OULUN SEUDUN
AMMATTIKORKEAKOULU

Antti Luoto

NÄKÖKULMIA SUOJAUTUMISEEN INTERNETRIKOLLISUUTTA VASTAAN

OULUN SEUDUN
AMMATTIKORKEAKOULU

ALBERTINKUJA 20, (PL 222) 90101 OULU
www.oamk.fi

NÄKÖKULMIA SUOJAUTUMISEEN INTERNETRIKOLLISUUTTA VASTAAN

Antti Luoto

Opinnäytetyö

Syksy 2013

Tietojenkäsittelyn koulutusohjelma

Oulun seudun ammattikorkeakoulu

ALBERTINKUJA 20, (PL 222) 90101 OULU
www.oamk.fi

TIIVISTELMÄ

Oulun seudun ammattikorkeakoulu
Liiketalouden amk tutkinto, tietojenkäsittelyn koulutusohjelma

---

Tekijä: Antti Luoto
Opinnäytetyön nimi: Näkökulmia suojautumiseen internetrikollisuutta vastaan
Työn ohjaaja: Ritva Virkkala
Työn valmistumislukukausi ja -vuosi: Joulukuu 2013
Sivumäärä: 37 + 1 liitesivu

Opinnäytetyön tarkoituksena on koota sellainen internetissä tapahtuva rikollinen toiminta, jonka kohteena voi olla kuka hyvänsä nettiä käyttävä kansalainen. Opinnäytetyössä tarkastellaan tietoverkkojen kautta tehtyjä rikollisuuden eri muotoja. Tarkastelu kohdistetaan niihin arkipäivän rikoksiin, joissa teko toteutetaan osin tai kokonaan internetin avulla. Tarkasteltavana olevissa rikoksissa on pyrkimyksenä harhauttaa ihmisiä internetissä välitettävän tiedon tai mahdollisesti haittaohjelman avulla tai tehdä uhkaus anonyyminä tai kirjoittaa anonyyminä loukkaavasti tai herjaavasti. Kohteena saattaa olla yksittäinen henkilö, mutta kohteena voi olla myös laaja rajoittamaton ihmisjoukko. Tietoverkkojen välityksellä rikollinen voi vaivattomasti ylittää valtioiden rajoja niin, että rikollinen toiminta tapahtuu kaukana sieltä, missä teon tosiasiallinen seuraus ilmenee.

Opinnäytetyössä selvitetään, mitä rikoslain tunnusmerkistöjä internetissä tapahtuva rikollinen toiminta täyttää. Opinnäytetyössä selvitetään myös mitkä ovat esitutkintaviranomaisen mahdollisuudet selvittää rikos, kun internetiä käytetään rikoksen tekemisessä

Asiasanat: nettirikollisuus, internet, rikollisuus, internetrikollisuus

ALBERTINKUJA 20, (PL 222) 90101 OULU
www.oamk.fi

ABSTRACT

Oulu University of Applied Sciences
Degree Programme in Business Information Systems

Author: Antti Luoto
Title of thesis: Perspectives on protection against Internet crimes
Supervisor: Ritva Virkkala
Term and year when the thesis was submitted: December 2013
Number of pages: 37 + 1 appendix

The purpose of this thesis is to collect the criminal activity in the Internet, which may be confronting any person who uses the Internet. The thesis examines various forms of criminality which are performed in the Internet. Examination focuses to the everyday offenses, where the act is carried out partly or entirely via the Internet. In these crimes people are tried to mislead with false information or they are victims of insult or malware or they have an experience of the threat. The target may be a single person, but it may also be directed at a large number of unlimited human. Through the network the criminals can easily crosses national boundaries so that the criminal activity is carried out far away from where the actual consequence occurs.

The study will examine what the Criminal Code offenses the internet criminal acts will fill. The study will also examine what possibilities the pre-trial investigation authorities have when they investigate these crimes.

Keywords: crime on-line, internet, cyber-crime, net

Sisällysluettelo

ALBERTINKUJA 20, (PL 222) 90101 OULU
www.oamk.fi

1 Johdanto

Internetrikokset edustavat maailmanlaajuisesti tiedossa olevaa ilmiötä, jonka seurauksena monet sen uhreiksi joutuneet ovat menettäneet rahansa, pahoittaneet mielensä, menettäneet uskonsa ihmiseen, joutuneet ilkeämielisten tai sairaiden ihmisten kohteeksi jne. Toisinaan internetrikosta voi olla vaikea tunnistaa, sillä toimintaa on monissa tapauksissa peitelty ja on annettu harhaanjohtavaa tai puutteellista tietoa, jonka seurauksena monet on saatu uskomaan vilpittömiin tarkoitusperiin.

Internetrikokset on ilmiönä aika uusi, koska internet itsessään ei ole ollut kansan saatavilla kuin neljännesvuosisadan. Internetin käyttäjien ja käytön määrä kasvaa vuosittain räjähdysmäisesti. Käyttäjien joukkoon mahtuu monenlaisia käyttäjiä. Käyttö on helppoa sekä maailmanlaajuista ja siksi se antaa myös otollisen maaperän rikolliselle toiminnalle ja rikolliselle mielenlaadulle.

Esitutkintaviranomaisista poliisi on nostanut tietoverkkorikokset yhdeksi painopisteeksi omassa toiminnassaan. Poliisin toiminta- ja taloussuunnitelmassa (TTS) vuosiksi 2013-2017 yhdeksi strategiseksi linjaukseksi on otettu tietoverkkorikosten tunnistaminen sekä poliisin läsnäolon lisääminen tietoverkoissa. Lisäksi varmistetaan tietotekniikkarikostutkinta ja siihen liittyvien valtakunnallisten palveluiden yhtenäistäminen. (Helminen 2012b, 227-228.)

2 Tutkimuksen tarkoitus ja siinä käytetty aineisto

Opinnäytetyössä on hyödynnetty kuvailevaa tutkimusmenetelmää. Olen valinnut tämän lähestymistavaksi siksi, koska pyrkimys ei ole luoda uutta tietoa aiheesta vaan tehdä havaintoja internetrikoksista ja mahdollisuuksista puuttua niihin esitutkinnallisin keinoin. Opinnäytetyö
on tutkimustyyppinen, ei varsinainen tutkimus.

Tutkimuksen avulla pyritään selvittämään, millaisia internetrikoksia on, miten niitä toteutetaan ja millä tavoin ne ilmenevät. Monet ovat joutuneet internetrikosten kohteiksi, mutta ei välttämättä uhreiksi, usein jopa tietämättään. Tämän vuoksi tutkimuksessa etsitään vastauksia myös siihen, miten voisi tunnistaa internetrikoksen ja siten välttyä siltä. Internetrikoksia on paljon ja osa on paikallisia tai valtakunnallisia, mutta osa on globaaleja valtioiden rajat ylittäviä tekoja.

Internetrikoksia on monenlaisia. On sellaisia, jotka on suunnattu tiettyyn henkilöön tai sitten kohteena voi olla satunnainen joukko ihmisiä ympäri maailmaa ja kaikkea siltä väliltä. Osalla rikoksista yritetään saada taloudellista hyötyä, osa tehdään puhtaasti kiusanteko mielessä tai jopa vahingoittamistarkoituksessa.

Tutkimuksessa käsitellään internetrikoksiin liittyvää lainsäädäntöä sekä Korkeimman oikeuden että Hovioikeuksien ratkaisuja. Kovinkaan paljon ei ole vielä Korkeimman oikeuden ratkaisuja liittyen internetrikoksiin, koska ne ovat rikosoikeudellisesti katsoen vielä varsin uusi rikollisuuden laji. Lisäksi näkökantaa laajennetaan aiheeseen liittyvän kirjallisuuden kautta sekä asiantuntija lausunnoilla.

3 Verkkorikollisuus ja verkkorikokset

Internetin toimintaperiaatteesta johtuen sitä ei hallinnoi mikään yksittäinen taho. Se on luonteeltaan rajat ylittävää ja käyttäjävetoinen viestintäkanava, jossa ei ole keskitettyä sääntelyä. Jotkut ovat käyttäneet käsitettä internetoikeus, joka on osaltaan harhaanjohtava. Internet on neutraali viestintäkanava, jonka perustehtävä on siirtää viestejä ja tietoja henkilöiden ja paikkojen välillä. Internetissä tapahtuvaa viestintää koskevat samat lait kuin muutakin viestintää. Internet on luonteeltaan kansainvälinen ja siihen kohdistuu useiden eri maiden lainsäädäntöä, joten ei voida puhua yhdestä kansallisesta internetoikeudesta. (Innanen 2012, 6-7.)

Verkossa voi tehdä samantapaisia laissa kriminalisoituja tekoja kuin tosimaailmassakin. Internet mahdollistaa tiedon vapaan saatavuuden ja mielipiteenvapauden, mutta se mahdollistaa samalla verkkorikollisuuden. Verkkorikoksilla, engl. cyber crime, tarkoitetaan rikoksia, jotka tehdään tietojärjestelmiä ja viestintäverkkoja hyödyntäen tai joiden kohteena ovat tietojärjestelmät ja –verkot. (Haasio 2013, 9.)

Verkkorikokset eli kyber-rikokset voidaan jakaa neljään pääryhmään (Majid 2013, 10).

1. Kyber-tunkeutumiset; tunkeudutaan toisen omaisuuteen aiheuttaen vahinkoa, kuten hakkeroimalla, nettisivuihin tehtävillä muutoksilla sekä viruksilla.

2. Kyber-petokset ja -varkaudet; rahan ja omaisuuden anastaminen, luottokorttivarkaudet, piratismi.

3. Kyber-pornografia; lain rikkominen epäsiveellisyydellä ja säädyttömyydellä.

4. Kyber-väkivalta; toisiin kohdistuvaa henkistä väkivaltaa tai siihen yllyttämistä, kuten vihapuheet ja kyttääminen.

3.1 Kyber-tunkeutumiset

Tunkeutumisissa käytetään erilaisia haittaohjelmia. Tunkeutumisia tapahtuu matojen, virusten, troijalaisten, takaovien, bottiverkkojen ja zombien avulla. Madot käyttävät hyväkseen turva-aukkoja ja leviävät koneesta toiseen näiden kautta. Mato ei pyri tekemään vahinkoa, mutta sen nopea leviäminen saattaa tukkia tietoverkkoja ja tietokoneita. Palomuurit ja käyttöjärjestelmien päivittäminen estävät tehokkaasti matojen leviämisen. Virukset leviävät yleensä sähköpostien liitteiden kautta. Kun liitetiedosto avataan, se tarttuu koneeseen ja levittää itseään eteenpäin. Troijalainen on ohjelma, joka ei levitä itseään eteenpäin, mutta se sisältää toimintoja, jotka eivät näy päällepäin. Toisinaan troijalainen päästessään koneeseen, avaa palomuuriin aukon ja päästää sitä kautta muita haitta ohjelmia, jotka valtaavat koneen. Takaovi on toiminto, joka on mukana sinänsä hyödyllisessä ohjelmassa. Takaoven kautta tekijä pääsee uhrin koneeseen ja voi ottaa sen haltuunsa. Haittaohjelma saattaa ottaa koneen verkkoyhteydet hallintaansa. Tällöin kone muuttuu zombieksi, joka jää odottamaan isäntänsä ohjeita irc-kanavalta ja toimii ohjeiden mukaisesti. Haittaohjelmien saastuttamista zombie-koneista voi muodostua jopa kymmenien tuhansien bottiverkkoja, joita rikollinen voi ohjailla. Bottiverkkoja voidaan käyttää miljoonien roskapostiviestien lähettämiseen, tietomurtojen ja hakkerointien peittämiseen, tehokkaaseen laskentaan ja palveluestohyökkäyksiin. (Järvinen 2012, 178-179.)

3.2 Kyber-petokset ja -varkaudet

Petosrikokset

Internet tarjoaa erinomaisen toimintaympäristön huijareille. Internetissä toimiminen ei rajoitu vain huijarin kotimaahan vaan toimintaympäristönä on koko maailma. Internetpetosten tutkinta on viranomaisille tutkinnan kannalta huomattavasti haasteellisempaa kuin perinteisten petosrikosten tutkinta. Onneksi rajat ylittävä huijaus on useimmiten alkeellista ja kielioppivirheitä sisältävä sekä epäuskottava. Kuitenkin kun huijausviestit lähetään useille sadoille tuhansille, niin aina löytyy joku hyväuskoinen, joka lähtee huijaukseen mukaan. Rikolliset kehittävät jatkuvasti uusia keinoja, joilla he yrittävät huijata sekä yrityksiä että yksityisiä henkilöitä. Sähköposti ja internet ovat avanneet mahdollisuuden tavoittaa suuria ihmismääriä helposti ja lähes olemattomin kustannuksin. Suuri-

mittaisten huijausyritysten takana on usein kansainvälinen järjestäytynyt rikollisuus, mutta joukossa on myös rikollista yksityisyritteliäisyyttä. (Haasio 2013, 37.)

Internetpetokset ovat lisääntyneet radikaalisti viime vuosina ja ne saavat koko ajan erilaisia muotoja. Yleisimpiä internetpetoksia ovat varastetun tavaran myyminen ínternetin kautta, olemattoman tavaran myyminen, annetaan myytävästä tuotteesta vääriä ja paikkansapitämättömiä tietoja, nettihuutokauppojen huutojen keinotekoinen nostaminen, nigerialaiskirjeet, romanttiset kirjeet, tietojen kalastelu, sijoitushuijaukset sekä laillisten taloussivujen väärentäminen. (Majid 2012, 80-88.)

Erittäin yleisiä kotimaisessa nettirikollisuudessa ovat netin kaupankäyntitilanteissa tehdyt petokset, joissa vain raha vaihtaa omistajaa ja itse tuote jää saamatta. Näissä voi välillä olla hankalaa tehdä rajanvetoa siviilioikeudellisen riita-asian ja rikoksen välillä. Siviilioikeudellisen riita-asian saa vireille käräjäoikeuden kansliaan toimitettavalla kirjallisella haastehakemuksella. Muutaman kympin tai satasen saatavan hakeminen voi kuitenkin tulla huomattavasti kalliimmaksi asiaan liittyvien erilaisten kustannusten ja kulujen takia. (http://www.poliisi.fi/nettipoliisi 23.11.2013.)

Nigerialaiskirjeitä lähetetään edelleen sähköpostitse. Nigerialaiskirjeissä uhri houkutellaan mukaan suuriin rahansiirtoihin erilaisilla peitetarinoilla. Tarinoissa vedotaan joko ihmisten auttamishaluun tai haluun saada helppoa rahaa, välillä molempiin yhtä aikaa. Tyypillinen tarina on, että jonkin afrikkalaisen valtion edesmenneen presidentin sukulainen on saamassa miljoonia dollareita, mutta ne pitäisi saada maasta ilman, että viranomaiset saavat asiasta vihiä. Sähköpostin vastaanottajaa pyydetään auttamaan ja lainaamaan tiliänsä hetkeksi, että rahat saadaan siirrettyä. Mitään rahoja ei ole, mutta uhrilta pyydetään aina enemmän ja enemmän rahaa järjestelykuluihin. Lopulta uhri on tilanteessa, että hän laittaa rahaa lisää, että saisi jo laittamansa rahat takaisin. Tavallisia ovat myös ilmoitukset huomattavista arpajais- tai lottovoitoista, vaikka viestinsaaja ei olisi mihinkään arpajaisiin koskaan osallistunutkaan. Viestissä kerrotaan, että viestinsaaja on voittanut huomattavan summan milloin missäkin arvonnassa. Tarinoita tulee eri maista ja kaava on periaatteessa sama kuin nigerialaiskirjeissä: voidakseen saada voittonsa lunastetuksi, pitää ensin lähettää pieni summa rahaa erilaisiin kuluihin, sitten vähän suurempi summa jne. (Järvinen 2012, 162-165.)

Romanssi- eli deittihuijauksissa ovat petollisia nettirakkaita. Internetin keskustelu- ja seurustelupalstoilla syntyneissä suhteissa tai roskapostien tapaan tuhansille lähetetyssä kirjeenvaihtopyyntöviestissä saattaa huijauksen kohteena oleva osapuoli rakastua oikeasti ja tulisesti, jolloin hänen on vaikea ymmärtää, että kaukainen rakastettu haluaakin vain hänen rahansa. Tyypillinen tarina on, että kyseessä on venäläinen tai afrikkalainen kaunotar, joka haluaa tutustua suomalaiseen mieheen. Kun keskusteluyhteys on avattu, nainen lähettää itsestään näyttäviä valokuvia. Myöhemmin hän kertoo häntä kohdanneesta vastoinkäymisestä ja pyytää pientä lahjoitusta. Pyydetyt summat kasvavat ja jos uhri alkaa empiä, nainen ilmoittaa olevansa tulossa Suomeen, kunhan vain saa rahat lentolippuun. (Järvinen 2012, 171-172.)

Myyjiä huijataan siten, että internetin kautta tavaroita myyvään henkilöön otetaan yhteyttä ja myytävästä tavarasta tarjotaan huomattavan suurta ylihintaa. Ostaja lähettää maksuksi shekin, joka ylittää sovitun kauppahinnan jopa tuhansilla euroilla. Erilaisiin syihin vedoten ostaja pyytää palauttamaan ylimääräisen osan shekin lunastuksen yhteydessä. Pankilta kuluu yleensä 5 pankkipäivää shekin katteen tai oikeellisuuden varmistamiseen. Jos ylimääräinen osa palautetaan heti lunastuksen yhteydessä ja shekki osoittautuukin myöhemmin väärennetyksi tai katteettomaksi, menetyksestä vastaa shekin lunastaja eli tässä tapauksessa myyjä. Sama toimii myös PayPalin kautta maksettaessa, koska maksajalla on muutama päivä aikaa perua tekemänsä maksu, jolloin saatuaan tavaran hän peruu maksun ja myyjä jää ilman suoritusta. (Haasio 2013, 40-41.)

Ostajaa huijataan siten, että ulkomaisella verkkosivulla tarjotaan myytäväksi esim. hyvää käytettyä autoa. Kun kiinnostunut ostaja ottaa myyjään yhteyttä, kauppa sovitaan tapahtuvaksi ulkomailla. Myyjä haluaa ostajaehdokkaan tallettavan rahaa ulkomaiseen pankkiin etumaksuksi voidakseen vakuuttua ostajan todella tulevan tapaamiseen. Myös myyntisivustossa voidaan kertoa, että ostaja voi tallettaa rahaa pantiksi ja siten varata kyseisen myyntikohteen itselleen. Vakuuttavuutta voidaan lisätä lähettämällä ostajaehdokkaalle lisäohje kehotuksella faksata jonkun tunnetun kansainvälisen pankin kautta rahansiirtomääräys, josta ilmenee rahojen nostoon tarvittava numerokoodi. (em., 42.)

Valheellisissa mainoksissa annetaan lukijalle kuva, että hän olisi voittanut jotain tai kun hän vastaa oikein muutamaan kysymykseen, niin hän saa jotain. Voiton tai tuotteen saaminen edellyttää matkapuhelinnumeron ilmoittamista. Ilmoitettuun numeroon tulee viesti, johon vastaamalla sitou-

tuu tilaamaan kalliin mobiilipalvelun. Varsinaista palkintoa ei tule, vaan tulee ilmoitus, että kyse on arvonnasta, johon osallistuminen maksaa jotain. (Järvinen 2012, 166-167.)

Yksi epärehellisten yrittäjien käyttämä huijausmuoto on ilmaisnäytteiden lähettäminen. Asiakkaalle lähetään veloituksetta näyte postikulujen hinnalla. Postikulut maksetaan joko pankki- tai luottokortilla. Asiakas on saanut jatkotilauksia, joista on ollut maininta korkeintaan pienellä tekstillä sivulauseessa. (Haasio 2013, 43.)

Aikaisemmin sähköpostiin tuli paljon roskapostia, mutta nykyiset suojauskeinot estävät roskapostej pääsemästä läpi. Siksi mainostajat ovat kehitelleet uusia lähestymiskeinoja. Avuksi on otettu sosiaalinen media. Sosiaalisen median kautta mainostaja pyrkii pääsemään sopivan kohteen seuraajaksi valehenkilöllisyydellä. Päästyään kohteen seuraajaksi valeseuraaja lähettää linkin, jota utelias kohde ei malta olla avaamatta. (Järvinen 2012, 168.)

Ulkomaisten maksullisten palveluiden kanssa saa olla tarkkana, koska jos ei ole täysin selvillä saattaa sitoutua ymmärtämättömyyttään ja tietämättömyyttään pitkäksi aikaa maksamaan jostakin palvelusta, vaikka palvelua ei enää käyttäisikään. Valittaminen kohtuuttomista sopimusehdoista vieraassa maassa on hankalaa ja voi tulla kalliiksi. Näissä bisnesideana voi olla se, että asiakas tyytyy maksamaan ylihinnoitetun palvelun oppirahana tai sitten ansaintalogiikka voi olla se, että jos asiakas ei maksa perintäkulut moninkertaistavat alkuperäisen summan. (Järvinen 2012, 173.)

Tietojen kalastelulla eli phishingillä yritetään hankkia pankkien verkkotunnuksia tai luottokorttitietoja. Sähköpostiviesteillä tiedustellaan ja kerätään erilaisia taloudellisiin asioihin liittyviä tietoja kuten luottokorttitietoja, tilitietoja sekä verkkopankkitunnuksia. Perusteluna tiedustelulle voi olla, että pankin ylläpito tarvitsee tietoja, koska jotain tiliin liittyvää maksua ei pystytty hoitamaan tai tilissä on muita ongelmia, tai voidaan kertoa jostain uusimis- tai muutosasiasta, joka vaatii asiakkaan tunnusten käyttämistä. Viesteissä on linkkinä valmiina www-osoite, jota klikkaamalla pääsee sivulle, joka näyttää pankin www-sivulta. Sivu on todellisuudessa pankin sivuksi väärennetty rikollisten hallussa oleva phishing-sivu. Nettipankkihuijausten kehittyneempi muoto on haittaohjelmat, jotka suorittavat tilisiirtoja asiakkaan tietämättä. Asiakas on huomaamattaan asentanut koneelleen haittaohjelman eli troijalaisen, joka aktivoituu asiakkaan alkaessa maksamaan laskua. Hait-

taohjelma muuttaa saajan tilin ja summat selaimessa, mutta näyttää maksajalle alkuperäisen laskun tiedot. (Haasio 2013, 44.)

Sijoituspetokset

Sijoituspetoksissa on useita toteutusmuotoja. Yleisin niistä on huijata sijoittamaan olemattomiin yhtiöihin. Sijoituspetoksissa ensimmäinen yhteydenotto tapahtuu puhelimitse, sähköpostilla tai keskustelupalstoilla. Myyjä syöttää ostajalle väärää tietoa ja antaa yltiöpositiivisen ansainta olettaman, joka houkuttaa sijoittamaan riskilläkin. Toinen tyypillinen keino on, että annetaan ymmärtää olevan sisäpiirin tietoa yhtiöstä ja yhtiön tulevista osakekursseista. Kyseessä on ns. dump and pump eli sijoitetaan yhtiöön hetkellisesti varoja ja heti, kun kurssi on noussut, otetaan varat ulos. Myyjä pyrkii nopeuttamaan päätöksen tekoa toteamalla esimerkiksi, että yhtiö on menossa pörssiin tai taustalla on muita huomattavia järjestelyjä - siksi sijoituksen teolla on kiire. Lopulta käy niin, että myyjä saa tuoton hetkellisesti kohonneesta kurssista ja kurssi nopeasti laskee ja usein alle sen arvon, jonka ostaja on maksanut ja lisäksi tulee ostajalle toimenpiteestä aiheutuneet kulut maksettaviksi. (Majid 2012, 88.)

Identiteettivarkaudet

Identiteettivarkautta itsessään ei ole Suomen rikoslaissa kriminalisoitu. Tämä tarkoittaa, että jonkin blogin, Twitter-tilin tai Facebook-profiilin perustaminen jonkun julkisuuden henkilön nimellä ei ole rikos. Rikolliseksi toiminta muuttuu vasta, kun sivuilla loukataan toisen kunniaa, levitetään yksityisyyden suojan piiriin kuuluvia tietoja, kiihotetaan kansanryhmää vastaan tai syyllistytään muuhun rikoslain tunnusmerkistön täyttävään tekoon. (Järvinen 2012, 257.)

Identiteettivarkauden muotona on esiintyminen toisena henkilönä. Identiteettivaras hankkii toisen henkilön nimitiedot, osoitteen ja luottokorttitiedot ja niitä hyväksikäyttäen hankkii itselle palveluita ja hyödykkeitä internetin kautta esimerkiksi tilaamalla tavaraa toisen henkilön laskuun, avaamalla puhelinliittymiä, ottamalla pikavippejä tai lainaamalla pankista rahaa. Tietoja saadaan murtautumalla internetissä oleviin tietokantoihin, pankkiautomaattiin asennettavasta lukulaitteesta (skimmaaminen), varastetun lompakon sisällöstä tai jopa kohdehenkilön roskia penkomalla. Usein nuo mainitut tiedot riittävät verkkokaupoissa ostosten tekemiseen. Identiteettivarkauksilla tehdään myös kiusaa tekemällä toisen tiedoilla verkkoyhteisöön profiili, jonne laitetaan epäsiveellistä aineistoa ja kirjoitetaan loukkaavia viestejä. (Haasio 2013, 47.)

Kiusaa voidaan tehdä laittamalla perätön deitti-ilmoitus internetiin. On tapauksia, joissa mies on tehnyt ex-vaimostaan hyvinkin härskin deitti-ilmoituksen, jonka jälkeen nainen on saanut lukemattomia yhteydenottoja ilmoituksen lukeneilta miehiltä. On tapauksia, joissa äijäporukassa tehdään vitsailumielessä jostakin miehestä homoseuraa hakeva deitti-ilmoitus. Molemmissa tapauksissa tekijät syyllistyvät kunnianloukkausrikokseen. Törkeän tekomuodon puolelle teko voi mennä, jos ilmoitukseen on liitetty esimerkiksi alastonkuvia, jolloin kyseeseen tulee myös yksityiselämää loukkaava tiedon levittäminen. (http://www.poliisi.fi/nettipoliisi 23.11.2013.)

Viestintäsalaisuuden loukkausrikos tulee kyseeseen aina, kun joku käyttää ilman lupaa sinun profiiliasi, jossa on mahdollista viestiä yksityisesti. Tämä koskee myös erilaisia pelitilejä, sähköposteja ja muita vastaavia palveluja. Oleellista asiassa ei ole se onko viestejä luettu, vaan onko tekijällä ollut mahdollisuus lukea palvelussa olevia viestejä. (em.)

3.3 Kyber-pornografia

Selkeästi yleisin internetiin liittyvä rikosnimike seksuaalirikosten osalta on lapsen seksuaalinen hyväksikäyttö. Internetissä tapahtuva lasten hyväksikäyttö on globaali ongelma ja asianomistajina on sekä tyttöjä, että poikia. Tutkimusten mukaan verkossa on lähestytty jopa joka viidettä nuorta hyväksikäyttötarkoituksessa. Lapsia ja nuoria houkutellaan uhreiksi useilla eri foorumeilla. Suosituimpia ovat Facebook, IRC-galleria sekä Kuvake. Hyväksikäyttäjillä on todettu olevan tietty toimintakaava. Aluksi he pyrkivät internetissä luomaan luottamuksellisen suhteen nuoreen. Sitten kun luottamus on syntynyt, ehdotetaan tapaamista. Kyse on manipulaatiosta, joka alkaa aikuisen lasta kohtaan osoittamalla huomiolla, kehuilla sekä välittämisellä joka saattaa edetä lahjojen ostamiseen saakka. Useimmiten kohteena ovat 13-15 -vuotiaat nuoret. (Haasio 2013, 76.)

Tarkkaa tutkimustietoa alalta on vaikea saada, mutta yksi tilasto vuodelta 2009 ilmoittaa seuraavanlaisia lukuja: (Holt 2012, 111-112)

- Keskimäärin 11 vuoden iässä altistutaan internetissä pornoon ensimmäistä kertaa
- Suurin internet pornon kuluttaja joukko löytyy 35-49 - vuotiaista
- 80 prosentilla 15-17 –vuotiaista on useita altistuksia kovaan pornoon
- 90 prosenttia 8-16 –vuotiaista on katsonut verkossa pornoa
- 7-17 – vuotiaista 29 prosenttia ilmoittaisi osoitteensa
- 7-17 –vuotiaista 14 prosenttia ilmoittaisi sähköpostiosoitteensa

- 100 000 internetsivustoa sisältää laitonta lapsipornoa
- Lapsipornossa liikkuu kolme miljardia dollaria vuosittain

Rikoslaissa seksuaalirikokset löytyvät rikoslain 20 luvusta. Tämän lisäksi on pykäliä rikoslain 17 luvussa sukupuolisiveellisyyttä loukkaavien kuvien levittämisestä. Tarkoituksena on suojella seksuaalista itsemääräämisoikeutta ja lapsia. Laissa tarkoitetaan sukupuoliyhteydellä sukupuolielimellä tapahtuvaa tai sukupuolielimeen kohdistuvaa tunkeutumista toisen kehoon. Seksuaalisella teolla tarkoitetaan tekoa, jolla tavoitellaan seksuaalista kiihotusta tai tyydytystä ja joka tekijä ja kohteena oleva henkilö sekä teko-olosuhteet huomioon ottaen on seksuaalisesti olennainen. Jos alaikäinen on aloitteentekijänä, vastuu on aina aikuisella. Alaikäisen kohdalla myös vanhemmat ovat asianomistajia ja heillä on oikeus vaatia rangaistusta. (http://www.poliisi.fi/nettipoliisi 23.11.2013.)

Seksuaalirikokset vanhenevat pääsääntöisesti alle 18-vuotiaiden kohdalla kun asianomistaja täyttää 28 vuotta eli kymmenen vuoden kuluttua täysi-ikäisyydestä. Rikos lapsen houkuttelemisesta seksuaalisiin tarkoituksiin vanhenee asianomistajan täytettyä 23 vuotta. Aikuisten osalta pätevät normaalit vanhenemisajat ja esimerkiksi raiskauksen osalta rikos vanhenee kymmenessä vuodessa. (em.)

Laissa ei ole suoraa mainintaa, kuinka suuri ikäero on hyväksyttävää osapuolten välille. Lailla ei ole tarkoitus rajoittaa nuorten keskinäisiä sukupuolisuhteita silloin, kun ne eivät sisällä toisen hyväksikäyttämistä. Lähtökohtaisesti esimerkiksi kahden 15-vuotiaan seksuaalissävytteistä keskustelua ei ole lailla syytä tarkoitus rajoittaa. Kehityseron arvioinnissa on merkitystä henkilön elämänkokemuksella, kehitystasolla, sekä kyvyllä tehdä itsenäisiä päätöksiä. (em.)

Lapsen seksuaalisen hyväksikäytön tekotavat voidaan jakaa netissä kolmeen eri kategoriaan: (Haasio 2013, 75)

- seksuaalissävytteisiin viesteihin
- lähetettyihin tai vastaanotettuihin seksuaalissävytteisiin kuviin/videoihin
- reaaliaikaiseen web-kamerayhteyteen, jossa esiinnytään seksuaalissävytteisesti

Lapsen houkuttelu seksuaalisiin tarkoituksiin kirjattiin lakiin kesäkuussa 2011. Houkuttelupykälä ja groomingina tunnettu tekomuoto täyttyy silloin, kun tekijä ehdottaa tapaamista tai muuta kanssakäymistä lapsen kanssa siten, että ehdotuksen sisällöstä tai olosuhteista muuten ilmenee tekijän tarkoituksena olevan valmistaa lapsipornokuvia tai kohdistaa lapseen seksuaalirikos. Tyypillisiä tekoja ovat, että lapsilta tai nuorilta pyydetään verkossa eroottissävyisiä valokuvia tai muuta vastaavaa materiaalia tai etsitään alaikäistä seksiseuraa. (em.)

Seksuaalipalvelujen ostaminen alaikäiseltä tulee kyseeseen silloin kun joku lupaa tai antaa korvauksen alle 18-vuotiaalle sukupuoliyhteydestä tai muusta seksuaalisesta teosta. internetissä kyseinen tapaus voi tulla kyseeseen esimerkiksi sellaisissa tapauksissa, joissa pyydetään esiintymään alasti webkameran välityksellä tai lähettämään alastonkuvia ja sitä vastaan tarjotaan korvauksena rahaa, päihteitä, lahjoja tai muuta sellaista. (http://www.poliisi.fi/nettipoliisi 23.11.2013.)

Pakottaminen seksuaaliseen tekoon voi tulla kyseeseen silloin, kun väkivallalla tai uhkauksella pakottaa toisen ryhtymään seksuaaliseen tekoon tai sellaisen teon kohteeksi ja se olennaisesti loukkaa toisen seksuaalista itsemääräämisoikeutta. Kyseinen nimike voi tulla kyseeseen esimerkiksi tapauksissa, joissa lasta on kiristetty esiintymään webkameran välityksellä alasti, tai muuten tekijä uhkaa pistää aikaisemmin saamiaan eroottisia valokuvia avoimesti esille nettiin. (em.)

3.4 Kyber-väkivalta

Uhkaukset

Internetissä tapahtuva koulu-uhkaus voi toteutua monella eri tavalla. Uhkaus voi tapahtua Messenger-keskusteluissa, julkisilla keskustelupalstoilla tai sähköpostin välityksellä. Uhkaus voi tapahtua myös siten, että internetissä julkaistaan kuva, missä on uhkaava kuvateksti. Rikosnimikkeinä täyttyy yleensä laiton uhkaus tai perätön vaarailmoitus. (http://www.poliisi.fi/nettipoliisi 23.11.2013.)

Laittoman uhkauksen tunnusmerkistö täyttyy koulu-uhkaus tapauksissa silloin, kun uhkauksessa yksilöidään tietty tai tietyt henkilöt. Mitä vakavammasta uhkauksesta on kyse, sitä vähemmän kohteen subjektiivisella kokemuksella on vaikutusta rikoksen tunnusmerkistön täyttymiseen. (em.)

Perätön vaarailmoitus voi toteutua silloin, kun ilmoituksen takia joudutaan tekemään pelastus- tai turvallisuustoimi viranomaisten taholta tai teko aiheuttaa pakokauhua. Teon tunnusmerkistö täyttyy, jos vastaanottaja ei tiedä sitä varmuudella perättömäksi ja että tavanomaisten ohjeiden ja rutiinien mukaan pelastus- tai turvallisuustoimeen olisi edes ryhdytty. Erona laittomaan uhkaukseen on se, että perätön vaarailmoitus ei kohdistu yksittäiseen henkilöön vaan johonkin tiettyyn kohteeseen. Esimerkiksi valokuva yhteisöpalvelussa, jonka kuvatekstissä uhataan, että tietty koulu räjähtää tiettyyn aikaan. Teko vaatii tahallisuutta ja sitä on välillä vaikea todistaa etenkin nuorten ajattelemattomien ns. hölmöilyviestien perusteella. (em.)

Oikeuspsykiatrian professori Nina Lindberg, oikeuspsykiatrian erikoislääkäri Eila Sailas nuorisopsykologian professori Riittakerttu Kaltiala-Heino ja sosiologian ja sosiaalipsykologian dosentti Atte Oksanen tutkivat vuosilta 2007-2009 koulusurmauhkaukset. Aineistossa oli mukana 77 uhkauksen tehnyttä henkilöä, joista 67 oli poikia. Henkilöt olivat iältään 13 ja 18 vuoden välillä. Tutkimuksessa kävi ilmi, että internetissä koulusurma-aikeistaan kertoneet nuoret olivat aikeissaan enemmän tosissaan kuin muissa tilanteissa esille tulleet uhkailut. Monet internetissä uhkauksen tehneistä oli jo suunnitellut, miten aikoisi uhkauksen toteuttaa. Joka viides oli tehnyt jo jotain valmisteluita. He kertoivat esimerkiksi tilanneensa erilaista välineistöä kuten aseita, veitsiä, rakennelleensa räjähteitä tai hankkineensa maastoutumisasusteita. Internetissä koulusurma-aikeista kertoviin nuoriin tulisi suhtautua vakavammin kuin muilla tavoin ilmaiseviin nuoriin. (Kaleva 23.11.2013.)

Internetkiusaaminen

Internetkiusaamisesta valta osa tapahtuu sosiaalisen mediassa (some). Tyypillisimpiä internetkiusaamisen muotoja ovat panettelu, seksuaalisesti häiritsevä kommentointi, ulkonäön arvostelu, toisen henkilön kuvien ja nimen väärinkäyttö sekä erityyppinen pilkkaaminen. Kiusaaminen saattaa kiusaajan mielestä olla vain pilaa, mutta kiusattu kokee sen toisin. Kiusaaminen on yleisesti koettu internetissä nuorten ongelmaksi. Nykyään yhä useammin aikuiset syyllistyvät internetkiusaamiseen. Häiritään esimerkiksi ex-puolisoa tai uhkaillaan täysin sivullisia ihmisiä keskusteluissa syntyneiden ristiriitojen takia. Kiusaamisen motiivina on voi olla mustasukkaisuus tai kateus. Esimiehen arvostelu tai naapurin panettelu ovat nykypäivänä tavallisia kiusaamisen muotoja. Identiteettivarkaus voi olla yksi kiusaamisen muodoista. (Haasio 2013, 62-64.)

Kunnianloukkauksesta voi olla kysymys, kun lähettää toiselle tai toisesta pilkkaavia ja ivaavia viestejä. Samoin valheellisen tiedon esittäminen toisesta, rasistiset huomautukset ja ulkonäköön voimakkaasti arvostelevat kommentit. Jos tällä toiminnalla aiheutetaan toiselle vahinkoa ja kärsimystä, tai häneen kohdistuvaa halveksuntaa, voi syyllistyä kunnianloukkaukseen. Toisen henkilön valokuvien loukkaava muokkaaminen ja niiden internetiin laittaminen täyttää kunnianloukkaus rikoksen tunnusmerkistön. Valokuvien osalta tulee huomioida, että se edellyttää usein kuvatun suostumusta. Tilanteesta riippuen kyse voi olla pelkästään palvelun sääntöjen rikkomisesta, eikä rikoksesta. Kunnianloukkauksen rangaistusasteikko on sakosta puoleen vuoteen vankeutta ja usein tulee kyseeseen myös rahallinen korvaus henkisistä kärsimyksistä. (http://www.poliisi.fi/nettipoliisi 23.11.2013.)

Törkeästä kunnianloukkauksesta voi olla kyse, kun tieto levitetään joukkotiedotusvälineen (eli esim. netti) kautta tai tieto muulla tavoin toimitetaan lukuisten ihmisten saataville. Tunnusmerkistö voi täyttyä, jos aiheutetaan suurta tai pitkäaikaista kärsimystä taikka erityisen suurta tai tuntuvaa vahinkoa. Henkisen vahingon mittaaminen on vaikeaa. Lisäksi törkeä tekomuoto edellyttää kokonaisarvostelua, jos edellä mainituista asioista täyttyy edes toinen ja rikos on myös kokonaisuutena arvosteltuna törkeä, tuomitaan törkeästä kunnianloukkauksesta sakkoon tai vankeuteen enintään kahdeksi vuodeksi. (em.)

Laiton uhkaus edellyttää, että uhatulla on perusteltua syytä olettaa, että hänen henkilökohtainen turvallisuutensa tai omaisuutensa on vakavassa vaarassa. Esimerkkinä voi olla tilanne, jossa kiusaaja lupaa hakata toisen tai jopa tappaa. Rikoksen täyttymisen osalta tärkeää on uhatun oma subjektiivinen kokemus uhkauksesta, ja siihen vaikuttaa myös uhkauksen aste rikoksen tunnusmerkistön täyttymiseen. Rangaistusasteikko laittomassa uhkauksessa on sakosta kahteen vuoteen vankeutta. (em.)

Yksityiselämää loukkaavan tiedon levittäminen voi olla kyse, kun levittää toisen yksityiselämästä arkaluotoisen tiedon, vihjauksen tai kuvan siten, että se aiheuttaa vahinkoa ja kärsimystä toiselle. Tieto pitää levittää joukkotiedotusvälineiden kautta tai muuten saattaa lukuisten ihmisten saataville. Erona kunnianloukkaukseen on se, että tieto on totta. Esimerkiksi kertoo toisen vakavasta sairaudesta tai sukupuolielämästä. Teko täyttyy myös laittamalla toista esittävän alastonkuvan ilman suostumusta nettiin. Rangaistusasteikko on sakkoa tai kaksi vuotta vankeutta sekä mahdolliset vahingonkorvaukset. (em.)

Viharikokset

Rasistisia tai eri aatteita, uskonnollista vakaumusta tai seksuaalista suuntautumista loukkaavia verkkosivuja on ympäri maailmaa. Rasistinen kirjoittelu on yksi vihapuheen muoto. Se ei ole terminä yksiselitteinen. Poliisiammattikoulussa tehdyn selvityksen mukaan viharikos voitaisiin määritellä seuraavasti: ”Viharikos on henkilöä, ryhmää, jonkun omaisuutta, instituutiota tai näiden edustajaa kohtaan tehty rikos, jonka motiivina ovat ennakkoluulot tai vihamielisyys uhrin oletettua tai todellista etnistä tai kansallista taustaa, uskonnollista vakaumusta tai elämänkatsomusta, seksuaalista suuntautumista, sukupuoli-identiteettiä, sukupuolen ilmaisua tai vammaisuutta kohtaan.” Viharikosta tai rasismirikosta itsessään ei ole rikoslaissa, mutta tyypillisiä rikoksia, jotka liittyvät viharikoksiin ovat kiihottaminen kansaryhmää vastaan, kunnianloukkaus sekä laiton uhkaus. (Haasio 2013, 110-111.)

Kiihottaminen kansanryhmää vastaan rikosnimikkeen sisältöä on muutettu vuonna 2011. Tarkoituksena muutoksessa oli täsmentää rikoksen tekotapaa ja suojelun kohteena olevaa ryhmää. Pykälän soveltamisalaa myös laajennettiin. Rikoksen tunnusmerkistö toteutuu kun asettaa yleisön saataville tai muutoin yleisön keskuuteen levittää tai pitää yleisön saatavilla tiedon, mielipiteen tai muun viestin, jossa uhataan, panetellaan tai solvataan jotakin ryhmää rodun, ihonvärin, syntyperän, kansallisen tai etnisen alkuperän, uskonnon tai vakaumuksen, seksuaalisen suuntautumisen tai vammaisuuden perusteella taikka niihin rinnastettavalla muulla perusteella. (http://www.poliisi.fi/nettipoliisi 23.11.2013.)

Uutena kohtana rikoslakiin luotiin törkeä kiihottaminen kansanryhmää vastaan. Törkeä rikos täyttyy jos kiihottamisessa kansanryhmää vastaan kehotetaan tai houkutellaan

1) joukkotuhontaan tai sen valmisteluun, rikokseen ihmisyyttä vastaan, törkeään rikokseen ihmisyyttä vastaan, sotarikokseen, törkeään sotarikokseen, murhaan tai terroristisessa tarkoituksessa tehtyyn tappoon, tai

2) muuhun kuin 1 kohdassa tarkoitettuun vakavaan väkivaltaan siten, että teolla selvästi vaarannetaan yleistä järjestystä ja turvallisuutta

Rikoksen tunnusmerkistön täyttyminen edellyttää olosuhdetahallisuutta, mutta ei tarkoitustahallisuutta. Tällöin tekijä on ollut tietoinen, että teolla uhataan, panetellaan tai solvataan. Tyypillinen

tunnusmerkistön täyttävä teko on esimerkiksi ryhmään kohdistuvan syrjinnän tai väkivallan hyväksyttävä tai toivottavana pitäminen. Kyseiseen ryhmään kuuluvia ihmisiä voidaan verrata eläimiin, loisiin tai muuten pitää alempiarvoisena, jolloin rikoksen tunnusmerkistö voi täyttyä myös. (em.)

4 Internetiin liittyvät rikokset rikoslaissa

4.1 Kiihottaminen kansanryhmää vastaan

> *Rikoslaki 11 luku 10 §, Kiihottaminen kansanryhmää vastaan*
>
> *Joka asettaa yleisön saataville tai muutoin yleisön keskuuteen levittää tai pitää yleisön saatavilla tiedon, mielipiteen tai muun viestin, jossa uhataan, panetellaan tai solvataan jotakin ryhmää rodun, ihonvärin, syntyperän, kansallisen tai etnisen alkuperän, uskonnon tai vakaumuksen, seksuaalisen suuntautumisen tai vammaisuuden perusteella taikka niihin rinnastettavalla muulla perusteella, on tuomittava kiihottamisesta kansanryhmää vastaan sakkoon tai vankeuteen enintään kahdeksi vuodeksi.*

Korkein oikeus on käsitellyt tapausta 2012, jossa A oli internetissä olevalla sivustollaan julkaissut kirjoituksen, jossa oli esitetty islaminuskoa ja somaleja loukkaavia lausumia. Tekstit olivat ”Profeetta Muhammad oli pedofiili, ja islam on pedofilian pyhittävä uskonto, siis pedofiiliuskonto. Pedofilia on Allahin tahto.” ja ”Ohikulkijoiden ryöstely ja verovaroilla loisiminen on somalien kansallinen, ehkä suorastaan geneettinen erityispiirre.” Kysymys oli siitä, oliko A menettelyllään syyllistynyt uskonrauhan rikkomiseen ja kiihottamiseen kansanryhmää vastaan. Lopullinen ratkaisu oli, että A:n syyksi luettiin kiihottaminen kansanryhmää vastaan ja uskonrauhan rikkominen, joista A tuomittiin yhteiseen 50 päiväsakon sakkorangaistukseen. (KKO 2012:58.)

Kouvolan hovioikeus on käsitellyt asiaa, jossa A on verkkolehden ylläpitämällä sivustolla julkaisemassaan kirjoituksessa otsikolla ”Kikkarapäälle kuonoon” yleisön keskuuteen levittänyt lausunnon ja tiedonannon, joissa panetellaan ja solvataan muslimeista koostuvaa uskonnollista, etnistä tai siihen rinnastettavaa ryhmää. A:n julkaisema kirjoitus sisältää asiallisesti ottaen syrjivän ja vahvasti yleistävän väitteen muslimien taipumuksesta väkivaltaisuuteen ja muuhun rikollisuuteen ja jopa terrorismiin. Hovioikeus katsoo kirjoituksen siten olevan sanottua ihmisryhmää solvaava ja panetteleva, koska siinä kerrotuin tavoin kuvataan kokonaiseen kansanryhmään kuuluvat ihmiset

rikollisina ja muihin nähden ala-arvoisina. Hovioikeus katsoo lausunnon loukkaavan näiden ihmisten ihmisarvoa. Lausunto on myös katsottu olevan kansanryhmää uhkaava, koska sen otsikossa esitetään voimatoimiin ryhtymistä muslimeja kohtaan hyväksyttävänä. Hovioikeus on tuominnut A:n 25 päiväsakkoon kiihottamisesta kansanryhmä vastaan. (KouHO 2012:9.)

4.2 Kunnianloukkaus

Rikoslaki 24 luku 9 § Kunnianloukkaus:

Joka 1) esittää toisesta valheellisen tiedon tai vihjauksen siten, että teko on omiaan aiheuttamaan vahinkoa tai kärsimystä loukatulle taikka häneen kohdistuvaa halveksuntaa, taikka 2) muuten kuin 1 kohdassa tarkoitetulla tavalla halventaa toista, on tuomittava kunnianloukkauksesta sakkoon tai vankeuteen enintään kuudeksi kuukaudeksi.

Edellä 1 momentin 2 kohdassa tarkoitettuna kunnianloukkauksena ei pidetä arvostelua, joka kohdistuu toisen menettelyyn politiikassa, elinkeinoelämässä, julkisessa virassa tai tehtävässä, tieteessä, taiteessa taikka näihin rinnastettavassa julkisessa toiminnassa ja joka ei selvästi ylitä sitä, mitä voidaan pitää hyväksyttävänä.

Kunnianloukkauksesta tuomitaan myös se, joka esittää kuolleesta henkilöstä valheellisen tiedon tai vihjauksen siten, että teko on omiaan aiheuttamaan kärsimystä ihmiselle, jolle vainaja oli erityisen läheinen.

4.3 Laiton uhkaus

Rikoslaki 25 luku 7 § Laiton uhkaus:

Joka nostaa aseen toista vastaan tai muulla tavoin uhkaa toista rikoksella sellaisissa olosuhteissa, että uhatulla on perusteltu syy omasta tai toisen puolesta pelätä henkilökohtaisen turvallisuuden tai omaisuuden olevan vakavassa vaarassa, on tuomittava, jollei teosta muualla laissa säädetä ankarampaa rangaistusta, laittomasta uhkauksesta sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

Helsingin hovioikeus on käsitellyt asiaa, jossa A on uhannut pääministeri B:tä ja valtiovarainministeri C:tä sekä eduskunnan koko henkilöstöä sellaisissa olosuhteissa, että heillä on ollut perusteltu syy pelätä henkilökohtaisen turvallisuutensa olevan vakavassa vaarassa. A on kirjoittanut eli julkaissut internetin uutisryhmässä "x" tekstin, jossa hän on uhannut ampua kiväärillä B:n ja C:n tai uhannut räjäyttää räjähdysaineella koko eduskunnan. A on lisäksi uhannut toimintansa seurauksena "tulevan ruumiita". Hovioikeus on katsonut, että koska uhkaus on tehty netinkeskusteluryh-

mässä, jossa on vain vähän lukijoita, eikä uhkausta ole saatettu uhattavien tietoon, A ei ole asiassa syyllistynyt laittomaan uhkaukseen. (HelHO 2012:1.)

4.4 Lapsiin ja nuoriin kohdistuvat seksuaalirikokset

Rikoslaki 20 luku 6 § Lapsen seksuaalinen hyväksikäyttö:

Joka koskettelemalla tai muulla tavoin tekee kuuttatoista vuotta nuoremmalle lapselle seksuaalisen teon, joka on omiaan vahingoittamaan tämän kehitystä, tai saa tämän ryhtymään sellaiseen tekoon, on tuomittava lapsen seksuaalisesta hyväksikäytöstä vankeuteen vähintään neljäksi kuukaudeksi ja enintään neljäksi vuodeksi.

Lapsen seksuaalisesta hyväksikäytöstä tuomitaan myös se, joka on sukupuoliyhteydessä kuuttatoista vuotta nuoremman lapsen kanssa, jos rikos ei 7 §:n 1 momentissa tarkoitetulla tavalla ole kokonaisuutena arvostellen törkeä. Lisäksi lapsen seksuaalisesta hyväksikäytöstä tuomitaan se, joka menettelee 1 momentissa tai edellä tässä momentissa tarkoitetulla tavalla kuusitoista mutta ei kahdeksantoista vuotta täyttäneen lapsen kanssa, jos tekijä on lapsen vanhempi tai vanhempaan rinnastettavassa asemassa lapseen nähden sekä asuu lapsen kanssa samassa taloudessa.

Yritys on rangaistava.

Rikoslaki 20 luku 8 a § Seksuaalipalvelujen ostaminen nuorelta:

Joka lupaamalla tai antamalla korvauksen saa kahdeksaatoista vuotta nuoremman henkilön ryhtymään sukupuoliyhteyteen tai muuhun seksuaaliseen tekoon, on tuomittava seksuaalipalvelujen ostamisesta nuorelta sakkoon tai vankeuteen enintään kahdeksi vuodeksi. Yritys on rangaistava.

Rikoslaki 20 luku 8 b § Lapsen houkutteleminen seksuaalisiin tarkoituksiin: Joka ehdottaa tapaamista tai muuta kanssakäymistä lapsen kanssa siten, että ehdotuksen sisällöstä tai olosuhteista muuten ilmenee tekijän tarkoituksena olevan 17 luvun 18 §:n 1 momentissa tarkoitetulla tavalla valmistaa kuvia tai kuvatallenteita, joissa sukupuolisiveellisyyttä loukkaavasti esitetään lasta, taikka kohdistaa lapseen tämän luvun 6 tai 7 §:ssä tarkoitettu rikos, on tuomittava lapsen houkuttelemisesta seksuaalisiin tarkoituksiin sakkoon tai vankeuteen enintään yhdeksi vuodeksi.

Jollei teosta muualla laissa säädetä ankarampaa rangaistusta, lapsen houkuttelemisesta seksuaalisiin tarkoituksiin tuomitaan myös se, joka houkuttelee kahdeksaatoista vuotta nuoremman henkilön ryhtymään sukupuoliyhteyteen tai muuhun

seksuaaliseen tekoon 8 a §:ssä tarkoitetulla tavalla taikka esiintymään sukupuolisiveellisyyttä loukkaavassa järjestetyssä esityksessä.

Edellä 2 momentissa tarkoitetun rikoksen yritys on rangaistava.

Korkein oikeus on käsitellyt 2004 vuonna tapausta, jossa vuonna 1949 syntynyt mies A oli 11-vuotiaalle tytölle B lähettämissään sähköpostiviesteissä käyttänyt ilmaisuja, jotka osoittivat, että hän oli pyrkinyt seksuaaliseen kanssakäymiseen tytön kanssa. A oli vastannut B:n erääseen netin kirjefrendipalstalle lähettämään viestiin. Käräjä- ja hovioikeudet olivat A:n tilanteessa tuominneet, mutta Korkein oikeus katsoi, että lapsen seksuaalinen hyväksikäyttö ei täyttynyt, koska A ei ollut saanut B:n nimi ja yhteystietoja todellista vaaraa teon toteutumiseksi ei ole aiheutunut. (KKO 2004:71.)

Helsingin hovioikeus on käsitellyt tapausta, jossa hovioikeudessa on ollut kysymys siitä, edellyttääkö lapsen seksuaalisen hyväksikäytön tunnusmerkistön toteutuminen molempien osapuolten samanaikaista läsnäoloa. Asiassa on riidatonta, että A on ollut viisi eri kertaa tietokoneeseensa yhdistetyn web-kameran kautta yhteydessä 15-vuotiaaseen H:hon. A on riisunut kameran edessä vaatteensa, näyttänyt H:lle sukupuolielimiään ja tyydyttänyt itseään kameran edessä H:n seuratessa tapahtumia kotonaan omalta tietokoneeltaan. Lisäksi A ja H ovat samanaikaisesti käyneet seksuaalisväritteistä keskustelua. Hovioikeus on päätynyt ratkaisussaan siihen, että A on syyllistynyt lapsen seksuaaliseen hyväksikäyttöön. (HelHO 2007:7.)

4.5 Luvaton käyttö

Rikoslaki 28 luku 7 § Luvaton käyttö:

Joka luvattomasti käyttää toisen irtainta omaisuutta taikka kiinteää konetta tai laitetta, on tuomittava luvattomasta käytöstä sakkoon tai vankeuteen enintään yhdeksi vuodeksi.

Yritys on rangaistava.

4.6 Pakottaminen seksuaaliseen tekoon

Rikoslaki 20luku 4 §: Pakottaminen seksuaaliseen tekoon

Joka väkivallalla tai uhkauksella pakottaa toisen ryhtymään muuhun kuin 1 §:ssä tarkoitettuun seksuaaliseen tekoon tai alistumaan sellaisen teon kohteeksi ja se olennaisesti loukkaa toisen seksuaalista itsemääräämisoikeutta, on tuomittava pakottamisesta seksuaaliseen tekoon sakkoon tai vankeuteen enintään kolmeksi vuodeksi.

Pakottamisesta seksuaaliseen tekoon tuomitaan myös se, joka käyttämällä hyväkseen sitä, että toinen tiedottomuuden, sairauden, vammaisuuden, pelkotilan tai muun avuttoman tilan takia on kykenemätön puolustamaan itseään tai muodostamaan tai ilmaisemaan tahtoaan, saa hänet ryhtymään 1 momentissa tarkoitettuun seksuaaliseen tekoon tai alistumaan sellaisen teon kohteeksi ja se olennaisesti loukkaa hänen seksuaalista itsemääräämisoikeuttaan.

Yritys on rangaistava.

4.7 Perätön vaarailmoitus

Rikoslaki 34 luku 10 § Perätön vaarailmoitus:

Joka tekee pommista, tulipalosta, merihädästä, suuronnettomuudesta tai muusta vastaavasta hädästä tai vaarasta perättömän ilmoituksen, joka on omiaan aiheuttamaan pelastus- tai turvallisuustoimen taikka pakokauhua, on tuomittava perättömästä vaarailmoituksesta sakkoon tai vankeuteen enintään yhdeksi vuodeksi.

4.8 Petos

Rikoslaki 36 luku 1 § Petos:

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.

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.

Yritys on rangaistava.

4.9 Tietomurto

Rikoslaki 38 luku 8 § Tietomurto:

Joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja, taikka sellaisen järjestelmän erikseen suojattuun osaan, on tuomittava tietomurrosta sakkoon tai vankeuteen enintään yhdeksi vuodeksi.

Tietomurrosta tuomitaan myös se, joka tietojärjestelmään tai sen osaan tunkeutumatta teknisen erikoislaitteen avulla oikeudettomasti ottaa selon 1 momentissa tarkoitetussa tietojärjestelmässä olevasta tiedosta.

Yritys on rangaistava.

Tätä pykälää sovelletaan ainoastaan tekoon, josta ei ole muualla laissa säädetty ankarampaa tai yhtä ankaraa rangaistusta.

4.10 Vahingonteko

Rikoslaki 35 luku 1 § Vahingonteko:

Joka oikeudettomasti hävittää tai vahingoittaa toisen omaisuutta, on tuomittava vahingonteosta sakkoon tai vankeuteen enintään yhdeksi vuodeksi.

Vahingonteosta tuomitaan myös se, joka toista vahingoittaakseen oikeudettomasti hävittää, turmelee, kätkee tai salaa tietovälineelle tallennetun tiedon tai muun tallennuksen.

Edellä 2 momentissa tarkoitetun vahingonteon yritys on rangaistava.

4.11 Viestintäsalaisuuden loukkaus

Rikoslaki 38 luku 3 § Viestintäsalaisuuden loukkaus:

Joka oikeudettomasti

1) avaa toiselle osoitetun kirjeen tai muun suljetun viestin taikka suojauksen murtaen hankkii tiedon sähköisesti tai muulla vastaavalla teknisellä keinolla tallennetusta, ulkopuoliselta suojatusta viestistä taikka

2) hankkii tiedon televerkossa välitettävänä olevan puhelun, sähkeen, tekstin-, kuvan- tai datasiirron taikka muun vastaavan televiestin sisällöstä taikka tällaisen

viestin lähettämisestä tai vastaanottamisesta, on tuomittava viestintäsalaisuuden loukkauksesta sakkoon tai vankeuteen enintään yhdeksi vuodeksi.

Yritys on rangaistava.

4.12 Yksityiselämää loukkaavan tiedon levittämisestä

Rikoslaki 24 luku 8 § Yksityiselämää loukkaava tiedon levittäminen:

Joka oikeudettomasti

1) joukkotiedotusvälinettä käyttämällä tai

2) muuten toimittamalla lukuisten ihmisten saataville

esittää toisen yksityiselämästä tiedon, vihjauksen tai kuvan siten, että teko on omiaan aiheuttamaan vahinkoa tai kärsimystä loukatulle taikka häneen kohdistuvaa halveksuntaa, on tuomittava yksityiselämää loukkaavasta tiedon levittämisestä sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

Yksityiselämää loukkaavana tiedon levittämisenä ei pidetä sellaisen yksityiselämää koskevan tiedon, vihjauksen tai kuvan esittämistä politiikassa, elinkeinoelämässä tai julkisessa virassa tai tehtävässä taikka näihin rinnastettavassa tehtävässä toimivasta, joka voi vaikuttaa tämän toiminnan arviointiin mainitussa tehtävässä, jos esittäminen on tarpeen yhteiskunnallisesti merkittävän asian käsittelemiseksi.

5 Esitutkinnalliset keinot ja mahdollisuudet

5.1 Rikosprosessi

Rikosprosessi on lailla säännelty menettely, jonka tarkoituksena yksittäistapauksissa on toteuttaa rangaistusvastuu. Rikosprosessia on luonnehdittu myös yksilöidyn teon rikosoikeudelliseksi selvittelyksi ja arvioimiseksi. Rikosprosessi jakaantuu neljään vaiheeseen; esitutkintaan, syyteharkintaan, oikeudenkäyntiin ja rangaistukseen ja sen täytäntöönpanoon. Tässä esityksessä keskitytään esitutkintaan. (Helminen 2012a, 16-17.)

5.2 Esitutkinta

Rikoksen esitutkinnassa poliisi selvittää onko tapahtunut rikos, missä olosuhteissa se on tapahtunut, sillä aiheutettu vahinko ja siitä saatu hyöty ja keitä asia koskee sekä muut syyteharkintaa ja

rikoksen johdosta määrättävää seuraamusta varten tarvittavat seikat. Selvityksen laatu ja laajuus ovat tapauskohtaisia ja niissä on huomioitava sekä rikosepäilyä tukeva että sitä vastaan puhuva aineisto. (Tolvanen 2011, 75.)

Poliisi on velvollinen toimittamaan esitutkinnan ilman aiheetonta viivytystä. Jokaiselle tutkittavaksi otettavalle rikosasialle poliisi nimeää tutkinnanjohtajan. Tutkinnanjohtaja vastaa tutkinnan etenemisestä. (em., 80.)

Poliisin on ilmoitettava sille tutkittavaksi tulleesta rikosasiasta myös syyttäjälle, kun jotakuta voidaan epäillä syylliseksi rikokseen. Ilmoitusta ei kuitenkaan tarvitse tehdä, jos asia on yksinkertainen. Tällaisia ovat esimerkiksi näpistys, lievä pahoinpitely tai liikenneturvallisuuden vaarantaminen. Esitutkinnan yleisistä periaatteista on säädetty esitutkintalaissa. (em., 83.)

Esitutkinta alkaa, kun esitutkintaviranomaiselle on tehty ilmoitus, jonka perusteella tai muuten on syytä epäillä rikosta. Ilmoitus voidaan tehdä henkilökohtaisesti, asiamiehen välityksellä, puhelimitse, kirjallisesti tai sähköisen rikosilmoitusjärjestelmän kautta. Lisäksi ilmoitus on voinut tulla esitutkintaviranomaisen tietoon muun tutkinnan yhteydessä. (Helminen 2012a, 261-262.)

Suurin osa rikoksista on virallisen syytteen alaisia. Tällöin esitutkinta on suoritettava, vaikka asianomistaja ei vaatisikaan rangaistusta. Myös syyttäjä saa nostaa syytteen ja on velvollinenkin nostamaan syytteen. Kun kyseessä on asianomistajarikos, on esitutkinnan toimittamisen edellytyksenä asianomistajan rangaistusvaatimus, ellei sitten ole kyse erittäin tärkeästä yleisestä edusta. (em., 298-299.)

Esitutkintatoimenpiteitä ei määritellä esitutkintalaissa. Tämä johtuu siitä, että esitutkintatoimenpiteen sisältö vaihtelee kussakin yksittäistapauksessa riippuen asiayhteydestä. Esitutkintatoimenpiteet jaotellaan taktiseen ja tekniseen tutkintaan. Taktisella tutkinnalla tarkoitetaan erilaisia toimenpiteitä rikosta koskevien tietojen hankkimiseksi, kuten tiedustelut, alustavat puhuttelut, kuulustelut ja suurin osa todistelusta. Teknistä tutkintaa on esineellisten todisteiden ja muiden ”mykkien todistajien” hyödyntämistä ja tallentamista todisteina. (em., 320.)

Kuulustelulla tarkoitetaan esitutkintaviranomaisen tekemää määrämuotoista esitutkintatoimenpidettä, jossa kuultavan henkilön suullisesti antamat relevantit tiedot kirjataan tai tallennetaan hä-

nen itsensä hyväksymässä muodossa. Kuulustelujen keskeinen funktio on selvittää, voidaanko jotakuta vastaan nostaa syyte ja kerätä tietoa muista esitutkinnassa selvitettävistä asioista. (Tolvanen 2011, 98.)

Kuulustelun yhteydessä saatuja tai muuten hankittuja kirjallisia selvityksiä voidaan käyttää todistelussa. Kirjallisella todisteella tarkoitetaan fyysistä todistuskappaletta, jonka todistusvoima liittyy todisteen sanalliseen selitykseen. Kirjallinen todiste voi olla kirjoitusta, erilaisina koodeina ja se voi olla talletettuna elektroniseen muotoon. Asiakirja on kirjallisen todisteen sijasta katselmusobjektina, kun kyse on käsialanäytteestä, kartasta, piirroksesta, valokuvista tms. (em., 162.)

Esitutkinnassa on mahdollisuus käyttää pakkokeinoja. Rikosprosessuaaliset pakkokeinot ovat toimenpiteitä, joilla puututaan yksilön lailla suojattuihin oikeushyviin rikosprosessin häiriöttömän kulun turvaamiseksi sekä saattamiseksi aineellisesti oikeaan tulokseen. Pakkokeinoja voidaan käyttää myös fyysistä pakkoa käyttäen. Pakkokeinojen käyttäminen edellyttää rikosta tai epäiltyä rikosta. Pakkokeinojen tarkoituksena on useita funktioita. Niillä turvataan rikosprosessin häiriötön kulku estämällä rikoksesta epäillyn pakeneminen. Pakkokeinoilla voidaan ottaa talteen ja varmistaa todisteita prosessin kohteena olevaan rikokseen. Pakkokeinoilla voidaan varmistaa rikoksella loukatun oikeustilan palauttaminen, jolloin puhutaan restituutiosta tai rikokseen perustuvan vahingonkorvausvaatimuksen täytäntöönpano eli reparaatio. Pakkokeinolla voidaan varmistaa rikoksen tuottaman hyödyn poisottaminen ja muiden menettämisseuraamusta eli konfiskaatiota koskevien vaateiden täytäntöönpano. Niillä voidaan myös estää rikollisen toiminnan jatkuminen. (Helminen 2012a, 659.)

Rikosprosessuaaliset pakkokeinot jaotellaan kolmeen pääryhmään. Vapauteen kohdistuvat pakkokeinot, joita ovat kiinniottaminen, nouto, pidättäminen, vangitseminen ja matkustuskielto. Muihin oikeushyviin kohdistuvia avoimia pakkokeinoja, joita ovat vakuustakavarikko, takavarikko sekä asiakirjan jäljentäminen, tutkimuspaikan tai –kohteen eristäminen, paikkaan kohdistuva etsintä ja henkilöön kohdistuva etsintä. Kolmantena ovat salaiset pakkokeinot. (em., 669-670.)

5.3 Salaisten pakkokeinojen käyttö

Salaisia pakkokeinoja ovat telekuuntelu, tietojen hankkiminen kuuntelun sijaan, televalvonta, tukiasematietojen hankkiminen, sijaintitietojen hankkiminen epäillyn tai tuomitun tavoittamiseksi, suunnitelmallinen tarkkailu, peitelty tiedonhankinta, tekninen tarkkailu, teleosoitteen tai telepääte-

laitteen yksilöintitietojen hankkiminen, peitetoiminta, valeosto, tietolähdetoiminta ja valvottu läpilasku. (Helminen 2012a, 670.)

Internetrikosten tutkinnassa tyypillisimpiä salaisia pakkokeinoja ovat televalvonta ja teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen. Salaisen pakkokeinon käytön yleisenä edellytyksenä on, että käytöllä voidaan olettaa saatavan rikoksen selvittämiseksi tarvittavia tietoja. (Tolvanen 2011, 333.)

Pakkokeinolaki 10 luku 6 § (1.1.2014 alkaen)

Televalvonta ja sen edellytykset

Televalvonnalla tarkoitetaan tunnistamistietojen hankkimista viestistä, joka on lähetetty 3 §:ssä tarkoitettuun viestintäverkkoon kytketystä teleosoitteesta tai telepäätelaitteesta taikka vastaanotettu tällaiseen osoitteeseen tai laitteeseen sekä teleosoitteen tai telepäätelaitteen sijaintitiedon hankkimista taikka teleosoitteen tai telepäätelaitteen käytön tilapäistä estämistä. Tunnistamistiedolla tarkoitetaan sähköisen viestinnän tietosuojalain 2 §:n 8 kohdassa tarkoitettua tilaajaan tai käyttäjään yhdistettävissä olevaa viestiä koskevaa tietoa, jota viestintäverkoissa käsitellään viestien siirtämiseksi, jakelemiseksi tai tarjolla pitämiseksi.

Esitutkintaviranomaiselle voidaan antaa lupa rikoksesta epäillyn hallussa olevan tai oletettavasti muuten käyttämän teleosoitteen tai telepäätelaitteen televalvontaan, kun epäiltyä on syytä epäillä:

1) rikoksesta, josta säädetty ankarin rangaistus on vähintään neljä vuotta vankeutta;

2) teleosoitetta tai telepäätelaitetta käyttäen tehdystä rikoksesta, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta;

3) seksikaupan kohteena olevan henkilön hyväksikäytöstä tai parituksesta;

4) huumausainerikoksesta;

5) terroristisessa tarkoituksessa tehtävän rikoksen valmistelusta;

6) törkeästä tulliselvitysrikoksesta;

7) törkeästä laittoman saaliin kätkemisestä;

8) panttivangin ottamisen valmistelusta; taikka

9) törkeän ryöstön valmistelusta.

Pakkokeinolaki 10 luku 7 § (1.1.2014 alkaen)

Televalvonta teleosoitteen tai telepäätelaitteen haltijan suostumuksella

Esitutkintaviranomainen saa kohdistaa televalvontaa rikoksesta epäillyn, asianomistajan, todistajan tai muun henkilön suostumuksella tämän hallinnassa olevaan teleosoitteeseen tai telepäätelaitteeseen, kun on syytä epäillä:

1) rikosta, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta;

2) rikosta, jonka johdosta teleosoite tai telepäätelaite on oikeudettomasti toisen hallussa;

3) teleosoitetta tai telepäätelaitetta käyttäen tehtyä lähestymiskiellon rikkomista, rikoslain 17 luvun 13 §:n 2 kohdassa tarkoitettua ilkivaltaa tai mainitun lain 24 luvun 1 §:n 3 kohdassa tarkoitettua kotirauhan rikkomista;

4) muuta kuin 3 kohdassa tarkoitettua teleosoitetta tai telepäätelaitetta käyttäen tehtyä rikosta; tai

5) seksikaupan kohteena olevan henkilön hyväksikäyttöä.

Jos esitutkinta koskee rikosta, jonka johdosta joku on saanut surmansa, hänen hallinnassaan olleeseen teleosoitteeseen tai telepäätelaitteeseen kohdistuva televalvonta ei edellytä surmansa saaneen oikeudenomistajien suostumusta.

Sähköisen viestinnän tietosuojalaki 6 luku 36 §:

Eräiden muiden viranomaisten tiedonsaantioikeus

Viranomaisten oikeudesta saada tunnistamistietoja rikosten ennalta estämiseksi, paljastamiseksi tai selvittämiseksi säädetään poliisilaissa, rajavartiolaissa (578/2005), henkilötietojen käsittelystä rajavartiolaitoksessa annetussa laissa (579/2005), tullilaissa (1466/1994) ja pakkokeinolaissa. (23.5.2008/343)

Tämän lain 14 a §:n perusteella säilytettäviä tietoja voivat saada palveluyrityksiltä ainoastaan viranomaiset, joilla on lain perusteella oikeus saada tiedot palveluyritykseltä. (23.5.2008/343)

3 momentti on kumottu L:lla 22.7.2011/855, joka tulee voimaan 1.1.2014. Aiempi sanamuoto kuuluu:

Poliisilla on 5 §:ssä säädetyn vaitiolovelvollisuuden estämättä oikeus saada teleyritykseltä:

1) rikoslain 16 luvun 9 a §:ssä tarkoitetun lähestymiskiellon rikkomisen, 17 luvun 13 §:n 2 kohdassa tarkoitetun ilkivallan tai 24 luvun 1 §:n 3 kohdassa tarkoitetun kotirauhan rikkomisen selvittämiseksi tarvittavia tunnistamistietoja liittymään otetuista yhteyksistä asianomistajan ja sen suostumuksella, jonka hallinnassa liittymä on; sekä (11.9.2009/686)

2) tilaajan tai päätelaitteen omistajan suostumuksella matkaviestimestä lähetettyjä viestejä koskevat tunnistamistiedot siltä osin kuin se on tarpeen sellaisen rikoksen selvittämiseksi, jonka johdosta matkaviestin tai siinä käytetty liittymä on oikeudettomasti toisen hallussa.

Edellä tässä pykälässä säädettyjen velvollisuuksien toteuttamisesta aiheutuvien kustannusten korvaamisesta säädetään viestintämarkkinalain 98 §:ssä.

Sähköisen viestinnän tietosuojalaissa on säädetty viestien luottamuksellisuudesta. Se tarkoittaa, että viestejä, tunnistamistietoja ja paikkatietoja saa käsitellä vain laissa erikseen säädettyihin tarkoituksiin. Tunnistamistietojen käytössä on yleensä kysymys viestinnän osapuolten selvittämisestä. (Helminen 2012a, 1048)

Poliisilla on rikosepäilytapauksissa oikeus saada teleyrityksiltä salaisten puhelinnumeroiden ja tietokoneiden pysyvien IP-osoitteiden lisäksi yhteyskohtaisesti muodostettavien IP-osoitteiden haltijatiedot ja matkapuhelimien päätelaitetunnisteet eli IMEI-koodit. Verkossa surffailtaessa tietokone tarvitsee IP-osoitteen. Osa näistä osoitteista on staattisia eli pysyviä ja osa on vaihtuvia eli dynaamisia. Vaihtuvissa osoitteissa IP-osoite annetaan yhteyskohtaisesti tietokoneen käyttöön. Vaihtuvissa osoitteissa on toisinaan hankalaa saada tietoon yhteyttä käyttäneen haltijatiedot. Tietojen saamisessa on tärkeää tietää yhteyden tarkka ajankohta. (Helopuro 2009, 290-293.)

6 Näkökulmia suojautumiseen internetrikollisuutta vastaan

Internetin käyttäjän joutuessa uhriksi tulee hänen pohtia tekeekö hän siitä rikosilmoituksen vai ei. Jos hän päätyy ratkaisuun, että tekee rikosilmoituksen, tulee miettiä, että millä kaikilla asioilla on merkitystä tapauksessa eli mitä seikkoja voi asiassa mahdollisesti käyttää todisteena, näyttönä rikoksesta ja näyttönä tekijää kohtaan. Se helpottaa esitutkintaviranomaisen työtä, saattaa nopeuttaa tutkintaa sekä antaa ilmoitusta tehtäessä parhaan kuvan tapahtuneesta, kun kaikki mahdollinen saatavissa oleva aineisto on käytettävissä heti. Esitutkinnan kannalta on tärkeää, että uhriksi joutunut kerää kaikki mahdolliset todisteet rikoksesta. Riippuen rikoksesta uhrin tulee toimia eritavoin eli rikoksen mukaisesti. Uhrin tulee säilyttää saamansa ja lähettämänsä viestit, ottaa ruutukopioita eli screen shotteja sivuilta, jotka saatetaan myöhemmin poistaa tai ne saattavat muuttua, pitää päiväkirjaa tapahtumista, sekä kaikki muu tapahtumaan liittyvä aineisto.

6.1 Kyber-tunkeutumiset

Kuten Järvinen (2012, 178-179) toteaa, niin haittaohjelmat pääsevät koneelle useimmiten sähköpostin ja tarkemmin sanottuna sähköpostin liitteiden kautta. Sinänsä viattomalta näyttävässä sähköpostissa voi olla liitetiedosto, jonka avaamalla samalla asentaa koneelleen haittaohjelman. Tältä välttyy, kun on tarkkaavainen sähköpostien käsittelyssä ja avaa vain tutuista lähteistä tulevia viestejä. Useat torjuntaohjelmat tunnistavat haittaohjelmia ja onnistuvat bloggaamaan ne ennen kuin ne asentuvat koneelle. Uutena ilmiönä on laittaa viesteihin linkkejä, jonka avaamalla jälleen asentaa haitta ohjelma. Myös tässä tapauksessa laadukas ja ajan tasalla oleva torjuntaohjelma voi pelastaa vahingolta.

Erittäin vakava uhka on usb-tikut. Saastunut usb-tikku voi saastuttaa koneen, eivätkä torjuntaohjelmat voi sitä joka tapauksessa estää. Siksi usb-tikkujen käytössä tulee olla erityisen varovainen. Kyber-tunkeutumisilta voi välttyä, kun käyttää tervettä järkeä ja huolehtii, että palomuuri ja virustorjunta ovat ajan tasalla.

6.2 Kyber-petokset ja -varkaudet

Internetpetokset

Internetissä tapahtuvat petokset ovat lisääntyneet radikaalisti maailmanlaajuisesti, kuten Majid (2012, 80-88) tuo esille. Niin on myös Suomessa. Suomessa tapahtuvista petoksista kansalliset petokset ovat yleisimpiä ja ne ovat useimmiten selvitettävissä. Usein petoksen tekijän jäljille päästään rahasiirtojen kautta. Esitutkintaviranomainen voi pankkitiedustelun kautta saada selville henkilön, jonka tilille rahasuoritus on mennyt. Tapaukset, joissa tekijä on ulkomailla, selvitysprosentti on erittäin heikko. Ulkomaisten tekijöiden nettiyhteyksien selvittäminen on hankalaa ja pyynnöt ulkomailta jäävät usein tuloksettomiksi. Lisäksi ulkomaiset tekijät ovat oppineet peittämään raha/tilisiirtonsa siten, ettei sitäkään kautta tekijää onnistuta selvittämään. Toinen keino selvittää huijari on IP-osoitteiden kautta, selvittää huijarin käyttämä tietokoneyhteys ja sitä kautta yhteyden haltija. Ongelmaksi tulevat ne yhteydet, jotka on tehty ns. yleisiltä koneilta, kuten kirjastoista ja internetkahviloista.

Sijoituspetokset

Sijoituspetoksissa vedotaan puhtaasti ihmisten luontaiseen ahneuteen. Petoksessa annetaan kuva, että on olemassa jotain sellaista tietoa, mitä ei kaikilla ole ja tätä tietoa hyväksi käyttämällä

voidaan tehdä tuottoisa sijoitus, kuten Majidkin (2012, 88) tuo esille. Lupaukset ovat epämääräisiä ja tarkemmin ajateltuna epärealistisia, mutta tuottoprosentti on ilmoitettu niin houkuttelevan korkeaksi, että jotkut ovat valmiita ottamaan riskin ja tekevät sijoituksen suuren voiton toivossa, vaikka sisimmässään saattavat ajatellakin, että voittoa ei tule. Lopulta käy niin, ettei tule voittoa ja sijoitettu pääomakin menetetään. Sijoituspetosten havaitsemiseen pätee vanha viisaus, että jos joku kuulostaa liian hyvältä, niin sitä se onkin.

Identiteettivarkaudet

Identiteettivarkauksilta suojautuu parhaiten terveen järjen käytöllä eli hieman miettii, mitä tietoja itsestään internetiin laittaa. Henkilötietojen antamisessa ja käyttämisessä netissä kannattaa olla huolellinen. Henkilötunnuksen loppuosaa ei tule antaa, kuten ei luottokortin numeroakaan kuin perustelluissa tapauksissa ja silloinkin varmistaa, että toimii suojatussa yhteydessä. Kuten Haasio (2013, 47) tuo esille, tietoja hankitaan tai saadaan perinteisen rikollisuuden keinoin eli kohdehenkilöä koskevista laskuista ja asiakirjoista. Tietoja saattaa löytyä anastetusta lompakosta tai kohdehenkilön roskalaatikoita penkomalla, jos roskiin on huolimattomasti laitettu itseään koskevia tietoja.

Jos henkilön nimellä on tehty väärä blogi, Facebook-profiili tai Twitter-tili, henkilö itse voi pyytää palvelun ylläpitäjältä tiedot tai sivut. Viranomaisilla ei ole valtuuksia poistattaa väärillä tiedoilla tehtyjä sivuja tai profiileja, jos palvelun ylläpitäjä ei niitä pyynnön perusteella poista.

Identiteettivarkauksilta välttyäkseen tulee tarkkailla postia ja pankin lähettämiä tiliotteita, sekä huolellisesti käsitellä henkilökohtaisia tietoja sisältävää materiaalia. Jos niitä laittaa roskiin, tulee huolehtia, että hävittää niistä kaikki henkilökohtaiset tiedot. Tänä päivänä sähköiset tiliotteet ja e-laskut ovat tulleet kansalaisten käyttöön ja ne saattavat olla jossakin määrin turvallisempia kuin paperiset dokumentit. Ainakin siihen saakka, kun tietomurtoa sähköisiin tietoihin ei tapahdu.
Netissä tieto hajautuu ja kun nettiin laitetaan jotain tietoa, sen pois saaminen voi olla mahdotonta. Siksi tulee miettiä, että mitä tietoja itsestään kannattaa nettiin laittaa. Laittaessaan nettiin tietoja itsestään, kannattaa aina muistaa, että niitä ei välttämättä saa sieltä ikinä pois. Eri sivustot pyytävät erilaisia tietoja ja usein hyvinkin laajasti henkilöä koskevaa tietoutta. Se mihin tiedot käytetään ja miten niitä käytetään, ei voi varmuudella joka tilanteessa tietää. Eri valtioissa on lainsäädäntö erilainen ja sen suhde nettiin ja nettirikollisuuteen erilainen. Se mikä on kiellettyä ja laitonta meillä, ei välttämättä ole muualla.

Perusteellinen harkinta on paikallaan, mitä itsestään haluaa julkaista avoimesti tai yksityisesti netissä. Tietylle kaveripiirille julkaistava materiaali voi olla hieman henkilökohtaisempaa, mutta silloinkaan ei voi olla varma, jääkö sähköinen tieto tuolle porukalla, vai meneekö se eteenpäin. Yleisenä ohjeena voisi olla, että älä pistä nettiin mitään sellaista yleiseen jakoon, mitä et uskaltaisi laittaa koulun tai työpaikan ilmoitustaululle.

6.3 Kyber-pornografia

Internet on pullollaan pornoa eri muodoissa. Huolestuttavaa on, että porno on nuorten ja lasten saatavilla samalla tavalla kuin aikuisillakin. Joillakin sivustoilla on rajoitteita, että sivuille on lupa mennä vain 18 vuotta täyttäneiden. Esto on kuitenkin viitteellinen, koska alaikäinenkin voi luoda profiilin, jossa hän väittää olevansa täysi-ikäinen. Lasten vanhempien tehtävänä on valistaa internetissä olevista vaaroista ja asioista, jotka eivät kuulu lapselle tai ole hyväksi lapselle. Lapsen pääsyä vahingollisille sivuille voi yrittää estää erilaisin estomäärityksin sekä internetin käyttörajoituksin kuten, että ilta- ja yöaikaan internetin käyttö on rajoitettu.

Suojatakseen lapsiaan hyväksikäytöltä, vanhempien tulisi kertoa lapsille, että internetissä tavattuihin henkilöihin tulee suhtautua varauksella ainakin siihen saakka, että varmistuu kuka on kyseessä. Kuten Haasio (2013, 76) tuo esille, että aikuiset osaavat taitavasti manipuloida lapsia ja nuoria ja saamaan heidät tekemään asioita, joita eivät muutoin tekisi. Samoin tulee korostaa, että puhelinnumeroa tai muutakaan yhteystietoa ei saa antaa tuntemattomille. Ja erityisesti, että verkossa kohdattua ihmistä ei tule lähteä tapaamaan.

6.4 Kyber-väkivalta

Internet houkuttaa helppoudellaan osaa ihmisistä purkamaan tuntojaan keskustelu- ja Chat-palstoilla. Purkaukset saattavat aiheuttaa reaktioita muissa internetissä olevissa ja tilanne saattaa ajautua intostilanteeseen ja mennä lopulta loukkaavaan kielenkäyttöön. Tai kirjoittelu voi olla suoraan johonkin tiettyyn henkilöön liittyvää negatiivista kirjoittelua.

Kuten Haasio (2013, 62) mainitsee, että internetkiusaamisesta suurin osa tapahtuu sosiaalisessa mediassa. Kiusaaminen ei ole pelkästään nuorten ongelma, vaan yhä enenemässä määrin aikuiset tekevät samaa. Joissakin palveluissa on mahdollista laittaa kiusaaja estolistalle. Kiusaajan voi ilmoittaa palvelun ylläpitäjälle ja silloin ylläpitäjä voi joskus poistaa pyynnöstä kiusaajan profiilin.

Jos kiusaaminen kohdistuu alaikäiseen ja se on jatkuvaa, tulee lapsen/nuoren keskustella vanhempiensa kanssa asiasta. Mikäli asia liittyy koulukiusaamiseen, on asiasta syytä ilmoitta koulunhenkilökunnalle ja yrittää sitä kautta löytää ratkaisu asiaan. Vanhemmat voivat toki ottaa yhteyttä suoraan kiusaajan vanhempiin.

Aikuisten kohdalla asiaa kannattaa yrittää sovitella ensin itse. Jos keskustelussa ei päästä hedelmälliseen lopputulokseen, on mahdollisuus ottaa yhteyttä nettipoliisiin. Nettipoliisi voi käydä huomauttamassa kiusaajaa, joka saattaa joissakin tilanteissa olla riittävä toimenpide. Ellei kiusaaminen edelleenkään lopu, voi asiassa tehdä rikosilmoituksen joko sähköisesti, henkilökohtaisesti poliisilaitoksella käymällä tai kirjoittamalla kirjallisen tutkintapyynnön. Asiaan liittyvät viestit on syytä säilyttää ja käyttää niitä todistusaineistona.

Monet mieltävät, että kirjoittaessaan internetissä nimimerkin suojassa tai muuten anonyymisti, voi harkitsemattomasti kirjoittaa mitä tahansa ja kenestä tahansa. Kuitenkin internetin käytöstä jää jälkiä. Jos kirjoittaminen täyttää rikoksen tunnusmerkitön ja asiassa esitutkinta aloitetaan, esitutkintaviranomainen voi saada selville kirjoittajan IP-osoitteen ja sitä kautta yhteyden haltijan tiedot palveluntuottajalta.

Yksi tämän päivän ”vitsaus” on internetissä tapahtuvat uhkaukset, joissa uhataan välillisesti suurta joukkoa. Nämä ovat tyypillisesti ns. koulu-uhkauksia. Uhkaus voi olla sanallista ja se voi olla kuva tai se voi olla vertauskuvallinen. Tyypillistä uhkauksille on, että se ei kohdennu johonkin tiettyyn henkilöön tai tiettyihin henkilöihin, vaan sen kohteena on satunnainen joukko ihmisiä. Pääosa uhkauksista on ajattelemattomuuksissaan nuorten henkilöiden tekemiä. Motiivina saattaa olla, että saisi vapaan koulupäivän tai että kokee tulleensa kaltoin kohdelluksi joltakin taholta tai jokin muu vähäinen syy. Murheellista asiassa on se, että usein kyseisenlaiset uhkaukset saavat paljon palstatilaa mediassa ja se on osaltaan ruokkimassa samanhenkisiä toteuttamaan samanlaisen tai hieman varioidun uhkauksen. Usein käykin niin, että uhkauksia tulee useampia lyhyen ajan sisällä.

Internet antaa helpon ja vaivattoman kanavan ilmaista mielipiteitään ja näkemyksiään muulle maailmalle. Haasio (2013, 110) tuo esille kirjoittelussa rasismin. Rasistinen kirjoittelu on yksi vihapuheen muoto. Vihapuheessa uhataan, panetellaan tai solvataan jonkun tai joidenkin todellista etnistä tai kansallista taustaa, uskonnollista vakaumusta tai elämänkatsomusta, seksuaalista

suuntautumista, sukupuoli-identiteettiä, sukupuolen ilmaisua tai vammaisuutta kohtaan. Jokainen terveellä järjellä ajatteleva aikuinen ihminen tietää, missä raja menee vihapuheen raja, vaikka se ei selvä olekaan. Kuitenkin tai tästä johtuen eräät haluavat tietoisesti kokeilla rajoja ja testata kuinka jyrkästi ja suoraan he voivat kirjoittaa asioista sananvapauden nimissä.

7 Lähteet

Innanen, A. &Saarimäki, J. 2012. Internetoikeus. Helsinki. Edita.

Haasio, A. 2013. Netin pimeä puoli. Saarijärvi. Saarijärven Offset Oy.

HelHO 2012:1

HelHO 2007:7

Helminen, K., Fredman, M., Kanerva, J., Tolvanen, M &Viitanen, M. 2012a. Esitutkinta ja pakkokeinot. Helsinki. Talentum.

Helminen, K., Kuusimäki, M. & Rantaeskola, S. 2012b. Poliisilaki. Helsinki. Talentum.

Helopuro, S., Perttula, J & Ristola, J. 2009. Sähköisen viestinnän tietosuoja. Helsinki. Talentum.

Holt, T. 2013. Crime on line. Correlates, Causes, and Context. Carolina. Carolina Academic Press.

Http://www.poliisi.fi/nettipoliisi 23.11.2013

Järvinen, P. 2012. Arjen tietoturva, vinkit ja ratkaisut. Saarijärvi. Saarjärven Offset Oy.

Kaleva 22.11.2013. Nettiuhkailut ovat vakavia.

KKO 2012:58

KKO 2004:71

KouHO 2012:9

Majid, Y. 2013. Cybercrime and society. Toinen painos. London. SAGE Publications Ltd.

Rikoslaki 19.12.1889/39

Tolvanen, M. & Kukkonen, R. 2011. Esitutkinta- ja pakkokeino-oikeuden perusteet. Helsinki. Talentum.

8 Liite

8.1 Vihjeitä internetin turvalliseen käyttöön

- Pidä tietoturva ajan tasalla. Päivitä palomuuri ja virustorjunta.
- Älä käytä liian helppoja salasanoja. Hyvä mitta on vähintään kahdeksan merkkiä, joista osa on erikoismerkkejä.
- Käytä eri palveluissa eri salasanoja ja vaihda niitä.
- Älä julkaise verkossa tarpeettomasti henkilötietojasi ja mieti, mitä informaatiota jaat muiden kanssa.
- Älä lataa harkitsemattomasti kuviasi internetiin.
- Kerran internetissä, aina siellä.
- Kun maksat verkossa pankki- tai luottokortilla huolehdi, että käytät salattua HTTPS-verkkoyhteyttä ja että kauppakumppani on luotettava.
- Älä koskaan anna pankkitunnuksiasi sähköpostitse.
- Älä avaa tuntemattomilta tulleita viestejä ja varsinkaan sen liitetiedostoa.
- Älä lankea liian hyviltä kuulostaviin tarjouksiin. Ilmaisia lounaita ei ole internetissäkään.
- Älä vastaa ketjukirjeisiin tai muihin sähköpostissa liikkuviin huijausyrityksiin.
- Poista evästeet ja sivuhistoria.
- Käytä yksityisyystyökaluja.
- Somessa ei tule jakaa: henkilötunnusta, syntymäpäivää, luottokorttien valokuvia, lomasuunnitelmia, kotiosoitetta, kouluja joita on käynyt, avomielisiä ajatuksia työstä tai työpaikasta, tunnustuksia päihteiden käytöstä, vihjeitä salasanoista ja vaarallisista harrastuksista.
- Käytä useampia selaimia.
- Käytä salanimiä yksityisemmissä asioissa.
- Piilota IP-osoitteesi VPN:llä (Hotspot Shield, hidemyass.com, overplay.net ja anonymizer.com) tai TOR-selaimella (http://torproject.org).
- Tarkista verkkomaineesi tekemällä hakuja hakukoneilla. Jos löytyy sellaisia hakutuloksia, joita et toivoisi olevan, voit pyytää alkuperäistä lähdettä poistamaan tiedon. Jos se ei ole mahdollista, niin ei-toivottuja hakutuloksia voi hukuttaa synnyttämällä runsaasti uutta sisältöä.
- Lisätietoa viranomaisilta osoitteista: cert.fi, tietoturvaopas.fi ja tietosuoja.fi.