VAASAN YLIOPISTO

KAUPPATIETEELLINEN TIEDEKUNTA

LASKENTATOIMEN JA RAHOITUKSEN AKATEEMINEN YKSIKKÖ

Marika Sihto

MYYNTIPETOKSET

Internetin kauppasivustoilla tapahtuvat petokset

Talousoikeuden
pro gradu -tutkielma

VAASA 2019

SISÄLLYS

KUVIO- JA TAULUKKOLUETTELO

LYHENTEET

EC3	*European Cyber Crime Centre*
EU	Euroopan unioni
EUCTF	*European Union Cybercrime Task Force*
ETS	*European Treaty Series*
GB	*Gigabyte* (Gigatavu)
GCI	*Global Cybersecurity Index*
GDPR	*General Data Protection Regulation*
ICT	*Information and Communications Technology* (Tieto- ja viestintätekniikka)
IOCTA	*Internet Organised Crime Threat Assessment*
IoT	*Internet of Things*
ITU	*International Telecommunications Union*
KKV	Kilpailu- ja kuluttajavirasto
KRP	Keskusrikospoliisi
M2M	*Machine-to-machine*
NIS	*Network and Information Systems*
NCS	*National Cybersecurity Strategy* (Kansallinen kyberturvallisuusstrategia)
OECD	*Organisation for Economic Cooperation and Development*
PIN	*Personal Identification Number*
RTN	Rikoksentorjuntaneuvosto
SopS	Suomen säädöskokoelman sopimussarja
TOR	*The Onion Router*
UNODC	*United Nations Office on Drugs and Crime*
UNTOC	*United Nations Convention against Transnational Organised Crime*
WLAN	*Wireless Local Area Network*
YK	Yhdistyneet kansakunnat
YJT	Yleinen järjestys ja turvallisuus
YTS	Yhteiskunnan turvallisuusstrategia

VAASAN YLIOPISTO

Laskentatoimen ja rahoituksen akateeminen yksikkö
Tekijä: Marika Sihto
Pro gradu -tutkielma: Myyntipetokset:
Internetin kauppasivustoilla tapahtuvat petokset
Tutkinto: Kauppatieteiden maisteri
Oppiaine: Talousoikeus
Työn ohjaaja: Brita Gyllenbögel
Valmistumisvuosi: 2019 **Sivumäärä: 101**

TIIVISTELMÄ

Tutkimuksen lähtösysäyksenä oli vuosien 2011–2012 aikana tapahtunut petoskokonaisuus, jossa lukuisiin yksityishenkilöiden Huuto.net-kauppasivuston profiileihin murtauduttiin ja niitä hyväksikäyttäen myytiin olemassa olematonta omaisuutta noin 150 000 euron arvosta. Tämän mahdollisti loppuvuodesta 2011 Suomessa tapahtuneet laajat tietovuodot: tuhansien ihmisten käyttäjätunnuksia ja salasanoja vuodettiin nettiin. Poliisissa kyseisen kokonaisuuden hahmottaminen kesti siksikin pitkään, että kokonaisuuteen liittyviä rikoksia tutkittiin yksittäistapauksina ja eri tavoin eikä tietoverkossa tapahtuvista rikoksista ja niiden tutkinnan erityispiirteistä ollut tuolloin vielä paljolti tietoa saati kokemusta. Lisäksi tietoturvasta ei juurikaan puhuttu eikä sitä koettu kovinkaan tärkeäksi asiaksi.

Yhteiskuntamme ja toimintaympäristömme on muuttunut tieto- ja viestintätekniikan (ICT) nopean kehityksen ja sen yleistymisen myötä. Aiemmin tietotekniikkaa hyödynnettiin teknisenä apuvälineenä, mutta sen käyttötavat ovat muuttuneet ja monipuolistuneet – ja meidän elinympäristömme kokonaisvaltaisesti sen myötä. Muutos informaatioyhteiskunnasta digitaalisen toimintaympäristön verkkoyhteiskunnaksi on tapahtunut nopeasti. Lisäksi yhteiskuntamme monet elintärkeät toiminnot ovat jo täysin riippuvaisia tietoteknisten järjestelmien ja niistä muodostuvan kybertoimintaympäristön toiminnasta sekä sen toimintavarmuudesta. Turvallisuusympäristö on monimutkaistunut ja muuttunut pysyvästi. Kohdatut haasteet ovat globaaleja. Rajojen merkitys häviää ja yhteistyön merkitys korostuu.

Lähes kaikki suomalaiset käyttävät internetiä. Monet perinteiset toiminnot ovat siirtyneet verkkoon: Suurin osa viranomais- ja pankkiasioinnista tapahtuu nykyään sähköisesti. Kaupat on siirtyneet pitkälti verkkomyyntiin ja myös kuluttajien välinen kaupankäynti netin eri kauppasivustoilla lisääntyy. Myös rikollisuutta ja turvallisuusuhkia esiintyy yhä enenevässä määrin tietoverkoissa. Tarvitsemme rikosoikeudellista suojaa myös verkossa. Poliisin tulee ennalta estää, paljastaa ja selvittää rikoksia myös netissä; rikosten tekemisen helppous ja poliisin määrän väheneminen pakottavat poliisin uudistamaan toimintatapojaan. Tietoturvallisuus ja laajemmin kyberturvallisuus eli digitaalisen maailman turvallisuus on tänä digitaalisena aikana maailmanlaajuisesti keskeisessä asemassa.

Tietotekniikan kehitys antaa myös aiheen uudistaa lainsäädäntöä. Perinteisiä rikoksia tehdään verkossa, uusia oikeudellisia kysymyksiä ilmenee jatkuvasti eikä aiempi sääntely kata uusia rikoksia tai rikosten tekotapoja digitaalisessa ympäristössä. Tähän havahduttiin niin YK:ssa kuin EU:ssakin ottamalla tietoverkot ja tietojärjestelmät erityissääntelyn kohteeksi. Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus ETS 185 (tietoverkkorikossopimus eli Budapestin sopimus) vuodelta 2001 on edelleen ainoa erityisesti tietoverkkorikollisuutta käsittelevä kansainvälinen sopimus. Sen johdosta Suomessakin aiemmin tietotekniikkaneutraalia lainsäädäntöä on ajantasaistettu. Haluan tutkielmallani valottaa tätä laajaa aihepiiriä ja selkiinnyttää eri käsitteitä. Toivon tietoverkkoihin liittyvän rikollisuuden tietoisuuden kasvavan ja myyntipetosten määrän vähenevän tämän tutkielman myötä.

AVAINSANAT: Myyntipetos, nettipetos, ICT, tietoverkkorikollisuus, kybertoimintaympäristö.

1. JOHDANTO

1.1. Tutkimuksen lähtökohdat

Suomi on yksi kehittyneimmistä yhteiskunnista, jonka toiminnat ovat riippuvaisia erilaisista sähköisistä verkoista ja niiden antamista palveluista. Yhteiskunnan palvelut tarjotaan sähköisinä, ja ne rakentuvat digitaalisista verkoista[1]. Tietotekniikan laaja-muotoinen hyödyntäminen on vakiintunut osa arkipäivän toimintoja[2]: vuonna 2018 tietoverkkoa eli internetiä käytti 16–89-vuotiaista suomalaisista 89 prosenttia ja alle 55-vuotiaista lähes kaikki käyttävät internetiä[3]. Suomi on riippuvainen tietoverkkojen ja tietojärjestelmien toiminnasta ja myös erittäin haavoittuvainen niihin kohdistuville häiriöille. Kansainvälisesti tästä sähköisessä muodossa olevan tiedon käsittelyyn tarkoitetusta ympäristöstä, joka muodostuu tietojärjestelmistä, on ryhdytty käyttämään termiä kybertoimintaympäristö.[4] Yhteiskuntamme monet toiminnot ovat riippuvaisia tietoteknisten järjestelmien ja niistä muodostuvan kybertoimintaympäristön toiminnasta ja toimintavarmuudesta[5]. Tietojärjestelmien ja tietoverkkojen häiriöttömän toiminnan varmistaminen on ehdoton edellytys sille, että yhteiskunnan perustoimintojen jatkuminen voidaan turvata[6].

Tietoturvallisuudella tarkoitetaan järjestelyjä, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus. Perinteisen tietoturvallisuuden rinnalle on 2010-luvulla noussut kyberturvallisuuteen liittyvä käsite, joka kuvastaa samalla toimintaympäristöön kohdistuvissa uhkissa tapahtunutta muutosta. Kyberturvallisuuden avulla pyritään huolehtimaan sähköisen, digitaalisen toimintaympäristön kokonais-turvallisuudesta. Se kattaa digitaalisessa toimintaympäristössä olevien tietojen ja palveluiden tietoturvallisuuden ohella myös tarvittavan muun toiminnan, etenkin kriittisen infrastruktuurin toiminnan: energian tuotanto ja jakelu, tietoyhteiskunnan palvelut, logistiikka ja finanssiala, samoin toiminnassa tarvittavan henkilöstön.[7] Kyber-turvallisuus on tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Sen voidaan ajatella olevan sama kuin digitaalisen maailman turvallisuus.[8]

---

[1] Kodin kyberopas 2017: 1.
[2] Saarenpää 2016: 28.
[3] Suomen virallinen tilasto 4.12.2018.
[4] Suomen kyberturvallisuusstrategia 2013: 1.
[5] HE 153/2006 vp: 4.
[6] Turvallisuuskomitea 2015: 116.
[7] Valtiovarainministeriö 2018: 15.
[8] Suomen kyberturvallisuusstrategia 2013: 13.

Sisäinen turvallisuus on valtion perustehtäviä. Sisäistä turvallisuutta ylläpitämällä ennaltaehkäistään ja torjutaan Suomeen ja sen väestöön kohdistuvia rikoksia, onnettomuuksia ja ympäristövahinkoja tai muita vastaavia häiriöitä ja uhkia sekä hallitaan niiden seuraukset[9]. Keskeiset sisäisen turvallisuuden ylläpidosta vastaavat viranomaiset ovat poliisi-, rajavartio-, tulli-, pelastus-, oikeus- ja vankeinhoitoviranomaiset, jotka toimivat myös yhteiskunnan normaalioloissa koko ajan operatiivisissa tehtävissä[10]. Sisäisestä turvallisuudesta ei ole olemassa yhtä selkeästi vakiintunutta määritelmää, mutta se on laajentunut kattamaan uhkien torjunnan lisäksi yksilöiden mahdollisuuden nauttia oikeusjärjestelmän hänelle suomista oikeuksista ja vapauksista sekä turvallisesta yhteiskunnasta ilman aiheellista pelkoa tai turvattomuutta; tähän sisältyvät sekä turvallisuustilanne että ihmisten kokema turvallisuuden tunne. Käsite on näin ollen laajentunut kattamaan muutakin kuin vain sisäministeriön hallinnonalan turvallisuustehtävän ja toimijakentän.[11] Valtioneuvoston tekemä ensimmäinen sisäisen turvallisuuden ohjelma 23.9.2004 ylitti viranomaisten sektorirajat[12].

Perinteisesti on ajateltu, että sisäisestä turvallisuudesta huolehtii poliisi ja ulkoisesta turvallisuudesta puolustusvoimat[13]. Sisäisen turvallisuuden perusta muodostuukin poliisin operatiivisesta toimintakyvystä koko maassa: suurin osa sisäisen turvallisuuden viranomaisten hälytystehtävistä on poliisitehtäviä, minkä lisäksi poliisi tutkii lähes kaikki viranomaisten tietoon tulleet rikokset. Sisäinen turvallisuus ei kuitenkaan ole vain operatiivisten viranomaisten toimintaa vaan sitä luovat myös yhteiskunnan arvot, kuten perus- ja ihmisoikeudet, sananvapaus, tasapuolinen oikeusjärjestelmä, tasa-arvo sekä yhdenvertaisuus. Henkilökohtaista turvaa suomalaisille tuovat elämän peruspilarit eli perhe, läheiset ja muut ihmissuhteet, oma koti, toimeentulo, työ ja terveys. Turvallisuuden tunteeseen vaikuttavat viranomais- ja palvelurakenteet (poliisi, pelastustoimi, sosiaali- ja terveystoimi, eläke ja koulutus) sekä valtiolliset tekijät (rauhallinen, turvallinen, itsenäinen ja demokraattinen maa).[14]

Sisäministeriön[15] alaisen poliisitoimen yhteiskunnallisena vaikuttavuustavoitteena on turvata oikeus- ja yhteiskuntajärjestystä, ylläpitää yleistä järjestystä ja turvallisuutta

[9] Yhteiskunnan turvallisuusstrategia 2017: 19.
[10] Turvallisuuskomitea 2018: 74.
[11] Sisäministeriö 2017a: 10-11; Turvallisuuskomitea 2015: 23.
[12] Valtioneuvoston periaatepäätös 23.9.2004.
[13] Sisäministeriö 2017a: 10.
[14] VNS 5/2016: 2, 8, 48.
[15] Vuoden 2014 alusta ministeriön nimi muuttui sisäasiainministeriöstä sisäministeriöksi.

(YJT)[16] sekä ehkäistä ennalta rikoksia, selvittää niitä ja saattaa ne syyteharkintaan; nämä ovat samalla myös poliisin lakisääteiset tehtävät[17]. Poliisitoimi jaetaan valvonta- ja hälytystoimintaan (järjestyspoliisi), rikostorjuntaan (rikospoliisi) ja lupahallintoon. Käytännössä poliisitoiminnan ydin on rikosten torjunnassa – sen laajassa merkityksessä. Poliisille on säädetty velvollisuus ennalta estää ja tutkia kaikkia rikoksia. Rikoksiksi on laissa määritelty sellaiset teot, jotka loukkaavat oikeus- ja yhteiskuntajärjestystä tai yleistä järjestystä ja turvallisuutta. Niin liikennevalvonta, hälytystehtävien hoitaminen, näkyvä partiointi asuinalueilla, koulupoliisitoiminta kuin rikoksesta epäillyn tarkkailukin tähtäävät kaikki viime kädessä rikosten torjuntaan, joko ennalta estävästi tai edistämällä rikoksen selvittämistä. Lupahallinnolla on silläkin tärkeä rooli rikosten torjunnassa: muun muassa henkilöllisyystodistusten antaminen oikein tiedoin ja aselupien tarkka harkinta vähentävät rikosten vaaraa, kun taas yleisötilaisuuslupaharkinta voi puolestaan ennaltaestää järjestyshäiriöitä ja jopa vakavien väkivaltarikosten mahdollisuutta.[18]

Valtiomme on muuttunut pohjoismaisesta, kansalaisia paljolti alistaneesta ja ohjanneesta hallintovaltiosta eurooppalaiseksi oikeusvaltioksi, jossa kunnioitetaan selkeämmin yksilön itsemääräämisoikeutta. Perinteisessä jälkiteollisessa yhteiskunnassa tietotekniikkaa hyödynnettiin jossain määrin teknisenä apuvälineenä, mutta tietotekniikan käyttö yleistyi ja monipuolistui, jolloin tästä tietokoneistuvasta yhteiskunnasta aloitettiin käyttää nimitystä informaatioyhteiskunta. Infrastruktuuri (erityisesti informaatioinfrastruktuuri), informaatio ja sen laadun merkitys sekä tietotekniikan eri käyttötavat ovat muuttaneet oleellisella tavalla ympäristömme. Nykyisessä digitaalisen toimintaympäristön verkkoyhteiskunnassa lakisääteisyyden merkitys kasvaa: yhä useammasta asiasta säädetään lailla. Tietotekniikan kehitys ja oikeudelliset kysymykset näkyvät verkkoyhteiskunnassa esimerkiksi tekijänoikeuksiin, sähköiseen kauppaan ja verkkomyyntiin sekä henkilötietojen ja digitaalisen identiteetin suojaan liittyvinä ongelmina.[19]

---

[16] Yleisen järjestyksen ja turvallisuuden alaan on katsottu kuuluvan ainakin kaiken sellaisen poliisitoiminnan, jonka tarkoituksena on luoda ja ylläpitää turvallista elin- ja toimintaympäristöä yhteiskunnan jäsenille, torjua ja estää ennakolta oikeudenloukkauksia ja häiriöitä sekä poistaa tapahtuneet häiriöt ja selvittää tapahtuneet oikeudenloukkaukset. HE 224/2010 vp: 70−71.

[17] Poliisilaki PoL (22.7.2011/872) 1 § Poliisin tehtävät. Poliisin tehtävänä on oikeus- ja yhteiskuntajärjestyksen turvaaminen, yleisen järjestyksen ja turvallisuuden ylläpitäminen sekä rikosten ennalta estäminen, paljastaminen, selvittäminen ja syyteharkintaan saattaminen.

[18] VNS 5/2016: 48–49.

[19] Saarenpää 2016: 24– 25, 28–31, 50, 59.

Tietotekniikan kehitys on johtanut digitaaliseen toimintaympäristöön, jonka ytimen muodostavat sähköisessä muodossa olevat tiedot. Tietotekniikka ei ole enää vain tekninen apuväline sekä yksilöille että organisaatioille, vaan olemme käytännössä yhä enemmän sidoksissa tuohon toimintaympäristöön ja sen asianmukaiseen käyttöön. Eri toimintoja suunniteltaessa oletusarvoksi on noussut toiminta verkkojen ja päätteiden avulla. Digitaaliseen arkeemme kuuluu tiedon ja palveluiden hyödyntäminen ilman sitoutumista aikaan tai paikkaan.[20] Suomalaiset käyttävät internetiä asioiden hoitamiseen, viestintään, medioiden seuraamiseen ja tiedonhakuun. Asioinnista yleisintä on verkkopankin käyttö: vuonna 2018 väestöstä käytti verkkopankkia 83 prosenttia. Verkossa osti tavaroita tai palveluita 47 prosenttia väestöstä. Viranomais- ja muita julkisia palveluita käytetään yhä enemmän internetin kautta ja niiden verkkosivuilta haetaan myös yleisesti tietoa. Internet on nykyisellään muutoinkin melkein kaiken tiedon lähde: suomalaiset hakevat tietoa erityisesti tavaroista ja palveluista sekä terveyteen, sairauksiin ja ravitsemukseen liittyvää tietoa. Myös netin joukkoviestimiä, verkkolehtiä ja televisioyhtiöiden uutissivuja, luetaan ja eri yhteisöpalveluja käytetään. Netin viestintätavoista yleisin on edelleen sähköposti, mutta pikaviestintätavat ovat nekin usean suomalaisen käytössä.[21] Sähköinen vertaisverkkokauppa eli kuluttajien välinen kauppa verkossa on noussut taloudellisesti merkittäväksi asiaksi.[22]

Tietoturva, yksityisyyden suoja, omaisuuden suoja sekä tieto- ja viestintäteknologia-alan yleinen ohjaus ovat korvaamattomia rakennettaessa ihmisten luottamusta tieto-yhteiskuntaa kohtaan. Tietoturvallisuus on tavoitetila, jossa tiedot, järjestelmät ja palvelut saavat asianmukaista suojaa niiden luottamuksellisuuteen, eheyteen ja käytettävyyteen kohdistuvia uhkia ja vahinkoja vastaan. Uhkia aiheuttavat niin laitteisto- ja ohjelmistoviat sekä luonnontapahtumat kuin tahalliset, tuottamukselliset ja tapaturmaiset inhimilliset teot.[23] Suojaa tietoturvallisuudelle annetaan lainsäädännön ja muiden toimenpiteiden avulla. Yhdistyneet kansakunnat (YK) tunnisti 1990-luvulla tietotekniikan väärinkäytön valtioiden rajat ylittäväksi rikokseksi[24]. Euroopan unioni (EU) käynnisti vuonna 1999 eEurope – Tietoyhteiskunta kaikille -aloitteen, jonka tavoitteena oli tietotekniikan levittäminen mahdollisimman laajalle ja joka korosti sekä verkkoturvallisuuden merkitystä että tietoverkkorikollisuuden torjuntaa[25]. Vuoden 2001 kuluessa internetin käyttö lisääntyi nopeasti Euroopassa, jolloin kävi ilmi, että verkko-

[20] Kodin kyberopas 2017: 1; Saarenpää 2016: 28, 31; Turvallisuuskomitea 2015: 116.
[21] Suomen virallinen tilasto 04.12.2018.
[22] Saarenpää 2016: 25.
[23] HE 233/1997: 4.
[24] Suomen kyberturvallisuusstrategia 2013: 33.
[25] Komission tiedonanto 8.12.1999.

ja tietoturva ovat keskeisiä tekijöitä taloudellisessa ja yhteiskunnallisessa kehityksessä. Suomessa hallintovaliokunta totesi tuolloin, että tieto- ja viestintäverkoista oli tullut yksi talouden keskeisistä tekijöistä, joten "tietokonerikollisuuden ennaltaehkäiseminen on tärkeää".[26]

Kun sisäisen turvallisuuden ohjelma käsittelee niin sanottujen normaaliolojen sisäistä turvallisuutta, linjattiin yhteiskuntamme varautumisen[27] eli poikkeusolojen toiminnan yleisperiaatteet valtioneuvoston periaatepäätöksenä poikkihallinnollisena strategiana ensimmäisen kerran vuonna 2003 (Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia) ja sitä päivitettiin seuraavan kerran vuonna 2006. Vuonna 2010 strategian nimi muutettiin Yhteiskunnan turvallisuusstrategiaksi[28] (YTS).[29] Sen myötä aloitettiin kansallisen kyberstrategian laatiminen[30]. EU:n kyberturvallisuusstrategia hyväksyttiin vuonna 2013 ja samana vuonna valtioneuvosto hyväksyi Suomen kyberturvallisuus-strategian[31], jonka mukaan turvallinen kybertoimintaympäristö helpottaa yksilöiden ja yritysten oman toiminnan suunnittelua, mikä puolestaan lisää taloudellista aktiviteettia. Strategisina linjauksina mainittiin muun muassa tehokkaan kyberturvallisuuden toteuttamisen edellytysten varmistaminen kansallisella lainsäädännöllä. Lisäksi tuli huolehtia siitä, että poliisilla on tehokkaat edellytykset ennalta ehkäistä, paljastaa ja selvittää kybertoimintaympäristöön kohdistuvia ja sitä hyödyntäviä rikoksia.[32]

Rikos on laissa rangaistavaksi säädetty inhimillinen – eli ihmisen tekemä – teko[33]. Suomessa rikosten sisältö ja rangaistavuus määritellään pääasiassa rikoslaissa (RL 19.12.1889/39), jolloin puhutaan niin sanotuista rikoslakirikoksista. Näitä ovat muun muassa omaisuusrikokset, henkeen ja terveyteen kohdistuneet rikokset, seksuaali-rikokset, rikokset oikeudenkäyttöä, viranomaista ja yleistä järjestystä vastaan, eräät liikennerikokset (rattijuopumukset) ja huumausainerikokset. Rikoslaki ei kuitenkaan yksinään luettele kaikki rikoksia vaan myös useissa muissa laeissa säädetään rikoksista ja rikkeistä, esimerkkinä tieliikennelain, ampuma-aselain ja järjestyslain vastaiset teot.

[26] Euroopan yhteisöjen komissio 2003: 5, 10; HaVL 5/2001 vp.
[27] Varautuminen on toiminta, jolla varmistetaan tehtävien mahdollisimman häiriötön hoitaminen ja mahdollisesti tarvittavat tavanomaisesta poikkeavat toimenpiteet häiriötilanteissa ja poikkeusoloissa. Yhteiskunnan turvallisuusstrategia 2017: 94.
[28] Valtioneuvoston periaatepäätös 16.12.2010.
[29] Valtioneuvoston periaatepäätös 23.9.2004:15; Yhteiskunnan turvallisuusstrategia 2017: 5.
[30] Kyber-etuliitteellä varustetut termit kuten kyberturvallisuus, kyberrikos, kyberhyökkäys ja kybersota tulivat laajempaan käyttöön Suomessa sen jälkeen, kun kansallisen kyberstrategian laatiminen aloitettiin vuonna 2011. Sisäministeriö 2017b: 11.
[31] Valtioneuvoston periaatepäätös 24.1.2013.
[32] Suomen kyberturvallisuusstrategia 2013: 1, 8, 10.
[33] Tapani & Tolvanen 2013: 3.

Noin kahdesta viiteen prosenttia väestöstä tekee yli puolet rikoslakirikoksista. Rikokset keskittyvät siten pienelle tekijäjoukolle, jolla on usein heikkoon sosioekonomiseen asemaan, päihteisiin, syrjäytymiseen tai mielenterveyteen liittyviä ongelmia. Tämän ryhmän tekemät rikokset ovat lisäksi luonteeltaan sellaisia, jotka näkyvät yhteiskunnassa ja jotka vaikuttavat ihmisten turvallisuuden tunteeseen: vahingontekoja, pahoinpitelyjä ja omaisuusrikoksia.[34]

Tieto- ja viestintätekniikan (ICT) verkostot, laitteet ja palvelut ovat yhä tärkeämpiä päivittäisessä elämässämme. Mutta kuten todellinen, fyysinen maailma, niin myös kybermaailma on alttiina erilaisille turvallisuusuhkille, jotka voivat aiheuttaa valtavia vahinkoja.[35] Haitat, väärinkäyttöyritykset ja rikollinen toiminta ovat valitettavasti myös osa verkon arkea: rikollisuutta ja muita turvallisuusuhkia esiintyy myös tietoverkoissa. Tietoverkkorikollisuus onkin osa tietoyhteiskunnan nurjaa puolta. Tietotekniikan käyttö ei tarjoa pelkästään valtavia etuja yhteiskunnalle, vaan myös tilaisuuden tehdä uudenlaisia rikoksia taikka perinteisiä rikoksia uusilla välineillä.[36] Yhteiskunnan muuttumisen myötä rikollisuus on siirtynyt enenevässä määrin tietoverkkoon (internetiin). Digitalisaation hyödyt ovatkin luotettavasti käytettävissämme vain, jos samalla varmistetaan tietojärjestelmien toiminta ja huolehditaan kyberturvallisuudesta. Turvallisuusympäristö on lisäksi monimutkaistunut ja muuttunut pysyvästi – ja myös sen ennustettavuus on heikentynyt. Globaalit haasteet korostavat yhteistyön merkitystä niin ympäristöuhkien, verkkorikollisuuden, rajat ylittävän rikollisuuden, laittoman maahantulon kuin terrorisminkin torjumisessa.[37]

Tietotekniikan kehitys antaa luonnollisesti aiheen uudistaa ja ajantasaistaa sääntelyä ja se näkyy vääjäämättä myös rikosoikeudellisessa sanktiosääntelyssä, sillä aiempi sääntely ei kata riittävästi uusia rikosten tekotapoja digitaalisessa toimintaympäristössä; tietoverkkorikollisuudella on paikkansa rikoslaissa säänneltyjen rikosten joukossa[38]. Ensimmäiset tietotekniikkarikoksia koskevat säännökset tulivat Suomessa voimaan vuonna 1991 osana rikoslain kokonaisuudistusta (RL 24.8.1990/769), jolloin muutettiin luvattoman käytön, petoksen, vahingonteon ja väärennyksen tunnusmerkistöjä käsittämään myös automaattisen tietojenkäsittelyn mahdollistamat teot (HE 66/1988).[39] Yhteiskunnan kehitys ja muutokset synnyttävät uusia oikeudellisia ongelmia, joihin on

[34] VNS 5/2016: 9.
[35] ITU 2017: 1.
[36] Tietosuojaryhmä 2001: 2.
[37] Kodin kyberopas 2017: 1; VNS 5/2016: 11, 13.
[38] Saarenpää 2016: 26.
[39] HE 94/1993: 1.12.1.1. Systematiikka ja sääntelyn tarve.

puututtava lainsäädännön keinoin. Sääntelyn muuttaminen vastaamaan toiminta-ympäristön realiteetteja vie aikaa – ja tuolloin kehityksen myötä syntyy jo taas uusia ongelmia, joihin lainsäätäjän on puututtava. Lainsäädäntö ei siten koskaan ole niin sanotusti ajan tasalla.

Tietoverkko on rikollisille edullisempi ja riski-hyöty/riski-vahinko -suhteessa entistä houkuttelevampi ympäristö toteuttaa rikoksia, joilla on taloudellinen tai jopa terroristinen tavoite. Myös perinteisiä rikoksia, kuten petoksia, lasten seksuaalista hyväksikäyttöä ja teollisuusvakoilua tehdään yhä enemmän kybertoimintaympäristössä. Tietoverkkorikosten määrät ovat lisääntyneet merkittävästi ja ne tulevat jatkossakin lisääntymään. Itse asiassa tuottoisin rikollisuus toimii tietoverkoissa ja etenkin verkossa tapahtuvien petosrikosten määrät ovat kasvaneet. Lisäksi tietotekniikan kehittyminen on luonut uusia mahdollisuuksia petoksiin ja muuhun rikolliseen toimintaan. Toimimme verkostoituneessa yhteiskunnassa osana globalisoituvaa maailmaa[40]. Verkkoyhteis-kunnassa myös maantieteellisten rajojen fyysinen vaikutus vähenee[41]. Tietoverkko-rikollisuus onkin suurelta osin rajat ylittävää rikollisuutta[42]. Siitä on tullut hyvin kattava rikollisuuden osa-alue ja sen vaikutukset kohdistuvat niin valtioihin, yksityisiin kansalaisiin kuin liiketoimintaankin.[43]

1.2. Tutkimustehtävä ja rajaukset

Omaisuusrikos on rikos, joka kohdistuu omaisuuteen: niitä ovat esimerkiksi varkaudet, kavallukset, petokset ja vahingonteot. Suurimman omaisuusrikosryhmän muodostavat varkausrikokset (varkaus RL 28:1 §, törkeä varkaus RL 28:2 § ja näpistys RL 28:3 §) ja niiden määrä on ollut laskussa koko 2000-luvun. Petosrikosten määrä on ollut Suomessa selvässä kasvussa 2010-luvulla ja kasvun vaikutukset ulottuvat viranomaisten lisäksi laajalti tavallisiin kansalaisiin. Yleinen tietotekniikan kehitys, verkkoasioinnin lisääntyminen niin tuotteiden ostamisessa kuin pankkipalveluissa sekä rikosten uhrien ilmoitusaktiivisuus selittävät petosrikollisuuden voimakasta kasvua. Normaalisti petos-rikoksilla tarkoitetaan rikoslain 36 luvun 1–3 pykälissä kriminalisoituja tekoja, joita ovat petos, törkeä petos ja lievä petos, sekä 37 luvun 8–11 pykälien maksuvälineiden käyttöön liittyviä petoksia eli maksuvälinepetosta ja sen törkeää ja lievää tekomuotoa[44]

[40] Valtiovarainministeriö 2018: 12.
[41] Saarenpää 2016: 28.
[42] HE 153/2006: 4.
[43] Sisäministeriö 2017b: 5, 7, 22; Suomen kyberturvallisuusstrategia 2013: 27.
[44] Oikeusministeriö 2017: 12.

(vaikkakin rikoslaissa on kriminalisoitu myös muita petosrikoksia[45]). Poliisin tietoon tullut petosrikollisuus kasvoi lyhyessä ajassa voimakkaasti vuodesta 2010 vuoteen 2016. Tilanne kaikkien petosrikosten osalta parani hieman vuoden 2016 jälkeen.[46]

Oheisessa taulukossa on poliisin vuosina 2010–2016 tilastoimat petokset ja niiden yritykset sekä maksuvälinepetokset lievine ja törkeine tekomuotoineen, samoin kyseisten nimikkeiden muutos prosentteina samalla aikavälillä:

	2010	2011	2012	2013	2014	2015	2016	Muutos 2010→ 2016
Törkeä petos	806	1 027	864	958	1 208	1 224	1 228	+ 52 %
Petos	7 865	9 026	11 092	11 292	10 777	12 561	11 819	+ 50 %
Lievä petos	5 880	6 433	7 144	8 053	8 127	8 890	8 858	+ 51 %
Törkeän petoksen yritys	151	131	196	141	151	243	211	+ 40 %
Petoksen yritys	1 192	1 273	1 732	2 463	3 335	3 348	3 139	+ 163 %
Törkeä maksu-välinepetos	124	147	126	122	123	194	161	+ 30 %
Maksuvälinepetos	3 876	5 5053	5 546	6 690	6 699	9 199	12 195	+ 215 %
Lievä maksu-välinepetos	448	458	548	788	946	1 581	2 754	+ 515 %

Taulukko 1. Poliisin tilastoima petosrikollisuus, poislukien vakuutuspetokset, vuosina 2010–2016 ja sen kehitys kyseisellä aikavälillä. (Oikeusministeriö 2017: 13.)

Omaisuusrikosten määrä on kaikkinensa vähenemässä: vuonna 2017 niitä tuli poliisin, tullin ja rajavartiolaitoksen tietoon 210 700, mikä oli 8,6 prosenttia vähemmän kuin vuonna 2016; vuonna 2018 omaisuusrikoksia tuli tietoon 205 100, eli laskua 2,7 prosenttia; vuonna 2019 suunta on edelleen alaspäin, sillä vuoden ensimmäisen neljänneksen aikana (tammi–maaliskuu) tapauksia tuli tietoon 41 000, mikä on 4,2 prosenttia vähemmän kuin edellisvuonna vastaavaan aikaan. Omaisuusrikosten suurimman ryhmän muodostavien varkausrikosten määrä laskee edelleen: 125 400 tapausta vuonna 2017, 122 000 tapausta vuonna 2018 ja vuoden 2019 tammi–maaliskuussa 22 400 tapausta, mikä on 5,4 prosenttia vähemmän kuin samana ajanjaksona

[45] Petosrikoksia ovat rikoslain 36 luvussa Petoksesta ja muusta epärehellisyydestä sanktioidut petos RL 36:1 §, törkeä petos RL 36:2 §, lievä petos RL 36:3 § ja vakuutuspetos RL 36:4 § sekä rikoslain 37 luvussa Maksuvälinerikoksista sanktioidut maksuvälinepetos RL 37:8 §, törkeä maksuvälinepetos RL 37:9 §, lievä maksuvälinepetos RL 37:10 § ja maksuvälinepetoksen valmistelu RL 37:11 §. Näiden lisäksi rikoslaissa on säädöksiä muistakin petosrikoksista, esimerkiksi rikoslain 29 luvussa Rikoksissa julkista taloutta vastaan sanktioidut veropetokset ja eri vakuutusmaksuihin ja avustuksiin liittyvät petokset sekä rikoslain 39 luvussa Velallisen rikoksista sanktioidut velallisen petokset.

[46] Oikeusministeriö 2017: 5, 9, 12–13.

vuotta aiemmin. Vuonna 2017 petoksia tuli ilmi 23 400, mikä oli 6,8 prosenttia vähemmän kuin vuonna 2016, mutta vuonna 2018 petosrikosten määrä nousi 23 800:aan eli niiden määrä kasvoi 1,9 prosenttia. Vuoden 2019 ensimmäisen neljänneksen aikana petoksia tuli ilmi 6 900 tapausta, mikä on 10,2 prosenttia enemmän kuin vuotta aiemmin – eli petosrikosten määrä näyttäisi olevan lisääntymään päin. Maksuvälinepetoksien määrä on sekin laskusuunnassa[47]: tapauksia tuli ilmi 6 700 vuonna 2017, mikä on 55,9 prosenttia vähemmän kuin vuonna 2016; 6 000 tapausta vuonna 2018 (laskua 10,2 prosenttia) ja vuoden 2019 alkuneljänneksellä 1 300 tapausta, mikä on 13,9 prosenttia vähemmän kuin edellisvuonna vastaavaan aikaan.[48]

Internet on mahdollistanut omaisuusrikoksien tekemisen tietoverkossa niin sanottuina nettipetoksina. Nettipetosten määrä on kasvanut tasaisesti maailmanlaajuisesti ja sama ilmiö on näkynyt Suomessakin 2010-luvulta alkaen. Nettipetokset ovat suosittuja, sillä niillä on mahdollista tavoittaa suuri kohderyhmä, kiinnijäämisriski on pieni ja mahdolliset rikoshyödyt ovat suuret[49]. Nettipetosten yhtenä muotona ovat tällekin tutkimukselle alkusysäyksen antaneet myyntipetokset, joissa myydään yleensä olemassa olematonta omaisuutta erilaisilla vertaisverkkokauppasivustoilla eli internetin osto- ja myyntisivustoilla, kuten Tori.fi- ja Huuto.net-sivustolla sekä esimerkiksi Facebookin eri kirpputoreilla. Yleisimmässä tapauksessa markkinasivustolla on akuutissa rahantarpeessa olevan petollisen myyjän myynti-ilmoitus. Kaupankäynnin yhteydessä ostaja suostuu maksamaan tuotteen myyjän ilmoittamalle tilille saamatta ensin kaupankäynnin kohteena olevaa tuotetta haltuunsa. Kauppasumman maksamisen jälkeen myyjään ei yleensä saakaan enää yhteyttä, eikä ostaja saa ostamaansa tuotetta.

Valtaosa Suomessa ilmitulleista rikoksista on poliisin kirjaamia ja tutkimia[50]. Yleensä ongelman myyntipetosten tutkinnassa aiheuttaa se seikka, että Suomen eri poliisilaitoksiin kirjataan tutkittavaksi yksittäinen rikosilmoitus petoksesta, vaikka myyjä harvemmin syyllistyy vain yhteen tekoon vaan "tehtailee" useita petoksia myymällä yhtä ja samaa tuotetta lukuisille eri henkilöille; netti on tekijälle otollinen ympäristö, sillä sen kautta petoksia voi kohdistaa ympäri maata asuviin potentiaalisiin uhreihin[51]. Mikäli myyjän henkilöllisyys ei ole rikosilmoituksen kirjaamishetkellä tiedossa,

[47] Osaltaan maksuvälinepetoksien määrän vähentymiseen on vaikuttanut Poliisihallituksen ohjeistus, jonka mukaan ulkomailla tapahtuneita rikosasioita ei enää kirjata rikosilmoituksiksi (eli R-ilmoitus) vaan sekalaisilmoituksiksi (niin sanottu S-ilmoitus), sillä kyseisten rikosten tunnusmerkistön mukainen tekopaikka ei ole Suomessa. Oikeusministeriö 2017: 13.
[48] Tilastokeskus 16.3.2018, 17.1.2019 ja 17.4.2019.
[49] Oikeusministeriö 2017: 14.
[50] Rikosilmoituksia kirjaavat myös Tulli ja Rajavartiolaitos.
[51] Oikeusministeriö 2017: 16.

kirjataan ilmoitus poliisin rikosilmoitusjärjestelmässä asianomistajan eli petoksen kohteeksi joutuneen kansalaisen kotipaikkakunnan poliisiin siellä tutkittavaksi. Jos puolestaan myyjä eli rikoksesta epäilty on tiedossa, kirjataan rikosilmoitus rikoksesta epäillyn kotipaikkakunnan poliisin tutkittavaksi.

Myyntipetoksissa suuri osa petollisista myyjistä pitää kauppasummat pieninä, jolloin ostajat eivät useinkaan tee rikosilmoitusta kauppasumman pienuuden takia. Hämmästyttävän suuriakin summia maksetaan – ja menetetään – ilmoittamatta asiasta mihinkään, koska ostaja-maksaja pitää omaa sinisilmäisyyttään ja tyhmyyttään syynä kauppasumman menettämiseen; tosin kauppaan tyytymätön ostaja saattaa antaa kyseisellä markkinapaikalla negatiivista palautetta myyjästä. Suuri osa myyntipetoksiin syyllistyvistä rahoittaa teoillaan päihteiden käyttöään ja pelihimoaan. Myyjä tarvitsee varat käyttöönsä heti, joten hänellä on kiire ja hänellä on myös antaa ostajalle useita vaihtoehtoisia pankkitilejä tai muita maksutapavaihtoehtoja, jotta kauppasumman siirtymisessä myyjän käyttöön ei tulisi pankkien välisistä rahansiirroista aiheutuvaa viivettä ja petollinen myyjä saisi varat käyttöönsä välittömästi.

Jotta myyntipetosten tutkinta olisi tuloksellista, tulisi jo rikosilmoituksen kirjaamis-vaiheessa saada tarpeellinen tieto rikoksesta, muun muassa käytetty kauppapaikka, myyjän käyttämät yhteystiedot sekä erityisesti pankkiyhteystiedot. Lisäksi poliisin olisi esitutkinnassa käytettävä lain sallimia ja tutkinnan kannalta tarpeellisia pakkokeinoja, selvitettävä saman tekijän kaikki myyntipetokset ja tutkittava ne keskitetysti siten, että kokonaisuus saatetaan yhtä aikaa syyttäjälle syyteharkintaan. Näin ei kuitenkaan usein tapahdu, vaan myyntipetoksia tutkitaan valitettavan usein yksittäistapauksina. Myös niistä kirjattujen rikosilmoitusten esitutkinta suoritetaan ja päätetään eri tavoin riippuen tutkintaa suorittavasta paikallispoliisista[52]: osan tutkinta keskeytetään, ellei rikoksesta epäilty ole tiedossa eikä asiaan vaikuttavaa selvitystä ole saatavissa (mitä kyllä yleensä ottaen on saatavissa)[53]; osa esitetään syyttäjälle rajoitettavaksi prosessiekonomiaan vedoten, jotta poliisi, syyttäjä ja tuomioistuin voi paneutua vakavampien rikosten selvittelyyn; osan tutkinta päätetään, mikäli myyjä on saatu palauttamaan kauppasumma asianomistaja-ostajalle; osa saatetaan syyttäjälle syyteharkintaan, mutta tällöinkin

[52] Esitutkintaa suorittaa Suomessa 11 paikallispoliisia (poliisilaitosta): Helsingin, Itä-Uudenmaan, Länsi-Uudenmaan, Hämeen, Kaakkois-Suomen, Lounais-Suomen, Sisä-Suomen, Pohjanmaan, Itä-Suomen, Oulun ja Lapin poliisilaitokset. Kussakin poliisilaitoksessa on yksi pääpoliisias0ema sekä useampia poliisiasemia ja yhteispalvelupisteitä.

[53] Esitutkinta saadaan sen aloittamisen jälkeen tutkinnanjohtajan päätöksellä keskeyttää, jos rikoksesta ei epäillä ketään ja jos asiaan vaikuttavaa selvitystä ei ole saatavissa. Esitutkinnan keskeyttämisestä päätettäessä on erityisesti otettava huomioon epäillyn rikoksen laatu. Esitutkintaa on jatkettava ilman aiheetonta viivytystä, kun edellytyksiä keskeytykselle ei enää ole. Esitutkintalaki 3:13 §.

yleensä siis yksittäisenä tapauksena. Ongelmana on, että poliisissa ei ole yhtenäistä näkemystä, käytäntöä taikka ohjeistusta siitä, miten myyntipetoksien esitutkinta tulisi käytännössä suorittaa.

Petosrikosten ehkäisy on viime vuosina noussut keskeiseksi rikoksentorjunnan ja viranomaistyön haasteeksi Suomessa. Oikeusministeriön yhteydessä toimiva asiantuntija- ja yhteistyöelin, Rikoksentorjuntaneuvosto (RTN), asetti työryhmän selvittämään yksityishenkilöihin kohdistuvan petosrikollisuuden tilannetta ja sen torjuntaa. Työryhmän toimikausi oli 1.3.–31.10.2017. Työryhmä kokosi rikoksentorjuntakatsauksen ja sen yhteyteen eri tahoille kohdistettuja suosituksia petosrikosten ehkäisemiseksi. Työryhmä päätti keskittyä kolmeen petosrikollisuuden aiheeseen niiden yleisyyden, torjuttavuuden ja niistä aiheutuvien rikoshaittojen perusteella. Yksi kolmesta painopisteestä oli tämänkin tutkielman aihe eli internetin eri markkinapaikoilla toteutettavat myyntipetokset; kaksi muuta olivat identiteettivarkaudet ja ikääntyneisiin uhreihin kohdistuvat petokset. Työryhmän mukaan tavalliset kansalaiset ja heidän tietoisuutensa lisääminen ovat keskeisessä asemassa useimpien petostyyppien ehkäisyssä. Myyntipetoksien osalta työryhmä suosittelee internetin markkinapaikkoja varoittamaan käyttäjiään huijauksista, mahdollisuuksien mukaan hyödyntämään niin sanottua välimiespalvelua kaupanteossa ja edellyttämään käyttäjiltään vahvaa sähköistä tunnistautumista. Työryhmän esittämä poliisin uudistettu toimintamalli myyntipetoksiin puuttumiseksi on tämän tutkielman lopussa.[54]

Kun yhteiskunnan riippuvuus tietojärjestelmistä kasvaa, kasvavat turvallisuusriskien lisäksi myös poliisin osaamisvaatimukset[55]. Osaamisen kehittäminen on eräs tärkeimmistä poliisihallinnon tehtävistä ja poliisilla tulee olla sekä osaava että motivoitunut henkilöstö, joka hoitaa kybertoimintaympäristössä tapahtuvien rikosten ennaltaehkäisemisen, taktisen esitutkinnan sekä digitaalisen todistusaineiston käsittelyn ja analysoinnin oikeusvarmalla tavalla[56]. Nyttemmin on siirrytty käyttämään tilisiirtojen lisäksi tai niiden sijaan erilaisia mobiilimaksuja, joilla rahansiirto eri pankkien välillä onnistuu helposti ja viiveettä. Toisinaan maksun välineenä käytetään virtuaalisia valuuttoja eli niin sanottuja kryptovaluuttoja (muun muassa bitcoin), joilla on käteisrahan kaltainen anonymiteetti. Ne asettavat uudenlaisia vaatimuksia rikostutkinnalle[57].

[54] Oikeusministeriö 2017: 9–11, 38.
[55] Poliisihallitus 2015a: 3.
[56] Sisäministeriö 2017b: 5, 7.
[57] Sisäministeriö 2017b: 13.

Tutkimustehtäväni on kuvailla nyky-yhteiskuntaamme osana kybertoimintaympäristöä, samoin siellä tapahtuvaa rikollisuutta. Selvitän tässä tutkimuksessa laajaa kybertoimintaympäristön käsitettä sekä systematisoin tietoverkkoihin liittyvää rikollisuutta ja rikosoikeudellista kehitystä. Analysoin vuonna 2012 ilmitullutta, laajaa Huuto.net-verkkokauppasivustoon liittyvää petoskokonaisuutta, joka antoi lähtösysäyksen tälle tutkielmalle. Paneudun tarkemmin myyntipetoksiin ja niiden tapahtumapaikkaan, vertaisvarkkokauppaan, esittellen samalla myös lyhyesti kaksi Suomen suosituinta internetin markkinapaikkaa eli Huuto.netin ja Tori.fi-sivuston. Lisäksi selvitän rikostutkintaa ja rikosprosessia sekä myyntipetosten esitutkintaa. MTV3 uutisoi 10.3.2019, että internetissä tapahtuva käytetyn tavaran myynti kasvaa (edelleen) jatkuvasti suomalaisten ostaessa ja myydessä yhä innokkaammin käytettyä tavaraa internetin markkinapaikoilla – ja lähes samaa tahtia lisääntyvät myös verkossa tapahtuvat huijaukset. Tyypillisimmin huijarit kauppaavat olematonta tai varastettua tavaraa tai jota ei ole aikomustakaan toimittaa ostajalle, mutta myös ostajista osa on epärehellisiä. Poliisille tehdään rikosilmoituksia eniten Tori.fi:n ilmoituksista.[58]

Tutkimukseni kohteena ovat ensinnäkin vain Suomessa tehdyt petokset, joita tutkitaan paikallispoliisissa. Keskityn siis tutkielmassani sellaisiin tietoverkossa tapahtuneisiin petoksiin, joissa sekä tekijä / rikoksesta epäilty että asianomistaja ovat Suomessa asuvia yksityishenkilöitä ja teot tapahtuvat internetin suomalaisilla kauppasivustoilla. Tutkimuskohteenani ovat siten myyntipetoksiksi kutsutut rikokset, jotka tapahtuvat käytännössä Tori.fi-sivustolla, sillä Huuto.net-sivuilla ei juurikaan enää tapahdu myyntipetoksia ja Facebookissa tapahtuneissa myyntipetoksissa esitutkinta ovat pitkälti samanlaista kuin Torilla tapahtuneissa petoksissa. Rajaan tutkielmani ulkopuolelle sellaiset nettipetokset, joissa rikoksesta epäilty tilaa asianomistajan tiedoilla tuotteita useista eri verkkokaupoista eli niin sanotut tilauspetokset. Tutkimuksen ulkopuolelle jäävät myös sellaiset tietoverkossa tapahtuneet petokset, joissa asianomistajan luottokorttitiedot on saatu haltuun tavalla tai toisella, minkä jälkeen korttia on käytetty eri tavoin (maksuvälinepetokset). Koska myynti-ilmoituksissa ei yleensä käytetä kenenkään toisen henkilön tietoja, ei myöskään identiteettivarkaus kuulu tämän tutkielman piiriin.

Selvitän esitutkinnan aikana tehtäviä toimenpiteitä, joilla on suuri merkitys myyntipetosten selviämisen ja itse esitutkinnan onnistumisen kannalta, mutta myös niiden ennalta estämisessä. Tämän tutkielman kohteena olevien, niin sanottujen perusmuotoisten myyntipetoksien tutkintaa ei voida periaatteessa keskeyttää: rikoksesta

[58] MTV3 10.3.2019.

epäilty voidaan selvittää käytetyn tilinumeron perusteella ja asiaan vaikuttavaa selvitystä on saatavilla. Käytännössä myyntipetoksia jää kuitenkin tutkimatta, sillä niiden tutkinnasta ei ole kaikissa poliisilaitoksissa tarvittavaa tietoa ja/tai taitoa. Tähän haluan osaltani käsillä olevalla tutkimuksellani puuttua.

1.3. Tutkimuksen metodologia ja rakenne

Tämän tutkimukseni lähtökohtana on vuonna 2012 ilmitullut laaja nettipetos-kokonaisuus. Tutkimus käsittää ensinnäkin verkkoympäristössä tapahtuvien myynti-petosten laajemman tapatumakentän – kybertoimintaympäristön – kuvailun. Tulen tarkastelemaan tietoverkkoihin liittyvää rikollisuutta, lainsäädäntöä ja sen kehitystä. Tehtävänäni on analysoida, tarkastella ja kuvailla myyntipetoksia sekä esittää omat tutkimustulokseni. Tutkimuskohde vaikuttaa tutkimusmenetelmän eli -metodin valintaan. ”Petos” on lailla rikokseksi määritelty teko ja sen tutkintaa ohjaavat erilaiset oikeudelliset säännöt. Oikeustiede on oppi oikeussäännöistä ja niiden soveltamisesta; se tutkii ja tulkitsee oikeutta. Oikeudellisten säädösten tulkinta tai normien soveltaminen käytäntöön on harkintaa tai oikeamminkin punnintaa, jolloin oikeustieteen metodi – tieteellinen tutkimusmenetelmä – osoittautuu näkökulmaksi oikeuteen; metodi on lähestymistapa oikeuteen, mitä käytetään tulkittaessa lainsäädäntöä, analysoitaessa oikeutta historiallisena ja yhteiskunnallisena ilmiönä taikka arvioitaessa oikeuden oikeudenmukaisuutta. Oikeustieteen ydinalueen, lainopin eli oikeusdogmatiikan, tutkimuksen kohteena on voimassa oleva oikeus. Lainoppi on oikeudellisia tekstejä tulkitseva tulkintatiede, jonka tehtäväksi on perinteisesti määritelty oikeussääntöjen sisällön selvittäminen (tulkinta) sekä oikeussääntöjen systematisointi.[59]

Yhteiskunnan sääntöjen joukossa oikeussäännöillä on oma erityinen asemansa verrattuna esimerkiksi uskonnon, moraalin tai tavan normeihin. Erot piilevät sääntöjen luomien oikeuksien ja velvollisuuksien luonteessa. Oikeusnormeille on tyypillistä, että ne ovat yhteiskunnassa (poliittista) valtaa käyttävän organisaation antamia ja ylläpitämiä. Lainsäädäntö ei muodosta suljettua, hyvin määriteltyä sääntöjärjestelmää. Kirjoitetun lain säännöt, säädökset, ovat usein epämääräisiä, epäselviä, epätäydellisiä, moniselitteisiä, jopa ristiriitaisia. Näin ollen säädöksiä joudutaan tulkitsemaan. Oikeudellinen tulkinta tarkoittaa merkityssisällön antamista lakitekstin ja muiden

[59] Aarnio 2006: 237–238; Hirvonen 2011: 4–6, 21–22, 36.

kirjallisessa muodossa annettujen oikeuslähteiden kielellisille ilmaisuille. Yksinkertaistettuna se tarkoittaa siis voimassa olevan oikeuden sisällön selvittämistä.[60]

Voidakseen tulkita oikeusnormeja ja perustella lain tulkintoja sekä sen soveltamista, on oleellista tietää, mitkä ovat oikeuslähteet[61]. Suomessa voimassa olevan oikeuden mukaan tuomioistuimen tulee perustella tekemänsä ratkaisu tavalla, joka osoittaa sen lainmukaiseksi[62]. Lainopissaoi keudellinen tulkinta osoitetaan lainmukaiseksi perusteluilla, jotka on johdettu vallitsevan oikeuslähdeopin rajaamasta lähdeaineistosta. Oikeuslähdeoppi on argumentaation kulmakivi. Siinä on sananmukaisesti kysymys "oikeuden lähteistä". Oikeuslähdeoppi vetää rajan juridisen/oikeudellisen ja ei-juridisen / ei-oikeudellisen välille. Tuomari ja tutkija, joiden kummankin tehtävä on antaa sisältö voimassa olevalle oikeudelle, ovat tiedollisesti samassa asemassa: heillä on niin sanotusti sisäinen näkökulma oikeusjärjestelmään. Säännösten tulkitsijoina tuomari ja tutkija katsovat asiaa siten samasta näkökulmasta. Heillä on käytössään samantyyppinen argumenttiaineisto (oikeuslähteet).[63]

Lainopin tutkimuskohteessa on kysymys kirjallisessa muodossa annetun tekstiaineiston tulkinnasta. Lainopillinen tulkinta tulee perustella tavalla, joka täyttää sekä lainmukaisuuden että kansalaisten perustellun oikeusturvaodotuksen vaatimukset. Jotta lainopin tutkijan esittämällä tulkintakannanotolla olisi oikeudellista merkitystä, sen perusteet eivät saa radikaalilla tavalla poiketa tuomioistuinten soveltamasta oikeuslähde- ja laintulkintaopista. Suomessa on voimassa olevan oikeuden tunnistamissäännön mukaan eriasteisesti velvoittavia oikeuslähteitä. Ensisijaisia oikeuslähteitä ovat eurooppaoikeudellinen ja kansallinen lainsäädäntö, tavanomainen oikeus eli maantapa (jollei säädännäistä oikeutta asiasta ole), lainvalmisteluaineisto eli kansallisen lainsäädännön tavoitteita selventävä tausta-aineisto kuten eduskunnan valiokuntien antamat lausunnot lakiesityksestä, varsinaiset hallituksen esitykset eduskunnalle sekä lainvalmistelussa käytettyjen komiteoiden tai toimikuntien mietinnöt, samoin prejudikaatit eli tuomioistuinten antamat ennakkoratkaisut. Toissijaisena ovat niin sanotut sallitut oikeuslähteet, joihin tuomarin on lupa vedota ratkaisua tehdessään, esimerkiksi lainopillinen kirjallisuus.[64]

---

[60] Aarnio 2006: 30–31; Kiikeri & Ylikoski 2011: 104; Siltala 2001: 22.
[61] Hirvonen 2011: 6.
[62] Oikeudenkäymiskaari 24.4 §; Laki oikeudenkäynnistä rikosasioissa 11.4 §.
[63] Aarnio 2006: 248, 256, 283.
[64] Aarnio 2006: 292; Siltala 2001: 25–26.

Koska tutkielmani keskittyy digitaalisessa toimintaympäristössä tapahtuviin myynti-petoksiin sekä niiden esitutkintaan, ei säännöksiä kuvaava ja ennakkotapauksia odottava perinteinen lainoppi yksinään täytä hyvän oikeustieteellisen tutkimuksen tunnus-merkkejä. Oikeustieteen tulisi aina ennakoida ja havainnoida muutoksia. Digitaalisessa toimintaympäristössä asioita on välttämätöntä arvioida entistä monipuolisemmin, jolloin teknistyyppinen selostava ja paljossa vain taaksepäin katsova perinteinen lainoppi jättää helposti havaitsematta jotain olennaista yhteiskunnan muutoksessa. Lainopillisen systematiikan ohittava laaja-alainen tieteenala, oikeusinformatiikka, liittyy oikeuden ja etenkin ihmisten oikeuksien ja yhteiskunnan suhteen arviointiin muuttuvassa yhteis-kunnassa. Oikeusinformatiikka jaetaan yleensä neljään toisistaan poikkeavaan alaan: oikeudellinen tietojenkäsittely, oikeudellisen informaation tutkimus, informaatio-oikeus sekä tietotekniikkaoikeus. Näistä kahden viimeisen välillä ei ole selkeää rajaa ja kansainvälisesti yleistynyt ilmaisu ICT-oikeus (*information and communication technology law*) kattaa usein lainopin tasolla operoidessaan tietotekniikkaoikeuden lisäksi myös suuren osan informaatio-oikeuden alasta.[65]

Informaatio-oikeudessa on kysymys ensisijaisesti ihmisen oikeuksista sekä niiden tukemisesta oikeusvaltiossa; se turvaa itsemäärämisoikeutemme toteutumista käsiteltäessä informaatiota verkkoyhteiskunnassa. Informaatio-oikeuden yleisiä peri-aatteita ovat oikeus tietää, oikeus tietoon, oikeus viestintään, informaation vapaus, informaation kulun vapaus, tiedollinen itsemääräämisoikeus, oikeus tietoturvaan sekä oikeus hyvään informaatiohallintoon. Näitä yleisiä periaatteita täydentävät ja niitä toteuttavat erityiset oikeusperiaatteet, joita ovat erityisesti henkilötietojen suoja, yksityisyys, avoimuus, viestinnän vapaus, sananvapaus ja julkisen palvelun periaate sekä sääntelyperiaatteena teknologianeutraalisuuden periaate.[66] Tietotekniikka-oikeudessa tutkitaan puolestaan tietotekniikan sekä sen tuotteiden ja palveluiden käyttöönottoon ja käyttämiseen liittyviä yksittäisiä, eri oikeudenaloille vaikuttavia oikeudellisia sääntely- ja tulkintaongelmia. Tietotekniikkaoikeuteen kuuluviksi luetaan ensisijaisesti sellaiset oikeudelliset kysymykset, joiden käsitteleminen ja ratkaiseminen edellyttävät niihin liittyvien tietoteknisten seikkojen ja/tai erityissääntelyn ymmärtämistä tai arviointia ja ymmärtämistä. Kysymys on siten yleensä oikeudellisen ongelman tunnistamisesta tietoteknisessä ympäristössä.[67]

[65] Saarenpää 2016: 28, 33, 45, 48, 81, 198.
[66] Saarenpää 2016: 163, 168–169.
[67] Saarenpää 2016: 197, 200.

Informaatioon ja informaatioinfrastruktuuriin liittyvät tietotekniikkarikokset ovat sekä yleisesti informaatio-oikeuden että tietotekniikkaoikeuden luontevia tutkimuskohteita sen ohella, että niiden viimekätinen sijaintipaikka käytännön tulkintatilanteessa löytyy rikosoikeudesta. Tämä tutkimus kuuluu ICT-oikeuden ja tarkemmin tietotekniikka-oikeuden piiriin. Niin kuin monien erityisalojen rikosten yhteydessä, on tässäkin tutkimuksessa tunnettava tietotekniikkaoikeutta ja rikosoikeutta.[68] Tietotekniikka-rikosten historiallista kehitystä ja oikeutta muuttuvana ilmiönä hahmottaessani tuon tutkimukseeni oikeushistoriallisen elementin[69]. Koska tutkimuksessani on osin kyse julkisen vallan ja yksityisen välisistä oikeussuhteista, on se vähäisessä määrin myös julkisoikeudellinen tutkimus. Perehtymiseni rikosprosessin esitutkintavaiheeseen sisällyttää tutkimukseeni piirteitä prosessioikeudesta. Huomioidessani poliisin sisäisen työnjaon, on tutkimuksellani myös hallinto-oikeudellinen puoli sen sijoittuessa tarkemmin poliisioikeuden alaan.

Lähestyn aihettani lainopillisin metodein tulkitsemalla voimassa olevia oikeussäädöksiä. Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus ETS 185[70] (eli niin sanottu Budapestin sopimus tai tietoverkkorikossopimus) on ainona erityisesti tieto-verkkorikollisuutta käsittelevä kansainvälinen sopimus ja kaiken kyberrikollisuuden torjunnan kehittämisen perusta[71]. Paneudun tutkimuksessani hallituksen esitykseen HE 153/2006, jolla yleissopimus ehdotettiin hyväksyttäväksi: se on pantu kansallisesti täytäntöön osana Suomen rikoslakia (19.12.1889/39). Euroopan parlamentin ja neuvoston direktiivi 2013/40/EU (tietoverkkorikosdirektiivi) puolestaan vahvistaa ne vähimmäissäännöt, jotka koskevat rikosten ja seuraamusten määrittelyä tieto-järjestelmiin kohdistuvien hyökkäysten alalla. Mielenkiinnon kohteena on siten myös rikoslain uudistus (10.4.2015/368), jolla tietoverkkorikosdirektiivi pantiin täytäntöön, sekä siihen liittyvä hallituksen esitys HE 232/2014 rikoslain eräiden tietoverkkorikoksia koskevien säännösten muuttamisesta. Perehdyn myös muihin rikoslainsäädännön uudistuksiin liittyviin hallituksen esityksiin. Lisäksi tutustun muun muassa Euroopan komission tiedonantoihin, Valtioneuvoston periaatepäätöksiin, eri ministeriöiden julkaisuihin sekä relevanttiin oikeuskirjallisuuteen, samoin aihepiiriin liittyvään uutisointiin.

Tässä tutkielmani johdantoluvussa kuvailin sen lähtökohdat, tutkimustehtävän rajauksineen sekä tutkielmassa käyttämäni metodin. Toisessa luvussa käsittelen kyber-

[68] Saarenpää 2016: 198.
[69] Hirvonen 2011: 28.
[70] Saatettu voimaan Suomessa Tasavallan presidentin asetuksella 60/2007 (SopS 60/2007).
[71] Sisäministeriö 2017b: 19.

toimintaympäristöä, kyberturvallisuutta sekä Suomen kyberturvallisuusstrategiaa. Kolmannen luvun aiheena ovat tietoverkkoihin liittyvä rikollisuus ja sen oikeudellinen kehitys, mutta läpikäyn myös kyseisen rikollisuuden kahta eri osa-aluetta eli tietoverkkorikollisuutta sekä tietoverkoissa tapahtuvaa rikollisuutta. Neljännessä Myyntipetokset-luvussa kerron vuosien 2011 ja 2012 aikana tapahtuneesta nettipetoskokonaisuudesta, jonka esitutkinnassa ilmitulleet ongelmat olivat sysäys tämän tutkielman tekemiseen. Lisäksi selvitän lyhyesti verkossa tapahtuvaa yksityishenkilöiden välistä kaupankäyntiä eli vertaisverkkokauppaa ja esittelen kaksi suomalaisten suosimaa internetin markkinapaikkaa: Huuto.net ja Tori.fi. Paneudun myös rikostutkintaan eli rikoksen johdosta suoritettavaa tutkintaan ja rikosprosessiin yleensä sekä myyntipetosten esitutkintaa suorittavan poliisin tutkintatoimenpiteisiin. Viides luku sisältää tutkimukseni johtopäätöksinä ne keinot, joilla mielestäni lisättäisiin tietoisuutta tietoverkkoihin liittyvästä rikollisuudesta ja edesautettaisiin vähentämään myyntipetosten määrää.

2. KYBERTOIMINTAYMPÄRISTÖ

Digitalisaation ytimen muodostavat sähköisessä muodossa olevat tiedot. Yhteiskuntamme useat toiminnot ovat riippuvaisia tietoteknisten järjestelmien ja niistä muodostuvan kybertoimintaympäristön toiminnasta ja toimintavarmuudesta.[72] Kybertoimintaympäristö on sähköisessä muodossa olevan informaation eli tiedon käsittelyyn tarkoitettu, yhdestä tai useammasta tietojärjestelmästä muodostuva toimintaympäristö. Tälle ympäristölle on tunnusomaista elektroniikan ja sähkömagneettisen spektrin käyttö datan ja informaation varastointiin, muokkaamiseen ja siirtoon viestintäverkkojen avulla; ympäristöön kuuluvat myös datan ja informaation käsittelyyn[73] liittyvät fyysiset rakenteet. Kybertoimintaympäristöön kohdistuvat uhkat ovat tietoturvauhkia, jotka toteutuessaan vaarantavat tietojärjestelmän oikeanlaisen tai sen tarkoitetun toiminnan. Joku voi vahingoittaa tietoverkkoja tai käyttää niitä vahingolliseen tarkoitukseen eli esimerkiksi rikokseen, kiusantekoon tai rikollisen materiaalin levittämiseen[74]. Kyberuhka on siten mahdollisuus sellaiseen kybertoimintaympäristöön vaikuttavaan tekoon tai tapahtumaan, joka toteutuessaan vaarantaa jonkin kybertoimintaympäristöstä riippuvaisen toiminnon.[75]

Vuoden 2018 lopussa 51,2 prosenttia maapallon väestöstä, 3,9 miljardia ihmistä, käytti internetiä[76]. Globaali internet-liikenteen määrä on kasvanut dramaattisesti: kun vuonna 1992 liikennettä oli 100 gigatavua (GB, *gigabyte*) päivässä, sitä oli kymmenen vuotta myöhemmin saman verran sekunnissa – ja liikennemäärän kasvu kiihtyy:[77]

VUOSI	GLOBAALI INTERNET-LIIKENNE
1992	100 GB / vuorokausi
1997	100 GB / tunti
2002	100 GB / sekunti
2007	2 000 GB / sekunti
2017	46 600 GB / sekunti
2022	150 700 GB / sekunti

Taulukko 2. Maailman internet-liikenteen kehitys gigatavuina (Cisco 2019).

[72] Turvallisuuskomitea 2015: 116.
[73] Informaation käsittely on tiedon keräämistä, tallettamista, käyttöä, järjestämistä, siirtämistä, luovuttamista, säilyttämistä, muuttamista, yhdistämistä, suojaamista, poistamista, tuhoamista sekä muita informaatioon (tietoihin) kohdistuvia toimenpiteitä. Suomen kyberturvallisuusstrategia 2013: 12.
[74] Kodin kyberopas 2017: 22.
[75] Suomen kyberturvallisuusstrategia 2013: 12–13.
[76] ITU 2018: 1.
[77] Cisco 2019.

Kun arvion mukaan 70 prosenttia maailman väestöstä käyttää internettiä vuoteen 2023 mennessä, kasvattaa tämä kattavampi maailmanlaajuinen tietoyhteiskuntamme entisestään tarvetta lisätä tietoverkko- ja kyberturvallisuutta[78]. Lisäksi erityisesti mobiilidatayhteydet lisääntyvät: niiden määrä tulee kasvamaan seitsenkertaisesti vuodesta 2017 vuoteen 2022. Kun vuonna 2018 internetyhteyksistä 41 prosenttia oli tietokoneyhteyksiä, vuoteen 2022 mennessä vain 19 prosenttia internetin käytöstä tapahtuu tietokoneella; tuolloin 44 prosenttia tulee olemaan älypuhelinyhteyksiä. Kybertoimintaympäristö on siten osa arjen elämää äly- ja verkko-ominaisuuksien tullessa osaksi yhä useampaa jokapäiväistä laitetta ja prosessia[79]. Nopeimmin kasvava laitekategoria tulee olemaan M2M (*machine-to-machine*)[80]: yli puolet nettiyhteyttä käyttävistä laitteista tulee olemaan M2M-laitteita vuoteen 2022 mennessä (yli 14,6 miljardia M2M-laitetta).[81] Tämän vuoksi onkin ehkä syytä jatkossa puhua esineiden internetin eli IoT:n (*Internet of Things*)[82] sijaan IoE:stä (*Internet of Everything*): internet on kaikkialla.

Tieto- ja viestintäteknologiasta (ICT) on tullut talouskasvumme selkäranka ja se on kriittinen voimavara, johon kaikki talouden alat luottavat. ICT tukee monimutkaisia järjestelmiä, jotka pitävät taloutemme käynnissä keskeisillä aloilla kuten rahoitus, terveys, energia ja liikenne. Monet liiketoimintamallit perustuvat internetin keskeytymättömään saatavuuteen ja tietojärjestelmien moitteettomaan toimintaan.[83] Teknologiaa hyödynnetään yhä laajemmin, mikä lisää yritystoiminnan, hallinnon ja arkielämän tehokkuutta, mutta samalla myös luonnononnettomuuksista ja tahallisesta toiminnasta johtuvat riskit ja haavoittuvuudet kasvavat. Tekninen infrastruktuuri, tietoverkot ja -järjestelmät kytkeytyvät tiiviisti toisiinsa. Kybertoimintaympäristöstä tulee yhä keskeisempi osa ulko-, turvallisuus- ja puolustuspolitiikkaa.[84] Erityisesti kriittiseen tietoinfrastruktuuriin kohdistuvista uhkista ja hyökkäyksistä suurin osa

[78] ITU 2018: 1.
[79] Sisäministeriö 2017a: 32.
[80] M2M eli *machine-to-machine* viittaa verkkoon kytkettyihin laitteisiin, jotka keräävät tietoa itsestään ja ympäristöstään. M2M-sovelluksia hyödyntävät muun muassa hälyttimet, maksupäätteet, useat kodin automatisointilaitteista, erilaiset älykkäät mittarit, myyntiautomaatit, videovalvontakamerat, terveydenhoitoalan monitorointi- ja valvontalaitteet sekä kuljetuksien, pakettien ja omaisuuden seurantaan tarkoitetut laitteet. Cisco 2019.
[81] Cisco 2019.
[82] Esineiden internet tarkoittaa sitä, että tietoteknologia on sulautunut arkisiin esineisiin kuten kodin laitteisiin, joita pystyy seuraamaan ja ohjaamaan internetin kautta muualta esimerkiksi tietokoneella, puhelimella tai tabletilla. Kodinkoneet ja muut laitteet ovat siis yhteydessä internetiin, mikä mahdollistaa niiden etäkäytön. Kodin kyberopas 2017: 11, 22; Sisäministeriö 2017b: 5.
[83] Euroopan komissio 2013: 2.
[84] Sisäministeriö 2017a: 32.

kohdistuu myös Suomeen maamme rajojen ulkopuolelta[85]. Perinteisen sodankäynnin sijaan nykyään varaudutaan itseasiassa kybersodankäynnin sijaan jo hybridisotaan, jossa yhteiskuntarauhan horjuttamiseen pyritään lukuisia eri komponentteja yhdistävillä operaatioilla[86].

Maailmanlaajuinen yhteisö hyödyntää enenevässä määrin informaatio- ja viestintäteknologiaa (ICT) sosiaalisen ja taloudellisen edistyksen avaintekijänä. Valtiot tunnustavat, että yhä nopeammin kiihtyvällä teknologisella kehityksellä ja digitalisaatiolla voidaan edistää kansalaisten vaurautta ja yleistä hyvinvointia. Kehityksen kääntöpuolena on kasvanut riippuvuus laajoista ja monimutkaisista teknisistä järjestelmistä sekä informaatioverkoista. Niihin kohdistuneet häiriöt voivat vaikuttaa nopesti ja laajasti muun muassa peruspalvelujen tuottamiseen sekä turvallisuusviranomaisten toimintakykyyn. Tieto- ja viestintäjärjestelmien käytön estyminen rinnastuu paljossa esimerkiksi sähköverkkojen käyttökatkoihin. Näiden verkkojen keskinäinen riippuvuussuhde on erityisen kriittinen yhteiskunnan toiminnoille ylipäätään. Verkkoyhteiskunnassa myös maantieteellisten rajojen fyysinen vaikutus vähenee. Teknologinen kehitys on tuonut mukanaan uudenlaisia uhkia, ja tietoverkoissa tapahtuva vakoilu, rikollisuus sekä valtioiden väliset operaatiot lisääntyvät. Valitettavasti kyberturvallisuus ei ole – vielä – monien kansallisten tai yritysmaailman teknologiastrategioiden ytimessä.[87]

2.1. Kyberturvallisuus

Viime vuodet ovat näyttäneet, että vaikkakin digitaalinen maailma tuo tullessaan valtavia etuja, se on myös haavoittuvainen. Kyberturvallisuus on yhä tärkeämpi osa elämäämme; sen on oltava erottamaton ja olennainen osa sitä prosessia, joka hyödyntää teknologista edistymistä eli digimuutosta. Paikallisten tietoverkkojen liittyminen toisiinsa maailmanlaajuisesti tarkoittaa, että kaikki ja mikä hyvänsä kansallisesta infrastruktuurista perus- ja ihmisoikeuksiimme voi vaarantua.[88] Kyberturvallisuus viittaa yleisesti niihin suojakeinoihin ja eri toimiin, joita voidaan käyttää sekä siviili- että sotilasalalla kybertoimintaympäristön suojaamiseen niiltä uhkilta, jotka voivat

[85] Turvallisuuskomitea 2015: 84.
[86] Hybridisodankäynnin komponentteja ovat infrastruktuuri ja energia, yhteiskuntarauha, talouspakotteet, sotilastoiminta, erikoisjoukot, ei-valtiolliset joukot (kapinalliset), diplomatia, informaatiovaikuttaminen ja propaganda sekä kyberhyökkäys. Turvallisuuskomitea 2018: 18.
[87] ITU 2015: iii; Saarenpää 2016: 28, 31–32; Turvallisuuskomitea 2015: 24.
[88] ITU 2015: iii; ITU 2017: 47.

vahingoittaa sen keskinäisiä, toisistaan riippuvia tietoverkkoja ja tietoinfrastruktuuria. Kyberturvallisuus pyrkii säilyttämään verkkojen ja infrastruktuurin saatavuuden ja eheyden sekä siinä olevien tietojen luottamuksellisuuden.[89]

Kyberturvallisuus kuvaa koko sähköisen toimintaympäristön turvallisuutta. Kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Tavoitetilassa kybertoimintaympäristöstä ei aiheudu vaaraa, haittaa tai häiriötä sähköisen tiedon käsittelystä riippuvaiselle toiminnalle eikä sen toimivuudelle. Luottamus kybertoimintaympäristöön perustuu siihen, että sen toimijat toteuttavat tarkoituksenmukaisia ja riittäviä tietoturvallisuusmenettelyjä, joiden avulla pystytään estämään tietoturvauhkien toteutuminen. Uhkien kuitenkin mahdollisesti toteutuessa kyseisten menettelyjen avulla niiden vaikutuksia pystytään estämään, lieventämään tai sietämään. Kyberturvallisuus käsittää yhteiskunnan elintärkeisiin toimintoihin ja kriittiseen infrastruktuuriin kohdistuvat toimenpiteet, joiden tavoitteena on saavuttaa kyky hallita ennakoivasti kyberuhkia ja tarvittaessa sietää kyseisiä uhkia ja niiden vaikutuksia, jotka voivat aiheuttaa merkittävää haittaa tai vaaraa Suomelle tai sen väestölle.[90]

Muutamina viime vuosina on tapahtunut paljon kyberuhkien saralla. Vuonna 2016 melkein prosentti kaikista lähetetyistä sähköposteista oli lähinnä haittaohjelmia (1/131 sähköpostiviestistä). Ransomware[91]-hyökkäykset vaikuttivat yhä enemmän yrityksiin ja myös yksityisiin kansalaisiin: haitallisia sähköpostiviestejä – jotka ovat muuta kuin suhteellisen vaaraton roskaposti – lähetettiin valtavia määriä umpimähkään valituille vastaanottajille. Hyökkääjät vaativat suurempia määriä lunnaita uhreiltaan: keskimääräinen lunnasvaade nousi vuonna 2016 tuhanteen dollariin (1 000 USD) oltuaan vuotta aiemmin 300 USD. Vuosi 2017 puolestaan osoitti, kuinka haavoittuvaisia yhteiskuntamme peruspalvelut ovat kyberuhkille: Toukokuussa tapahtui ennennäkemättömän massiivinen kyberhyökkäys, kun WannaCry-niminen ”kryptomato” (kiristysohjelma) levisi räjähdysmäisesti satoihin tuhansiin järjestelmiin ympäri maailmaa aiheuttaen suuria häiriöitä yrityksille ja sairaaloille yli 150 maassa. Ohjelma salasi saastuneen

[89] Euroopan komissio 2013: 3.
[90] Suomen kyberturvallisuusstrategia 2013: 13.
[91] Tietoverkossa voi joutua kiristyksen kohteeksi esimerkiksi tietokoneen tiedostoja salaavan kiristyshaittaohjelman (Ransomware) kautta, joka voi päästä laitteelle ilmaisen ohjelman lataamisen yhteydessä tai sähköpostiviestin liitetiedoston kautta. Kiristysohjelma lukitsee kaikki tiedostot ja pyytää maksamaan lunnaat, jonka maksamisen jälkeen saattaa saada niin sanotun salausavaimen. Se on pieni ohjelmisto, joka poistaa lukituksen. Lunnaiden maksaminen ei ole tae siitä, että salaus poistuu. Tuolloin menettää sekä tiedostot että maksamansa lunnassumman. Kiristysohjelmien kohteena ovat usein tavalliset tietoverkon käyttäjät. Kodin kyberopas 2017: 19.

tietokoneen tärkeät tiedostot, minkä jälkeen verkkorikolliset vaativat lunnaiden maksamista (bitcoineina) vastineeksi salauksen purkamisesta ja tiedostojen palauttamisesta. Kyberhyökkäykset aiheuttavat merkittäviä taloudellisia menetyksiä, mitä teki myös kesäkuussa 2017 maailmalla vielä laajemmalle levinnyt NotPetya-haittaohjelma.[92]

Sekä WannaCry että Petya olisi voitu estää tai niiden vaikutusta olisi voitu heikentää, jos useammissa organisaatioissa olisi noudatettu tietoturvallisuuteen liittyviä perus-ohjeita (muun muassa haavoittuvuuksien korjaaminen ja asianmukaisten prosessien määrittäminen)[93]. Tapahtumat ovatkin saaneet eri tahot ymmärtämään myös yhteistyön merkityksen kyberturvallisuuden nimissä. Valtioiden ja yritysten (alan sidosryhmien) onkin oltava tietoisia kyberturvallisuuden tasostaan ja tunnistettava ne alueet, joilla kyberturvallisuutta on parannettava.[94] Euroopan komission presidentti, Jean-Claude Juncker totesi 13.7.2017 pitämässään puheessaan seuraavaa:

> *"Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks. […] Cyber-attacks know no borders and no one is immune. This is why, today, the Commission is proposing new tools, including a European Cybersecurity Agency, to help defend us against such attacks."*[95]

Tämän seurauksena vuonna 2004 perustetun EU:n verkko- ja tietoturvaviranomaisen, ENISA:n (*European Union Agency for Network and Information Security*), toimintaa vahvistettiin ja siitä muodostettiin EU:n kyberturvallisuusvirasto.

Tieto- ja viestintätekniikka (ICT) aiheuttaa yhden kriittisimmistä haasteista maailman-laajuiselle turvallisuudelle. Kun kyberturvallisuus on maailmassa keskeisessä asemassa, on välttämätöntä, että valtiot toteuttavat ratkaisuja, jotka tarjoavat turvallisen internetin sen käyttäjille ja että ne sitoutuvat tulevien haasteiden vaatimiin parannuksiin.[96] Vaikka kybertietoisuus on lisääntynyt, on tietoturvaosaajista kuitenkin pulaa. Osaajien niukkuus motivoi innovoimaan uusia tietoturvapalveluita ja teknologisia ratkaisuja markkinoille. Organisaatiot ovat puolestaan valmiimpia kertomaan kokemistaan tietoturvauhkista ja niiden vaikutuksista liiketoiminnallisiin päätöksiin eikä maineenmenetystä enää pelätä. Tietoturva-aukkojen etsimisestä on tullut osa normaalia tietoturvan kehitystoimintaa. Esineiden internet, IoT, muuttaa erilaisten vahingontekorikosten toteutusmenetelmiä[97]

[92] Cisco 2018: 6; ITU 2017: iii, 7; Viestintävirasto 9.2.2018.
[93] Cisco 2018: 7.
[94] ITU 2017: iii.
[95] Euroopan komissio 2017.
[96] ITU 2018: 11.
[97] Sisäministeriö 2017b: 5.

ja kiristyshaittaohjelmat ovat osaltaan löytäneet uusia tartuntakohteita: IoT-laitemäärät lisääntyvät ja niiden tietokoneita heikommat suojaukset tekevät niistä houkuttavan tartuntapinnan. Tietoturvattomat verkkoon kytketyt IoT-laitteet toimivat heikosti, niihin ei ole saatavilla päivityksiä ja ne unohdetaan käyttämättömänä verkkoon, mistä niitä kaapataan haittakäyttöön.[98]

YK:n järjestöistä vanhin, vuonna 1865 perustettu Kansainvälinen televiestintäliitto ITU (*International Telecommunications Union*), on YK:n tietoliikenteeseen ja viestintätekniikkaan eli ICT-alaan keskittyvä erityisjärjestö[99] ja myös maailman ainut virallinen ICT-statistiikan lähde. ITU julkaisee maailmanlaajuista tilannekatsausta kyberturvallisuudesta eli niin sanottua GCI-raporttia, joka pohjautuu ITU:n vuoden 2007 globaaliin kyberturvallisuusagendaan[100]. Raportissa valtiot listataan sen saaman kyberturvallisuusindeksiluvun (*Global Cybersecurity Index*, GCI) mukaiseen järjestykseen, mikä mittaa valtioiden kyberturvallisuuden kehitystä[101]. Raporteilla pyritään tarjoamaan valtioille asianmukaiset vaikuttimet tehostaa kyberturvallisuussuunnitelmiaan. Niiden perimmäinen tavoite on edistää maailmanlaajuista kyberturvallisuuskulttuuria ja sen integroitumista tieto- ja viestintätekniikan (ICT) ytimeen.[102]

Ensimmäinen ITU:n kyberturvallisuusraporteista julkaistiin huhtikuussa 2015 (*Global Cybersecurity Index & Cyberwellness Profiles*) ja se koski vuoden 2014 kyberturvallisuustilannetta[103]. Järjestyksessään toinen raportti (GCI 2017) koski vuoden 2016 tilannetta[104]. GCI 2018[105] -raportin luonnosversio julkaistiin 27.3.2019. Raportin mukaan maailman valtioiden pitää toimia yhdessä kyberturvallisuuskysymysten ratkaisemiseksi ja kyberuhkien lieventämiseksi. Valtioiden välillä on eroja niin tietoisuuden, ymmärryksen kuin tiedon suhteen, samoin niiden valmiudessa toteuttaa

---

[98] Viestintävirasto 9.2.2018.
[99] Kaikki 193 YK:n jäsenmaata ovat myös ITU:n jäseniä, 194. jäsen on Palestiina. Myös alan yritykset ja akateemiset organisaatiot voivat liittyä sen jäseneksi ja näitä yksityisjäseniä ITU:lla on melkein 800. Suomi liittyi ITU:n jäseneksi 1.9.1920 ja sitä edustaa ITU:n kokouksissa yleensä Liikenne- ja viestintävirasto, Traficom.
[100] *Global Cybersecurity Agenda* (GCA).
[101] GCI-raportti mittaa seuraavia osa-alueita: oikeudelliset toimenpiteet (*legal*), tekniset toimenpiteet (*technical*), organisoituminen (*organisational*), valmiuksien kehittäminen (*capacity building*) ja yhteistyö (*cooperation*). ITU 2017: V; ITU 2018: iii.
[102] ITU 2015: iii.
[103] ITU 2015.
[104] ITU 2017.
[105] Vuonna 2014 ITU-jäsenvaltioista vain 54 prosenttia osallistui raportin julkaisuun, vuonna 2017 siihen otti osaa jo 69 prosenttia jäsenvaltioista ja vuonna 2018 jäsenvaltioista noin 80 prosenttia ilmoitti yhteystahon GCI-raporttia varten. Ellei jokin jäsenvaltio ilmoita erityistä GCI-yhteystahoa, ITU ottaa yhteyden kyseisen valtion institutionaaliseen tahoon, joka esimerkiksi Suomessa on liikenne- ja viestintäministeriö. ITU 2018: 7.

tarkoituksenmukaisia strategioita. Maailman valtioiden on tehtävä yhteistyötä muun muassa tietoverkkorikollisuuden ja kriittistä infrastruktuuria kohtaan tehtävien kyberhyökkäysten saralla. Tulevaisuuden kyberuhkat saattavat aiheuttaa mittavia taloudellisia ja yhteiskunnallisia vahinkoja, joten suunnitelmista niiden ehkäisemiseksi on sovittava kansainvälisesti.[106]

Suurimmalla osalla maailman valtioista on kansallinen kyberturvallisuusstrategia (NCS, *National Cybersecurity Strategy*) ja ne toteuttavat kyberturvallisuuteen liittyviä kampanjoita sekä järjestävät alan asiantuntijakoulutusta[107]. Valtioiden osallistumisaste kyberturvallisuutta käsitteleviin foorumeihin ja järjestöihin on korkea. Toisaalta julkisen ja yksityisen sektorin välistä yhteistyötä pitäisi kaikkinensa lisätä.[108] Euroopan valtioiden tilanne kyberturvallisuuden suhteen on parantunut muun muassa EU:n laajuisen tieto- ja viestintätekniikan (ICT) tuotteiden, palveluiden ja prosessien sertifiointijärjestelmän käyttöönoton, EU:n yleisen tietosuoja-asetuksen[109] (GDPR, *General Data Protection Regulation*) täytäntöönpanon ja EU:n verkko- ja tietoturva-direktiivin[110] (NIS- eli *Network and Information Systems* -direktiivin) ansiosta.[111]

Kyberuhkat kyseenalaistavat nyky-yhteiskuntamme, jonka sähköiset palvelut, tietojen eheys ja luottamuksellisuus sekä internetin tehokkuus kaikki liittyvät tieto- ja viestintä-järjestelmiin (ICT) sekä kyberturvallisuuteen. Kyberturvallisuus on asia, jonka sekä valtiot että yritykset kokevat tärkeäksi tehokkaan digitaalisen hallinnon aikaansaamiseksi. Kyberturvallisuus suojelee valtion (julkista) infrastruktuuria, jolloin siihen ja sen toimintaan voidaan luottaa. Valtiot kehittelevät aina vain sofistikoituneempia sähköisiä hallintoja ja lisäävät sekä verkkopalvelujensa saatavuutta että integroituja palvelujärjestelmiä. Nämä kaikki saattavat johtaa entistä kehittyneempiin kyber-uhkiin.[112] Suomessakin viranomaisilla on velvollisuus tarjota digitaalisia palveluja: Laki digitaalisten palvelujen tarjoamisesta (HE 60/2018) on annettu eduskunnalle 3.5.2018.

[106] ITU 2018: 11.
[107] Vuonna 2018 kyberturvallisuusstrategia oli 58 prosentilla valtioista, kun vuotta aiemmin sellainen oli puolella valtioista; kampanjoita järjestettiin 66 prosentissa valtioista verrattuna vuoden 2017 tilanteeseen, jolloin niitä järjestettiin 59 prosentissa valtioita; koulutusta järjestettiin 63 prosentissa valtioissa vuonna 2018 ja 52 prosentissa vuonna 2017. ITU 2018: 13.
[108] Vuonna 2018 kansainvälisiin tapahtumiin osallistui 79 prosenttia valtioista, mutta vain 49 prosentilla valtioista on voimassa järjestelyt, jotka mahdollistavat julkisen ja yksityisen sektorin yhteistyön kyber-turvallisuuteen liittyvissä asioissa. ITU 2018: 14.
[109] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679.
[110] Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148.
[111] ITU 2018: vii, 13.
[112] ITU 2018: 15.

Ehdotettu laki toimeenpanee saavutettavuusdirektiivin[113] Suomessa. Saavutettavuus on osa yhdenvertaisuuden toteuttamista – ja yhdenvertaisuus on Suomen perustuslaissa (PL 11.6.1999/731) säädetty perusoikeus (PL 2:6 §). Lisäksi digitaaliset palvelut ovat osa viranomaisten palveluvalikoimaa, joten palvelujen saavutettavuus kaikille on myös osa hyvän hallinnon toteuttamista, mihin meillä Suomessa on myös perustuslaillinen oikeus (PL 2:21 §).[114]

2.2. Suomen kyberturvallisuusstrategia

Tietoturvallisuuden kasvava merkitys havaittiin kansallisella politiikkatasolla[115] ja nimenomaan automaattisen tietojenkäsittelyn sekä uusien tiedonsiirtomuotojen yleistyminen nosti esiin tarpeen tarkastella tietoa ja tietoliikennettä omana kokonaisuutenaan myös rikosoikeudellisen sääntelyn kannalta (HE 94/1993)[116]. Pääministeri Paavo Lipposen II hallituskauden aikana 1999–2003[117] säädösympäristön todettiin kehittyneen merkittävästi, mutta viestintäverkkojen sääntelyssä jatkettiin teknologianeutraalia sääntelyä. Erityisesti internetin itsesääntelyyn sekä laittoman ja haitallisen aineiston torjumiseen liittyvään työhön osallistuttiin aktiivisesti: hallitus osallistui EU:n toimielinten työhön muun muassa eEurope 2005 -tietoyhteiskunta-ohjelman valmistelussa. Hallituksen asettama tietoturvallisuusasioiden neuvottelukunta[118] laati kansallisen tietoturvakatsauksen pohjalta ehdotuksensa kansalliseksi tietoturvastrategiaksi, joka tuli hallituksen vahvistettavaksi keväällä 2003. Tietoturvahallintoa uudistettiin siten, että Viestintävirastosta tehtiin merkittävä tietoturva-alan virasto.[119]

Seuraavan, pääministeri Matti Vanhasen, hallituksen[120] ohjelmassa 24.6.2003 todettiin seuraavaa: Suomen asemaa vahvistetaan yhtenä maailman johtavista tietoyhteiskunnista. Hallituksen liikenne- ja viestintäpolitiikalla parannetaan kansalaisten hyvinvointia sekä elinkeinoelämän ja julkishallinnon tuottavuutta ja kilpailukykyä edistämällä tietotekniikan ja tietoyhteiskunnan palvelujen käyttöä. Hallitus panostaa vahvasti tieto-

[113] Euroopan parlamentin ja neuvoston direktiivi julkisen sektorin elinten verkkosivustojen ja mobiilisovellusten saavutettavuudesta (EU) 2016/2102.
[114] HE 60/2018: 6.
[115] Saarenpää 2016: 168
[116] HE 94/1993 vp: 133.
[117] Lipposen II hallitus toimi 15.4.1999–17.4.2003.
[118] Tietoturvallisuusstrategian ja sen toteutusta koordinoivan kansallisen tietoturvallisuusasioiden neuvottelutoimikunnan toimikausi loppui keväällä 2007. LVM 2009: 10.
[119] Valtioneuvoston kanslia 2003a: 24.
[120] Vanhasen I hallitus toimi 24.6.2003–19.4.2007.

yhteiskuntakehityksen edistämiseen. Hallitus harjoittaa aktiivista tietoyhteiskunta-politiikkaa, jonka tavoitteena on lisätä tuottavuutta ja kilpailukykyä ja alueellista tasa-arvoa hyödyntämällä tieto- ja viestintäteknologiaa kaikilla yhteiskunnan osa-alueilla. Kehitetään tietoyhteiskunnan palveluita koskevaa lainsäädäntöä. Julkisen hallinnon virastojen ja laitosten siirtymistä sähköiseen asiointiin vauhditetaan voimakkaasti. Kansalaisten ja yritysten luottamusta tietoyhteiskunnan palveluihin edistetään tieto-turvaa ja viestinnän yksityisyyden suojaa parantamalla. Tietoturvauhkiin ja tieto-tekniikkarikollisuuteen varaudutaan lainsäädäntöä uudistamalla.[121]

Vanhasen hallitusohjelma käynnisti poikkihallinnollisia politiikkaohjelmia, joista yksi oli tietoyhteiskuntaohjelma. Kyseinen hallituksen ohjelma kohdistui tietoyhteiskunnan mahdollisuuksien hyödyntämiseen ja sillä huolehdittiin siitä, että tietoyhteiskunnan säädösympäristö oli ajan tasalla[122]. Sen seurauksena Suomi sai vuonna 2003 ensimmäisen kansallisen tietoturvallisuusstrategiansa, joka nosti tietoturvan poliittiselle agendalle ja merkittäväksi aiheeksi yhteiskunnalliseen keskusteluun; tietoturvatietämys ja -ymmärrys olivat kasvaneet. Kyseinen tietoturvallisuusstrategia oli myös ensimmäinen Euroopassa ja mahdollisesti ensimmäinen maailmassa.[123] Vuoden 2003 kansallista tietoturvallisuusstrategiaa seurasi valtioneuvoston periaatepäätös joulukuussa 2008 kansalliseksi tietoturvastrategiaksi, jonka avulla pyrittiin luomaan suomalaisille (kansalaiset, yritykset, viranomaiset ja muut toimijat) turvallinen arki tietoyhteis-kunnassa. Suomen todettiin olevan osa globaalia tietoverkkotaloutta ja suurimman osan tietoturvauhkista ja -hyökkäyksistä kohdistuvan maahamme rajojen ulkopuolelta. Globalisaatio ei kuitenkaan ole ainoastaan uhka vaan myös mahdollisuus, joten Suomen tuli – ja tulee edelleen – toimia aktiivisesti kansainvälisessä viranomaisyhteistyössä niin tietoturvauhkien ennaltaehkäisemiseksi kuin haittojen vähentämiseksi.[124]

Askel kattavamman sääntelyn suuntaan oli vuonna 2010 voimaan tullut asetus tieto-turvallisuudesta valtionhallinnossa (1.7.2010/681), joka korosti tietoturvallisuus-periaatteen merkitystä: asetuksessa määriteltiin yleiset tietoturvallisuusvaatimukset valtionhallinnon viranomaisten asiakirjoille[125]. Toisaalta samana vuonna valtio-neuvoston selonteossa eduskunnalle digitaalisesta agendasta (VNS 10/2010 vp[126]) tyydyttiin vain yleisesti korostamaan tietoturvallisuuden merkitystä ja luettelemaan

[121] Valtioneuvoston kanslia 2003b: 23, 43.
[122] Valtioneuvoston kanslia 2003b: 54.
[123] LVM 2009: 5.
[124] LVM 2009: 3.
[125] 2 luku – Yleiset tietoturvallisuusvaatimukset.
[126] Tuottava ja uudistuva Suomi – Digitaalinen agenda vuosille 2011–2020. Valtioneuvoston selonteko eduskunnalle. VNS 10/2010 vp.

yksittäisiä toimenpiteitä sen käytännölliseksi parantamiseksi.[127] Tasavallan presidentti ja valtioneuvoston ulko- ja turvallisuuspoliittinen ministerivaliokunta päättivät 8.11.2011 pidetyssä yleisistunnossaan asettaa poikkihallinnollisen työryhmän laatimaan kansallisen kyberturvallisuusstrategian osana Yhteiskunnan turvallisuusstrategian (YTS) toimeenpanoa[128]; kyberturvallisuus on kiinteä osa yhteiskunnan kokonaisturvallisuutta ja sen toimintamalli noudattaa YTS:ssä määritettyjä periaatteita ja toimintatapoja[129]. Suomen ensimmäinen kyberturvallisuusstrategia hyväksyttiin valtioneuvoston yleisistunnossa tammikuussa 2013[130]. Myös EU valmisteli omaa kyberturvallisuusstrategiaansa ja myös se hyväksyttiin vuonna 2013.

Suomen kyberturvallisuusstrategialla haluttiin luoda yhteinen ymmärrys kyberturvallisuudesta ja vahvistaa yhteiskunnan kokonaisturvallisuutta. Strategian mukaan hyvin toimiva kybertoimintaympäristö on Suomelle kilpailuetu ja mahdollisuus. Lisäksi turvallinen kybertoimintaympäristö helpottaa yksilöiden ja yritysten oman toiminnan suunnittelua, mikä lisää taloudellista aktiviteettia. Sen lisäksi, että hyvä toimintaympäristö parantaa Suomen kansainvälistä houkuttelevuutta investointikohteena, todettiin kyberturvallisuuden itsessään olevan uusi ja vahvistuva liiketoiminnan alue.[131] Kyberturvallisuusstrategia käynnisti koko yhteiskunnan kattavan kyberturvallisuuden edellyttämän varautumisen ja jatkuvuudenhallinnan suunnittelun.[132] Helmikuussa 2013 aloitti toimintansa Turvallisuuskomitea avustamaan valtioneuvostoa ja ministeriöitä laajoissa kokonaisturvallisuuteen liittyvissä asioissa. Turvallisuuskomitean tehtävistä ja toiminnan periaatteista säädetään valtioneuvoston asetuksessa Turvallisuuskomiteasta (77/2013).[133] Turvallisuuskomitea hyväksyi kyberturvallisuusstrategian ensimmäisen toimeenpano-ohjelman 11.3.2014 ja on säännöllisesti arvioinut sen toteutumista[134].

Kyberuhkien torjunnassa tarvitaan viranomaisten, elinkeinoelämän, järjestöjen ja kansalaisten välillä yhteinen käsitys turvallisuuskulttuurista sekä eri toimijoiden välillä luottamusta ja yhteistoimintaa, jotta turvallisuus olisi riittävällä tasolla keskinäisriippuvuuksien yhteiskunnassa.[135] Suomen kansallisessa kyberturvallisuusstrategiassa edellytettiin koko yhteiskunnan ympärivuorokautisen tietoturvatoiminnan kehittämistä.

[127] Saarenpää 2016: 168.
[128] Puolustusministeriö 2013.
[129] Suomen kyberturvallisuusstrategia 2013: 5.
[130] Valtioneuvoston periaatepäätös 24.1.2013.
[131] Suomen kyberturvallisuusstrategia 2013: 1.
[132] Puolustusministeriö 2013.
[133] Turvallisuuskomitea.fi: Turvallisuuskomitea – toiminta ja tehtävät.
[134] Turvallisuuskomitea 2017: 4.
[135] Turvallisuuskomitea 2015: 115.

Liikenne- ja viestintäministeriön alaiseen Viestintävirastoon perustettiinkin vuoden 2014 alussa aloittanut Kyberturvallisuuskeskus yhdistetyn kyberturvallisuuden tilannekuvan tuottamiseksi ja ylläpitämiseksi; keskus kerää tietoa kybertapahtumista ja välittää sitä eri toimijoille. Kybertoimintaympäristöön kohdistuvien ja sitä hyödyntävien rikosten esitutkintaviranomaisena toimii poliisi, joka toimii tiiviissä yhteistyössä Kyberturvallisuuskeskuksen kanssa. Kyberturvallisuusstrategiassa linjattiin, että poliisin riittävistä toimivaltuuksista, resursseista sekä osaavasta ja motivoituneesta henkilöstöstä tulee huolehtia. Kybertoimintaympäristöön kohdistuvien ja sitä hyödyntävien rikosten ennaltaehkäiseminen, taktinen esitutkinta sekä digitaalisen todistusaineiston käsittely ja analysointi tulee hoitua.[136]

Euroopan parlamentti ja EU:n neuvosto totesivat, että verkko- ja tietojärjestelmillä ja tietopalveluilla on elintärkeä tehtävä yhteiskunnassa. Niiden luotettavuus ja turvallisuus ovat olennaisen tärkeitä talouden ja yhteiskunnan toiminnoille ja erityisesti EU:n sisämarkkinoiden toiminnalle. Turvapoikkeamien laajuus, esiintymistiheys ja vaikutukset kasvavat ja muodostavat merkittävän uhan verkko- ja tietojärjestelmien toiminnalle. Kyseiset järjestelmät voivat myös joutua sellaisten tahallisten haitallisten toimien kohteeksi, joiden tarkoituksena on vahingoittaa tai häiritä niiden toimintaa ja siten haitata taloudellisen toiminnan harjoittamista, aiheuttaa huomattavia taloudellisia tappioita, heikentää käyttäjien luottamusta ja aiheuttaa merkittävää vahinkoa unionin taloudelle. Verkko- ja tietojärjestelmät – ja ensisijaisesti internet, helpottavat olennaisesti tavaroiden, palvelujen ja ihmisten liikkumista rajojen yli. Tämän ylikansallisen luonteen vuoksi näiden järjestelmien merkittävät häiriöt, olivatpa ne tahallisia tai tahattomia ja riippumatta siitä, missä ne tapahtuvat, voivat vaikuttaa yksittäisiin jäsenvaltioihin ja koko unioniin. Verkko- ja tietojärjestelmien turvallisuus on sen vuoksi olennaisen tärkeää sisämarkkinoiden moitteettomalle toiminnalle.[137]

EU:n direktiivi toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa (EU) 2016/1148 annettiin 6.7.2016. Tällä EU:n verkko- ja tietoturvadirektiivillä (eli niin sanotun NIS-direktiivin[138]) halutaan taata korkea verkko- ja tietojärjestelmien turvallisuus Euroopan unionissa. Direktiivi tuli voimaan elokuussa 2016 ja se tuli saattaa osaksi kansallista lainsäädäntöä 9.5.2018 mennessä. Suomessa direktiivin voimaantulo aiheutti muutoksia useisiin eri lakeihin[139]. Tietyille yhteiskunnan toiminnan kannalta keskeisten palveluiden ja eräiden

[136] Suomen kyberturvallisuusstrategia 2013: 5, 7–8.
[137] (EU) 2016/1148.
[138] *Network and Information Systems* -direktiivi.
[139] Säädöskokoelma 281–292.

digitaalisten palveluiden tarjoajille annettiin tietoturvallisuuteen liittyvää riskienhallintaa ja häiriöiden raportointia koskevia velvoitteita. Lisäksi säädettiin näiden velvoitteiden valvonnasta, viranomaisten välisestä tietojen vaihdosta sekä yleisestä tietoturvallisuuteen liittyvästä viranomaistoiminnasta.[140]

Turvallisuuskomitea ”puskee kyberturvallisuutta parantavia hankkeita eteenpäin”: sen hyväksymä ja 20.4.2017 julkaisema Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017–2020 kokosi yhteen julkisen hallinnon merkittävät kyberturvallisuutta parantavat hankkeet ja toimenpiteet[141]. Globalisaatiosta ja digitalisoitumisesta johtuen Suomen turvallisuusympäristö on muuttunut nopeasti. Turvallisuus- ja toimintaympäristön muutosten myötä kansallisen turvallisuuden uhat, kuten vakoiluun ja terrorismiin liittyvät ilmiöt ja hankkeet tapahtuvat yhä useammin tietoverkoissa, mikä edellyttääkin myös kybertoimintaympäristöön ulottuvia viranomaisvaltuuksia. Toimeenpano-ohjelmaa tarkastellaan ja mitataan vuosittain.[142] Maaliskuussa 2018 julkaistussa valtioneuvoston Kyberturvallisuuden strateginen johtaminen Suomessa -raportissa[143] laadittiin toimenpide-ehdotuksia yhteiskunnan ja julkisen hallinnon strategisen kyberturvallisuuden johtamiseen, kybertoimintaympäristön laajojen häiriötilanteiden hallintaan sekä kyberturvallisuuden tilan mittaamiseen[144]. Raportin suositukset ja havainnot otetaan huomioon myös uuden kyberturvallisuusstrategian laatimisessa[145]; Suomen kyberturvallisuusstrategia 2019 lähti lausuntokierrokselle 6.3.2019[146].

[140] HE 192/2017:1.
[141] Turvallisuuskomitea.fi: Turvallisuuskomitea puskee kyberturvallisuutta parantavia hankkeita eteenpäin
[142] Turvallisuuskomitea 2017: 6.
[143] Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 28/2018.
[144] Lehto, Limnéll, Kokkomäki, Pöyhönen & Salminen (2018): 8.
[145] Turvallisuuskomitean tiedote 18.5.2018.
[146] Turvallisuuskomitean tiedote 6.3.2019.

3. TIETOVERKKOIHIN LIITTYVÄ RIKOLLISUUS

Erilaisten verkossa tapahtuvien tietoteknisten toimintojen yleistyessä myös niihin kohdistuva ja niissä tapahtuva rikollisuus lisääntyy. Moderni tietojenkäsittely eri muodoissaan ja heikon tietoturvan tietoverkot ovat kuitenkin osoittaneet helpon rikosten teon houkuttavuuden yhteiskunnallisena ilmiönä. ’Skimmaus’ (*skimming*) eli maksukortin magneettijuovan tietojen kopiointi[147] on sirukorttien yleistyessä vähentymässä, mutta sitä tapahtuu edelleen, samoin ransomware-hyökkäyksiä. Tietoverkkorikolliset ovat tulleet agressiivisemmiksi ja he ottavat entistä useammin suoraan yhteyttä uhreihinsa: uhri manipuloidaan sosiaalisin keinoin toimimaan rikollisten haluamalla tavalla (*social engineering*). Verkossa olevan lapsiin kohdistuneen seksuaalisen materiaalin määrä kasvaa[148]. Sisäpiiri hyökkäyskanavana ja liiketoiminnan tuhoamiseen pyrkivät kyberhyökkäykset ovat yleistyneet.[149] Kiinnijäämisriski on verraten pieni, vaikka periaatteessa tietoverkossa kaikesta jääkin jälkiä. Rikolliset käyttävät lisäksi anonyymejä kryptovaluuttoja laittomien toimiensa rahoittamiseen. Uusi trendi on *’cryptojacking’* eli kryptovaluuttojen louhinta käyttämällä luvatta kaistanleveyttä ja käsittelytehoa. Nykyisin niin sanottu näkymätön verkko (*darknet*) eli se osa internetiä, mitä normaalikäyttäjä ei tavanmaisesti kohtaa, tunnetuimpana TOR-verkko[150], on enimmäkseen erilaisen rikollisen toiminnan aluetta.[151]

Erilaiset tieto- ja tietotekniikkarikokset ovat saaneet merkittävästi huomiota osakseen mediassa lähinnä uutuusarvostaan johtuen. Näistä tietoverkkojen kautta tehtävistä rikoksista käytetään myös termiä kyberrikos, joita ovat muun muassa petokset, häirintä, uhkailu, laittoman materiaalin levittäminen tai palvelunestohyökkäys. Kyberrikollisuus on tärkein tavalliseen netin käyttäjään kohdistuva uhka[152]. Kyberrikollisuus kehittyy kohtalaisen tuoreena rikollisuudenlajina vauhdikkaasti ICT-tekniikan kehittymisen, uusien verkkopalvelujen käyttöönoton ja internetin käyttäjien määrän vahvan kasvun

---

[147] Skimmaus on yksi maksuvälinepetoksen (RL 8–10 §) tekomuoto. Skimmauslaite lukee magneettikortilta tiedot ja lähettää ne tietoverkkoja pitkin rikolliselle, joka siirtää tiedot tyhjälle kortille ja käy nostamassa rahat jossakin päin maapalloa. Tästä syystä sirullinen maksukortti on turvallisempi. Kodin kyberopas 2017: 31.

[148] Kyseisenlaista materiaalia ovat muun muassa CSEM eli *Child Sexual Exploitation Material,* CAM eli *Child Abuse Material* ja SGEM eli *Self-Generated Explicit Material*.

[149] Sisäministeriö 2017b: 13.

[150] TOR tulee sanoista *The Onion Router* (suomeksi sipulireititin). Se on vapaasti käytettävissä ja ladattavissa oleva maksuton ohjelmisto, joka mahdollistaa verkon anonyymin käytön kenelle tahansa. Järjestelmä salaa TOR-verkon käyttäjän verkkoliikenteen ja suojaa käyttäjänsä identiteetin, sijainnin sekä verkossa toimimisen.

[151] IOCTA 2018: 7–8; Saarenpää 2016: 186, 210.

[152] Kodin kyberopas 2017: 22.

myötä[153]. Lisäksi internetin leviäminen, pilvipalveluiden[154] lisääntyminen ja langattomien laitteiden eksponentiaalinen kasvu ovat osaltaan luoneet uudenlaisen alustan kyberrikollisuuden kasvulle[155].

Maailmanlaajuisesti kyberrikollisuuteen liittyvä lainsäädäntö on hyvin implementoitu: vuonna 2018 tarpeellinen lainsäädäntö on 91 prosentissa valtioista, mikä on parannusta vuoden 2017 tilanteeseen, jolloin lainsäädäntö oli voimassa 79 prosentissa valtioista[156]. Suomen rikoslaissa tietoverkkorikokset eivät kuitenkaan ole yhtenäinen kokonaisuus. Lainvalvontaviranomaisten eli poliisin, Tullin ja Rajavartiolaitoksen tietoon tullutta rikollisuutta tilastoitaessa ei tietoverkkorikoksia tilastoida erikseen eikä niitä ole mainittu lainkaan Suomen virallisessa tilastossa. Esimerkiksi tieto- ja viestintärikokset on keskitetty yhteen rikoslain lukuun (RL 38 luku), mutta tietojärjestelmän luvattomaan käyttöön sovelletaan samaa pykälää kuin ajoneuvon luvattomaan käyttöön (RL 28:7§) ja tietovahingon aiheuttamiseen vahingonteon pykälää (RL 35:1 §).

Suomen ensimmäisessä sisäisen turvallisuuden ohjelmassa 2004 keskeisinä uhkatekijöinä mainittiin turvallisuusviranomaisten viesti- ja tietojärjestelmien haavoittuvuus sekä internet[157]. Toisen, vuoden 2008 ohjelman mukaan tietoverkkoihin oli syntynyt huomattavat mittasuhteet saavuttanut rikollinen infrastruktuuri ja yhtenä keskeisenä alueena mainittiinkin tietoverkkorikollisuuden ja internetin käyttöön liittyvien riskien torjunta. Rajat ylittävänä rikollisuutena ohjelmassa käsiteltiin fyysisten, maantieteellisten rajojen ylittävää rikollisuutta, vaikkakin tietoverkkorikosten vaikutusten todettiin ulottuvan usein usean valtion alueelle: verkossa toimii valtion rajojen yli toimivia rikollisryhmiä, jotka tavoittelevat helposti rahaksi muutettavaa tietoomaisuutta, kuten luottokorttitietoja tai verkkopalvelujen käyttäjätunnuksia.[158] Vuoden 2012 ohjelmassa todettiin tietoverkkorikollisuuden lisääntyvän sitä mukaa, kun ihmiset toimivat ja viettävät yhä enemmän aikaa tietoverkoissa; tietoverkkojen avulla voitiin

[153] Poliisin toimintaympäristö 2018: 103.
[154] Pilvipalvelu on tietojen tallennuspalvelu. Tietojenkäsittelyssä se merkitsee resurssien joustavaa hyödyntämistä kiinteistä sijainpaikoista poiketen: pilvestä saa tiedot käyttöön mistä tahansa ja millä tahansa laitteella. Kun tiedon käsittely ulkoistetaan pois omilta palvelimilta, ei täsmällistä tietoa siitä missä ja miten tietoja käsitellään ole aina saatavilla. Hyvin järjestettynä ja määriteltynä pilvipalvelun käytöstä ei välttämättä seuraa ongelmia, mutta pahimmassa tapauksessa ulkoistamisen riskit ovat merkittäviä. On olemassa mahdollisuus, että rikollinen murtautuu pilvipalveluun ja saa pääsyn siellä oleviin tietoihin. Kodin kyberopas 2017: 17–18; Saarenpää 2016: 67.
[155] Lehtonen 2016: 268–269.
[156] ITU 2018: 12.
[157] Sisäisen turvallisuuden ohjelma 2004: 14.
[158] Sisäisen turvallisuuden ohjelma 2008: kuvailulehti, 11–12.

myös saavuttaa suuria rikoshyötyjä vähäisillä investoinneilla. Toimenpiteet keskittyivät kuitenkin yritysten tietopääomaan kohdistuvia riskien vähentämiseen.[159]

Vuoden 2013 kansallisen kyberturvallisuusstrategian yksi keskeisistä tavoitteista oli kehittää tilannekuvatyötä, mikä oli myös pääministeri Juha Sipilän hallitusohjelmaan[160] kirjattu tavoite. Tietoverkkorikokset ja niihin liittyvä tieto muodostavat yhden osan kybertilannekuvasta. Tietoverkkorikollisuuden tilannekuvatyön kehittäminen aloitettiin poliisissa perustamalla Kyberrikostorjuntakeskus (poliisin kyberkeskus) keväällä 2015. Kyberkeskuksen perustaminen mahdollisti aiempaa laajemmat edellytykset tietoverkkorikollisuuden tutkintaan, ennaltaehkäisyyn ja tilannekuvatyöhön.[161] Poliisihallitus asetti myös kybertyöryhmän laatimaan poliisille kokonaisvaltaisen kybersuunnitelman ja pohtimaan kyberturvallisuuden parantamista sekä luomaan kattavan käsityksen tietoverkkorikollisuuden ja tietoturvallisuuden tilasta, niitä koskevista toimenpiteistä sekä eri organisaatioiden vastuista ja tarpeista[162].

Poliisin sisäisen tilannekuvan kehittäminen alkoi vuoden 2015 syksyllä valtioneuvoston rahoittaessa Tietoverkkorikollisuuden tilannekuvahankkeen[163], jolla kartoitettiin tietoverkkorikollisuuden nykytila ja luotiin pohja tietoverkkorikollisuuden tilannekuvatyön kehittämiselle poliisissa voimassa olevan lainsäädännön viitekehyksessä ja jo olemassa olevin resurssein; lyhyen tähtäimen ratkaisuun päädyttiin, koska lainsäädännölliset muutokset ovat hitaita ja tietoverkkorikollisuus kehittyy ilmiönä nopeasti, jolloin pitkän tähtäimen tavoitteiden lisäksi on tarve nopeammille ratkaisuille.[164] Saman vuoden Turvallinen Suomi[165] -julkaisussa todettiin uhkakuvina, että valtion johtamisessa tarvittaviin tieto- ja viestintäteknologiaa hyödyntäviin palveluihin ja niitä ohjaaviin tietoihin voidaan vaikuttaa kybertoimintaympäristössä ja niiden käyttöä voidaan häiritä, estää tai lamauttaa. Järjestäytynyt rikollisuus ammattimaistuu ja kansainvälistyy

[159] Sisäisen turvallisuuden ohjelma 2012: 22, 47.
[160] Sipilän hallitus toimi hallituksena 29.5.2015 alkaen kariutumiseensa asti 8.3.2019, minkä jälkeen se jatkoi toimintaansa toimitusministeriönä uuden hallituksen muodostamiseen asti.
[161] Leppänen ym. 2016: 6.
[162] Poliisihallitus asetti poliisin kybertyöryhmän 25.3.2015 toteuttamaan poliisin kokonaisvaltaisen kybersuunnitelman ja pohtimaan kyberturvallisuuden parantamista. Työ tehtiin viidessä alatyöryhmässä.
[163] Selvityshanke kesti lokakuusta 2015 helmikuuhun 2016 ja se toteutettiin Poliisiammattikorkeakoululla. Muut selvitykseen osallistujat olivat Poliisin Kyberrikostorjuntakeskus, Viestintäviraston Kyberturvallisuuskeskus ja Tampereen yliopisto. Hanke toimi linjassa poliisin kybertyöryhmän kanssa ja siinä esiintuodut kehittämisehdotukset olivat osa kybertyöryhmän selvitystä.
[164] Leppänen, Linderborg & Saarimäki 2016: 2, 6, 8, 30; Sisäministeriö 2017b: 7–8.
[165] Turvallinen Suomi -julkaisut juontavat juurensa jo monen vuosikymmenen ajan julkaistuihin kokonaismaanpuolustuksen avainteoksiin. Yhteiskunnan nopea muutos luo tarpeen tiedon jatkuvalle uudistamiselle, miksi julkaisun rakennetta ja sisältöä arvioidaan jatkuvasti vuosittain. Turvallisuuskomitea 2015: 3–4.

Suomessakin. Henkilöiden, pääomien ja tavaroiden vapaata liikkuvuutta hyödyntämällä on helppo toteuttaa rikoksia ja pakoilla rikosvastuuta. Suomi oli toistaiseksi säästynyt suurta vahinkoa aiheuttaneilta tietoverkkorikoksilta, mutta tietoverkoissa tapahtuvan rikollisuuden arvioitiin lisääntyvän. Kansallisen yhteistyön lisäksi tarvittiin kykyä toimia kybertoimintaympäristössä Suomen rajojen ulkopuolella.[166]

Digitaalinen toimintaympäristö on olennainen osa rikollisuuden ja rikostorjunnan toimintaympäristöä, sillä tietoverkkoympäristössä tehdään yhä suurempi osa poliisin tietoon tulleista rikoksista. Lisäksi tähän kyberympäristöön tahallisesti toteutetun kohdistuvan poikkeaman taustalla on lähes aina rikos. Tietoverkkorikollisuudesta on tullut hyvin kattava rikollisuuden osa-alue ja sen vaikutukset kohdistuvat niin valtioihin, yksityisiin kansalaisiin kuin liiketoimintaan. Digitalisaation seurauksena rikolliset voivat toimia verkossa nopeasti ja valtioiden rajat ylittäen; samalla todistusaineisto digitalisoituu ja on entistä helpompi kätkeä ja tuhota. EU:n sisäisen turvallisuuden strategian yksi tärkeimmistä painopistealueista vuosille 2015–2020 on tietoverkko-rikollisuuden torjunta. Suomessa poliisi panostaa tietoverkkorikollisuuden torjuntaan osana järjestäytyneen rikollisuuden torjuntaa.[167] Poliisi uutisoi 29.3.2019 järjestäytyneen rikollisuuden uhan kasvavan Euroopassa ja että EU:n rikostorjunnan painopistealueiksi vuosille 2018–2020 on määritelty kyberrikollisuus, huumausaine-rikollisuus, laittoman maahantulon järjestäminen, järjestäytynyt omaisuusrikollisuus, ihmiskauppa, laittomat ampuma-aseet, ympäristörikokset ja EU:n taloudellisiin intresseihin kohdistuvat petokset[168].

Tietokoneisiin, tietotekniikkaan ja tietoverkkoihin liittyvien rikosten suojeluobjekti voidaan ilmaista termillä ’tietojenkäsittelyrauha’, josta esiintyy oikeuskirjallisuudessa myös latinankielinen nimitys ’Pax Computationis’. Tietojenkäsittelyrauha kuvaa yhdellä ilmaisulla sen, mitä esimerkiksi YK:n, OECD:n[169], Euroopan neuvoston ja Suomen valtioneuvoston tietoturvallisuuspäätökset selittävät tarkemmin kolmen peruskäsitteen eli luottamuksellisuuden (*confidentiality*), eheyden (*integrity*) ja käytettävyyden (*availability*) avulla. Tietoturvallisuus kuvaa sekä fyysisen että digitaalisen tiedon luottamuksellisuuden, käytettävyyden ja eheyden turvaamista. Tietoturvallisuus onkin tavoitetila, jossa sekä tiedot, järjestelmät että palvelut saavat asianmukaista suojaa niin normaali- kuin poikkeusoloissakin lainsäädännön ja muiden toimenpiteiden avulla

[166] Turvallisuuskomitea 2015: 24, 119–120.
[167] Sisäministeriö 2017b: 7, 12, 19–20; Suomen kyberturvallisuusstrategia 2013: 27.
[168] Poliisi 29.3.2019.
[169] *Organisation for Economic Cooperation and Development* eli Taloudellisen yhteistyön ja kehityksen järjestö. Suomi on ollut vuonna 1961 perustetun OECD:n jäsen vuodesta 1969 alkaen.

niiden luottamuksellisuuteen, eheyteen ja käytettävyyteen kohdistuvia laitteisto- ja ohjelmistovioista, luonnontapahtumista tai tahallisista, tuottamuksellisista ja tapaturmaisista inhimillisistä teoista johtuvia uhkia ja vahinkoja vastaan. Kyberturvallisuus puolestaan kuvaa koko sähköisen toimintaympäristön turvallisuutta, johon kuuluu tiedon lisäksi koko muu infrastruktuuri tietoverkoista sovelluksiin.[170]

Vuonna 1988 lainsäätäjä Suomessa totesi rangaistavaksi teonkuvan, jossa tietojenkäsittelyjärjestelmä saadaan tuottamaan virheellistä tietoa; kysymyksessä on rikoslain säännös niin sanotusta tietojenkäsittelypetoksesta (HE 66/1988)[171]. Vuonna 1993 tietojärjestelmien toimivuus ja tietohallinnon luotettavuus sinänsä voitiin ’nykyaikaisessa yhteiskunnassa’ nähdä itsenäisenä oikeushyvänä ja tuolloin lainsäädännöllä pyrittiin turvaamaan niin sanottua tietokonerauhaa (HE 94/1993)[172]. Vuonna 1997 ’haitaksi’ todettiin paitsi suoranainen, esimerkiksi tiedostojen hävittämisenä tai muuttumisena syntyvä vahinko, myös mikä tahansa muu sellainen vaikutus tieto- tai telejärjestelmän toimintaan, joka jollain tavalla loukkaa järjestelmän haltijan tai muun sen käyttöön oikeutetun oikeutta järjestelmän käyttöön eli niin sanottua tietojenkäsittelyrauhaa (HE 233/1997)[173]. Euroopan neuvoston vuoden 2001 tietoverkkorikollisuutta koskevan yleissopimuksen eli niin sanotun tietoverkkorikossopimuksen (ETS 185)[174] tarkoituksena onkin tietojenkäsittelyrauhan turvaaminen. Sopimuksen mukaan on tavoitteen toteuttamiseksi ensisijainen ja tehokkain keino riittävästä tietoturvasta huolehtiminen, minkä lisäksi tarvitaan myös rikosoikeudellista suojaa.[175]

Tietoverkkorikossopimuksen nimessä tietoverkkorikos tarkoittaa samaa asiaa kuin tietotekniikkarikos. Tietotekniikkarikoksella tarkoitetaan yhtäältä rikosta, joka kohdistuu tietojärjestelmään, ja toisaalta rikosta, joka tehdään tietojärjestelmän avulla. Yhteistä näille kahdelle rikostyypille on se, että niiden tekoympäristönä on tietojärjestelmä ja niiden tekeminen yleensä edellyttää jonkinlaista asiantuntemusta tietojärjestelmien toiminnasta. Koska tietotekniikkarikoksissa todistusaineisto on lähes yksinomaan sähköisessä muodossa, sen muuntelu ja hävittäminen on poikkeuksellisen helppoa. Tietotekniikkarikollisuus on myös rajat ylittävää rikollisuutta, minkä vuoksi tutkinta-

[170] HE 233/1997: 4; Sisäministeriö 2017b: 11.
[171] Tietojenkäsittelypetos, RL 36:1.2 §. Tietojenkäsittelypetokseen kuuluu aina tietojenkäsittelyn lopputuloksen vääristäminen. Tietojenkäsittelyyn puututaan hyötymistarkoituksessa vääristämällä tietojenkäsittelyn lopputulos syöttämällä tietojenkäsittelylaitteeseen vääriä tietoja tai muuten puuttumalla koneelliseen tietojenkäsittelyyn. HE 66/1988: 133.
[172] Tietomurto, RL 38: 8 §. Tietomurtoa koskevilla säännöksillä pyritään turvaamaan niin sanottua tietokonerauhaa eli tietojärjestelmiä ulkopuolista tunkeutumista vastaan. HE 94/1993: 133, 155.
[173] HE 233/1997: 9.
[174] *Convention on Cybercrime* ETS no. 185, tunnettu myös niin sanottuna Budapestin sopimuksena.
[175] HE 153/2006 vp: 13.

toimenpiteiden nopeus on ratkaisevassa asemassa eikä kansainvälinen yhteistyö siedä viivyttelyä. Tietoverkkorikossopimus ja sen kansallinen voimaansaattaminen pyrki suojelemaan yhteiskuntaamme tietotekniikkarikollisuudelta sekä sen aiheuttamilta vahingoilta yhtenäistämällä ja laajentamalla sitä koskevia rangaistussäädöksiä, samoin tehostamalla rikostutkintaa ja kansainvälistä oikeudellista yhteistyötä. Kyseinen yleissopimus on tullut kansainvälisesti voimaan 1.7.2004.[176]

Euroopan komissio[177] julkaisi puolestaan tiedonannon turvallisemman Internetin aikaansaamiseksi (KOM(2000) 890)[178] vuonna 2001 ja sitä päivitettiin vuonna 2007 tiedonannolla Tavoitteena yleinen toimintalinja tietoverkkorikollisuuden torjumiseksi (KOM(2007) 267). Siinä tietoverkkorikollisuuden torjunnan todettiin olevan keskeisimpiä kysymyksiä liittyen nyky-yhteiskunnassa yhä tärkeämmäksi muuttuvien tietojärjestelmien turvallisuuteen. Tietoverkkorikollisuudelle ei ollut sovittu yhteistä määritelmää; ’tietoverkkorikollisuutta’, ’tietokonerikollisuutta’ ja ’huipputeknologiaa käyttävää rikollisuutta’ käytettiin usein samassa merkityksessä. Komissio tarkoitti tietoverkkorikollisuudella rikoksia, jotka tehdään sähköisiä viestintäverkkoja ja tietojärjestelmiä hyödyntäen tai jotka kohdistuvat mainittuihin verkkoihin ja järjestelmiin.[179] Vuoden 2013 EU:n kyberturvallisuusstrategiassa (JOIN(2013)[180]) Euroopan komissio totesi tietoverkkorikollisuuden viittaavan yleisesti laajaan valikoimaan erilaisia rikollisia toimia, joissa tietokoneet ja tietojärjestelmät ovat joko ensisijainen työkalu tai ensisijainen kohde.[181]

Käytännössä tietoverkkorikollisuus jaetaan Euroopan komissiossa kolmeen alaryhmään, joista ensimmäiseen kuuluvat perinteiset rikollisuuden muodot, kuten petokset ja väärentäminen, mitkä ovat tehty käyttäen sähköisiä verkkoja ja tietojärjestelmiä. Toinen ryhmä sisältää laittomaan sisältöön liityvät rikokset, muun muassa lapsen seksuaalista hyväksikäyttöä esittävän tai rotuvihaan yllyttävän materiaalin, julkaisemisen sähköisissä viestimissä. Kolmas ryhmä käsittää rikokset, joita esiintyy ainoastaan sähköisissä verkoissa, kuten hyökkäykset tietojärjestelmiä vastaan, palvelunesto tai hakkerointi.[182]

---

[176] HE 153/2006 vp: 4.
[177] Euroopan komissio on ainoa EU:n toimielin, joka voi esittää lainsäädäntöä Euroopan parlamentin ja neuvoston hyväksyttäväksi. Sen tehtäviin kuuluu uusien lakiehdotusten valmistelu sekä EU:n lainsäädännön toteutumisen valvominen.
[178] Komission tiedonanto neuvostolle, Euroopan parlamentille, talous- ja sosiaalikomeitealle ja alueiden komitealle: Turvallisempaan tietoyhteiskuntaan tietojärjestelmien turvallisuutta parantamalla ja tietokonerikollisuutta ehkäisemällä. Brysseli 26.1.2001.
[179] Euroopan yhteisöjen komissio 2007; Saarenpää 2016: 212.
[180] *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*.
[181] Euroopan yhteisöjen komissio 2013: 3.
[182] Euroopan yhteisöjen komissio 2013: 3.

Komissio totesikin jo vuonna 2007, että useimmat rikokset on mahdollista tehdä sähköisiä verkkoja hyödyntäen. Erityisen yleisiä perinteisen rikollisuuden muotoja ovat erityyppiset petokset ja näiden yritykset; esimerkiksi väärän henkilöllisyyden käyttöä, *phishing*-hyökkäyksiä[183], roskapostia ja haittaohjelmia[184] voidaan hyödyntää suurimittaisissa petoksissa. Internetin välityksellä toteutettava huumausaineiden sekä uhanalaisten eläinten ja aseiden laiton kansallinen ja kansainvälinen kauppa muodostavat kasvavan ongelman. Lisäksi on yhä enemmän verkkosivustoja, jotka käsittävät laitonta sisältöä. Kyseisenlaisiin sivustoihin on erittäin vaikea puuttua lainvalvonnan keinoin. Laajamittaiset hyökkäykset tietojärjestelmiä tai organisaatioita ja yksityishenkilöitä vastaan olivat jo tuolloin hyvin yleisiä.[185]

Suomen vuoden 2008 sisäisen turvallisuuden ohjelmassa tietoverkkorikollisuus jaettiin tekotapojen perusteella Euroopan komission tavoin kolmeen ryhmään: Ainoastaan tietoverkoissa esiintyvinä rikoksina mainittiin esimerkiksi tietomurrot, palveluksenestohyökkäykset ja haittaohjelmien avulla tapahtuvat ns. identiteettivarkaudet; ne uhkaavat teknisten järjestelmien toimintaa ja saattavat myös vaarantaa niistä riippuvaisia yhteiskunnan kriittisiä perustoimintoja. Tietoverkkorikokset voivat liittyä laittomaan tietosisältöön, kuten esimerkiksi rotuvihaan yllyttämiseen, lasten seksuaalista hyväksikäyttöä esittävän materiaalin julkaisemiseen tai tekijänoikeuksien suojaaman materiaalin levittämiseen. Tavanomaisia rikoksia, kuten petoksia ja väärennyksiä, toteutetaan tietoverkoissa tavoitteena lisätä tehokkuutta, taloudellisuutta sekä mahdollisuutta häivyttää tekijään itseensä viittaavat jäljet. Ohjelmassa todettiin, että tietokoneet, tiedonsiirtoverkot ja erilaiset päätelaitteet liittyvät lähes aina talousrikosten sekä monien muiden tavanomaisten rikosten toteuttamiseen.[186]

Vaikkakaan tietoverkkorikoksesta ei ole vakiintunutta määritelmää, niissä kaikissa korostetaan teknologiaa tekovälineenä, kohteena tai ympäristönä. Määritelmät ovat

---

[183] *Phishingissä* eli niin sanotussa verkkourkinnassa yritetään huijausviestein saada käsiin verkkopankkien käyttäjätunnuksia ja salasanoja, jotta päästäisiin käsiksi asiakkaan tileillä oleviin varoihin; kysymyksessä ovat usein ulkomailta käsin toimivat rikolliset. Sisäministeriö 2017b: 22.

[184] Haittaohjelmat leviävät muun muassa sähköpostien ja saastuneiden nettisivujen kautta. Haittaohjelmia ovat esimerkiksi kiristysohjelmat, vakoiluohjelmat, tietojenkalastelu sekä tietokoneen kaappaus ja palvelunestohyökkäykset. Vakoiluohjelmat ovat haittaohjelmia, jotka keräävät tietoa laitteen käyttäjästä ja lähettävät sitä hyökkääjälle. Vakoiluohjelman voi saada tietokoneelleen esimerkiksi lataamalla netistä ilmaisia ohjelmia, joiden kylkiäisenä koneelle tulee haittaohjelmia, tai niitä levitetään sähköpostiviestissä olevaan liitetiedostoon. Sniffer-niminen haittaohjelma tallentaa koneen ja netin välistä liikennettä yrittäen saada haltuunsa salasanoja ja tunnuksia. Keylogger-haittaohjelma seuraa näppäinten painalluksia ja nauhoittaa ne saaden selville kaiken, mitä koneella tehdään, mukaan lukien salasanat. Kodin kyberopas 2017: 16, 19–20.

[185] Euroopan yhteisöjen komissio 2007.

[186] Sisäisen turvallisuuden ohjelma 2008: 12.

moninaiset ja termien käyttö on usein kontekstiriippuvaista sekä osin päällekäistä[187]. Englanninkielisestä *cyber crime* -käsitteestä käytetään termejä kyberrikos ja kyberrikollisuus sekä tietotekniikkarikos ja tietoverkkorikos toistensa synonyymeinä – toisinaan käytetään termejä tietoverkoissa tapahtuvat rikokset (*cyber enabled crimes*) ja tietoverkkorikokset (*cyber depended crimes*), jotta tiedetään, mistä rikostyypistä keskustellaan[188]. Nykyään käytetään myös termiä digitaalinen rikos (*digital crime*). Sana 'kyber' viittaa sähköiseen tietojenkäsittelyyn eli tietotekniikkaan, sähköiseen tiedonsiirtoon, tietoverkkoihin ja tietokoneisiin[189]. Yleiskielessä kyber-etuliite on ainakin osin korvannut aiemman tieto- ja tietoverkko-etuliitteen kuvaamaan toimintaympäristön muutosta, jossa tietotekninen ympäristö on globaali ja josta modernit yhteiskunnat ovat voimakkaasti keskinäisriippuvaisia. Verkkoympäristö, tietoverkkoympäristö, sähköinen toimintaympäristö, digitaalinen toimintaympäristö, kybertoimintaympäristö ja kyberavaruus ovat nekin toistensa synonyymejä ja tarkoittavat samaa asiaa kuin englannin kielen käsite *cyber space*.[190]

Suomessa Poliisihallituksen asettama kybertyöryhmä otti vuonna 2015 kantaa kauan aikaa sitten tunnistettuun haasteeseen eli tietoverkkorikoksen ja tietoverkkoja hyväksikäyttäen tehtyjen rikosten suhteeseen. Tietoverkkorikoksella tarkoitetaan samaa kuin kyberrikoksella, joilla tarkoitetaan sellaisten rikosten tekomuotoja, joita esiintyy ainoastaan tietojärjestelmissä, kuten esimerkiksi hakkerointi, hyökkäykset tietojärjestelmiä vastaan, haittaohjelmien avulla tehdyt identiteettivarkaudet ja palvelunestohyökkäykset. Tietoverkkoja hyväksikäyttäen tehdyillä rikoksilla tarkoitetaan perinteisiä rikollisuuden tekomuotoja, jotka on tehty tietoverkko- tai tietojärjestelmiä hyväksikäyttäen kuten esimerkiksi nettipetokset, maksuvälinepetokset, lapsen seksuaalista hyväksikäyttöä esittävän materiaalin levittäminen, piratismi ja muut tekijänoikeusrikokset, rahanpesu, kunnianloukkaukset ja rasismi.[191] Poliisissa tietoverkkorikokset on siis jaettu tietoverkkoympäristöön kohdistuviin rikoksiin eli niin sanotusti puhtaisiin tietoverkkorikoksiin sekä tietoverkkoympäristöä hyväksi käyttäen tehtyihin rikoksiin.[192]

Tietoverkkorikollisuus on suuressa määrin piilorikollisuutta ja ilmoitusmäärät pieniä. Esimerkiksi Helsingissä tutkittiin törkeää tietomurtoa, jossa uhreja oli 50 000, mutta

[187] Leppänen ym. 2016: 8.
[188] Poliisin toimintaympäristö 2018: 104.
[189] Kodin kyberopas 2017: 22.
[190] Sisäministeriö 2017b: 10–11.
[191] Leppänen ym. 2016: 25; Poliisihallitus 2015b.
[192] Sisäministeriö 2017b: 10.

siitä kirjattiin vain yksi rikosilmoitus. Sen lisäksi tietoverkkorikosten tilastointimahdollisuudet ovat puutteelliset. Puhtaita tietoverkkoon, tietojärjestelmään tai sen sisältämiin tietoihin kohdistuvia rikoksia voidaan rikosnimikkeiden perusteella saada tilastoiduksi, kun taas tietoverkkoympäristöä hyväksikäyttäen tehtyjen rikosten määristä ei ole saatavilla tilastotietoa. Nimikkeitä on runsaasti ja rajanvedot ovat epäselviä, joten pelkästään rikosnimikkeiden perusteella ei nykyisellään pystytä tuottamaan poliisin rikosilmoitusjärjestelmästä luotettavaa tietoa tietoverkkorikosten lukumääristä, tekotavoista ja rikoksella aiheutettujen vahinkojen määrästä. Iso osa samoilla rikosnimikkeillä kirjattavista teoista voidaan kuitenkin tehdä joko tietoverkkoympäristössä tai reaalimaailmassa.[193]

3.1. Tietoverkkoihin liittyvä rikosoikeudellinen kehitys

Tietokoneiden, tietojärjestelmien ja tietoverkkojen merkityksen muutokseen liittyy monien oikeudellisten kysymyksenasetteluiden sekä viime kädessä oikeuksien muutostarpeita sekä muutoksia. Siinä missä verkkojen käytön alkuvaihe oli rikosoikeudellisesti vähemmän kiinnostavaa aikaa, olivat tietojenkäsittely ja tietoverkot yleistyessään muuttuneet niin uusien rikostyyppien teon foorumeiksi kuin ammatillisen rikollisuuden kohteeksi. Rikostutkinnassa oli tieto- ja viestintätekniikan (ICT) käyttöönoton aluksi törmätty suhteellisen harvoin tilanteisiin, joissa perinteinen lainsäädäntö ei soveltuisi myös tietotekniikkarikoksiin. Suomen rikoslakia on tietoteknisen kehityksen myötä kuitenkin jouduttu täsmentämään useaan otteeseen ensin informaatioyhteiskuntaan ja sittemmin verkkoyhteiskuntaan siirtymisen mukaisesti.[194]

Euroopan neuvosto käsitteli *tietokonerikoksia* jossain määrin jo vuonna 1981. Se asetti asiantuntijakomitean selvittämään eri tietokonerikosten ilmenemismuotoja, laatimaan kansallisille lainsäätäjille ohjenormeja ja kehittämään myös alan käsitteistöä. Kyseisessä tietokonerikoskomiteassa omaksuttiin linja, joka pyrki välttämään ylipäätään tietotekniikan ja tietokonerikollisuuden merkityksen ylikorostamista; automaattinen tietojenkäsittely oli tuolloin uusi ilmiö – ja vaikkakin se oli luonut eräitä uusia rikoksentekomahdollisuuksia sekä aikaansaanut uudenlaisia piirteitä monille perinteisille rikoksille, tietotekniikan kehitys oli komitean mukaan otettava huomioon rikosoikeusjärjestelmää kehitettäessä kuitenkin muun järjestelmän osana eikä erillisenä ilmiönä. Suomessakin on ollut lähtökohtana tietotekniikkaneutraali rikoslainsäädäntö; näin siitä huolimatta,

[193] Sisäministeriö 2017b: 23–24.
[194] Saarenpää 2016: 29, 210–211, 186.

että yhteiskuntamme eteni kohti verkkoyhteiskuntaa[195]. Euroopan neuvoston tietokonerikoskomiteassa vähemmistöön jääneen käsityskannan mukaan tietotekniikka olisi tullut määritellä kriminaalipolitiikassa kokonaan uudeksi elämänalueeksi ja yleinen luottamus tietotekniikkaan kokonaan uudeksi oikeushyväksi, joka vaati omintakeisen sääntelyn.[196]

Tietokonerikoskomitean työ siihen sisältyvine suosituksineen valmistui vuonna 1989 ja Euroopan neuvoston ministerikomitea hyväksyi suositukset samana vuonna. Komitea suositti, että rangaistavaksi säädettäisiin vähintään tietokonepetos, tietokoneväärennys, datan tai ohjelmiston vahingoittaminen, tietokonesabotaasi, luvaton tietojärjestelmään tunkeutuminen ja luvaton viestin sieppaaminen. Jäsenmaita kehotettiin antamaan raporttinsa vuoden 1993 aikana lainsäädännön kehityksestä tietokonerikollisuuden alalla. Suomen rikoslaki on peräisin vuodelta 1889 ja sitä on useasti muutettu. Suomessa oli saatu jo vuonna 1988 voimaan tulleeseen henkilörekisterilakiin (471/87) säännös, jossa kriminalisoitiin oikeudeton tunkeutuminen automaattisen tietojenkäsittelyn avulla ylläpidettyyn henkilörekisteriin. Oli kuitenkin aika ja halu saattaa tieto- ja viestintärikokset nopean teknisen kehityksen tasalle myös Suomessa. Niitä koskevat säännökset olivat hajallaan eri laeissa ja ne soveltuivat huonosti “nykyaikaiseen” (tuon ajan) tietotekniikkaan, joka oli muuttanut tiedon käsittelyn, tallennuksen ja siirron teknisiä keinoja. Lisäksi tieto- ja viestintätekniikan kehitys oli synnyttänyt aivan uusia ilmiöitä, joita koskevat tarpeelliset rangaistukset puuttuivat kokonaan.[197]

Tietokonerikoskomitean suosituksen mukaan tietokonepetoksena tuli rangaista sellainen datan tai ohjelmiston syöttäminen tietojärjestelmään, sen hävittäminen tai käytön estäminen taikka muu tiedonkäsittelyn lopputulokseen vaikuttava tietojenkäsittelytapahtumiin puuttuminen, joka aiheuttaa toiselle omaisuuden menetyksen tai taloudellista vahinkoa. Tietokoneväärennys tarkoitti komitean mukaan sellaista datan tai ohjelmiston syöttämistä, muuttamista, hävittämistä tai sen käytön estämistä taikka muuta tietojenkäsittelyyn puuttumista sellaisella tavalla taikka sellaisissa olosuhteissa, että tekoa olisi pidettävä väärennysrikoksena, jos sen kohteena olisi ollut väärennysrikoksen perinteinen kohde kuten asiakirja tai muu sellainen todistuskappale. Datan tai ohjelmiston vahingoittaminen koski sen oikeudetonta hävittämistä, vahingoittamista, huonontamista tai sen käytön estämistä. Tietokonesabotaasilla tarkoitettiin sellaista datan tai ohjelmiston syöttämistä, muuttamista, hävittämistä tai pimittämistä taikka tietokonejärjestelmiin puuttumista, jonka tarkoituksena on estää tietokoneen tai

[195] Saarenpää 2016: 185.
[196] HE 94/1993: 17–18.
[197] HE 94/1993: 1, 11, 17–18, 137.

televiestintäjärjestelmän toiminta. Luvaton järjestelmään tunkeutuminen tarkoitti turvajärjestelyt murtamalla tehtyä oikeudetonta tunkeutumista tietojärjestelmään tai tietoverkkoon ja tietokonejärjestelmässä kulkevien viestien sieppaaminen olisi säädettävä rangaistavaksi silloin, kun se tapahtuu oikeudettomasti ja teknisiä apuvälineitä hyväksikäyttäen.[198]

Suomessa toteutettiin rikoslain kokonaisuudistus, jolla rikoslaki saatettiin vastaamaan muuttuneita olosuhteita. Uudistus toteutettiin vaiheittain vuosina 1980 – 1999 ja sen ensimmäinen vaihe koski omaisuus-, vaihdanta- ja talousrikoksia; siihen sisältyvät uudet säännökset tulivat voimaan vuoden 1991 alusta (RL 769/1990).[199] Tuolloin toteutettiin petoksen, väärennyksen, luvattoman käytön ja vahingonteon tunnusmerkistöjen nykyaikaistaminen siten, että ne soveltuvat myös automaattisen tietojenkäsittelyn mahdollistamien tekojen arvostelemiseen.[200] Muiden maiden esimerkkiä seuraten uuden tietotekniikan vaikutukset otettiin huomioon siten, että ensisijaisesti tarkistettiin ja täydennettiin perinteisiä käsitemääritelmiä ja rikostunnusmerkistöjä. Rikoslain petossäännökseen lisättiin niin sanotun tietokonepetoksen kriminalisointi (RL 36:1.2 §): petosrikos voi ilmetä myös koneellisen tietojenkäsittelyn lopputuloksen vääristämisenä eli niin sanottuna tietokonepetoksena – eli ihmisen erehdyttämiseen rinnastettiin koneellisen tietojenkäsittelyn lopputuloksen vääristely.[201]

Rikoslain kokonaisuudistuksen ensimmäisessä vaiheessa muutettiin väärennysrikoksia koskevia säännöksiä (RL 33:1–3 §) siten, että väärennyksen kohteena voi olla myös automaattiseen tietojenkäsittelyyn soveltuva tallenne. Tekniikka oli monessa tapauksessa tehnyt esineen käytön riippumattomaksi esineen hallinnasta. Niinpä toisen omistaman tietokoneen käyttö puhelinlinjan välityksellä tuli rangaistavaksi luvattomana käyttönä (RL 28:7 §), vaikkei tietokoneen fyysistä haltuunottoa ollut tapahtunut. Uudistettu vahingontekosäännös (RL 35:1.2 §) sisälsi tietokoneelle tallennetun tiedon tai muun tallennuksen oikeudettoman hävittämisen, turmelemisen, kätkemisen tai salaamisen. Säännöksen katsottiin kattavan myös tietokonesabotaasin lievemmät muodot, mutta vakavimmat tietojärjestelmän toimintaan kohdistuvat loukkaukset tulivat arvosteltaviksi rikoslainsäädännön toisessa vaiheessa säädetyn uuden tuhotyösäännöksen rinnakkaisen teonkuvauksen nojalla (RL 34:1.2 §): vaarantamisen kohteena

[198] HE 94/1993: 18–19.
[199] HE 66/1988: 1; HE 94/1993: 1.
[200] HE 94/1993: 133.
[201] HE 66/1988: 128, 130.

ovat eräät yhteiskunnalle tärkeät toiminnot[202] ja omaisuuden vahingoittamisen ohella tekotapana on vahingoittamista perusteellisempi teko, tuhoaminen; teko edellytti oikeudetonta puuttumista tuotanto-, jakelu- tai tietojärjestelmän toimintaan.[203]

Rikoslakia vuonna 1995 uudistettaessa pyrittiin nopea tietotekniikan kehitys ottamaan huomioon. ”Nykyaikainen” tietotekniikka oli muuttanut tiedon käsittelyn, tallennuksen ja siirron teknisiä keinoja. Lisäksi tieto- ja viestintätekniikan kehitys oli synnyttänyt aivan uusia ilmiöitä, joita koskevat rangaistussäännökset puuttuivat kokonaan. Rikoslain kokonaisuudistuksen toisessa vaiheessa tieto- ja viestintärikoksia koskevat säännökset uudistettiin kokonaan ja ne keskitettiin yhteen rikoslain lukuun (38 luku), mikä on omiaan korostamaan tiedon ja viestinnän entistä suurempaa merkitystä. Laadittiin viestintäsalaisuuden loukkausta, tietoliikenteen häirintää ja tietomurtoa koskevat täysin uudet rangaistussäännökset. Uudistukset sisältänyt rikoslain muutos astui voimaan 1.9.1995 (RL 578/1995). Lain esitöiden (HE 94/1993) mukaan ’tieto’ voi viitata tietoon informaationa tai se voi myös tarkoittaa niin sanottua ’dataa’, joka kuvaa tietoa esittäviä merkkejä. Esitöissä tarkennettiin, että tiedossa informaationa on kyse itse tiedon sisällöstä, mutta tietorikoksissa rikosoikeudellisen suojelun kohteena on informaation lisäksi tietojärjestelmien luotettavuus yleensä. Kyseisen hallituksen esityksen mukaan viestinnällä ymmärretään tiedon lähettämisen ja vastaanottamisen muodostamaa kokonaisuutta, jolloin viestintärikoksissa loukataan viestintäsalaisuutta.[204]

Viestintäsalaisuuden loukkaus (RL 38:3–4 §) koski sekä tietokonejärjestelmässä välitettävän viestin sieppaamisen että televerkossa välitettävänä olevan puhelun, sähkeen, tekstin-, kuvan- tai datasiirron sisällön oikeudettoman tiedon hankkimista. Tietoliikenteen häirintä (RL 38:5–6 §) puolestaan kriminalisoi tele- tai radioviestinnän oikeudettoman estämisen, siinä käytettävien laitteiden toimintaan puuttumisen sekä häiritsevien viestien lähettämisen ilkivaltaisessa tarkoituksessa. Tietomurron sanktiointi (RL 38:8 §) liittyi luvattoman käytön rangaistussääntelyyn, mikä Suomen rikoslain-säädännössä on perinteisesti ollut hyvin laaja. Tietokoneen luvaton käyttö oli rangaistavaa jo rikoslain kokonaisuudistuksen ensimmäisen vaiheen säännösmuutoksen jälkeen, kun tapauksia ei erotettu enää sillä perusteella, kenen hallussa luvattomasti käytetty irtain omaisuus on; nimike kattoi myös tietojärjestelmän luvattoman etäkäytön

[202] Ne yhteiskunnalliset toiminnot, joita säännös suojaa, ovat energiahuolto, yleinen terveydenhoito, maanpuolustus, oikeudenhoito sekä muu näihin rinnastettava yhteiskunnan tärkeä toiminto, jollaisena voidaan pitää myös poliisin tietokonejärjestelmää, valtiovieraiden suojelua ja muuta merkittävää turvallisuusjärjestelyä.
[203] HE 94/1993: 18–19, 117, 120–121.
[204] HE 94/1993: 11, 132–133.

viestintälinjojen välityksellä. Rikoslakiin haluttiin kuitenkin ottaa säännös, joka kriminalisoi erityisesti turvajärjestelyn murtamalla oikeudettomasti tapahtuneen tunkeutumisen tietojärjestelmään. Tällöin rangaistavaa oli jo pelkkä järjestelmään murtautuminen, vaikkei varsinaista järjestelmän luvatonta käyttöä tapahtuisikaan.[205]

Tietokoneviruksien[206] valmistaminen ja levittäminen todettiin aiheuttavan yleistä vaaraa, joten teko kriminalisoitiin ottamalla rikoslakiin (RL 951/1999) yleisvaarallisia rikoksia koskevaan 34 lukuun uusi säännös vaaran aiheuttaminen tietojenkäsittelylle (RL 34:9a §). Aiemmin viruksen valmistaminen tai levittäminen ei sellaisenaan ollut rangaistavaa. Sitä, jonka toimenpiteiden seurauksena virus oli saastuttanut tietojärjestelmän oli voitu rangaista vasta sitten, kun aktivoitunut virus oli aiheuttanut vahinkoa. Kun virus oli hävittänyt tai turmellut tallennetun tiedon, täyttyi vahingontekorikoksen tunnusmerkistö, mikäli aiheuttaja oli menetellyt tahallisesti tarkoituksenaan toisen vahingoittaminen. Viruksen leviäminen saattaa myös olla sattumanvaraista taikka toisen huolimattomuudesta johtuvaa. Sen aiheuttama vahinko saattaa myös olla ainoastaan vähäistä eikä tallennettua tietoa häviä tai turmellu. Virustartunnan aiheuttaessa vakavaa vaaraa teko voisi tulla rangaistavaksi tuhotyönä. Vaaran aiheuttamisessa tietojenkäsittelylle edellytettiin tekijältä tahallisuutta eli tarkoituksena aiheuttaa haittaa tietojenkäsittelylle tai tieto- tai telejärjestelmän toiminnalle. Teon kriminalisointi tuli voimaan 1.1.1999.[207]

Suomessa lainsäätäjä ehdotti vuonna 2003 muuttamaan tietojenkäsittelypetoksen (RL 36:1.2 §) määritelmää ja korvaamaan sanan ’tieto’ sanalla ’data’, joka vastasi tietoverkkorikossopimuksessa käytettyä datan määritelmää: data tarkoittaa sellaisessa muodossa olevien tosiseikkojen, tietojen tai käsitteiden esitystä, että se soveltuu käsiteltäväksi tietojärjestelmässä, mukaan lukien ohjelmat, joiden avulla tietokone pystyy suorittamaan jonkin toiminnon. Keskeistä datan määritelmässä on, että tiedon – ollakseen dataa – pitää olla sähköisessä tai muussa sellaisessa muodossa, että se sellaisenaan soveltuu käsiteltäväksi tietojärjestelmässä; yleissopimuksen tultua voimaan sana ’data’ tuli käytettäväksi muuallakin rikoslaissa sekä pakkokeinolainsäädännössä. Lisäksi ehdotettiin muutenkin muuttamaan tietoteknistä käsitteistöä: lainsäädännössä aiemmin käytetty tietojenkäsittelylaite viittasi sellaiseen tietotekniseen ympäristöön,

[205] HE 94/1993: 1–2, 19, 21, 133.
[206] Lain esitöiden mukaan tietokonevirus tai atk-virus tarkoittaa sellaista tietokoneohjelmaa tai ohjelmakäskyjen sarjaa, joka on tarkoitettu haittaamaan tietojenkäsittelyä tai tieto- tai telejärjestelmän toimintaa taikka vahingoittamaan järjestelmän sisältämiä tietoja tai ohjelmistoja. Kyseisiä ohjelmia koskeva terminologia on harhaanjohtavaa, sillä virukset ovat vain yksi tällaisten ohjelmien alalaji, vaikkakin ne ovat yleisin ohjelmatyyppi. HE 233/1997: 3.
[207] HE 233/1997: 1, 6–8.

johon tietoverkot eivät vielä oleellisena osana kuuluneet, kun ehdotettu käsite ’tietojärjestelmä’ kattaa sekä tietoverkot että yksittäiset tietokoneet. (HE 2/2003.)[208]

Euroopan neuvosto otti tietoverkot ja tietojärjestelmät erityissääntelyn kohteeksi niiden yhteiskunnallisen merkityksen vuoksi vuonna 2001, mikä konkretisoitui jo aiemmin mainittuna Euroopan neuvoston tietoverkkorikollisuutta koskevana yleissopimuksena (ETS 185) eli niin sanottuna tietoverkkorikossopimuksena. Yleissopimuksessa käytettiin termiä tietoverkkorikos synonyyminä tietotekniikkarikokselle ja se kattoi kaksi rikostyyppiä: tietojärjestelmään kohdistuvat rikokset ja tietojärjestelmän avulla tehtävät rikokset. Suomen rikoslakia täydennettiin yleissopimuksen edellyttämällä tavalla vuonna 2007 (RL 540/2007). Yleissopimuksella ja sen kansallisella voimaansaattamisella pyritään suojelemaan yhteiskuntaa tietotekniikkarikollisuudelta ja sen aiheuttamilta vahingoilta rangaistussäädöksiä yhteinäistämällä ja laajentamalla sekä tehostamalla rikostutkintaa ja kansainvälistä oikeudellista yhteistyötä. Rikoslakiin lisättiin uudet tietojärjestelmän häirintää (RL 38: 7a–b §) ja tietoverkkorikosvälineen hallussapitoa (RL 34:9b §) koskevat rikosnimikkeet. Vaaran aiheuttamista tietojenkäsittelylle koskevaa teonkuvausta (RL 34:9a §) muutettiin siten, että se kattoi tietokoneviruksen levittämisen lisäksi myös muiden tietoverkkorikosvälineiden[209] levittämisen. Lisäksi säädettiin uusi tietoverkkorikosvälineen hallussapidon sanktioiva pykälä. Nämä muutokset edustivat yleiseurooppalaista havahtumista verkkoyhteiskunnan kehityksen varjopuoliin. (HE153/2007.)[210]

Suomen oikeuskäytännössä oli katsottu, että ilman omistajan lupaa tapahtuva suojaamattoman langattoman lähiverkon eli WLAN[211]- tai muun vastaavan tyyppisen langattoman tietoverkon ja internet-yhteyden käyttäminen voi täyttää luvattoman käytön tunnusmerkistön (RL 28:7–9 §)[212]. Rikoslainsäännöksiä aikoinaan laadittaessa ei kyseisenlaisia verkkoja ollut olemassa ja luvatonta käyttöä koskevat säännökset laadittiin alun perin sellaisia tapauksia ajatellen, että luvattomasti käytetty omaisuus on

[208] HE 2/2003: 16-17.
[209] Muina tietoverkkorikosvälineinä lain esitöissä mainittiin tietomurto-ohjelmat, tietomurtolaitteet sekä salasanat. HE 153/2006: 8.
[210] HE 153/2006 vp: 4, 8; Saarenpää 2016: 73, 185.
[211] WLAN eli Wireless Local Area Network on yleisesti käytetty keino yhdistää tietokone langattomasti internetiin. WLAN on lähiverkko, johon erilaiset päätelaitteet voidaan yhdistää ilman kaapeleita. WLAN ei välttämättä mahdollista internet-yhteyttä vaan se voi myös muodostaa rajatulle käyttäjäryhmälle tarkoitetun sisäisen verkon eli niin sanotun intranetin. HE 277/2010: 3.
[212] WLAN:in käyttö on todettu tuomioistuimessa rangaistavaksi luvattomana käyttönä vain yhdessä tapauksessa, mutta asian ratkaisi hovioikeus, mikä on todennäköisesti vaikuttanut oikeuskäytäntöön ja viranomaisten toimintaan. Lisäksi asia sai paljon huomiota tiedotusvälineissä. Näin ollen tekoa saatettiin pitää yleisesti rangaistavana. HE 277/2010: 5.

käyttöhetkellä käyttäjän hallussa. Säännöksiä muutettiin 1990-luvun alussa siten, ettei niiden soveltamisen kannalta ollut merkitystä sillä, kenen hallussa luvattomasti käytetty omaisuus oli. Tämän katsottiin soveltuvan tilanteisiin, joissa ”atk-hakkerit” tunkeutuivat puhelinlinjan välityksellä toisen tietokonejärjestelmään ja käyttivät sitä luvatta laittomasti ”varastaen tietokoneaikaa” (HE 66/1988). Lainsäätäjä ehdotti vuonna 2010, ettei suojaamattoman langattoman tietoverkkoyhteyden kautta muodostetun internet-yhteyden käyttämisestä enää rangaistaisi eli suojaamattoman WLAN- ja vastaavan tyyppisen langattoman tietoverkon käyttäminen sekä sen kautta tapahtuvan internet-yhteyden luvattoman käytön rangaistavuus nimenomaan suljettiin pois (RL 190/2011). (HE 277/2010.)[213]

Tietoverkkojen muuttuminen yleiseksi keskustelu- ja viestintäalustaksi johti jo vuonna 2003 tietoverkkorikossopimuksen täydentämiseen vuonna 2006 voimaan tulleella lisäpöytäkirjalla (ETS 189), joka koskee pääosin julkisessa tietoverkoissa esitettäviä tekoja eli tietojärjestelmien välityksellä tapahtuvaa rasistista ja muukalaisvihamielistä viestintää; vastaava lisäys tehtiin Suomen rikoslakiin vuonna 2011 (RL 511/2011)[214]. Julkisesti internetissä esitettävä rasistinen ja muukalaisvihamielinen propaganda kriminalisoitiin. Uutena tekotapana kiihottamisessa kansanryhmää vastaan (RL 11:10 §) mainitaan aiemman levittämisen sijaan yleisön saataville asettaminen, jolloin kiihottamispykälä soveltuu muun muassa tahalliseen linkkien perustamiseen rasistista tai muuta sellaista kiihottamista sisältäville internetsivuille silloin, kun linkittäminen täyttää kiihottamissäännöksen elementit. Myös yleisön saatavilla pitäminen kriminalisoitiin, koska haluttiin varmistaa, että rikolliseen levittämiseen kuuluu myös saatavilla pitäminen. Lisäksi säännöksen ilmaisu ’lausuntoja tai muita tiedonantoja’ korvattiin nykyaikaisemmalla käsitteistöllä ’tiedon, mielipiteen tai muun viestin’, mikä painottaa kiihottamisrikoksen laajaa soveltuvuutta mihin tahansa sisällöltään rasistiseen ilmaisuun riippumatta sen esitysmuodosta.[215] (HE 317/2010.)

Uusin vaihe tietoverkkorikosten sääntelyssä on Euroopan parlamentin ja neuvoston tietojärjestelmiin kohdistuvia hyökkäyksiä koskeva niin sanottu tietoverkkorikos-direktiivi (2013/40/EU). Suomen tietoverkkorikoksia koskevaa lainsäädäntöä oli viimeksi uudistettu merkittävästi tietoverkkorikossopimuksen kansallisella voimaan-saattamisella, joka tosin sisälsi kattavammat ja laajemmat määräykset tietoverkko-rikoksista kuin nyt lainsäätäjällä implementoitavana oleva tietoverkkorikosdirektiivi.

[213] HE 277/2010: 1, 3–4.
[214] Saarenpää 2016: 185.
[215] HE 317/2010: 1, 5, 13.

Direktiivin voimaansaattaminen aiheutti lähinnä muutoksia rikoslain eräisiin tietoverkkorikoksia koskeviin säännöksiin (HE 232/2014). Muutokset 4.9.2015 voimaan saattanut uudistus (RL 368/2015) merkitsi tietoverkkorikosten kriminalisoinnin selvää ankaroittamista.[216] Kyseisten muutosten kanssa sovitettiin eduskuntakäsittelyssä yhteen rikoslain järjestäytyneitä rikollisryhmiä koskevien säännösten yhtenäistämiseen liittyvät 1.10.2015 voimaan tulleet muutokset (RL 564/2015)[217].

Direktiivin mukaisesti tietoverkkorikosvälineen käyttöön hankkiminen kriminalisoitiin ja siitä tuli rangaistavaa vaaran aiheuttamisena tietojenkäsittelynä (RL 34:9a §). Viestintäsalaisuuden loukkaus (RL 38:3 §) muutettiin kattamaan jatkossa myös tietojärjestelmän sisäisen luottamuksellisen datan siirron, tietomurto (RL 38:8 §) pääsyn tietojärjestelmässä olevaan dataan sekä siitä tiedon hankkimiseen ja kyseisten rikosten enimmäisrangaistuksia korotettiin[218]. Rikoslakiin lisättiin uudet datavahingontekoa koskevat säännökset (RL 35:3a–c §), jonka törkeän muodon enimmäisrangaistus oli jopa viisi vuotta vankeutta; kvalifiointiperusteet lainsäätäjä liitti niin sanottujen bottiverkkojen käyttöön, rikollisjärjestöön, huomattavaan vahinkoon sekä elintärkeään infrastruktuurin – ja samat kvalifiointiperusteet lisättiin myös törkeää tietoliikenteen häirintää ja törkeää datavahinkoa koskeviin teonkuvauksiin. Uutta oli myös identitettivarkautta koskeva kriminalisointi (RL 38:9b §). Lakiin lisättiin myös direktiivin velvoitteiden mukaisesti tietojärjestelmän[219] ja datan[220] määritelmät.[221]

3.2. Tietoverkkoympäristöön kohdistuvat rikokset

Tietotekniikkarikos ei ole ollut legaalikäsite vaan alun perin kysymys oli kriminaalipoliittisesta ja kriminologisesta käsitteestä kuten talousrikokset. Siksi tietotekniikkarikoksen käsitteen alasta, merkityssisällöstä sekä terminologiasta yleensä on ollut suurta

[216] HE 232/14: 1, 3; Saarenpää 2016: 212.
[217] HE 263/2014: 1, 28.
[218] Aiemmin sekä viestintäsalaisuuden loukkauksen että tietomurron rangaistusasteikko oli sakkoa tai vankeutta enintään yksi vuosi, kun jatkossa niiden enimmäisrangaistus on kaksi vuotta vankeutta. Lisäksi törkeän tietomurron enimmäisrangaistus korotettiin kahdesta vuodesta kolmeen vuoteen vankeutta. HE 232/2014: 1, 54, 56.
[219] RL 38:13.1 §. Tietojärjestelmällä tarkoitetaan 1) laitetta tai toisiinsa kytkettyjä tai liitettyjä laitteita, joista yksi tai useampi on ohjelmoitu automaattista tietojenkäsittelyä varten sekä 2) dataa, jota kyseisessä laitteessa tai toisiinsa kytketyissä tai liitetyissä laitteissa varastoidaan, käsitellään, haetaan tai välitetään sen tai niiden toimintaa, käyttöä, suojausta tai huoltoa varten.
[220] RL 38:13.2 §. Datalla tarkoitetaan myös 1) sellaisessa muodossa olevien tosiseikkojen, tietojen tai käsitteiden esitystä, että se soveltuu käsiteltäväksi tietojärjestelmässä sekä 2) ohjelmaa, jonka avulla tietojärjestelmä pystyy suorittamaan jonkin toiminnon.
[221] HE 232/14: 1; Saarenpää 2016: 186.

erimielisyyttä kansainvälisestikin. Suomessa on käytetty synonyymeinä termejä atk-rikos ja tietokonerikos (*computer crime*). Kansainvälisessä kirjallisuudessa on käytetty myös ilmaisuja tietokoneen väärinkäyttö (*computer abuse*) ja tietokoneisiin liittyvät rikokset (*computer-related crime*) riippuen siitä, miten laaja merkityssisältö termille on haluttu antaa. Suomessa on ryhdytty puhumaan tietotekniikkarikoksista ja annettu painoarvoa tiedonsiirtoon ja tietoon (dataan ja tietoon infromaationa) kohdistuviin rikoksiin eli tieto- ja viestintärikoksiin. Painotettaessa televerkkoihin liittyviä rikoksia on käytetty nimitystä informaatio- ja viestintäteknologiarikokset (*ICT-crime*). Nyttemmin puhutaan tietoverkkorikoksista, mikä liittyy Euroopan neuvoston yleissopimukseen tietoverkkorikollisuudesta ja EU:n tietoverkkorikosdirektiiviin.[222]

Olennaiseksi piirteeksi on hyväksytty se, että tietotekniikkaan kuuluva hyödyke muodostaa joko rikoksen tekovälineen tai rikoksen kohteen. Ominaispiirteenä on pidetty sitä, että rikoksen tekoympäristönä on tietojärjestelmä siihen kuuluvine laitteineen. Rikoksen tekeminen myös edellyttää tekijältä tietotekniikan tuntemusta tai ainakin sen hyväksikäyttöä.[223] Euroopan poliisivirasto, Europol, käyttää termiä ’*cyber-dependent crime*’ tarkoittaen sillä rikoksia, jotka voidaan tehdä vain tietokoneiden, tietoverkkojen tai muun tieto- ja viestintätekniikan (ICT) avulla; selvennyksenä todetaan, ettei kyseisiä rikoksia voi toteuttaa ilman internetiä ja esimerkkeinä kyseisenlaisista rikoksista Europol nimeää haittaohjelmien luomisen ja levittämisen, hakkeroinnin sekä palvelunestohyökkäykset [224].

Suomen poliisissa tietoverkkorikoksista käytetään nykyisin myös termiä kyberrikos. Nämä rikostyypit on jaettu tietoverkkoympäristöön kohdistuviin rikoksiin eli niin sanottuihin puhtaisiin tietoverkkorikoksiin ja tietoverkkoympäristöä hyväksi käyttäen tehtyihin rikoksiin. Rikoksen kohdistuessa tietoverkkoympäristöön, on kyse sellaisten rikosten tekomuodoista, joita esiintyy ainoastaan tietoverkoissa tai tietojärjestelmissä ja rikos kohdistuu tietoverkkoon, tietojärjestelmään tai siinä olevaan dataan.[225] Nämä tietoverkkorikokset suoritetaan tietokoneella tai muulla päätelaitteella ja ne tapahtuvat tietoverkossa. Rikoksen kohde on yleensä tietoverkossa sijaitseva laite, tietojärjestelmä, tietokanta tai muu tietoa sisältävä ohjelmallinen osa (ohjelmisto). Koska tietoverkkorikoksista saisi kirjoitettua kokonaan oman tutkielmansa, tarkoitus on tässä esimerkinomaisesti läpikäydä yleisimpiä tekomuotoja. Ne kaikki löytyvät rikoslain 38 lukuun kirjatuista tieto- ja viestintärikoksista.

[222] Lehtonen 2018: 76–77.
[223] Lehtonen 2018: 78–79.
[224] IOCTA 2018.
[225] Sisäministeriö 2017b: 10.

Tietoverkkoympäristöön kohdistuvista rikoksista tunnetuin lienee ’hakkerointi’, jolloin tunkeudutaan luvatta tietoverkkoon tai tietojärjestelmään ja esimerkiksi tuhotaan tietojärjestelmässä olevia tietoja tai käytetään järjestelmää omiin tarkoituksiin[226]. Kyseinen teko on kriminalisoitu tietomurtona (RL 38:8 §):

> *Joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja tai dataa, taikka sellaisen järjestelmän erikseen suojattuun osaan, on tuomittava tietomurrosta sakkoon tai vankeuteen enintään kahdeksi vuodeksi.*
>
> *Tietomurrosta tuomitaan myös se, joka tietojärjestelmään tai sen osaan tunkeutumatta*
> *1) teknisen erikoislaitteen avulla tai*
> *2) muuten teknisin keinoin turvajärjestelyn ohittaen, tietojärjestelmän haavoittuvuutta hyväksi käyttäen tai muuten ilmeisen vilpillisin keinoin*
> *oikeudettomasti ottaa selon 1 momentissa tarkoitetussa tietojärjestelmässä olevasta tiedosta tai datasta..*

Tietomurtosäännöksellä pyritään muun muassa turvaamaan tietojärjestelmiä ulkopuolista tunkeutumista vastaan. Tietomurrosta on myös törkeä tekomuoto, joka täyttyy silloin, kun tietomurto tehdään osana järjestäytyneen rikollisryhmän toimintaa tai erityisen suunnitelmallisesti ja tietomurto on myös kokonaisuutena arvostellen törkeä. Rikoksentekijä on tuomittava törkeästä tietomurrosta sakkoon tai vankeuteen enintään kolmeksi vuodeksi. Tietomurron yritys on aina rangaistava teko (RL 38:8a §).[227]

Modernia vaaraa tietojärjestelmille edustavat tietokonevirukset. Tietokoneeseen voidaan tartuttaa haittaohjelma (virus tai muu vastaava), jolloin tietojärjestelmä tekee ei-toivottuja toimia tietokoneessa, esimerkiksi vakoilee tai lähettää tietoa tietylle komentopalvelimelle. Viruksen levittäminen ja valmistaminen on säädetty rangaistavaksi vaaran aiheuttamisena tietojenkäsittelylle (RL 34:9a §)[228]:

> *Joka aiheuttaakseen haittaa tai vahinkoa tietojenkäsittelylle taikka tieto- tai viestintäjärjestelmän toiminnalle tai turvallisuudelle*
>
> *1) tuo maahan, hankkii käyttöön, valmistaa, myy tai muuten levittää taikka asettaa saataville*
> *a) sellaisen laitteen tai tietokoneohjelman taikka ohjelmakäskyjen sarjan, joka on suunniteltu tai muunnettu vaarantamaan tai vahingoittamaan tietojenkäsittelyä tai tieto- tai viestintäjärjestelmän toimintaa taikka murtamaan tai purkamaan sähköisen viestinnän teknisen suojauksen tai tietojärjestelmän suojauksen, taikka*

[226] Sisäministeriö 2017b: 10.
[227] Lehtonen 2018: 136.
[228] Lehtonen 2018: 139–140.

> *b) tietojärjestelmän toiselle kuuluvan salasanan, pääsykoodin tai muun vastaavan tiedon taikka*
> *2) levittää tai asettaa saataville ohjeen 1 kohdassa tarkoitetun tietokoneohjelman tai ohjelmakäskyjen sarjan valmistamiseksi,*
>
> *on tuomittava, jollei teosta muualla laissa säädetä ankarampaa tai yhtä ankaraa rangaistusta, vaaran aiheuttamisesta tietojenkäsittelylle sakkoon tai vankeuteen enintään kahdeksi vuodeksi.*

Haittaohjelman kaappaama koneen omistaja voi olla itse ”identiteettivarkauden uhri” tai hänen konettaan on voitu käyttää hyväksi muun, johonkin toiseen järjestelmään kohdistuneen rikoksen, esimerkiksi tietoverkkohyökkäyksen, tekemisessä. Kyseessä voi myös olla kiristyshaittaohjelma, joka salaa haittaohjelman avulla saastuneen koneen kiintolevyt ja siihen liitetyt verkkolevyt, jolloin koneen käyttäjä ei enää pääse mihinkään sisältöönsä käsiksi. Tämän jälkeen uhria vaaditaan maksamaan yleensä bitcoineina eli virtuaalirahana tietty summa, jota vastaan toimitettaisiin salauksen purkava avain. Kiristyksessä saatetaan käyttää tiedostojen salaamisen lisäksi palvelunestohyökkäyksen tai yksityisyyttä koskevan tiedon levityksen uhkaa.[229]

Palvelunestohyökkäyksien kohteena ovat tyypillisesti sähköposti- tai internet-palvelimet sekä muut vastaavat viestien siirtoa, reititystä sekä jakelua hoitavat palvelimet ja hyökkäyksessä tätä palvelinta pyritään ylikuormittamaan. Hyökkäyksen kohteena olevan tietojärjestelmän toimintaa tarkoituksellisesti estetään tai hidastetaan. Palvelunestohyökkäys tulee rangaistavaksi tietoliikenteen häirintänä (RL 38:5 §)[230]:

> *Joka puuttumalla postiliikenteessä taikka tele- tai radioviestinnässä käytettävän laitteen toimintaan, lähettämällä ilkivaltaisessa tarkoituksessa radiolaitteella tai televerkossa häiritseviä viestejä tai muulla vastaavalla tavalla oikeudettomasti estää tai häiritsee postiliikennettä taikka tele- tai radioviestintää, on tuomittava tietoliikenteen häirinnästä sakkoon tai vankeuteen enintään kahdeksi vuodeksi.*

Lisäksi erikseen on kriminalisoitu sekä tietoliikenteen häirinnän törkeä tekomuoto (RL 38:6 §) että sen lievä tekomuoto (RL 38:7 §); kaikkien tekomuotojen yritys on myös säädetty rangaistavaksi[231]. Koska häirintä voi kohdistua tietojärjestelmien välisen liikenteen lisäksi myös itse tietojärjestelmään, säädettiin Suomessa täydentävä tietojärjestelmän häirinnän sanktioiva säännös (RL 38:7a §)[232]:

> *Joka aiheuttaakseen toiselle haittaa tai taloudellista vahinkoa dataa syöttämällä, siirtämällä, vahingoittamalla, muuttamalla tai poistamalla taikka muulla niihin rinnastettavalla tavalla oikeudettomasti estää tietojärjestelmän toiminnan tai aiheuttaa*

[229] Sisäministeriö 2017b: 10, 21.
[230] HE 153/2006: 17; Lehtonen 2018: 143; Sisäministeriö 2017b: 10.
[231] Lehtonen 2018: 144.
[232] HE 153/2006: 17; Lehtonen 2018: 145.

sille vakavaa häiriötä, on tuomittava tietojärjestelmän häirinnästä sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

Myös tietojärjestelmän häirinnän törkeä muoto kriminalisoitu (RL 38:7b §). Erikseen on kriminalisoitu kummankin tekomuodon yritys.

Tietoverkkorikoksia ei sellaisenaan tilastoida. Oheiseen taulukkoon on listattu poliisin tietoon tulleita tietojenkäsittelyä ja viestintää koskevia rikoksia rikosnimikkeittäin vuosien 2010 ja 2016 välisenä aikana:

Ilmoitettu kpl	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**
Törkeä viestintäsalaisuuden loukkaus	1	1	6	3	4	0	3
Salassapitorikos	29	57	45	48	40	48	41
Tietoliikenteen häirintä	25	79	50	93	57	85	67
Henkilörekisteririkos	36	91	148	119	488	122	105
Vaaran aiheuttaminen tietojenkäsittelylle	2	7	1	6	36	4	4
Viestintäsalaisuuden loukkaus	295	297	268	279	297	298	414
Viestintäsalaisuuden loukkauksen yritys	1	0	1	0	0	1	3
Lievä tietoliikenteen häirintä	8	3	5	9	5	6	9
Tietoliikenteen häirinnän yritys	0	1	1	0	0	1	0
Tietoliikenteen lievän häirinnän yritys	0	1	0	0	0	0	0
Tietomurto	292	410	503	580	339	347	409
Törkeä tietomurto	1	8	14	5	6	3	8
Suojauksen purkujärjestelmärikos	0	0	0	0	2	0	0
Tietoverkkorikosvälineen hallussapito	2	1	0	2	4	2	3
Sähköisen viestinnän tietosuojarikkomus	2	0	1	3	1	0	2
Tietokoneohjelman suojauksen poistovälineen luvaton levittäminen	0	0	0	0	0	0	0
Datavahingonteko	0	0	0	0	0	2	14
Datavahingonteon yritys	0	0	0	0	0	0	1
Lievä datavahingonteko	0	0	0	0	0	1	0
Törkeä datavahingonteko	0	0	0	0	0	0	30
Tietojärjestelmän häirinnän yritys	0	0	0	0	1	4	0
Tietojärjestelmän häirintä	3	3	9	11	11	30	38
Törkeä tietojärjestelmän häirintä	0	0	0	0	3	7	16
YHTEENSÄ	**699**	**963**	**1 059**	**1 171**	**1 300**	**964**	**1 149**

Taulukko 3. Tietojenkäsittelyä ja viestintää koskevia poliisin tietoon tulleita rikoksia rikosnimikkeittäin vuosilta 2010–2016. (Sisäministeriö 2017b: 25.[233])

[233] Kyseisen taulukon lähteenä Sisäministeriön julkaisussa on mainittu ”Polstat helmikuu 2017”.

Tilastokeskuksen Suomen virallisissa tilastoissa julkaistaan viranomaisten tietoon tullut rikollisuus neljännesvuosittain ja vuosittain. Vaikka kyseessä olevat tietoverkkoympäristöön kohdistuvat rikokset eli niin sanotut puhtaat tietoverkkorikokset ovat selkeämpi kokonaisuus kuin tietoverkkoympäristöä hyväksi käyttäen tehdyt rikokset, ei ylläolevan taulukon rikosnimikkeitä ei julkaista kyseisissä rikostilastoissa lainkaan. Se kuitenkin antaa jonkinlaista osviittaa tietoverkkoympäristöön kohdistuvien rikosten lukumäärästä. Tilastokeskuksen tilastolla kuvataan kuitenkin vain niitä rikoksia, joista on tehty rikosilmoitus. Suuri osa tapahtuneista rikoksista jää piiloon eli ne eivät edes tule viranomaisten tietoon tai niitä ei ilmoiteta rikoksina.

3.3. Tietoverkkoympäristöä hyväksi käyttäen tehdyt rikokset

Toinen tietoverkkorikostyyppi ovat tietoverkkoympäristöä hyväksi käyttäen tehdyt rikokset. Tietoverkkoja hyväksikäyttäen tehdyillä rikoksilla tarkoitetaan perinteisiä rikollisuuden tekomuotoja: lähes kaikki rikokset voidaan tehdä tietoverkkoja tai tietojärjestelmiä hyödyntäen. Näin tehtyjen rikosten määrät ovatkin kasvaneet. Erityispiirteenä verkkoa hyödyntäville rikoksille on se, että ne ovat yksittäisinä tekoina vähäisiä, mutta suuren uhrimäärän vuoksi niillä aiheutetut vahingot ovat kokonaisuutena mittavia. Suurin tietoverkkoja hyödyntäen tehty rikosryhmä ovat omaisuusrikokset, lähinnä maksuvälinepetokset ja petokset, mutta niitä ovat myös rahanpesu- (RL 32:6–7 §) ja kiristysrikokset (RL 31:3–4 §). Verkkoympäristö on sekä lisännyt että laajentanut rikosentekomahdollisuuksia lapsiin ja nuoriin kohdistuvassa seksuaalisessa hyväksikäytössä ja hyväksikäyttöä sisältävän aineiston levittäminen pilvipalveluiden avulla on yleistynyt. Tietoverkoissa voidaan myös siellä tapahtuvan häirinnän ja hyökkäyksellisen toiminnan lisäksi pyrkiä vaikuttamaan mielipiteisiin ja päätöksentekoon. Osa netissä esiintyvästä vihapuheesta kuuluu sananvapauden piiriin, mutta osa on viharikollisuutta ja tulee sanktioiduksi esimerkiksi kunnianloukkauksena (RL 24:9 §) tai kiihottamisena kansanryhmää vastaan (RL 11:10 §).[234]

Erityisesti tietoteknologiaa hyödyntävät petokset ovat lisääntyneet; tietotekniikan kehittyminen on luonut uusia mahdollisuuksia petoksiin ja muuhun rikolliseen toimintaan. Maksuvälinepetosten (RL 37:8–10 §) määrään vaikuttaa esimerkiksi se, että maksukorttien omistajat ovat ilmoittaneet korttitietojaan netissä olevalle huijaussivustolle, jossa on mainostettu vaikkapa euron matkapuhelinta. Internetin petos-

[234] Sisäministeriö 2017b: 10–11, 17–18, 22.

rikoksilla (RL 36:1–3 §) on useita eri toteutustapoja[235]. Oheisessa taulukossa on yleisimpiä yksityishenkilöön kohdistuvia huijausmuotoja:

Myyntipetos	Myyntipetokset liittyvät yksittäisten henkilöiden välisiin tilanteisiin internetin markkinapaikoilla. Yleensä ostajalle myydään olematonta tuotetta, jota hänelle ei toimiteta maksun jälkeen. Huijaus toimii myös toisin päin: myyjälle toimitetaan väärennetty pankkikuitti osoitukseksi tuotteen maksusta tuotetta noudettaessa tai pyydetään postittamaan tuote nopeasti.
Phishing / kalastelu	Phishingillä tarkoitetaan henkilö-, pankki- ja luottokorttitietojen kalastelua. Huijauksen tarkoituksena on hyödyntää anastettuja tietoja esimerkiksi ostoksissa ja verkkopalveluissa. Myös salasanojen, tunnusten ja puhelinnumeroiden kalastelun tarkoituksena on saada taloudellista hyötyä. Huijarit voivat tavoitella tietoja esimerkiksi esiintymällä poliiseina tai pankin virkailijoina.
Tilausansa	Tilausansoissa kuluttaja saa tyypillisesti verkkokaupalta tai puhelinmyyjältä laskun tuotteesta, jota ei ole ymmärtänyt tilanneensa. Sopimusehtoihin voi olla piilotettuna yllättäviä seikkoja, joita kuluttaja ei huomaa.
Valelasku	Yksityishenkilöille (tai yrityksille) lähetetään postitse tai sähköpostitse oikealta näyttäviä laskuja tavaroista tai palveluista, joita ei ole tilattu eikä saatu. Lasku vaaditaan maksamaan, vaikka siihen ei ole velvollisuutta.
Nettirakas / romanssihuijaus	Romanssihuijauksen uhria lähestytään valeprofiilin avulla. Yksi tyypillinen valeprofiili on ulkomailla palveleva amerikkalainen upseeri. Huijausta saatetaan pohjustaa pitkään, jotta saavutetaan uhrin luottamus ja romanttinen kiinnostus tekijään. Huijauksen uhriin vedotaan rahan tarpeella. Tämän petostyypin haitat voivat olla hyvin suuria; yksittäiset uhrit ovat menettäneet jopa yli 100 000 euroa.
Sijoitushuijaus	Tyypillisessä sijoitushuijauksessa ulkomainen huijari soittaa uhrille ja esittäytyy esimerkiksi sijoitusneuvojaksi, arvopaperinvälittäjäksi tai salkunhoitajaksi. Hän tarjoaa asiakkaalle osake-, kiinnelaina- tai kiinteistösijoituksia, optioiden kauppaa tai valuuttakauppaa ja lupaa rahoille korkeita tuottoja. Huijarit markkinoivat sijoituksia myös internetissä. Todellisuudessa uhri ei saa sijoituksista tuottoa vaan menettää rahansa. Rikoshaitat voivat olla hyvin suuria.
Nigerialaiskirjeet, lotto- ja arpajais-voitot	Uhriin otetaan yleensä yhteyttä sähköpostitse. Hänelle luvataan suuria rahasummia, jos hän osallistuu niiden saamiseksi tarvittavien kulujen maksamiseen. Samaan petostapaan perustuvat ulkomaiset lotto- ja arpajaisvoitot, joissa petoksen kohteen väitetään voittaneen osallistumatta arvontaan. Voiton toimittamiseksi henkilöä pyydetään eri verukkeilla maksamaan rahaa viestin lähettäjälle. Toinen variaatio samasta huijauksesta on ulkomailta lähetetty virallisen näköinen kirje, jossa kerrotaan voitosta. Näiden yhteydenottojen tavoitteena voi olla myös henkilökohtaisten tietojen, pankki- ja tilitietojen saaminen identitettivarkautta varten.

Taulukko 4. Yleisiä yksityishenkilöihin kohdistuvia huijausmuotoja. (Oikeusministeriö 2017: 42).

Kaikki ylläolevan taulukon tapaukset ovat rikosoikeudellisesti petoksia. Perusmuotoisen petoksen (RL 36:1 §) teonkuvaus rikoslaissa on seuraava:

[235] Oikeusministeriö 2017: 10.

> *Joka, hankkiakseen itselleen tai toiselle oikeudetonta taloudellista hyötyä taikka toista vahingoittaakseen, erehdyttämällä tai erehdystä hyväksi käyttämällä saa toisen tekemään tai jättämään tekemättä jotakin ja siten aiheuttaa taloudellista vahinkoa erehtyneelle tai sille, jonka eduista tällä on ollut mahdollisuus määrätä, on tuomittava petoksesta sakkoon tai vankeuteen enintään kahdeksi vuodeksi..*

Sama rikoslain kohta on käytössä myös silloin, kun petokseen syyllistytään tietoverkko-ympäristöä hyväksikäyttäen. Kyseinen niin sanottu tietokoneavusteinen petos on sanktioitu rikoslain 36 luvun 1 pykälän 2. momentissa:

> *Petoksesta tuomitaan myös se, joka 1 momentissa mainitussa tarkoituksessa dataa syöttämällä, muuttamalla, tuhoamalla tai poistamalla taikka tietojärjestelmän toimintaan muuten puuttumalla saa aikaan tietojenkäsittelyn lopputuloksen vääristymisen ja siten aiheuttaa toiselle taloudellista vahinkoa.*

Jos petos, huomioon ottaen tavoitellun hyödyn tai aiheutetun vahingon määrä taikka muut rikokseen liittyvät seikat, on kokonaisuutena arvostellen vähäinen, on kyseessä lievä petos (RL 36:3 §), josta on rangaistuksena sakkoa. Petoksesta on myös törkeä tekomuoto (RL 36:2 §):

> *Jos petoksessa*
> *1) tavoitellaan huomattavaa hyötyä,*
> *2) aiheutetaan huomattavaa tai erityisen tuntuvaa vahinkoa,*
> *3) rikos tehdään käyttämällä hyväksi vastuulliseen asemaan perustuvaa erityistä luottamusta tai*
> *4) rikos tehdään käyttämällä hyväksi toisen erityistä heikkoutta tai muuta turvatonta tilaa*
> *ja petos on myös kokonaisuutena arvostellen törkeä, rikoksentekijä on tuomittava törkeästä petoksesta vankeuteen vähintään neljäksi kuukaudeksi ja enintään neljäksi vuodeksi.*

Jo pelkkä petoksen ja törkeän petoksen yritys ovat rangaistavia tekoja, eli tekomuodot on sanktioitu, vaikkei taloudellista vahinkoa syntyisikään.

Useimmiten netissä tapahtuvassa petoksessa on kyse myynti- tai tilauspetoksesta. Myyntipetokset ovat yksittäisten henkilöiden välistä kaupantekoa, jossa ostaja maksaa tuotteen etukäteen myyjälle joko pankkitilille tai nyttemmin jollain muulla maksu-välineellä saamatta koskaan ostamaansa tuotetta. Tilauspetoksissa osapuolena on useimmiten yritys, jolta yritetään ostaa tavaraa väärillä henkilö- tai luottokorttitiedoilla. Tilauspetoksiin liittyy normaalisti myös identiteettivarkaus (RL 38:9a §)[236] eli kolmannen osapuolen erehdyttäminen käyttämällä oikeudettomasti toisen henkilötietoja, tunnistamistietoja tai muuta vastaavaa yksilöivää tietoa aiheuttaen taloudellista vahinkoa tai vähäistä suurempaa haittaa sille, jota tieto koskee; toisen tiedot haltuun

[236] Identiteettivarkaus lisättiin rikoslakiin 4.9.2015.

saamisen jälkeen hänen nimissään tilataan tuotteita eri yrityksiltä ja laskut tuotteista tulevat luonnollisesti tilaajan maksettavaksi. Niin sanotussa verkkourkinnassa eli tietojenkalastelussa (*phising*) yritetään sähköpostiviestein saada selville verkkopankkien käyttäjätunnuksia ja salasanoja sekä maksukorttien tietoja, jotta päästäisiin käsiksi asiakkaan tilillä oleviin varoihin tai käyttämään luottokorttia. Kalastelusähköpostiviesteillä yleensä houkutellaan osallistumaan kilpailuun tai vastaamaan kyselyyn ja kiitokseksi luvataan vaikka kallis matkapuhelin eurolla, jonka saadakseen tulee antaa henkilötietoja. Ne päätyvät kuitenkin rikollisten haltuun.[237]

Koska nykypäivänä lähes kaikki rikokset voidaan toteuttaa niin reaalimaailmassa kuin tietoverkkoympäristössä tai sitä hyväksikäyttäen, ei ole mahdollista saada tietoa tietokoneavusteisten petosten lukumääristä pelkästään rikosnimikkeiden perusteella: tietoverkossa tapahtuneita petoksia (tietokonepetoksia) ei luokitella erikseen, vaan ne sisältyvät eri petosnimikkeisiin. Lisäksi viranomaisten tietoon tulevan rikollisuuden määrään vaikuttaa muun muassa ilmoitusalttius, joka on lisääntynyt sähköisen rikosilmoituksen tekemismahdollisuuden myötä; kirjaamisalttius, johon vaikuttaa poliisin osaaminen ja valitettavasti myös viitseliäisyys; sekä poliisin kontrollitoiminnan kohdistaminen, jolloin poliisi panostaa nettipetosten tutkintaan ja niiden ennaltaehkäisyyn. Suomessa tehdyt nettipetokset saadaan pääosin selvitettyä, mutta ulkomailta käsin tehtyjen rikosten tutkinta on vaikeaa eikä suurinta osaa kyseisenlaisista petoksista edes tutkita.[238]

[237] Kodin kyberopas 2017: 20, 25; Sisäministeriö 2017b: 12, 22.
[238] Sisäministeriö 2017b: 23–24.

4. MYYNTIPETOKSET

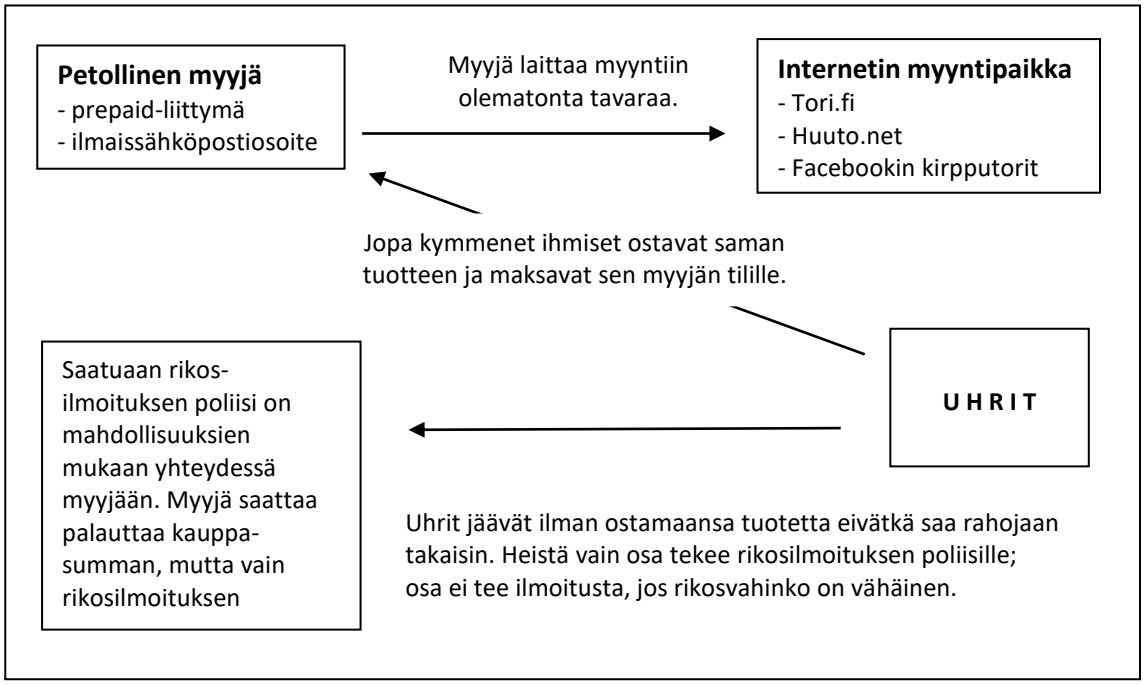
Vertaiskaupalla tarkoitetaan yksityishenkilöiden keskenään käymää käytetyn tavaran kauppaa, josta ei peritä arvonlisäveroa[239]. Käytetyn tavaran myynnistä kertyy harvoin voittoa ja tuloverolain (TVL 1535/1992) mukaan omassa tai perheen käytössä olleesta tavallisesta koti-irtaimistosta saatu luovutusvoitto on verovapaata 5 000 euroon asti vuodessa (TVL 48 §). Tuotteita myydään ja ostetaan suoraan muilta kuluttajilta. Vertaiskauppaa käydään muun muassa perinteisillä kirpputoreilla sekä kauppojen ja työpaikkojen ilmoitustauluilla. Vertaisverkkokaupalla tarkoitetaan puolestaan vertaiskauppaa, jota käydään internetissä. Verkossa kauppaa voidaan käydä erilaisilla kaupankäyntiin tehdyillä alustoilla sekä sosiaalisen median palveluissa: eniten käytetään netin erilaisia markkinapaikkoja, kuten Tori.fi-sivustoa tai Huuto.netiä, mutta myös erilaiset Facebook-ryhmät ovat suosittuja[240]. Kaupan liitto[241] teetti ja julkaisi ensimmäisen vertaisverkkokauppaselvityksen 24.11.2015, kun internetin eri foorumeilla ja kauppapaikoilla tapahtunut kuluttajien välisen vertaiskauppa yleistyi vauhdikkaasti. Tärkeimpänä syynä ostaa tuotteita toisilta kuluttajilta on rahansäästö.[242]

Netti tarjoaa rikollisille uusia väyliä huijata[243]. Myyntipetos on petos, joka liittyy yksityishenkilöiden väliseen kaupankäyntiin näillä internetin eri markkinapaikoilla. Petoksessa on aina kysymys tahallisesta teosta. Tarkoituksena on saada itselleen oikeudetonta taloudellista hyötyä käyttämällä hyväksi toisen erehdystä. Myyntipetoksissa hyödynnetään yleensä uhrin varomattomuutta tai hyväuskoisuutta[244]. Myyntipetostapauksissa myyjä myy markkinapaikalla yleensä ottaen olemassa olematonta tavaraa. Valtaosa myyjistä ei edes salaa omaa identiteettiään, vaan tekee myynnin omilla tiedoillaan ja omaa tilinumeroaan käyttäen. Tekoa säätelee pitkälti tekijän sen hetkinen akuutti rahantarve. Tekijällä tekohetkellä oleva tieto siitä, että hän jää kiinni ja saa tuomion, on toissijainen. Osa myyjistä pyrkii salaamaan henkilöllisyytensä käyttämällä maksutapana muuta kuin pankkitiliä. Tällöin myyjä on luonut myyntitapahtumaa varten jonkun ilmaisen sähköpostiosoitteen ja hankkinut

[239] Arvonlisäveroa suoritetaan arvonlisäverolain 1501/1993 (1 § 1 kohdan) mukaan valtiolle liiketoiminnan muodossa Suomessa tapahtuvasta tavaran ja palvelun myynnistä – eikä yksityishenkilöiden välinen kauppa ole liiketoimintaa.
[240] Kodin kyberopas 2017: 33.
[241] Kaupan liitto on kaupan alan valtakunnallinen edunvalvontajärjestö, jonka tehtävänä on edistää suomalaista kauppaa.
[242] Kaupan liitto 24.11.2015.
[243] Kodin kyberopas 2017: 32.
[244] Oikeusministeriö 2017: 24.

prepaid-puhelinliittymän. Maksutapa on valittu siten, että viranomaisten on vaikeampi selvittää varojen saajan henkilöllisyys.

Myytäväksi on valittu suosittu tuote (esimerkiksi älypuhelin, pelikonsoli, kannettava tietokone tai Muumi-astioita) huokeaan hintaan. Huijaukset myös noudattelevat sesonkivaihteluita: keväisin myydään polkupyöriä ja talvisin suksia, syksyisin tehdään asuntohuijauksia ja suosittujen konserttien alla myydään konserttilippuja[245]. Oikeaan aikaan ja helposti saatavilla ohjeet myyntipetosten ehkäisemiseksi ovat tärkeitä[246]. Kiinnostuneita ostajia on lukuisia ja kymmenet eri ihmiset eri puolelta Suomea ostavat toisistaan tietämättä saman tuotteen maksaen sovitun kauppasumman myyjälle. Uhrit jäävät ilman ostamaansa tuotetta eivätkä he myöskään saa maksamaansa kauppasummaa takaisin. Vain osa asianomistajista eli tehdyssä kaupassa petoksella varojaan menettäneistä henkilöistä tekee asiasta rikosilmoituksen. Joissain tapauksissa myyjä palauttaa kauppasumman rikosilmoituksen tehneelle uhrille, jolloin asian tutkinta poliisissa normaalisti päätetään – ja rikoksen tekijä saa pitää kaikilta muilta kauppakumppaneiltaan saamansa varat. Yleisimmin tapahtuva myyntipetoskuvio on kuvattu oheisessa kaaviossa:



Kuvio 1. Esimerkki yleisestä internetin myyntipetoksesta. (Oikeusministeriö 2017: 22.)

[245] MTV3 10.3.2019.
[246] Oikeusministeriö 2017: 24.

Myyntipetoksissa rikoksentekijän tarkoituksena on erehdyttää uhri maksamaan hänelle kauppasumma. Kyse on rahasta, ei tuotteesta. Myyntipetosten kohteeksi päätyy tavallisia netin markkinapaikoilla kauppaa käyviä ihmisiä. Yksittäisissä tapauksissa uhrien kokemat taloudelliset menetykset ovat usein suhteellisen pieniä, mutta joissakin tapaukissa etukäteen maksettu – ja menetetty – kauppasumma voi olla huomattavan suuri. Petollinen myyjä saattaa saada itselleen jopa tuhansia euroja. Vaikka myynti-petokset ovat yleisiä, jäävät monet tapaukset poliisilta piiloon. Myyntipetoksia onkin tärkeää ehkäistä siellä, missä niitä tehdään. Internetin markkinapaikkojen ylläpitäjät varoittavat käyttäjiään huijauksista ja asiasta on puhuttu paljon eri medioissa, mutta siitä huolimatta myyntipetoksia tapahtuu edelleen.[247]

Perusmuotoiseen myyntipetokseen ei liity tietomurtoa (RL 38:8 §), koska tekijä ei murtaudu mihinkään. Siihen ei myöskään liity identiteettivarkautta (RL 38:9a §), koska petollinen myyjä käyttää keksittyä identiteettiä. Mikäli rikokseen liittyy toinen henkilö, rikoskumppani, jonka pankkitilille myyjä on saanut petoksella hankkimansa kauppa-summan tai osan siitä, syyllistyy kyseinen rikoskumppani rahanpesuun, jonka yritys on myös sanktioitu (RL 32: 6 §):

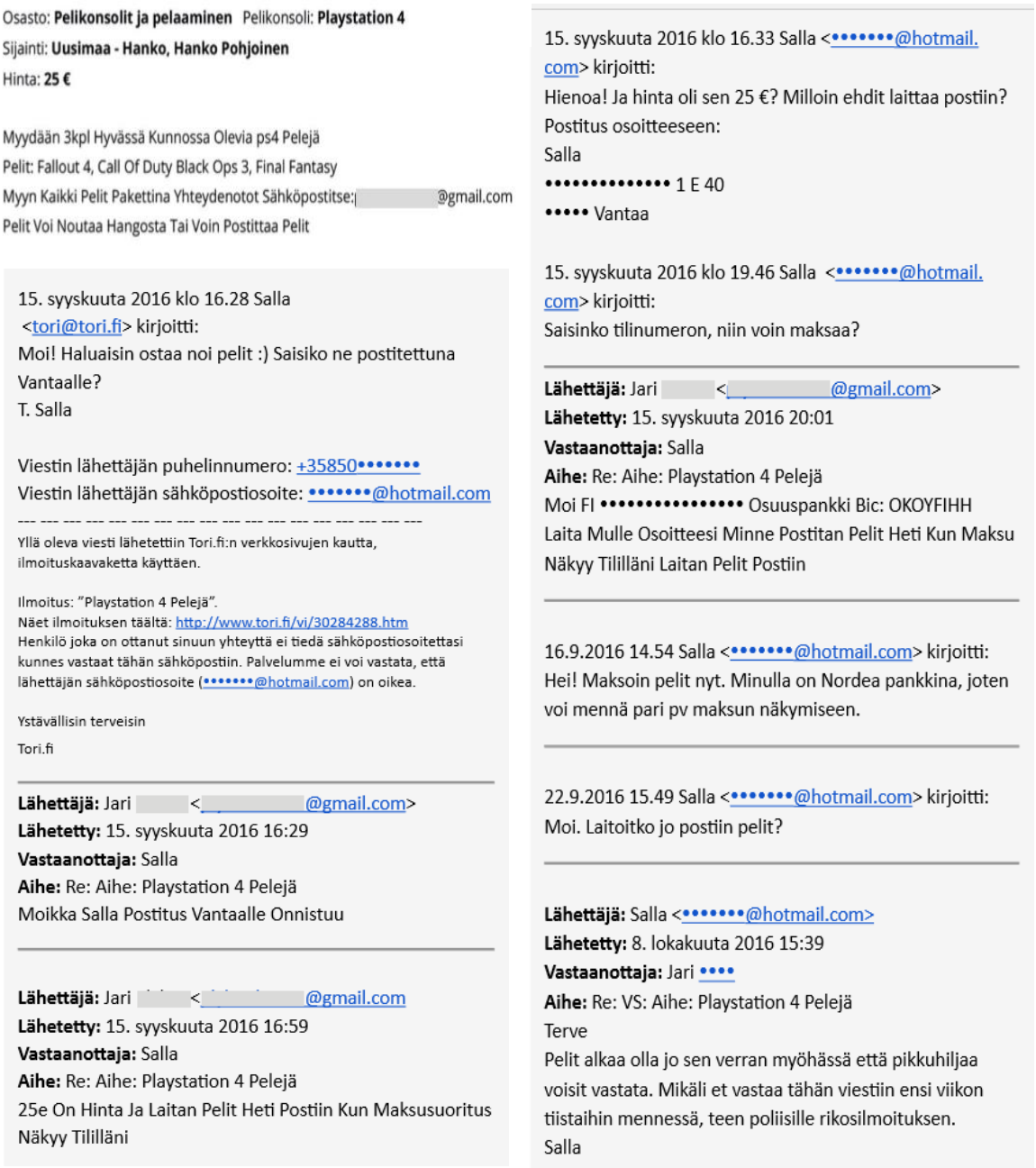
> *Joka*
>
> *1) ottaa vastaan, käyttää, muuntaa, luovuttaa, siirtää, välittää tai pitää hallussaan rikoksella hankittua omaisuutta, rikoksen tuottamaa hyötyä tai näiden tilalle tullutta omaisuutta hankkiakseen itselleen tai toiselle hyötyä tai peittääkseen tai häivyttääkseen hyödyn tai omaisuuden laittoman alkuperän tai avustaakseen rikoksentekijää välttämään rikoksen oikeudelliset seuraamukset taikka*
>
> *2) peittää tai häivyttää rikoksella hankitun omaisuuden, rikoksen tuottaman hyödyn taikka näiden tilalle tulleen omaisuuden todellisen luonteen, alkuperän, sijainnin tai siihen kohdistuvat määräämistoimet tai oikeudet taikka avustaa toista tällaisessa peittämisessä tai häivyttämisessä,*
>
> *on tuomittava rahanpesusta sakkoon tai vankeuteen enintään kahdeksi vuodeksi.*

Jos teko ei ole rangaistava rahanpesuna, on se tuomittava kätkemisrikoksena (RL 32:1 §):

> *Joka kätkee, hankkii, ottaa huostaansa tai välittää toiselta varkaus-, kavallus-, ryöstö-, kiristys-, petos-, kiskonta- tai maksuvälinepetosrikoksella saatua omaisuutta taikka muulla tavoin ryhtyy sellaiseen omaisuuteen, on tuomittava, jollei teko ole rangaistava rahanpesuna, kätkemisrikoksesta sakkoon tai vankeuteen enintään yhdeksi vuodeksi kuudeksi kuukaudeksi.*

[247] Oikeusministeriö 2017: 38.

Ohessa on esimerkkitapaus siitä, miten eräs hyvinkin tavanomainen myyntipetostapaus eteni, kun ostaja – ja tuleva asianomistaja petokseen – otti yhteyttä tapauksessa Tori.fi-palstalla olleen myynti-ilmoituksen jättäjään kauppasivuston ilmoituksen kautta ja kaupoista sovittiin sähköpostitse:



Osasto: **Pelikonsolit ja pelaaminen** Pelikonsoli: **Playstation 4**
Sijainti: **Uusimaa - Hanko, Hanko Pohjoinen**
Hinta: **25 €**

Myydään 3kpl Hyvässä Kunnossa Olevia ps4 Pelejä
Pelit: Fallout 4, Call Of Duty Black Ops 3, Final Fantasy
Myyn Kaikki Pelit Pakettina Yhteydenotot Sähköpostitse: @gmail.com
Pelit Voi Noutaa Hangosta Tai Voin Postittaa Pelit

15. syyskuuta 2016 klo 16.28 Salla <tori@tori.fi> kirjoitti:
Moi! Haluaisin ostaa noi pelit :) Saisiko ne postitettuna Vantaalle?
T. Salla

Viestin lähettäjän puhelinnumero: +35850•••••••
Viestin lähettäjän sähköpostiosoite: •••••••@hotmail.com

Yllä oleva viesti lähetettiin Tori.fi:n verkkosivujen kautta, ilmoituskaavaketta käyttäen.

Ilmoitus: "Playstation 4 Pelejä".
Näet ilmoituksen täältä: http://www.tori.fi/vi/30284288.htm
Henkilö joka on ottanut sinuun yhteyttä ei tiedä sähköpostiosoitettasi kunnes vastaat tähän sähköpostiin. Palvelumme ei voi vastata, että lähettäjän sähköpostiosoite (•••••••@hotmail.com) on oikea.

Ystävällisin terveisin
Tori.fi

Lähettäjä: Jari <@gmail.com>
Lähetetty: 15. syyskuuta 2016 16:29
Vastaanottaja: Salla
Aihe: Re: Aihe: Playstation 4 Pelejä
Moikka Salla Postitus Vantaalle Onnistuu

Lähettäjä: Jari <@gmail.com
Lähetetty: 15. syyskuuta 2016 16:59
Vastaanottaja: Salla
Aihe: Re: Aihe: Playstation 4 Pelejä
25e On Hinta Ja Laitan Pelit Heti Postiin Kun Maksusuoritus Näkyy Tililläni

15. syyskuuta 2016 klo 16.33 Salla <•••••••@hotmail.com> kirjoitti:
Hienoa! Ja hinta oli sen 25 €? Milloin ehdit laittaa postiin?
Postitus osoitteeseen:
Salla
•••••••••••••• 1 E 40
••••• Vantaa

15. syyskuuta 2016 klo 19.46 Salla <•••••••@hotmail.com> kirjoitti:
Saisinko tilinumeron, niin voin maksaa?

Lähettäjä: Jari <@gmail.com>
Lähetetty: 15. syyskuuta 2016 20:01
Vastaanottaja: Salla
Aihe: Re: Aihe: Playstation 4 Pelejä
Moi FI •••••••••••••••• Osuuspankki Bic: OKOYFIHH
Laita Mulle Osoitteesi Minne Postitan Pelit Heti Kun Maksu Näkyy Tililläni Laitan Pelit Postiin

16.9.2016 14.54 Salla <•••••••@hotmail.com> kirjoitti:
Hei! Maksoin pelit nyt. Minulla on Nordea pankkina, joten voi mennä pari pv maksun näkymiseen.

22.9.2016 15.49 Salla <•••••••@hotmail.com> kirjoitti:
Moi. Laitoitko jo postiin pelit?

Lähettäjä: Salla <•••••••@hotmail.com>
Lähetetty: 8. lokakuuta 2016 15:39
Vastaanottaja: Jari ••••
Aihe: Re: VS: Aihe: Playstation 4 Pelejä
Terve
Pelit alkaa olla jo sen verran myöhässä että pikkuhiljaa voisit vastata. Mikäli et vastaa tähän viestiin ensi viikon tiistaihin mennessä, teen poliisille rikosilmoituksen.
Salla

Kuvio 2. Esimerkki myyntipetoshuijauksen etenemisestä. (Kodin kyberopas 2017: 34–35.)

Nykyisin myyjä saattaa ehdottaa kauppasumman maksamista esimerkiksi Paysafe-cardeina[248]. Niitä myydään monissa kaupoissa, huoltoasemilla ja kioskeilla. Myyjä on normaalisti hyvin avulias neuvoessaan Paysafecardin käytöstä. Sellaisen ostaessa ostaa itse asiassa PIN-koodin, jonka arvo on joko 10, 25, 50 tai 100 euroa ja koodi tulostuu myyntipisteestä saadulle ostoskuitille; kyseinen paysafecard-tuloste on yhtä arvokas kuin sen ostosumma. Paysafecard käy maksuvälineenä joissain verkkokaupoissa, koodilla voi maksaa tuhansilla pelejä, yhteisöpalveluita, elokuvia ja musiikkia tarjoavilla sivustoilla ja koodin arvon voi myös syöttää omalle my paysafecard -tililleen myöhempää käyttöä varten. Myyjä pyytää saada PIN-koodin itselleen ennen tuotteen lähettämistä. Vaikka sekä kuitissa että Paysafecardin sivuilla mainitaan, ettei Paysafe-card PIN-koodia tule koskaan ilmoittaa puhelimitse tai sähköpostitse, ostaja suostuu antamaan koodin myyjälle, joka saa välittömästi haltuunsa koodin raha-arvon. Sen jälkeen myyjään ei saakaan enää yhteyttä. Pyyntö käyttää Paysafecardia maksamiseen pitäisi soittaa hälytyskelloja eikä kyseistä ostotapahtumaa tulisi sen käyttöä ehdottaneen myyjän kanssa tehdä. Jos myyjä ehdottaa maksun suorittamista virtuaalivaluuttana, esimerkiksi bitcoinina, viittaa se vielä vankemmin petolliseen kaupankäyntiin.

Huijareista 95 prosenttia esiintyy myyjänä, mutta myös ostaja voi olla epärehellinen[249]. Myyntipetoksesta esiintyykin niin sanottu käänteinen tekotapa. Siinä petollinen tekijä esiintyy ostajana ja ottaa yhteyttä markkinapaikalla olevan myynti-ilmoituksen jättäjään ilmoittaen halustaan ostaa kyseinen tuote. Tekijä ei luonnollisestikaan esiinny omalla nimellään vaan hän käyttää täysin tekaistua nimeä tai hän käyttää oikeudetta jonkun muun henkilöllisyyttä, jolloin hän syyllistyy identiteettivarkauteen (RL 38:9a §). Tekijä maksaa sovitun kauppasumman ja postituskulut myyjälle, mutta väärentää maksu-tositteen ja toimittaa sen myyjälle. Normaalisti petollisella ostajalla ei ole käytössä saman pankin tiliä kuin myyjällä, joten maksun saapumisessa myyjän pankkitilille ”menee muutama pankkipäivä”. Myyjä on kuitenkin saanut tositteen hänelle tulossa olevasta maksusta ja lähettää tuotteen ostajalle. Kauppasummaa hän ei kuitenkaan koskaan saa, koska maksutapahtumaa ei ole tosiasiassa edes tehty. Petollinen ostaja syyllistyy tekaistun maksutositteen osalta petoksen lisäksi myös väärennykseen, jonka yrityskin on rangaistava teko (RL 33: 1§):

> *Joka valmistaa väärän asiakirjan tai muun todistuskappaleen tai väärentää sellaisen käytettäväksi harhauttavana todisteena taikka käyttää väärää tai väärennettyä todistuskappaletta tällaisena todisteena, on tuomittava väärennyksestä sakkoon tai vankeuteen enintään kahdeksi vuodeksi.*

[248] Tietoja Paysafecardista saatavilla internet-sivustolla https://www.paysafecard.com/fi-fi/
[249] MTV3 10.3.2019.

Mikäli petollinen ostaja on kyseisenlaisessa käänteisessä myyntipetoksessa esiintynyt väärillä henkilötiedoilla, hänellä on oletettavasti myös tuon henkilön jokin henkilötodistus (passi, henkilökortti tai ajokortti) hallussaan. Riippumatta tavasta, jolla petollinen ostaja on saanut henkilötodistuksen haltuunsa, hän syyllistyy rikokseen. Jos tekijä on anastanut henkilötodistuksen sen alkuperäiseltä omistajalta – joko sellaisenaan tai esimerkiksi anastaessaan lompakon, jossa sai muun siellä olevan omaisuuden lisäksi haltuunsa myös henkilötodistuksen, kyseeseen tulee rikoksena varkaus (RL 28:1 §) tai sen lievempi tekomuoto, näpistys (RL 28:3 §):

> *Joka anastaa toisen hallusta irtainta omaisuutta, on tuomittava varkaudesta sakkoon tai vankeuteen enintään yhdeksi vuodeksi kuudeksi kuukaudeksi.*
>
> *Jos varkaus, huomioon ottaen anastetun omaisuuden arvo tai muut rikokseen liittyvät seikat, on kokonaisuutena arvostellen vähäinen, rikoksentekijä on tuomittava näpistyksestä sakkoon.*

Tekijä syyllistyy kätkemiseen saatuaan henkilötodistuksen haltuunsa joltakulta muulta, esimerkiksi sen alun perin anastaneelta henkilöltä. Jos hän on löytänyt henkilötodistuksen ja kyseessä on löytötavara. Löytötavaralaki (778/1988, 4 §) velvoittaa löytötavaran talteen ottajan eli löytäjän ilmoittamaan löydöstä ilman aiheetonta viivytystä omistajalle tai toimittamaan löytötavaran poliisille. Mikäli näin ei toimi, on rangaistus löytötavaran anastamisesta on säädetty rikoslaissa kavalluksen sanktioivan pykälän (RL 28:4 §) toisessa momentissa:

> *Joka anastaa hallussaan olevia varoja tai muuta irtainta omaisuutta, on tuomittava kavalluksesta sakkoon tai vankeuteen enintään yhdeksi vuodeksi kuudeksi kuukaudeksi.*
>
> *Kavalluksesta tuomitaan myös se, joka anastaa löytämiään tai erehdyksen kautta haltuunsa saamiaan varoja tai muuta irtainta omaisuutta.*

Ostaja pyytää postittamaan kaupanteon kohteena olevan tuotteen henkilötodistuksessa olevan henkilön tiedoilla esimerkiksi Smartpost-automaattiin. Koska lähetyksen saapumisesta tulee tieto ostajan myyjälle antamaan puhelinnumeroon, saa ostaja noudettua postilähetyksen. Mikäli postilähetys pitää noutaa henkilökohtaisesti asioiden Postin palvelupisteen tiskiltä, saa ostaja valitettavan usein noudettua postilähetyksen, vaikkei hän näyttäisi henkilötodistuksen kuvan henkilöltä. Lähetyksen noutaja joutuu myös kuittaamaan sen vastaanottamisen allekirjoituksellaan, jolloin täyttyy väärennyksen tunnusmerkistö. Petollinen ostaja saattaa myös värvätä toisen henkilön noutamaan postilähetyksen erityisesti silloin, kun henkilötodistus on vastakkaisen sukupuolen tiedoilla. Tällöin rikoksen esitutkinnassa tulee huomioida rikoslaissa myös

sanktioidut yllytys (RL 5:5 §) ja avunanto (RL 5:6 §). Ne tulee huomioida myös, jos noudossa käytetään väärennettyä valtakirjaa, jolla petollinen ostaja valtuuttaa jonkun muun noutamaan postilähetyksen hänen puolestaan; tällöin täyttyy jälleen väärennyksenkin tunnusmerkistö.

Markkinapaikoilla kauppaa tekeville yksityishenkilölle on tehty lukuisia eri ohjeistuksia usean eri toimijan taholta. Niissä kaikissa korostuu samat huomiot ja neuvotaan tekemään samat toimenpiteet: Myyjän saama palaute tulee tutkia; kauppapaikoilla voi antaa palautetta ja saada selville, mitä muut ostajat ovat kertoneet myyjästä. (Kauppapaikkojen ylläpitäjät myös poistavat epärehelliseksi osoittautuneita myyjiä ja ostajia palveluistaan.) Monen myynti-ilmoituksen kuva on otettu internetistä; kuvasta voi tehdä netissä kuvahaun ja myyjää voi pyytää kirjoittamaan tietty sana lapulle, ottamaan kuvan kaupanteon kohteena olevasta tuotteesta lapun kanssa ja lähettämään kuvan ostajalle. Kauppahinnan maksamiseen voi käyttää postiennakkoa, jolloin ostaja saa tarkistaa saamansa paketin sisällön ennen kuin tuote maksetaan. Toisinaan maksamiseen on käytössä välityspalvelu. Tällöin ostaja maksaa kauppasumman välityspalvelulle, joka välittää sen edelleen myyjälle vasta sitten, kun tuote on ostajalla. Liian houkutteleva myynti-ilmoitus voi olla merkki siitä, että myyjä saattaa myydä anastettua omaisuutta tai olematonta omaisuutta. Lisäksi myyjällä oleva kiire saada kaupat aikaiseksi on yksi varoitusmerkeistä.[250]

4.1. Huuto.net-petoskokonaisuus

Loppuvuodesta 2011 tapahtui Suomessa sarja suuria tietovuotoja[251]. Yli 16 000 suomalaisen henkilötunnuksia, osoitteita, puhelinnumeroita ja sähköpostiosoitteita sisältävä tiedosto vuodettiin verkkoon 5.11.2011; kyseessä oli Suomen historian suurin henkilötietovuoto. Viikkoa myöhemmin, 12.11.2011, tapahtui jättimäinen tietovuoto, kun suomalaiselle keskustelupalstalle vuodettiin noin 500 000 suomalaista sähköpostiosoitetta; kyseessä oli määrällisesti todennäköisesti Suomen suurin tietovuoto. 16.11.2011 tapahtui kolmas tietovuoto, kun verkkoon vuodettiin Netcar.fi-verkko-

[250] Kodin kyberopas 2017: 34.

[251] Tietovuoto vai tietomurto? Tietomurrossa tietoihin on päästy käsiksi palvelussa tai sovelluksessa olevaa tietoturva-aukkoa hyödyntäen. Tiedot on saatu murtautumalla palveluun. Tietomurron avulla saatuja tietoja ei välttämättä vuodeta nettiin, vaan niitä voidaan käyttää esimerkiksi identitettivarkauksiin. Tietovuoto voi tapahtua joko tietomurron seurauksena tai ilman tietomurtoa. Tiedot voivat vuotaa julkisuuteen esimerkiksi yrityksen tai organisaation sisältä henkilöltä, jolla on ollut pääsy kyseisiin tietoihin. Tietovuoto voi siten olla tahallinen tapahtuma tai se voi tapahtua vahingossa. Mikro-PC 8.12.2011: 21.

palvelun yli 12 000 käyttäjän tunnukset ja salasanat. Uudesta salasanavuodosta uutisoitiin jälleen 28.11.2011, kun suomalaiseen Terve Media -palveluun kuuluvaan Helistin.fi-verkkopalveluun murtauduttiin ja palvelun yli 70 000 käyttäjän tunnukset, sähköpostiosoitteet ja salasanat vuodettiin verkkoon; samat käyttäjätunnukset kävivät useisiin muihinkin Terve Median palveluihin.[252] Tietovuodot jatkuivat, kun matkailu-aiheiselle Napsu.fi-sivustolle tehtiin tietomurto ja yli 16 000 käyttäjätunnusta, salasanaa ja sähköpostiosoitetta selville vuodettiin nettiin. Napsu.fi:n ylläpitäjän mukaan salasanat olivat salatussa muodossa, mutta suojaus oli ilmeisesti pystytty murtamaan.[253]

Ei ole tiedossa, kuka kyseisiä tietoja milloinkin vuosi nettiin. Napsu.fi-sivustolta saatuja asiakastietoja hyväksikäyttäen tehtiin Suomen mittakaavassa yksi suurimmista netti-petoskokonaisuuksista, joissa murtauduttiin onnistuneesti Huuto.net-verkkokauppa-sivustolla lukuisten yksityishenkilöiden käyttäjätileille (profiileihin). Parhaan palaute-historian omanneet käyttäjäprofiilit otettiin käyttöön. Tämä oli mahdollista siksi, että useat henkilöt käyttivät samaa salasanaa sekä Napsu.fi- että Huuto.net-sivustoilla. Käyttäjätilejä hyväksikäyttäen pääasiassa olemassa olematonta omaisuutta myytiin pääosin kesäkuun 2011 ja helmikuun 2012 välisenä aikana siten, että tekijät saivat itselleen noin 150 000 euron edestä petoksella hankittua varallisuutta. Petoksella hankittuja varoja myös ohjattiin eräiden rahansiirtoon erikoistuneiden yritysten kautta eri yhtiöiden niin sanotuille pelitileille ja varoja tuloutettiin tätä kautta tekijöille. Näin toimien yritettiin häivyttää päätekijöiden osallisuus rikoksiin. Asianomistajia eli petetyksi tulleita uhreja oli kyseisessä nettipetoskokonaisuudessa 315 ja rikoksesta epäiltyjä 17.

Asiakokonaisuudessa jo aiemminkin nettipetoksiin syyllistynyt ja näistä vankeus-tuomionkin saanut päätekijä, Viljar Kivi[254], oli aktiivisesti selvittänyt lukuisten henkilöiden Huuto.net-käyttäjätunnuksia ja -salasanoja. Hän teki tietomurrot pääasiassa yksin ja otti parhaat profiilit itselleen käyttöön. Kivi luovutti muita tietomurron kohteeksi joutuneita profiileja kahdelle muulle, poliisin pienemmiksi päätekijöiksi katsotuille J:lle ja V:lle, jotka myös itse tunkeutuivat Huuto.net-käyttäjäprofiileihin ja tekivät kauppaa. Päätekijä-Kivi kehitteli rakennelman ”bulvaaneiksi” katsottavien tilin-haltijoiden käytöstä ja heidän kanssaan tehdyistä sopimuksista. Kunkin bulvaanin tilille

[252] Mikro-PC 8.12.2011: 20.
[253] Helsingin Sanomat 3.12.2011.
[254] Tuomioistuimen päätökset ovat julkisia asiakirjoja ja tuomitun nimi on aina julkinen tieto, mutta sitä ei aina kuitenkaan julkaista mediassa. Yleensä julkaisun rajana pidetään yli 2 vuoden vankeustuomion saamista, mutta nimen julkistamista ei voida päättää kaavamaisesti rangaistuksen ankaruuden perusteella. Julkisen sanan neuvosto (JSN) on antanut asiassa periaatelausuman asiasta:
http://www.jsn.fi/periaatelausumat/nimi-rikosuutisissa-1981/

ohjattiin enintään 10 000 euroa, jottei heille tuomittavat rangaistukset muodostuisi liian ankariksi. Bulvaanit olivat poikkeuksetta nuoria miehiä, joilla oli ollut heikko rahatilanne ja joita houkutti helppo ja nopea tapa saada rahaa. Sopimuksen mukaisesti bulvaanien tuli ottaa teot omille nimilleen eikä paljastaa itse päätekijöitä.

Petokset tehtiin tietomurtoja hyväksi käyttäen; kokonaisuudessaan tietomurtoja oli vähemmän kuin itse petoksia. Samalla rikolliseen käyttöön kaapatulla profiililla tehtiin useampi kauppa. Käytännössä tietomurrot ja niiden avulla tehdyt petokset loppuivat, kun poliisi otti Kiven asian vuoksi kiinni helmikuussa 2012. Tietomurtojen osalta oli laadittu suuri määrä erillisiä rikosilmoituksia. Osa ilmoituksista sidottiin poliisin suorittamassa esitutkinnassa tiettyyn petosrikokseen ja toimitettiin sen yhteydessä syyteharkintaan. Osa erillisinä rikosilmoituksina käsitellyistä tietomurroista kohdistettiin tiettyyn asiakokonaisuuteen kuuluvaksi ja siirrettiin syyteharkintaan jonkin sivupääpöytäkirjan alapöytäkirjana. Pääpöytäkirjan[255] siirtyessä syyteharkintaan noin 30 tietomurtoa koskevaa rikosilmoitusta oli vielä tutkinnan alaisena. Syyte asiakokonaisuudessa nostettiin 29.1.2013. Päätekijä-Kiveä ei tavoitettu kutsuttavaksi asian pääkäsittelyyn, jolloin vastaajia asiassa oli 16. Heidän osaltaan Helsingin käräjäoikeus antoi kansliatuomion 16.5.2014 (R 13/2692).

Päätekijän osalta asia käsiteltiin Helsingin käräjäoikeudessa 29.8.2014 ja kansliatuomio annettiin 22.9.2014. Helsingin Sanomat uutisoi 23.9.2014 Helsingin käräjäoikeuden tuominneen Suomen todennäköisesti aktiivisimman nettipetosmiehen, Viljar Kiven, 24, yli 300 rikoksesta. Kivi sai tuomion Huuto.net-verkkohuutokauppaan liittyvästä petosvyyhdestä eli vuosina 2011–2012 tehdyistä 280 petoksesta, 51 tietomurrosta sekä kahdeksasta petoksen yrityksestä. Kivi myönsi oikeudessa kaikki teot. Petostehtailut Kivi aloitti vapauduttuaan muihin rikosepäilyihin liittyneestä tutkintavankeudesta kesäkuun 2011 alussa. Käräjäoikeus kovensikin tuomiossaan Kiven rangaistusta hänen aikaisemman rikoshistorian vuoksi. Lisäksi Kivi oli Huuto.net-huutokauppaan liittyviin rikoksiin syyllistyessään aikaisemman ehdollisen vankeusrangaistuksensa koeajalla. Nyt

[255] Asiakokonaisuudessa pääpöytäkirjana toimi rikosilmoitus 8010/R/6908/12. Pääpöytäkirjan lisäksi poliisin suorittamassa esitutkinnassa laadittiin lukuisia sivupääpöytäkirjoja siten, että pääsääntöisesti jokaista pankkitiliä kohti, jolle petoksella saatuja varoja ohjattiin, laadittiin yksi sivupääpöytäkirja. Sivupääpöytäkirjat laadittiin Helsingin poliisilaitoksella pankkitiedusteluilla saatujen tiliotteiden tietojen perusteella. Niissä käsiteltiin pääsääntöisesti ne petokset, joissa asianomistajat eivät itse olleet tehneet asiassa rikosilmoitusta. Vastaavasti sivupääpöytäkirjojen alapöytäkirjoina olivat ne rikosilmoitukset, joista asianomistaja oli jo itse tehnyt rikosilmoituksen. Yleensä ilmoitus oli tehty asianomistajan asuinpaikan poliisilaitoksella ja kirjattu kyseisessä poliisissa tutkittavaksi.

täytäntöönpantava puolentoista vuoden ehdollinen tuomio sisältyi Kiven saamaan saamaan kolmen vuoden ja kahden kuukauden vankeustuomioon.[256]

Asiakokonaisuuden laajuus poliisissa selvisi, kun erillisissä yksittäisissä myynti-petoksista kirjatuissa rikosilmoituksissa oli sama myyjäprofiili, mutta kaupoissa saatuja varoja ohjattiinkin eri henkilöiden pankkitileille. Lisäksi tuolloin tietomurtoja tehtiin kaikkiaan varsin vähän, joten hakemalla tietomurrosta kirjatut rikosilmoitukset, poliisi pystyi sarjoittamaan rikossarjaan kuuluvat myyntiprofiilien anastukset. Sarjoittamista tosin hankaloitti se, että tietomurto-nimikkeen sijasta oli käytetty muita rikosnimikkeitä. Tehtyjä tietomurtoja pystyttiin yhdistämään tutkittavana oleviin tai tutkittavana olleisiin petoksiin; osa tähän laajaan kokonaisuuteen kuuluvista rikosilmoituksista oli jo saatettu syyteharkintaan eri syyttäjänvirastoihin, mutta ne "vedettiin takaisin" Helsingin poliisin tutkittavaksi. Suoritettiin lukuisia pankkitiedusteluja ja löydettiin asianomistajia, jotka eivät olleet tehneet asiassaan rikosilmoitusta jouduttuaan petoksen kohteeksi. Petoksella eri tileille ohjattuja varoja takavarikoitiin ja tileiltä pankkiautomaattinostoin varoja suorittaneiden henkilöllisyys selvitettiin. Rikoksesta epäillyt kuulusteltiin ja heistä muutamat otettiin kiinni, pidätettiin ja vangittiin ja määrättiin vapauttamisen jälkeen matkustuskieltoon. Asiassa suoritettiin kotietsintöjä ja otettiin poliisin haltuun takavarikoitavaa omaisuutta. Asiakokonaisuuden laajuuden vuoksi syytteennostamisen määräajan pidennystä haettiin Helsingin käräjäoikeudelta useaan otteeseen; lukuisten asianomistajien yksityisoikeudelliset vaatimukset tuli selvittää.

Ongelman kyseisen petosvyyhden tutkinnassa aiheutti se seikka, että yksittäisiä rikosilmoituksia oli kirjattu Suomen eri poliisilaitoksiin tutkittavaksi; yhteistä niille oli petosnimike. Vaikkakin varoja oli ohjattu samoille tilille (jolloin myös rikoksesta epäilty on yksi ja sama henkilö eli tilin omistaja) ei tapauksia ollut tutkittu yhdessä. Tietomurron osalta kirjaamistavoissa oli suurta eroa: osa tietomurroista oli kirjattu erillisinä rikosilmoituksina ja osa petosjutun yhteyteen; osa teoista kirjattiin tietomurto-nimikkeellä, osa luvattomana käyttönä ja osa viestintäsalaisuuden loukkauksena – tämä siitä huolimatta, että tekotapa oli kaikissa tapauksissa sama. Lisäksi eri rikosilmoituksien esitutkinnasta vastaavat tutkijat ja tutkinnanjohtajat suorittivat tutkintaa eri tavoin ja rikosilmoituksista osan tutkinta keskeytettiin, osa saatettiin syyttäjälle syyteharkintaan yksittäisenä tapahtumana. Kyseinen petoskokonaisuus ja siinä tulleet ongelmat olivat alkusysäys tämän tutkielman tekemiselle. Ongelmat eivät ole vuoteen 2019 mennessä poistuneet, vaikkakin asiaa on pohdittu oikeusministeriön alaisessa rikoksentorjunta-

[256] Helsingin Sanomat 23.9.2014.

neuvoston (RTN) asiantuntijatyöryhmässä vuoden 2017 aikana[257]. Poliisissa ei edelleenkään ole yhtenäistä näkemystä ja toimintamallia myyntipetoksien tutkinnasta.

4.2. Vertaisverkkokaupat

Yleensä yksityishenkilöt myyvät internetin kauppapaikoilla käytettyä tavaraa. Kilpailu- ja kuluttajavirasto (KKV) ohjeistaa sivustollaan käytetyn tavaran kaupasta, että jos käytetty tavara on ostettu yritykseltä tai muulta elinkeinonharjoittajalta, on kyseessä kuluttajansuojalain (38/1978) alainen kauppa, jolla on myös kuluttajansuojalain mukainen suoja. Kuluttajansuoja tuo turvaa vain, kun ostaa yritykseltä, se ei koske yksityishenkilöiden välistä kauppaa[258]. Eli jos käytetty tavara on ostettu yksityiseltä henkilöltä, ei kyseessä ole kuluttajakauppa. Vertaiskauppaan ei siis sovelleta kuluttajansuojalakia vaan kauppalakia (355/1987). Tavara katsotaan ostetuksi yksityishenkilöltä myös silloin, kun se on ostettu yrityksen pitämältä kauppapaikalta, jossa selkeästi ilmenee kaupan tapahtuvan yksityishenkilöiden kesken. Kyseisenlaisina kauppapaikkoina mainitaan esimerkiksi itsepalvelukirpputorit, myynti-ilmoituksia tarjoavat verkkokirpputorit ja verkkohuutokaupat. Tässä yksityishenkilöiden välisessä kaupassa ostajan velvollisuudet ovat suuremmat kuin kuluttajakaupassa. Koska kahden yksityishenkilön välinen kauppa ei kuulu kuluttajansuojalain piiriin, ei ostaja voi myöskään turvautua kuluttajaneuvonnan apuun [259]

Kauppalaki koskee irtaimen[260] omaisuuden kauppaa ja sitä sovelletaan osittain myös kuluttajakauppaan. Lain mukaan ostaja ei ole velvollinen maksamaan ennen kuin tavara on sopimuksen mukaisesti asetettu hänen saatavilleen tai määrättäväkseen. Ennen kauppahinnan maksamista ostajalla on oikeus tarkastaa tavara tavan mukaisesti tai siten kuin olosuhteisiin nähden on asianmukaista, jollei tällainen tarkastus ole yhteensopimaton sovitun luovutus- ja maksutavan kanssa (KauppaL 49 §). Suomessa on kuitenkin sopimusvapaus, joten lain säännöksiä ei sovelleta, mikäli sopimuksesta, sopijapuolten omaksumasta käytännöstä taikka kauppatavasta tai muusta tavasta, jota on pidettävä sopijapuolia sitovana, johtuu muuta (KauppaL 3 §). Internetin kauppapaikoilla tehtävistä ostotapahtumista kaupankäynnin osapuolet saavat halutessaan sopia toisin.

[257] RTN:n asiantuntijatyöryhmän toimintakausi oli 1.3.–31.10.2017.
[258] Kodin kyberopas 2017: 33.
[259] https://www.kkv.fi/Tietoa-ja-ohjeita/Viat-viivastykset/tavaran-vika-tai-puute/kaytetyn-tavaran-virhe/
[260] Irtain omaisuus (irtaimisto) on omaisuutta, joka ei ole kiinteää, esimerkiksi huonekalut ja kulkuneuvot. Vastakohtana on kiinteä omaisuus, joka on omistuksessa oleva tarkoin rajattu maanpinnan osa aineksineen, mukaan lukien esineet, joita ei voi rikkomatta tai niiden laatua muuttamatta siirtää toiseen paikkaan (kiinteistö).

Yleiseksi käytännöksi onkin muodostunut kauppahinnan maksaminen myyjälle etukäteen, vaikkei millään kauppasivustolla näin kehoteta toimimaan. Normaalisti kauppahintaan lisätään myös postimaksu, jotta myyjä voi heti kauppasumman saatuaan postittaa kaupanteon kohteena olevan tuotteen ostajalle.

Kaupankäynti internetin sivustoilla perustuu pitkälti luottamukseen. Yksityisten myyjien ja ostajien käyttämillä netin markkinapaikoilla tulisi olla saatavilla riittävästi tietoa markkinapaikoilla tapahtuvista huijauksista, sillä yleisimmin myyntipetoksia tapahtuu näillä vertaisverkkokauppasivuistoilla. Selkeät, ajantasalla olevat ja hyvin sijoitellut ohjeet epäilyttävien ilmoitusten tunnistamiseksi auttaisivat ehkäisemään huijatuksi tulemista. Ohjeiden tulisi myös olla näkyvillä niille käyttäjille, jotka ovat ostamassa tai myymässä tuotetta ja ohjeita tulisi korostaa erityisesti niissä tuotekategorioissa, joihin liittyy eniten myyntipetoksia. Kauppasivustojen turvallisuuskäytänteillä voidaan myös ehkäistä petosten mahdollisuus kokonaan vaatimalla sivuston käyttäjiltä vahvaa sähköistä tunnistautumista[261]. Lisäksi käyttäjille annettavat palautteet sekä välimiespalvelun (niin sanottu escrow-palvelu[262]) käyttö ennaltaestävät myyntipetoksien tekemistä.[263]

Kaupan liiton lokakuussa 2015 tekemän selvityksen mukaan epävarma talous- ja työllisyystilanne, verkkokaupan yleistyminen mutta myös ympäristötietoisuuden nousu saavat ihmiset ostamaan yhä enemmän toisiltaan. Vertaisverkkokauppa eli internetin kautta käytävä kauppa ei ole marginaali-ilmiö: jo tuolloin yli puolet suomalaisista oli käynyt joskus vertaisverkkokauppaa. Suomalaiset kuluttajat ostivat toisilta kuluttajilta verkon välityksellä 1.1.2014–30.9.2015 välisenä aikana tutkimuksessa tarkasteltuja tavaroita noin 500 miljoonalla eurolla ja autoja, moottoriajoneuvoja, veneitä ja tarvikkeita yli 900 miljoonalla eurolla. Vertaisverkkokaupan mittaluokkaa voi verrata suomalaisten Virossa vuonna 2014 tuotteisiin ja palveluihin kuluttamaan summaa, joka oli 477 miljoonaa. Suomalaiset kuluttajat ostivat vuonna 2014 lisäksi kotimaisista verkkokaupoista selvityksen tuotteita (poislukien autot, veneet ja niin edelleen) 1 480 miljoonalla eurolla ja ulkomaisista verkkokaupoista 1 420 miljoonalla eurolla.[264]

[261] Vahva sähköinen tunnistautuminen voi tapahtua joko pankkien verkkopankkitunnuksia, Väestörekisterikeskuksen kansalaisvarmennetta tai teleyritysten mobiilivarmenteita käyttämällä.
[262] Virolaisella osta.ee-nettihuutokauppapalvelulla on käytössään escrow-palvelu, jossa kauppasumman maksaminen kaupan osapuolten välillä tapahtuu ulkopuolisen osapuolen kautta. Se pitää tuotteesta maksettuja varoja hallussaan, kunnes ostaja on vastaanottanut tuotteen. Oikeusministeriö 2017: 44.
[263] Oikeusministeriö 2017: 24.
[264] Kaupan liitto 24.11.2015.

Kuluttajien pääasiallisena vertaisverkon ostopaikkana oli jo kyseisen Kaupan liiton vuonna 2015 tekemän tutkimuksen aikana Tori.fi-sivusto ja toiseksi suosituimpana kauppapaikkana oli Huuto.net-sivusto.[265] Vuonna 2016 Anniina Lehtonen teki Poliisiammattikorkeakoulun opinnäytetyön (AMK) ”Nettipetosten kasvu 2010 luvulla. Nettipetokset selityksenä petosten kokonaismäärän kasvulle?” Tuossa opinnäytetyössä oleva taulukko selventää hyvin myyntipetosten määrässä tapahtunutta muutosta suhteessa eri internetin kauppapaikkoihin vuosina 2010–2015:

Nettipetosten määrä nettisivustoilla	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**
Tori.fi	64	348	703	2 221	2 863	4 869
Huuto.net	128	664	604	494	303	290
Facebook	16	65	98	222	510	563
Nettipetokset yhteensä	**208**	**1 077**	**1 405**	**2 937**	**3 676**	**5 749**
Kasvu-% edellisestä vuodesta		417,8	30,5	109,0	25,2	56,4

Taulukko 5. Myyntipetosten määrä eri myyntisivustoilla vuosina 2010–2015 ja määrän vuosittainen kasvu. (Lehtonen 2016: 19.)[266]

Taulukossa näkyy yleinen myyntipetosten määrän kasvu, mutta myös vuoden 2011–2012 Huuto.net-petoskokonaisuus, samoin Facebookin yleistyminen markkinapaikkana ja siellä tapahtuvien petosten määrän kasvu. Huuto.netissä tapahtuvia huijauksia on pystytty kitkemään pitkälti sillä, että palvelun käyttäminen vaatii nykyisin järeämmän rekisteröitymisen kuin Tori.fi[267]. Vähittäiskaupan kamppaillessa supistuvan kysynnän kanssa kuluttajienvälinen kaupankäynti kasvaa. Edelleen jatkuvan hitaan talouskasvun aikana vertaiskauppa näyttäytyy kuluttajille houkuttelevana vaihtoehtona edullisten hintojen vuoksi. Vertaiskauppa nähdään myös mahdollisuutena kierrättää itselle tarpeettomaksi jäänyttä tavaraa.[268] MTV3:n uutisoinnissa 10.3.2019 todettiin suomalaisten ostavan ja myyvän innokkaasti käytettyä tavaraa internetin markkinapaikoilla – ja samalla lisääntyvät myös vertaisvertaiskauppaan liittyvät huijaukset[269]. Selvennän seuraavaksi kahden suosituimman kauppapaikan eli Huuto.netin ja Tori.fi:n toimintaa lähinnä niiden verkkosivuilta selviävän tiedon perusteella keskittyen myyntipetosten kannalta olennaisiin asioihin.

[265] Yksi tuolloin käytetyistä sivuistoista, Keltainenpörssi.fi, lopetti toimintansa itsenäisenä verkkopalveluna 30.6.2016 ja kaupankäynti siirtyi Huuto.net-palveluun. Kaupan liitto 24.11.2015.
[266] Lehtonen oli kerännyt taulukon tiedot poliisin Rikitrip-tietojärjestelmästä.
[267] MTV3 10.3.2019.
[268] Kaupan liitto 24.11.2015.
[269] MTV3 10.3.2019.

4.2.1 Huuto.net

Kuluttajien välinen kaupankäynti eli vertaiskauppa koki vuonna 1999 mullistuksen Huuto.netin perustamisen myötä. Huuto.net oli Suomen ensimmäinen internetiä hyödyntävä huutokauppa-alusta. Palvelun suosio kasvoi vuosien varrella tasaisesti ja se kehittyi verkkohuutokaupasta monipuoliseksi vertaiskaupan alustaksi, jonka kautta myydään kaikkea mahdollista. Nimestään huolimatta moni Huuto.netin kaupoista ei enää synny alkuperäisellä huutokauppamenetelmällä. Vuonna 2007 Huuto.net muuttui entistä monipuolisemmaksi vertaiskaupan alustaksi, kun palvelussa pystyi myydä myös kiinteällä Osta heti -hinnalla. Sittemmin on tullut mahdolliseksi solmia kauppa ennalta määrätyllä kiinteällä hinnalla, mikä on yhä useamman kaupan tekotapa. Vuonna 2008 myös yrityskäyttäjät toivotettiin tervetulleeksi palveluun ja Taloustutkimus nosti Huuto. netin Suomen tunnetuimmaksi verkkobrändiksi.[270]

Vuoden 2012 lopulla uutisoitiin nettihuutokaupan tehostavan valvontaa: Huuto.net sai runsaasti negatiivista julkisuutta huijariryhmän napattua käyttäjiltä noin 150 000 edestä rahaa käyttämällä hyväkseen verkkoon vuodettuja salasanoja. Vaikkakaan salasanoja ei saatu tietoon Huuto.netin järjestelmästä, siellä onnistuttiin käyttämään muualta vuodettuja salasanoja, koska huutokaupan asiakkaat käyttivät samoja salasanoja eri sivustoilla. Kysymyksessä oli aiemmin käsitelty Huuto.net-petoskokonaisuus. Sen seurauksena Huuto.net tehosti valvontaa, paransi tietoturvaansa huijareita vastaan ja ohjeisti käyttäjiään varovaiseen nettishoppailuun muun muassa muistuttamalla netti-kaupan vanhalla viisaudella ”jos jokin tarjous kuulostaa liian hyvältä ollakseen totta, se useimmiten on juuri sitä”. Samaa salasanaa ei saa käyttää eri palveluissa tietovuotojen uhan vuoksi. Maksua ei myöskään pitäisi maksaa kuin myyjän henkilökohtaiselle pankkitilille. Hälytyskellojen tulisi soida, jos myyjä ei suostu tapaamaan tai lähettämään tuotetta postiennakolla ennakkotarkastusoikeudella tai jos myynnissä oleva tuote on uusi ja haluttu, mutta myynnissä huomattavasti normaalia markkinahintaan halvemmalla. Huuto.net myös vankisti tietoliikenteensä seurantaa ja seurasi entistä tarkemmin epäilyttäviä käyttäjiä ja kohteita.[271]

Uudistunut Huuto.net julkaistiin vuonna 2013[272]. Palveluun rekisteröityneet käyttäjät asioivat Huuto.netissä nimimerkillä ja käyttäjien välistä luottamusta halutaan edistää tarjoamalla mahdollisuus varmentaa omat henkilötietonsa palvelussa omilla pankki-

[270] Sanoma 28.4.2014.
[271] Kauppalehti 29.8.2012.
[272] Sanoma 28.4.2014.

tunnuksillaan, jolloin muut käyttäjät näkevät henkilön olevan tunnistautunut käyttäjä. Käyttäjän tulee antaa palveluun rekisteröityessään vaaditut rekisteröintitiedot, joiden avulla hänet voidaan tunnistaa ja yksilöidä ja jotka hän sitoutuu pitämään ajan tasalla. Käyttäjän tulee myös valita salasanalla suojattu käyttäjätunnus palvelun käyttämistä varten. Väärien käyttäjätietojen antamisen mainitaan erikseen olevan rikos. Huuto.netiin ei saa automaattisesti käyttöoikeutta: mikäli kaikkia käyttäjätietoja ei ole annettu, ne on annettu puutteellisesti tai epäasiallisesti taikka käyttäjä ei muuten täytä käyttöoikeuden myöntämisen edellytyksiä, käyttöoikeutta ei välttämättä myönnetä. Lisäksi palveluun rekisteröityvän tulee olla täysivaltainen. Yhdellä henkilöllä voi olla vain yksi tunnus.

Nykyisin Huuto.net on Sanoma Media Finland Oy:n tuottama ja ylläpitämä verkkopalvelu. Palvelussa kaupanteko tapahtuu käyttäjien kesken heidän erikseen sopimin ehdoin eikä Sanoma Media Finland Oy ole palveluntarjoana kaupan osapuoli missään suhteessa vaan se tarjoaa käyttäjilleen kauppapaikan. Huuto.net-sivustojen mukaan myyminen on helppoa ja luotettavaa. Myyminen on helppoa siksi, että kaupat hoidetaan myyjän puolesta ja palvelun ansiosta välttyy turhilta yhteydenotoilta, alustavilta varauksilta, anonyymeiltä kauppakumppaneilta sekä erillisten kauppasopimuksien teolta. Myyjä jättää ilmoituksen, Huuto.net hoitaa kaupat myyjän puolesta, minkä jälkeen myyjä vastaanottaa maksun ja luovuttaa tuotteen. Kauppojen syntyessä Huuto.net ilmoittaa sekä myyjälle että ostajalle tuotteen kauppahinnan sekä kauppakumppanin yhteystiedot. Huuto.net-myyjä voi myös lähettää tuotteen ostajalle edullisesti lähikaupasta Huutopakettilähetyksenä.

Ilmoittaminen ja myyminen on tavallisille käyttäjille Huuto.netissä helppoa, sillä se vaatii vain käyttäjätunnuksen luomista palveluun. Käyttö on myös ilmaista: Huuto.net on ilmainen yksityismyyjille, jotka solmivat alle 50 kauppaa vuodessa. Perusilmoittelun lisäksi myyjille on tarjota maksullisia lisäpalveluja. Lisäksi palveluntarjoaja voi periä välityspalkkion kaupan kohteen myyntihinnasta. Huuto.netissä voi aina myös antaa palautetta muista käyttäjistä, joiden kanssa on käynyt kauppaa. Myyjän käyttäjäpalautteeseen suositellaankin aina tutustumaan ennen tarjouksen tekemistä ja suosimaan tunnistautuneita myyjiä ennakkomaksettavissa lähetyksissä. Tällä aktiivisella palautteen antamisella ja sen käyttämisellä halutaan varmistaa, että Huuto.net on luotettava kauppapaikka. Huuto.net onkin pysynyt suosittuna vertaisverkkokauppana[273]: sillä on 1,7 miljoonaa käyttäjää.

[273] MTV3 10.3.2019.

4.2.2. Tori.fi

Vuonna 2009 Suomeen perustettu Tori.fi on osa globaalia Schibsted Media Groupia, joka toimii 30 maassa. Tori on kasvanut kymmenessä vuodessa keskeiseksi osaksi suomalaista elämää. Se on Suomen suurin ja suosituin kuluttajien välinen kauppapaikka internetissä: yli 2,4 miljoonaa suomalaista käyttää Toria kuukausittain[274]. Tori on Suomen seitsemänneksi vierailluin verkkosivusto. Sivustolle voi lisätä ilmoituksen ilmaiseksi, nopeasti ja helposti eikä se vaadi rekisteröitymistä; nykyisin palveluun voi tosin rekisteröityä ja luoda itselleen Tori-tilin. Toriin jätettiin yhteensä yli 10,3 miljoonaa ilmoitusta vuonna 2018[275], jolloin ilmoittajat tienasivat Torin kautta yhteensä 626 miljoonaa euroa. Kauppoja tehtiin 3,05 miljoonaa kappaletta. Kuluttajien välinen kauppa näkyy myös kansantalouden tasolla: Torin myynti-ilmoitusten pyyntihintojen summa mitataan vuositasolla miljardeissa euroissa. Vuosittain Torin ilmoituksista on huijausilmoituksia noin tuhat eli puoli promillea kaikista sivuston ilmoituksista.[276] Tiivis yhteistyö viranomaisten kanssa auttaa kuitenkin ehkäisemään huijauksia.

Tori.fi-sivuston turvallisuudesta on tietoa Lehtosen opinnäytetyössä vuodelta 2016. Hän haastatteli Antti Lehtoa (tuolloinen titteli *Content and Security Manager*), joka vastasi Torin turvallisuudesta, sisällöstä, ilmoitusten moderoinnista sekä yhteistyöstä poliisin, tullin ja muiden oikeudenhaltijoiden kanssa. Nettisivuston käyttäjä- ja myyntimäärän kasvaessa myös rikolliset ovat siirtyneet sinne. Tori.fi:llä on moraalinen vastuu ihmisten turvallisuudesta heidän sivustollaan. Sivuston turvallisuutta oli lähdetty kehittämään muutamaa vuotta aikaisemmin, sillä sivustosta haluttiin mahdollisimman luotettava ja turvallinen paikka ihmisten ostaa ja myydä tuotteita. Tuolloin aloitettiin myös aktiivinen yhteistyö poliisin kanssa ja erityisesti tiedonvaihto Keskusrikospoliisin (KRP) ja Poliisihallituksen kanssa oli kehittynyt valtavasti. Nettipetosten tekijöihin varauduttiin ja turvallisuuteen panostettiin erityisesti tekniikkaan satsaamalla. Toriin saattaa tulla jopa 50 000 ilmoitusta päivässä ja kaikki ilmoitukset käydään läpi ennen julkaisua;

[274] Mielenkiintoisena kuriositeettina mainittakoon Torin *Second Hand Effect* eli kierrätysvaikutus, jonka mukaan käytetyn tavaran kauppa eli vertaiskauppa auttaa pienentämään hiilijalanjälkeä. Schibsted kävi lävitse sen kymmenestä eri kauppapaikasta kerättyjä tietoja ja muutti käyttäjiensä kaupankäynnin ympäristöhyödyt numeroiksi; mukana olleista sivuistoista yksi oli Tori Suomesta. Käytetyn tavaran kaupan eli tavaroiden kierrättämisen vaikutus päästöjen säästöihin vuonna 2017 oli jopa 21,5 miljoonaa tonnia hiilidioksidipäästöjä ja 1,2 miljoonaa tonnia muovia vuodessa. Tavaroiden uudelleen käyttäminen pienentää hiilijalanjälkeä ja käytetyn tavaran kauppa on teko, jolla todella on vaikutusta. Sivuston 'Kauppiaille'-kohdassa tosin mainitaan, että tutkimusten mukaan Torissa kuukausittain vierailevista 2,4 miljoonasta kävijästä vain 20 prosenttia on halukkaita ostamaan käytettyä tavaraa. Kauppiaille halutaankin tarjota mahdollisuus päästä kiinni Torissa olevien kuluttajien ostopotentiaaliin Tori-kaupan avulla, joka on yrityksille, toiminimille ja autoliikkeille tarkoitettu palvelu.

[275] Tutkielman kirjoitushetkellä toukokuussa 2019 Torissa oli 1 192 745 ilmoitusta.

[276] MTV3 10.3.2019.

läpikäynti tapahtuu niin koneälyllisesti kuin manuaalisestikin. Tekniikan ansiosta Tori.fi onkin Lehdon mukaan yksi turvallisimmista tämänkaltaisista sivustoista maailmassa.[277]

Torilla tapahtunutta rikollisuutta tilastoidaan. Niin sanottu ’*consumer to consumer*’ eli kuluttajien välinen rikollisuus on kasvussa. Muita Torissa esiintyviä rikollisuuden tyyppejä ovat muun muassa ’*phishing*’ eli tietojen kalastelu (esimerkiksi henkilötunnuksen tai pankkitunnusten urkkiminen), ulkomailta käsin tehdyt rikokset, eläimiin kohdistuvat rikokset. Tori.fi haluaa helpottaa poliisin työtaakkaa. Torin turvallisuustiimi ennaltaehkäisee paljon rikoksia poimimalla selkeästi petolliseen tarkoitukseen tehtyjä ilmoituksia pois sivustolta. Epärehelliset sivuston käyttäjät poistetaan, kun taas palveluun tunnistautuva asiakas on luotettava myyjä[278]. Myös Torin asiakkaat auttavat aktiivisesti petosten ehkäisyssä ilmoittamalla petoksista sekä esimerkiksi tunnistessaan aitoina myytäviä väärennöksiä tai jäljitelmiä. Lisäksi Tori antaa poliisille tietoa ahkerista nettipetostelijoista tai muuten epäilyttävistä henkilöistä sarjoittamalla eli tunnistamalla ja tulkitsemalla kahden tai useamman yksittäisen rikostapauksen tai rikossarjan keskinäiset suhteet, yhteydet ja yhtäläisyydet. Sivustolta löytyy paljon ohjeita, miten tunnistaa mahdollinen rikollinen toimija.[279]

Torin käyttäjä löytää ohjeet turvalliseen kaupankäyntiin ’Turvallisuus’-linkin takaa, mikä on Tori.fi-sivun alaosassa yhtenä vaihtoehtona muiden linkkien (Asiakaspalvelu, Tori yrityksenä, Mainostajille, Blogi ja Tietosuoja) mukana. Turvallisen kaupankäynnin päävalikko sisältää turvallisuusohjeet, ”Älä osta sikaa säkissä” eli vinkkejä verkkoostamiseen, sekä erilliset ohjeet lemmikkeihin liittyvään kaupankäyntiin. Verkkoostamisen vinkit ohjeistavat mihin tulisi kiinnittää huomiota ennen kaupan solmimista, pyytämään kuitin tai vahvistuksen tuotteesta, kysymään myyjältä lisäkuvia, varmistamaan myyjän henkilöllisyyden ja neuvovat mitä tulee tehdä, jos myyjä ei lähetä maksettua tuotetta. Turvallisuusohjeina käsitellään päänäkymässä kalasteluviestit, myyjän opas, ostajan opas, annetaan esimerkkejä huijaustapauksista ja kerrotaan ulkomaisesta kaupankäynnistä. Ilmiantokaavakkeella voi ilmiantaa asiattoman tai epäilyttävän ilmoituksen tai ilmoittajan. Lisää turvallisuusartikkeleja saa näkyviin linkin takaa ja ne liittyvät muun muassa vuokra-asuntoihin, loppuunmyytyihin konsertteihin, palveluihin, polkupyöriin ja autoihin.

---

[277] Lehtonen 2016: 28–30.

[278] Haastatteluhetkellä 7.6.2016 Lehto kertoi tavoitteesta kehittää Tori.fi-sivustoa siten, että asiakas voi ilmoittaa itsestään enemmän tai vähemmän tietoja. Henkilö, joka tunnistautuu palveluun saa tietynlaisen luotettavan myyjän leiman itselleen. Ne käyttäjät, jotka eivät ilmoita paljon tietoa itsestään näyttävät taas hieman epäilyttävimmiltä. Lehtonen 2016: 30.

[279] Lehtonen 2016: 30–31.

Myyjän oppaassa annetaan muistisääntöjä myyjälle, joka tekee kauppaa netissä. Kaupat on helpoin sopia kasvotusten, jolloin kannattaa valita jukinen paikka, mutta jos ostaja tulee noutamaan tuotteen, ostajan ei sinänsä tarvitse tietää kuin katuosoite, sillä tuotteen voi tuoda hänelle esimerkiksi taloyhtiön parkkipaikalle. Noudon aikana olisi hyvä, ettei myyjä olisi yksin kotona (jos kaupat on sovittu sinne). Mikäli ostaja asuu kauempana, suositellaan tutustumaan eri postitusvaihtoehtoihin. Yleisimpänä tapana postitettavien tuotteiden kanssa on maksu ensin tilille ja paketti postiin. Ohjeessa muistutetaan lähettämään ostajalle lähetystunnus, mutta mikäli kyseessä on pieni tuote, niin myös valokuva kirjeestä kertoo lähetyksen tiedot. Postiennakkotapauksessa voi pyytää postimaksun etukäteen, jotta myyjälle ei aiheudu ylimääräisiä kustannuksia, mikäli ostaja ei noudakaan pakettia postista. Myyjää muistutetaan käymään poistamassa ilmoitus, kun tuote on saatu myytyä. Lisäksi myyjän tulisi käyttäytyä kauppatilanteessa asiallisesti sekä hyvien tapojen mukaisesti.

Ostajan oppaassa annetaan heti neuvo olla lähettämättä rahaa etukäteen näkemättä tuotetta tai varmistamatta, että tuote saapuu maksun yhteydessä! Vaikka myyjä ilmoittaa henkilötietonsa tai pankkitilinsä numeron, se ei turvaa huijaukselta. Erityiseen varovaisuuten kehotetaan kun tarjous vaikuttaa liian hyvältä ollakseen totta, toinen osapuoli kiirehtii jatkuvasti ostopäätöksiä, joku tiedustelee ostajan pankkitilin tai luottokortin numeroa tai kun ostaja maksaa suuren rahasumman tuntemattomalle henkilölle. Myyjän numero kehotetaan varmistamaan numerotiedustelusta; prepaid-liittymässä on aina riskinsä. Varoitusmerkkien pitäisi soida, kun myyjä välttelee kohtaamista. Myyjän henkilöllisyyden varmistamiseksi voi myös käyttää hakukonetta. Kauppoja kannattaa sopia kasvotusten, mutta mikäli tuote tulee postitse, olisi suositeltavaa tehdä kaupat postiennakolla. Myyjältä suositellaan pyydettäväksi paketin lähetystunnus ja kuvan kirjeestä, jos tuote lähetetään kirjeenä.

4.3. Rikostutkinta

Rikostutkinta käynnistyy, kun epäillystä rikoksesta tehdään ilmoitus esitutkinta-viranomaiselle, yleensä poliisille, tai kun esitutkintaviranomainen itse epäilee rikoksen tapahtuneen. Jotta voitaisiin puhua rikoksesta, on oikeustosiseikkojen oltava olemassa ja niiden on täytettävä jonkin rikoksen tunnusmerkistö: jonkun henkilön on täytynyt

syyllistyä rikokseen ja tämä tapahtuma voidaan määritellä ajallisesti ja paikallisesti[280]. Rikoksen ilmitulo käynnistää esitutkinta- ja syyttäjäviranomaisista sekä tuomioistuimista koostuvan valtion lainkäyttökoneiston. Valtiovallalla (julkisella vallalla) on vastuu siitä, että todettu rikos tai perusteltu rikosepäily johtaa tehokkaaseen – mutta myös puoluettomaan – tutkintaan ja oikeudenkäyntiin.[281] Suomessa poliisi on yleinen esitutkintaviranomainen ja sen toimintaa säädellään poliisilailla (PolL 22.7.2011/872). Poliisin yhtenä tehtävänä on rikosten ennalta estäminen, paljastaminen, selvittäminen sekä syyteharkintaan saattaminen (PolL 1.1 §). Muut rikostutkintaa suorittavat tahot ovat Rajavartiolaitos, Puolustusvoimat ja Tulli, jotka ovat niin sanottuja erityisiä esitutkintaviranomaisia; niille on annettu lainsäädännössä pysyvä oikeus ja velvollisuus tutkia omalla toimialallaan tapahtuneita rikoksia[282].[283]

Laissa poliisin hallinnosta (PolHalL 10.7.2015/860 1 §) säädetään, että poliisitoimi kuuluu sisäministeriön hallinnonalaan. Sisäministeriö vastaa poliisin toimialan ohjauksesta ja valvonnasta. Poliisiyksikköjä ovat valtakunnallisena yksikkönä Suojelupoliisi (Supo) sekä Poliisihallitus (Poha) ja sen alaiset yksiköt: valtakunnalliset yksiköt Keskusrikospoliisi (KRP) ja Poliisiammattikorkeakoulu (Polamk) sekä paikallishallintoviranomaisena poliisilaitokset, joista teen selkoa tarkemmin myöhemmin; poliisitoimesta Ahvenanmaan maakunnassa säädetään erikseen. Poliisin hallintolaki (PolHalL 14.2.1992/110) ja asetus (15.3.1996/158) määrittävät poliisin eri yksiköiden keskinäisen työnjaon. Poliisin hallintolain (7 §) mukaan paikallispoliisin tehtäviin kuuluu valtaosa esitutkintaan tulevien rikosten selvittämisestä, mutta poliisin valtakunnalliset yksiköt eli KRP ja Supo tutkivat kuitenkin eräät rikokset.[284]

Poliisi toimii pääsääntöisenä toimivaltaisena viranomaisena tietoverkkorikosten ennalta estämisessä, selvittämisessä ja syyteharkintaan saattamisessa. Tulli ja Rajavartiolaitos suorittavat omilla toimialoillaan rikostutkintaa ja niihin liittyen tietoverkkoja ja tietotekniikkaa hyväksi käyttävien rikosten tutkintaa. Poliisille erittäin tärkeä yhteistyökumppani tietoverkkorikostutkinnassa ja kybertilannekuvan ylläpidossa on Kyberturvallisuuskeskus, mutta sitä ovat tietoverkkorikollisuuden ennalta estämisessä,

[280] Frände 2012: 533–534. Teoksessa Prosessioikeus.
[281] Virolainen 2012: 65. Teoksessa Prosessioikeus.
[282] Niemi 2012: 850. Teoksessa Prosessioikeus.
Rajavartiolaitoksen toimivallasta esitutkintaan säädetään rajavartiolaissa (RVL 15.7.2005/578), sotilasviranomaisten eli Puolustusvoimien tekemästä rikostorjunnasta säädetään laissa sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa (28.03.2014/225) ja Tullin suorittaman tullirikosten esitutkinnasta säädetään tullilaissa (TulliL 29.12.1994/1466). Niemi 2012: 850–851.
[283] Helminen, Fredman, Kanerva, Tolvanen & Viitanen 2014: 125, 133.
[284] Helminen ym. 2014: 126.

paljastamisessa ja selvittämisessä myös Puolustusvoimat, valtioneuvoston tilannekeskus (VNTIKE) sekä valtiovarainministeriö valtion omiin tietojärjestelmiin liittyen. Näiden viranomaisten lisäksi myös yksityisillä toimijoilla on merkittävä rooli tietoverkkorikollisuuden torjunnassa; pisimmällä yhteistyö on finanssisektorin kanssa. Muutoin poliisin ja elinkeinoelämän välinen säännöllinen tietoverkkorikollisuuden torjuntaa koskeva yhteistyö ja tiedonvaihto ovat Suomessa vasta alkuvaiheessa. Erityisesti tietoturva-alan yrityksien kanssa yhteistyötä tulisi merkittävästi tiivistää: niillä on erittäin hyvä kuva suomalaisiin yrityksiin kohdistuvista uhista.[285]

Tietoverkkorikostorjunnan tehtävänjakoa, koordinointia ja tutkintavastuita poliisin eri yksiköiden välillä käsitellään Poliisihallituksen antamassa ohjeessa vakavien tietoverkkorikosten torjunnan järjestämisestä (2020/2013/3780) sekä määräyksessä Keskusrikospoliisin ja muiden poliisiyksiköiden välisestä tehtävänjaosta sekä yhteistyöstä rikostorjunnassa (2020/2013/4613). Näissä asiakirjoissa painotetaan erityisesti verkostoitumista tietoverkkorikosten esitutkintaan ja tietotekniseen tutkintaan erikoistuneiden tutkijoiden välillä. Supon rooli tietoverkkorikostorjunnassa on ennaltaestää ja paljastaa terrorismia, laitonta tiedustelutoimintaa ja valtion turvallisuutta vaarantavaa ääriliikkeiden toimintaa sekä tutkia vakoilurikoksia niin reaalimaailmassa kuin tietoverkoissa. Lisäksi Supo tekee ennalta estävää turvallisuustyötä kyberuhkien torjunnassa lisäämällä uhkia koskevaa tietoisuutta viranomaisissa ja yksityisen sektorin organisaatioissa. Supo myös selvittää haittaohjelmahyökkäyksiä yhteistyössä muiden viranomaisten ja tarvittaessa myös yksityisen sektorin kanssa.[286]

KRP:ssä toimiva kyberrikostorjuntakeskus (poliisin kyberkeskus) on tietoverkkorikosten esitutkintaan erikoistunut yksikkö. Poliisin kyberkeskuksessa tutkitaan pääasiallisesti tietoverkkoympäristössä tehtyjä laajempia kansainvälisiä rikoskokonaisuuksia. Se myös vastaa tietoverkkorikostorjunnasta eli rikoksina hakkeritapauksista, palvelunestohyökkäyksistä sekä muista vakavista ja kansainvälisistä tietojärjestelmiin kohdistuneista rikoksista. Kyberkeskus toimii yhteistyössä muiden poliisiyksiköiden kanssa tietoverkoissa tapahtuvan lasten seksuaalisen hyväksikäytön ja maksukorttiliikenteen torjunnassa.[287] Lisäksi poliisin kyberkeskus tarjoaa poliisihallinnolle kybertoimintaympäristön palveluja, keskeisimpänä digitaaliforensiikka ja tietoverkkoihin liittyvä tiedonhankinta. KRP:n tietoteknisen tutkinnan yksikkö on osa

[285] Sisäministeriö 2017b: 25, 27.
[286] Sisäministeriö 2017b: 25–26.
[287] Nämä rikollisuuden osa-alueet vastaavat niitä, joista myös Europolin European Cyber Crime Center (EC3) vastaa.

poliisin kyberkeskusta. Lisäksi KRP:n rikostekninen laboratorio palvelee koko poliisihallintoa teknistä erityisosaamista ja -resursseja edellyttävissä tapauksissa.[288]

EU:n jäsenmaiden tietotekniikka- ja tietoverkkorikostorjunnan asiantuntijoiden yhteistyöryhmän, *European Union Cybercrime Task Force*n (EUCTF) työskentelyyn osallistuvat eri maiden kansallisten tietotekniikkarikosyksiköiden päälliköt. Suomen edustaja on KRP:stä. KRP on Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen[289] mukainen 24/7/365 -periaatteella toimiva yhteyspiste. Suomen poliisi tekee kansainvälistä operatiivista yhteistyötä Europolin kanssa. Europolin Alankomaihin perustama *European Cyber Crime Centre* (EC3) on keskeinen toimija tietoverkkorikostorjunnassa ja Suomen poliisi on lähettänyt sinne asiantuntijan. Poliisin kyberkeskus osallistuu asiantuntijaryhmän toimintaan, jonka tarkoituksena on auttaa ja osallistua Interpolin toimintaan tietoverkkorikostorjunnassa[290]. Suomi tekee kansainvälistä yhteistyötä myös osallistumalla YK:n kriminaalipoliittisen toimikunnan työhön. Esimerkiksi YK:n järjestäytyneen kansainvälisen rikollisuuden vastainen yleissopimus (UNTOC[291]) ja useat YK:n yleiskokouksen päätöslauselmat antavat mahdollisuuksia kansainväliselle yhteistyölle. YK:n huumeiden ja rikollisuuden torjunnasta vastaava toimisto (UNODC[292]) on valmistellut ohjelman tietoverkkorikostorjuntaan[293].[294]

Suomessa tietoverkkorikollisuuden tutkinnasta vastaavat paikalliset poliisilaitokset. Paikallispoliisi on Suomessa jakautunut 11 poliisilaitokseen, jotka ovat Helsingin, Itä-Uudenmaan, Länsi-Uudenmaan, Hämeen, Kaakkois-Suomen, Lounais-Suomen, Sisä-Suomen, Pohjanmaan, Itä-Suomen, Oulun ja Lapin poliisilaitos.[295] Paikallispoliisin toiminta on järjestetty siten, että poliisilaitos vastaa poliisin tehtävistä sen toimialueellaan (PolHalL 6 §). Myös esitutkintatehtävät jakautuvat alueperiaatteen mukaan, kuten paikallispoliisin tehtävät yleensä: kukin 11 poliisilaitoksesta hoitaa lähtökohtaisesti niiden rikosten esitutkinnan, jotka ovat tapahtuneet kyseisen poliisilaitoksen alueella.[296] Poliisilaitosten päivittäistutkinnan yksiköissä tutkitaan valtaosa tietoverkko-

[288] Sisäministeriö 2017b: 26.
[289] Budapestin sopimus.
[290] Singaporeen on perustettu Interpolin *Global Complex for Innovation* (IGCI), joka tekee kansainvälistä operatiivista yhteistyötä muun muassa tietoverkkorikollisuuden torjunnassa (*Digital Crime Centre*) ja avustaa jäsenmaita tietoverkkorikostorjunnassa sekä tukee niiden osaamisen kehittämisessä. Sisäministeriö 2017b: 28.
[291] *United Nations Convention against Transnational Organised Crime*
[292] *United Nations Office on Drugs and Crime*.
[293] *Global Programme on Cybercrime.*
[294] Sisäministeriö 2017b: 28–29.
[295] Kussakin poliisilaitoksessa on yksi pääpoliisiasema sekä useampia poliisiasemia ja yhteispalvelupisteitä.
[296] Helminen ym. 2014: 127.

ympäristössä tehdyistä rikoksista, muun muassa petokset ja kunnianloukkaukset. Vaativammat ja laajemmat kokonaisuudet tutkitaan joko poliisilaitosten päivittäistutkinnassa niin sanottuna projektitutkintana tai sitten pitkäkestoisen ja keskitetyn rikostutkinnan yksiköissä. Kaikissa poliisilaitoksissa toimii nykyään digitaalisen todistusaineiston käsittelyyn ja analysoimiseen eli digitaaliforensiikkaan erikoistuneita yksiköitä.[297]

Rikosprosessi eli oikeudenkäynti rikosasioissa on lailla säännelty menettely, jossa väitetään, että on tapahtunut rikos ja jossa kyseisestä rikoksesta vaaditaan rangaistusta vastaajalle eli rikoksesta epäillylle (syytetylle)[298]; rikosprosessin tarkoituksena on siten saada rikoksen tehnyt henkilö vastuuseen teostaan. Rikosvastuun toteutuminen edellyttää rikosoikeudellisen oikeudenmukaisuuden toteutumista: vain rikoksen tehnyttä henkilöä voidaan rangaista ja annetun rangaistuksen on oltava oikeudenmukaisessa suhteessa sekä tekijän syyllisyyteen että rikoksen vakavuusasteeseen. Se myös korostaa rikosprosessin tehokkuutta sekä totuuden selvittämistä ja rikoslain oikeaa soveltamista. Rikosprosessiin voidaan laajassa mielessä katsoa kuuluvan myös oikeudenkäyntiä edeltävät alkuvaiheet eli poliisin rikosepäilyn perusteella suorittama esitutkinta sekä virallisen syyttäjän esitutkinnan perusteella tekemä syyteharkinta ja syytettä koskeva päätöksenteko.[299]

Rikosprosessin eri vaiheissa on selvitettävä epäillyn rikoksen tapahtuminen, rikoksen tehneen henkilön henkilöllisyys sekä hänen syyllisyytensä tapahtuneeseen rikokseen, rikoksen asianomistajat eli vahinkoa kärsineet, samoin rikoksen perusteella esitettävät vaatimukset[300]. Rikosprosessilla on kaksoisfunktio: sen menneisyyteen suuntautuva (retrospektiivinen) tehtävä on toteuttaa rikosvastuu eli rikosoikeus oikeudenmukaisesti yksittäistapauksessa sekä antaa oikeussuojaa rikokseen perustuvia oikeudenloukkauksia kohtaan; rikosprosessin tulevaisuuteen suuntautuva (prospektiivinen) tehtävä on kriminaalipoliittinen eli sen keskeinen tehtävä on vaikuttaa ihmisten käyttäytymiseen

[297] Sisäministeriö 2017b: 25–26.

[298] Yksi oikeudenmukaisen oikeudenkäynnin perustekijöistä on syyttömyysolettama: Rikoksesta epäiltyä on kohdeltava esitutkinnassa syyttömänä (ETL 4:2 §); osa epäilyistä jää toteennäyttämättä tai osoittautuu jopa vääriksi, miksi käytetäänkin termiä ’(rikoksesta) epäilty’. Helminen ym. 2014: 94.
Kun asia lähtee poliisilta syyttäjälle syyteharkintaan, käytetään samasta henkilöstä termiä ’syytetty’. Oikeudenkäynnissä hänestä käytetään termiä ’vastaaja’.

[299] Virolainen 2012: 64, 78. Teoksessa Prosessioikeus.

[300] Rikoksesta johtuvat yksityisoikeudelliset vaatimukset, kuten rikosperusteinen korvausvaatimus ja omaisuuden palauttamisvaatimus, kuuluvat siviiliprosessiin, ei rikosprosessiin. Niin sanotusta adheesioprosessista johtuen voidaan syytteeseen tarkoitettuun rikokseen perustuvat yksityisoikeudelliset vaatimukset käsitellä rikoksesta nostetun syytteen yhteydessä liitännäisvaatimuksina eli rikosjuttuun kumuloituna. Virolainen 2012: 65. Teoksessa Prosessioikeus.

ohjaavasti siten, että rikosten tekemistä voitaisiin ennaltaehkäistä. Rangaistuksilla, kiinnijäämisriskillä ja rikosten selvittämisellä pyritään ehkäisemään ja minimoimaan rikollisuutta. Kyseiset kaksi funktiota eivät ole toisensa poissulkevia vaan toisiaan täydentäviä.[301]

Rikostutkinnassa on käytössä inkvisitorinen menetelmä eli tutkimismenetelmä, sillä kyseessä on nimenomaisesti rikoksen tutkinta ja asian selvittely. Tuolloin valtion viranomaisten tehtävä on huolehtia asian tutkimisesta rikosvastuun toteuttamiseksi. Rikosprosessin myöhäisemmässä vaiheessa on käytössä akkusatorinen menetelmä eli syyttämismenetelmä. Tuolloin syyttäjällä on aktiivinen rooli ja prosessi on syyttäjävetoinen: syyttäjän esittämä syyte (rangaistusvaade) määrittelee oikeudenkäynnin kohteen ja syyttäjä esittää oikeudenkäyntiaineiston. Tuomioistuimella on passiivinen rooli eli se ei osallistu asian selvittämiseen: tuomari ratkaisee asian esitetyn oikeudenkäyntiaineiston perusteella. Syytesidonnaisuus tarkoittaa sitä, että tuomioistuin saa kuitenkin tuomita syytetyn vain siitä teosta, josta rangaistusta on vaadittu. *Jura novit curia* -periaatteen mukaisesti tuomioistuin on velvollinen tuntemaan lain ja soveltamaan sitä viran puolesta omasta aloitteestaan olematta sidottu syytteessä mainittuun rikosnimikkeeseen eikä lainkohtaan, millä perusteella rangaistusta on vaadittu.[302]

Rikostutkintaa sääntelevät keskeisesti esitutkintalaki (ETL 22.7.2011/805) ja pakkokeinolaki (PKL 22.7.2011/806). Nämä kaksi rikostutkintaa koskevaa yleislakia sisältävät keskeiset säännökset esitutkinnasta eli epäillyn rikoksen oikeudellisesta selvittämisestä sekä siinä käytettävistä pakkokeinoista eli viranomaisten suorittamista toimenpiteistä, joilla voidaan puuttua henkilöiden oikeuspiiriin.[303] Rikosten esitutkintaa koskeva yleislaki on esitutkintalaki, joka sisältää säännökset lain soveltamisalasta, esitutkinnan toimittamisvelvollisuudesta, siinä noudatettavista yleisistä periaatteista[304], esitutkintaviranomaisista, tutkinnanjohtajan ja tutkijan esteellisyydestä, saapuvillaolosta esitutkinnasta, kuulusteluista, muista esitutkintatoimenpiteistä, esitutkinta-aineiston tallentamisesta, esitutkinnan päättämisestä sekä suppeasta esitutkinnasta.[305] Esitutkinta-

[301] Virolainen 2012: 65, 78–79. Teoksessa Prosessioikeus.
[302] Niemi 2012: 845 ja Virolainen 2012: 199–200, 208–210. Teoksessa Prosessioikeus.
Laki oikeudenkäynnistä rikosasioissa ROL 11.7.1997/689 11:3 §. Tuomioistuin saa tuomita vain siitä teosta, josta rangaistusta on vaadittu. Tuomioistuin ei ole sidottu rikosnimikkeeseen eikä lainkohtaan, jonka nojalla rangaistusta on vaadittu
[303] Helminen ym. 2014: 6.
[304] ETL 4 luvussa mainitut esitutkintaperiaatteet ovat tasapuolisuusperiaate (ETL 1 §), syyttömyysolettama (ETL 2 §), oikeus olla myötävaikuttamatta rikoksensa selvittämiseen eli niin sanottu itsekriminointisuoja (ETL 3 §), suhteellisuusperiaate (ETL 4 §), vähimmän haitan periaate (ETL 5 §) sekä hienotunteisuusperiaate (ETL 6 §).
[305] HE 222/2010: 12.

lain mukaan esitutkinta on toimitettava ilman aiheetonta viivytystä, vaikkakin esitutkintatoimenpiteet voidaan olosuhteiden sitä edellytettäessä asettaa tärkeysjärjestykseen (ETL 3:11 §).

Rikoksia tutkittaessa niitä tutkivilla viranomaisilla on lailla säädetty oikeus puututtua ihmisten oikeuksiin erilaisin toimenpitein. Näiden niin sanottujen rikosprosessuaalisten pakkokeinojen käyttämistä koskeva yleislaki on pakkokeinolaki. Siinä säädetään rikoksen esitutkinnassa ja joissakin tapauksissa myös sen jälkeen käytettävistä pakkokeinoista eli kiinniottamisesta, pidättämisestä, vangitsemisesta, matkustuskiellosta, hukkaamiskiellosta, vakuustakavarikosta, takavarikosta, etsinnästä (paikkaan kohdistuva etsintä ja henkilöön kohdistuva etsintä) sekä salaisiksi pakkokeinoiksi kutsuttavista telekuuntelusta, televalvonnasta ja matkaviestimien sijaintitiedon hankkimisesta sekä teknisestä tarkkailusta. Pakkokeinolaissa on lisäksi säännöksiä muista pakkokeinoista, joita ovat muun muassa poistumisen estäminen, tutkimuspaikan eristäminen, henkilötuntomerkkien ottaminen sekä DNA-tunnisteiden määrittäminen ja tallettaminen.[306] Esitutkinta- ja pakkokeinolaki tulivat kokonaan uudistettuina voimaan vuoden 2014 alussa[307]. Tällä menettelytapoja koskevalla uudistetulla sääntelyllä pyritään edistämään oikeusturvan sekä perus- ja ihmisoikeuksien toteutumista. Esitutkintaan vaikuttaa myös osaltaan prosessioikeuden alaan kuuluva oikeudenkäynnistä rikosasioissa annettu laki (ROL 11.7.1997/689)[308].

Prosessiekonomia tarkoittaa viranomaisresurssien tarkoituksenmukaista kohdentamista, viranomaistoiminnan tehostamista sekä rikosasioiden esitutkinnan, syyteharkinnan ja tuomioistuimen nopeuttamista turvaten kuitenkin niin rikoksesta epäillyn kuin asianomistajankin oikeudet. Prosessiekonomian kannalta saadaan suurin hyöty silloin, kun resurssit saadaan mahdollisen tehokkaaseen käyttöön jo esitutkinnan aikana. Esitutkinnan tehokkuuden kannalta onkin yleisesti eduksi, jos se voidaan aloittaa mahdollisimman pian rikoksen tekemisen jälkeen. Tällöin on parhaat edellytykset saada näyttöä tapahtuneesta rikoksesta ja esimerkiksi omaisuutta takavarikkoon tuomittavan vahingonkorvauksen turvaamiseksi. On lisäksi oletettavaa, että resursseja vapautuisi myös sellaisten tekojen tutkintaan, jotka saattaisivat jäädä esitutkintaviranomaisilta huomaamatta tai muusta syystä esitutkinnan ulkopuolelle taikka joiden esitutkinta ei olisi ajan kulumisen vuoksi enää todennäköisesti tuloksellista. Tämä olisi rikosoikeudellisen ennaltaehkäisyn eli prevention kannalta suotavaa, koska yleinen näkemys

[306] HE 222/2010: 12.
[307] Lait uudistettiin kokonaan esitutkinta-, pakkokeino- ja poliisilainsäädännön kokonaisuudistuksessa.
[308] Helminen ym. 2014: 6.

on, että preventioon vaikuttaa ensi sijassa kiinnijäämisriksi eikä niinkään seuraamusten ankaruus.[309]

Yleensä ottaen tietotekniikkarikoksia koskeva todistusaineisto on lähes yksinomaan sähköisessä muodossa. Kyseisenlaisen todistusaineiston muuntelu ja hävittäminen on poikkeuksellisen helppoa, miksi tutkintatoimenpiteiden nopeus on ratkaisevassa asemassa.[310] Esitutkinnassa tekijästä (rikoksesta epäillystä) tiedetään tämän tutkielman aiheena olevassa myyntipetoksessa myyjän vertaisverkkokaupassa antamat tiedot eli vähintään käyttäjätunnus ja/tai kaupankäynnissä myyjän käyttämä nimi sekä jokin myyjän käyttämä yhteystieto, yleensä sähköpostiosoite ja/tai puhelinnumero. Jos myyntipetos on tapahtunut Facebookin eri palstoilla kauppaa käydessä, ei petollisesta myyjästä välttämättä ole tiedossa kuin käyttäjäprofiilin nimi, kenen kanssa kaupat on yleensä sovittu Messenger-viestipalvelussa. Ostajan (asianomistajan) tehdessä asiassaan rikosilmoituksen poliisille, hän on jo maksanut ostamastaan tuotteesta kauppasumman, joko kokonaisuudessaan tai osittain, saamatta rahoilleen vastinetta eli ostamaansa tuotetta – muutenhan ostaja ei tekisi asiastaan rikosilmoitusta. Normaalitapauksissa tällöin on tiedossa tekijän tilinumero.

Kuten aiemmin kävi ilmi, erityisesti poliisin ja finanssisektorin välinen yhteistyö tietoverkkorikollisuuteen liittyen on pitkällä. Myös Tori.fi tekee yhteistyötä poliisin kanssa. Poliisilla on kuitenkin myös laaja lakiin perustuva tiedonsaantioikeus. Tästä säädetään poliisilaissa:

PolL 4:2.1 §. Tietojen saanti viranomaiselta.

> *Poliisilla on päällystöön kuuluvan poliisimiehen pyynnöstä oikeus saada viranomaiselta ja julkista tehtävää hoitamaan asetetulta yhteisöltä poliisille kuuluvan tehtävän suorittamiseksi tarpeelliset tiedot ja asiakirjat maksutta ja salassapitovelvollisuuden estämättä, jollei sellaisen tiedon tai asiakirjan antamista poliisille tai tietojen käyttöä todisteena ole laissa nimenomaisesti kielletty tai rajoitettu.*

PolL 4:3.1–2 §. Tietojen saanti yksityiseltä yhteisöltä tai henkilöltä.

> *Poliisilla on päällystöön kuuluvan poliisimiehen pyynnöstä oikeus saada rikoksen estämiseksi tai selvittämiseksi tarvittavia tietoja yhteisön jäsentä, tilintarkastajaa, toimitusjohtajaa, hallituksen jäsentä tai työntekijää velvoittavan yritys-, pankki- tai vakuutussalaisuuden estämättä. Poliisilla on sama oikeus saada 6 luvussa tarkoitetussa poliisitutkinnassa tarvittavia tietoja, jos tärkeä yleinen tai yksityinen etu sitä vaatii.*

[309] HE 58/2013: 12–13.
[310] HE 153/2006: 4.

> *Poliisilla on yksittäistapauksessa oikeus pyynnöstä saada teleyritykseltä ja yhteisötilaajalta yhteystiedot sellaisesta teleosoitteesta, jota ei mainita julkisessa luettelossa, taikka teleosoitteen tai telepäätelaitteen yksilöivät tiedot, jos tiedot ovat tarpeen poliisille kuuluvan tehtävän suorittamiseksi. Poliisilla on vastaava oikeus saada postitoimintaa harjoittavalta yhteisöltä jakeluosoitetietoja.*

Myyntipetoksen esitutkinnassa poliisin olennaisin tehtävä on selvittää heti, kenen tilille petoksella saatu kauppasumma on maksettu. Poliisin pankille tekemässä tiedustelussa tulee selvittää kyseisen tilin tilinomistaja sekä muut käyttöoikeuden haltijat. Lisäksi pankilta pyydetään kyseisen tilin tilitiedot tarpeeksi pitkältä ajanjaksolta rikollisen toiminnan laajuuden selvittämiseksi. Koska petollinen myyjä sopii kaupoista useamman henkilön kanssa, on mahdollista, että kyseisestä myyjästä on jo tehty poliisille rikosilmoitus. Mikäli poliisin järjestelmistä selviää, että sama pankkitilinnumero on mainittu jo jossain muussa rikosilmoituksessa, on selvää, että kyseessä ei ole yksittäistapaus. Tällöin pankkitiedustelussa myös määrätään ”jäädyttämään” kyseinen pankkitili, jolloin tililtä ei saa enää varoja ulos. Tilillä olevat varat takavarikoidaan, jolloin tili ja sen varat erotetaan haltijansa määräysvallasta ja samalla pyritään turvaamaan asianomistajan etu[311]. Takavarikosta ja sen edellytyksistä säädetään pakkokeinolaissa (PKL 7:1 §):

> *Esine, omaisuus tai asiakirja voidaan takavarikoida, jos on syytä olettaa, että:*
> *1) sitä voidaan käyttää todisteena rikosasiassa;*
> *2) se on rikoksella joltakulta viety; tai*
> *3) se tuomitaan menetetyksi.*
>
> *Mitä 1 momentissa säädetään, koskee myös tietoa, joka on teknisessä laitteessa tai muussa vastaavassa tietojärjestelmässä taikka sen tallennusalustalla (data). Tässä luvussa asiakirjasta säädettyä sovelletaan myös datan muodossa olevaan asiakirjaan. (20.5.2016/357)*

Poliisin määräyksestä haltuun otetut eli takavarikoidut varat pitää pystyä yhdistämään tiettyyn asianomistajaan, jolloin omaisuus voidaan myös ”korvamerkitä” asianomistajalle sellaisenaan palautettavaksi; tätä vaihtoehtoa ei ole, mikäli varat otetaan vakuustakavarikkoon (PKL 6 luku): vakuustakavarikossa olevat varat voidaan käyttää velallisen muidenkin ulosottovelkojen maksamiseen ja tällöinkin on otettava huomioon suojaosuus, joka on 22,41 euroa päivässä (672,30 euroa kuukaudessa) velallisen itsensä osalta vuonna 2019[312]. Varojen takavarikoiminen rikoksesta epäillyn pankkitililtä

[311] Helminen ym. 2014: 967–968.

[312] Ulosoton nettisivujen mukaan palkasta, eläkkeestä, työttömyyskorvauksesta ja äitiyspäivärahasta voidaan ulosmitata pääsääntöisesti 1/3. Myös lomarahat, luontoisedut, provisiot ja erilaiset palkkiot ovat palkkatuloa. Sosiaaliavustukset ja -tuet, kuten asumistuki ja lapsilisät eivät ole ulosmittauskelpoisia. Suojaosuudesta määrätään vuosittain laissa kansaneläkkeen ja eräiden muiden etuuksien indeksitarkastuksista.

edellyttää, että takavarikon perusteeseen liittyvä osuus on erotettavissa muista tilillä olevista varoista. Lisäksi tilinomistajan on saatava käyttöönsä tilille tulleet mahdolliset etuudet ja korvaukset. Jos pankkitilillä on useammalta eri asianomistajalta peräisin olevia varoja, on selvitettävä pankilta, missä järjestyksessä varat ovat pankkitilille tulleet, jotta ne voidaan palauttaa oikealle omistajalleen.[313]

Tilinomistajan tiliin liitettyjen verkkopankkitunnuksien takavarikoinnilla estetään se, ettei rikoksesta epäilty pääse avaamaan niillä uusia pankkitilejä. Petoksella varat saanut henkilö saadaan todennäköisesti ottamaan yhteyttä pankkiin, jonne poliisin on syytä ilmoittaa esitutkintaa hoitavan poliisin yhteystiedot. Rahan tarpeessa myyntipetoksia tekevä rikoksesta epäilty haluaa saada tilinsä ja sillä olevat varat itselleen. Näin toimien hänet motivoidaan tulemaan poliisilaitokselle selvittämään asiaa, jolloin säästetään aikaa: ei ole tarpeen ensin kutsua rikoksesta epäiltyä esitutkintaan ja mahdollisesti noutaa epäilty poliisilaitokselle hänen jätettyä kutsun noudattamatta (ETL 6:1 ja 6:2 §) ja samalla myös vältytään tekemästä kuulusteluun noutoa varten yleinen kotietsintä henkilön löytämiseksi (PKL 8:3 §). Pankkia pyydetään tekemään pankkitiedustelussa määrätyt toimenpiteet pikimmiten, samoin toimittamaan poliisille siinä pyydetyt tarkemmat tiedot. Myyntipetoksessa käytetyn tilin tiliotteelta selviää suoraa rikoksen laajuus: tilillä näkyy kaikkien petoksellisen myyjän kanssa kauppaa tehneiden maksusuoritukset. Maksajien nimitietojen perusteella selviää, mitkä jo poliisille tehdyt rikosilmoitukset liittyvät samaan kokonaisuuteen.

Tiliotteen tietojen perusteella poliisi saa selville muut mahdolliset asianomistajat. Yksittäisen asianomistajan osalta petoksella saatu kauppasumma on normaalisti alle 500 euroa, jolloin tekona on kysymyksessä lievä petos (RL 36:3 §). Se on niin sanottu asianomistajarikos: syyttäjä ei saa nostaa syytettä lievästä petoksesta, ellei asianomistaja ilmoita sitä syytteeseen pantavaksi (RL 36:8 §). Asianomistajarikoksen esitutkinta voidaan suorittaa tai aloittaa ilman syytepyyntöä, jos asianomistaja ei syystä tai toisesta tiedä rikoksen tapahtuneen eikä tutkintaa voida sen onnistumista vaarantamatta lykätä.[314] Poliisi voi siis suorittaa esitutkintaa myös niiden asianomistajien osalta, joiden henkilöllisyys ei vielä ole selvillä, jotka eivät mahdollisesti tiedä tulleensa petetyiksi tai jotka eivät ole tehneet asiassaan rikosilmoitusta.

Rikoksen forumsääntelystä eli tekopaikan määrittelemisestä on säännökset rikoslaissa (RL 10.1 §): rikos katsotaan tehdyksi sekä siellä, missä rikollinen teko suoritettiin, että

[313] Helminen ym. 2014: 968.
[314] Niemi 2012: 854. Teoksessa Prosessioikeus.

siellä, missä rikoksen tunnusmerkistön mukainen seuraus ilmeni.[315] Petoksessa tekopaikka on sekä se paikka, josta tekijä antaa erehdyttävän tiedon, että se paikka, jossa taloudellinen vahinko ilmenee. Poliisin hallinnosta annetun lain (PolHalL 15c §) mukaisia alueperiaatesäännöksiä poliisimiehen toimialueesta ja toimivelvollisuudesta noudatetaan myös esitutkinnassa ilmoituksen vastaanottovaiheesta alkaen. Poliisimies on ilman eri määräystä velvollinen ryhtymään kiireellisiin toimiin koko maassa myös toimialueensa ulkopuolella ja vapaa-aikanaan, jos se on välttämätöntä vakavan rikoksen estämiseksi, tällaista rikosta koskevan tutkinnan aloittamiseksi tai yleistä järjestystä ja turvallisuutta (YTJ) uhkaavan vaaran torjumiseksi taikka jos se näihin rinnastettavan muun erityisen syyn vuoksi on tarpeen. Ellei erikseen ole toisin määrätty, tutkintavastuu on sillä poliisilaitoksella, jonka alueella rikos on tapahtunut.[316]

Myyntipetos tulee yleensä kuitenkin ilmi asianomistajan ilmoittaessa asiasta kotipaikkansa poliisille. Tapahtuneesta kirjataan rikosilmoitus ja tekopaikaksi kirjataan toissijainen tekopaikka eli paikka, jossa rikoksen seuraus ilmeni (asianomistajan kotipaikka). Rikosilmoituksen esitutkinnasta vastaa kyseinen poliisilaitos. Jos kuitenkin rikosilmoitusta kirjatessa poliisin järjestelmistä selvitetään ja selviää, että vastaavista tapauksista on jo kirjattu rikosilmoituksia ja niistä käy ilmi rikoksesta epäilty sekä hänen kotipaikkansa, kirjataan rikoksen tekopaikaksi rikollisen teon suorituspaikka eli rikoksesta epäillyn kotipaikka ja rikosilmoitus tulee tutkittavaksi kyseisessä poliisilaitoksessa. Tällaisessa tapauksessa asianomistajalta on tutkinnan joutuisuuden vuoksi syytä ottaa välittömästi asianomistajakuulustelu, selvittää hänen vaatimuksensa sekä saada tarvittava todistusaineisto esitutkintamateriaalin liitteeksi; tämä on syytä tehdä silloinkin, kun rikosilmoitus kirjataan vieraan poliisilaitoksen tutkittavaksi – siitä huolimatta, että rikosten esitutkinta suoritetaan alueperiaatteen mukaisesti.

Kun tutkittavana on useita saman tekijän myyntipetoksia sisältävä kokonaisuus, on vahva presumtio, että yhden ja saman henkilön kaikki rikokset käsitellään samassa oikeudenkäyntitilaisuudessa[317]. Tämä liittyy rangaistuksen mittaamiseen: tuomioistuimen on paljon helpompi mitata vastaajalle oikeudenmukainen rangaistus, kun sillä on ”käytössään” kaikki hänen tekemäksi katsotut rikokset tuomioistuimen tuomitessa yhteistä rangaistusta (RL 7 luvun Rikoksien yhtymisestä kirjoitettujen säännösten)

[315] Frände 2012: 390. Teoksessa Prosessioikeus.
[316] Helminen ym. 2014: 291.
[317] Rikosyhteyteen perustuvien oikeuspaikkojen sääntely (ROL 4:3–5 §) koskee tapauksia, joissa tuomioistuimessa tutkitaan syytteet useammasta kuin yhdestä rikoksesta. Kysymys voi olla subjektiivisesta rikosyhteydestä (sama henkilö on tehnyt useita rikoksia, ks. ROL 5:18.1 §) tai objektiivisesta rikosyhteydestä (saman rikoksen tekemiseen on osallistunut useampi henkilö). Frände 2012: 392.

perusteella.[318] Esitutkintalaissa säädetään esitutkintaviranomaisen ja syyttäjän esitutkintayhteistyöstä (ETL 5 luku). Valtakunnansyyttäjänviraston ohjeen (VKS:2013:4) mukaisista rikosasioista on ilmoitettava syyttäjälle: Poliisin on ilmoitettava syyttäjälle tutkittavaksi tulleesta rikoksesta muun muassa silloin, kun tutkittava rikoskokonaisuus sisältää lukuisia eri asianomistajiin kohdistuneita tekoja tai useita eri tekijöitä (esim. omaisuus- tai petosrikossarjat); niiden yhdessä käsittely syyteharkinnassa ja tuomioistuimessa edistää asian selvittämistä.[319] Poliisi ja syyttäjän tulee neuvotella esitutkintayhteistyön järjestämiseen liittyvistä kysymyksistä (ETL 5:3.3 §), jolloin tulee myös sovittavaksi myyntipetosten forum eli tutkintapaikka, jolloin rikoskokonaisuuteen liittyvien rikosilmoitusten tutkinta keskitetään tietylle poliisilaitokselle.

Esitutkinnassa on kyse rikosasian valmistelusta syyteharkintaan ja rikosoikeudenkäyntiin. Laki (ETL 1:2 §) velvoittaa selvittämään esitutkinnassa seuraavat asiat::

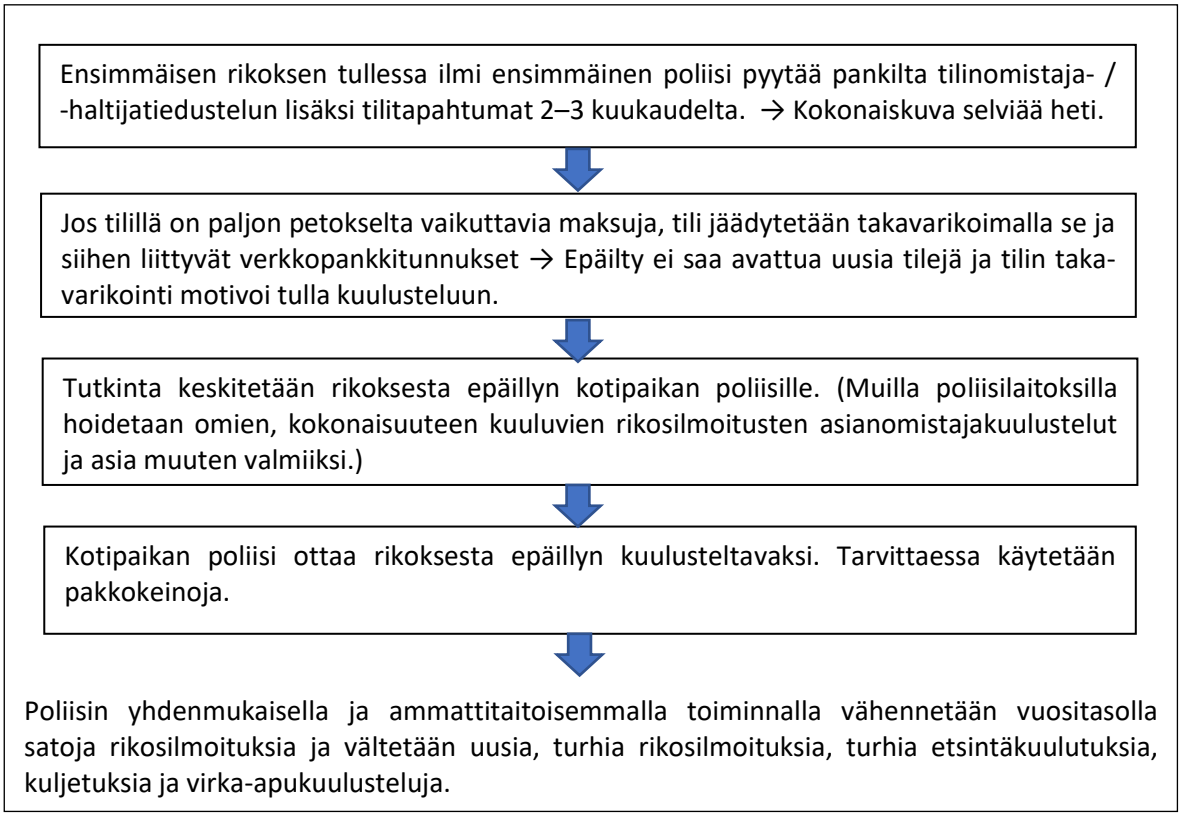
> *1) asian laadun edellyttämällä tavalla epäilty rikos, sen teko-olosuhteet, sillä aiheutettu vahinko ja siitä saatu hyöty, asianosaiset sekä muut syyteharkintaa ja rikoksen johdosta määrättävää seuraamusta varten tarvittavat seikat;*
>
> *2) mahdollisuudet rikoksella saadun omaisuuden palauttamiseksi ja rikoksen johdosta tuomittavan menettämisseuraamuksen tai asianomistajalle tulevan vahingonkorvauksen täytäntöönpanemiseksi;*
>
> *3) asianomistajan yksityisoikeudellinen vaatimus, jos hän oikeudenkäynnistä rikosasioissa annetun lain (689/1997) 3 luvun 9 §:n nojalla on pyytänyt syyttäjää ajamaan hänen vaatimustaan; ja*
>
> *4) suostuuko asianomistaja ja aikooko rikoksesta epäilty suostua asian käsittelemiseen käräjäoikeudessa oikeudenkäynnistä rikosasioissa annetun lain 5 a luvussa tarkoitetussa kirjallisessa menettelyssä.*

Asia on valmisteltava esitutkinnassa siten, että syyteharkinta ja asianosaisten etujen valvominen voidaan suorittaa asianmukaisesti ja että todistelu voidaan pääkäsittelyssä ottaa vastaan yhdellä kertaa tai asia voidaan ratkaista kirjallisessa menettelyssä (ETL 1:2.2 §). Rikosasia on ollut mahdollista ratkaista pääkäsittelyä toimittamatta niin sanotussa kirjallisessa menettelyssä vuodesta 2006 alkaen, jos mistään syyttäjän syytteessä tarkoitetusta yksittäisestä teosta ei ole säädetty ankarampaa rangaistusta kuin sakko tai vankeutta enintään kaksi vuotta, tekohetkellä täysi-ikäinen vastaaja tunnustaa teon ja sekä vastaaja että asianomistaja suostuvat asian käsittelyyn kirjallisessa menettelyssä eikä pääkäsittelyn toimittaminen ole myöskään kokonaisuutena arvioiden

[318] Frände 2012: 573. Teoksessa Prosessioikeus.
[319] Niemi 2012: 851. Teoksessa Prosessioikeus.

tarpeellista. Kirjallisessa menettelyssä ei voida tuomita rangaistukseksi ankarampaa rangaistusta kuin yhdeksän kuukautta vankeutta. (ROL 5a:1 §.)

Poliisi kehittää aktiivisesti omaa toimintaansa tehostaakseen myyntipetosten selvittämistä. Koska yksi ja sama petollinen myyjä syyllistyy useampaan myynti-petokseen lyhyen ajan sisällä, on olennaista selvittää tutkittavana olevan rikoksen kokonaiskuva heti pyytämällä myyntipetoksessa käytetyn tilin tiliotteet riittävän pitkältä ajanjaksolta. Kun rikollisen toiminnan laajuus on selvinnyt, poliisi tekee päätöksen tilin sulkemisesta uusien petosrikosten ehkäisemiseksi.[320] Keskittämällä myyntipetosten esitutkinta vältetään se tilanne, että saman rikoksesta epäillyn tekemiä myyntipetoksia käsiteltäisiin yksittäisinä tekoina, mikä ei ole myöskään petollisen myyjän etu tulevan rangaistuksen mittaamista ajatellen. Poliisin kehittämää uudistettua toimintamallia myyntipetoksiin puuttumiseksi on kuvattu oheisessa kuviossa:



Kuvio 3. Poliisin uudistettu toimintamalli myyntipetoksiin puuttumiseksi. (Oikeus-ministeriö 2017: 43).

[320] Oikeusministeriö 2017: 24.

5. JOHTOPÄÄTÖKSET

Ensin poliisilla oli tutkittavana yksi yksittäinen internetin markkinapaikalla tapahtunut myyntipetos, joka täytti lievän petoksen tunnusmerkistön. Kyseinen rikos oli kuitenkin osa laajempaa petoskokonaisuutta, sillä tietoverkkokympäristössä on samalla myynnissä olevalla tuotteella lukuisia ostajia, jotka toisistaan tietämättä tekevät siitä myyjän kanssa kaupat. Kauppasumma maksetaan näppärästi myyjän ilmoittamalle tilille verkkopankissa ja myyjä saa petoksella hankkimansa varat käyttöönsä samoin tein, minkä jälkeen myyjään ei enää saakaan yhteyttä. Myyjä on kadonnut – muttei sentään bittiavaruuteen. Rikoksia tutkivalla poliisilla on käytettävissään lain mahdollistamat keinot saada petollisen myyjän henkilöllisyys selville. Myyntipetoksissa yhteistyö pankin kanssa korostuu ja se toimiikin käytännössä hyvin. Yhteistyössä pankin kanssa on mahdollista lopettaa akuutissa rahantarpeessa olevan myyntipetosten tekijän petoskierre.

Esitutkinnasta vastaavan poliisin pitää tiedostaa, että kysymyksessä on tuskin koskaan yksittäinen teko. Se ei myöskään saa ajatella vain oman poliisilaitoksensa tutkinnassa olevia rikosilmoituksia pitäen tiukasti kiinni alueperiaatteesta vaan on nähtävä laajempi kokonaisuus. Hyväksi havaitulla ja tämänkin tutkielman lopuksi esitetyllä toimintamallilla sekä poliisilaitosten välisellä yhteistyöllä laajatkin nettipetoskokonaisuudet saadaan nopeasti selville. Lisäksi petoksella hankittu omaisuus on mahdollista saada pikimmiten takavarikkoon ja palautetuksi oikealle omistajalleen. Myös rikoksesta epäillyn tavoitteluun menevä aika minimoituu, kun hänet motivoidaan ottamaan itse yhteyttä pankkiin ja edelleen poliisiin. Esitutkinnan keskittämisellä saadaan petollisen myyjän kaikki rikokset yhdellä kertaa syyttäjälle syyteharkintaan siten, että rikoksesta epäillyn / syytetyn / tuomitun teostaan saama rangaistus on oikeudenmukainen. Uusi toimintamalli mahdollistaa myös sen, ettei vain osa tapauksista tule tutkituksi ja että ne kaikki tulee käsitellyksi samalla tavoin.

Tietoteknisen kehityksen myötä useimmat kaupalliset toimijat (pankit ensimmäisten joukossa) ovat siirtyneet tietoverkkoihin, mutta siellä ovat myös valtionhallinto ja julkiset palvelut – sähköisessä muodossa; henkilökohtainen asiointi on kaikkinensa on vähentynyt huomattavasti ja se vähenee edelleen. Kivijalkakaupat huventuvat ja verkkokauppa helppoudellaan kukoistaa. Yhä useammat yhteiskuntamme toiminnoista ja peruspalveluista ovat nykyään riippuvaisia tietoteknisistä järjestelmistä. Lisäksi useat näistä järjestelmistä ovat toisistaan keskenään riippuvaisia. Tämä kybertoimintaympäristöksi kutsuttu kokonaisuus verkottuu yli valtioiden rajojen ja on erittäin haavoittuvainen: kyber- eli tietoturvauhkat toteutuessaan vaarantavat tietojärjestelmän

ja siten koko niistä muodostuvan maailmanlaajuisen verkoston toiminnan. Uhkat ovat globaaleja ja niiden torjuminen on tehtävä yhteistyössä muiden valtioiden kanssa. Yksittäinen valtio ei voi omilla toimillaan näitä uhkia torjua ja nujertaa.

Kyberturvallisuus käsittää koko sähköisen toimintaympäristön turvallisuuden. Se siten sisältää tietoturvallisuuden, jolla pyritään varmistamaan sähköisessä muodossa olevan tiedon eli datan käytettävyys, eheys ja luottamuksellisuus. Tutkielman lähtökohtana olevaa petoskokonaisuutta tarkastellessa tuli selkeästi ilmi, että tietoturvallisuus on olennainen osa digitaalisen toimintaympäristön verkkoyhteiskuntaa. Vuoden 2011 suuret tietovuodot havahduttivat verkossa toimivat yritykset tietoturvan tärkeyteen. Tietovuodot ja niitä seurannut Huuto.net-petoskokonaisuus uutisoitiin laajasti valtakunnanmediassa, jolloin asia tuli myös kansalaisten tietoisuuteen. Yritykset ovat parantaneet tietoturvaansa ja yksityishenkilöt ovat valveutuneempia netissä toimiessaan.

Rikollisuutta on myös tietoverkoissa, missä asiat tapahtuvat nopeasti. Kaikkien tietotekniikkarikosten esitutkinnassa nopeus on ratkaiseva tekijä, niin myös tämänkin tutkielman aiheena olevien myyntipetosten tutkinnassa. Poliisin tulee priorisoida mitättömältäkin vaikuttavan lievän petoksen tutkinta, kun kysymyksessä on internetin kauppapaikalla tapahtunut myyntipetos. Tärkeänä alkutoimenpiteenä esitutkintaa suorittavan poliisin tulee selvittää tili, jolle kauppasumma on maksettu, minkä jälkeen otetaan pikimmiten yhteys pankkiin rikollisen toiminnan laajuden selvittämiseksi. Huuto.net-sivustoilla ei tapahdu käytännössä petoksia enää lainkaan. Vaikka Tori tekee yhteistyötä poliisin kanssa ja auttaa petollisten toimijoiden selvittämistä, olisi käyttäjien rekisteröitymisen vaatiminen huomattavasti tehokkaampi keino vähentää Tori.fi-sivustoilla tapahtunutta rikollista toimintaa. Mutta niin kauan kun hyvä ja haluttu tuote on saatavissa halvalla, osa suomalaisista on valmis sen ostamaan. Myyntipetokset eivät tule koskaan loppumaan kokonaan.

LÄHDELUETTELO

VIRALLISLÄHTEET

HaVL 5/2001. Valtioneuvoston selvitys komission tiedonannosta "Turvallisempaan tietoyhteiskuntaan tietojärjestelmien turvallisuutta parantamalla ja tietokonerikollisuutta ehkäisemällä".

HE 66/1988 vp. Hallituksen esitys Eduskunnalle rikoslainsäädännön kokonaisuudistuksen ensimmäisen vaiheen käsittäväksi rikoslain ja eräiden muiden lakien muutoksiksi.

HE 94/1993 vp. Hallituksen esitys Eduskunnalle rikoslainsäädännön kokonaisuudistuksen toisen vaiheen käsittäviksi rikoslain ja eräiden muiden lakien muutoksiksi.

HE 233/1997 vp. Hallituksen esitys Eduskunnalle laiksi rikoslain muuttamisesta.

HE 2/2003 vp. Hallituksen esitys Eduskunnalle laiksi rikoslain 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 277/2010 vp. Hallituksen esitys Eduskunnalle laiksi rikoslain 28 luvun 7 §:n muuttamisesta.

HE 317/2010 vp. Hallituksen esitys Eduskunnalle Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen lisäpöytäkirjan, joka koskee tieto-

järjestelmien välityksellä tehtyjen luonteeltaan rasististen ja muukalaisvihamielisten tekojen kriminalisointia, hyväksymisestä ja laiksi sen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta sekä laeiksi rikoslain ja tietoyhteiskunnan palvelujen tarjoamisesta annetun lain 15 §:n muuttamisesta.

HE 58/2013 vp. Hallituksen esitys eduskunnalle syyteneuvottelua koskevaksi lainsäädännöksi ja syyttämättä jättämistä koskevien säännösten uudistamiseksi.

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

HE 263/2014 vp. Hallituksen esitys eduskunnalle laiksi rikoslain järjestäytyneitä rikollisryhmiä koskevien säännösten yhtenäistämiseksi.

HE 192/2017. Hallituksen esitys eduskunnalle laeiksi Euroopan unionin verkko- ja tietoturvadirektiivin täytäntöönpanoon liittyvien lakien muuttamisesta.

HE 60/2018: Hallituksen esitys eduskunnalle laeiksi digitaalisten palvelujen tarjoamisesta sekä sähköisestä asioinnista viranomaistoiminnassa annetun lain muuttamisesta.

VNS 5/2016 vp. Valtioneuvoston selonteko sisäisestä turvallisuudesta.

KIRJALLISUUS

Aarnio, Aulis (2006). Tulkinnan taito – ajatuksia oikeudesta, oikeustieteestä ja yhteiskunnasta. Helsinki: WSOY.

Frände, Dan & Erkki Havansi, Dan Helenius, Risto Koulu, Juha Lappalainen, Heidi Lindfors, Johanna Niemi, Jaakko Rautio, Jyrki Virolainen (2012). Prosessioikeus. 4. uud. painos. Helsinki: Sanoma Pro.

Hirvonen, Ari (2011). Mitkä metodit? Opas oikeustieteen metodologiaan. Yleisen oikeustieteen julkaisuja 17. Saatavilla: https://issuu.com/arihirvonen/docs/mitk___metodit_paino

Kiikeri, Mika & Petri Ylikoski (2011). Tiede tutkimuskohteena. Filosofinen johdatus tieteentutkimukseen. 3. painos. Helsinki University Press.

Lehto, Martti, Jarno Limnéll, Tuomas Kokkomäki, Jouni Pöyhönen & Mirva Salminen (2018). Kyberturvallisuuden strateginen johtaminen Suomessa 2018. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 28/2018. Valtioneuvoston kanslia, 29.3.2018. Saatavilla: http://urn.fi/URN:ISBN:978-952-287-532-7

Lehtonen, Anniina (2016). Nettipetosten kasvu 2010-luvulla. Nettipetokset selityksenä petosten kokonaismäärän kasvulle? Poliisiammattikorkeakoulun opinnäytetyö / AMK. Saatavilla: https://www.theseus.fi/bitstream/handle/10024/119318/Lehtonen_Annina.pdf?sequence=1&isAllowed=y

Lehtonen, Asko (2016): Digitalisaation edistäminen tietoturvalainsäädännön avulla. Teoksessa Society trapped in the network: does it have a future? Lapin yliopisto. Saatavilla: http://urn.fi/URN:ISBN:978–952–484–917–3

Lehtonen, Asko (2018). Tietotekniikkaoikeus. Informaatio- ja tietotekniikkaoikeus (ICT-rätt). Luentokalvot 2018.

Leppänen, Anna, Karl Linderborg & Jarkko Saarimäki (2016). Tietoverkkorikollisuuden tilannekuva. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 17/2016. Valtioneuvoston kanslia, 19.4.2016. Saatavilla: http://tietokayttoon.fi/documents/10616/2009122/17_Tietoverkkorikollisuuden+tilannekuva.pdf/6ef911d2-cbe8-43bd-aafa-e10ed573f28a?version=1.0

Helminen, Klaus & Markku Fredman, Janne Kanerva, Matti Tolvanen, Marko Viitanen (2014). Esitutkinta ja pakkokeinot. 5., uudistettu painos. Helsinki: Talentum.

Saarenpää, Ahti (2016). Oikeusinformatiikka. Teoksessa: Oikeus tänään. Osa I, sivut 17-223. Toim. Marja-Leena Niemi. Neljäs uudistettu painos. Lapin yliopiston oikeustieteellisiä julkaisuja C 64. Rovaniemi: Lapin yliopisto.

Siltala, Raimo (2001). Johdatus oikeusteoriaan. Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisut.

Tapani, Jussi & Matti Tolvanen (2013): Rikosoikeuden yleinen osa. Vastuuoppi. Toinen, uudistettu painos. Talentum.

MUUT LÄHTEET

Cisco (2018). Annual Cybersecurity Report. Saatavilla: https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/acr2018/acr2018final.pdf?dtid=odicdc000016&ccid=cc000160&oid=anrsc005679&ecid=8196&elqTrackId=686210143d34494fa27ff73da9690a5b&elqaid=9452&elqat=2

Cisco (2019). Cisco Visual Networking Index: Forecast and Trends, 2017–2022. Saatavilla: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.pdf

Euroopan yhteistöjen komissio (2003): Komission tiedonanto neuvostolle, Euroopan parlamentille, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle – Kohti maailmanlaajuista kumppanuutta tietoyhteiskunnan alalla: EU:n näkökulma Yhdistyneiden kansakuntien tietoyhteiskuntahuippukokoukseen (WSIS). KOM(2003) 271.

Euroopan yhteisöjen komissio (2007). Tavoitteena yleinen toimintalinja tietoverkko-rikollisuuden torjumiseksi. Komission tiedonanto neuvostolle, Euroopan parlamentille ja alueiden komitealle KOM(2007) 267. 22.5.2007. Saatavilla: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:FI:HTML

Euroopan yhteisöjen komissio (2013). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. JOIN(2013) 1 final. 7.2.2013. Saatavilla: https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

Euroopan komissio (2017). Cybersecurity. State of the Union 2017. Euroopan komission kyberturvallisuustiedote. Saatavilla: https://www.consilium.europa.eu/media/21480/cybersecurityfactsheet.pdf

Helsingin Sanomat 3.12.2011. Tietovuotojen sarja sai jatkoa: 16 000 tunnusta ja salasanaa julki. Teksti: Juhani Saarinen. Saatavilla: https://www.hs.fi/kotimaa/art-2000002512882.html

Helsingin Sanomat 23.9.2014. Nettipetosten ennätysmies tuomittiin yli 300 uudesta rikoksesta. Teksti: Lasse Kerkelä. Saatavilla (tilaajille): https://www.hs.fi/kotimaa/art-2000002763654.html

IOCTA (2018). Internet Organised Crime Threat Assessment 2018. Europol. Saatavilla: https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018

ITU (2015). Global Cybersecurity Index & Cyberwellness Profiles. Iternational Telecommunications Union, April 2015. Saatavilla: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf

ITU (2017). Global Cybersecurity Index 2017. International Telecommunication Union. Saatavilla: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

ITU (2018). Global Cybersecurity Index 2018. International Telecommunication Union. Saatavilla: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf

Kaupan liitto 24.11.2015. Ensimmäinen vertaisverkkokauppaselvitys julkaistu. (*Linkki vertaisverkkokauppatutkimuksen laajaan aineistoon on sivustolla*). Saatavilla: https://kauppa.fi/jaesenille/tilastot_ja_tutkimukset/ensimmainen_vertaisverkkokauppaselvitys_julkaistu_25321

Kauppalehti 29.8.2012.. Nettihuutokauppa tehostaa valvontaa. Saatavilla: https://www.kauppalehti.fi/uutiset/nettihuutokauppa-tehostaa-valvontaa/b3c3fecb-c844-39a6-addb-926384a7c49b

Kodin kyberopas (2017). Ohjeita digitaaliseen arkeen. Helsinki: Turvallisuuskomitean sihteeristö. Saatavilla: https://turvallisuuskomitea.fi/wp-content/uploads/2017/04/Kodin_kyberopas_TK_2017_verkkojulkaisu.pdf

Komission tiedonanto 8.12.1999. e-Europe – Tietoyhteiskunta kaikille. Saatavilla: http://eur-lex.europa.eu/legal-content/FI/TXT/HTML/ ?uri=LEGISSUM:l24221&from=EN

LVM (2009). Valtioneuvoston periaatepäätös kansalliseksi tietoturvastrategiaksi. Liikenne- ja viestintäministeriön julkaisuja 62/2008. Saatavilla: http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/78296/Valtioneuvoston_periaatepäätös_kansalliseksi_tietoturvastrategiaksi_%28su-ru-eng_LVM62-2008%29.pdf?sequence=1&isAllowed=y

Mikro-PC 8.12.2011. Näin tapahtui Suomen suurin tietovuoto. Teksti: Ossi Jääskeläinen. Saatavilla: http://mikropc.net/nettilehti/pdf/0812201120.pdf

MTV3 10.3.2019. Nettikirpputorien huijareita on vaikea tunnistaa, poliisille tuhansia rikosilmoituksia vuosittain: "Huijarit pyrkivät luomaan paniikin ostajalle". Saatavilla: https://www.mtvuutiset.fi/artikkeli/nettikirpputorien-huijareita-on-vaikea-tunnistaa-poliisille-tuhansia-rikosilmoituksia-vuosittain-huijarit-pyrkivat-luomaan-paniikin-ostajalle/7270768#gs.0vpp33

Oikeusministeriö (2017). Petosrikollisuus ja sen ehkäisy. Rikoksentorjuntakatsaus 2017. Oikeusministeriön julkaisu 58/2017. Saatavilla: http://urn.fi/URN:ISBN:978-952-259-659-8

Poliisi 29.3.2019. Järjestäytyneen rikollisuuden uhka kasvaa Euroopassa – Uudet kansainväliset rikollisjengit laajentaneet toimintaansa Suomeen. Saatavilla: https://www.poliisi.fi/uutiskaruselli/1/0/jarjestaytyneen_rikollisuuden_uhka_kasvaa_euroopassa_uudet_kansainvaliset_rikollisjengit_laajentaneet_toimintaansa_suomeen_79347

Poliisihallitus (2015a). Poliisin toiminta- ja taloussuunnitelma 2016 - 2019 ja tulos-suunnitelma 2015. 9.3.2015. POL-201S-3384. Saatavilla: https://www.poliisi.fi/instancedata/prime_product_julkaisu/intermin/embeds/poliisiwwwstructure/30223_Poliisin_toiminta-_ja_taloussuunnitelma_2016-2019_ja_tulossuunnitelma_2015_2.pdf?eaabcab3d384d588

Poliisihallitus (2015b). Esitys poliisin kybertoimivaltuuksien muutostarpeista. Työryhmän loppuraportti 27.5.2015. POL-2015-3879. Poliisihallinnon toimintaa ohjaava asiakirja.

Poliisihallitus (2017). Selvitys 1.9.2016−31.12.2017 Itä-Uudenmaan poliisilaitokselle kirjatuista petosrikoksista, joissa asianomistajana luonnollinen henkilö. Ei julkinen.

Poliisin toimintaympäristö (2018). Poliisiammattikorkeakoulun katsaus. Toim. Vesa Muttilainen & Vesa Huotari. Poliisiammattikorkeakoulun raportteja 132. Saatavilla: https://www.theseus.fi/bitstream/handle/10024/155638/POLAMK%20Rap%20132_web.pdf?sequence=1&isAllowed=y

Puolustusministeriö (2013). Suomen kyberturvallisuusstrategia valmis. Tiedote 24.1.2013. Saatavilla: https://www.defmin.fi/ajankohtaista/tiedotteet/ 2013?5730_m=5368

Sanoma 28.4.2014. Huuto.net täytti 15 vuotta – Suomen suurimmassa vertaiskaupassa on ollut kaupan yli 300 miljoonaa kohdetta. Lehdistötiedote. Saatavilla: https://sanoma.com/fi/tiedote/huuto-net-taytti-15-vuotta-suomen-suurimmassa-vertaiskaupassa-on-ollut-kaupan-yli-300-miljoonaa-kohdetta/

Sisäisen turvallisuuden ohjelma (2004). Arjen turvaa – Sisäisen turvallisuuden ohjelma. Valtioneuvoston yleisistunto 23.9.2004. Sisäasianministeriön julkaisuja 44/2004.

Sisäisen turvallisuuden ohjelma (2008). Turvallinen elämä jokaiselle – Sisäisen turvallisuuden ohjelma. Valtioneuvoston yleisistunto 8.5.2008. Sisäasianministeriön julkaisuja 16/2008. Saatavilla: https://api.hankeikkuna.fi/asiakirjat/f7385955-ffc4-4d20-b4d7-84d7a48d5a70/6486ca5d-2f4c-4959-9f61-857d2ee15561/JULKAISU_20080708072751.pdf

Sisäisen turvallisuuden ohjelma (2012). Turvallisempi huomen. Valtioneuvoston periaatepäätös 14.6.2012. Sisäasiainministeriön julkaisusarja 26/2012. Saatavilla: http://urn.fi/URN:ISBN:978-952-491-761-2.

Sisäministeriö (2017a). Hyvä elämä – turvallinen arki. Valtioneuvoston periaatepäätös sisäisen turvallisuuden strategiasta 5.10.2017. Sisäministeriön julkaisu 15/2017. Saatavilla: http://urn.fi/URN:ISBN:978-952-324-138-1

Sisäministeriö (2017b). Tietoverkkorikollisuuden torjuntaa koskeva selvitys. Sisäministeriön julkaisu 14/2017. Saatavilla: http://urn.fi/URN:ISBN:978-952-324-136-7

Suomen kyberturvallisuusstrategia (2013). Valtioneuvoston periaatepäätös 24.1.2013. Helsinki: Turvallisuuskomitean sihteeristö. Saatavilla: https://turvallisuuskomitea.fi/wp-content/uploads/2018/05/Suomen-kyberturvallisuusstrategia-ja-taustamuistio.pdf

Tietosuojaryhmä (2001): Lausunto 4/2001 tietoverkkorikollisuutta koskevasta Euroopan neuvoston yleissopimusluonnoksesta. 5001/01/FI/lopullinen. WP 41. Saatavilla: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp41fi.pdf

Tilastokeskus 16.3.2018. Suomen virallinen tilasto. Rikos- ja pakkokeinotilasto. Viranomaisten tietoon tullut rikollisuus 2017, 4. vuosineljännes. Saatavilla: http://www.stat.fi/til/rpk/2017/04/rpk_2017_04_2018-03-16_fi.pdf

Tilastokeskus 4.12.2018. Suomen virallinen tilasto. Väestön tieto- ja viestintätekniikan käyttö. 1. Suomalaisten internetin käyttö 2018 – viestintää, asiointia, tiedonhakua ja medioiden seuraamista. Saatavilla: https://www.tilastokeskus.fi/til/sutivi/2018/sutivi_2018_2018-12-04_kat_001_fi.html

Tilastokeskus 17.1.2019. Suomen virallinen tilasto. Rikos- ja pakkokeinotilasto. Viranomaisten tietoon tullut rikollisuus 2018, 4. vuosineljännes. Saatavilla: http://www.stat.fi/til/rpk/2018/04/rpk_2018_04_2019-01-17_fi.pdf

Tilastokeskus 17.4.2019. Suomen virallinen tilasto. Rikos- ja pakkokeinotilasto. Viranomaisten tietoon tullut rikollisuus 2019, 1. vuosineljännes. Saatavilla: http://www.stat.fi/til/rpk/2019/01/rpk_2019_01_2019-04-17_fi.pdf

Turvallisuuskomitea (2015). Turvallinen Suomi – Tietoja Suomen kokonaisturvallisuudesta 2015. Turvallisuuskomitean julkaisu. Saatavilla:

https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/Turvallinen-Suomi-_-2015.pdf

Turvallisuuskomitea (2017). Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017 – 2020. Saatavilla: https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/Toimeenpano-ohjelma-2017-2020-final.pdf

Turvallisuuskomitea (2018). Turvallinen Suomi 2018. Tietoja Suomen kokonaisturvallisuudesta. Turvallisuuskomitean julkaisu. Saatavilla: https://turvallisuuskomitea.fi/wp-content/uploads/2018/01/Turvallinen_Suomi_2018.pdf

Turvallisuuskomitean tiedote 18.5.2018. Tuore vertailu nostaa Suomen kyberturvallisuuden kansainväliseen kärkeen. Saatavilla: https://turvallisuuskomitea.fi/tag/kyber/

Turvallisuuskomitean tiedote 6.3.2019. Suomen kyberturvallisuusstrategia 2019 lausuntokierrokselle. Saatavilla: https://turvallisuuskomitea.fi/tiedote-suomen-kyberturvallisuusstrategia-2019-lausuntokierrokselle/

Valtioneuvoston kanslia (2003a). Pääministeri Paavo Lipposen II hallituksen ohjelman seurantaraportti. Valtioneuvoston kanslian raportteja 2003/1. Saatavilla: https://vnk.fi/documents/10616/622934/R0103_Pääministeri+Lipposen+2.+hallituksen+ohjelman+seurantaraportti.pdf/38ff88f5-e6ce-438f-8105-7a18b887d181?version=1.0

Valtioneuvoston kanslia (2003b). Pääministeri Matti Vanhasen hallituksen ohjelma 24.6.2003. Valtioneuvoston kanslian julkaisut. Saatavilla: https://valtioneuvosto.fi/documents/10184/369117/hallitusohjelma-vanhanen.pdf/da627124-c0ee-4015-9642-197b11013c02

Valtiovarainministeriö (2018). Julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelma. Toim. Kimmo Rousku. Valtiovarainministeriön julkaisu 32/2018. Saatavilla: http://urn.fi/URN:ISBN:978-952-251-975-7

Viestintävirasto 9.2.2018. Tietoturvan vuosi 2017 -katsaus ilmestynyt. Saatavilla: https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/02/ttn2018 02091159.html

Yhteiskunnan turvallisuusstrategia (2017). Valtioneuvoston periaatepäätös 2.11.2017. Helsinki: Turvallisuuskomitean sihteeristö. Saatavilla: https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/YTS_2017_suomi.pdf