokeinoista.

Pakkokeinojen tarkoituksena on käytännössä todisteiden hankita ja rikosprosessin turvaaminen[107]. Pakkokeinojen käytön laajentamisesta oli ehdotettu etenkin telekuuntelun ja televalvonnan osalta. Tahtotila oli, että jatkossa telekuuntelu- ja televalvontalupa haettaisiin henkilösidonnaisesti[108]. Tämä tarkoittaa sitä, että tuomioistuimelta ei tarvitsisi hakea telekuuntelu- ja televalvontalupaa telepäätelaite- tai teleosoitekohtaisesti, vaan hakemus olisi sidottuna henkilöön[109]. Oikeuskansleri pitää ehdotusta sinänsä tervetulleena, mutta hänen näkemyksensä mukaan ehdotus vaatisi muutamia tarkennuksia. Hän mainitsee, että vaikka lupa olisi henkilösidonnainen, tulisi silti tuomioistuimen tietoon saattaa ne telepäätelaitteet tai -osoitteet, joihin telepakkokeinoja sovellettaisiin[110]. Tämä lakimuutosehdotus tuli poliisilakiin hallituksen esityksessä (275/2022) ja pakkokeinolakiin hallituksen esityksessä (217/2022). Aiemmassa luvussa käsiteltiin se, että minkälainen vaikutus tällä on etenkin kyberrikostorjunnan osalta. Se on merkittävä, koska kuten mainittu, että esim. prepaid-liittymää ja puhelinta vaihtamalla pystyi kiertämään televalvontaa ja telekuuntelua melko tehokkaasti[111].

---

[106] Helsingin HO 21.3.2014 Diaarisalainen.
[107] Pölönen, 1997, s. 1209.
[108] PeVL 98/2022 vp, s. 3.
[109] PeVL 98/2022 vp, s. 3.
[110] OKV/348/21/2022.
[111] Poliisihallitus, 2015, s. 14.

4 Johtopäätökset

Tutkielmassa tarkasteltiin kyberrikollisuutta ja poliisin kybertoimivaltuuksia lainopillisesta näkökulmasta. Tarkastelu keskittyi lähinnä poliisin toimivaltuuksiin kansallisen lainsäädännön kannalta ja kyberrikollisuuden ja kyberrikosten määrittelyyn. Tarkastelun tavoitteena oli vastata asetettuihin tutkimuskysymyksiin eli mitä toimivaltuuksia poliisilla on torjua kyberrikollisuutta oikeuden näkökulmasta ja mitä oikeudellisia haasteita poliisi kohtaa kyberrikollisuuden torjunnassa.

Kyberrikollisuus ja kyberrikokset ovat haastava, teknologisesti kehittynyt ja valtionrajat ylittävä ilmiö[112]. Kyberrikollisuuden määrittely on keskeneräinen ja osaltaan harhaanjohtava, koska ilmiölle ei ole yhtä selkeää määritelmää[113]. Lisäksi teknologian nopea kehitys ja rikosten kansainvälinen luonne luovat haasteita poliisille. Poliisin toimivaltuudet ovat hyvinkin selvästi ja tarkasti määritelty kansallisessa lainsäädännössä. Se ei kuitenkaan tarkoita, että ne olisivat riittävät juuri kyberrikostorjuntaan. Poliisin tehtävistä ja toimivaltuuksista säädetään lailla. Poliisin tehtävät ja toimivalta rikosten ennalta estämiseksi ja paljastamiseksi tulee poliisilaista, mutta toimivaltuudet rikosten selvittämiseksi ja syyteharkintaan saattamiseen tulevat pakkokeinolaista ja esitutkintalaista. Poliisin merkittävimmät toimivaltuudet kyberrikollisuuden torjuntaan ovat salaiset tiedonhankintakeinot poliisilaista ja salaiset pakkokeinot pakkokeinolaista, koska näitä toimia voidaan kohdistaa tehokkaasti tietoverkkoihin esim. televalvontaa ja peitetoimintaa.

Poliisin kyberrikostorjunnan haasteet tulevatkin lähinnä kansallisen lainsäädännön haasteista yhteensovittaa lainsäädäntö siten, että sillä kyetään vaikuttamaan myös kyberympäristössä. Lainsäädännössä tulisi olla tiettyjen toimivaltuuksien osalta erillisiä ohjeita tai säädöksiä kybertoimintaympäristön osalta. Esimerkkinä tästä on mm. peitetoiminnasta säätäminen (PolL 5:28 ja PKL 10:27), koska näissä peitetoiminnan edellytyksistä tietoverkoissa säädetään erikseen.

---

[112] Sisäministeriö, 2017, s. 5, 19–20.
[113] UNODC, 2013, s. 14; Nevalainen, 2019a, s. 135.

Tutkielmassa pyrittiin määrittelemään kyberrikollisuus ja kyberrikokset aiemman tutkimuksen perusteella, mutta tutkimus kyberrikollisuudesta oikeudellisena ilmiönä on vähäistä[114]. Tämän vuoksi aiemman tutkimuksen käyttö etenkin kyberrikollisuuden ja kyberrikosten osalta oli melko haastavaa ja tutkielmassa kyberrikollisuutta ja kyberrikoksia pyrittiin käsittelemään melko laajasti.

Tutkielmassa käy ilmi varsin hyvin se, että lainsäädäntö on melko hyvin ajan tasalla. Lain ajan tasaisuus tulee kuitenkin usein hieman viiveellä, kun kyse on kyberrikollisuuden torjuntaan vaikuttavasta lainsäädännöstä. Esimerkkinä poliisihallituksen työryhmän loppuraportissa vuonna 2015 oli mainittu merkittäväksi ongelmaksi televalvonta- ja telekuunteluluvan telepäätelaite ja teleosoitekohtaisuus, koska rikolliset pystyivät vaihtamaan telepäätelaitteita ja teleosoitteita[115]. Kuten tutkielmassa käy ilmi, tähän saatiin muutos vasta vuoden 2022 hallituksen esityksissä. Teknologian kehitys on siis nopeampaa kuin lainsäädännönkehitys, mikä tuo suuria haasteita myös poliisille. Teknologian nopea kehitys tarkoittaa sitä, että uusia rikoksentekomuotoja tulee jatkuvasti lisää ja teknologian kehityksen myötä anonyymiys on lisääntynyt. Tämä tuo haasteita poliisille siinä, että lainsäädännön kehitys ei vastaa teknologian kehitystä, jolloin siirtymäaikana poliisi kohtaa valtavia haasteita. Toinen merkittävä haaste kyberrikollisuuden torjunnassa on rikosten valtionrajat ylittävä luonne. Tämä on ongelma sen takia, että kansalliset toimivaltuudet eivät päde ulkomailla, jolloin on tukeuduttava vieraan valtion viranomaisiin. Jokainen valtio ei kuitenkaan syystä tai toisesta ole aina yhteistyöhaluinen, jolloin kyberrikollisuuden torjuntaan jää valtava aukko.

Jatkotutkimuksen tarve aiheesta on mielestäni suuri. Etenkin kyberrikollisuuden tai tietoverkkorikollisuuden selkeä ja oikeudellisesti pätevä määrittely olisi tarpeen. Se vaatisi tutkimusta kyberrikosten tunnusmerkistöistä, oikeuskäytännöstä, käsitteiden laaja-

---

[114] Aaltonen ja muut, 2021, s. 967; Nevalainen, 2019a, s. 131.
[115] Poliisihallitus, 2015, s. 14.

alaista määrittelyä ja näiden kaikkien osalta tieteellistä yhteisymmärrystä käsitteistä. Toisaalta myös lainsäädännöllistä tutkimusta olisi tarpeen tehdä teknologian kehityksen yhteydessä muutenkin. Jatkotutkimusta tarvittaisiin siitä, kuinka lainsäädäntö ja etenkin poliisin toimivaltuuksiin liittyvä lainsäädäntö reagoi teknologiseen kehitykseen ja sitä, kuinka reagointia voitaisiin kehittää.

Lähteet

Aaltonen, M., Luomala, M. & Paasonen, J. (2021). Kyberrikokset tuomioistuimissa – tarkastelussa rikoslain 38 luvun mukaiset tieto- ja viestintärikokset, *Defensor Legis, 4/2021,* 966–987. Edilex.

Cross, S., Hirrle, S. INTERPOL (2021). National Cybercrime Strategy Guidebook.

Edwards, G. (2020). *Cybercrime investigators handbook*. John Wiley & Sons, Inc. Noudettu 2.10.2025 osoitteesta https://doi.org/10.1002/9781119596318.

Fredman, M., Rautio, L., Tolvanen, M. & Viitanen, M. (2025). *Esitutkinta ja pakkokeinot* (7., uudistettu painos). Alma Insights.

Hankilanoja, A. (2014). *Poliisin salainen tiedonhankinta*. Talentum.

Helminen, K., Kuusimäki, M., & Rantaeskola, S. (2012). *Poliisilaki*. Talentum.

Helminen, K., Fredman, M., Kanerva, J., Tolvanen, M., & Viitanen, M. (2014). *Esitutkinta ja pakkokeinot* (5., uudistettu painos). Talentum.

Kaakinen, M. & Näsi, M. (2021). Kyberrikollisuus. Teoksessa I. Kolttola (toim.). *(Katsauksia 49/2021) Rikollisuustilanne 2020 : Rikollisuuskehitys tilastojen ja tutkimusten valossa* (s. 123–134). Helsingin yliopisto. Noudettu 29.9.2025 osoitteesta http://hdl.handle.net/10138/337259.

Lappi-Seppälä, T., Hakamies, K., Helenius, D., Melander, S., Nuotio, K., Ojala, T., & Rautio, I. (2022). *Rikosoikeus* (Viides, uudistettu painos). Alma Talent.

Looi, J. C., Allison, S., Bastiampillai, T., Maguire, P. A., Kisely, S., Reutens, S., & Looi, R. C. (2025). Cybersecurity lessons from the Vastaamo psychotherapy data breach for psychiatrists and other mental healthcare providers. *Australasian Psychiatry*, *33*(1), 106–110. Noudettu 2.10.2025 osoitteesta https://doi.org/10.1177/10398562241291340.

Määttä, T., (2016). Metodinen pluralismi oikeustieteessä – Ympäristöoikeudellisen tutkimuksen suuntaukset ja menetelmät. Teoksessa Miettinen, T. (toim.), *Oikeustieteellinen opinnäyte: Artikkeleita oikeustieteellisten opinnäytteiden vaati mukasista, metodista ja arvostelusta*. (s. 135–222) Edita.

Murphy, C. (2024). *Understanding cybercrime*. Euroopan parlamentti. Noudettu 3.10.2025 osoitteesta https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760356/EPRS_BRI(2024)760356_EN.pdf.

Nevalainen, S. (2019b). Suomen kyberrikostorjunnan strategiset suuntaviivat 2010–2019, *Defensor Legis, 6/2019,* s. 883–901. Edilex.

Nevalainen, S. (2019a). Kyberrikokset ja Suomen rikosoikeus, *Defensor Legis, 2/2019,* s. 131–148. Edilex.

Norrman, W. (2004). *Tietoverkkorikostyöryhmän mietintö: Tiivistelmä lausunnoista*. Oikeusministeriö. Noudettu 24.11.2025 osoitteesta https://julkaisut.valtioneuvosto.fi/server/api/core/bitstreams/67f5e407-d0df-40d1-be86-0a887cd57f79/content

Poliisihallitus (2015, 2. kesäkuuta). *Poliisin kybertoimivaltuudet*. Työryhmän loppuraportti, POL-2015-3879.

Poliisihallitus (2023, 9. maaliskuuta). *Poliisihallituksen kertomus sisäministeriölle poliisin salaisesta tiedonhankinnasta ja sen valvonnasta vuonna 2022.* POL-2022-159163.

Pölönen, P. (1997). Salaisista pakkokeinoista ja tiedustelutoiminnasta, *Lakimies, 8/1997,* s. 1206–1232. Edilex.

Riekkinen, J. (2019). *Sähköiset todisteet rikosprosessissa (2019)*. Alma Talent.

Sisäministeriö (2017). *Tietoverkkorikollisuuden torjuntaa koskeva selvitys 14/2017.* Noudettu 4.10.2025 osoitteesta https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79866/Tietoverkkotorjuntaselvitys_VERKKO_.pdf?sequence=1&isAllowed=y.

Sisäministeriö (2022a, 25. marraskuuta). *Sisäisen turvallisuuden rahastosta (ISF) rahoitetut hankkeet.* Noudettu 5.11.2025 osoitteesta https://eusa-rahastot2021.fi/documents/96414315/142767238/Rahoitetut+ISF-hankkeet+25.11.22.pdf/00ce1795-f66c-0c1f-8c3c-7691a7bb7a99/Rahoitetut+ISF-hankkeet+25.11.22.pdf?t=1670493078939.

Tilastokeskus (2025). *Tietoon tulleet rikokset ja niiden selvittäminen rikosnimikkeittäin muuttujina Vuosi, Viranomainen, Rikos ja Tiedot.* Noudettu 5.11.2025 osoitteesta

https://pxdata.stat.fi/PxWeb/pxweb/fi/StatFin/StatFin__rpk/statfin_rpk_pxt_13gw.px/table/tableViewLayout1/.

Tolvanen, M., (2013). Rikosprosessuaaliset pakkokeinot aineettomiin oikeuksiin kohdistuvien rikosten tutkinnassa, estämisessä ja paljastamisessa. *Lakimies 7–8/2013,* s. 1296–1318. Edilex

UNODC. (2013). *COMPREHENSIVE STUDY ON CYBERCRIME - Draft February 2013*. Noudettu 29.9.2025 osoitteesta https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Valtioneuvosto (2024), *Suomen kyberturvallisuusstrategia 2024–2035,* Noudettu 8.10.2025 osoitteesta https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165860/VNK_2024_11.pdf?sequence=1&isAllowed=y.

Vuorenpää, M., Helenius, D., Hietanen-Kunwald, P., Hupli, T., Koulu, R., Lappalainen, J., Lindfors, H., Niemi, J., Rautio, J., Saranpää, T., Turunen, S., & Virolainen, J. (2021). *Prosessioikeus* (Kuudes, uudistettu painos). Alma Talent.

Yar, M., & Steinmetz, K. F. (2023). *Cybercrime and society*. Sage.

Virallislähteet

HE 146/2000 vp. Hallituksen esitys Eduskunnan laeiksi tietoyhteiskunnan palvelujen suojasta sekä rikoslain 38 luvun ja eräiden viestintälakien muuttamisesta.

HE 153/2006 vp. Hallituksen esitys Eduskunnalle Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen hyväksymisestä, laiksi sen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta sekä laeiksi rikoslain, pakkokeinolain 4 luvun, esitutkintalain 27 ja 28 §:n ja kansainvälisestä oikeusavusta rikosasioissa annetun lain 15 ja 23 §:n muuttamisesta.

HE 222/2010 vp. Hallituksen esitys Eduskunnalle esitutkinta- ja pakkokeinolainsäädännön uudistamiseksi

HE 224/2010 vp. Hallituksen esitys Eduskunnalle poliisilaiksi ja eräiksi siihen liittyviksi laeiksi

HE 221/2013 vp. Hallituksen esitys eduskunnalle tietoyhteiskuntakaareksi sekä laeiksi maankäyttö- ja rakennuslain 161 §:n ja rikoslain 38 luvun 8 b §:n muuttamisesta.

HE 232/2014 vp. Hallituksen esitys eduskunnalle laiksi rikoslain eräiden tietoverkkorikoksia koskevien säännösten muuttamisesta ja eräiksi siihen liittyviksi laeiksi.

HE 217/2022 vp. Hallituksen esitys eduskunnalle laeiksi pakkokeinolain ja esitutkintalain muuttamisesta sekä niihin liittyviksi laeiksi

HE 275/2022 vp. Hallituksen esitys eduskunnalle laiksi poliisilain muuttamisesta

HE 105/2023 vp. Hallituksen esitys eduskunnalle laiksi rikoslain muuttamisesta sekä eräiksi muiksi laeiksi

LaVM 29/2014 vp.

PeVL 98/2022 vp.

Oikeustapaukset

Helsingin HO 21.3.2014 Diaarisalainen

KKO: 2003:36

KKO: 2022:23

Itä-Suomen HO 25.9.2018/496

Ylimpien laillisuusvalvojien ratkaisut

Oikeuskanslerin lausunto OKV/348/21/2022