VAASAN YLIOPISTO

KAUPPATIETEELLINEN TIEDEKUNTA

TALOUSOIKEUDEN YKSIKKÖ

Antti Mikola

YHTEISÖJEN TIETOJÄRJESTELMIEN TIETOTURVAN OIKEUDELLINEN SUOJA

Talousoikeuden

pro gradu –tutkielma

VAASA 2012

SISÄLLYSLUETTELO sivu

VAASAN YLIOPISTO

Kauppatieteellinen tiedekunta
Tekijä: Antti Mikola
Tutkielman nimi: Yhteisöjen tietojärjestelmien tietoturvan oikeudellinen suoja
Ohjaaja: Brita Herler
Tutkinto Kauppatieteiden maisteri
Yksikkö Talousoikeuden yksikkö
Oppiaine Talousoikeus
Linja ICT-juridiikan linja
Aloitusvuosi 2004
Valmistumisvuosi 2012 **Sivumäärä**: 75

TIIVISTELMÄ

Tietotekniikka liittyy läheisesti nykyaikaiseen yhteiskuntaan ja lähes kaikkeen toimintaan ympärillämme. Tietotekniikan lisääntymisen ja kehittymisen myötä myös tietotekniikkaan liittyvä rikollisuus on kasvanut. Tietoturva on tietojenkäsittelyn perustavia elementtejä. Se on tietoteknisten järjestelmien toimivuuden kannalta elintärkeää.

Tutkimuksen tavoitteena on selvittää, minkälaisia tietotekniikkaan liittyvät tietoturvaa loukkaavat rikokset ovat, ja miten lainsäädäntö niitä suojaa. Tutkimuksessa kuvataan myös lainsäädännön kehittyminen alkaen kansainvälisestä yhteistyöstä ja lainsäädännöstä päätyen kansalliseen lakiin. Tutkimuksessa keskitytään yhteisöjen tietojärjestelmien tietoturvaan eli tietojenkäsittelyrauhaan ja siihen liittyviin loukkauksiin.

Tutkimusongelmaa selvitetään lainopillisella eli oikeusdogmaattisella metodilla ja pääpaino tutkimuksessa on oikeussääntöjen kehittymisen ja sisällön selvittämisessä ja niiden tulkinnassa. Tutkimuksessa käydään läpi muutamia oikeustapauksia aiheen havainnollistamiseksi.

Tutkimuksessa havaittiin, että tekniikan nopea kehittyminen ja rikollisuuden kansainvälinen luonne aiheuttavat vaikeuksia lainsäädännölle. Lainsäädäntötyö vie oman aikansa, kun taas tekniikan uudet innovaatiot leviävät nopeasti, niin myös rikosten tekovälineet ja tavat. Selvää on, että myös tekniikan monimutkaistuminen vaikeuttaa lainsäädäntöä ja rikosten tutkintaa. Muita havaintoja olivat rikosten uhrien epäselvä asema joidenkin rikosten osalta lainsäädännössä.

Tietojärjestelmien tietoturva määritellään yleisesti kolmella tavoitetilalla, luottamuksellisuus, tiedon eheys ja käytettävyys. Tietojärjestelmän tietoturvaa kutsutaan oikeustieteessä myös tietojenkäsittelyrauhaksi.

AVAINSANAT:

Tietoturva, tietojenkäsittelyrauha, tietoturvaloukkaukset, tietomurto

1. JOHDANTO

Tietotekniikka eri muodoissaan kuuluu välillisesti tai välittömästi kaikkein suomalaisten elämään ja sen vaikutus kasvaa yhä edelleen, halusimme tai emme. Tietojärjestelmät yhteyksineen ja verkkoineen helpottavat elämäämme monin tavoin. Sähköposti on helppo ja nopea tapa kirjallisen viestin lähettämiseen ja lehden luku verkossa alkaa olla hyvin yleistä. Pankissa on käytävä enää harvoin, osan tarvitsemistamme hyödykkeistä voimme tilata verkkokaupasta ja joulutervehdykset voimme lähettää helposti verkossa. Nuoriso on mieltynyt sosiaalisen median eri muotoihin ja Internetin musiikkipalveluista voimme kuunnella mielikappaleemme nopeasti ja vaivattomasti.

Yrityksille toimivat tietojärjestelmät ovat toiminnan kannalta välttämättömiä. Nykysuomessa tuskin on yhtään yritystä, joka ei itse tai välillisesti käytä tietojärjestelmiä. Yritysten hallintoon tietotekniikka on kuulunut jo pitkään. Tekniikan kehittymisen myötä syntyy jatkuvasti uusia tapoja käyttää tietotekniikkaa. Kun liikkumisen hinta on energiahintojen ja työajan kallistumisen myötä noussut, yritykset käyttävät videoneuvotteluita tai etätyötä kustannustensa kurissa pitämiseksi. Järjestelmien käyttötavat laajentuvat jatkuvasti ja käytön määrä lisääntyy. Tietotekniikan avulla luodaan myös uusia liiketoimintamahdollisuuksia. Tänään voimme tuskin kuvitella mitä kaikkea tietotekniikalla voidaan kymmenen vuoden kuluttua tehdä.

Toimivien tietojärjestelmien uhkana on kuitenkin tietojärjestelmiin kohdistuva rikollisuus ja ilkivalta. Se voi olla harrastelijamaista tai ammattimaista. Molemmat tavat ja tahot vaikeuttavat yritysten ja yhteiskunnan toimintaa. Harmittomalta tuntuva ”hakkerin” pila voi aiheuttaa yritykselle mittaamattomat vahingot. Tunnussanoja kalastelevat viestit ovat jatkuvasti atk:ta käyttävälle tuttuja. Uhkia toimivalle tietotekniikalle on paljon ja valitettavasti niidenkin monimuotoisuus ja innovatiivisuus ovat kasvussa. Tämä tutkimus keskittyy kuvaamaan yhteisöjen tietojärjestelmiä uhkaavia tietotekniikkarikoksia ja järjestelmiä suojaavaa lainsäädäntöä.

1.1 Tutkimuskohteen kuvaus

Tietotekniikka on nykypäivänä olennainen osa toimivaa yhteiskuntaa. Tietotekniikan historia on lyhyt, ensimmäiset tietokoneet rakennettiin vasta 1940-luvulla. Suomeen ensimmäiset tietokoneet tulivat 1950-luvulla. 1960- ja 1970-luku olivat ns. suurkonei-

den aikaa. Koko ala alkoi muuttua voimakkaasti 1980-luvun puolivälissä, kun IBM julkaisi ensimmäisen henkilökohtaisen PC-koneensa. Samaan aikaan kehitettiin ensimmäiset standardoidut, laiteriippumattomat käyttöjärjestelmät. Näiden tapahtumien ansiosta tietokoneiden määrä lisääntyi voimakkaasti ja niissä käytettävien ohjelmien hinnat halpenivat niin, että tietokoneita ryhdyttiin hankkimaan laajasti yrityksiin ja myöhemmin myös koteihin.

1990-luvulla tietokoneiden väliset tietoverkot kokivat mullistuksen kun maailmanlaajuinen internet-verkko alkoi yleistyä. Suomessa internetin käytön lisääntymistä kuvaavat luvut; koti-internet oli 1998 n. 18 %:ssa kotitalouksista ja 2005 n. 60 %:ssa kotitalouksista (Tilastokeskus, 2006). 2000-luvulla tietoverkkojen leviäminen lähes jokaiseen talouteen toi mukanaan ns. sosiaalisen median. Viime vuosina se on levinnyt voimakkaasti lähes kaikkien suomalaisten elämään.

Tänä päivänä tietotekniikka alkaa olla osa lähes kaikkien kansalaisten arkea. Positiivisten ansioiden ja vaikutteiden sivussa on kehittynyt myös negatiivinen puoli eli tietotekniikkaan liittyvät rikokset. Esillä ovat olleet erilaiset laitteistojen toimintaa vaikeuttavat virukset. Viime aikoina laajat tietomurrot ovat olleet lehtien otsikoissa. Nämä ilmiöt, virukset ja tietomurrot, uhkaavat tietotekniikan tietoturvaa.

Kotikäyttäjälle tietotekniikan toimimattomuus on usein pelkästään harmillista. Yhteiskunnassa on nykyisin monia asioita, joiden sujuvuus riippuu tietotekniikan toimivuudesta. Toimimattomuus tai virheellinen data saattaa aiheuttaa suuria ongelmia. Lehtonen ottaa esimerkiksi tällaisesta terveydenhuollon ja ilmaliikenteen valvonnan (1999: 146). Yrityksille toimivat tietojärjestelmät ovat elinehto ja joidenkin yritysten toiminta voi pysähtyä kokonaan, kun tietojärjestelmä lopettaa toimimasta. Tietotekniikan käytön ja toimivuuden kannalta tietojärjestelmien tietoturva on oleellinen ja välttämätön asia. Tietotekniikan *tietoturva* (engl. data security) tarkoittaa tietojärjestelmien suojaamista asiattomalta muuttamiselta ja käytöltä siten, että samalla taataan tietojen eheys ja saatavuus. (Järvinen 2002: 451). Laajemmin tietoturva määritellään esimerkiksi seuraavasti. *Tietoturva* on niiden hallinnollisten, teknisten ja fyysisten toimenpiteiden kokonaisuus, jolla tietoturvallisuutta yrityksen, osaston, järjestelmän tai yksittäisen henkilön tiedoille ja niiden käsittelylle rakennetaan ja ylläpidetään. (Paananen 2001: 355).

Suomessa ei ole yhtä lakia koskien tietoturvaa tai tietotekniikkaa, vaan siihen liittyvä lainsäädäntö on hajallaan eri säännöksissä. Tietojärjestelmien rakentamisen ja ylläpidon kannalta tärkeitä lakeja ovat mm. perustuslaki, julkisuuslaki (1999/621), henkilötietola-

ki (523/1999), Laki yksityisyyden suojasta työelämässä (759/2004), sähköisen viestinnän tietosuojalaki (SVTSL 516/2004)(Laaksonen, Nevasalo, Tomula, 2006: 23). Nämä lait siis määrittävät asioita, jotka ovat huomioitava tietojärjestelmien rakentamisessa, ja niiden käytössä. Lainsäädännön yksi keskeisin asia on yksityishenkilöiden tietojen turvaaminen. Tietoturvan loukkauksista taas säädetään kokonaisuutena rikoslaissa.

Tässä tutkimuksessa keskitytään selvittämään tietojärjestelmien tietoturvaan kohdistuvia loukkauksia ja loukkauksiin liittyvää lainsäädäntöä. Tietotekniikassa tietoturva jaetaan perinteellisesti kolmeen erilliseen osaan tai ominaisuuteen. Esimerkiksi Valtioneuvoston periaatepäätöksessä tietoturvallisuuden kehittämisessä valtiohallinnossa, määritellään edellä mainitut kolme peruskäsitettä seuraavasti.

1. Luottamuksellisuus; tiedot ovat vain niiden käyttöön oikeutettujen saatavissa eikä niitä paljasteta tai muutoin saateta sivullisten käyttöön.
2. Eheys; tiedot ja järjestelmät ovat luotettavia, oikeellisia ja ajantasaisia eivätkä ne ole laitteisto- ja ohjelmistovikojen, luonnontapahtumien tai oikeudettomien inhimillisen toiminnan seurauksena muuttuneet tai tuhoutuneet
3. Käytettävyys; järjestelmien tiedot ja muodostamat palvelut ovat tarvittaessa niihin oikeutettujen käytettävissä.

(Valtiovarainministeriö, 1999: 3)

Jako on ollut tekniikan kirjallisuudessa käytössä jo pitkään. Tuomas Pöysti yhdistää tekniikkaan perustuvan kolmijaon lainsäädäntöön. Näitä kolmea peruselementtiä käytetään niin teknisessä kuin oikeustieteellisessä keskustelussa (Pöysti 2001: 5). Tämä jako on varsin yleisesti hyväksytty lähtökohta.

Nykyisin lähes kaikkien suomalaisten arkipäivään kuuluu tietotekniikka ja laajentuneen käytön myötä mukaan tulee alaan liittyvä rikollisuus. Kaikki tietotekniikkaan liittyvät rikokset eivät suinkaan ole tietotekniikkarikoksia. Tietokoneen varastaminen ”pelkkänä koneena” ei esimerkiksi ole tietotekniikkarikos, vaan varkaus. Seuraavassa määritelmä, joka valaisee käsitettä tietotekniikkarikos.

Tietotekniikkarikos on rangaistava teko, jonka kohteena, välikappaleena tai tekoympäristönä on tietojärjestelmä siihen kuuluvine laitteineen ja jonka tekeminen ja/tai rikosprosessuaalinen käsitteleminen edellyttää tietoteknistä tietämystä. (Pihlajamäki 2004: 48).

Tietoturvaa kutsutaan oikeustieteen puolella myös toisella nimellä. Aikaisemmin määriteltyä tietoturvaa kutsutaan oikeustieteen kirjallisuudessa myös tietojenkäsittelyrauhaksi. Tietojenkäsittelyrauha on sisällöltään teknisesti sama asia kuin tietoturva. Seuraava määritelmä liittää sen myös tietotekniikkarikokseen.

Tietotekniikkarikosten määritelmän mukaisilla teoilla on havaittavissa yksi yhteinen nimittäjä: koska niiden kohteena, välikappaleena tai tekoympäristönä on tietojärjestelmä siihen kuuluvine laitteineen, ne kaikki loukkaavat luonteeltaan jossain määrin kotirauhaan rinnastettavissa olevaa niin sanottua *tietojenkäsittelyrauhaa*, josta on käytetty myös nimitystä *pax computations*. (Pihlajamäki 2004: 55).

Tietotekniikkarikokset ovat vaikeasti konkretisoitavia ja vaativat mielestäni selventävän kuvauksen ja esimerkkejä asioiden yksiselitteisyyden tueksi. Rikosten luonteesta saa parhaiten käsityksen, kun tarkastellaan erilaisia tietotekniikkarikosten jaotteluita. Ne paljastavat näkökulman ja sitä kautta rikosten luonteen. Kun tietotekniikkarikoksia alettiin tutkia reilu kolmekymmentä vuotta sitten, nimettiin rikokset sen ajan tavan mukaan seuraavasti. Petos, joka tehdään tietokoneella, on tietotekniikkapetos. Väärennös johon käytettiin tietotekniikkaa, on tietotekniikkaväärennys jne. Loogisemmat jaottelut syntyivät myöhemmin. Alettiin puhua esimerkiksi tietojärjestelmään murtautumisesta tai dataan kohdistuvista rikoksista, ja sekä siitä mitkä rikosnimikkeet liittyvät datan muuttamiseen tai tuhoamiseen.

Seuraavassa käsitellään muutamia erilaisia rikosten jakotapoja. Niistä selviää paremmin mistä on kyse. Euroopan Yhteisöjen Komissio antoi vuonna 2002 ehdotuksen Neuvoston puitepäätökseksi. Komissio julkaisi samassa esityksessä tietotekniikkarikoksista seuraavan jaon. Rikoslajit olivat; 1) tietojärjestelmään murtautuminen 2) tietojärjestelmän häirintä 3) tietoja ilkivaltaisesti muuttavat tai tuhoavat ohjelmat 4) telekuuntelu 5) naamioituminen. (Euroopan Yhteisöjen Komissio 2002: 2-3). Jako on aika pelkistetty ja varsinkin viimeinen kohta on melko harvoin käytetty.

Euroopan Yhteisöjen komission jako on siis listan alkukohdiltaan aikaisemmin esitetyn Valtioneuvoston jaon kaltainen. Ensimmäisenä on tietojärjestelmään murtautuminen eli luottamuksellisuuden rikkominen. Tietoa muuttavat ja/tai tuhoavat rikokset kohdistuvat eheyteen ja tietojärjestelmän häirintä käytettävyyteen.

Asko Lehtonen jaottelee tietotekniikkarikoksia Informaatio- ja tietotekniikkaoikeuden luentosarjassa seuraavasti, pääjako on varallisuuteen kohdistuvat ICT-rikokset ja tiedon

integriteettiin (vahingonteko) kohdistuvat rikokset (Lehtonen, 2009: 60, 90). Näkökulma on siis mitä tiedolle tehdään, hyödynnetään vai tuhotaan. Esitykseen liittyvä tarkempi jaottelu on hienojakoinen, erilaisia rikoksia on lueteltu n. 20 kappaletta).

Seuraavassa Pihlajamäen esittelemä jako, joka on tietoturvan perusjako, luottamuksellisuus, eheys ja käytettävyys, ja tämän esityksen kannalta loogisempi ja selvempi. Jaossa hän yhdistää useat rikosnimikkeet tietoturvan perusjakoon.

Tietomurto kohdistuu tietojenkäsittelyn luottamuksellisuutta kohtaan. Tiedot ovat tarkoitettu vain niiden käyttöön oikeutettujen saatavissa. *Yritysvakoilu* on tietomurto vietynä pidemmälle, tunkeutumisen jälkeen seuraa tietojen hyväksikäyttöä. *Luvaton käyttö* on myös rikos luottamuksellisuutta kohtaan, teko ei edellytä tietojen käyttöä, pelkkä tunkeutuminen järjestelmään riittää. (Pihlajamäki, 2004: 121).

Tietojenkäsittelypetos, tietotekninen väärennys ja tietovahingon aiheuttaminen puolestaan ovat tekoja, jotka suoranaisesti kohdistuvat tietojärjestelmien dataan ja vaikuttavat myös datan edustaman informaation sisältöön. (Pihlajamäki, 2004: 121). Tämä ryhmä koskee siis tietojen eheyttä.

*Palvelunestohyökkäykse*t ovat tyypillisiä käytettävyyttä haittaavia rikollisia toimia. Niissä järjestelmä ”tukehdutetaan” suurella määrällä yhteydenottoyrityksiä. Monestikaan ”uhrin” tietojärjestelmään ei tarvitse murtautua, estetään vain varsinaisten käyttäjien pääsy järjestelmään. Usein myös yhteydenottoyrityksiin on valjastettu tietokoneita joiden omistajat eivät edes tiedä, että heidän järjestelmänsä osallistuu rikolliseen toimintaa. Näissä tapauksissa rikokseen liittyy vielä luvaton käyttö. Jos palvelunestohyökkäykset toteutetaan rikoksentekijöiden omilta tietojärjestelmiltä, nämä rikokset kohdistuvat silloin pelkästään käytettävyyteen

Kolmanteen kategoriaan, eli käytettävyyteen, Pihlajamäki nostaa vielä rikosnimikkeistä vaaran aiheuttamisen tietojenkäsittelylle. Se ei kuitenkaan ole yhtä yksiselitteinen asia kuin aikaisemmin mainitut rikosnimikkeet. *Vaaran aiheuttaminen tietojenkäsittelylle* poikkeaa luonteeltaan muista tässä mainituista teoista, sillä rikos voi täyttyä, vaikkei sen kohteena olevaan tietojenkäsittelyyn olisi vielä varsinaisesti millään tavoin puututtu. Tällainen teko on esimerkiksi palveluestohyökkäys. Toisaalta sitten säännöksessä tarkoitettu vahingollinen tai haitallinen ohjelma tai ohjelmakäskyjen sarja, saattaa joutuessaan kosketuksiin tietojenkäsittelyn kanssa luonteestaan riippuen, loukata kaikkia tietoturvallisuuden elementtejä, joskin ensisijaisesti mahdollinen loukkaus kohdistuu tietojen

eheyteen ja käytettävyyteen. Tästä esimerkkinä Pihlajamäki ottaa esille niin sanotun virusohjelman. (Pihlajamäki, 2004: 121-122). Viimeisenä rikosnimikkeenä käsitellään *tietojärjestelmän häirintä*. Se on otettu mukaan rikoslakiin vasta 2007. Tietojärjestelmän häirintä on myös yleensä tietojärjestelmän käytettävyyteen kohdistuva rikos.

1.2 Tutkimusongelma ja sen rajaus

Tutkimuksessa tarkastellaan yhteisöjen tietojärjestelmien kohdistuvia loukkauksia, niihin liittyvää lainsäädäntöä ja niiden seurauksia. Suomen lainsäädännöstä tuodaan esiin vain yhteisöjen tietojenkäsittelyrauhaan liittyviä loukkauksia koskevat säännökset. Lainsäädännön kehittyminen ja historia käydään lyhyesti läpi. Lainsäädännössä keskitytään rikoslain säännöksiin. Kaikissa rikoksissa, myös tietotekniikkarikoksissa oleellinen, pakkokeinolaki ja sen kehittyminen jätetään tutkielman ulkopuolelle. Siihen on tietotekniikan osalta tehty paljon muutoksia 2000-luvulla, todistusaineiston takavarikointia, salakuuntelua yms. liittyen. Se jätetään kuitenkin kokonaisuudessaan ajan ja tiedon määrän hallitsemiseksi tutkielman ulkopuolelle.

Tutkimusongelma on tiivistetysti sanottuna, selvittää minkälainen on Suomessa tehty tietotekniikkarikos ja mitä siitä oikeudellisessa mielessä seuraa. Mihin rikoksilla pyritään ja mitkä ovat rikosten tunnusmerkit. Lisäksi käsitellään myös rangaistuksia ja näyttökysymyksiä ja muita vastuukysymyksiä. Edelleen käsitellään vahingonkorvauskysymyksiä, koska ne ovat oleellisia tämän tyyppisissä rikoksissa.

Tutkimuksessa selvitetään myös esimerkkien avulla, miten hyvin nykylainsäädäntö toimii näissä rikoksissa. Oikeustapausten ja oikeuskirjallisuuden avulla selvitetään, mitä mahdollisia ongelmakohtia lainsäädännössä on ja miten lainsäädäntöä voitaisiin kehittää. Työn yhtenä ajatuksena on ymmärtää sekä tietotekniikan tarpeet ja ominaisuudet sekä niiden yhteensovittaminen oikeustieteen kanssa.

Kansainvälistä yhteistyötä lainsäädännön kehittämiseksi käydään läpi melko laajasti kokonaiskuvan saamiseksi lähihistoriasta. Yhteistyö ja erilaiset kansainvälisten järjestöjen raportit kuvaavat hyvin tietotekniikkarikollisuuden kehittymistä ja lainsäädännön reagoimista siihen. Tutkimusongelmaa selvitetään lainopillisella eli oikeusdogmaattisella metodilla ja pääpaino tutkimuksessa on oikeussääntöjen sisällön selvittämisessä ja tulkinnassa.

1.3 Tutkimuksen lähteet

Suomessa on lähdetty siitä, että erillisiä tietotekniikkarikoksia koskevaa lainsäädäntöä ei luoda. Rikoksia koskeva säännöstö on normaalin muun lain yhteydessä. Pääosin tietotekniikkarikoksista säädetään rikoslaissa. Tutkimuksessa hyödynnetään rikoslain tietotekniikkarikoksia koskevia lukuja ja lakien esitöitä, pääasiassa hallituksen esityksiä. Varsinainen lakiteksti on lain soveltamisen kannalta usein hyvin niukka ja lain merkityksen ymmärtäminen vaatii esitöiden huomioimista. Esitöistä käsitellään hallituksen esitykset.

Peruslähdeaineistona käytetään alan kirjallisuutta ja aiheesta tehtyjä opinnäytteitä ja väitöskirjoja. Niitä on tietotekniikkarikoksista tehty Suomessa joitakin. Joissakin kohdissa tietolähteenä ovat alan ammattilehdissä olevat artikkelit. Jonkun verran käytetään myös atk-tekniikkaan liittyviä perusteoksia.

Kansainvälisen yhteistyön ja kansainvälisen oikeuskäytännön kehittymisen osuuteen käytetään erilaisten kansainvälisten järjestöjen selvitystöitä ja niiden julkaisemia lainsäädäntösuosituksia sisältäviä raportteja. Tätä työtä järjestöt tekivät voimakkaimmin 1980- ja 1990-luvulla. Kyseessä olevia järjestöjä ovat mm. OECD, Euroopan Neuvosto, YK ja Euroopan Unioni.

Otan esiin myös muutaman oikeustapauksen. Suomessa tietotekniikkarikokset ja erityisesti tietomurrot päätyvät harvoin oikeuteen, mutta muutamia laajasti käsiteltyjä tapauksia on olemassa. Niiden lisäksi esillä on myös muutamia uusia tapauksia, joiden ansiona ovat niiden linjaa luovat ratkaisut. Joidenkin oikeustapausten ongelmana on niiden ikä, uusia oikeustapauksia on harvoja ja tietotekniikkarikosten ollessa kyseessä, maailma muuttuu nopealla vauhdilla. Uusien oikeustapausten niukkuuden takia esityksessä käydään läpi myös käräjäoikeuden ratkaisuja.

1.4 Tutkimuksen rakenne ja eteneminen

Tutkimuksen johdannossa esittelen tutkimuksessa käsiteltävää aihealuetta yleisesti. Siinä määritellään tutkimuksen kannalta keskeiset termit ja kerron tutkimuksen tavoitteet ja rajaukset. Jonkun verran tuon esiin aihealueen, tietoturvan ja sen loukkausten, vaikutuksia käytännön elämässä. Sitten esitän, kuinka tutkimuksessa on hyödynnetty lähteitä.

Johdannossa kerron myös, minkälainen on tutkimuksen rakenne ja kuinka tutkimus etenee.

Toisessa pääluvussa käydään läpi tietotekniikkaan liittyvän lainsäädännön kansainvälisen yhteistyön historia. Eri organisaatioiden työtä lainsäädännön kehittämiseksi käydään läpi melko laajasti. Eri raporttien ja suositusyhteenvetojen kautta pyrin antamaan kuvan siitä, kuinka tietotekniikkarikollisuuteen on alettu reagoida. Melko nopeasti, alun hieman hapuilevista raporteista ja perusasioista, on päästy selkeämpiin kannanottoihin ja yksityiskohtaisempaan käsittelyyn. Kansainvälisessä osassa tietotekniikkaa koskevaa lainsäädäntöä käsitellään kokonaisuudessaan, siinä ei rajoituta pelkästään tutkielman ydinkohtiin, järjestelmien tietoturvaan ja niiden alakohtiin. Ensimmäisten raporttien kannanottojen yleisyydestä johtuen se olisi käytännössäkin ollut mahdotonta. Toisen luvun lopussa kerrotaan miten kansainvälinen yhteistyö on vaikuttanut Suomen lainsäädäntöön.

Kolmannessa luvussa alussa käsitellään Suomen tietotekniikkaan liittyvät lainsäädännön kehittymistä. Sitten keskitytään yksi kerrallaan erillisiin rikosnimikkeisiin. Aluksi käydään läpi luottamuksellisuuteen liittyvät tietomurto, yritysvakoilu ja luvaton käyttö. Kolmannessa kappaleessa esitetään myös poliisin tilastoja rikosten määristä. Tilastoista selviää kuinka rikoksia on 2000-luvulla tullut poliisin tietoisuuteen. Sen jälkeen paneudutaan kolmeen luottamuksellisuuteen kohdistuvaan rikosnimikkeeseen, niitä koskeviin säädöksiin, niiden vaiheisiin, peruslakitekstiin ja lainvalmistelutyön materiaaliin, pääosin hallituksen esityksiin. Kahdesta rikosnimikkeestä, tietomurrosta ja luvattomasta käytöstä, käydään esimerkin avulla läpi käytäntöä. Yritysvakoilusta on lyhyesti esitettävän esimerkin löytäminen vaikeaa.

Seuraavassa kappaleessa käydään läpi tietojen eheyteen liittyvät rikosnimikkeet. Ne ovat tietojenkäsittelypetos, maksuvälinepetos, tietotekninen väärennys. Viidennessä kappaleessa käydään läpi tietojärjestelmän käytettävyyteen liittyvät rikosnimikkeet, vaaraan aiheuttamien tietojen käsittelylle, vahingonteko ja vielä viimeisenä lainsäädäntöön tullut tietojärjestelmän häirintä

Tiedon eheyteen ja käytettävyyteen liittyy useasti erilaisilla haittaohjelmilla tehnyt rikokset. Siksi haittaohjelmat ja niiden käyttötavat käydään lyhyesti läpi neljännen luvun alussa. Tarkoituksena on esitellä ohjelmatyypit ja käyttötarkoitukset siten, että luvun loppupuolella esitetyt rikokset ja niiden toteutus olisi helpompi ymmärtää. Haittaohjelmat ovat usein rikollisten työkaluja rikosten tekemisessä. Niitä käytetään usein kun ky-

symyksessä ovat väärennys, petos, maksuvälinepetos, vahingonteko, vaaran aiheuttaminen tietojenkäsittelylle tai tietojärjestelmän häirintä. Esityksessä haittaohjelmista ei pyritä kattavaan esitykseen vaan tiiviiseen perusasioiden kuvaamiseen.

Kappaleessa 6 käsitellään tulossa olevaa tietotekniikkaan ja tietoturvallisuuteen liittyvää direktiiviä. Ehdotus tulevasta direktiivistä on annettu 2010. Lopullinen direktiivi lienee valmis 2013.

Tutkimuksen viimeisessä luvussa tarkastellaan yhteenvetona tutkimusongelman ja tehtävän asioita ja esitetään mahdollisia parannuksia nykykäytäntöihin.

2. KANSAINVÄLINEN YHTEISTYÖ

Tietotekniikan kehittyminen 1970-luvun puolivälissä ja henkilökohtaisen tietokoneen kehittäminen, mullisti koko tietotekniikka-alan ja sai aikaan suuria muutoksia myös yhteiskunnassa. Mikrotietokoneen käyttöönotto vaikutti koko läntiseen maailmaan hyvin samanaikaisesti. Yhdysvallat oli teknisesti hieman edellä muita, mutta koko Länsi-Eurooppa koki muutoksen samanaikaisesti. Muutos kaikkine mahdollisuuksineen ja lieveilmiöineen ei jäänyt huomaamatta myöskään kansainvälisiltä yhteistyöorganisaatioilta. 1980-luvulta lähtien on tietotekniikkarikoksiin liittyvää tutkimustyötä tehty useissa kansainvälisissä organisaatioissa ja järjestöissä. Seuraavassa käydään läpi merkittävimpien järjestöjen ja niiden julkaisemien raporttien keskeistä sisältöä. Näiden esitysten perusteella voidaan nähdä miten tietoisuus tietotekniikkaa uhkaavista vaaroista huomattiin Euroopassa. Ajan kuluessa voidaan nähdä myös raporttien sisällön kehittyminen tiedon ja kokemuksen kasvaessa.

2.1 Kansainvälinen yhteistyö lainsäädännön perustana

Tietotekniikkarikoksissa ja tietotekniikkarikoksiin liittyvässä lainsäädännössä kansainvälisen yhteistyön merkitys on rikollisuuden kansainvälisen luonteen vuoksi erityisen tärkeää. Erilaisilla suosituksilla ja sopimuksilla on pyritty saamaan lainsäädäntö eri maissa samansuuntaiseksi, mutta omat lainsäädännön piirteet huomioivaksi. Pihlajamäki jakaa kirjassaan kansainvälisen kriminaalipolitiikan kovaan arsenaaliin ja pehmeään arsenaaliin. Tietotekniikkarikollisuus liittyy pehmeään arsenaaliin. Hän perustelee kirjassaan, että pehmeä lähestymistapa sopii paremmin kansainväliseen yhteistyöhön. Hän esittää kannassaan, että tietotekniikkaan liittyvät rikokset ovat usein tietotekniikan avulla suoritettuja vanhojen rikosten uusia muotoja. Näin kansallisissa lainsäädännöissä on tavallaan jo pohja uusien rikosten lainsäädännölle. Näin saattoikin tilanne olla n. 10-20 vuotta sitten. Nyt kuitenkin tietotekniikkarikoksissa on tekoja, jotka ovat tyypillisiä vain tietotekniikan avulla toteutettuna. Siinä mielessä asiat ovat jonkun verran muuttuneet. Hän kuvaa tuon aikaista tilannetta ja tapaa toimia seuraavasti:

> Huomattavasti helpompaa on antaa suosituksia ja ohjeita, joissa määritellään suuntaviivat tarpeellisille kriminalisoinneille ja annetaan niille jokseenkin yleinen sisältö – epäkohdaksi jää tällöin kuitenkin se, että suositusten noudattaminen ei perustu muuhun kuin moraaliseen tai poliittiseen sitovuuteen.

> Tietotekniikkarikoksia koskevan kansainvälisen yhteistyön tärkeimmäksi tavoitteeksi on noussut eri valtioissa voimassa olevan kansallisen rikoslainsäädännön saattaminen mahdollisimman yhdenmukaiseksi niin, että samantapaiset menettelyt olisivat kriminalisoitu. (Pihlajamäki, 2004: 62)

Kansainvälinen osuuden aluksi käydään läpi OECD:n eli Taloudellisen yhteistyön ja kehityksen järjestön tekemä raportti. Sen jälkeen kerrotaan Euroopan Neuvoston kahdesta raportista ja lyhyesti Yhdistyneiden kansakuntien ja Euroopan Unionin tekemistä raporteista. Lopuksi käsitellään yhteistyön vaikutusta Suomen lainsäädäntöön.

2.2 Taloudellisen yhteistyön ja kehityksen järjestö (OECD)

Taloudellisen yhteistyön ja kehityksen järjestö, OECD, perustettiin vuonna 1961 harmonisoimaan ja kehittämään jäsenmaidensa talouskasvua ja vapaakauppaa sekä lisäämään yhteiskunnallista hyvinvointia. OECD jatkoi 1948 perustetun Euroopan taloudellisen yhteistyöjärjestön, OEEC:n toimintaa. Siihen kuuluu 34 jäsenvaltiota, lähinnä Länsi-Euroopasta ja Pohjois- ja Väli-Amerikasta. (OECD 2011)

OECD asetti vuonna 1984 asiantuntijaryhmän selvittämään jäsenmaiden rikoslainsäädäntöä tietotekniikkarikosten osalta. Työryhmän laatima raportti julkaistiin vuonna 1986 ja on nimeltään Computer-related Crime: Analysis of Legal Policy. Kyseessä on ensimmäinen laajamittain hanke tietotekniikan alalta. (Pihlajamäki 2004: 64—65)

Raportin pääasiallisena tavoitteena oli antaa jäsenmaille ohjeita ja suosituksia tietotekniikkarikosten varalle. Raportissa selvitettiin myös kaikkien jäsenmaiden tietotekniikkaan liittyvän lainsäädännön tila. Selvityksen perusteella maat jaettiin kahteen ryhmään, niihin joissa nykyinen lainsäädäntö on riittävä ja niihin joissa lainsäädäntöä on kehitettävä. Tuon raportin mukaan valtaosa jäsenmaista kuului ryhmään, jossa ei siinä vaiheessa edellytetä lainsäädännön kehittämistoimenpiteitä.

Varsinaisesti raportissa ei määritelty tietotekniikkarikosta tarkasti, mutta luokiteltiin ja kuvattiin yleisimmät mahdolliset rikokset viiteen eri kategoriaan. Luettelo on seuraava:

a) Sellainen tahallinen datan ja/tai ohjelmiston syöttäminen, muuttaminen, hävittäminen ja/tai käytön estäminen, jonka tarkoituksena on saada aikaan rahan tai muun varallisuuden laiton siirtyminen;

b) Sellainen tahallinen datan ja/tai ohjelmiston syöttäminen, muuttaminen, hävittäminen ja/tai käytön estäminen, jonka tarkoituksena on väärennys;
c) Sellainen tahallinen datan ja/tai ohjelmiston syöttäminen, muuttaminen, hävittäminen ja/tai käytön estäminen taikka muu tietojärjestelmään puuttuminen, jonka tarkoituksena on estää tietokone- tai televiestintäjärjestelmän toiminta;
d) Sellainen suojatun tietokoneohjelman haltijan yksinoikeuden loukkaaminen, jonka tarkoituksena on hyödyntää ohjelmaa kaupallisesti ja saattaa se markkinoille;
e) Sellainen tietoinen ja tietokone- ja/tai televiestintäjärjestelmästä vastaavan henkilön luvatta tapahtunut tunkeutuminen järjestelmään, joka on tehty joko (i) turvajärjestelyjä murtamalla tai (ii) muuten petollisesti taikka vahingontuottamistarkoituksessa.

(Pihlajamäki, 2004: 67)

Näitä erilaisia rikoksia sitten vertailtiin eri maiden lainsääntöön. Tekniikka oli siis varsin yksinkertainen mutta selkeä. Tässä vaiheessa Suomessa ei lainsäädäntöön ollut tehty vielä mitään nimenomaisesti tietotekniikkarikoksia huomioivaa. Kysymykset koskivat siis laajasti tietoturvaan kohdistuvia toimia. Kohta d liittyi tekijänoikeusasioihin. OECD:n ansiot tässä raportissa olivat raportin oikea-aikaisuus.

OECD tekee jatkuvasti työtä tietotekniikkarikollisuuden ehkäisemiseksi ja lainsäädännön hyväksi. Seuraavan mainittavan suosituksen se antoi sähköiseen kaupankäyntiin. Suositus julkaistiin v. 2000 nimellä Guidelines for Consumer Protection in the Context of Electronic Commerce. Suosituksen lähtökohta oli, että sähköisen kaupan asiakkaalla pitää olla sama turva kuin perinteellisen kaupan asiakkaalla. (OECD 2011)

2.3 Euroopan Neuvosto

Euroopan vanhin ja laajin poliittinen yhteistyö- ja ihmisoikeusjärjestö on Euroopan neuvosto. Se on perustettu 1949 ns. Lontoon sopimuksella ja se koostuu nykyisin 47 jäsenvaltiosta. Neuvoston tehtävänä on edistää jäsenmaidensa yhtenäisyyttä, suojella ihmisoikeuksia ja moniarvoista demokratiaa, parantaa elinolosuhteita sekä edistää inhimillisiä arvoja. Euroopan neuvosto on työskennellyt atk-kysymysten parissa jo 1980-luvun alusta alkaen. Se antoi suosituksen henkilötietojen käsittelystä tietojärjestelmistä jo 1981. Seuraavat kaksi suositusta olivat sitten laajoja ja merkittäviä. (Council of Europe 2011)

2.3.1 Recommendation No. R(89)9

Lähes samanaikaisesti OECD:n kanssa, vuonna 1985, myös Euroopan neuvosto asetti asiantuntijakomitean miettimään tietotekniikan kehitystä ja sen merkitystä jäsenmaiden lainsäädännölle. Asiantuntijaryhmän julkaiseman raportin nimi oli "Recommendation No. R(89)9 on Computer-related Crime and Final Report of the European Committee on Crime Problems". Raportti julkaistiin 1990. Komitean tavoitteet olivat i) analysoida aikaisempien tutkimusten valossa tietotekniikkarikollisuuden eri muotoja, ii) tutkia, missä laajuudessa lainsäädäntöön tulisi sisällyttää tällaisen rikollisuuden uusia muotoja, iii) tutkia, miten laajalti eurooppalaiset yleissopimukset rikosoikeuden alalla mahdollistavat taistelun uusimuotoista rikollisuutta vastaan ja laatia näistä asioista raportti (Pihlajamäki 2004: 68).

Raportin englanninkielinen versio 115 sivua pitkä ja se jakaantuu viiteen osaan 1. Yleiset kysymykset, 2. ohjeita kansalliseen lainsäädäntöön, 3. prosessuaaliset lakiongelmat, 4. kansainvälinen näkökulma ja 5. muita näkökohtia atk-rikollisuuteen.

Asiantuntijakomissiossa käytiin pitkään keskustelua siitä pitääkö lainsäädännön lähtökohtana olla erillinen atk-rikollisuuteen keskittyvät lait vai korjataanko nykyistä lainsäädäntöä vastaamaan uuden tekniikan tuomiin haasteisiin. Komitean suositus oli, että nykyistä lainsäädäntöä korjataan ja tästä tuli Suomenkin lainsäädäntötekniikan lähtökohta.

Lauri Lehtimaja oli mukana atk-rikoskomiteassa ja hän kertoi kuinka vastakkain olivat kaksi eri tapaa suhtautua atk-rikollisuuteen. Toisen kannan mukaan tulisi laatia erillisiä atk-rikollisuuden lakeja ja toisen kannan mukaan nykyisen lainsäädännön kehittäminen riittäisi. Komiteassa linja, jossa atk:n katsottiin vain olevan uusi ilmiö, joka oli luonut eräitä uusia rikoksentekomahdollisuuksia, tuli valituksi etenemistavaksi ja lainsäädännön kehittämispohjaksi otettiin nykyinen lainsäädäntö. (Lehtimaja, 1989)

Raportissa annetaan suosituksia kansallisille lainsäätäjille. Suositukset oli jaettu kahteen ryhmään, minimisuosituksiin ja valinnaislistaan. Minimisuositukset esitetään tässä lyhyen listan muodossa; (Council of Europe, 1990: 5, 36–59)

1. Tietokonepetos.
2. Tietokonevääreennys.
3. Datan tai ohjelmiston vahingoittaminen.

4. Tietokonesabotaasi.
5. Luvaton järjestelmään tunkeutuminen.
6. Luvaton viestin sieppaaminen
7. Luvaton kappaleiden valmistaminen suojatusta tietokoneohjelmasta.
8. Luvaton kappaleiden valmistaminen integroidun piirin piirimallista.

Listan esimerkkirikokset kuvaavat ensimmäisten raporttien tapaa käsitellä tietotekniikkaan liittyviä rikoksia. Malli ja nimikkeet otettiin totutuista rikoksista, siis ilman tietotekniikkaakin toteutetuista, tai niistä rikoksista joita on tuona aikana tehty. Jos tämän hetkisen näkemyksen mukaan arvioi listaa, voidaan lähteä aluksi jaosta, jossa neljä ensimmäistä kohtaa liittyvät olemassa olevan datan tai tiedon muuttamiseen jollain tavalla. Viides kohta sisältää vain järjestelmään tunkeutumisen eli tietomurron. Kohdat 7 ja 8 taas liittyvät olemassa olevien tuotteiden kopioimiseen. Näin kuvattuna listan rikokset olivat kuitenkin varmaankin helpommin ymmärrettävissä.

Valinnaislistalla on neljä tekomuotoa, atk-ohjelman tai datan oikeudeton muuttaminen, taloudelliseen hyötyyn tähtäävä tietokonevakoilu, tietokoneen luvaton käyttö ja siihen aikaan yleinen luvaton tietokoneohjelmien kopiointi ja niiden myynti.

Kolmannessa luvussa komissio ottaa kantaa myös prosessioikeudellisiin kysymyksiin. Yleisesti tuodaan esille prosessuaalisen lain kehittymättömyys suurimmassa osassa maita, vain muutamassa maassa asiat on komission mielestä hyvin. Tarkennettuna esille nousivat kolme erillistä tarkastelunäkökulmaa tai kohtaa; pakkokeinot todistusten saamiseksi, rikosprosessissa kerättävien henkilötietoihin liittyvät asiat ja tietoteknisten todistusaineiston hyväksyttävyys tuomioistuimissa (Council of Europe, 1990:70). Yhteenvetona Komissio suosittelee näiden asioiden huomioimista lainsäädännön kehittämisessä (Council of Europe, 1990:71).

Neljännessä luvussa Komissio tuo uudelleen esiin tietotekniikkarikosten kansainvälisen luonteen (transfrontier character) ja suosittaa lainsäädännön yhtenäistämistä tutkinnan helpottamiseksi ja sellaisten yhteistyösopimusten tekoa, jotka tehostavat ja auttavat rikostutkintaa.

Tämän lisäksi erilliskysymyksenä kappaleessa viisi käsiteltiin tietoturvallisuutta, tietotekniikkarikosten uhrien asemaa ja yksityisyyden suojaa tietotekniikkarikoksiin liittyen. Tässä kohdassa Komissio ehdotti asian selvittämisen jatkamista erillisen asiantuntija-

ryhmän kanssa. Tietoturvan osalta esille tuotiin lainsäädännön ohessa tekniikan kehittämisen tarve ja sen kouluttaminen käyttäjille.

Listan moni kohta, minimisuosituslistassa kohdat 7 ja 8, koskevat selkeästi erilaisten digitaalisten töiden kopiointia, joiden tekijänoikeudet ja kopioinnin laittomuus tuli nopeasti saattaa selkeästi lakiin. (Council of Europe, 1990)

2.3.2 Recommendation No. R (95)13

Seuraava Euroopan Neuvoston julkaisema ohjeistus oli asiantuntijakomitean vuonna 1991 alkanut työ joka julkaistiin syyskuussa 1995. Raportissa suositeltiin huomioimaan ko. raportti kunkin maan uudistaessa lainsäädäntöään. Itse suosituksia oli 18 kohtaa ja ne olivat jakaantuneet 7 pääkohtaan. Pääkohdat olivat:

1. Etsintä ja takavarikko (Search and seizure)
2. Tekninen tarkkailu (Technical Surveillance)
3. Velvollisuudet yhteistyöhön tutkintaviranomaisten kanssa (Obligations to co-operate with the authorities)
4. Elektroninen todistusaineisto (Electronic Evidence)
5. Salaustekniikan käyttö (Use of Encryption)
6. Tutkimus, tilastointi ja koulutus (Research, statistics and training)
7. Kansainvälinen yhteistyö (Intenational Cooperation)

Tämä lista pitää sisällään viranomaisten toimintakykyyn liittyviä asioita. Viranomaisten toimintaa rikollisuutta vastaan yritettiin parantaa ja yhdenmukaistaa jäsenvaltioissa ja tietyiltä osin jäsenvaltioille suositeltiin rikostutkimuksen kannalta oleellisten yhteistyösopimusten tekemistä. (Council of Europe, 1995: 1—4)
Ensimmäisessä kohdassa halutaan laillistaa todisteiden etsintä tietojärjestelmän haltuunotolla. Tavoitteena on tekstin mukaan saada säädökset samanlaiseksi, on kysymys sitten perinteellisistä dokumenteista, tai tietokoneen tiedostosta. Toisessa kohdassa halutaan viranomaisille oikeudet digitaalisen viestinnän tekniseen tarkkailuun. Kolmannessa kohdassa halutaan viranomaisille oikeus vaatia teknistä apua erilaisten, rikostutkimukseen kuuluvien järjestelmien käyttämiseen. Neljännen kohdan mukaan halutaan digitaalisten todisteiden käytön säädökset samanlaisiksi kuin vastaavilla perinteisillä todisteilla. Samalla kehotetaan viranomaisia kehittämään digitaalisen materiaalin säilytystä ja siirtelyä eri maiden välillä. Viidennen kohdan mukaan, toivotaan materiaalin

salausten käyttöä vain siinä määrin kun ehdottomasti välttämätöntä. Kuudennessa kohdassa kehotetaan huolehtimaan tutkimuksissa mukana olevien ja yleisesti viranomaisten jatkuvasta kouluttamisesta kyseessä oleviin teknisiin asioihin. Viimeisessä kohdassa tuodaan esiin välitön tarve sopia yhteistyökäytännöistä tietotekniikkarikoksien tutkinnassa eri maiden välillä. (Council of Europe, 1995: 1—4)

2.4 Yhdistyneet Kansakunnat

Yhdistyneiden Kansakuntien organisaatiossa on kriminaalipoliittinen yksikkö, The Commission on Crime Prevention and Criminal Justice. Kyseinen organisaatio on järjestänyt kansainväliseen rikollisuuteen kohdistuvia kongresseja viiden vuoden välein vuodesta 1955. Tietotekniikkarikollisuus ja atk-rikokset otettiin merkittäväksi aihealueeksi 1990 Kuuban Havannassa pidetyssä kongressissa. Tämän kongressin päätöslauselmaan kirjattiin seuraavat tietotekniikkarikollisuuteen kohdistuvat tavoitteet. Tavoitteet:

1) Modernisoimalla kansallisia rikoslakeja, mihin tähtääviä toimenpiteitä ovat
    a. sen varmistaminen, että voimassa olevat lait riittävästi soveltuvat tietoteknisessä ympäristössä tehtyihin tekoihin;
    b. uusien kriminalisointien luominen silloin, kun se on tarpeen;
    c. sen varmistaminen, että lait riittävästi soveltuvat puheena olevien tekojen tutkintaan ja syytteeseenpanoon; sekä
    d. tietotekniikkarikosten ehkäisemis-, tutkimis- ja syytteeseenpanomenettelyn tehokkuuden lisääminen
2) parantamalla tietoturvallisuutta ja rikosten ehkäisymenetelmiä;
3) järjestämällä riittävä koulutus taloudellisten ja tietotekniikkarikosten ehkäisemiseksi, tutkinnasta ja syytteeseenpanosta vastuussa oleville
4) liittämällä informatiikan opetukseen myös tietojenkäsittelyetiikan(computer ethics) koulutusta;
5) määrittelemällä suhtautumistavat tietotekniikkarikosten uhreihin; ja
6) lisäämällä kansainvälistä tietotekniikkarikosten torjumiseksi tehtävää yhteistyötä

(Pihlajamäki, 2004: 86)

Yhdistyneet Kansakunnat julkaisi myös kirjan atk-rikollisuudesta. Kirjan nimi on United Nations Manual on the Prevention and Control of Computer-related Crime. Se julkaistiin 1994. Kirja on asiasisällöltään laaja ja se jakaantuu seitsemään alalukuun. Käsi-

teltävät aiheet ovat; tietotekniikkarikollisuus ilmiönä, toisessa ja kolmannessa luvussa käsitellään aineellista rikosoikeutta, neljännessä prosessuaalisia kysymyksiä, viidennessä rikollisuuden ehkäisemistä ja viimeisessä kohdassa kansainvälistä yhteistyötä. (UN 1999: 2–3)
Kirja eroaa aikaisemmin tehdyistä raporteista siten, että se ei pyri antamaan jäsenvaltioille ja heidän lainsäätäjilleen mitään tarkkoja ohjeita lain valmisteluun suoranaisesti mutta käy muuten asiaan kuuluvia asioita hyvin tarkasti läpi. Viidennessä luvussa esiintyvä jaottelu tietoturvan parantamiseksi on myöhemmin yleistynyt jako. Eri osa-alueet ovat; (UN 1999: 40-42)

1) hallinnollinen ja organisatorinen tietoturvallisuus (administrative and organizational security);
2) henkilöstöturvallisuus (personnel security);
3) fyysinen turvallisuus (physical security);
4) tietoliikenneturvallisuus (communications-electronic security);
5) laitteisto- ja ohjelmistoturvallisuus (hardware and software security);
6) käyttöturvallisuus tai tietoaineistoturvallisuus (operations security); sekä
7) sattumanvaraisuussuunnittelu (contingency planning)

Yhdistyneet Kansakunnat toimii maailmanlaajuisesti ja laajemmalla alueella kuin aikaisemmin esille tuodut organisaatiot. Se on laajin tietotekniikkarikollisuuteen suosituksia antanut organisaatio. Siten sen merkitys kansainvälisesti on huomattava.

YK:n myöhemmät kongressit, kymmenes Kairossa vuonna 1995, vuonna 2000 Wienissä, vuonna 2005 Bangkokissa ja vuonna 2010 Salvadorissa Brasiliassa eivät ole käsitelleet tietotekniikkarikoksia enää yhtä laajasti vaan päähuomion veivät muut kansainvälisen rikollisuuden muodot. (UN, 2011)

2.5 Euroopan unioni

Euroopan unioni (EU) ei toimintansa alkuvaiheessa kiinnittänyt tietotekniikkarikoksiin niin suurta huomiota kuin jotkut aikaisemmin esille tuodut yhteisöt. Sitten pääpaino oli aluksi teleliiketoimintaa koskevassa lainsäädännössä. Ensimmäinen konkreettinen toimenpide tietojärjestelmien puolella oli oikeastaan COMCRIME-projekti joka käynnistettiin 1996. Ensimmäinen Komission tiedonanto Neuvostolle, Euroopan Parlamentille,

Talous ja sosiaalikomitealle ja alueiden komitealle annettiin 23.1.2001. Tiedonannon nimi oli ”Turvallisempaan tietoyhteiskuntaan tietojärjestelmien turvallisuutta parantamalla ja tietokonerikollisuutta ehkäisemällä”. Tiedonanto jakaantui seitsemän kohtaan ja viimeisessä seitsemännessä kohdassa (Päätelmät ja ehdotukset) annettiin ehdotuksia aiheen vaatimista kehityshankkeista ja toimenpiteistä. Ehdotukset olivat tiedonannossa vielä varsin ylimalkaisia ja ne jakaantuvat säännösehdotuksiin ja muihin ehdotuksiin. Nopeasti tämän tiedonannon jälkeen, vuoden 2001 lopussa tehty Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus perustui myös 1996 käynnistettyyn COMCRIME-projektiin. Tässä julkaisussa oli jo siirrytty huomattavasti syvällisempään asioiden käsittelyyn. Sopimuksen sisällöstä ei vallinnut täysi yksimielisyys, joka johtikin siihen, että sopimuksen allekirjoitusten ja voimaantulo kesti lähes viisi vuotta. Yleissopimuksen sisältö ja Neuvoston puitepäätös 2005/222/YOS olivat pohjana Suomessa hallituksen esitykseen HE 153/2006. Molemmissa dokumenteissa tuotiin esiin ja korostettiin eri maiden rikosoikeudellisten sääntöjen lähentymistarvetta ja vastavuoroisen tunnustamisen soveltamisessa ennen oikeudenkäyntiä annettuihin määräyksiin. Yleissopimus oli tullut kansainvälisesti voimaan 1.7.2004. Asiat käydään tarkemmin läpi Suomen lainsäädäntöä koskevassa osassa.

Euroopan unionin panostus tietotekniikkaan liittyvään lainsäädäntöön alkoi 1990-luvun lopulla ja keskittyi voimakkaammin aluksi tele- tai viestintätoimialaan. Tietotekniikkaan liittyvä tekninen kehitys on sittemmin viime vuosina lähentänyt teletekniikkaa ja tietotekniikkaa toisiinsa. Kehitys on alkanut 2000-luvun alussa ja jatkuu edelleen. Lähentynyt viestintä- ja palveluinfrastruktuuri korvaa vähitellen nykyiset kiinteät matka- puhelin- internet- ja yleisradioverkot. Tätä kehitystä koskien ja silmällä pitäen, on EU antanut useita direktiivejä viimeisen kymmenen vuoden aikana. EU:n tieto- ja viestintätekniikkaan liittyvät tavoitteet ovat markkinoiden mahdollisimman tehokas toiminta ja yksilön tietoturvan riittävä suoja. Televiestintämarkkinat avattiin kokonaan kilpailulle 1. tammikuuta 1998 direktiivillä 96/19/EY. Järjestelmää haluttiin kuitenkin melko nopeasti uudistaa ja siksi uusi sääntelypaketti hyväksyttiin huhtikuussa 2002 ja uusia asioita alettiin soveltaa kaikissa jäsenvaltioissa 25. heinäkuuta 2003. Sääntelypaketti koostuu kaikkiaan yhdestä yleisestä direktiivistä ja neljästä erityisestä direktiivistä. Nämä direktiivit ovat 2002/21/EY sähköisen viestintäverkkojen ja –palveluiden yhteisestä sääntelyjärjestelmästä (puitedirektiivi), direktiivi 2002/20/EY sähköisten viestintäverkkojen ja niiden liitännäistoimintojen käyttöoikeuksista ja yhteen liittämisestä (käyttöoikeusdirektiivi), direktiivi 2002/227/EY yleispalvelusta ja käyttäjien oikeuksista sähköisten viestintäverkkojen ja –palveluiden alalla (yleispalveludirektiivi) sekä direktiivi 2002/58/EY henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (säh-

köisen viestinnän tietosuojadirektiivi). Näiden direktiivien luomaa kokonaisjärjestelmää on sittemmin uudistettu 2007. Näiden direktiivien säännöstely on suurelta osin Suomessa toteutettu uudistamalla viestintämarkkinalakia (393/2003), sähköisen viestinnän tietosuojalakia (516/2004) ja rikoslakia. Direktiivejä on annettu näiden lisäksi ainakin sähköisestä kaupasta ja sähköisestä allekirjoituksesta. (HE 112/2002: 21-30)

Direktiivit ovat Euroopan unionin jäsenvaltioille tarkoitettuja lainsäädäntöohjeita. Direktiivit antaa Euroopan unionin neuvosto ja Euroopan parlamentti yhdessä tai neuvosto yksin. Direktiivit tarjoavat tavallaan lainsäädäntöyhteistyön muodon EU:n ja jäsenvaltioiden välille. Ne sitovat SEUT 288(3) artiklan mukaan jäsenvaltioita vain sisältämänsä lainsäädäntötavoitteen osalta. Direktiivit eivät ole yleisesti sovellettavia, vaan ne vaativat kansallisen lainsäädäntötoimia toisin kuin asetukset. Direktiivin sitova velvoite on toteutettava kansallisen oikeuden sitovalla säännöksellä. Direktiivin implementoinnille asetettu määräaika vaihtelee muutamasta päivästä muutamaan vuoteen direktiivin sisällön mukaan. (Raitio, 2011:141)

Euroopan unionin sisällä tehdään yhteistyötä myös eri viranomaisryhmien kesken. Näistä toimijoista voidaan ottaa esille Europol, joka on Euroopan unionin poliisivirasto. Sen avulla tehostetaan kansainvälistä rikostorjuntaa. Toimintatapoja ovat tietoverkkoilmiöiden tarkastelu, juttujen sarjoittaminen ja hyväksi havaittujen rikostutkintamenetelmien jakaminen. Eurojust on Unionimaiden syyttäjäviranomaisten edustajisto. Eurojustin rooli korostuu ennen muuta usean valtion välisiä toimivaltuuskysymyksiä ratkottaessa. (Kuusimäki, 9)

2.6 Ammatilliset järjestöt

Atk-rikollisuutta koskevassa kirjallisuudessa tuodaan esiin myös ammatillisia järjestöjä, jotka tekevät yhteistyötä taistellessaan tietotekniikkarikollisuutta vastaan. Interpol, kansainvälinen rikospoliisijärjestö toimii maailmanlaajuisesti. Siihen kuuluu 187 jäsenvaltiota. Heidän tutkijansa auttavat jäsenvaltioiden viranomaisia rikostutkimuksessa mm. todisteiden hankinnassa. Interpolin päämaja on Ranskassa. (Interpol 2011)
Toinen ammatillinen järjestö on Kansainvälinen rikosoikeusyhdistys (International Association of Penal Law). Se on perustettu Pariisissa 1924. Yhdistys on vanhin rikosoikeuden tutkijoiden yhdistys maailmassa. Yhdistys järjesti 1994 kongressin Rio de Janeirossa jossa yhtenä pääaiheena olivat tietotekniikkarikokset. (IAPL 2011)

2.7. Yhteenveto kansainvälisestä yhteistyöstä

Edellä on esitetty lyhyesti Suomen kannalta merkityksellisin kansainvälinen yhteistyö koskien tietotekniikkarikoksia ja tietotekniikkarikollisuutta. Ensimmäiset hankkeet 1980-luvulla olivat uraa uurtavia. Keskeiset tavoitteet kansainvälisessä yhteistyössä oli aloittaa kaikissa jäsenvaltioissa lainsäädännön uudistaminen ja samalla lainsäädännön harmonisoiminen. Itse lainsäädännön uudistusten keskeisimmät asiat olivat tietojärjestelmiin tunkeutumalla suoritettavien rikosten huomioiminen lainsäädännössä. Toisena asiakokonaisuutena oli erilaisten digitaalisten tuotteiden kopioinnin kieltäminen lainsäädännöllä. Kolmas tärkeä asiakokonaisuus oli yksilön tietosuojan parantaminen lainsäädännöllä ja neljäs kokonaisuus oli työkalujen kehittäminen viranomaisille taistelussa atk-rikollisuutta vastaan. Ajan kuluessa uudistukset ovat 2000—luvulle mennessä konkretisoituneet ja suurin osa suosituksista on päätynyt kansalliseen lainsäädäntöön. Työ jatkuu kuitenkin koko ajan. 1980– ja 1990– lukujen suurten asiakokonaisuuksien aika on kuitenkin ohi, nyt työtä tehdään pienempiin kokonaisuuksiin keskittyen. Pääsyy tähän on tietotekniikan käytön ja tavallaan ”tietomassan” nopea kasvaminen. Maailmanlaajuisesti tietotekniikkarikoksia säätelevän lainsäädännön uudistamiseksi ja yhtenäistämiseksi tekevät työtä Xingan mukaan mm. seuraavat organisaatiot; APEC, eli Aasian ja Tyynen meren maiden talousjärjestö, Euroopan neuvosto, EU, OAS eli Amerikan valtioiden liitto, Kansainyhteisön maat, G8-valtiot, OECD ja YK. (Xingan, 2008: 308-309)

.

3. LUOTTAMUKSELLISUUTEEN LIITTYVÄT RIKOKSET

3.1 Lainsäädännön kehittyminen

3.1.1 Aika ennen Euroopan unionia

Tietotekniikan kansainvälisen luonteen takia monet kansainväliset järjestöt alkoivat kiinnittää tietotekniikkarikoksiin erityistä huomiota. Tutkimuksia ja suosituksia tehtiin useita, kuten edellisessä kappaleessa kerroin. Suomessa kehitystyö alkoi kansainvälisten järjestöjen suositusten mukaisesti. 1980-luvulla HE 94/1993 mukaan ensimmäisen kerran aihetta käsiteltiin Euroopan Neuvostossa vuonna 1981 annetussa taloudellista rikollisuutta koskevassa suosituksessa (Recommendation No. R(81) 12. Aikaisemmin esitetyn mukaisesti moni eri järjestö antoi raportteja ja suosituksia lainsäädännön kehittämiseksi. Voimakkain toimija Länsi-Euroopan osalta oli Euroopan Neuvosto, jonka raportin mukaan lainsäädännön kehittämistä alettiin valmistella. Suomen lainsäädännön peruslinjaksi valittiin olemassa olevan lainsäädännön kehittäminen. Toinen vaihtoehto olisi ollut, että lainsäädäntöön olisi kehitetty erikseen tietotekniikkaan kohdistuvat lait. Päätös linjan valitsemisesta tehtiin Euroopan Neuvoston kriminaalipoliittisen komitean(European Committee on Crime Problems, CDPC) hyväksymän raportin ”Recommendation No. R(89)9” hengen mukaisesti. Raportti käsitteli tietotekniikkarikoksia laajasti ja sen perusteella hallitus antoi esityksen HE 94/1993 jonka perusteella rikoslaki muutettiin ensimmäistä kertaa 1.9.1995 voimaan tulleessa laissa (21.4.1995/578) tietotekniikkarikokset huomioivaksi.

Suomen rikoslakiin tehtiin kokonaisuudistus 1990-luvulla. Se toteutettiin kahdessa vaiheessa. Kansainvälisen lainsäädäntöyhteistyön edellyttämät muutokset aloitettiin näiden uudistusten yhteydessä.

Alkuperäinen Euroopan Neuvoston esitys piti sisällään kaksi listaa, minimisuositukset ja valinnaislistan. Listan kohdista valinnaislistan ”Tietokoneen luvaton käyttö” oli jo huomioitu lainsäädännössämme HE 66/1988 mukaan tehdyissä muutoksissa lailla 769/1990. Pääosa listan suosituksista toteutettiin HE 94/1993 perusteella, mutta muuta-

mia korjauksia tehtiin jo ennen kokonaisuudistusta edellä mainitun ”Tietokoneen luvaton käyttö” – kohdan lisäksi.

3.1.2 Euroopan unionin aika

Suomi liittyi Euroopan unionin jäseneksi 1.1.1995. Liittymisen myötä lainsäädäntöön vaikuttavat olosuhteet muuttuivat selkeästi. Liittymissopimuksen mukaan Suomen tuli kehittää lainsäädäntöään Euroopan unionin haluamaan suuntaan. Atk-tekniikkaan liittyvän lainsäädännön kehittäminen aloitettiin telemarkkinoista. Euroopan unionin sisällä televiestintämarkkinat avattiin kokonaan kilpailulle 1. tammikuuta 1998 direktiivillä 96/19/EY. Tämä aiheutti telealan lainsäädännön uusimisen. Telemarkkinoiden kilpailun sääntelyyn julkaistiin telemarkkinalaki 472/1997. Tekniikka kehittyi ja teleala ja atk-ala lähenivät nopeasti toisiaan. Telemarkkinat tarvitsivat lainsäädännön uusimista melko nopeasti telemarkkinalain voimaan tulon jälkeen, ja niin voimaan saatettiin markkinaviestintälaki (393/2003). Tämä laki perustui viiteen eri direktiiviin, jotka julkaistiin 2002 ja 2003. Direktiiveissä käsiteltiin viestintämarkkinoiden toimivuuden kannalta keskeiset asiat. Viestintämarkkinoiden sääntelyyn liitettiin myös sähköisen viestinnän tietosuojalaki (516/2004) joka nimensä mukaisesti sääntelee yksityisyyden suojaa sähköisessä viestinnässä. (HE 112/2002).

Osittain telealan lainsäädännön kehittämisen kanssa Euroopan unionissa aloitettiin atk-alalle keskittyvä COMCRIME-projekti, joka käynnistettiin 1996. Hankkeen alla julkaistiin useita suosituksia ja raportteja 1990-luvun lopulla. CONCRIME-hanke jatkoi siitä mihin muu kansainvälinen yhteistyö ja eri toimijat olivat 1990-luvun puoleen väliin päässeet. Vuoden 2001 lopulla julkaistiin Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus (Convention on Cybercrime –ETS no 185).

Tietoverkkorikollisuutta koskeva yleissopimus on sisällöltään voimakkaasti uudistuksia ajava. Se aiheutti paljon keskustelua ja osin siksi kesti kauan ennen kuin jäsenvaltiot alkoivat allekirjoittaa ja ratifioida sopimusta. Nyt sen on allekirjoittanut ja ratifioinut 30 maata, osa Euroopan unionin ulkopuolelta. 16 maata on allekirjoittanut sopimuksen, mutta eivät ole ratifioineet sitä.

Euroopan unionin neuvosto julkaisi puitepäätöksen 2005/222/YOS helmikuun 24. 2005. Ouitepäätöksen ja Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen uudistukset alettiin siirtää Suomen lainsäädäntöön 2006-2007. Niihin perustuu pää-

osin HE 153/2006. Hallituksen esityksen mukaan ETS no 185 on ensimmäinen tietotekniikkarikoksia koskeva yleissopimus (HE 153/2006, 2). Lain esitöiden mukaan yleissopimuksella pyritään yhteiskunnan suojelemiseen tietotekniikkarikoksilta yhtenäistämällä ja laajentamalla rikoksia koskevia rangaistussäännöksiä sekä tehostamalla rikostutkintaa ja kansainvälistä oikeudellista yhteistyötä. 2007 voimaan tullut rikoslain tarkistus toi useita muutoksia lakiin. Tämän jälkeen ei rikoslakiin ole tehty tietotekniikkarikoksiin kohdistuviin säännöksiin muutoksia muutamia aivan pieniä korjauksia lukuun ottamatta.

Tässä esityksessä keskitytään johdannon mukaisesti tietoturvaa tai tietojenkäsittelyrauhaa loukkaavien rikosten ja niitä koskevan lainsäädännön käsittelyyn. Esityksen pääkappaleet ovat kolmas, neljäs ja viides kappale. Niissä käydään lainsäädäntö läpi rikosnimikkeittäin. Tässä kappaleessa käsitellään tietoturvan luottamuksellisuuteen kohdistuvia asioita, seuraavassa kappaleessa tietojen eheyteen liittyviä rikosnimikkeitä ja viidennessä käytettävyyteen liittyvät rikosnimikkeet.

Tietoturvan luottamuksellisuus tarkoittaa, että tiedot ovat vain niiden käyttöön oikeutettujen saatavissa eikä niitä paljasteta tai muutoin saateta sivullisten käyttöön. Luottamuksellisuuteen kohdistuvia rikosnimikkeitä on Suomen laissa kolme kappaletta, tietomurto, luvaton käyttö ja tietomurron erityistapaus, yritysvakoilu.

3.2 Tietomurto

3.2.1 Säännöksen kehittyminen

Yleisin tietoturvan luottamuksellisuuteen kohdistuva rikos on nimikkeeltään tietomurto. Tietomurtoa käsitellään RL 38 luvun 8§:ssä. Lehtonen (s.164-165) määrittelee tietomurron seuraavasti; Tässä säännöksessä kriminalisoidusta tietomurrosta voidaan tuomita se, joka a)käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka b) turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu 1) tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja, taikka 2) sellaisen järjestelmän erikseen suojattuun osaan.

Rikokselle on tunnusomaista, että tekijä pääsee sisään tietojärjestelmään johon hänellä ei ole lupaa tai oikeutta päästä eli tunkeutuminen järjestelmään on oikeudetonta. Rikos

on asianomistajarikos ja rangaistuksena tekijä voidaan tuomita sakkoihin tai enintään vuodeksi vankeuteen.

HE 94/1993 kohdassa 38 luvun 8 § tietomurto, tarkennetaan kriminalisoitua tekoa. Tunkeutuminen voi tapahtua joko työasemalta tai tietoliikenneyhteyden kautta. Se on nykypäivänä varmasti yleisin tekninen yhteys ja tietomurtoa suunnittelevalle luonnollisin yhteys. Tietojärjestelmällä tarkoitetaan tietojärjestelmää laajasti. Järjestelmä ei ole ainoastaan fyysinen kokonaisuus vaan kattaa mm. järjestelmällä tuotetut palvelut. Esiin tuodaan myös, että kyseessä on sähköinen tietojärjestelmä, ei siis käsin tai manuaalisesti pidetty järjestelmä. Teon rangaistavuuden edellytyksenä on, että järjestelmään on murtauduttu. Tämä tarkoittaa sitä, että järjestelmässä on suojaus, esimerkiksi salasana. (HE 94/1993: 175—176)

Nykypäivänä järjestelmissä alkaa olla myös muita, vaikeammin murrettavia tunnistusmenetelmiä kuten sormenjäljet, iiris-tunnistus jne. Suojauksen tapaa ei ole hallituksen esityksessä määritelty.

Lehtonen (s.165—166) nostaa esiin myös tilanteen jossa järjestelmään tunkeutuminen on tehty jonkun salasanoilla luvallisesti. Lain mukaan tämä ei olisi oikeudetonta. Lehtosen mukaan tietomurron kriminalisoinnilla suojataan tietojärjestelmää eikä yksinomaan tunnuksenhaltijaa. Ratkaisuna hän tuo esille sen, että monet edellyttävät, ettei tunnuksia saa luovuttaa muille.

Tunkeutumisen tulee olla tahallista. Tahattomuus tulee kysymykseen usein vain yrityksen sisäisissä järjestelmissä jossa osasta toiseen siirtyminen ei ole yhtä hyvin suojattu kuin järjestelmän ulkopuolelta tuleville tarkoitettu suojaus. Tietojärjestelmän luonteella ei ole merkitystä teon arvioimisessa. Rikos on täyttynyt heti kun viimeinenkin ”portti” on murrettu. Sillä käytetäänkö tietoja mihinkään tai muutetaanko mitään, on merkitystä siinä mielessä, että teko voi muuttua luvattomaksi käytöksi. Luvun 2 §:ssä laajennetaan tietomurto-käsitettä myös siten, että järjestelmän tiedon hankkiminen muilla teknisillä apukeinoilla ilman murtautumista on myös rangaistavaa. Tämä varmistus on tekniikan kehittyessä paikallaan. (HE 94/1993: 176)

Luvun 3 §:ssä mainitaan, että myös tietomurron yritys on rangaistavaa. Eli myös yritys salasanan selvittämiseksi on jo rangaistavaa. (HE 94/1993: 177)

Luvun 4 §:ssä kerrotaan, että tietomurtosäännökset ovat toissijaisia. Käytännössä voisi kai ajatella, että tietomurron toteutumisen jälkeen alkaa välittömästi järjestelmän luvaton käyttö. Tietojen käytettävyyden tai luotettavuuden kannalta kai onnistunut tietomurto tuo aina esiin epäilyn tietojen luotettavuudesta tai oikeellisuudesta. Lehtonen kuvaa tilannetta (s.168) Tietomurron itsenäinen soveltamisala on kovin suppea, mikä johtuu luvattoman käytön laajasta rangaistavuudesta. (HE 94/1993: 177)

Rikoslakia tarkennettiin vuonna 2007(540/2007). HE 153/2006 mukaan 38 luvun 8 §:aan lisättiin termi *törkeä tietomurto*. Momentin 1 kohdassa viitataan järjestäytyneeseen rikollisryhmään tekijänä. Hallituksen esityksessä määritellään järjestäytynyt rikollisryhmä vähintään kolmen ihmisen yhteenliittymäksi jonka tarkoituksena on tehdä rikos. Lisäksi järjestäytyneisyys edellyttää jonkinasteista hierarkiaa ja työnjakoa. Kyseisen rikoksen rangaistusasteikoksi ehdotetaan sakkoa tai vankeutta enintään kaksi vuotta.

3.2.2 Tietomurrot käytännössä

Tietotekniikkarikosten määrää Suomessa on vaikea tarkasti arvioida. Jotain arvioita rikollisuuden yleisyydestä saadaan tarkastelemalla poliisiin rikostilastoja. Tilastojen luotettavuutta heikentää se, että esimerkiksi tietomurto on asianomaisrikos ja helposti jää ilmoittamatta koska tietojärjestelmän suojauksen heikkoutta halutaan peitellä.

Poliisin tilastoista löytyvät tiedot RL 38 luvun käsittelemistä rikoksista tilastoituna.

Taulukko 1. Poliisin tietoon tulleet tieto- ja viestintärikokset vuosilta 2004-2010
Taulukko (Jounio, Anu 2011: 23)

	2004	2005	2006	2007	2008	2009	2010
Salassapitorikos	24	17	29	33	31	35	40
Viestintäsalaisuuden loukkaus	187	173	214	238	241	275	319
Viestintäsalaisuuden loukkauksen yritys	2	1	1	2	0	4	1
Törkeä viestintäsalaisuuden loukkaus	11	2	5	0	5	1	2
Tietoliikenteen häirintä	31	44	45	42	41	36	32
Törkeä tietoliikenteen häirintä	2	5	1	3	4	8	3
Tietomurto	94	120	122	153	196	153	315
Tietomurron yritys	9	8	6	10	5	8	8
Henkilörekisteririkos	27	41	28	27	24	42	40

Yhteensä	387	411	451	508	547	562	760

Taulukko 2. Rangaistukset rikoksittain vuosilta 2005-2009 (käräjäoikeudet ja hovioikeus ensimmäisenä oikeusasteena)
Taulukko (Jounio, Anu 2011: 24)

	2005	2006	2007	2008	2009
Salassapitorikos	1	1	0	0	2
Salassapitorikkomus	1	1	0	2	0
Viestintäsalaisuuden loukkaus	9	10	7	5	8
Viestintäsalaisuuden loukkauksen yritys	0	0	0	2	0
Törkeä viestintäsalaisuuden loukkaus	7	0	0	1	0
Tietoliikenteen häirintä	9	4	2	3	2
Törkeä tietoliikenteen häirintä	1	1	0	0	1
Lievä tietoliikenteen häirintä	0	1	0	0	0
Tietomurto	0	1	1	4	4
Tietomurron yritys	5	0	1	0	0
Henkilörekisteririkos	6	8	12	4	5

Jos tarkastellaan tietomurtojen osalta taulukkoa 1, voidaan todeta, että tietomurrot ovat kolminkertaistuneet seitsemässä vuodessa, 94:stä 314:sta. Taulukosta 2 taas nähdään, että tuomio on annettu viiden vuoden aikana vain 10 rikoksesta kun niitä on poliisin tietoon tullut vastaavan viiden vuoden aikana 744 kappaletta. Tämä suhde on hälyttävä, vain reilu prosentti rikoksista saa tuomion. Tilastojen vertailussa on se vaikeus, että tietoon tullut rikos, ei päädy oikeuteen varmaankaan samana vuonna. Se ei kuitenkaan muuta pääasiaa. Vain harva rikos tulee esiin oikeudessa. Tämä on asia johon viranomaisten tulisi paneutua. Vaikka kyseessä on asianomaisrikos, niin tuomioon päättyneiden juttujen suhde tietoon tulleisiin rikoksiin, on kyllä huolestuttava.

Vaikka tietomurtoja tehdään jatkuvasti paljon ja poliisillekin niitä ilmoitetaan vuosittain satoja, käsiteltyjä oikeustapauksia on vähän. Syytteen nostamiseen on kova kynnys koska asiat ovat usein erittäin monimutkaisia ja julkisuus antaa asiasta ilmoittaneesta sellaisen käsityksen, että tietotekniikan suojaukset on hoidettu huonosti. Xingan esittää kir-

jassaan syitä tietomurron tai yleisemmin atk-rikoksen ilmoittamatta jättämiselle. 1) vahinko ei ole niin suuri, että uhri katsoo olevan tarpeellista tehdä ilmoitusta, 2) uhri on jotenkin osallisena tai sekaantunut tapaukseen, 3) julkisuuden pelko, 4) viranomaisiin yhteydenotto koetaan vaikeaksi, 5) ei uskota viranomaisten tai poliisin kykyyn selvittää asia. (Xingan 2008:222)

Otan ensimmäisenä käytännön esimerkkinä esiin tässä tapauksen joka sattui Helsingissä ja Turussa. Tapaus on kuvattuna Pihjamäen (Pihlajamäki 2004:132-136) kirjassa ja hän toimi itse syyttäjänä alioikeudessa kyseisessä asiassa. Asia eteni käräjäoikeudesta korkeimpaan oikeuteen asti.

”Porttiskannausjuttu”

A oli syytteen mukaan 23.11.1998 Helsingissä yrittänyt murtaa turvajärjestelyn tunkeutuakseen oikeudettomasti OPK-Osuuspankin tietojärjestelmään. A oli suorittanut niin sanotun porttiskannauksen eli erityistä tietokoneohjelmaa käyttämällä skannannut läpi osuuskunnan internettiin yhteydessä olevan verkon kaikki osoitteet tarkoituksenaan löytää avoimia välityspalvelimia. Skannaus ei ollut läpäissyt osuuskunnan tietojärjestelmän palomuuria. Mikäli A olisi löytänyt avoimen välityspalvelimen, olisi hän sitä kautta kyennyt saamaan jatkoyhteyden internettiin niin, että yhteys olisi näyttänyt tuleen tästä palvelimesta. Vaadin A:lle rangaistusta tietomurron yrityksestä. (KKO: 1)

Turun käräjäoikeus kuitenkin hylkäsi syytteen. Sen mielestä ei ollut riittävästi näyttöä siitä, että A olisi tehnyt rikoksen eli kyseisen porttiskannauksen. Pihlajamäki kertoo tapauksesta vielä siten, että hänen mielestään näyttö oli vahva ja varsinkin kun syytetty oli esitutkinnassa myöntänyt teon. Oikeudessa A kuitenkin kiisti teon ja toi esiin, että joku on väärentänyt hänen IP-osoitteensa ja käyttänyt luvatta hänen tietokonettaan. Näin asia eteni Turun hovioikeuteen.

Hovioikeus perusteli tapausta seuraavin sanoin.

> On riidatonta, että kysymyksessä oleva yhteys oli tullut A:n koneen IP-osoitteella. A on kertonut, että hän on mielenkiinnon vuoksi tehnyt aikaisemmin porttiskannauksia. A ei kuitenkaan tiennyt, että olisi skannannut osuuskunnan verkon. Joku muu oli saattanut väärentää IP-osoitteen ja tehdä porttiskannauksen siten, että oli näyttänyt siltä, että yhteys oli tullut A:n koneelta.

> Vaikka tutkinnassa on jätetty selvittämättä, mistä puhelinnumerosta yhteys oli tullut, oli jutussa kuullun kahden todistajan kertomuksesta pääteltävissä, että oli epätodennäköistä, että yhteys olisi tullut muualta kuin A:n koneelta. A:llä on ollut koneellaan sellainen ohjelmisto, jolla kyseinen teko on voitu tehdä.
>
> Hovioikeus katsoi näytetyksi, että A oli tehnyt syytteessä tarkoitetun skannauksen. Ei ollut uskottavaa, että A olisi tehnyt skannauksen muussa tarkoituksessa kuin, että hän olisi myös tunkeutunut tietojärjestelmään, jos sellainen mahdollisuus olisi löytynyt. A:n teko täytti siten tietomurron yrityksen tunnusmerkistön. (KKO: 2)

Pihlajamäki kertoo kirjassaan muita yksityiskohtia joita oikeuden päätöksestä ei käy ilmi. Näistä kommenteista tulee mieleen, että hän todennäköisesti oli oikeassa mutta ehdotonta näyttöä rikoksesta vain ei ollut.

Yksi esimerkki asioista joita ei huomioitu, olivat asiantuntijoiden lausunnot. Jos joku muu olisi tehnyt yhteydenotot, niin kuin syytetty esitti, niin todistajien K:n ja P:n kertomuksista ilmeni, että vastaus olisi kuitenkin tullut A:lle eikä tuntemattomalle porttiskannauksen tekijälle. Porttiskannaus olisi tuolloin ollut tekijälleen hyödytön.

A sai tapauksessa korkeimmalta oikeudelta valitusluvan. Korkein oikeus antoi tuomionsa 8.4.2003. Korkein oikeus ei muuttanut tuomiota. Korkein oikeus perusteli kantaansa ja rikosta muun muassa seuraavasti:

> Porttiskannausohjelmalla on näin olleen mahdollista järjestelmällisesti selvittää tietojärjestelmän mahdollisia aukkoja ja sen heikkoja kohtia. Toimenpiteen avulla kyetään saamaan tietoja, jotka mahdollistavat myös luvattoman pääsyn kohteena järjestelmään. Ohjelmaa käyttämällä hankitun tiedon avulla voidaan siten laissa tarkoitetuin tavoin murtaa tietojärjestelmän turvajärjestely. Kuten lain esitöissä todetaan jo se, että yrittää hankkia tällaisen luvattoman pääsyn järjestelmään mahdollistavan tiedon, on rangaistavaa, jos se tehdään tarkoituksella oikeudettomasti tunkeutua tietojärjestelmään.
>
> A on kiistänyt, että hänen tarkoituksensa olisi ollut tunkeutua osuuskunnan tietojärjestelmään. A:n mukaan hänen tarkoituksenaan on ollut internetissä liikkuessaan tällä tavoin etsiä joko avointa välityspalvelinta tai muuta kiinnostavaa. Korkein oikeus toteaa, ettei luvallista avoimien palvelinten tai palvelun etsintään internetissä tarvita tällaista ohjelmaa. Skannauksen ominaisuuksien vuoksi ei ole muutoinkaan uskottavaa, että A olisi käyttänyt ohjelmaa ensisijaisesti tässä tarkoituksessa. Kun kyseessä olevan tietojärjestelmän skannaaminen on ollut järjestelmällistä eikä ole ollut uskotta-

> vaa, että tällaisen skannauksen kautta saatavalla tiedolla olisi ollut A:lle käyttöä muussa tarkoituksessa kuin luvattomasti tietojärjestelmään pyrittäessä, Korkein oikeus katsoo, että A on suorittanut skannauksen tarkoituksin sen kautta saatavan tiedon avulla tunkeutua tietojärjestelmään. Näin ollen A on syyllistynyt hovioikeuden hänen syykseen lukemaan osuuskunnan tietojärjestelmään kohdistuneeseen tietomurron yritykseen. (KKO: 4)

Näin syytetyn A:n esitys, että porttiskannauksella ei murtauduta väkisin mihinkään, vaan etsitään kohtia joissa sisään voi päästä murtautumatta, torjuttiin.

3.2.3 Tuomituista vahingonkorvauksista

Ensimmäisenä esimerkkinä kerrottua ns. ”porttiskannausjuttua” käsittelivät Markku Fredman ja Petteri Järvinen Defensor Legis-lehdessä numerossa 4/2003. He ottivat voimakkaasti kantaa tuomioistuimen määräämiin vahingonkorvauksiin. Kirjoituksen idea oli siinä, että käräjäoikeuden päätöksessä selvästi tuotiin esiin se, että syytetty ei päässyt tunkeutumaan uhrina olleen pankin järjestelmään. Kuitenkin pankki esitti yhteensä 110 000 markan korvausvaatimukset. Hovioikeus pienensi korvausta 75 000 markkaan ja korkein oikeus piti korvaussumman samana. Mielestäni kirjoittajat täysin oikeutetusti kysyvät mitä kustannuksia tunkeutumisen yrityksestä on voinut tulla kun järjestelmän sisään ei päästy. Mikäli pankin turvajärjestelmät ovat niin heikkoja, että pelkkä porttiskannaus aiheuttaa kymmenen tuhannen euron selvityskulut, turvajärjestelyjä on syytäkin parantaa. Niin skannauksia kuin tietomurron yrityksiä tapahtuu kymmeniä, ellei satoja vuorokaudessa. (Fredman, Järvinen 2003)

Kirjoituksessa kyseenalaistetaan myös päätös, että porttiskannaus on tietomurron yritys. Tapaus ja tämä kirjoitus osoittaa, että asiat eivät suinkaan ole yksiselitteisiä. Tässä viimeisessä väittämässä kirjoittavat provosoivat. Jos kyse ei olisi tietomurrosta, niin sisään pääsyn jälkeen kuitenkin luvattomasta käytöstä.

3.3 Yritysvakoilu

Yritysvakoilun toteutustapaan voi liittyä tietomurto jolloin se on tietojärjestelmän luottamuksellisuuden loukkaus. Yritysvakoilun eri tapoja tuodaan rikoslaissa esiin useampia mutta tässä keskitytään vain tietotekniikkapohjaiseen osaan. Yritysvakoilua käsitellään RL 30 luvun 4 §. Yritysvakoilu määritellään mainitun lain 11 §:ssä;

Yrityssalaisuudella tarkoitetaan tässä luvussa liike- tai ammattisalaisuutta taikka muuta vastaavaa elinkeinotoimintaa koskevaa tietoa, jonka elinkeinonharjoittaja pitää salassa ja jonka ilmaiseminen olisi omiaan aiheuttamaan taloudellista vahinkoa joko hänelle tai toiselle elinkeinonharjoittajalle, joka on uskonut tiedon hänelle.

Yritysvakoilusta säädettiin aikaisemmin SopMenL:n 4§:n 1 momentissa. Tekstistä puuttui kuitenkin viittaukset erilaisiin tekotapoihin jotka nyt haluttiin mukaan uuteen säännökseen. Tekotapaa tarkennetaan HE 66/1988 seuraavasti. Tunkeutuminen olisi ymmärrettävä tietotekniikan terminä, pääsyn hankkimisena tietojärjestelmään ”hakkerin” keinoin esimerkiksi tietokonetta, modeemia ja puhelinta käyttämällä. Tietojärjestelmällä tarkoitettaisiin erilaisia tietojenkäsittelylaitteita ja niiden välisiä tietoliikenneyhteyksiä. Myös tietojärjestelmän tulisi olla ulkopuolisilta suojattu, jolloin tunkeutuminen edellyttäisi jonkin turvajärjestelmän murtamista tai käyttäjäkontrollin läpäisemistä samalla tavoin kuin mitä henkilörekisterilain (471/87) 45§:ssä on säädetty. (HE 1988/66: 83)

3.4 Luvaton käyttö

3.4.1 Säännöksen kehittyminen

Toinen tietoturvan luottamuksellisuuteen kohdistuva rikos on nimikkeeltään luvaton käyttö.: Luvattoman käyttöä koskevat säännökset löytyvät rikoslain 28 luvun kohdissa 7, 8 ja 9. Säännös on luonteeltaan yleinen eli tietotekniikan ei mainita erikseen. Luvattoman käytön kohteena voi olla irtain omaisuus tai kiinteä omaisuus, koneet tai laitteet.

> Lehtonen kirjoittaa luvattomasta käytöstä seuraavasti. Rikoksen kohteena voi olla millainen tahansa irtain esine. Kiinteän koneen tai laitteen suhteen ei ole merkitystä sillä seikalla, onko asianomainen kone tai laite siviilioikeudellisesti a) irtainta omaisuutta tai b) kuuluuko se kiinteään omaisuuteen aineosana. Tietokone voi siten olla luvattoman käytön kohteena siitä riippumatta, onko se sijoitettu esimerkiksi pöydälle vai onko se pysyvästi kiinnitetty (pultattu) rakennuksen lattiaan. Käyttö voi olla luvatonta siitä riippumatta, käytetäänkö toisen omaisuutta a) sen käyttötarkoitusta vastaavalla tavalla tai b) jollain muulla tavalla. Tekijän hyötytarkoitus ei kuulu luvattoman käytön rangaistavuuden edellytyksiin. Luvattoman käyttäjän ei tarvitse tavoitella hyötyä eikä käytön edellytetä tuottavan hänelle hyötyä. (Lehtonen, 2002:161)

Uuden lain valmistelu on HE:ssä 66/1988. Uudella, 24.8.1989 voimaan tulleella lailla korvattiin aikaisemmin rikoslain 38 luvun 6 §:ssä olleet luvattoman käytön säännökset. Vanhassa lakitekstissä hallussa oleva omaisuus ja toisen hallussa oleva omaisuus oli eriteltynä. Nyt tästä jaosta luovuttiin. Uudessa lainsäädännössä päädyttiin jakamaan teot lievään luvattomaan käyttöön, luvattomaan käyttöön ja törkeään luvattomaan käyttöön. Uudessa lainsäädännössä päädyttiin siihen, että luvaton käyttö on aina asianomistajarikos, aikaisemmin luvaton käyttöönotto oli virallisen syytteen alainen rikos. Hallituksen esityksen perusteella pääpaino uudistuksessa keskittyi ajoneuvoihin kohdistuviin rikoksiin.

Lakitekstiä on korjattu kerran myöhemmin eli 4.3.2011 muutettiin 28 luvun 7§ siten, että lakiin lisättiin maininta ”Luvattomana käyttönä ei pidetä suojaamattoman langattoman tietoverkkoyhteyden kautta muodostetun internet-yhteyden käyttämistä” Kyseinen tapa, suojaamattoman langattoman verkon käyttö oli sallittua kaikissa Suomen lähinaapurimaissa.(HE 277/2010)

3.4.2 Turun HO 2009:793

Seuraavassa kuvataan kaksi käytännön esimerkkiä luvattomasta käytöstä. Ensimmäisenä juttu jonka ratkaisi Turun hovioikeus. Lain muutokseen 13.5.2011 tarpeellisuutta valaisee osittain seuraava tapaus. Juttu oli alun perin esillä Salon käräjäoikeudessa ja myöhemmin siis Turun hovioikeudessa 2008-2009.

Tapauksessa 1. syytetty A oli käyttänyt kerrostalossa naapurinaan asuneen B:n langatonta lähiverkkoa ottamalla sen välityksin yhteyttä internettiin. Samaa henkilöä A syytettiin kohdassa 2. myös siitä, että hän oli käyttänyt hänelle kuulumatonta käyttäjätunnusta kahdesti ja tunkeutunut C Oy:n sähköpostijärjestelmään. Kohdan 1. syyte oli lievä luvaton käyttö ja kohdan 2. tietomurto.

Vastauksenaan kohtaan 1. henkilö A kiisti syyllisyytensä lievään luvattomaan käyttöön. Vastaaja myönsi käyttäneensä naapurinsa yhteyttä mutta tehneensä sen vahingossa. Kohtaan 2. vastaaja kiisti syyllisyytensä syytteessä mainittuun tekoon.

Käräjäoikeuden ratkaisu oli seuraava. Käräjäoikeus katsoi selvitetyksi, että A on syyllistynyt siihen, mistä hänelle on vaadittu rangaistusta syytekohdassa 1.

Perusteluina käräjäoikeudella oli seuraavaa: Käräjäoikeus piti toteennäytettynä naapurin yhteyden käytön. Käräjäoikeuden mielestä A:n olisi pitänyt pyytää lupa naapurin Wlan-yhteyden käyttöön. Syytetty, tietokonealan asiantuntijana ei ollut uskottava väittäessään, että yhteyden käyttö olisi tapahtunut vahingossa. Tämän lisäksi A oli toistanut tekonsa lukuisia kertoja jolloin sitä ei voida pitää vahinkona vaan tahallisena tekona. (Turun HO: 3)

Kohdan 2 syytteen käräjäoikeus hylkäsi. Perustelut olivat seuraavat;

> Vaikka A oli aikoinaan huolehtinut C Oy:n sähköpostiverkosta, hän ei asemansa perusteella ole saanut tietoonsa työntekijöiden salasanoja. Pelkkä yhtiön edustajan ilmoitus, että työntekijät ovat kertoneet salasanansa A:lle, ei riitä osoittamaan, että näin on tapahtunut. Yhtiön C Oy:n sähköpostijärjestelmään oli tunkeuduttu aiemmin mainitun naapuri B:n IP-osoitteesta. Yhteyttä oli rikoksen tekemisen aikaa käyttänyt neljä muutakin henkilöä joten ei ollut varmaa, että kyseessä oli syytetty A. A:n omalta, poliisin takavarikoidulta koneelta ei löytynyt näyttöjä C Oy:n järjestelmään tunkeutumisesta. (Turun HO: 4)

Tapauksen jatkokäsittely tapahtui Turun hovioikeudessa. Tuomio on annettu 31.3.2009. Syytetty oli vaatinut, että hänen saamansa tuomio lievästä luvattomasta käytöstä hylätään ja syyttäjä oli vaatinut, että A:n vaatimus hylätään. Turun hovioikeus antoi seuraavan vastauksen: A on käyttänyt B:n lähiverkkoa ja tullut tietämään olleensa vieraassa verkossa. A on tästä huolimatta jatkanut verkon käyttöä toistuvasti. A on ollut tietoverkkoihin hyvin perehtynyt henkilö ja langattoman verkon ominaisuudet ovat hänelle tuttuja. (Turun HO: 5—6)

Perusteluissaan hovioikeus tuo esille, että suojaamattoman verkkoyhteyden käytön rangaistavuudessa on ollut epätietoisuutta. Luvaton käyttö on ollut rangaistavaa vain tahallisesti käytettynä. Lisäksi hovioikeus mainitsee, että toisen henkilön suojaamattoman verkkoyhteyden käyttö ei ole jokamiehenoikeus. Nyt siis lakia on myöhemmin muutettu ja suojaamattoman langattoman verkon käyttö ei ole rangaistavaa. (Turun HO: 6)

Pariinkin kertaan perusteluista löytyy maininta jossa puhutaan siitä, että rangaistavuus ei edellytä, että käytettävä omaisuus olisi käyttäjän hallussa. Tämä kannanotto on varmaankin yleisesti ottaen tarpeellinen mutta samalla se ilmaisee kuinka vaikeita ja abstraktisia asioita käsitellään. Tietotekniikassa ei enää pitkään aikaan ole ollut oleellista tai samalla tavoin tärkeää fyysinen hallussapito.

3.4.3 Vaasan HO 2002:745

Toinen, huomattavasti laajempi esimerkki on tapaus, josta on käytetty nimeä TCB-juttu, syytetyn käyttämän nimimerkin mukaan. Kyseessä on hakkeri, joka 1990-luvun lopulla tunkeutui kymmeniin, ellei satoihin tietojärjestelmiin. Asia oli ensin esillä Jyväskylän käräjäoikeudessa ja sen jälkeen Vaasan hovioikeudessa. Pihlajamäki kuvaa lyhyesti tapausta seuraavasti; (Pihlajamäki, 2004:164-165)

> P oli 1.9.1997–1.7.1998 Jyväskylässä käyttämällä lupaan perustuvan oikeutensa ylittäen työnantajansa A Oy:n tietojärjestelmää sekä luvattomasti Jyväskylän ammattikorkeakoulun tietojärjestelmää, johon oli hänelle kuulumatonta käyttäjätunnusta käyttäen oikeudettomasti tunkeutunut, ottanut näiden tietojärjestelmien välityksellä yhteyksiä (84 asianomistajan) tietojärjestelmiin ja
>
> 1. käyttämällä hänelle kuulumattomia käyttäjätunnuksia ja salasanoja oikeudettomasti tunkeutunut mainittujen asianomistajien tietojärjestelmiin, joita oli luvattomasti käyttänyt siirtymiseen järjestelmästä toiseen sekä jäljempänä syytekohdissa 3–5 selostettavaan toimintaan
>
> 2. kohdassa 1 selostetulla luvattomalla käyttämisellä aiheuttanut (viidelle asianomistajalle) näiden olot huomioon ottaen erityisen tuntuvaa haittaa tunkeutumisen seurauksena tehtyjen selvittelytoimenpiteiden aiheuttamana lisätyönä sekä näistä toimenpiteistä johtuneista käyttökatkoksista aiheutuneen työajan menetyksenä sekä käyttäjille ja asiakkaille tarkoitettujen palveluiden estymisenä;
>
> 3. edellä kerrottujen käyttämisten yhteydessä oikeudettomasti turmellut ja salannut (50 asianomistajan) tietojärjestelmiin tallennettuja tietoja asentamalla niin kutsuttuja takaporttiohjelmia ja muuttamalla olemassa olevia ohjelmia tällaisiksi samoin kuin poistamalla järjestelmien keräämiä lokitiedostoja; sekä
>
> 4. tietoverkossa tapahtuvaa liikennettä kuuntelemaan suunniteltuja ja muunnettuja tietojenkäsittelyohjelmia käyttämällä oikeudettomasti hankkinut tietoja (31 asianomistajaa) tietojärjestelmien kautta liikkuneista datasiirroista tarkoituksin kerätä itselleen käyttäjätunnuksia ja salasanoja.
>
> 5. Lisäksi P oli 14.11.1997–20.6.1998 Jyväskylässä, saatuaan syytekohdasta 1–4 kerrotuin tavoin eli tietojärjestelmiin tunkeuduttuaan tietoverkossa tapahtuvaa liikennettä kuuntelemaan suunniteltuja tai muunnettuja tietojenkäsittelyohjelmia käyttämällä haltuunsa toisille kuuluvia käyttäjätunnuksia tai salasanoja, joko välittömästi niitä hyödyntäen tai saatuaan niitä käyttämällä itselleen järjestelmien pääkäyttäjän oikeudet, tällä tavoin suojauksen murtaen tunkeutunut useaan sähköpostilaatikkoon ja oikeudettomasti hankkinut tieto-

> ja niihin talletetuista (154 asianomistajan) lähettämistä ja vastaanottamista ulkopuolisilta suojatuista viesteistä.
>
> Kohdan 2 luvatonta käyttämistä ja kohtien 4 ja 5 viestintäsalaisuuksien loukkauksia oli, huomioon ottaen niiden laajamittaisuus ja järjestelmällisyys, pidettävä kokonaisuutena arvostellen törkeänä.

Jutun selvityksen kannalta oli hyvä, että syytetty oli aluksi hyvin yhteistyöhaluinen. Muuten tämän kokoluokan jutun tutkinta olisi ollut valtava työ, osin jopa mahdoton. Ulkomaille kohdistuneita rikkeitä ei edes pyritty selvittämään. Jutussa oli kaikkiaan 137 sellaista asianosaista, jotka vaativat syytetylle rangaistusta. Asianosaisista noin puolet oli yrityksiä ja julkisia yhteisöjä ja noin puolet yksityishenkilöitä. Osa syytteistä koski siis myös törkeää viestintäsalaisuuden loukkausta ja sitä ei tämän esityksen rajauksen perusteella käsitellä. Kaiken kaikkiaan asianomaiset vaativat vahingonkorvauksia syytetyltä 800.000 markkaa Alioikeuden tuomio oli 5 kk ehdollista vankeutta ja syytetylle tuomittiin kaikkiaan vahingonkorvauksia ja oikeudenkäyntikuluja maksettavaksi 450.000 markkaa. Hovioikeus korotti ehdollisen vankeuden pituuden 7 kuukauteen mutta piti vahingonkorvausten määrän samana.

Tapauksen tutkinnassa oli käynyt ilmi se, että suurin osa uhreista oli laiminlyönyt tietoturvallisuutensa hoitamisen melko perusteellisesti. Se on varmasti yksi tekijä joka selittää kuinka suureen määrään yrityksiä tekijä on pystynyt tunkeutumaan. Toisaalta hän on tutkimuksen mukaan ollut työssään järjestelmällinen. Hovioikeuden käsittelyssä syytetty yritti myös vähätellä tekoaan mm. sillä, että Helsingin Yliopiston järjestelmiin oli tehty samaan aikaan useampia tietomurtoja. Tähän hänellä oli todistaja mutta hovioikeus ei huomioinut asiaa.(Vaasan HO: 7)

Hovioikeuden päätöksessä esiin nousivat mm. seuraavat asiat. Käräjäoikeus oli hylännyt osan syytteistä koskien luvatonta käyttöä sen perusteella, että tietojärjestelmää ei olisi käytetty sille ominaisella tavalla. Hovioikeuden mukaan rikoslain 28 luvun 7§ sanamuoto ei rajaa rangaistavan käyttäytymisen alaa vaan siihen, että rikoksen kohteena olevaa ominaisuutta käytetään vain sille ominaisella tavalla. Myös lainkohdan esitöissä (HE 66/1988 vp. s. 43) ja oikeuskäytännöstä (KKO 1998:25) on pääteltävissä, että luvattoman käytön kriminalisoinnilla suojataan omistajalle kuuluvaa oikeutta päättää esineen käytöstä riippumatta esineen tyypillisestä käyttötarkoituksesta. (Vaasan HO: 8)

Toinen asia jonka hovioikeus nosti esiin, oli kyse yhdestä vain useammasta rikoksesta. Tässä kanta oli selvä, eli kyseessä on yksi rikos. Tämä päätös koski muutamaa isoa

asiakasta joihin kohdistuneet rikokset olivat mukana sekä kohdassa 1 että 2. (Vaasan HO: 10)

Kohdassa ”erittäin tuntuva haitta ja kokonaisuusarviointi” hovioikeus lausuu seuraavaa;

> Lainkohdan ”rikoksen uhrille tämän olot huomioon ottaen erityisen tuntuvaa” – ilmaisulla viitataan sinänsä rikoksen uhrin taloudellisiin ja muihin olosuhteisiin. Lainkohdan sanamuodolla on kuitenkin tarkoitettu saattaa ankaramman rikosvastuun piiriin myös ne tilanteet, joissa aiheutunut vahinko tai haitta ei ole sinällään kovin suuri mutta josta on esimerkiksi uhrin vähävaraisuudesta johtuen aiheutunut hänelle huomattavaa vahinkoa tai haittaa (LaVM 6/1990 vp. s.8 ja HE 66/1988 vp s. 37). Tähän tarkoitukseen nähden ei rikoksen uhrin hyvällä taloudelliselle asemalle voida antaa ratkaisevaa merkitystä. Muussa tapauksessa esimerkiksi valtioon tai sen virastoihin kohdistuvaa luvatonta käyttöä ei voitaisi katsoa törkeäksi muutoin kuin erittäin harvinaisissa tilanteissa. Lainsäätäjän ei voida katsoa tarkoittaneen tätä. (Vaasan HO: 12)

Kohdassa syytetyn tahallisuus tuodaan esiin se, että syytetty ei katsonut tekoaan tahalliseksi, eikä oman käsityksensä vuoksi voinut ymmärtää aiheuttamansa haittaa. Hovioikeus kuitenkin arvioi, että syytetty oli tietotekniikkaa opiskeltuaan tietoteknisiltä taidoiltaan ja osaamiseltaan sellaisella tasolla, että hänen on pitänyt ymmärtää tekevänsä haitta. Opiskelun lisäksi syytetty oli ollut yhden asianomaisen luona työharjoittelussa joka oli osittain ollut tietoturva-alan työtä. (Vaasan HO: 13)

Näistä kolmesta käytännön esimerkistä käy ilmi, että ovatpa teot miten suppeita tai laajoja tahansa, asialla ovat olleet vielä ”amatöörit”. Mitään selvää taloudellista hyötymistä ei ole esimerkiksi tavoiteltu.

4. TIEDON EHEYTEEN LIITTYVÄT RIKOKSET

Edellisessä kappaleessa käsiteltiin tietojärjestelmän luottamuksellisuuteen liittyvät rikosnimikkeet. Tässä kappaleessa käydään läpi tiedon eheyteen ja seuraavassa kappaleessa tiedon käytettävyyteen liittyvät rikosnimikkeet. Teknisesti tiedon eheys ja käytettävyys voidaan helposti eritellä ja tunnistaa, mutta niihin kohdistuvat rikokset ja rikollisten toimet voivat tapahtua samalla kertaa. Tiedon eheydellä tarkoitetaan sitä, että mikään ulkopuolinen taho ei pysty muuttamaan tiedon sisältöä. Tietojärjestelmän käytettävyys liittyy järjestelmän toiminnan turvaamiseen. Verkkoyhteyksien ja itse tietokoneen tulee toimia kun tietoa halutaan käyttää.

4.1 Tietojen käsittelyyn liittyvät haittaohjelmat ja muut haitan tekotavat

4.1.1 Haittaohjelmat

Haittaohjelmat ovat tänä päivänä kiinteästi tietotekniikkaan liittyvä negatiivinen ilmiö. Lähes päivittäin on lehdissä esillä erilaiset laitteistojen toimintaa vaikeuttavat virukset ja varsinkin viime aikoina laajat tietomurrot. Käyn lyhyesti läpi haittaohjelmat ja muut haitantekotavat. Näin siksi, että lukija saisi nopeasti käsityksen siitä, minkälaisia haittaohjelmia on olemassa ja mitä niillä voidaan saada aikaan. Se auttaa hahmottamaan paremmin sitä ongelmaa johon lainsäädännöllä pyritään löytämään helpotusta.

Haittaohjelmat ovat ohjelmia joiden tarkoitus on häiritä tietojärjestelmien toimintaa. Haittaohjelmien tyyppejä ovat tietokonevirukset, tietokonemadot, troijalaiset, vakoiluohjelmat ja muut haittaa aiheuttavat ohjelmat. Petteri Järvinen määrittelee haittaohjelman seuraavasti: Sana haittaohjelma (malware) viittaa kaikkiin niihin ohjelmiin, jotka asentuvat tietokoneelle salaa tai lupaa kysymättä ja tuottavat käyttäjälle haittaa (Järvinen 2006, 77).

Tässä esityksessä ei ole järkevää käydä laajasti haittaohjelmia läpi, vaan muutamin esimerkein kertoa olemassa olevista, erilaisesta haittaohjelmatyypistä. Tunnetuin haittaohjelmatyyppi suurelle yleisölle on varmaankin tietokonevirus. *Tietokonevirus* on haittaohjelmatyyppi, joka leviää liittämällä itsensä osaksi ohjelmaa tai dokumenttia. Tietoko-

nevirukset eivät leviä itsestään tietokoneesta toiseen, kuten tietokonemadot, vaan ne ovat riippuvaisia käyttäjän vuorovaikutuksesta. (Lillbacka, 17). Virukset tuhoavat yleensä tietokoneen tiedostoja.

Toinen yleinen haittaohjelmatyyppi on *tietokonemato*. Tietokonemadot ovat ohjelmia, jotka lisääntyvät, toimivat itsenäisesti ja liikkuvat verkkoyhteyksiä pitkin. Tietokonevirusten ja tietokonematojen keskeisin ero on tapa jolla ne lisääntyvät ja leviävät. (Lillbacka, 22)

Tietokonematojen suurin haitta on yleensä niiden nopea leviäminen ja tietojärjestelmien kapasiteetin syöminen. Muutama vuosi sitten kun tietokonemadot yleistyivät, joidenkin matojen kohdalla seurattiin kuinka nopeasti ne levisivät ympäri maailmaa. Kyse oli usein vain muutamasta päivästä. Monesti madot olivat melko vähän harmia aiheuttavia ja niiden poistaminen koneelta onnistui helposti.

Kolmas tunnettu haittaohjelmatyyppi on ns. troijalainen. Esikuvansa mukaisesti troijalainen siirtyy tietojärjestelmästä toiseen jonkun muun ohjelman sisällä tai kylkiäisenä. Ennen yleinen levitystapa oli laittaa troijalainen sähköpostin liitteeksi ja kun sähköpostin avasi, troijalainen siirtyi avaajan tietojärjestelmään. Troijalaiset eivät pyri siirtymään koneesta toiseen itsenäisesti. Hyvin usein troijalaiset tuhoavat tiedostoja.

Neljäs tunnettu ohjelmatyyppi on spyware-ohjelmat. Ne leviävät esimerkiksi verkkosivustojen ja ilmaisohjelmien kautta. Niiden tarkoitus on hankkia kohdejärjestelmästä tietoja esimerkiksi sähköpostin lähettämistä varten. Muita tavoiteltavia tietoja ovat salasanat, tilinumerot jne.

Yhteenvetona haittaohjelmisto voidaan sanoa, että niiden tarkoitus on hankkia tietoa järjestelmän käyttäjästä, tuhota tiedostoja tai aiheuttaa muuten vaan haittaa.

4.1.2 Palvelunestohyökkäykset

Haittaohjelmien lisäksi huomiota ovat herättäneet erilaiset verkkohyökkäykset. Verkkohyökkäys on toiminta, jossa tietoverkon ja siihen kytkettyjen laitteiden välistä verkkoliikennettä heikennetään, häiritään, estetään, kaapataan, tuhotaan tai muutetaan. Verkkohyökkäys kohdistuu myös tietoverkkoon kytkettyjen laitteiden sisältämään tietoon. Palvelunestohyökkäyksen (Denial of Service, DoS) tarkoituksena on estää tai heikentää

verkkojen, järjestelmien tai sovellusten käytettävyyttä, esimerkiksi kuluttamalla järjestelmien resursseja niin paljon, että palvelun normaali käyttö estyy (Valitiovarainministeriö, 7). Palvelunestohyökkäykset ovat olleet esillä mm. erilaisten kansalaisjärjestöjen ja painostusryhmien toiminnassa. Yksi tunnetuimmista tapauksista liittyy Venäjän ja Viron välillä olleen patsaskiistan yhteyteen muutama vuosi sitten. Viron valtion sivustot olivat säännöllisten hyökkäysten kohteensa siitä lähtien, kun kiista neuvostoaikaisen sotilasmuistomerkin siirtämisestä pois Tallinnan keskustasta kärjistyi. Hyökkäyksistä epäiltiin Venäjää, mutta Naton mukaan ei ollut selvää kuka hyökkäykset toteutti. (Helsingin Sanomat, 1)

4.1.3 Bottiverkot

Kolmas ryhmä, joka tässä yhteydessä kannattaa mainita, on bottiverkko. Tietokoneet joihin on asennettu sama botti, eräänlainen haittaohjelma, muodostavat verkon, jota hyökkääjä voi hallita. Ison verkon hallinta onnistuu tavallaan samalla nopeudella ja vaivalla kuin yhden koneen hallinta. Verkon luomisen jälkeen hyökkääjä voi lähettää botille erilaisia käskyjä ja käyttää sitä haittatarkoituksiin. Bottiverkoissa voi olla satoja tai tuhansia koneita. Bottiverkot ovat verkkohyökkäysten teon työkaluja.

Ymmärtääkseen miksi haittaohjelmia tehdään, tulee tuoda esille myös tekijöiden taustoja. Siinäkin suhteessa on muutos tapahtunut. Haittaohjelmien tekijät ovat ajan kuluessa vaihtuneet. Aikanaan viruksia ja matoja kirjoittivat lähinnä nuoret, joita viehätti luvattoman toiminnan houkutus ja sen harrastajapiireissä tuottama kunnia. Tänään harrastajien tilalle ovat tulleet ammattilaiset, jotka tavoittelevat taloudellista hyötyä. Haittaohjelmien levittäjinä toimivat yhä useammin kansainväliset liigat ja järjestäytynyt rikollisuus. (Järvinen 2006, 77)

Tietokonerikollisuus täyttää nykyisellään menestyksellisen liiketoiminnan vaatimukset. Sangen vaatimattomallakin panoksella voidaan hankkia suurta hyötyä. Toistaiseksi meitä suomalaisia on suojannut massiiviselta tietoverkkorikollisuudelta erikoinen kieli sekä hyvä valmius käyttää tietoturvatyökaluja ja noudattaa tietoturvakäytänteitä. (Kuusimäki, 11)

Haittaohjelmien luonnetta, kekseliäisyyttä ja business-ajattelua kuvaa seuraava esimerkki. Tapauksesta on ollut tietoa lehdistössä aivan viime aikoina. Poliisi joutui laittamaan sivuilleen tällaisen tiedotteen.

Tietokoneen käyttäjiä lähestytään Suomen poliisin nimissä. Käyttäjän tietokone lukkiutuu ja ruudulle tulee viesti, jossa kerrotaan suomeksi poliisin nimissä lukituksen johtuvan laittomasta internet-selailusta, tai muusta laittomasta aktiviteetista internetissä. Samassa viestissä kerrotaan, että lukitus voidaan poistaa maksamalla 100 euron sakko PaySafe-palvelun kautta. Viestillä tai lukituksella ei ole mitään tekemistä Suomen poliisin kanssa. Poliisi ei lukitse käyttäjien tietokoneita verkon yli tai pyydä maksua niiden avaamisesta. (Poliisi, 1) Vastaavanlaista on tehty aiemmin mm. Ruotsin poliisin, Saksan keskusrikospoliisin ja Lontoon Metropolitan Policen nimissä. Tekijät ovat todennäköisesti ulkomaalaisia koska viestissä on erittäin paljon kielivirheitä. Kyseessä on ns. ransomware eli haittaohjelma, jonka avulla kiristetään haittaohjelman uhrilta rahaa. Olen itse nähnyt ohjelman ja se oli vaikuttava muutamia yksityiskohtia lukuun ottamatta.

4.2 Väärennys

4.2.1 Säännöksen kehittyminen

Tietoturvan tietojen eheyttä loukkaavista teoista käsitellään ensimmäisenä väärennys. Väärennys on rikos, jota koskevat säännökset ovat rikoslain 33 luvussa. Luvun ensimmäisessä pykälässä lausutaan näin; 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. Perussäännös on tehty rikoslain kokonaisuudistuksen yhteydessä 24.8.1990/769. Lukuun on lisätty Euroopan unionin puitepäätöksen 2001/413/YOS edellyttämät muutokset 2003. (514/2003). Lisäyksen mukaan myös rikoksen yritys on rangaistavaa.

Luvun 2 §:ssä käsitellään törkeä väärennys. Pykälän toisen momentin mukaan, jos rikoksentekijä käyttää väärennysrikoksen tekemistä varten hankittua teknistä laitteistoa, taikka muuten toimii erityisen suunnitelmallisesti, katsotaan teko törkeäksi. Törkeän väärennyksen rangaistus on vankeutta vähintään neljä kuukautta ja enintään neljä vuot-

ta. 3 §:n mukaan jos teko on vähäinen, voidaan henkilö tuomita lievästä väärennöksestä sakkoon. Myös väärennysaineiston hallussapidosta voidaan tuomita luvun 4 §:n mukaan sakkoon tai vankeuteen enintään kuudeksi kuukaudeksi.

Euroopan Unionin Komission tiedonanto Neuvostolle, Euroopan Parlamentille, Talous ja sosiaalikomitealle ja alueiden komitealle vuodelta 2001 johti Suomessa tietotekniikkaan liittyvän lainsäädännön tarkistuksiin. Hallitus antoi niistä esityksen 153/2006. Hallituksen esityksen kohdassa 7 artikla käsitellään tietokoneavusteinen väärennys. Artiklassa tuodaan selkeästi esiin se, että tietokoneen avulla tehty dokumentti tai sitä vastaava data tietojärjestelmässä on väärennys kuten aikaisemmin tehdyt paperiväärennykset.

Vaikka tämä nykyään tuntuu selvältä asialta, aina ei ole ollut näin. Pihlajamäki kertoo kirjassaan korkeimman oikeuden päätöksestä KKO 1985 II 60. Kyseisessä tapauksessa tietokoneelle tehty tilien muuttaminen hyötymistarkoituksessa ei johtanut rangaistukseen väärennyksestä koska korkein oikeus ei pitänyt tietojärjestelmän dataa väärennyksessä tarkoitettuna asiakirjana. Henkilö kuitenkin tuomittiin petoksesta.(Pihlajamäki, 176)

4.2.2 KKO:2012:54

Rikoslain väärennystulkinnat ovat edelleen vaikeita. KKO antoi keväällä 2012 tuomionsa tapauksesta joka oli alkanut 2007 Vantaan käräjäoikeudessa. Tapaus on ainakin siinä mielessä mielenkiintoinen, että tuomiot vaihtelivat eri oikeusasteissa.

Oikeuden pöytäkirjojen mukaan syytetty A oli hankkinut laitteen, jolla puhelimen IMEI-koodi pystytään muuttamaan. Puhelimen IMEI-koodi on puhelimen yksilöivä koodi, josta ilmenee missä puhelin on valmistettu ja mikä ohjelmaversio puhelimeen on alun perin asennettu. Koodi noudattaa kansainvälistä standardia ja se on yksikäsitteinen koko maailmassa. Syytetty oli hallussaan olevalla laitteella muuttanut matkapuhelimensa IMEI-koodia ja yrittänyt päästä puhelimella puhelinverkkoon. Yritys oli onnistunut hetkeksi.

Vantaan käräjäoikeudessa syyttäjä vaati teosta rangaistuksia mm. nuorena henkilönä tehdystä väärennyksestä tai vaihtoehtoisesti väärennysaineiston hallussapidosta. Vantaan käräjäoikeus oli antanut tuomionsa 30.8.2007. Käräjäoikeus hylkäsi syytteet väärennyksestä ja väärennysaineiston hallussapidosta nuorena henkilönä. Ainoa tuomio minkä henkilö A sai, oli sakko nuorena henkilönä tehdystä kätkemisrikkomuksesta.

Käräjäoikeus totesi, ettei A:n menettely täyttänyt rikoksen tunnusmerkistöä. Oikeuden mielestä syytetyn tarkoituksena ei ollut käyttää muunneltua koodia sellaisessa yhteydessä ja sellaisella tavalla, jossa joku muu voisi erehtyä sen oikeellisuudesta. A:n koodiksi antama 000-merkkisarja ei missään määrin muistuttanut oikeaa IMEI-koodia ja se tuskin oli sellainen, jonka puhelinverkko syytteessä tarkoitetulla tekopaikalla tunnistaisi. (KKO:2012:54, 1)

Asia eteni hovioikeuteen. Syyttäjä vaati, että A tuomitaan syytteen mukaisesti kohdassa 3 ensisijaisesti väärennyksestä tai toissijaisesti väärennysaineiston hallussapidosta. Helsingin hovioikeus antoi asiasta tuomionsa 17.10.2008. Hovioikeus tuomitsi A:n nuorena henkilönä tehdystä väärennyksestä ja hänen syykseen luetusta kohdan 2 rikoksesta, nuorena henkilönä tehdystä kätkemisrikoksesta, yhteiseen sakkorangaistukseen. Lisäksi hovioikeus tuomitsi rikoksessa käytetyn laitteiston valtiolle menetetyksi.

Hovioikeus perusteli päätöstään sillä, että matkapuhelimen IMEI-koodi voi olla rikoslain 36 luvun 1 ja 6 §:ssä tarkoitettu todistuskappale. A oli kertonut suunnittelevansa matkapuhelinten huoltoyrityksen perustamista osaksi syynä kokeilla tekaistua koodia. Hovioikeus ei pitänyt kertomusta uskottavana. Hovioikeus kuuli myös todistajana Nokia Oyj:n tuotteiden turvallisuudesta vastaavaa henkilöä ja Nokian tutkimuskeskuksen johtavaa tutkijaa. Heidän kertomuksensa perusteella A:lla ei voinut olla mitään syytä muuttaa IMEI-koodia. He pitivät myös mahdollisena, että A olisi voinut päästä puhelimellaan verkkoon ja käyttämään sitä. Näiden selvitysten perusteella hovioikeus katsoi A:lla olleen todellinen tarkoitus käyttää väärentämäänsä IMEI-koodia ja näin syyllistynyt väärennykseen.

Tuomioon haettiin valituslupaa korkeimmasta oikeudesta ja valituslupa myönnettiin. Valituksessaan A vaati, että syyte nuorena henkilönä tehdystä väärennyksestä hylätään ja hänet vapautetaan tältä osin tuomitusta sakkorangaistuksesta sekä menettelyseuraamuksesta. Syytetyn perusteluna oli, että koodia vaihtamalla hän ei ollut aikonut harhauttaa ketään. Kokeilun jälkeen hän oli vaihtanut koodin takaisin. A kertoi hankkineensa ulkomailta postimyynnistä Flasher Box-laitteen. Hänellä ei mielestään ollut myöskään hallussaan pääasiallisesti väärennysrikoksen tekemiseen tarkoitettua laitetta eikä muutakaan väärennysaineistoa.

Korkeimman oikeiden ratkaisu. Hovioikeuden tuomiota muutetaan.

A:ta vastaan ajettu syyte nuorena henkilönä tehdystä väärennyksestä ja vaihtoehtoinen syyte väärennysaineiston hallussapidosta (syytekohta 3, tekoaika 1.12.2005 - 23.8.2006) hylätään. A tuomitaan käräjäoikeuden hänen syykseen lukemasta nuorena henkilönä tehdystä kätkemisrikkomuksesta (syytekohta 2, tekoaika 20.3. - 31.3.2006) 20 päiväsakkoon eli maksamaan sakkoa 6 euron päiväsakon rahamäärän mukaan 120 euroa. Menettämisseuraamusta koskeva vaatimus hylätään ja A vapautetaan hovioikeuden tuomitsemasta menettämisseuraamuksesta. Takavarikot 6840/R/6802/06/KEY/1 ja 6840/R/16606/06/TVP/1 kumotaan sekä Flasher box -laite, tietokoneohjelma ja tietokonetarvikkeet määrätään palautettavaksi A:lle.

Muilta osin hovioikeuden tuomiota ei muuteta. (KKO 2012:54, 4)

Korkein oikeus toi ratkaisunsa perusteeksi esille mm. seuraavat asiat. A oli kertomansa mukaan vain kokeilumielessä muuttanut laitteen avulla oman puhelimensa IMEI-koodia 000-muotoiseksi eli viisitoista merkkiä pitkäksi nollanumerosarjaksi. Sitten hän oli saanut sen avulla hetkeksi yhteyden verkkoon. Korkein oikeus toteaa ensiksikin, että A:n henkilöllisyys on verkkopalvelun käyttöoikeuden osalta ollut palvelun ylläpitäjän tunnistettavissa hänen puhelimessaan olevan SIM-kortin perusteella. IMEI-koodilla ei ole merkitystä verkkopalvelun käyttöoikeuden osalta. Korkein oikeus katsoo, että tässä tapauksessa numerosarjaltaan mahdottoman IMEI-koodin avulla aikaansaadulla hetkellisellä verkkoyhteydellä on täytynyt olla vain vähäinen merkitys verkko-operaattorin näkökulmasta. Normaali verkkokäyttö oli A:lta epäonnistunut väärän IMEI-koodin vuoksi. Niin Korkeimman oikeuden päätös väärennyksen osalta olikin syytteen hylkääminen. Sen perusteella mitä on esitetty, Korkein oikeus katsoo, ettei A ole käyttänyt puhelimeensa väärentämäänsä IMEI-koodia harhauttavana todisteena. Asiassa ei ole väitetty, että A:lla olisi ollut aikomus lisäksi jollakin muulla tavalla käyttää sanottua väärennettyä IMEI-koodia harhauttavana todisteena oikeudellisesti merkityksellisessä yhteydessä. Tämän vuoksi Korkein oikeus katsoo, että A ei ole syyllistynyt siihen väärennysrikokseen, josta syyttäjä on hänelle vaatinut rangaistusta. (KKO 2012:54, 4)

Rikoslain säännöksissä ei mitenkään oteta kantaa siihen miten väärennös pitäisi tehdä. HE 153/2006 joka perustuu Yleissopimuksen selitysmuistioon, luetellaan tekotavat. Tekotapoina tulevat ensinnäkin kyseeseen järjestelmässä oleva dataan kajoavat tekotavat eli vahingoittaminen, tuhoaminen, turmeleminen, muuttaminen ja poistaminen. Tekotapaluettelo on samanlainen niin datan vahingoittamiskohdassa kuin tietokoneavusteisessa väärennyksessä. (HE 153/2006, 9)

4.3 Petos

4.3. 1 Säännöksen kehittyminen

Toinen tietojärjestelmän tietojen eheyttä loukkaava rikos on petos. Petosta koskeva rikoslain osa on luku 36. Alkuperäinen petosta koskeva rikoslain 36 luku tuli voimaan 1991. Lain ensimmäisen momentin teksti, josta käy esiin teon tapa, on seuraava:

Joka hankkii 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.

Säännöstä tarkennettiin 2003 toisella momentilla. Tarkennuksessa tuotiin selvästi esiin myös se, että petos voi tapahtua myös tietojärjestelmää hyväksi käyttäen. Myös teon yritys on rangaistava.

Luvun toisessa pykälässä tuodaan esiin rikoksen törkeän muodon tunnusmerkit: 1) jos petoksessa tavoitellaan huomattavaa hyötyä, 2) aiheutetaan huomattavaa tai erityisen tuntuvaa vahinkoa, 3) rikos tehdään käyttämällä hyväksi vastuullisen asemaan perustuvaa erityistä luottamusta tai 4) rikos tehdään käyttämällä hyväksi toisen erityistä heikkoutta tai muuten turvatonta tilaa ja petos on myös kokonaisuudessaan törkeä, rikoksentekijä on tuomittava törkeästä petoksesta vankeuteen vähintään neljäksi kuukaudeksi ja enintään neljäksi vuodeksi.

Luvun 3 §:ssä on säännökset lievästä petoksesta, joka on sitten 8 §:n mukaan asianomistajarikos eikä syyttäjä saa nostaa syytettä ilman asianomistaja ilmoita sitä syytteeseen pantavaksi.

Hallituksen esityksen 153/2006 mukaan Suomen lainsäädäntö vastaa Euroopan Unionin puitepäätöksen 2001/413/YOS edellyttämää säännöstöä ja näin ollen lakia ei tarvitse näiltä osin muuttaa.

4.3.2 Petos vai näpistys

Petoksia ja huijauksia yritetään tehdä tietoverkkojen avulla jatkuvasti. Poliisi ja kuluttajavirasto ovat laatineet luettelon yleisimmistä petos ja huijaustyypeistä. Listalla ovat n. nigerialaiskirjeet, niihin verrattavat lotto- ja arpajaisvoitot ja muut tekaistut avunpyynnöt. Toisena listalla ovat myyjien huijaukset internet-kaupassa, ostaja ei saa tilattua tai maksettua tuotetta ja myyjä katoaa. Ostajaa huijataan myös ylihintaisilla tuotteilla ja etumaksuilla. Verkossa leviävät myös ketjukirjeet ja verkostomarkkinointi, josta hyötyy organisaation ylin taso. Yleistä, lähes päivittäistä ovat myös pankkitili-, luottokortti- ja henkilötietojen kalastelu (ns. phishing) ja tietojen kalastelu ohjaamalla käyttäjä valesivustoille (ns. pharming). (Muttilainen, 53-54)

Tietokoneavusteisia petoksia ja niistä seuranneita oikeudenkäyntejä on Suomessa käyty harvoin. Seuraavassa on yksi sellainen, ei petosoikeudenkäynti mutta se sopii tähän aiheeseen. Hyvinkään käräjäoikeus oli tuominnut syytetyn rikoslain 28 luvun 3 §:n 1 momentin mukaan nuorena henkilönä tehdystä näpistyksestä. Henkilö A oli 12.2.2010-5.3.2010 anastanut Habbo.fi tiliin liittyviä virtuaalisia huonekaluja. Huonekalujen arvo oli 465 euroa.

A oli valittanut tuomiosta hovioikeuteen. A oli perustellut vaatimustaan sillä, että anastuksen kohde oli ollut aineeton omaisuus ja ettei aineeton omaisuus voi olla näpistyksen kohteena.

Kouvolan hovioikeus antoi keväällä 2011 päätöksen, ettei Habbo Hotellista vietyjen huonekalujen varastaminen ole varkausrikos. Hovioikeuden perusteluista ilmenee, että lain mukaan ei voida rangaista näpistyksestä tai varkausrikoksesta, jos kyseessä on ei-materiaalinen omaisuus.

Internetissä toimivan Habbo Hotel -palvelun niin sanottuja sähköisiä tai virtuaalisia huonekaluja ei voida pitää esitöissä tarkoitettuna irtaimena omaisuutena. Kysymys on aineettomasta omaisuudesta, jolla on taloudellinen arvo.(Kouvolan HO, 1)

> Rikosoikeuden keskeinen periaate on laillisuusperiaate. Se on ilmaistu Suomen perustuslain 8 §:ssä ja lisäksi rikoslain 3 luvun 1 §:ssä. Jälkimmäisen lainkohdan 1 momentin mukaan rikokseen syylliseksi saa katsoa vain sellaisen teon perusteella, joka tekohetkellä on laissa nimenomaan säädetty rangaistavaksi, ja 2 momentin mukaan rangaistuksen ja muun ri-

> kosoikeudellisen seuraamuksen on perustuttava lakiin. Lain esitöiden (HE 44/2002 vp s. 29) perusteella tuomioistuin ei rangaistussäännöstä soveltaessaan saa mennä lain kirjaimen ulkopuolelle eikä täydentää lakia analogiapäätelmään turvautumalla. Korkeimman oikeuden ratkaisuista (KKO 2007:67 ja 81) ilmenevän oikeusohjeen mukaan käsitteiden tulkinta on kuitenkin välttämätöntä ja oikeutettua myös yksittäisiä rikostunnusmerkistöjä sovellettaessa edellyttäen, että tulos on sopusoinnussa tunnusmerkistöstä ilmenevän, rangaistusuhalla tavoitellun suojan kanssa ja että lopputulos on kohtuudella tekijän ennalta arvattavissa. (Kouvolan HO:2011:3, 2)
>
> Rikoslain 28 luvun varkausrikoksia ja näpistystä koskevien säännösten tarkoituksena ei ole turvata kaikkea omaisuutta. Tämä käy ilmi rikoslain 28 luvun 1 §:n 1 momentin sanamuodosta, jossa anastuksen kohteen edellytetään olevan irtainta omaisuutta. Lisäksi lainsäätäjä on edellä mainituissa esitöissä selvästi rajannut säännösten soveltamisalaa. Muun muassa rahavarojen ei ole katsottu olevan irtainta omaisuutta silloin, kun ne ovat sähköisessä muodossa. Lainsäätäjä ei ole myöskään katsonut sähköä ja lämpöä irtaimeksi omaisuudeksi, mutta niiden osalta on säädetty oma säännöksensä, jonka perusteella niihin sovelletaan edellä mainittuja säännöksiä. (Kouvolan HO:2011:3, 3)

Ilmeisestikin kuvatun teon tekijää olisi voitu syyttää lievästä petoksesta. Oikeuden pöytäkirjoista ei kuitenkaan selviä tarkasti miten teko on tehty.

4.4 Maksuvälinepetos

4.4.1 Säännöksen kehittyminen

Viime aikoina lehdistössä on ollut esillä maksuautomaattien kautta tapahtuneet rikokset. Erilaisilla menetelmillä on saatu selville uhrin luotto- tai maksukorttiin liittyvät tunnukset, joita on sitten käytetty rahan siirtämiseen uhrin tililtä rikoksen tekijöille. Kysymys on silloin maksuvälinepetoksesta. Maksuvälinepetoksen kohdalla on kysymys erityisrikoksesta, joka eräissä tapauksissa muodostaa yhden tietokonepetoksen alalajin (Pihlajamäki, 204).

Maksuvälinepetoksen säännökset ovat rikoslain 37 luvussa 8:ssä. 8 §:n ensimmäisessä momentissa on säännöksen teksti:

Joka hankkiakseen itselleen tai toiselle oikeudetonta taloudellista hyötyä, 1) käyttää maksuvälinettä ilman sen laillisen haltijan lupaa, lupaan perustuvan oikeutensa ylittäen tai muuten ilman laillista oikeutta tai 2) luovuttaa maksuvälineen tai maksuvälinelomakkeen toiselle saattaakseen sen ilman laillista oikeutta käytettäväksi on tuomittava maksuvälinepetoksesta sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

9 §:ssä on säännös törkeästä maksuvälinepetoksesta. Siitä rangaistus on vähintään 4 kuukautta ja enimmillään 4 vuotta vankeutta. Törkeän maksuvälinepetokseen tuomitaan, jos aiheutetaan huomattavaa tai erityisen tuntuvaa vahinkoa tai rikos muuten on erityisen suunnitelmallisesti tehty. Luvusta löytyy myös lievän maksuvälinepetoksen säännökset 10 §:stä. Siitä rangaistus on sakko. Lainsäädäntöä kiristettiin 2003 ja mukaan otettiin maksuvälinepetoksen valmistelu. Sen säännökset ovat 11 §:ssä ja sen mukaan henkilö jolla on maksuvälinepetoksen tekemiseen tarvittavia välineitä tai materiaalia tuomitaan sakkoon tai enimmillään vuodeksi vankeuteen. 12 §:ssä tarkennetaan mitä maksuvälineillä tarkoitetaan, pankki-, maksu- tai luottokorttia.

Euroopan neuvoston raportti vuodelta 2001 ei erittele varsinaisesti maksuvälinepetosta muusta tietokoneavusteisesta petoksesta, vaan käsittelee sen samalla artiklassa 8. HE 153/2006 mukaan kyseisen artiklan maksuvälinepetokseen viittaavat asiat on riittävällä tasolla hoidettu Suomessa rikoslain 37 luvussa.

4.4.2 Maksukorttirikollisuus on kasvava ilmiö

Suomessa on vaikea saada luotettavia tilastoja poliisin tietoon tulleista tietotekniikkaan liittyvistä rikoksista. Kyse ei ole siitä, että tietoja jotenkin salailtaisiin. Tietotekniikan termistö on rikosten osalta vielä melko nuorta joka johtaa siihen, että tilastoja tehdään usein erilaisien kriteerien perusteella. Ongelmana tilastoissa on myös se, että vertailtaessa rikostilastoja ja esimerkiksi tuomioita, ajallinen viive on vaikea arvioida tarkasti. Joistakin erillisrikoksista on saatavissa tarkkoja tietoja, kuten maksukorttirikoksista. Seuraavassa on maksukorttirikosten määrän kehittyminen viimeisen viiden vuoden aikana.

Suomessa tehdyt, poliisin tietoon tulleet maksukorttirikosten määrä on kasvanut seuraavasti. Vuosittaiset kokonaismäärät 2007-2011.(Poliisi KRP, 3)

2007	3784
2008	3835
2009	5166
2010	4517
2011	5670

Maksukorttirikollisuudessa on kysymys suurimittaisesta rikollisesta toiminnasta. Europolin mukaan, vuonna 2010, maksukorttirikollisuus aiheuttaa Euroopan unionin alueella vuosittain n. 1,5 miljardin euron tappiot. (Poliisi KRP, 2)

Rikosten tekeminen motiivina on raha. Neljä yleisintä tekotapaa ovat poliisin mukaan

1) maksukorttien avaintietojen kopioiminen verkosta haittaohjelmilla. Korteilla tilataan sitten helposti rahaksi vaihdettavaa tavaraa.
2) maksukorttien kopioiminen ns. skimmauslaitteilla automaateilta. Tietojen avulla luoduilla korteilla nostetaan automaateilta rahaa.
3) kopioitujen tietojen avulla valmistetaan aidon kortin näköisiä kortteja joilla ostetaan helposti rahaksi vaihdettavaa tavaraa
4) automaateilla asioivien kansalaisten PIN-koodi kurkitaan olan yli ja varastetaan sitten maksukortti, jolla sitten nostetaan rahaa.

(Poliisi KRP, 1)

Maksuvälinepetoksiin kuuluu muitakin rikoksia kuin maksukorttirikokset mutta ne ovat ylivoimaisesti suurin rikoksen tekotapa maksuvälinepetoksissa.

4.4.3 Oulun käräjäoikeus R 12/714

Joitakin maksuvälinepetoksia on saatu selvitettyä ja niin pitkälle, että tekijät on voitu asettaa syytteeseen. Seuraavassa kuvataan Oulun käräjäoikeudessa keväällä 2012 ollut tapausta. Tuomio jutussa annettiin 13.4.2012 kolmelle ulkomaalaistaustaiselle henkilölle törkeästä maksuvälinepetoksesta rikoslain 37 luvun 9 §:n mukaan.

Tapauksen kulku oli lyhyesti seuraava. Kolme mieshenkilöä oli yhdessä tuonut maahan ja pitäneet hallussaan erityisesti maksuvälinelomakkeen valmistamiseen soveltuvia välineitä ja tarvikkeita eli pankki- ja luottokorttien kopiointilaitteita. He olivat myös hankkineet erityisesti tietoverkoissa tapahtuvaan maksuliikenteeseen soveltuvia tallenteita, eli korttien magneettiraitojen ja tunnuslukujen tietoja sisältäviä tiedostoja. Syksyn 2011 aikana he olivat asentaneet 15 pankkiautomaattiin kyseiset lukulaitteet ja korttien salai-

sia tunnuslukuja kuvaavat kamerat. Näin hankkimansa tunnusluvut he olivat luovuttaneet ulkomaille saattaakseen maksuvälineet näin ilman lupaa käytettäväksi. Kuvattujen tunnuslukujen avulla korteista oli valmistettu kopioita ja korttikopioiden ja kuvattujen tunnuslukujen avulla korttien ja tilien alkuperäisten omistajien tileiltä oli Yhdysvalloissa nostettu tai yritetty nostaa rahaa.

Syyttäjän rangaistusvaatimus olivat 1) törkeä maksuvälinepetos rikoslain 37 luvun 9 §:n mukaan 2) maksuvälinepetoksen valmistelu rikoslain 37 luvun 11 §:n mukaan.

Kaikki syytetyt kiistivät kaikki syytteensä.

Tuomiot olivat kaikille kolmelle samanlaiset. Kukin henkilö tuomittiin törkeästä maksuvälinepetoksesta 2 vuodeksi 2 kuukaudeksi vankeuteen. Heidät tuomittiin myös menettämään valtiolle rikoksentekovälineinä maksukorttien kopiointilaitteet. Tuomioon liittyi myös yksityisoikeudellinen korvausvelvollisuus, joka oli yhteensä lähes 100.000 euroa. Korvaukseen olivat oikeutettuja useat pankit ja luottolaitokset.

Oikeus perusteli tuomioita seuraavasti. Tärkein todiste rikoksesta saatiin 26.9.2011, kun rikoksentekijät otettiin kiinni Kokkolassa ja heidän hallustaan löytyi pankkiautomaattien kuvauksessa tarvittavat skimmauslaitteet. Laitteita oli yhteensä neljä kappaletta. Heidän puhelimiensa paikantamistietojen mukaan voitiin todistaa, että he olivat olleet jokaisella niistä paikkakunnista joilla skimmausta oli tapahtunut. Henkilötodistaja kuultiin keskusrikospoliisin rikosinsinööriä, jonka todistuksen mukaan henkilöiltä takavarikoiduista tallenteista löytyi ”huonolaatuista” maksukorttidataa. Sormenjälkien avulla todistettiin henkilöiden yhteys käytettyihin skimmauslaitteisiin. Rikos täytti myös törkeän petoksen tunnusmerkit

> Rikoksen suunnitelmallisuuteen viittaa se, että kyseiset laitteet sopivat vain Suomessa oleviin OTTO-automaatteihin. Teko toteuttaa siis myös rikoslain 37 luvun 9 §:n 2-kohdassa mainitun kvalifiointiperusteen. Rikos on myös kokonaisuutena arvostellen törkeä, koska se on kohdistunut useisiin automaatteihin useilla eri paikkakunnilla toistuvasti lähes 2 kuukauden aikana ja on kohdistunut laajaan joukkoon maksukorttien käyttäjiä. (Oulun KO, 15)

5 KÄYTETTÄVYYTEEN LIITTYVÄT RIKOKSET

Tietojenkäsittelyn tietoturvan kolmas tekijä, tietojärjestelmän käytettävyys on kolmesta tekijästä vaikein määritellä. Luottamuksellisuuteen liittyy tietojärjestelmään tunkeutuminen ja tietojen eheyteen tietojen muuttaminen, molemmat ovat tekoina yksiselitteisiä. Käytettävyyden estäminen voi tapahtua monella tavalla, lopputulosta voi kuitenkin arvioida yksiselitteisesti, onko järjestelmä käytettävissä vai ei. Määrittelyn vaikeus johtuu osaksi siitä, että tietoliikenteen osuus on noussut nopeasti oleelliseksi osaksi tietojärjestelmän käyttöä. Käytettävyyteen liittyvät myös yleisimmin tekniset ongelmat. Taustalla on internetin yleistyminen ja sen mukanaan tuomien monien teknisten asioiden yleistyminen. Tällä hetkellä on meneillään voimakas siirtyminen ns. pilvipalveluihin, joka tekee tietojärjestelmän käytettävyyden entistä riskialttiimmaksi. Pienyritykset luopuvat perinteisistä lähiverkoista ja käyttävät yrityksen sisälläkin internet-verkkoa. Tietojärjestelmän käytettävyys liittyy lähes aina jotenkin järjestelmän tietoverkkoyhteyksiin. Toinen tiedon eheyden ja käytettävyyden välisen määrittelyn vaikeus on siinä, että tällä hetkellä monet haittaohjelmien kategoriat voivat kohdistua näihin molempiin tietoturvan osa-alueisiin. Esimerkiksi, on olemassa tietokoneviruksia tai haittaohjelmia jotka muuttavat kohdejärjestelmänsä tiedostoja ja on viruksia jotka ainoastaan estävät järjestelmän käytön. Tästä syystä vaaran aiheuttaminen tietojenkäsittelylle voidaan liittää käytettävyyden estämisen lisäksi myös tietojen eheyttä loukkaaviin rikoksiin. Rikollisen toiminnan lopputulos on kuitenkin se, että tietojärjestelmän käyttäjä ei jostain syystä pysty käyttämään järjestelmäänsä. Suomen lainsäädännössä tietojärjestelmän käytettävyyteen kohdistuvia tekoja kriminalisoidaan nimikkeillä vaaran aiheuttaminen tietojenkäsittelylle, vahingonteko ja tietojärjestelmän häirintä. Niitä koskevat säännökset ovat rikoslain 34 luvun 9 a ja b §:ssä, 35 luvun 2 ja 3 §:ssä, 38 luvun 7 a ja 7 b §:ssä.

5.1 Vaaran aiheuttaminen tietojenkäsittelylle

5.2.1 Säännöksen kehittyminen

Rikoslain 34 lukuun lisättiin 1.12.1999 uusi 9 a §. HE 4/1999:ssä esiteltiin lainsäädäntöön täysin uusi asia, tietokonevirus. Hallituksen esityksessä ehdotetaan niin kutsutun

tietokoneviruksen valmistaminen ja levittäminen kriminalisoitavaksi rikoslakiin otettavalla uudella säännöksellä. Tietokoneviruksella tarkoitetaan tietojenkäsittelylle, tieto- tai telejärjestelmän toiminnalle haittaa aiheuttamaan tai sellaisen järjestelmän sisältämiä tietoja tai ohjelmistoja vahingoittamaan, suunniteltua tietokoneohjelmaa tai ohjelmakäskyjen sarjaa. (HE 4/1999, 1).

Näin tietokoneviruksen tekeminen ja levittäminen kriminalisoitiin. Seuraamusta tästä rikoksesta olisi sakkoa tai vankeutta enintään kaksi vuotta.

Säännöksen sisältöön jouduttiin palaamaan Neuvoston puitepäätöksen 2005/222/YOS 6:n artiklan perusteella. Hallituksen esityksessä todettiin, että nykyinen lainsäädäntö kattaa ainoastaan tietokoneviruksen ja vastaavan haittaohjelman valmistamisen ja levittämisen. Säännöksiin tulisi lisätä ohjelmien hallussapito ja kiellettyihin ohjelmiin lisätä tietomurtoon kehitetyt ohjelmat. Näin päädyttiin tällä hetkellä voimassa olevaan säännökseen 34 9 a § vaaran aiheuttaminen tietojenkäsittelylle ja 34 9 b § tietoverkkorikosvälineen hallussapito.

Lakia uudistettiin vielä 2011. Syyteoikeutta tarkennettiin. Syyttäjä ei saa nostaa syytettä viestintäsalaisuuden loukkauksesta, törkeästä viestintäsalaisuuden loukkauksesta, tietojärjestelmän häirinnästä, tietomurrosta tai suojauksen purkujärjestelmärikoksesta, ellei asianomistaja ilmoita rikosta syytteeseen pantavaksi tai ellei rikoksentekijä rikosta tehdessään ole ollut yleistä posti- tai teletoimintaa harjoittavan laitoksen palveluksessa taikka ellei erittäin tärkeä yleinen etu vaadi syytteen nostamista. Tuomioistuimen on tällaista rikosta koskevaa asiaa käsitellessään varattava tietosuojavaltuutetulle tilaisuus tulla kuulluksi. (HE 286/2010)

5.2.2 Porin käräjäoikeus

Porin käräjäoikeudessa oli 2008 käsiteltävänä tapaus jossa syytetty sai tuomion vaaran aiheuttamisesta tietojenkäsittelylle. Syytetty oli valmistanut tai asettanut saataville sellaisia tietokoneohjelmia tai ohjelmakäskyjen osia joilla saattoi aiheuttaa haittaa tai vaaraa tietojenkäsittelylle tai tietojärjestelmälle.

Syytetty oli rikoksen tekoajankohtana laatinut kolmannen henkilön pyynnöstä useita haittaohjelmia, jotka hän oli luovuttanut tälle ohjelmien levittämistä varten. Syytetty oli valmistanut tekoajankohtana ainakin nimeämänsä Borg, Life-bot ja SiRa-nimiset haittaohjelmat ja tehnyt kahdesta viimeksi mainitusta ohjelmasta useita kymmeniä eri variaa-

tioita, jotka häneltä ohjelman tilannut henkilö oli levittänyt maailmanlaajuisesti sähköpostilähetysten yhteydessä, miljooniin eri osoitteisiin.

Syyttäjän rangaistusvaatimus oli 1) vaaran aiheuttaminen tietojenkäsittelylle rikoslain 34 luvun 9a §:n mukaan. Tapahtuma-aika oli 1.5.2005-27.6.2006 Porissa. Syyttäjä vaati myös rikosvälineen menettämistä valtiolle, rikoslaki 10 luku 4 §. Asianomistajan, Oy Renholm & Co Ab vaatimus oli, tietokoneen kovalevyn ja sen asennuskustannusten korvaus 528,20 euroa. (Porin Ko, 1-2)

Syytetty oli tunnustanut menetelleensä syytteessä selostetulla tavalla. Hän oli myös tarkentanut toimiaan ja kertonut tehneensä ohjelman, joka avaa tietokoneen takaportin. Tietojen poimiminen koneelta on edellyttänyt erillistä ohjelmaa ja ohjelmointia, ja nämä ohjelmat ovat olleet jonkun muun tekemiä. (Porin KO, 2)

Käräjäoikeuden ratkaisun mukaan syytetty on syyllistynyt vaaran aiheuttamiseen tietojenkäsittelylle. Käräjäoikeus perusteluiden mukaan syytetty oli tehnyt haittaohjelmien edellä kuvatun mukaisesti. Sen lisäksi käräjäoikeuden mukaan saastuneita tietokoneita oli löytynyt 7.994 kappaletta. Suomesta oli haittaohjelmia löytynyt neljästä yrityksestä. Syytetyn tekemien ohjelmien avulla työn tilaaja oli saanut haltuunsa n. 64 miljoonaa sähköpostiosoitetta. Ohjelmien avulla aikaansaadussa bot-verkossa oli ollut kymmeniä tuhansia tietokoneita. Vaaran aiheuttamista tietojenkäsittelylle koskeva rikoslain 34 luvun 9 a §:ää on muutettu syytteessä tarkoitetun tekoajan jälkeen. Lähtökohta on se, että rikokseen sovelletaan sitä lakia, joka oli voimassa rikoksen tekohetkellä. Vaikka lakia on muutettu, sen seuraamukset ovat samat.

Syytetyn tuomio vaaran aiheuttamisesta tietojenkäsittelylle on 7 kuukautta vankeutta. Käräjäoikeuden mukaan syyllisen aikaisemmat rangaistukset estävät ehdollisen tuomion. Vankeusrangaistus muutettiin yhdyskuntapalveluksi 162 tuntia. Tämän lisäksi rikoksentekoväline tuomittiin menetetyksi valtiolle. Syyllinen velvoitettiin korvaamaan myös asianomistajan, Oy Renholm & Co Ab vaatimus 528,20 euroa.

5.2 Vahingonteko ja tietojärjestelmän häirintä

Viimeisinä rikosnimikkeinä käsitellään vahingonteko ja tietojärjestelmän häirintä. Niitä koskevia oikeudenkäyntejä on käyty Suomessa vähän. Syynä tähän voi olla, että tietojärjestelmän häirintä on melko uusi rikosnimike, se on ollut lainsäädännössä vasta noin

viisi vuotta. Vahingonteko taas mielestäni edellyttää lain tekstin perusteella fyysistä vahingontekoa tietojärjestelmää kohtaan, ja sen suojaaminen on sen vuoksi paljon helpompaa.

5.2.1 Vahingonteko

Euroopan neuvoston raportti vuodelta 2001, 4:n artikla Datan vahingoittaminen sisältää asioita, joita on Suomen lainsäädännössä käsitelty rikoslain 35:ssä luvussa vahingonteko. Artiklan 1 kappaleen mukaan tahallinen ja oikeudeton datan vahingoittaminen, tuhoaminen, turmeleminen, muuttaminen tai poistaminen on säädettävä rangaistavaksi teoksi. Säännökset ovat pysyneet muuttumattomina rikoslain kokonaisuudistuksesta saakka, mutta luvun sisältö vastaa Hallituksen esityksen 153/2006 mukaan vaadittavia säännöksiä eikä siten aiheuta tarvetta uudistaa ko. lukua.

Rikoslain 35:ssä luvussa tuodaan esiin, että myös teon yritys on rangaistava.

Luvun 2 §:ssä määritellään törkeä vahingonteko. Sen tunnusmerkkinä on vahingonteolla aiheutettu 1) erittäin suurta taloudellista vahinkoa, 2) rikoksen uhrille tämän olot huomioon ottaen erityisen tuntuvaa vahinkoa ja 3) historiallisesti tai sivistyksellisesti erityisen arvokkaalle omaisuudelle huomattavaa vahinkoa. Törkeän vahingonteon rajaus antaa tuomioistuimelle melko paljon tulkinnan varaa. Myös teon yritys on rangaistavaa. Rikoksentekijä on törkeän teon ollessa kyseessä tuomittava vähintään 4 kuukauden ja enimmillään 4 vuoden vankeusrangaistukseen.

Luvun 3 §:ssä säännellään lievä vahingonteko jonka rangaistuksena on sakko. 6 §:n mukaan silloin kun kyseessä on yksityinen omaisuus, syyttäjä ei saa nostaa syytettä, ellei asianomistaja ilmoita rikosta syytteeseen pantavaksi. Luvun 7 §:ssä on ehdot toimenpiteistä luopumiselle. Vahingonteosta ja lievästä vahingonteosta voidaan jättää ilmoitus tekemättä, syyte ajamatta tai rangaistus tuomitsematta, jos rikoksen tekijä on korvannut vahingon ja vahingonkorvaus harkitaan riittäväksi seuraamukseksi.

Kun vahingontekoa ja vaaran aiheuttamista tietojenkäsittelylle vertailee, on lain esitöiden mukaa niillä se ero, että vaaran aiheuttamisen tietojenkäsittelylle tunnusmerkki on jonkinlaisen työkalun käyttäminen. Lain esitöissä mainitaan tietokoneohjelma tai ohjelmakäskyn sarja. Vahingonteon osalta käytettävää välinettä ei mainita. HE 153/2006:n tekstin mukaan tuomittava on se, joka toista vahingoittaakseen oikeudettomasti hävittää,

turmelee tai salaa tietovälineelle tallennetun tiedon tai muun tallennuksen. Tekstistä voi tulkita sen, että kyseessä on fyysinen vahingonteko. Tietojärjestelmälle aiheutettuja vahingonteko on päätynyt tuomioistuimeen ilmeisen vähän.

5.2.1 Tietojärjestelmän häirintä

Euroopan Unionin Komission tiedonanto Neuvostolle, Euroopan Parlamentille, Talous ja sosiaalikomitealle ja alueiden komitealle vuodelta 2001 otti esiin artiklassa 5 tietojärjestelmän häirinnän. Tekninen kehitys oli tietojenkäsittelyssä jatkunut ja esiin otettiin pari erilaista näkökulmaa joiden takia Suomenkin lainsäädäntöön tuli uusia muutoksia. Artiklan ensimmäisen momentin mukaan tahallinen ja oikeudeton tietojärjestelmän toiminnan vakava estäminen dataa syöttämällä, siirtämällä, vahingoittamalla, tuhoamalla, turmelemalla, muuttamalla tai poistamalla on säädettävä rangaistavaksi teoksi (HE 153/2006, 10).

HE 153/2006 mukaan artiklan selitysmuistion kohdista 65-70 tuotiin esiin uusi tietojärjestelmän häirinnän tapa. Varsinaisen artiklan tekstissä sitä ei mainita, mutta ainakin hallituksen esityksessä se kuvataan näin. Toimintahäiriö voi seurata tarkoituksellisesta ylikuormituksesta tai esimerkiksi syötettävän datan häiriöitä aiheuttavista ominaisuuksista. Hyökkäys ei siten kohdistu järjestelmässä olevaan dataan, vaan järjestelmän toimintaan. Tällainen esimerkiksi sähköpostipalvelimeen kohdistuvana, niin sanottu palvelunestohyökkäys, mainitaan selitysmuistiossa esimerkkinä artiklan tyypillisestä soveltamistilanteesta.

Tuohon aikaan Suomen lainsäädännöstä löytyi maininta tietoliikenteen häirinnästä ja hallituksen esityksen mukaan silloinen tietoliikenteen häirintää koskeva sääntely kattoi siten käytännössä artiklan ydinalueen (HE 153/2006, 10). Hallituksen esitys ei kuitenkaan tyydy siihen, vaan ehdottaa muutoksia lainsäädäntöön nimenomaisen tietojenkäsittelyn häirinnän kriminalisoimiseksi, jos se tapahtuu palveluestohyökkäyksen omaisesti. Näin rikoslakiin lisättiin 38 lukuun kohdat 7 a § tietojärjestelmän häirintä ja 7 b § törkeä tietojärjestelmän häirintä.

Säännöksessä tietojärjestelmän häirinnäksi luettiin haitta tai taloudellinen vahinko joka syntyy dataa syöttämällä, siirtämällä, vahingoittamalla, muuttamalla tai poistamalla taikka muulla siihen rinnastettavalla tavalla oikeudettomasti. Jos toimenpiteet estävät tietojärjestelmän toiminnan tai aiheuttavat sille vakavaa häiriötä, on tekijä tuomittava,

jollei teosta laissa säädetä ankarampaa tai yhtä ankaraa rangaistusta, tietojärjestelmän häirinnästä sakkoon tai vankeuteen enintään kahdeksi vuodeksi. Törkeämmästä muodosta rangaistus on 7 b §:ssä vähintään neljä kuukautta ja enintään neljä vuotta vankeutta. Molemmissa kohdissa myös teon yritys on rangaistava. Pykälää sovelletaan ainoastaan, jollei teosta muualla laissa säädetä ankarampaa tai yhtä ankaraa rangaistusta

Lain esitöiden mukaan ehdotettua uutta pykälää joudutaan todennäköisesti sen toissijaisuuden vuoksi soveltamaan vain harvoin. Ehdotettu pykälä on kuitenkin tarpeellinen koska yleissopimuksessa mainitut 3 ja 5 artiklat koskevat kaikentyyppistä tietojärjestelmän häirintää, myös sellaista, joka kohdistuu yksittäiseen tietokoneeseen ja sellaista, joka ei edes välillisesti liity viestien siirtoon. Käytännössä häirintä tulee tapahtua ko. tietojärjestelmän luona. Tietoliikenteen häirintää koskeva sääntely kattaa siten artiklojen ydinalueen ja ehdotettu tietojärjestelmän häirintää koskeva sääntely loput.

Pykälässä edellytetään, että teko on oikeudeton ja tahallinen sekä tehty vahingoittamis- tai haittaamistarkoituksessa ja että sen seurauksena tietojärjestelmän toiminta joko estyy tai häiriintyy vakavasti.

Tietojärjestelmän häirintää koskevia oikeusjuttuja ei ole ollut tietojeni mukaan tuomioistuinten käsittelyssä.

Näiden kolmen viimeisen rikosnimikkeen määritelmät lain esitöissä ovat epäselvät. Osittain epäselvyys johtuu varmaan siitä, että rikosnimikkeet ovat rikoslaissa hieman erilaiset kuin komission tiedonannossa. Toinen syy on minusta se, että ikään kuin varmuuden vuoksi monessa paikassa luetellaan mahdolliset tekotavat varsin laajasti ja ne menevät osittain päällekkäin eri artiklojen tekotapojen kanssa.

6. LAINSÄÄDÄNNÖN KEHITTYMINEN TULEVAISUUDESSA

Suomen tietotekniikkaan liittyvä lainsäädäntö on viimeiset vuodet perustunut Euroopan Unionin direktiiveihin ja suosituksiin. Omaehtoista lainsäädäntöä ei tietotekniikka-alalla ole ollut. Annetut suositukset on toteutettu määrätietoisesti ja ilmeisen seikkaperäisesti.

6.1 Uusi direktiivi

Nyt Euroopan parlamentti ja neuvosto ovat kokoamassa uutta direktiiviä tietotekniikkaan liittyvään lainsäädäntöön. Ehdotus uudesta direktiivistä on julkaistu 2010. Tarkoitus on julkaista uusi direktiivi ja kumota vanha 2005/222/YOS. Euroopan parlamentti haluaa arvioita ja kommentteja jäsenvaltioilta uuden direktiivin sisällöstä ja toteutustavasta. Ehdotuksen perusteluista ja tavoitteista selviää, että lainsäädäntö ei kaikissa EU-maissa ole edennyt toivotulla tavalla. Ehdotuksessa kannustetaan jäsenvaltioita viemään päätettyjä asioita eteenpäin ja painotetaan uudistusten tarvetta. Uuden direktiivin keskeiset kehittämisasiat voidaan jakaa lainsäädännön kehittämiseen, yhteistyön ja tietojen vaihdon kehittämiseen jäsenvaltioiden kesken ja rikollisuuden tilastoinnin kehittämiseen.

Ehdotus sisältää viisi eri vaihtoehtoa lainsäädännön uudistamiseksi. Vaihtoehdot ovat 1) nykytilanteen säilyttäminen, ei uusia EU:n toimia, 2) ohjelman laatiminen tietojärjestelmään kohdistuvien hyökkäysten torjunnan lujittamiseksi muilla kuin lainsäädännöllisillä toimenpiteillä, 3) puitepäätöksen sääntöjen kohdennettu päivittäminen (nykyisen puitepäätöksen korvaaminen uudella direktiivillä), jotta voidaan puuttua tietojärjestelmiin kohdistuvien laajamittaisten hyökkäysten (bottiverkot) uhkaan, ja kun on kyse siitä, että rikoksentekijän henkilöllisyys on salattu, parantaa yhteyspisteiden tehokkuutta ja korjata tietoverkkohyökkäyksiä koskeva tilastotietojen puute, 4) tietoverkkorikollisuuden torjumiseen tähtäävän kattavan EU-lainsäädännön käyttöön ottaminen, 5) tietoverkkorikollisuutta koskevan Euroopan neuvoston yleissopimuksen päivittäminen. (KOM(2010)517, 4-5).

Nyt tehdyn ehdotuksen pääasiallinen sisältö on Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen (Sop 60/2007, ETS 185) ja puitepäätöksen

2005/222/YOS mukainen. Näiden asioiden osalta Suomen lainsäädännöstä löytyy vastaavat säännökset. Yleissopimuksen on tällä hetkellä allekirjoittanut 30 valtiota joista 17 on EU:n jäsenvaltiota.

6.2 Sisällön yksityiskohdat

Uudistuksen asiasisällön kohteena ovat seuraavat asiat. Ammattimaisen tietokonerikollisuuden uhka on kasvanut. Sitä vastaan ehdotetaan voimakkaampia toimenpiteitä. Asia tuodaan hyvin painokkaasti esiin. Myös neuvoston päätelmissä marraskuulta 2008 kehotettiin ripeään toimintaan EU:n tasolla ja päivittämään puitepäätös 2005/222/YOS. Ehdotuksessa tuodaan esiin, että jäsenvaltiot eivät yksin pysty riittävästi suojelemaan tehokkaasti kansalaisiaan tietoverkkorikollisuudelta. Ehdotuksen tavoitteet saavutetaan parhaiten Euroopan unionin kokonaisvaltaisella toiminnalla seuraavista syistä: uudistuksilla lähennetään edelleen jäsenvaltioiden aineellista rikosoikeutta ja menettelysääntöjä, millä on myönteinen vaikutus tietotekniikka- tai verkkorikollisuuden torjuntaan. Ensinnäkin se on tapa estää rikoksentekijöitä muuttamasta sellaisiin jäsenvaltioihin, joissa tietoverkkohyökkäystä koskeva lainsäädäntö on lievempi. Toiseksi yhteisten määritelmien ansiosta tietoja voidaan vaihtaa sekä kerätä ja verrata. Kolmanneksi torjuntatoimenpiteiden vaikuttavuus EU:ssa paranee ja kansainvälinen yhteistyö tiivistyy. (EU KOM (2010)517, 8-9)

Ehdotuksessa on myös joitakin säännöksiä, joita vastaavia asioita ei löydy edellä mainituista asiakirjoista, (Sop 60/2007, ETS 185) ja puitepäätös 2005/222/YOS:stä. Lisänä ovat ns. bottiverkkojen luokittelu raskauttavaksi olosuhteeksi. Euroopan Komissio ehdottaa myös toimia rikollisoikeudellisen yhteistyön kehittämiseksi. Yksi keino on ympärivuorokautisten yhteyspisteverkoston luominen. Verkosto toimii valtaosassa jäsenvaltioita, mutta pisteiden toiminta tulisi saada ympärivuorokautiseksi. Joissakin maissa ko. pisteitä ei vielä ole ja siksi pisteiden perustaminen ja ympärivuorokautinen päivystys halutaankin sitovaksi. Näiden ehdotusten lisäksi rikosten kattava tilastointi koetaan tärkeäksi. Euroopan komissio antoi tiedonannon 28.3.2012, jonka mukaan Komissio ehdottaa myös yhteisen verkkorikostutkimuskeskuksen perustamista. Tällä toimella halutaan nopeuttaa rikostutkimuksen kehittymistä ja koota verkkorikollisuutta koskeva tieto yhteen paikkaan. (EU KOM(2012) 140, 2-5).

6.3 Asian etenemisaikataulu

Valtioneuvosto on lähettänyt kirjelmän eduskunnalle uudesta ehdotuksesta. Kirjeen mukaan uuden direktiivin tavoitteena on yhtenäistää tietojärjestelmärikoksia koskevaa lainsäädäntöä ja tehostaa oikeus- ja muiden toimivaltaisten viranomaisten, poliisin ja muiden lainviranomaisten yhteistyötä. Kirjeen mukaan joihinkin rikoksiin, ainakin vaaran aiheuttaminen tietojärjestelmälle ja tietoverkkorikosvälineen hallussapito, on Suomen lakiin lisättävä törkeä tekomuoto. Mitä todennäköisimmin myös rikosten rangaistusten enimmäismäärät tulevat nousemaan. Muuten direktiivi rikoslakiin ei aiheuta suurta uudistamistarvetta.(OM U50/2010, 2-4)

Direktiiviehdotuksen käsittely neuvoston työryhmässä on aloitettu tammikuussa 2010. Neuvottelut Euroopan parlamentin kanssa ovat alkaneet keväällä 2012. Direktiivi julkaistaneen vuoden 2012 loppupuolella tai keväällä 2013. Ehdotuksen 17 artiklan mukaan direktiivin saattaminen jäsenvaltioiden lainsäädäntöön tulee tapahtua kahden vuoden sisällä direktiivin hyväksymisestä.

7. JOHTOPÄÄTÖKSIÄ

Tämän tutkimuksen perusteella Suomi on tähän mennessä välttynyt suurilta tietotekniikkaan perustuvilta rikoksilta. Tärkeä rooli tässä asiassa varmaan on ollut se, että yhteiskunta on hyvin järjestäytynyt, niin järjestelmien käyttäjät, lainsäädäntö kuin rikoksia tutkivat tahotkin. Valmius hoitaa tällaisia asioita on hyvä. Osittain tilanne voi selittyä sillä mitä Kuusimäki sanoi Suomen tilanteesta, toistaiseksi meitä suomalaisia on suojannut massiiviselta tietoverkkorikollisuudelta erikoinen kieli sekä hyvä valmius käyttää tietoturvatyökaluja ja noudattaa tietoturvakäytänteitä (Kuusimäki, 11).

Tämän tutkimustyön edetessä on minulle jäänyt mieleen viisi asiaa, joita pidän muita tärkeämpänä kokonaisuuden kannalta. Ne ovat tekniikan nopea kehittyminen, toimintaympäristön kansainvälisyys, lainsäädäntöön liittyvien asioiden monimutkaistuminen, joissakin rikoksissa uhrin asema ja joissakin rikostilanteissa, rikoksista tiedottaminen. Käyn seuraavassa läpi nämä asiat hieman tarkemmin.

Mikko Huuskonen kirjoittaa Lakimies-lehdessä artikkelin tietotekniikan kehityksestä ja sen aiheuttamista ongelmista lainsäädännölle. Hän tuo kirjoituksessaan esille sen suuren epäsuhdan, joka on tietotekniikan kehityksen nopeudella, verrattuna lainsäädännön kehittymisen nopeuteen. Hän esittää osaratkaisuksi tuomioistuinten roolia. Huomioiden myös lakia säätävien menettelyjen hitaus suhteessa teknologiseen kehitykseen, on ilmeistä, että tuomioistuinten rooli oikeutta luovina ratkaisijoina korostuu tulevina vuosina (Huuskonen, 2011:1013).

Tekniikan nopea kehittyminen on varmaan yksi suurimmista ongelmista. Lainsäätäjälle tekniikan nopea kehittyminen on ongelma, mutta erityisen suuri ongelma se on rikoksia selvittävälle viranomaiselle. Sari Kajantie kirjoittaa artikkelissaan Haaste-lehdessä poliisin vaikeuksista rikosten selvittelyssä. Tietoverkko on kaikin puolin mainio alusta tuottoa tavoittelevien rikosten toteuttamiseen johtuen verkon ominaispiirteiden lisäksi viranomaisten toimivaltuuksista. Verkko on globaali, viranomainen ei ole. Verkko on nopea, viranomaisten tietojenvaihtoinstrumentit eivät ole. Kyse ei ole viranomaisten heikkoudesta tai instrumenttien suunnitteluvirheestä, sinänsä. Kyse on toiminnan reunaehtojen muuttumisesta. Lähinnä Suomessa on aivan erityisenä ongelmana myös viranomaisten kansalliset toimivaltuudet, jotka eivät ole omiaan suojaamaan rikosuhrin oikeusturvaa verkossa. (Kajantie, 1) Moneen kertaan on tuotu esiin se kuinka kansainvälistä

tietotekniikkarikollisuus on. Siihen kun liitetään vielä se, että eri maissa on erilaiset resurssit ja mahdollisuudet jakaa viranomaisille tietoa ja kouluttaa henkilökuntaa, syntyy asiasta varmasti ongelma. Euroopan unionin viimeisessä tietotekniikkaan liittyvässä direktiiviehdotuksessa tuodaan selkeästi esille se, että Euroopan unionin jäsenvaltioiden lainsäädännön kehittyminen ja muu edellytetty yhteistyö ei ole kulkenut samaa tahtia, toiset maat ovat hoitaneet asiansa hyvin, toiset eivät. (EU KOM (2010)517, 2-3)

Tutkimuksessa on moneen kertaan painotettu tutkimuskohteena olevan asian *kansainvälisyyttä*. Kansainvälisyys merkitsee yhteistyötä lainsäätämisessä ja rikosten tutkinnassa. Rikosten tekeminen voi tällä alalla tapahtua kaukana varsinaisesta rikospaikasta. Lainsäätämisen ja osin myös rikostutkinnan tulisi kehittyä kokonaisvaltaisesti kaikkialla samaan tahtiin. Kun kyseessä on Euroopankin osalta kymmeniä valtioita, on tehtävä haasteellinen.

Tekniikan nopeaan kehittymiseen liittyy myös se, että käsiteltävät *asiat monimutkaistuvat*. Mikko Huuskosen ehdottama tuomioistuinten roolin korostuminen nopeasti muuttuvassa maailmassa on varmaan hyvä ehdotus. Koulutus ja panostus syyttäjien, rikostutkijoiden ja tuomareiden tietotaitoon on tärkeää. Sillä voitaneen ainakin osaksi purkaa paineita jatkuvaan lain uudistamiseen. Samat keinot tepsivät myös seuraavaan ongelmaan, tietotekniikan monimutkaistumiseen. Tarvitaan tutkimustyötä ja koulutusta ja sen tulee kohdistua viranomaisiin ympäri Eurooppaa tai jopa koko maailmaa.

Kun nyt tässä tutkimuksessa olen seurannut tietotekniikkaan liittyvän lainsäädännön kehittymistä, niin väistämättä tulee mieleen kysymys, kuinka kauan rikoslakiin voidaan lisätä tietotekniikkaan liittyviä asioita. Rikoslakiin ei voida kirjata tai kirjaaminen on ainakin vaikeaa, sellaisia kokonaisuuden hallintaan tarvittavia asioita, kuten on tehty esimerkiksi viestintämarkkinalaissa ja sähköisen viestinnän tietosuojalaissa. Tietotekniikkarikoksiin liittyvät asiat olisivat paremmin hallittavissa, jos ne olisivat erillisessä laissa, johon voitaisiin lisätä kokonaistilanteen hallintaa tarvittavia muitakin säännöksiä, kuin vain rikoksiin liittyviä asioita. Asiat monimutkaistuvat koko ajan.

Kun lainsäätäjät aikoinaan päättivät, että tietotekniikkaan liittyviä lakeja ei tehdä ainakaan rikoslain osalta erillisenä vaan osana olemassa olevaa rikoslakia, ei varmaankaan täysin vielä nähty mihin kehitys tietotekniikan osalta johtaa. Kannattaisiko tietotekniikkaan koskevat rikosasiat laittaa erilliseen lakiin, siitä kannattaa varmaan keskustella. Minusta tietojenkäsittelyrauhana tunnetun asian hallinta voisi olla helpompaa jos sitä käsittelevä laki olisi olemassa, vaikka sitten niin, että varsinaiset rikosasiat olisivatkin

edelleen rikoslaissa. Kun vertaa kuinka sähköisen viestinnän tietosuojalaissa on voitu tiettyjä asioita säännellä, olen vakuuttunut, että se voisi olla samaan tyyliin ratkaisu tietojärjestelmienkin osalta.

Tietotekniikkarikosten *uhrin asema* on mielestäni lainsäädännössä jäänyt epäselväksi. Joissakin rikoksissa uhriin kohdistuva vahinko tai haitta on huomioitu. Otetaan esimerkiksi tässäkin tutkielmassa esillä olleet maksuvälinepetokset. Uusi maksupalvelulaki selkeytti uhrin asemaa. Lain 7 luvun 62 §:n mukaan maksuvälinepetoksen uhriksi joutunut ei vastaa vahingosta kuin 150 euron osalta, ellei maksuvälineen haltija on toiminut tahallisesti tai törkeän huolimattomasti. Tietomurtoon liittyviä identiteettivarkauksia ei ole vielä käsitelty suomalaisessa oikeusistuimessa, mutta varmaan niitäkin tulee tulevaisuudessa esiin. Sen kaltaisissa rikoksissa voi seurata erittäin mittavat vahingot. Nyt uusi, tulossa oleva direktiivi ehdottaa, että toisen nimissä tehtyä tietotekniikkarikosta käsiteltäisiin aina törkeänä rikoksena. Mutta edelleen uhrin aseman selkiyttäminen kaipaa kehitystyötä.

Mielestäni sellaisista tietojärjestelmiin kohdistuvista loukkauksista tulisi pääsääntöisesti ilmoittaa Viestintävirastoon, jossa joku kolmas osapuoli voi joutua ilman syytään rikoksen uhriksi. Ilmoitettavien rikosten määrittely voi olla vaikeaa. Nythän lakiin on kirjattu *ilmoitusvelvollisuus* joissakin erityistapauksissa, ilmoitusvelvollisuuden kattavuutta tulisi kuitenkin edelleen lisätä. Jos yrityksillä olisi velvollisuus ilmoittaa tietoturvaloukkauksista, niin se pakottaisi yritykset huolehtimaan tietoturvastaan paremmin. Ne alkaisivat vaatia parempaa palvelua tietoturvaresursseilta, ovatpa ne sitten yrityksen omia resursseja tai ostettuja. Tästä taas seuraisi se, että tietoturvasta vastaavat alkaisivat vaatia paremmin tietoturvaa suojaavia ohjelmia ohjelmatoimittajilta ja murtojen teko vaikeutuisi. Tietomurrot saisivat ainakin hetkellisesti enemmän julkisuutta, joitakin tuomioita varmaan tulisi ja ”hakkerit” alkaisivat ymmärtää, että kyseessä on rikos josta voi seurata rangaistus. Kun tapauksia tulisi enemmän, poliisin rutiinit kehittyisivät ja tietotekniikan käyttäjätkin havahtuisivat olemaan tarkempia järjestelmien käyttämisessä ja työnantajat kouluttaisivat työntekijänsä paremmin.

LÄHDELUETTELO

Council of Europe (2011] [online]. Siteerattu 5.12.2011 Saatavana World Wide Webissä: <URL:http://conventions.coe.int/?pg=/general/IntroConv_en.asp>

Council of Europe (1990). *Computer-related Crime: Recommendation No. R (89) 9*. Strasbourg. 114 s.

Council of Europe, Recommendation No. R (95) 13. *Concerning Problems of Criminal Procedure Law Connected with Information Technology* [online]. Siteerattu 25.11.2011 Saatavana World Wide Webissä: <URL:http://www.coe.int/t/dghl/standardsetting/media/Doc/CM/Rec%281995%29013_en.asp>

Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus ETS no:185 [on line]. Siteerattu 25.6.2012 Saatavana World Wide Webissä: <URL:http://www.coe.int/t/dghl/standardsetting/t-cy/ETS%20185%20Finnish.pdf

Euroopan neuvoston puitepäätös 2005/222/YOS. *Tietojärjestelmiin kohdistuvista hyökkäyksistä* [on line]. Siteerattu 3.8.2012 Saatavana World Wide Webissä: http://eur-lex. europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:FI:PDF

Euroopan neuvoston puitepäätös 2001/413/YOS. *Muihin maksuvälineisiin kuin käteiseen rahaan liittyvien petosten ja väärennysten torjunnasta* [on line]. Siteerattu 5.8.2012 Saatavana World Wide Webissä: <URL:http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:149:0001:0004:FI:PDF

Euroopan yhteisöjen komissio (2012) COM(2012)140. *Rikostentorjunta digitaaliaikana: Euroopan verkkorikostorjuntakeskuksen perustaminen* [on line]. Siteerattu 28.7.2012 Saatavana World Wide Webissä: <URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:FI:PDF

Euroopan yhteisöjen komissio (2010). *Ehdotus Euroopan parlamentin ja neuvoston direktiivi tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepää-*

töksen 2005/222/YOS kumoamisesta KOM(2010) 517 [on line]. Siteerattu 25.7.2012 Saatavana World Wide Webissä: <URL:http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2010)0517_/com_com(2010)0517_fi.pdf

Euroopan yhteisöjen komissio (2007). *Tavoitteena yleinen toimintalinja tietoverkkorikollisuuden torjumiseksi* KOM(2007) 267 [on line]. Saatavissa Internetissä: <URL:http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:FI:PDF

Euroopan yhteisöjen komissio (2002). *Tietojärjestelmiin kohdistuvista hyökkäyksistä.* KOM(2002) 173 [on line]. Saatavissa Internetissä: <URL:http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2002:0173:FIN:FI:PDF

Euroopan yhteisöjen komissio (2000). *Turvallisempaan tietoyhteiskuntaan tietojärjestelmien turvallisuutta parantamalla ja tietokonerikollisuutta ehkäisemällä*. KOM(2000) 890 [on line]. Saatavissa Internetissä: <URL:http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0890:FIN:EN:PDF

Fredman Markku & Järvinen Petteri(2003). *Korkeimmasta oikeudesta*. Defensor Legis N:o 4/2003, s.764-769

HE 277/2010 vp. Hallituksen esitys Eduskunnalle laiksi rikoslain 28 luvun 7§:ssä muuttamisesta [on line]. Saatavissa Internetissä: <URL: http://www.finlex.fi/fi/esitykset/he/2010/20100277

HE 153/2006 vp. 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 [on line]. Saatavissa Internetissä: <URL:http://www.finlex.fi/fi/esitykset/he/2006/20060153

HE 2/2003 vp. Hallituksen esitys Eduskunnalle rikoslain muuttamisesta [on line]. Saatavissa Internetissä: <URL: http://www.finlex.fi/fi/esitykset/he/2003/20030002

HE 112/2002 vp. Hallituksen esitys Eduskunnalle viestintämarkkinoita koskevan lainsäädännön muuttamisesta [on line]. Saatavissa Internetissä: <URL:http://www.finlex.fi/fi/esitykset/he/2002/20020112

HE 4/1999 vp. Hallituksen esitys Eduskunnalle laiksi rikoslain muuttamisesta [on line]. Saatavissa Internetissä: <URL:http://www.finlex.fi/fi/esitykset/he/1999/19990004

HE 94/1993vp. Hallituksen esitys Eduskunnalle rikoslainsäädännön kokonaisuudistuksen toisen vaiheen käsittäviksi rikoslain ja eräiden muiden lakien muutoksiksi [on line]. Saatavissa Internetissä: <URL:http://www.finlex.fi/fi/esitykset/he/1993/19930094

HE 66/1988 vp. Hallituksen esitys rikoslainsäädännön kokonaisuudistuksen ensimmäisen vaiheen käsittäviksi rikoslain ja eräiden muiden lakien muutoksiksi [on line]. Saatavissa Internetissä:

Helsingin Sanomat(2007) Nato, Viron nettihyökkäykset suunniteltu hyvin [on line]. Siteerattu 25.7.2012. Saatavissa World Wide Webissä: <URL:http://www.hs.fi/ulkomaat/artikkeli/Nato+Viron+nettihyökkäykset+toteutettu+ja+suunniteltu+hyvin/1135227354187

Huuskonen, Mikko (2011). *Tietoverkkojen uusista oikeuskysymyksistä*. Lakimies 5/2011 s. 1008-1013

IAPL (2011) [online]. Siteerattu 2.12.2011. Saatavissa World Wide Webissä <URLhttp://www.penal.org/?page=mainaidp&id_rubrique=13&lang=en>

Interpol (2011) [online] Siteerattu 4.12.2011. Saatavissa World Wide Webissä <http://www.interpol.int/About-INTERPOL/Overview>

Jounio, Anu (2011). *Tieto- ja viestintärikokset rikoslain 38§ luvussa*. Lapin yliopisto: Oikeustieteiden tiedekunta, pro gradutyö. 71 s.

Järvinen, Petteri (2002). *Tietoturva ja yksityisyys*. Porvoo: WS Bookwell. 456 s.

Järvinen, Petteri (2006). *Paranna tietoturvaasi*. Porvoo: WS Bookwell. 352 s.

Kajantie, Sari (2010). *Ammattimainen rikollisuus tietoverkossa* [on line].. Siteerattu 8.8.2012. Saatavissa World Wide Webissä <URL:http://www.haaste.om.fi/Etusivu/Juttuarkistoaiheittain/Poliisi/1284989796049

Kuusimäki, Matti (2009). Hämähäkkejä verkossa. Puhe ECT Forum 09, 23.9.2009 [on line]. Siteerattu 4.8.2012. Saatavissa World Wide Webissä <URL:http://www.eis.fi/ect/fp/ECT09_230909_Plenary_Kuusimaki.pdf

Laaksonen Mika, Nevasalo Terho, Tomula Karri (2006). *Yrityksen tietoturvakäsikirja*. Helsinki: Edita Publishing Oy. 324 s.

Lehtimaja, Lauri (1989)*Eurooppalaisesta atk-rikospolitiikasta*. Teoksessa: Rikosoikeudellisia kirjoitelmia VI. Rikosoikeuden juhlavuonna 1989, toim. Raimo Lahti. Suomalaisen lakimiesyhdistyksen julkaisuja A-sarja N:o 185. Vammala 1989,

Lehtonen, Asko (1999). *Tietokoneviruksella aiheutettu vahinko ja oikeudellinen vastuu.* Rovaniemi: Lapin yliopistopaino.

Lehtonen, Asko (2002). *”Kun kalteri kolahtaa” – johdatus tietoturvarikoksiin.* Rovaniemi: Lapin yliopistopaino.

Liikenne – ja viestintäministeriö (2011). *Suomi tietoturvan suunnannäyttäjäksi* [online]. Siteerattu 31.1.2011. Saatavissa World Wide Webissä: <URL:http://www.lvm.fi/c/document_library/get_file?folderId=1551284&name=DLFE-11972.pdf&title=Julkaisuja%2017-2011>

Lillbacka, Juhani (2012). *Informaatiosodankäynti – tietoverkkojen vaarat*. Tampereen Ammattikorkeakoulu: Tietotekniikka, opinnäytetyö. 67 s.

Muttilainen, Vesa & Kankaanranta, Terhi (2011). *Talousrikollisuuden kehityssuunnat ja toimintaympäristö vuosina 200-2009.* Poliisiammattikorkeakoulun raportteja 91 [online]. Siteerattu 20.07.2012. Saatavissa World Wide Webissä:

<URL:http://www.poliisiammattikorkeakoulu.fi/poliisi/poliisioppilaitos/home.nsf/pages/949E60F49A750F77C22575A2003EB560?Opendocument

OECD (2011) [online]. Siteerattu 2.12.2011. Saatavissa World Wide Webissä <URL:http://www.oecd.org/pages/0,3417,en_36734052_36734103_1_1_1_1_1,00.html>

Oikeusministeriö (2010) *Valtioneuvoston kirjelmä Eduskunnalle ehdotuksesta Euroopan parlamentin ja neuvoston direktiiviksi tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS kumoamisesta* [on line]. Siteerattu 12.8.2012. Saatavissa World Wide Webissä: <URL:http://217.71.145.20/TRIPviewer/show.asp?tunniste=U+50/2010&base=eru&palvelin=www.eduskunta.fi&f=WOR

Paananen, Juha (2001). *Tietotekniikan peruskirja*. Porvoo: WS Bookwell. 452 s.

Pihlajamäki, Antti (2004). *Tietojenkäsittelyrauhan rikosoikeudellinen suoja*. Jyväskylä: Gummerus Kirjapaino Oy, 294 s.

Poliisi, keskusrikospoliisi. *Maksukorttirikollisuus on kasvava ilmiö* [on line]. Siteerattu 2.8.2012. Saatavissa World Wide Webissä: <URL:http://www.poliisi.fi/poliisi/krp/home.nsf/pages/57AB59140EEDBC15C225799C002B56EA

Poliisi. *Itä-Uudenmaan poliisin tiedote* [on line]. Siteerattu 2.8.2012. Saatavissa World Wide Webissä: <URL:http://www.poliisi.fi/poliisi/ita-uusimaa/home.nsf/PFBD/7FF2D302EBAEE133C22579BB004C2A53

Pöysti, Tuomas (2001). *Information Security Commentary*, Institute for Law and informatics: University of Lapland, Finland

Raitio, Juha (2011). *Euroopan integraatio ja Euroopan unionin rakenteet*. Helsinki: Unigrafia Oy. 244s.

Tilastokeskus, *Tietotekniikasta on tullut osa suomalaista arkipäivää* [online]. Siteerattu 1.12.2011. Saatavissa World Wide Webissä: <URL:http://www.stat.fi/ajk/tiedotteet/v2006/tiedote_017_2006-03-08.html >

UN (2011) [online]. Siteerattu 2.12.2011 Saatavissa World Wide Webissä <URL:http://www.unodc.org/unodc/en/commissions/CCPCJ/session/index.html

UN International review of criminal policy - *United Nations Manual on the prevention and control of computer-related crime* [online]. Siteerattu 28.11.2011. Saatavissa World Wide Webissä: <URL:http://www.ifs.univie.ac.at/~pr2gq1/rev4344.html (60 of 60) [1999-05-12 11:11:38]>

Valtiovarainministeriö: *tietoturvapoikkeamiin varautuminen* [online]. Siteerattu 12.8.2012. Saatavissa World Wide Webissä <URL:https://www.vahtiohje.fi/web/guest/tietoturvapoikkeamiin-varautumi-nen;jsessionid=CBCA4500562AE8D27E3020360142EF656C10957561418CE08F79D744179B17BEE0A25F9688EAAA00C7CAA6

Valtiovarainministeriö (1999). *Valtioneuvoston periaatepäätös valtiohallinnon tietoturvallisuudesta* [online]. Siteerattu 22.11.2011. Saatavissa World Wide Webissä: <URL:http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/6294_fi.pdf >

Xingan, Li (2008). *Cybercrime and deterrence: networking legal systems in the networked information society*. Turku: Uniprint 358 s.

OIKEUSTAPAUSLUETTELO

Korkein oikeus

8.4.2003 taltio 811	KKO:2003:36	s. 2 ja 4
29.5.2012 taltio 991	KKO:2012:54	s. 1-4

Hovioikeus

31.3.2009 taltio 793	Turun HO:2009:793	s. 2 – 7
18.6.2002 taltio 745	Vaasan HO:2002:745	s. 8 – 12
10.3.2011 R10/863	Kouvolan HO:2011:284	s.3

Käräjäoikeudet

3.6.2008 asiano:R08/563	Porin käräjäoikeus	s. 1 – 6
13.4.2012 asiano:R12/714	Oulun käräjäoikeus	s.1 – 22