Tieto- ja viestintärikokset rikoslain 38 luvussa

Lapin yliopisto
Oikeustieteiden tiedekunta
Oikeusinformatiikka
Maisteritutkielma
Anu Jounio
Syksy 2011

TIIVISTELMÄ

Lapin yliopisto, oikeustieteiden tiedekunta

Työn nimi: Tieto- ja viestintärikokset rikoslain 38 luvussa

Tekijä: Anu Jounio

Oppiaine: Oikeustieteiden tiedekunta / Oikeusinformatiikka

Työn laji: Maisteritutkielma x Lisensiaatintutkimus__

Sivumäärä: IX + 71

Vuosi: syksy 2011

Tiivistelmä:

Tutkielmassani käsittelen tieto- ja viestintärikoksia rikoslain 38 luvussa. Tietotekniikkaan liittyvät rikokset on otettu huomioon rikoslainsäädännössä kahdella tavalla. Silloin kun tietotekniikan väärinkäytökset ovat luonteeltaan samantyyppisiä kuin perinteiset rikokset, on tarkistettu näitä rikoksia koskevia säännöksiä. Jos tietotekniikka on tuonut mukanaan uudenlaista käyttäytymistä, on säädetty uusia tietotekniikkaan liittyviä tunnusmerkkejä.

Tietotekniikkarikos määritellään rangaistavaksi teoksi, jonka kohteena, välikappaleena tai tekoympäristönä on tietojärjestelmä siihen kuuluvine laitteineen ja jonka tekeminen ja / tai rikosprosessuaalinen käsittely välittömästi edellyttää tietoteknistä erityistietämystä. Tietotekniikkarikoksissa on rangaistavaa vain se, mikä on rangaistavaksi säädettyä. Tietotekniikan jatkuva muuttuminen on luonut paineita uudistaa rikoslakia, koska haitallisia tekoja ei aina ole ollut mahdollista katsoa rikoksiksi ilman rikosten tunnusmerkistöjen uudistamista.

Tieto- ja viestintärikokset ovat hyvin kansainvälisiä rikoksia. Tietoverkkoja pitkin rikokset ylittävät helposti valtioiden rajoja. Tästä johtuen kansainvälistä yhteistyötä on harjoitettu paljon.

Rikoslain 38 luku uudistui vuonna 1995 käsittämään tieto- ja viestintärikokset. Tällä hetkellä siihen kuuluu 12 eri pykälää. Kyseistä lukua on muutettu lakimuutoksin 5 kertaa vuoden 1995 jälkeen. Tieto- ja viestintärikosten määrät ovat nousseet koko ajan. Vuonna 2010 rikosilmoituksia tehtiin rikoslain 38 luvun osalta 760 kappaletta.

Tulevaisuudessa tietoteknisen kehityksen myötä säännöksiä tullaan muuttamaan. Tällä hetkellä suunnitelmissa on ainakin henkilötietolakiin tulevat muutokset uuden henkilötietodirektiivin sekä uuden identiteettilain säätämisen myötä.

Avainsanat: tieto- ja viestintärikokset, atk-rikokset, tietosuoja, identiteetti : varkaus

Suostun tutkielman luovuttamiseen Rovaniemen hovioikeuden käyttöön x

Suostun tutkielman luovuttamiseen kirjastossa käytettäväksi x

SISÄLLYSLUETTELO

LÄHTEET

Kirjallisuus

Castrén Kirsi: Henkilörekisterien turvana lait ja lokitiedostot, Tietosuoja 1/2009 s. 28-30.

Castrén Kirsi: Identiteetti on suojaamisen arvoinen. Tietosuoja 4/2010 s. 14-15.

Fredman Markku, Järvinen Petteri: Tietomurto, vahingonkorvaus, korvauksen sovittelu. Oikeustapauskommentti. Defensor Legis 4/2003, s. 764-769.

Frände Dan: Yleinen rikosoikeus. Edita. Helsinki 2005

Hallberg Pekka: Perusoikeusjärjestelmä sivut 29-58. Teoksessa Perusoikeudet 2. uudistettu painos. Helsinki 2011.

Heinonen Risto: Digitaalinen minä. Edita. Helsinki 2001

Helopuro Sanna, Perttula Juha, Ristola Juhapekka: Sähköisen viestinnän tietosuoja. Taletum. Helsinki 2009

Innanen Antti, Saarimäki Jarkko: Internet-oikeus. Edita. Helsinki 2009.

Jordan Tim: Hacking digital media and society series. Polity Press. Cambridge 2008.

Järvinen Petteri: Salausmenetelmät. Docendo Finland Oy. Jyväskylä 2003.

Järvinen Petteri: Tietoturva & yksityisyys. Docendo Finland Oy. Jyväskylä 2002.

Jääskinen Niilo: Euroopan unioni. Oikeudelliset perusteet. Talentum Helsinki 2007.

Korhonen Rauno: Perusrekisterit ja henkilötietojen suoja. Informaatio-oikeudellinen tutkimus yksityisyyden suojasta yhteiskunnan perusrekisteritietojen käsittelyssä. Lapin yliopisto. Rovaniemi 2003.

Korhonen Rauno: Informaatio-oikeuden asemasta oikeuksien kentässä. Teoksessa Oikeusteorian poluilla. Juhlakirja professori Rauno Halttunen. Toimittanut Sauli Mäkelä. Lapin yliopiston oikeustieteellisiä julkaisuja Sarja C 42 Rovaniemi 2006.

Korhonen Rauno: Poliisin valvontakeinot ja kansalaisten yksityisyyden suoja. Edita. Helsinki 2005.

Korhonen Rauno: Sähköinen asiointi ja viestintä sivut 411 - 535. Teoksessa Oikeusjärjestys osa III. 7. täydennetty painos. Rovaniemi 2010.

Lagus Antti J.: Sisäisen turvallisuuden ohjelmassa tietoverkkorikoksia laitetaan kuriin. Tietosuoja 1/2008 s. 22-25.

Lehto Tero: Tietotekniikkarikosten määrä kasvaa - poliisiylijohtaja huolissaan. Tietokone 27.1.2011.
http://www.tietokone.fi/uutiset/paatero_tietotekniikkarikokset_kasvava_ongelma. Viitattu 30.7.2011

Linden Mikael: Enemmän kuin tekniikkalaji. Tietosuoja 4/2010 s. 10-13.

Nuutila Ari-Matti: Rikoslajit sivut 519-536. Teoksessa Encyclopaedia Iurica Fennica IV Rikos- ja prosessioikeus. Suomalaisen lakimiesyhdistyksen julkaisuja C-sarja n:o 27. Gummerus Kirjapainotaito Oy, Jyväskylä 1995.

Mäkinen Olli: Internet ja etiikka. BJT Kirjastopalvelu Oy, Helsinki Gummerus Kirjapaino Oy. Vaajakoski 2006.

Männikkö Päivi: Henkilökohtaista. Tietosuoja 4/2010 sivu 9.

Männikkö Päivi: Identiteettiohjelma valmistui, työ jatkuu. Tietosuoja 1/2011 sivu 31.

Niiniluoto Ilkka: Informaatio, tieto ja yhteiskunta. Filosofinen käsiteanalyysi. 5. täydennetty painos. Oy Edita Ab. Helsinki 1996.

Ojanen Tuomas: EU-oikeuden perusteita. Uudistettu laitos. Edita. Helsinki 2010

Pihlajamäki Antti: Tietotekniikkarikokset sivut 685-686. Teoksessa Encyclopaedia Iurica Fennica IV Rikos- ja prosessioikeus. Suomalaisen lakimiesyhdistyksen julkaisuja C-sarja n:o 27. Gummerus Kirjapainotaito Oy, Jyväskylä 1995.

Pihlajamäki Antti: Tietojenkäsittelyrauhan rikosoikeudellinen suoja. Datarikoksia koskeva sääntely Suomen rikoslaissa. Suomalaisen lakimiesyhdistyksen julkaisuja A-sarja No 258. Helsinki 2004

Pihlajamäki Antti: Tietoverkkorikollisuuden sääntely kiristyy. Tietosuoja 1/2007. s. 27-29.

Poroila Tiia: Usein uteliaisuudesta. Tietosuoja 1/2009, s. 26-27.

Rautio Ilkka: RL 38:Tieto- ja viestintärikokset. Teoksessa Rikosoikeus. Kolmas uudistettu painos. WSOYpro. Helsinki 2009.

Rautvuori Marjo: Pakkokeino loukkaa aina yksityisyyttä. Tietosuoja 2/2011, s. 5-7.

Ross Jeffrey Ian: Criminal investigations. Cybercrime. New York 2010

Saarenpää Ahti: Oikeusinformatiikka sivut 713-726. Teoksessa Encyclopaedia Iurica Fennica VII Oikeuden yleistieteet. Suomalaisen lakimiesyhdistyksen julkaisuja C-sarja n:o 30. Gummerus Kirjapainotaito Oy, Jyväskylä 1999.

Saarenpää Ahti: Oikeusinformatiikka sivut 411-545. Teoksessa Oikeusjärjestys osa I. 7. täydennetty painos. Rovaniemi 2011.

Saarenpää Ahti: Henkilö- ja persoonallisuusoikeus sivut 231-410. Teoksessa Oikeusjärjestys osa I. 7. täydennetty painos. Rovaniemi 2011.

Talus Anu: Komissio haluaa kokonaisvaltaista tietosuojaa. Tietosuoja 1/2011, s. 38-40.

Tavi Hannele: Varastettu identiteetti. LakimiesUutiset 2/2011, s. 60-61.

Timonen Pekka: KKO:n ratkaisut kommentein 2006:II. Talentum Helsinki 2007.

Viljanen Veli-Pekka: Yksityiselämän suoja (PL10 §) sivut 389-413. Teoksessa Perusoikeudet 2. uudistettu painos. Helsinki 2011.

Xingan Li, Cybercrime: An Introduction. Lex Publishing. Joensuu 2005.

Xingan Li, Cybercrime and deterrence: Networking legal systems in the networked information society. Turku 2008.

Virallislähteet

HE 94/1993 vp: Hallituksen esitys Eduskunnalle rikoslainsäädännön kokonaisuudistuksen toisen vaiheen käsiteltäviksi rikoslain ja eräiden muiden lakien muutokseksi

HE 96/1998 vp: Hallituksen esitys Eduskunnalle henkilötietolaiksi ja eräiksi siihen liittyviksi laeiksi

HE 184/1999 vp: Hallituksen esitys Eduskunnalle yksityisyyden, rauhan ja kunnian loukkaamista koskevien rangaistussäännösten uudistamiseksi

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

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

HE 286/2010 vp: Hallituksen esitys eduskunnalle syyttäjälaitosta koskevan lainsäädännön uudistamiseksi.

Henkilöllisyyttä koskeva hanke (identiteettiohjelma). Työryhmän loppuraportti. Sisäasiainministeriö . Helsinki 2010

KOM(2010) 609: Komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle. Kattava lähestymistapa henkilötietojen suojaan Euroopan unionissa. Bryssel 4.11.2010

Poliisin tulostietojärjestelmä

Tietotekniikkatutkinnan järjestäminen poliisissa. Työryhmän loppuraportti. Poliisin ylijohdin julkaisusarja 7/2008. Sisäasiainministeriö. 2008

Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus (SopS 60/2007)

Valtakunnansyyttäjänviraston ratkaisu 15.4.2008
http://www.vksv.oikeus.fi/Etusivu/Ratkaisuja/Ratkaisuja2008/1208352670868

Sähköiset lähteet

www.datainspektionen.se

www.eduskunta.fi

www.hare.vn.fi

www.tilastokeskus.fi

Oikeuskäytäntö

KKO 2003:36 (hakusanat: tietomurto, vahingonkorvaus, korvauksen sovittelu)

KKO 2006:61 (hakusanat: salassapitorikos, asianajaja)

KKO 2009:3 (hakusanat: yksityiselämän suoja, sananvapaus, kunnianloukkaus, salassapitorikos, rikokseen osallisuus, avunanto, yllytys, rikosten yhtyminen, lainkonkurrenssi)

Lyhenteet

EU = Euroopan unioni

HE = hallituksen esitys Eduskunnalle

KKO = Korkein oikeus

PKL = pakkokeinolaki

SVTSL = Sähköisen viestinnän tietosuojalaki

YK = Yhdistyneet kansakunnat

JOHDANTO

Tietotekniikasta on tullut modernin yhteiskunnan alue, jonka nopea tekninen kehitys on jouduttu ottamaan huomioon myös rikosoikeudellisessa sääntelyssä. Positiivisen kehityksen rinnalle on tullut myös negatiivinen puoli, rikollisuus. Kukapa ei olisi kuullut tietomurroista tai viruksista. Nämä kaikki ovat rikollisen toiminnan ilmentymiä.

Suomessa tietotekniikka on otettu huomioon rikoslainsäädännössä kahdella tavalla. Silloin kun tietotekniikan väärinkäytökset ovat luonteeltaan samantyyppisiä kuin perinteiset rikokset, on tarkistettu näitä rikoksia koskevia säännöksiä. Esim. petossäännöstä on muutettu siten, että koneellisen tietojenkäsittelyn lopputuloksen muuttaminen on rinnastettu perinteiseen ihmisen erehdyttämiseen. Vastaavalla tavalla, jos tietotekniikka on tuonut mukanaan uudenlaista käyttäytymistä, on säädetty uusia tietotekniikkaan liittyviä tunnusmerkistöjä.[1]

Kohdistan tutkimukseni koskemaan rikoslain (19.12.1889/39) 38 lukua. Olen huomioinut, että tieto- ja viestintärikoksia on säädelty myös muissakin rikoslain luvuissa[2], mutta maisteritutkielmani ei perehdy näihin rikoslain säännöksiin. Tutkimustehtäväni on tutkia rikoslain 38 luvun sisältö ja tulevaisuus. Tehtävänäni on myös tutkia, miten ja miksi rikoslain 38 luku muuttui vuonna 1995 rikoslain kokonaisuudistuksen myötä.

Työni tavoitteena on selvittää mitä tieto- ja viestintärikoksilla tarkoitetaan, mitä rikoslain 38 luku pitää sisällään sekä millainen historiallinen lainsäädännöllinen kehitys tieto- ja viestintärikoksilla on ollut rikosalain 38 luvussa. Tieto- ja viestintärikokset ovat lisäksi hyvin kansainvälisiä rikoksia. Pyrin esittelemään työssäni kansainvälisiä elimiä, joiden tarkoituksena on harmonisoida tieto- ja viestintärikosten säädöksiä.

Tämä tutkimus kuuluu informaatio-oikeuden piiriin. Oikeusinformatiikka on oikeustieteellinen tutkimus- ja opetusala. Sen puitteessa opetetaan ja tutkitaan oikeuden ja informaation sekä oikeuden ja tietotekniikan välisiä suhteita eri muodoissaan sekä niiden yhteydessä ilmeneviä oikeudellisia sääntely- ja tulkintakysymyksiä. Oikeusinformatiikka jakaantuu eri osa-alueisiin ja maisteritutkielmani sisältyy tietotekniikkaoikeuteen.

[1] Nuutila 1995, s. 529.

[2] Esimerkiksi rikoslain 28 luvun 7-9 §:t käsittelevät luvattoman käytön tunnusmerkistön, yrityssalaisuuden rikkomisesta ja yrityssalaisuuden väärinkäytöstä on säädelty rikoslain 30 luvun 4-6 §:ssä. Myös väärennös (33 luvun 1-3 §:t), maksuvälinepetos (37 luvun 8-10 §:t), vaaran aiheuttaminen tietojenkäsittelylle (34 luvun 9a§) sekä tietoverkkovälineen hallussapito (34 luvun 9b §) ovat tieto- ja viestintärikoksia.

Tietotekniikkaoikeudella tarkoitetaan *Saarenpään* mukaan *”sitä oikeusinformatiikan osaa, minkä puitteissa tutkitaan tietotekniikan sekä sen tuotteiden ja palveluiden käyttöönottoon ja käyttämiseen liittyviä yksittäisiä, eri oikeudenaloille vaikuttavia oikeudellisia sääntely- ja tulkintaongelmia”*.[3]

Tutkielma rakentuu seitsemästä eri luvusta. Ensimmäisenä määrittelen yksityisyyden, henkilötiedon ja tietosuojan käsitteet. Sen jälkeen kerron mitä tieto- ja viestintärikoksilla tarkoitetaan.

Kolmannessa pääjaksossa selvitän tieto- ja viestintärikosten kriminalisointia. Miten tieto- ja viestintärikokset on säännelty Suomessa ja milloin sääntely on aloitettu. Esittelen myös tieto- ja viestintärikosten kansainvälistä yhteistyötä.

Neljännessä pääjaksossa kerron rikoslain 38 luvun sisällön. Miten luku on rakentunut ja millainen tunnusmerkistö siihen liittyy. Tuon ilmi rikosilmoitusten määriä ja tuomioiden lukumääriä, kun rikoslain 38 luvun säännökset ovat päärikoksia.

Viidennessä pääjaksossa esittelen lakimuutokset, jotka ovat liittyneet rikoslain 38 lukuun sen jälkeen kun lukuun tehtiin suurempi muutos vuonna 1995. Kuudennessa jaksossa käsittelen tieto- ja viestintärikoksia muissa rikoslain luvuissa kuin 38 luvussa.

Lopuksi käsittelen hieman tulevaisuutta. Mitä tulevaisuus tuo mahdollisesti tullessaan rikoslain 38 lukuun ja esittelen yhden tämän hetken tärkeimmästä esityksestä uuden lain säätämiseen. Kyseessä on identiteettilain säätäminen.

[3] Saarenpää 2011, s. 527.

1 TIETOSUOJA YKSITYISYYDEN JA HENKILÖTIETOJEN SUOJANA

1.1 Yksityisyys

Perustuslain 10 §:n 1 momentin mukaan *"jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään erikseen lailla"*. Jokaisella on oikeus yksityisyyteen eli oikeuteen elää oma elämänsä niin kuin itse haluaa. Kukaan ulkopuolinen ei voi aiheettomasti puuttua kenenkään yksityiselämään.[4]

Yksityiselämän suojalla ja yksityisyydellä on ihmiselle tärkeä merkitys. Yksityiselämään kuuluu muun muassa yksilön oikeus vapaasti solmia ja ylläpitää suhteita muihin ihmisiin ja ympäristöön sekä oikeus määrätä itsestään. Lisäksi siihen kuuluu myös se, että kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton eli viestisalaisuus. Kirje- ja puhelinsalaisuus on käytännössä tärkein luottamuksellisen viestin muoto, mutta säännös koskee myös viestinnän uusia tekniikoita.[5]

Saarenpään mukaan yksityisyys voidaan määritellä ainakin kymmeneen eri osa-alueeseen: fyysiseen yksityisyyteen, alueelliseen yksityisyyteen, sosiaaliseen yksityisyyteen, mediayksityisyyteen, anonymiteettiin, yksityisyyteen henkilötietojen käsittelyssä, tiedolliseen omistusoikeuteen, oikeuteen tulla arvioiduksi oikeassa valossa, potilasyksityisyyteen sekä viestintäyksityisyyteen.[6]

Jokaisella on oikeus yksityisyyteen ja oikeus vaieta omista asioistaan ellei tietojenantovelvollisuus viranomaiselle perustu lakiin[7]. Itsemääräämisoikeuden puitteissa yksilöllä on oikeus päättää itse itseään koskevista asioista. *Saarenpää* jakaa itsemääräämisoikeuden viiteen eri osaan. Ne ovat oikeus sisäiseen vapauteen, oikeus ulkoiseen vapauteen, oikeus kompetenssiin, oikeus valtaan ja oikeus tietoon.[8]

Oikeudella sisäiseen vapauteen tarkoitetaan sitä, että jokaisella on oikeus henkiseen loukkaamattomuuteen. Ulkopuolisilla ei ole oikeutta loukata kenenkään kunniaa tms. Oikeus ulkoiseen vapauteen merkitsee oikeutta olla fyysisesti yksin ja liikkua ja valita

[4] Hallberg 2011, s. 45.
[5] Hallberg 2011, s. 46.
[6] Saarenpää 2011, s. 319-324.
[7] Korhonen 2003, s. 103.
[8] Saarenpää 2011, s. 243.

asuinpaikkansa vapaasti. Termillä kompetenssi tarkoitetaan kelpoisuutta eli yksilöllä on kelpoisuus toimia yhteiskunnassa eli jokaisen oikeus toimia itse omassa asiassaan.[9]

Oikeus valtaan merkitsee esimerkiksi oikeutta määrätä omasta terveydestämme, ruumiistamme ja meitä koskevasta informaatiosta. Ihmisen katsotaan omistavan oikeudellisesti itsensä. Jokaisella on myös tiedollinen itsemääräämisoikeus eli oikeus määrätä omista tiedoista.[10]

1.2 Henkilötieto

Perustuslain 10 §:n 1 momentin jälkimmäisen virkkeeseen sisältyy sääntelyvaraus, jonka mukaan henkilötietojen suojasta säädetään tarkemmin lailla. Henkilötietojen suoja kuuluu yksityiselämän suojan piiriin[11]. Kyseisellä lailla tarkoitetaan henkilötietolakia (22.4.1999/523).

Henkilötiedolla tarkoitetaan henkilötietolain 3 §:n mukaan kaikenlaisia luonnollista henkilöä tai hänen elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi.

Henkilötieto liittyy identiteetin käsitteeseen. Henkilötieto muodostaa osajoukon identiteettitiedosta, mutta kaikki identiteettitieto ei ole henkilötietolain tarkoittamaa henkilötietoa.[12] Identiteetti sisältää kaiken sellaisen tiedon, jonka avulla identiteetin haltijat voidaan erotella toisistaan[13].

Jokaisella henkilöllä on vain yksi henkilöllisyys, mutta identiteettejä voi olla useita elämässä, kuten yksityishenkilönä, työntekijänä tai kansalaisena. Identiteetti sisältää henkilötietoja, ne voivat olla todellisia, mutta yhtä hyvin keksittyjäkin. On vaikea varmistua siitä, että henkilö on se, joka hän väittää olevansa ja samalla suojataan henkilöllisyyttä.[14]

---

[9] Saarenpää 2011, s. 243-244.
[10] Saarenpää 2011, s. 244-245.
[11] Viljanen 2011, s. 396.
[12] Henkilöllisyyden luomista koskeva hanke (identiteettiohjelma). Työryhmän loppuraportti 2010, s. 17.
[13] Tavi 2011, s. 61.
[14] Männikkö 2010, s. 9.

Identiteetti näyttelee suurta osaa myös virtuaalisessa maailmassa. Tällöin identiteetistä puhutaan sähköisen identiteetin muodossa. Sähköinen identiteetti on kokoelma henkilön käyttäjätietoja jossain organisaatiossa tai verkkopalvelussa[15]. Verkkoyhteiskunnassa identiteetin varastaminen ei ole vaikeaa. Jokainen voi varastaa toisen identiteetin ja sen myötä minuuden. Vastaavasti jokainen voi joutua varkauden uhriksi. Identiteetin varkaudesta on lukuisia muunnelmia, mutta yhteistä kaikille on se, että joku käyttää toisen ihmisen identiteettiä esittämään itseään. Identiteetin tietoja käytetään usein laittomaan tekoon, esimerkiksi ostetaan toisen luottokelpoisuudella tavaroita tai palveluja, joita ei ole tarkoitustaan maksaa.[16]

1.3 Tietosuoja

Tietosuojalla tarkoitetaan ihmisen henkilötietojen sekä henkilökohtaiseen toimintaan liittyvien tietojen keräämisen ja käsittelyn rajoittamista niin, ettei henkilön yksityisyys turhaan vaarannu.[17] Termit tietosuoja ja henkilötietojen suoja ovat synonyymejä, vaikkakin käsitteille voidaan löytää myös hieman erilainen sisältö. Tällöin tietosuojalla tarkoitetaan koko tietosuojalainsäädäntöä. Henkilötietojen suojalla taas tarkoitetaan lähinnä perustuslain 10.1 §:n säännöstä, henkilötietodirektiiviä sekä henkilötietolakia.[18]

Henkilötietojen suojan ja tietosuojan käsitteet on kuitenkin syytä erottaa toisistaan. Oikeudellinen peruskäsite on henkilötietojen suoja. Se on tietosuojalainsäädännön avulla toteutettavaa yksilön perusoikeuksien, yksityisyyden suojaa. Termiä tietosuoja käytetään puhuttaessa henkilötietojen suojan oikeudellisesta sääntelystä.[19]

Käsite on kuitenkin *Saarenpään* mukaan harhaanjohtava. Ensisijaisena tavoitteena on suojata luonnollisia henkilöitä ja heidän oikeuksiaan, ei suinkaan vain tietoja. Tietosuojalainsäädäntö suojaa yksilöitä ja heidän perusoikeuksiaan henkilötietojen käsittelyn avulla toteutettavaa informaatioväkivaltaa vastaan.[20]

---

[15] Linden 2010, s. 11.
[16] Heinonen 2001, s. 63, 201.
[17] Järvinen 2002, s. 21.
[18] Korhonen 2010, s. 511.
[19] Saarenpää 2011, s. 325.
[20] Saarenpää 2011, s. 325.

Sähköisen viestinnän tietosuojalain (16.6.2004/516, lyhenne SVTSL) 1 luvun 2 §:n 13 kohdan mukaan tietoturvalla tarkoitetaan hallinnollisia ja teknisiä toimia, joilla varmistetaan se, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla sekä sitä, ettei tietoja voida muuttaa muiden kuin siihen oikeutettujen toimesta ja että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä. Myös valtioneuvoston asetuksessa tietoturvallisuudesta valtionhallinnossa (1.7.2010/681) määritellään tietoturvallisuus samalla tavoin. Tietoturvallisuudella tarkoitetaan em. asetuksen 1 luvun 3 §:n 2 kohdan mukaan tietojen salassapitovelvollisuuden ja käyttörajoitusten noudattamiseksi sekä tietojen saatavuuden, eheyden ja käytettävyyden varmistamiseksi toteutettavia hallinnollisia, teknisiä ja muita toimenpiteitä ja järjestelyjä.

Kirjallisuudesta löytyy *Korhosen* mukaan erilaisia yrityksiä määritellä termi tietoturvallisuus. Sillä tarkoitetaan muun muassa järjestelmien, tietojen ja palveluiden suojaamista sekä normaali- että poikkeusoloissa oikeudellisten, hallinnollisten ja teknisten toimenpiteiden avulla. Tietoturvallisuutta voidaan myös kuvata asiantilana, joka saavutetaan estämällä informaatioon ja sen käsittelyyn sekä tietoliikenteen luottamuksellisuuteen[21], eheyteen[22] ja käytettävyyteen[23] kohdistuvien uhkien toteutumista sekä rajoittamalla uhkista aiheutuvia vahinkoja.[24]

Niin kansainvälisessä kuin kotimaisessakin keskustelussa tietosuoja sekä tietoturvallisuus (tietoturva) sekoitetaan usein toisiinsa. Yhtenä syynä tähän *Korhosen* mukaan on se, että tietosuojalainsäädäntö muodostaa tietoturvallisuusoikeuden keskeisen normilähteen. Mutta tietosuojalla ja tietoturvallisuudella tarkoitetaan kuitenkin eri asioita. Tietosuoja muodostuu oikeudellisesti normeista, jotka koskevat yksityisyyden suojaa henkilötietojen käsittelyssä.[25]

Tietoturvasta huolehtiminen tarkoittaa siten toimijan ja sen asiakkaiden tai käyttäjien käyttämän verkko-, viestintä- tai lisäarvopalvelun luottamuksellisuuden, eheyden ja käytettävyyden varmistamista hallinnollisin ja teknisin toimin. Käsitteet kuitenkin liit-

[21] Tiedot, järjestelmät ja palvelut ovat vain niihin oikeutettujen saatavissa eikä niitä luvatta paljasteta tai muutoin saateta sivullisten tietoon. Korhonen 2010, s. 512.
[22] tarkoitetaan sitä, etteivät tiedot, järjestelmät tai palvelut ole laitteisto- tai ohjelmistovikojen, luonnontapahtumien tai oikeudettoman inhimillisen toiminnan seurauksena muuttuneet tai tuhoutuneet. Korhonen 2010, s. 512.
[23] tiedot, järjestelmät ja palvelut ovat tarvittaessa niihin oikeutettujen esteettä ja häiriöittä hyödynnettävissä oikeaan aikaan. Korhonen 2010, s. 512.
[24] Korhonen 2010, s. 511-512.
[25] Korhonen 2010, s. 511.

tyvät toisiinsa olennaisella tavalla: tietosuojaa pyritään toteuttamaan muun muassa tietoturvalla.[26]

Tietoturvallisuus on myös riskienhallintaa, jolloin sillä on läheiset yhteydet informaatio- ja tietotekniikkariskeihin. Tietotekniikkariskit ovat tietotekniikan ja sille rakentuvien järjestelmien toiminnassa ilmeneviä häiriöitä tai virheitä. Vakavimpana tietoturvallisuusuhkana yhteiskunnan ja valtion turvallisuuden kannalta *Korhosen* mukaan on informaatiosota (verkkosodankäynti). Yhteiskunnan toiminnot ovat yhä riippuvaisempia tietotekniikasta ja samalla siten haavoittuvia. Hyökkäys esimerkiksi energianjakelua, maksuliikennettä tai viestintää ylläpitäviin tietojärjestelmiin saattaa muodostua ratkaisevaksi sota- tai kriisitilanteessa sen lopputuloksen kannalta.[27]

Informaatiosota käsitteenä on kuitenkin vielä vakiintumaton. Sillä voidaan tarkoittaa toimenpiteitä, joiden tarkoituksena on päästä käsiksi konfliktin osapuolen hallussa olevaan informaatioon ja tämän käyttämiin tietojärjestelmiin, hyödyntää tai vaikuttaa niihin sekä suojella omia tietojärjestelmiä tällaisilta toimenpiteiltä.[28]

Yksityisyyttä, yksityiselämän suojaa ja tietosuojaa koskeva oikeuskulttuuri on Pohjoismaissa suhteellisen yhtenäinen muiden ohella Euroopan neuvoston ihmisoikeussopimuksen ja EU:n henkilötietodirektiivin vaikutuksesta. Silti merkittäviäkin eroavaisuuksia on pohjoismaiden henkilötietolakien välillä erityisesti niiden käsitteistöissä (privatlivets fred, personlig integritet, personvern) on selkeitä eroja verrattaessa esimerkiksi Suomen säännösten virallisia ruotsinkielisiä versioita muiden Pohjoismaiden lakiteksteihin.[29]

Käsitteiden välisistä hierarkkisista suhteista on erilaisia mielipiteitä suomalaisessa oikeustieteessä. Esimerkiksi yksityisyyden käsitteen osalta on eriäviä näkemyksiä jopa niissä 1990-luvun hallituksen lakiesityksissä, jotka käsittelevät perustuslakia, henkilötietolakia ja rikoslain yksityiselämän suojaa koskevia uudistuksia. Oikeuslähdepohjalla onkin vaikutusta tarkastelun lopputulokseen. Eräät oikeustieteilijät katsovat yläkäsitteeksi yksityiselämän suojan, toiset taas yksityisyyden suojan. *Korhonen* pitää tekstissään yk-

[26] Innanen - Saarimäki 2009, s. 104.
[27] Korhonen 2010, s. 512-513.
[28] Korhonen 2010, s. 513-514.
[29] Korhonen 2005, 21.

sityisyyttä yläkäsitteenä, jonka alla ovat muun muassa yksityiselämän suoja ja henkilötietojen suoja sekä eräät muut yksityisyyteen kuuluvat arvot ja intressit.[30]

[30] Korhonen 2005, 22.

2 MITÄ TIETO- JA VIESTINTÄRIKOKSILLA TARKOITETAAN?

2.1 Tieto, data ja informaatio

Tieto- ja viestintärikosten nimikkeessä ovat käsitteet tieto ja viestintä. Alkuun on hyvä kertoa mitä ne tarkoittavat. Käsite tieto on monimerkityksinen sana. Se kuvaa tietämystä yleensä sekä viittaa tietoon informaationa tai tarkoittaa ainoastaan dataa[31]. *Niiniluodon* mukaan tieto on ihmisen ajattelun tulos tai kohde. Usein sanat data, informaatio, tietämys ja sanoma ovat synonyymejä tieto-sanalle.[32]

Tieto on hyvin perusteltu tosi uskomus. Jos tieto ei olisi hyvin perusteltua, se olisi pelkkää luuloa. Tieto on myös totta ja tämä ehto erottaa sen erehdyksestä ja uskomus taas arvauksesta. Usko on vakaumus, jossa uskova nojautuu perusteisiin, mitkä hänelle ovat arvokkaat ja painavat.[33]

Data kuvaa tietoa esittäviä merkkejä. Viestinnällä ymmärretään tiedon vastaanottamisen ja lähettämisen muodostamaa kokonaisuutta.[34] Datan ei tarvitse olla tietokoneella käsiteltävässä muodossa vaan sillä tarkoitetaan tiedon merkkejä, jotka ovat luettavissa, käsiteltävässä tai viestittävissä muodossa[35].

Informaatio on vastaanotetun datan ihmiselle tuottamaa mielle tai merkitys.[36] Vastaanottaja itse tulkitsee viestin merkityksen. Viesti, jota ei ole purettu tai avattu, on dataa. Data siis muuttuu informaatioksi, kun sen sisältämä viesti on tulkittu. Kun data on avattu ja sen sisältämä informaatio tulkittu, syntyy tieto. Viestintä on kommunikaatiota eli viestin lähettämistä lähettäjältä vastaanottajalle[37].

[31] HE 94/1993 vp. s. 132.
[32] Niiniluoto 1996, s. 48.
[33] Niiniluoto 1996, s. 57.
[34] HE 94/1993 vp. 132.
[35] Pihlajamäki 2004, s. 26-27.
[36] Niiniluoto 1996, s. 43.
[37] Niiniluoto 1996, s. 24.

2.2 Tietotekniikkarikokset

Oikeusinformatiikan[38] yksi neljästä osa-alueesta on tietotekniikka-oikeus[39]. Tietotekniikkaoikeuden piirissä käsitellään asioita, jotka kuuluvat jatkuvasti ja pysyvästi myös muiden oikeustieteen alojen piiriin.[40] *Saarenpään* mukaan tietotekniikkaoikeuden puitteissa tutkitaan tietotekniikan sekä sen palveluiden ja tuotteiden käyttämiseen ja käyttöönottoon liittyviä yksittäisiä, eri oikeudenaloille vaikuttavia oikeudellisia sääntely- ja tulkintaongelmia. Tieto- ja viestintärikokset ovat tietotekniikkarikoksia ja ne kuuluvat tietotekniikkaoikeuteen.[41]

Tietotekniikkaoikeus syntyi heti sen jälkeen, kun tietotekniikan käyttöön liittyvien oikeudellisten kysymyksien olemassaolo havaittiin. Ensimmäisen askeleen otti Yhdysvallat 1960-luvulla. Syntyi computer law, joka koski tietokoneiden ja niiden ohjelmien sopimuksia sekä tietotekniikan immateriaalioikeudellisia kysymyksiä.[42]

Myöhemmin tietotekniikkaoikeus on vakiintunut ammatillisen osaamisen sekä oikeudellisen keskustelun erityisalueeksi. Informaatio-oikeuden ja tietotekniikkaoikeuden välillä ei ole suurta rajaa. Esimerkiksi sähköistä henkilökorttia pystytään katsomaan monesta eri näkökulmasta. Oikeudellisena ilmiönä henkilötietojen suojan näkökulmasta sekä infrastruktuurin kehitykseen liittyen ovat informaatio-oikeutta, mutta elektronisen kaupan näkökulmasta se on kauppaoikeutta sekä tietotekniikkaoikeutta. Lisäksi näkökulmana voi olla myös persoonallisuusoikeus digitaalisen identiteetin osoittajana. Tietotekniikkarikokset taas ovat sekä informaatio-oikeuden, tietotekniikkaoikeuden sekä rikosoikeuden tutkimuskohteita.[43]

Tietotekniikkarikoksiin liittyvä akateeminen tutkimus on uusi ala koko maailmassa. Tietotekniikkarikoksille on tunnusomaista se, että se käsittelee monta eri alaa (rikosoikeus, oikeusinformatiikka, tietotekniikka), mutta *Rossin* mukaan tutkimuksia on alettu tekemään enenevässä määrin ja kirjallisuuttakin on jo saatavilla. Mutta *Ross* huomauttaa

[38] Oikeusinformatiikka on oikeustieteellinen tutkimus- ja opetusala. Sen puitteissa opetetaan ja tutkitaan oikeuden ja informaation sekä tietotekniikan ja oikeuden välisiä suhteita eri muodoissaan samoin kuin niiden yhteydessä ilmeneviä oikeudellisia sääntely- ja tulkintakysymyksiä.
[39] Muita osa-alueita oikeusinformatiikan erityisessä osassa ovat: oikeudellinen tietojenkäsittely, oikeudellisen informaation tutkimus ja informaatio-oikeus.
[40] Saarenpää 1999, s. 714.
[41] Saarenpää 2011, 527.
[42] Saarenpää 2011, 527.
[43] Saarenpää 2011, 527.

samalla, että usein kirjallisuus on jo julkaistaessa vanhentunutta. Ja tämähän johtuu tietotekniikan nopeasta kehityksestä. Esimerkkinä kasvavasta kiinnostuksesta tietotekniikkarikoksia kohtaan on akateemisen aikakauslehden, International Journal of Cyber Criminology, julkaiseminen.[44]

Suomessa akateeminen tietotekniikkarikoksien tutkimus kuuluu jo aiemmin esittelemääni oikeusinformatiikan alaan. Mutta aivan hyvin se voisi kuulua rikosoikeuden piiriin. Miksi näin? *Korhosen* artikkelin mukaan oikeusinformatiikka tutkii informaation ja oikeuden sekä tietotekniikan ja oikeuden välistä suhdetta. Oikeusinformatiikkaan tietotekniikkarikokset ovat luonteva tutkimusala ja myös kansainvälisesti katsottunakin tietotekniikkaoikeus ja informaatio-oikeus ovat hyvin lähellä toisiaan.[45]

Tietotekniikkaoikeuteen kuuluviksi luetaan lähtökohtaisesti sellaiset oikeudelliset kysymykset, joiden käsitteleminen ja ratkaiseminen edellyttävät niihin liittyvien tietoteknisten seikkojen ymmärtämistä. Kysymys on siten oikeudellisen ongelman tunnistamisesta tietoteknisessä ympäristössä.[46]

Käsitteenä tietotekniikkarikos on eräänlainen yläkäsite, johon sisältyy erityyppiset tietoteknisessä ympäristössä tehdyt rikokset, kuten esimerkiksi tietoverkkorikokset. Rikoksen tekovälineenä tai teon kohteena on tieto- tai tiedonsiirtojärjestelmä laitteineen. Määritelmät viittaavat niin tietokoneisiin, dataan tai informaatioon, mutta myös tietoverkkomaailmaan, joka on syntynyt Internetin käytön laajenemisen mukana.[47]

Poliisihallinnon tietotekniikkatutkinnan kehittämistä suunnitteleva työryhmä on esittänyt, että poliisitoimessa otettaisiin käyttöön käsite tietotekniikkarikos, jolla tarkoitetaan:

1) tietoverkkorikoksia: rikos, joka on tehty tietoverkossa ja se kohdistuu tietoverkkoihin liitettyihin tietojärjestelmiin, kuten palvelunestohyökkäykset, haittaohjelmien avulla tehdyt rikokset kuten pankkiyhteyksien kaappaaminen.

2) tietoverkkoja hyväksikäyttäen tehtyjä rikoksia: rikokset, joissa tietoverkko on vain väline rikoksen tekemiselle, kuten esimerkiksi perinteiset Internet petokset, maksuvälinepetokset tietoverkoissa, rahanpesu ja piratismi.

---

[44] Ross 2010, s. 26-27.
[45] Korhonen 2006, s. 91.
[46] Saarenpää 2011, 528.
[47] Tietotekniikkatutkinnan järjestäminen poliisissa 2008, s. 8.

3) tietotekniikkaa hyväksikäyttäen tehtyjä rikoksia: Tietoteknisessä ympäristössä tehdyt rikokset, joita ei ole tehty tietoverkkojen kautta. Rikokset on tehty esimerkiksi yrityksen paikallisessa tietojärjestelmässä tietotekniikkaa hyödyntäen tai tietojärjestelmään kohdistuen, kuten esimerkiksi petokset, vahingonteot sekä tietotekniset väärennökset ja kavallukset.[48]

Jordanin mukaan tietoverkkorikollisuuteen kuuluu lisäksi myös tietoverkkoväkivalta. Väkivalta aiheuttaa niin psykologista kuin fyysistäkin vahinkoa. Tätä tapahtuu esimerkiksi eri foorumeilla.[49]

Mielestäni työryhmän esitys kuvaa hyvin sitä, mitä tietotekniikkarikos on ja antaa samalla määritelmän tieto- ja viestintärikoksille. Tietotekniikkarikos on rikos, joka kohdistuu tietojärjestelmään ja se on myös rikos, joka tehdään tietojärjestelmän avulla. Yhteistä rikostyypeille on se, että tietojärjestelmä toimii tekoympäristönä ja niiden tekeminen edellyttää asiantuntemusta tietojärjestelmien toiminnasta.

Tietotekniikkarikokset liittyvät kiinteästi tietotekniseen kehitykseen. Mutta lainsäädäntö on tullut perässä koko ajan ja se ei ole antanut poliisin suorittamaan esitutkintaan, syyttäjän tai tuomioistuinten toimintaan riittävää sääntelyä. Asiaan kiinnitettiin Suomessa enemmän huomiota vasta 1990-luvun alussa, kun pohdittiin yksityiskohtaisemman sääntelyn tärkeyttä tieto- ja viestintärikoksissa. Vuonna 1995 koettiin merkittävä uudistus, kun tieto- ja viestintärikokset saivat rikoslaista oman lukunsa rikoslain kokonaisuudistuksen myötä.

[48] Tietotekniikkatutkinnan järjestäminen poliisissa 2008, s. 9.
[49] Jordan 2008, s. 92.

3 TIETO- JA VIESTINTÄRIKOSTEN KRIMINALISOINTI JA KANSAINVÄLINEN YHTEISTYÖ TIETO- JA VIESTINTÄRIKOSTEN PARISSA

3.1 Yleistä

Ensimmäinen elektroninen tietokone, ENIAC[50], valmistettiin vuonna 1946 Yhdysvalloissa. Tietokoneiden mukana tulivat myös tietokonerikokset, mutta *Xinganin* mukaan tietokonerikokset eivät ole olleet samanlaisia koko ajan, vaan ne ovat kehittyneet neljässä eri vaiheessa.[51]

Ensimmäinen vaihe ajoittuu 1940- luvun lopulta 1960-luvun loppuun. Tänä aikana tietokonerikollisuus syntyi. Kriminalisoinneilla ei pyritty asiaan vaikuttamaan. Toinen vaihe ajoittuu 1970-luvulta 1980-luvun lopulle. Tietokonerikokset kehittyivät ja kriminalisointiin herättiin. Kolmas vaihe sijoittuu 1990-luvulla, jolloin tietokonerikokset laajenivat ja kriminalisointiin kiinnitettiin huomiota. Tähän aikakauteen liittyy Internetin käyttöönotto. Viimeinen vaihe alkoi vuoden 2000 tienoilla, jolloin tietokonerikollisuus on jo jokapäiväistä ja lakeja sen estämiseksi on jo tehty.[52]

Tieto oli 1990-luvun puolivälissä yhteiskunnassa tärkeä resurssi, joka vaati oman ja omintakeisen oikeussuojan. Tiedon kasvu ja kehitys johtui uudenlaisesta tietotekniikasta. Samalla kun tietotekniikka tehosti yhteiskunnan toimintoja, se oli aikaansaanut uudenlaista haavoittuvuutta. Tästä aiheutui ongelmia ainakin kolmella alueella: tiedon tallennuksessa, käsittelyssä ja siirrossa.[53]

Tietotekniikkarikoksiin liittyviin lainsäädäntöhankkeisiin on Suomessa ryhdytty jo 1980-luvun loppupuolella. Samaan aikaan myös muualla Euroopassa suunniteltiin omia lainsäädäntöjä.[54] *Xingan* kertoo väitöskirjassaan, että aluksi tietotekniikkarikoksia ei katsottu omaksi rikosalakseen. Tietotekniikkarikos oli ihan normaali rikos, se miten se

[50] lyhenne sanoista Electronic Numerical Integrator And Computer
[51] Xingan 2005, s. 60.
[52] Xingan 2005, s. 61-75.
[53] HE 94/1993 vp. s. 132.
[54] Pihlajamäki 2004, s. 105.

tehtiin tai kohdistuiko se tietojärjestelmiin ei ollut merkitystä. Eihän esimerkiksi murhan tunnusmerkistökään muutu sen mukaan millä tekovälineenä se tehdään.[55]

Pihlajamäen mukaan Ruotsi on ollut edelläkävijän asemassa nykyaikaisen tietotekniikan käyttöön ja siihen kohdistuneiden väärinkäytöksien sääntelyhankkeissa. Ruotsin datalagen on vuodelta 1973 (1973:289). Lain tarkoituksena oli estää sellaisten henkilötietojen tallentaminen tietoteknisin apuvälinein, joiden käyttäminen saattaisi vaarantaa asianomistajan yksityisyyttä.[56]

Tietotekniikkarikollisuus on nopeasti rajat ylittävää rikollisuutta, josta johtuen kansainvälistä yhteistyötä on harjoitettu paljon. Globaalin ongelman on aiheuttanut Internetin käyttö.[57] On tärkeää, että eri maiden tietotekniikkarikoksiin liittyvät säännökset vastaisivat toisiaan. Tällä voidaan minimoida mahdollisuus siitä, että jostain valtiosta muodostuisi tietotekniikkarikosten tekijöille sellainen suojasatama (computer crime heaven) tai paratiisi (data paradise), jossa rikollista toimintaa harjoitettaisiin ilman pelkoa viranomaisten puuttumista asiaan.[58]

3.2 Tieto- ja viestintärikosten kriminalisoinnista

3.2.1 Lainsäädäntötekniikan valinta

Tiedonsiirtomuotojen yleistyminen ja automaattisen tietojenkäsittelyn yleistyminen nostivat esiin tarpeen tarkastella tietoa ja tietoliikennettä omana kokonaisuutenaan myös rikosoikeudellisen sääntelyn kannalta. Tietotyö ja automaattisen tietojenkäsittelyn sovellukset ulottuivat lähes kaikkiin inhimillisiin toimintoihin ja niinpä siitä aiheutuvat vaatimukset oli otettava huomioon kaikilla lainsäädäntölohkoilla. Kaikki OECD-maat, lukuun ottamatta Yhdysvaltoja, katsoivat, ettei tarvita erillistä atk-rikoslakia, vaan että atk-rikoksiinkin on mahdollisimman pitkälle sovellettava olemassa olevia rikossäännök-

[55] Xingan 2008, s. 113.
[56] Pihlajamäki 2004, s. 105.
[57] Xingan 2005, s. 116.
[58] Pihlajamäki 2004, s. 161.

siä.[59] Valittavana oli kaksi eri vaihtoehtoa: joko sisällyttää uudet säännökset jo olemassa olevaan lakiin tai luoda kokonaan uusi säännöstö.

Automaattista tietojenkäsittelyä pidettiin uutena ilmiönä, jonka kautta se oli luonut uusia rikoksentekomahdollisuuksia sekä uudenlaisen ympäristön perinteisille rikoksille. Tästä johtuen uudet rikokset oli otettava huomioon jo olemassa olevan rikosoikeusjärjestelmän osana eikä erillisenä ilmiönä.[60]

Suomen rikoslaki on peräisin vuodelta 1889 ja sitä on uudistettu useita kertoja, mutta vielä ennen vuotta 1995 siitä puuttuivat tarkat tieto- ja viestintärikoksiin liittyvät kohdat.[61] Tieto- ja viestintärikosten sääntelyä oli, mutta se esiintyi muiden lakien joukossa. Tämän seurauksena tieto- ja viestintärikoksille muodostettiin rikoslakiin oma lukunsa.

3.2.2 Tieto- ja viestintärikoksille oma luku rikoslakiin

Nykyaikainen tietotekninen kehitys on tuonut mukanaan uudentyyppistä käyttäytymistä. Tämä on aiheuttanut sen, että on säädetty uusia tietotekniikkaan liittyviä tunnusmerkistöjä.[62] Muiden mukana Suomi päätti sen, että mitään erillistä atk-lakia ei säädetä, vaan ne tieto- ja viestintärikokset, jotka eivät jo olleet rikoslaissa, käsitellään yhdessä luvussa.

Ennen vuoden 1995 rikoslain uudistusta hallituksen esityksen mukaan tieto- ja viestintärikostyypit käsitellään lukusystemaattisesti yhtenä kokonaisuutena, vaikka ne perinteisen oikeushyväjaotuksen näkökulmasta muodostavat jossakin määrin epäyhtenäisen ryhmän. Ne kun kohdistuvat osaksi yksilöön ja osaksi koko yhteiskuntaan sekä sisältävät ainesosia niin rauhaa, vapautta, kunniaa, yksityiselämää kuin yleistä järjestystäkin loukkaavista ja vaarantavista rikoksista. Toisaalta myös tietojärjestelmien toimivuus ja tietohallinnon luotettavuus sinänsä voidaan nykyaikaisessa yhteiskunnassa nähdä itse-

[59] HE 94/1993 vp. s. 133.
[60] Pihlajamäki 2004, s. 7.
[61] HE 94/1993 vp. s. 1.
[62] Nuutila1995, s. 529.

näisenä oikeushyvänä. Lisäksi niiden sijoittaminen yhteen lukuun on omiaan korostamaan tiedon ja viestinnän entistä suurempaa merkitystä.[63]

Tieto- ja viestintärikokset liitettiin osaksi rikoslain 38 lukua (lakimuutos 21.4.1995/578). Ennen vuoden 1995 rikoslain kokonaisuudistusta luku käsitti salaisuuden rikkomisen. Luvun ensimmäisessä pykälässä säädettiin yksityisen tai perheen salaisuuden luvattomasta ilmaisusta muun muassa asianajajan toimesta. Luvussa säädettiin myös kirjesalaisuudesta. Uusien tieto- ja viestintärikosten säännöksien lisääminen rikoslain 38 lukuun oli perusteltu. Vanha luku käsitteli samanlaisia asioita kuin nykyään luvussa käsitellään.

Tieto- ja viestintärikokset muuttuvat tietotekniikan kehityksen myötä ja rikosnimikkeiden ollessa samassa luvussa, auttaa se luomaan kokonaiskuvan tieto- ja viestintärikoksista sekä helpottaa lakimuutoksien tekemistä.[64]

Rikoslain kokonaisuudistuksen myötä lain 38 luku vahvistettiin 21.4.1995 käsittämään tieto- ja viestintärikokset. Voimaan laki tuli 1.9.1995.

Useat kansainväliset järjestöt alkoivat 1980-luvulla kiinnittää erityistä huomiota tietotekniikan nopean kehityksen myötä syntyneeseen uuteen rikosten lajiin, tietotekniikkarikoksiin. Muun muassa OECD:n ja Euroopan neuvoston piirissä on tehty laajaa selvitystyötä, jonka tuloksena molemmat järjestöt julkaisivat lainsäädäntösuosituksia sisältäneet raportit. Myös kansainvälinen rikosoikeusyhdistys AIDP, YK ja Kansainvälinen poliisijärjestö Interpol ottivat tietotekniikkarikokset erityistarkastelun kohteeksi. Erityisesti Euroopan neuvoston suositukset ovat olleet useassa valtiossa ohjeena kansallisia rikoslakeja uudistettaessa, minkä vuoksi kriminalisoinnit ovat jokseenkin yhdensuuntaisia.[65]

[63] HE 94/1993 vp. s. 133.
[64] HE 94/1993 vp. s. 133.
[65] Pihlajamäki 1995, s. 685.

3.3 Kansainvälinen yhteistyö

3.3.1 OECD

Kansainvälinen yhteistyö alkoi jo 1984, kun OECD:n[66] tieto- ja viestintäpoliittinen komitea ICCP[67] asettivat ad hoc-asiantuntijatyöryhmän[68]. Työryhmän oli määrä tutkia rikoslakien harmonisointimahdollisuutta jäsenmaiden alueella. Jo tällöin ilmeni mielipiteiden jakautumista siinä, miten tietotekniikkarikoksia tulisi lainsäädännössä käsitellä. Säädetäänkö tietotekniikkarikoksiksi oma laki vai hyödynnetäänkö jo olemassa olevia kriminalisointeja.[69]

OECD:n toimenkuvassa ei rikosoikeudellisilla kysymyksillä ole ollut erityistä osuutta, vaikkakin työryhmän tutkimuksilla on ollut hyvin suuri merkitys siihen, miten tieto- ja viestintärikosten lainsäädäntöä on alettu suunnittelemaan, tehdäänkö oma atk-laki vai käytetäänkö hyväksi jo olemassa olevaa rikosoikeutta. Usea valtio, Suomi mukaan lukien, onkin valinnut jälkimmäisen vaihtoehdon.

3.3.2 Euroopan Unioni ja Euroopan neuvosto

Myös Euroopan Unionissa on huomattu tietoverkkorikoksien kasvu. Koska Euroopan Unioni ei omaa välitöntä rikosoikeudellista sääntelyvaltaa, se on pyrkinyt vaikuttamaan asioihin välillisesti. Euroopan Unioni tuottaa direktiivien puitteissa tietotekniikkarikosten sääntelyyn vaikuttavaa lähdeaineistoa ja lisäksi se teettää tietotekniikkarikoksia koskevia selvityksiä.[70]

---

[66] Taloudellisen yhteistyön järjestö, joka on perustettu vuonna 1961 harmonisoimaan ja kehittämään jäsenmaiden yhteiskunnallista hyvinvointia. On vuonna 1948 perustetun Euroopan taloudellisen yhteistyöjärjestön jatkaja.
[67] Committee for Information, Computer and Communications Policy.
[68] Työryhmän julkaisema raportti (Computer related Crime. Analysis on Legal Policy) julkaistiin vuonna 1986.
[69] Pihlajamäki 2004, s. 64-65.
[70] Saarenpää 2011, s. 538.

Euroopan neuvosto on lähes kaikki Euroopan valtiot käsittävä sosiaali-, kulttuuri-, ihmisoikeus- ja lainsäädäntöyhteistyökysymyksiä käsittelevä kansainvälinen järjestö.[71]

Euroopan neuvostossa tietotekniikkarikoksia on käsitelty jo 1980-luvun alusta lähtien. Euroopan neuvosto on ottanut ohjelmaansa suojella tietoa/dataa niin yksityisen kuin julkisenkin sektorin puolella.[72]

Vuonna 1985 Euroopan neuvostoon asetettiin asiantuntijakomitea, jonka tarkoituksena oli tutkia ongelmia, jotka liittyvät tietotekniikkarikollisuuteen, analysoida tietotekniikkarikollisuuden eri muotoja aikaisempien tutkimuksien valossa sekä tutkia lainsäädännön kehittämistä. Komitea päätti työnsä vuonna 1989 julkaisemalla raportin.[73]

Vuonna 1991 Euroopan neuvosto asetti asiantuntijakomitean, PC-PC, selvittämään tietotekniikkarikoksiin liittyviä prosessioikeudellisia kysymyksiä. Komitea päätti työnsä vuonna 1995. Julkaisemassaan raportissa käsitellään rikostutkinnan kohteena olevaa elektronisessa muodossa olevaa dataa ja asetettiin kyseenalaiseksi se, onko viranomaisilla käytettävissään vastaavia keinoja todistusaineiston hankkimiseksi tietoverkkoihin ja -järjestelmiin kohdistuneista rikoksista verrattuna tilanteisiin, joissa kysymyksessä on aineellisiin ja konkreettisiin objekteihin kohdistuneista rikoksista ja niiden tulkinnasta.[74]

Cybercrime-työryhmä aloitti toimintansa vuonna 1997 ja sen päämääränä oli valmistella kansainvälinen yleissopimus PC-R-CC:n ja PC-PC:n suositusten pohjalta. Yleissopimus valmistui vuonna 2001 ja sitä kutsutaan nimeltä Convention on Cybercrime eli Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus.[75]

Yleissopimus on avoin kaikille valtioille. Suomessa rikoslain 38 luku muutettiin yleissopimusta vastaavaksi syyskuussa 2007. Merkittävimpinä uudistuksina voidaan pitää tietojärjestelmän häirintää sekä törkeää tietomurtoa koskevia säännöksiä. Lisäksi eräitä rangaistuksia kovennetaan. Nämä muutokset kertovat kaikki yhdenmukaisesti aikaisempaa vakavammasta suhtautumisesta tietotekniikkarikoksiin *Saarenpään* mukaan.[76]

Vuonna 2001 kokoontui PC-RX ensimmäiseen istuntoonsa. Komitean tehtävänä oli valmistaa tietoverkkosopimukseen ensimmäinen lisäpöytäkirja. Lisäpöytäkirja allekir-

[71] Jääskinen 2007, s. 229.
[72] Xingan 2008, s. 314.
[73] Pihlajamäki 2004, s. 68.
[74] Pihlajamäki 2004, s. 79.
[75] Pihlajamäki 2004, s. 79-81.
[76] Saarenpää 2011, s. 537.

joitettiin vuonna 2003. Pöytäkirja velvoittaa kriminalisoimaan tietoverkkojen välityksellä tapahtuvan rasistisen ja muukalaisvastaisen aineiston levittämisen.[77]

3.3.3 Yhdistyneet Kansakunnat

Kriminaalipoliittinen yksikkö on toiminut 1980-luvulta lähtien Yhdistyneiden Kansakuntien sihteeristön yhteydessä. Sen toiminta on keskittynyt niin kutsuttuun valkokaulusrikollisuuteen (white collar crime) ja vallan väärinkäyttöön (abuse of power). Yksikkö on kiinnittänyt erityistä huomiota myös tietotekniikan lisääntyvään käyttöön rikosten kontrolloimisessa ja ehkäisemisessä. Vuoden 1990 kokouksen yhtenä teemana olivat tietotekniikkarikokset ja kokouksen suosituksen mukaan asiantuntijakokous pidettiin 1992 ja sen pohjalta muodostui tietotekniikkarikoskäsikirja.[78]

Pihlajamäen mukaan tietotekniikkakäsikirja poikkeaa aikaisemmista raporteista siinä mielessä, että se ei anna jäsenvaltioille lainsäädäntösuosituksia eikä se edellytä jäsenvaltioiden tekevän minkäänlaisia toimenpiteitä. Käsikirjassa käsitellään esimerkiksi tietotekniikkarikosta ilmiönä, aineellista rikosoikeutta datan, informaation haltijan ja yksityisyyden suojan kannalta sekä kansainvälistä yhteistyötä.[79]

3.3.4 Kansainvälinen rikosoikeusyhdistys AIDP

Kansainvälinen rikosoikeusyhdistys on perustettu Pariisissa vuonna 1924. Järjestö on maailman tärkein rikosoikeustieteilijöiden yhdistys, johon kuuluu yli 3000 jäsentä noin 70 maasta. AIDP järjestämän rikosoikeuskongressin yhtenä neljästä teemasta vuonna 1994 olivat tietotekniikkarikokset.[80]

Järjestö on julkaissut raportin, josta saa kattavan selvityksen tietotekniikkarikosten kehityksestä ja lainsäädännöstä. Raportti tehtiin yhteensä 29 maasta saadusta selvityksestä. Myös AIDP:n raportti tuli samanlaiseen tulokseen, kuin muidenkin järjestöjen tutki-

[77] Pihlajamäki 2004, s. 84-85
[78] Pihlajamäki 2004, s. 85-87
[79] Pihlajamäki 2004, s. 87
[80] Pihlajamäki 2004, s. 95.

mukset, että tietotekniikka on synnyttänyt uusia oikeudellista suojelua kaipaavia intressejä. Ellei perinteinen rikoslaki ole riittävä, niin on joko täydennettävä jo olemassa olevia säännöksiä tai kehitettäviä uusia. Päätöslauselmissaan korostettiin OECD:n ja Euroopan neuvoston työtä kriminalisoinnin kohteeksi suositeltavien menettelytapojen täsmentämisessä.[81]

[81] Pihlajamäki 2004, s. 95, 97.

4 RIKOSLAIN 38 LUKU

4.1 Luvun säännökset

Tietotekniikkarikos määritellään rangaistavaksi teoksi, jonka kohteena, välikappaleena tai tekoympäristönä on tietojärjestelmä siihen kuuluvine laitteineen ja jonka tekeminen ja/tai rikosprosessuaalinen käsittely välttämättömästi edellyttää tietoteknistä erityistietämystä. Tietotekniikkarikokset voidaan jakaa toisaalta datarikoksiin eli tietoa sisältäviin merkkeihin kohdistuviin rikoksiin. Tietotekniikkarikoksia laajassa mielessä ovat myös eräät aineettomien oikeuksien loukkaukset samoin kuin eräät yksityisyyden suojaa loukkaavat teot.[82]

Tietotekniikkarikoksissa rangaistavaa on vain se, mikä on rangaistavaksi säädettyä. Kyse on legaliteettiperiaatteesta eli laillisuusperiaatteesta.[83] Kyseessä olevan teon on oltava rikoslain mukaan rangaistavaa. Verkkorikollisuuden jatkuva muuttuminen on luonut paineita uudistaa rikoslakia, koska haitallisia tekoja ei aina ole ollut mahdollista katsoa rikoksiksi ilman rikosten tunnusmerkistöjen uudistamista.

Tieto- ja viestintärikokset ovat säännelty Suomen rikoslain 38 luvussa. Kuten jo aikaisemmin olen esitellyt, tieto- ja viestintärikokset liitettiin osaksi rikoslain 38 lukua vuonna 1995 (lakimuutoksella 21.4.1995(578)). Sen jälkeen lukua on uudistettu useamman kerran ja lakimuutokset on vahvistettu 22.4.1999/525, 9.6.2000/531, 30.11.2001/1118, 11.5.2007/540 sekä 13.5.2011/441.

Ensin uudistusvuorossa oli henkilörekisteririkos, sitten viestintäsalaisuuden loukkaus ja tietoyhteiskunnan palvelujen suojaamiseen liittyvät uudistukset sekä toiseksi viimeisenä Euroopan neuvoston tietoverkkosopimuksen tuomat muutokset. Viimeisin muutos tapahtui toukokuussa, kun rikoslain 38 luvun 10 §:n sanamuotoa hieman muutettiin. Kerron edellä mainituista lakimuutoksista enemmän tuonnempana.

[82] Pihlajamäki 1995, s. 685.
[83] Saarenpää 2011, s. 537.

Tällä hetkellä rikoslain 38 luku (578/1995) tieto- ja viestintärikoksista käsittää seuraavaa:

1 § Salassapitorikos (578/1995)

2 § Salassapitorikkomus (578/1995)

3 § Viestintäsalaisuuden loukkaus (531/2000)

4 § Törkeä viestintäsalaisuuden loukkaus (578/1995)

5 § Tietoliikenteen häirintä (578/1995)

6 § Törkeä tietoliikenteen häirintä (578/1995)

7 § Lievä tietoliikenteen häirintä (578/1995)

7 a § Tietojärjestelmän häirintä (540/2007)

7 b § Törkeä tietojärjestelmän häirintä (540/2007)

8 § Tietomurto (578/1995)

8 a § Törkeä tietomurto (540/2007)

8 b § Suojauksen purkujärjestelmärikos (1118/2001), (ennen 8 a §)

9 § Henkilörekisteririkos (525/1999)

10 § Syyteoikeus (441/2011)

11 § Menettämisseuraamus (1118/2001)

12 § Oikeushenkilön rangaistusvastuu (540/2007)

Ruotsin rikoslaissa, brottsbalkenissa (1962:700), ei ole vastaavaa lukua tieto- ja viestintärikoksista. Tietotekniikkaan liittyviä rikoksia on toki kriminalisoitu, mutta ne on sijoitettu muiden kokonaisuuksien joukkoon.

Tietotekniikkarikosten määrästä on vaikeaa saada selvitystä, koska niitä ei ole tilastoitu erikseen. Rikosten nimellä voi hakea kappalemääriä, mutta kun kyseessä on tieto- ja viestintärikokset, ongelmaksi muotoutuu se, että rikosmääriä voidaan etsiä vain rikoslain 38 luvusta. Jos kyseessä on esimerkiksi petos, joka täyttää tieto- tai viestintärikok-

sen tunnusmerkit, ei määriä pystytä laskemaan, koska loppusummaksi tulisi kaikki petokset. Mutta rikoslain 38 luvun osalta määrien tarkkailu onnistuu.

Tietotekniikkarikollisuus on tyypillisesti piilorikollisuutta, sillä asianomistajat ovat yleensä varsin haluttomia ilmoittamaan rikoksia poliisille.[84] *Laguksen* mukaan syynä voi olla esimerkiksi pelko siitä, että ei haluta muiden tietävän, että yrityksellä on ongelmia tietoturvallisuuden kanssa. Lisäksi yrityksissä saatetaan olla sitä mieltä, että vaikka rötöstelijä saataisiin kiinni, vahinkoa ei kuitenkaan saada korjattua.[85] Lisäksi voi olla tapauksia, joissa henkilö ei edes tiedä tulleensa rikoksen uhriksi.[86]

Tieto- ja viestintärikosten määriä voidaan tutkia rikoslain 38 luvun osalta. Alla olevasta taulukosta ilmenee poliisille ilmoitetut rikoslain 38 luvun rikosmääriä vuodesta 2004 vuoteen 2010.

Taulukko 1. Poliisin tietoon tulleet tieto- ja viestintärikokset vuosilta 2004-2010[87]

	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**

Lähde Poliisin tulostietojärjestelmä

Mielenkiintoista on huomata, että rikosmäärät ovat nousseet tasaisesti. Vuodesta 2004 vuoteen 2010 rikosmäärät ovat kaksinkertaistuneet. Tämä jos mikä osoittaa sen, että yhteiskunnan rikollisuus on siirtynyt ja siirtyy koko ajan enemmän verkkomaailmaan. Ylivoimaisesti eniten rikosilmoituksia on tehty viestintäsalaisuuksien loukkauksista ja tietomurroista, mutta muutkin rikosilmoitukset ovat yleistyneet.

[84] Pihlajamäki 1995, s. 685-686.
[85] Lagus 2008, s. 23.
[86] Lehto 2011
[87] Poliisin tulostietojärjestelmässä olevat lukumäärät rikoksista muuttuvat sitä mukaan, kun uusia rikosilmoituksia tehdään. Merkitystä on aina siitä milloin mahdollinen rikos on tehty eli jos rikosilmoituksen kohteena olevan rikoksen tekoaika on vuodelta 2010, tulee se ilmi sen vuoden tilastoihin, ei rikosilmoituksen tekovuoteen. Tilastot päivitetään tietyn väliajoin ja tällä hetkellä muutoksia voi tulla vielä vuoden 2010 tietoihin. Aikaisemmat vuodet eivät muutu. Käsittelemäni tilasto on päivitetty 5.7.2011.

Suurin harppaus on tapahtunut 2009 - 2010, kun rikosilmoitusten määrät ovat nousseet 198 kappaleella. Tietomurtojen osuus on kasvanut myös huimasti samaan aikaan. Mutta tieto- ja viestintärikosten rikosilmoitusten määrä ei näy itse tuomioiden määrissä. Niitä kun annetaan vieläkin harvoin.

Taulukko 2. Rangaistukset rikoksittain vuosilta 2005 - 2009 (käräjäoikeudet ja hovioikeus ensimmäisenä oikeusasteena)[88]

	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
Tietojärjestelmän häirintä	0	0	1	0	0
Tietomurto	0	1	1	4	4
Tietomurron yritys	5	0	1	0	0
Henkilörekisteririkos	6	8	12	4	5
Yhteensä	**39**	**27**	**24**	**21**	**22**

Kuten yllä olevasta taulukosta käy ilmi, lukumäärät eivät vastaa lainkaan rikosilmoitusten määriä. Tilastokeskuksen taulukot eivät ole aivan käyttökelpoisia, koska henkilö esitetään tilastossa yhtä monta kertaa kuin hänestä on tehty ratkaisuja. Yhteen ratkaisuun voi sisältyä monta eri rikosnimikettä. Lisäksi tilastossa sovellettava esitystapa on niin sanottu päärikos-sääntö. Päärikos-säännön mukaan kutakin syytettyä tai tuomittua kuvataan ratkaisun ankarimman rangaistuslajin törkeimmällä rikoksella.[89] Jos henkilö on tehnyt myös muitakin rikoksia, tulee syytetystä tai tuomiosta siis vain yksi merkintä törkeimmän rikoksen kohdalle. Usein rikoslain 38 luvun säännöksissä rangaistuslaji ei kilpaile muiden rikosten rangaistuslajien kanssa, koska rangaistusasteikot ovat matalat.

Taulukon 2 mukaan rangaistusten lukumäärät eivät ole muuttuneet radikaalisti viiden vuoden aikana. Vaikka rikosilmoitusten määrät ovat kasvaneet, mutta rangaistusten lukumäärät eivät, niin tämä on osoitus siitä, että rikollisuuden täytyy olla koko ajan vakavampaa. Tilastoon tulisi muutoksia, jos rikoksen tekijä tekisi vain yhden rikoksen tai että vakavin rikos kuuluisi rikoslain 38 luvun piiriin.

[88] Suomen virallinen tilasto (SVT): Syytetyt, tuomitut ja rangaistukset [verkkojulkaisu]. ISSN=1798-6680. Helsinki: Tilastokeskus [viitattu: 26.7.2011].
Saantitapa: http://tilastokeskus.fi/meta/til/syyttr.html
[89] http://tilastokeskus.fi/meta/til/syyttr.html. Viitattu 26.7.2011

Tieto- ja viestintärikoksissa tuomitaan usein sakkoihin. Tuomioistuinten linja onkin ollut tieto- ja viestintärikoksissa toistaiseksi lempeä. Esimerkiksi, jotta henkilörekisteririkoksesta tuomittaisiin vankeutta, pitäisi rikoksen olla todella törkeä. Myös uhreille maksetut korvaukset henkisestä kärsimyksestä ovat olleet kansainvälisesti katsottuna alhaisia.[90] Syyttämättä jättäminen voi antaa signaalin, ettei yksityisyyden loukkaaminen ole oikeusjärjestelmän silmissä vakava asia. Eräissä tieto- ja viestintärikoksissa syytteestä on luovuttu, vaikka tietosuojavaltuutettu onkin lausunnossaan katsonut syyttämisen olevan perusteltu.[91]

Tuomioistuinten lempeä linja näkyy myös tilastokeskusten tilastoissa tutkittaessa keskimääräisiä rangaistuksia. Tietomurtojen osalta vuonna 2009 oikeudessa tuomittuja oli neljä kappaletta. Kaikki tuomiot johtivat sakkorangaistukseen, jossa keskimääräinen rangaistus oli 21,3 päiväsakkoa. Toinen rikoslaji, josta tehdään paljon rikosilmoituksia, on viestintäsalaisuuden loukkaus. Vuonna 2009 oikeudessa tuomittuja oli kahdeksan kappaletta. Yksi tapaus jätettiin tuomitsematta, syyte hylättiin yhdessä ja kahdessa tapauksessa asia raukesi. Sakkorangaistukseen tuomittiin neljä henkilöä. Keskimääräinen rangaistus oli 26,9 päiväsakkoa.[92]

Korkeimmat sakkorangaistukset tuomitaan henkilörekisteririkoksen kohdalla. Vuonna 2009 keskimääräinen sakkorangaistus oli 31 päiväsakkoa, edellisenä vuonna luku oli 35 päiväsakkoa.[93] Mutta kokonaisuutena ajatellen sakkomäärät ovat todella pieniä. Jos syytetyn tulot eivät ole kovinkaan suuret, niin sakkomäärät eivät nouse korkeiksi. Enemmän merkitystä on varmasti vahingonkorvaussummalla, joka voi nousta suureksikin.

[90] Castrén 2009, s. 29.
[91] Castrén 2009, s. 30.
[92] Suomen virallinen tilasto (SVT): Syytetyt, tuomitut ja rangaistukset [verkkojulkaisu]. ISSN=1798-6680. Helsinki: Tilastokeskus [viitattu: 26.7.2011]. Saantitapa: http://tilastokeskus.fi/meta/til/syyttr.html
[93] Suomen virallinen tilasto (SVT): Syytetyt, tuomitut ja rangaistukset [verkkojulkaisu]. ISSN=1798-6680. Helsinki: Tilastokeskus [viitattu: 26.7.2011]. Saantitapa: http://tilastokeskus.fi/meta/til/syyttr.html

4.2 Rikoslajit

4.2.1 Salassapitorikokset

Oikeuskielessä kuvataan tiettyyn asiaan kohdistuvaa ilmaisukieltoa käsitteillä salassapito- ja vaitiolovelvollisuus. Käsitteiden sisältö ja keskinäinen suhde eivät aina ole täysin selviä. Salassapitovelvollisuus liittyy asiakirjoihin sisältyvien salassa pidettäviin asioihin ja usein salassapitovelvollisuudesta puhutaan vain siinä merkityksessä, ettei viranomaisen hallussa olevaa asiakirjaa saa näyttää eikä siitä antaa jäljennöksiä ulkopuolisille. Kyse on niin sanotusta asiakirjasalaisuudesta.[94]

Viranomaisen julkisuudesta annetun lain (21.5.1999/621) 6 luvun 22§:n mukaan viranomaisen asiakirja on pidettävä salassa, jos se on lailla säädetty salassa pidettäväksi tai jos viranomainen on lain nojalla määrännyt sen salassa pidettäväksi tai jos se sisältää sellaisia tietoja, joista on lailla säädetty vaitiolovelvollisuus. Salassa pidettävää viranomaisen asiakirjaa ei saa näyttää eikä luovuttaa sivulliselle ilman julkisuuslaissa mainittuja poikkeuksia.

Asiakirjasalaisuutta laajempi käsite on vaitiolovelvollisuus, joka koskee erityisesti virkamiehiä. Vaitiolovelvollisuus tarkoittaa sitä, että virkamies ei saa luvatta ilmaista jotakin seikkaa. Vaitiolovelvollisuudesta on säädetty virkamieslaissa ja laissa, joiden säännökset oikeuttavat viranomaisia saamaan kansalaisten yksityisyyden tai yhteisöjen taloudellisen toiminnan kannalta herkkiä tietoja.[95]

Salassapitovelvollisuutta ja vaitiolovelvollisuutta ei kuitenkaan voida Suomen lainsäädännössä erottaa toisistaan. Samassa säännöksestä saattaa seurata velvollisuus pitää asiakirja salassa sekä vaieta muistakin asiaan liittyvistä seikoista. Salassapitovelvollisuutta käytetään myös eräänlaisena yläkäsitteenä, johon kuuluu sekä asiakirjasalaisuuden säilyttämisvelvollisuus, että muuta salaisuutta koskeva vaitiolovelvollisuus.[96]

Salassapitorikos on säännelty rikoslain 38 luvun 1§:ssä ja sen mukaan

[94] HE 94/1993 vp. s. 146.
[95] Rautio 1999, s. 908-909.
[96] HE 94/1993 vp. s. 146.

> *Joka laissa tai asetuksessa säädetyn taikka viranomaisen lain nojalla erikseen määrää-män salassapitovelvollisuuden vastaisesti*
> *1) paljastaa salassa pidettävän seikan, josta hän on asemassaan, toimessaan tai tehtävää suorittaessaan saanut tiedon, taikka*
> *2) käyttää tällaista salaisuutta omaksi tai toisen hyödyksi,*
> *on tuomittava, jollei teko ole rangaistava 40 luvun 5 §:n mukaan, salassapitorikoksesta sakkoon tai vankeuteen enintään yhdeksi vuodeksi.*

Pykälä ei ole puuttunut salassapitovelvollisuuden laajuuteen, myös salassapitovelvollisuuden sisältö on jätetty kokonaan muusta lainsäädännöstä riippuvaiseksi[97]. Vaikka pykälässä ei ole sitä nimenomaan todettu, tekijältä edellytetään subjektiivisessa suhteessa tahallisuutta. Salassapitovelvollisuus on esimerkiksi voitu ulottaa asioihin, jotka asian laadun vuoksi on pidettävä salassa. Rangaistussäännöksen soveltaminen tällöin edellyttää, että tekijä on tiennyt menettelevänsä häntä sitovan velvollisuuden vastaisesti.[98]

Salassapitorikokset kuuluvat yksityisyyttä suojaaviin säännöksiin. Rikoslaissa ei säädetä itse salassapitovelvollisuudesta vaan ainoastaan sen rikkomiseen liittyvästä rangaistusuhasta.[99] Rikoslain salassapitorikossäännöksiä (rikoslain 38 luvun 1 ja 2 §:t) sovelletaan salassapitovelvollisuuden rikkomiseen, kun tekijänä on muu kuin virkamies tai julkisyhteisön työntekijä. Virkasalaisuuden rikkomisesta on omat säännöksensä rikoslain 40 luvun 5 §:ssä. Asia ilmenee pykälään sisältyvästä toissijaisuuslausekkeesta. Hallituksen esityksen mukaan pykälä syrjäytyy lisäksi useimmiten myös niissä tapauksissa, joissa salassapitovelvollisuuden rikkominen on jonkin vakavamman rikoksen osa. Tällaisia rikoksia voisivat olla esimerkiksi yrityssalaisuuden tai valtiosalaisuuden rangaistava paljastaminen.[100]

Säännöksessä ei esitetä tekijäpiiriä koskevaa esimerkkiluetteloa, vaan salassapitovelvollisten henkilöiden määrittely on jätetty erityislainsäädännön varaan. Rikoksen tekijäpiiri on hyvin vaihteleva, mikä johtuu siitä, että eri asemassa olevat henkilöt voivat olla salassapitovelvollisia tai tulla salassapitovelvollisiksi monilla erilaisilla perusteilla. Tekijäpiiri käsittää muun muassa lääkärit, asianajajat, heidän ammat-

[97] Säännös on niin sanottu epätäydellinen rikossäännös, jossa on yksilöity salassapitorikoksen tekotavat, mutta salassapitovelvollisuuden aineellinen sisältö on jätetty muussa lainsäädännössä määriteltäväksi.
[98] HE 94/1993 vp. s. 146.
[99] Rautio 2010, s. 1030.
[100] HE 94/1993 vp. s. 147.

tiapulaisensa, mutta myös erilaisten lakisääteisten tehtävien suorittajat, asiamiehet, asiantuntijat ja luottamushenkilöt.[101]

Salassapitorikoksessa on kaksi eri tekotapaa rikoslain 38 luvun 1 §:n 1 momentin 1-2 kohdan mukaan. Rangaistavaa on sekä salaisuuden paljastaminen, että sen käyttäminen omaksi tai toisen hyödyksi. Kysymys on niin sanotusta yksityisestä hyödystä. Seikan tulee olla sellainen, josta salassapitovelvollinen henkilö on toimessaan, asemassaan tai tehtävässään saanut tiedon. Säännöksen yksityiskohtaisempi sisältö ilmenee aina asianomaisen salassapitovelvollisuuden asettavasta säädöksestä tai viranomaisen lain nojalla antamasta määräyksestä. Paljastamisella tarkoitetaan salassa pidettävien seikkojen ilmaisemista joko suullisesti tai kirjallisesti.

Salassapitovelvollisuuden rikkomisen moitittavuus voi suuresti vaihdella esimerkiksi lääkärin ja maatalousyrittäjän vuosilomittajan vastuuta ja tehtäviä vertailtaessa. Salassapitorikoksen arvostelussa onkin kiinnitettävä huomiota siihen, että millainen vastuu tietyssä tehtävässä olevalta voidaan edellyttää, mutta myös siihen, kuinka merkittävästä salattavasta seikasta on kysymys. Erot on otettava huomioon sekä rangaistuslajia valittaessa että rangaistusta mitattaessa.[102]

Koska salassapitovelvollisuuden rikkomiset ovat paheksuttavuudeltaan hyvinkin erilaisia, on ollut tarkoituksenmukaista ottaa rikoslakiin myös lievempää tekomuotoa koskeva säännös. Salassapitorikkomus rikoslain 38 luvun 2 §:n mukaan

> *Jos salassapitorikos, huomioon ottaen teon merkitys yksityisyyden tai luottamuksellisuuden suojan kannalta taikka muut rikokseen liittyvät seikat, on kokonaisuutena arvostellen vähäinen, rikoksentekijä on tuomittava salassapitorikkomuksesta sakkoon.*
>
> *Salassapitorikkomuksesta tuomitaan myös se, joka on syyllistynyt sellaiseen 1 §:ssä tarkoitettuun salassapitovelvollisuuden rikkomiseen, joka on erikseen säädetty salassapitorikkomuksena rangaistavaksi.*

Salassapitorikkomuksen perusteena on teon merkitys yksityisyyden tai luottamuksen suojan kannalta. Myös muut rikokseen liittyvät seikat saattavat johtaa salassapitorikoksen lievempää tekomuotoa koskevan säännöksen soveltamiseen. Pykälän 2. momentti

[101] HE 94/1993 vp. s. 147.
[102] HE 94/1993 vp. s. 147.

tarkoittaa tapauksia, joissa 1 §:ssä tarkoitettu salassapitovelvollisuuden sisältävässä säädöksessä nimenomaan on säädetty vain salassapitorikkomuksensa rangaistavaksi.

Salassapitovelvollisuus väistyy eräissä tapauksissa muualla laissa säädetyn ilmaisuvelvollisuuden johdosta. Esimerkiksi oikeudenkäymiskaaren 17 luvun 23 §:n 3 momentissa on säännös siitä, milloin todistajana oikeudessa kuultava henkilö on velvollinen kertomaan muuten salassa pidettävän tiedon. Tämä ei koske kumminkaan syytetyn oikeudenkäyntiavustajaa.

Korkeimman oikeuden ratkaisussa (KKO 2006:61) kysymys oli siitä, oliko asianajaja ilmaissut päämieheltään saamiaan asianajosalaisuuteen liittyviä tietoja luvattomasti poliisin esitutkinnan aikana. Asianajaja ei ollut rikoksesta epäillyn asemassa, mutta hän puolustautui päämiehensä menettelyn johdosta häneen mahdollisesti kohdistuvaa rikosepäilyä vastaan. [103]

Toisin kuin käräjäoikeus, hovi- ja korkein oikeus katsoivat, että asianajaja ei ole syyllistynyt salassapitorikokseen. Korkein oikeus katsoi, että tällaisessa tilanteessa tietojen ilmaiseminen ei ollut tapahtunut luvattomasti. Salassa pidettävien seikkojen esilletuominen oli ollut hyväksyttävää, koska asianajajan oli pitänyt puolustautua mahdollisesti kohdistuvaa rikosepäilyä vastaan. Käräjäoikeuden mielestä asianajaja oli syyllistynyt salassapitorikokseen, koska hän ei ollut rikoksesta epäillyn asemassa.[104]

Ratkaisullaan korkein oikeus vahvisti oikeustieteessä esitetyn kannan siitä, että asianajosalaisuus voi väistyä tilanteessa, jossa asianajajan on välttämätöntä vedota asianajosalaisuuden alaiseen tietoon, jotta hän voi vapautua omaa oikeudellista asemaansa vaarantavasta tilanteesta. Käytännössä merkittävä viesti ratkaisussa *Timosen* mukaan on se, ettei asianajajan välttämättä tarvitse olla rikoksesta epäillyn (tai syytetyn) asemassa voidakseen vapautua asianajosalaisuudesta. Se, miten laajalti asianajaja voi asianajosalaisuudesta poiketa, ratkaistaan tapauskohtaisesti. Tässä tilanteessa otetaan huomioon muun muassa entisen päämiehen asianajajaa syyllistävien väitteiden vakavuus ja laatu.[105]

[103] KKO 2006:61
[104] KKO 2006:61
[105] Timonen 2007, s. 41.

Esimerkki salassapitorikoksen syrjäytymisestä vakavamman rikoksen osana on Korkeimman oikeuden ratkaisu (KKO 2009:3). A oli tuomittu rangaistukseen seksuaalirikosasiassa, johon liittyvä oikeudenkäyntiaineisto oli lainkohtia ja tuomiolauselmaa lukuun ottamatta määrätty salassa pidettäväksi. Myöhemmin A oli ollut toimittaja B:n haastateltavana television ajankohtaisohjelmassa huoltoriitoihin liittyvistä insestiväitteistä. Ajankohtaisohjelmassa A syyllistyi sekä yksityiselämää loukkaavan tiedon levittämiseen sekä salassapitorikokseen. Korkeimman oikeuden ratkaisun mukaan menettely tulee tässä tapauksessa rikosoikeudellisesti riittävästi arvioiduksi pelkästään yksityiselämää loukkaavaa tiedon levittämistä koskevan, salassapitorikosta ankaramman seuraamuksen mahdollistavan rangaistussäännöksen perusteella. Tämän vuoksi vastaajia ei sen lisäksi tuomittu rangaistukseen salassapitorikoksesta tai siihen osallisuudesta.[106]

4.2.2 Viestintärikokset

4.2.2.1 Viestintäsalaisuuden loukkaus

Perustuslain 10 § turvaa yksityiselämän suojan. Kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton. Kirjesalaisuus on tekniikan kehittyessä muuttunut käsittämään yleisen viestintäsalaisuuden, joka ei tee eroa viestinnän toteutustapojen välillä. Viestintäsalaisuus turvaa niin puheluiden, tekstiviestien kuin sähköpostienkin luottamuksellisuuden.[107]

Sähköiseen viestintään sovelletaan sähköisen viestinnän tietosuojalain säännöksiä. Sähköisen viestinnän tietosuojalain 2 §:n 1 kohdan mukaan viestillä tarkoitetaan viestintäverkossa osapuolten välillä valikoituville vastaanottajille välitettävää sähköpostia, puhelua, puheviestiä, tekstiviestiä ja muuta vastaavaa sanomaa. Sähköinen viestintä tapahtuu käytännössä aina jonkin laitteen tai laitteiden välityksellä.

Viestintäverkolla tarkoitetaan SVTSL 2 §:n 2 kohdan mukaan toisiinsa liitetyistä johtimista ja laitteista muodostuvaa järjestelmää, joka on tarkoitettu viestien siirtoon tai jakeluun johtimella, radioaalloilla, optisesti tai muulla sähkömagneettisella tavalla.

[106] KKO 2009:3
[107] Järvinen 2003, s. 250

Perustuslain luottamuksellisen viestinnän suojalla on tarkoitus turvata yleisesti luottamuksellisen viestin salaisuutta. Jokaisella on oikeus luottamukselliseen viestintään ilman, että ulkopuoliset saavat oikeudettomasti tiedon hänelle osoitettujen tai hänen lähettämiensä viestien sisällöstä. Luottamuksellisen viestinnän ydinalueena on suojata luottamukselliseksi tarkoitetun viestin sisältö ulkopuolisilta. Lisäksi luottamuksellisen viestinnän turvaava perusoikeus antaa suojaa myös sellaisille viestiä koskeville tiedoille, joilla voi olla merkitystä viestin säilymiselle luottamuksellisena. Sähköisessä viestinnässä tällaisilla tiedoilla on tarkoitettu tunnistamistietoja.[108] SVTSL 2 §:n 8 kohdan mukaan tunnistamistiedolla tarkoitetaan tilaajaan tai käyttäjään yhdistettävissä olevaa tietoa, jota viestintäverkoissa käsitellään viestien siirtämiseksi, jakelemiseksi tai tarjolla pitämiseksi.

Sähköisen viestinnän tietosuojalain rangaistussäännökset ovat rikoslain 38 luvussa. Rikoslain 38 luvun 3 §:n mukaan

> *Joka oikeudettomasti*
>
> *1) avaa toiselle osoitetun kirjeen tai muun suljetun viestin taikka suojauksen murtaen hankkii tiedon sähköisesti tai muulla vastaavalla teknisellä keinolla tallennetusta, ulkopuoliselta suojatusta viestistä taikka*
>
> *2) hankkii tiedon televerkossa välitettävänä olevan puhelun, sähkeen, tekstin-, kuvan- tai datasiirron taikka muun vastaavan televiestin sisällöstä taikka tällaisen viestin lähettämisestä tai vastaanottamisesta,*
>
> *on tuomittava viestintäsalaisuuden loukkauksesta sakkoon tai vankeuteen enintään yhdeksi vuodeksi.*
>
> *Yritys on rangaistava.*

Viestintäsalaisuuden loukkauksen tunnusmerkistö jakaantuu nykyään kahteen osaan rikoslain 38 luvun 3 §:n 1 momentin 1-2 kohdan mukaan. Ensimmäinen käsittää kirjesalaisuuden loukkaamisen täydennettynä sähköisesti tallennettua viestiä koskevalla lisäyksellä. Toinen osa käsittää puhelin-, lennätin- tai muun telesalaisuuden loukkaamisen. Ennen lakimuutosta viestintäsalaisuuden loukkaus käsitti myös salakuuntelun[109.] Mutta nykyään salakuuntelu on säännelty rikoslain 24 luvun 5§:ssä. Ruotsissa viestin-

[108] Innanen, Saarimäki 2009, s. 28.
[109] HE 94/1993 vp. s. 148.

täsalaisuuden loukkaus ja salakuuntelu on kriminalisoitu brottsbalkenin (SFS 1962:700) 4. luvun (Om brott mot frihet och frid) 8, 9 ja 9 a §:issä.

Kirjesalaisuudella tarkoitetaan viestin lähettämistä, kun lähetys on suljettu ja sisältää vastaanottajalle tarkoitetun viestin. Vaikka säännöksessä mainitaankin esimerkkinä kirje, ei sen tarvitse olla kuitenkaan kirjallisessa muodossa. Myös suljettu atk-tallenteita sisältävä paketti tulee kyseeseen. Kirjesalaisuus koskee lisäksi sähköisesti tai muulla tavalla sanottua elektronista postia eli tietokoneesta toiseen välitettyjä viestejä, jotka ovat vain tietyn käyttäjän tai käyttäjien luettavaksi tarkoitettuja.[110]

Rikoslain 38 luvun 3 §:n 2 kohdan rangaistussäännös ei sovellu tilanteisiin, jos puhelinkeskusteluun osallistuja tallentaa sen nauhalle. Silloinhan tietoa ei ole hankittu oikeudettomasti. Eräillä työpaikoilla saattaa esiintyä tilanteita, joissa nauhoitetaan työntekijöiden soittamia puheluita asiakkaille. Mutta tähän tarvitaan työntekijän suostumus. Nauhoituksella halutaan varmistaa toimeksiantoja sekä turvata myyntityötä.[111]

Verkko- ja viestintäpalvelun tarjoamista kutsutaan teletoiminnaksi. Teletoimintaa on sekä yleistä että erityistä. Viestintämarkkinalain (23.5.2003/393) 2 luvun 4 §:n 1 kohdan yleinen teletoiminta on viestintäviraston toimiluvan vaativaa toimintaa, jossa televerkon käyttäjien piiriä ei ole rajoitettu. Yleistä teletoimintaa harjoittavat teleyritykset. Niitä voivat olla esimerkiksi sähköpostipalvelun tarjoajat sekä viranomaisverkoissa toimintaa harjoittavat tahot[112].

Yrityksen tai yhteisön omaa tarvetta varten toteuttamat viestintäverkot ja viestien välityspalvelut voidaan katsoa etukäteen rajatulle käyttäjäpiirille tarjotuiksi. Erityistä teletoimintaa harjoittavat esimerkiksi yrityksen työntekijöilleen ja koulun opiskelijoilleen tarjoamat palvelut verkon laajuudesta tai käyttäjämäärän suuruudesta riippumatta. Myös luonnollisen henkilön itselleen ja lähipiirilleen toteuttamia palveluita voidaan pitää erityisenä teletoimintana.[113]

Rikoslain 38 luvun 3 § koskee niin yleistä kuin erityistä teletoimintaa. Se suojaa televiestiä nimenomaan silloin, kun se on televerkossa välitettävänä, ellei siitä ole lailla säädetty poikkeusta. Esimerkiksi tutkintavankeudesta annetun lain (23.9.2005/768) 8

[110] HE 94/1993 vp. s. 148-149.
[111] HE 94/1993 vp. s. 151-152, Rautio 2009, s. 1037.
[112] Innanen, Saarimäki 2009, s. 59-60.
[113] Innanen, Saarimäki 2009, s. 176.

luvussa säädetään oikeudesta tutkintavankeudessa olevan vangin puhelujen kuuntelemiseen.[114]

Rikoslain 38 luvun 4 §:n mukaan viestintäsalaisuuden loukkaus on törkeä, jos:

> *Jos viestintäsalaisuuden loukkauksessa*
>
> *1) rikoksentekijä käyttää rikoksen tekemisessä hyväksi asemaansa sähköisen viestinnän tietosuojalaissa (516/2004) tarkoitetun teleyrityksen palveluksessa tai muuta erityistä luottamusasemaansa, (16.6.2004/517)*
>
> *2) rikoksentekijä käyttää rikoksen tekemistä varten suunniteltua tai muunnettua tietojenkäsittelyohjelmaa tai teknistä erikoislaitetta tai rikos muuten tehdään erityisen suunnitelmallisesti taikka*
>
> *3) rikoksen kohteena oleva viesti on sisällöltään erityisen luottamuksellinen taikka teko huomattavasti loukkaa yksityisyyden suojaa*
>
> *ja viestintäsalaisuuden loukkaus on myös kokonaisuutena arvostellen törkeä, rikoksentekijä on tuomittava törkeästä viestintäsalaisuuden loukkauksesta vankeuteen enintään kolmeksi vuodeksi.*
>
> *Yritys on rangaistava.*

Ensimmäinen ankaroittamisperuste (RL 38 luvun 4 §:n 1 momentin 1 kohta) perustuu siihen, että rikoksentekijä käyttää rikosta tehdessään hyväksi erityistä asemaansa. Tämä koskee niitä henkilöitä, jotka ovat yleistä teletoimintaa harjoittavan laitoksen palveluksessa. Myös muun erityisen luottamusaseman hyväksikäyttäminen voi johtaa tämän ankaroittamisperusteen soveltamiseen. Luottamusasemalla tarkoitetaan esimerkiksi henkilöä, joka hoitaa yksityisen televerkon käyttötehtäviä tai huolehtii sen kunnossapidosta.

Toisella ankaroittamisperusteella (RL 38 luvun 4 §:n 1 momentin 2 kohta) tarkoitetaan sitä, että rikos tehdään erityisen suunnitelmallisesti tai rikoksentekijä käyttää rikoksen tekemistä varten suunniteltua tai muunnettua tietojenkäsittelyohjelmaa tai teknistä erikoislaitetta.

[114] HE 94/1993 vp. s. 151.

Kolmas ankaroittamisperuste (RL 38 luvun 4 §:n 1 momentin 3 kohta) koskee rikoksen kohteena olleen teon yksityisyyttä loukkaavaa vaikutusta tai teon sisältöä. Jos viesti on luonteeltaan erityisen luottamuksellinen ja rikoksentekijä on tiennyt sen tai teko loukkaa huomattavasti yksityisyyden suojaa, niin tällöin voidaan soveltaa ankarampaa rangaistusasteikkoa, mikäli teon kokonaisarvostelu sitä edellyttää.

Rikoslain 38 luvun 3 ja 4 §:n soveltaminen voi tulla kysymykseen sekä silloin, kun niissä tarkoitetun teon kohteensa on luottamuksellinen viesti, että silloin, kun teko kohdistuu luottamukselliseen viestiin liittyvään tunnistamistietoon.[115] Tunnistamistiedolla tarkoitetaan SVTSL 2 §:n 8 kohdan mukaan tilaajaan tai käyttäjään yhdistettävissä olevaa tietoa, jota viestintäverkoissa käsitellään viestien siirtämiseksi, jakelemiseksi tai tarjolla pitämiseksi.

Erityisen luottamuksellista viestintää pyritään suojaamaan erilaisilla turvakeinoilla kuten salaamisjärjestelmillä tai käyttämällä erikoiskuriireja. Mutta tällä ei ole merkitystä lähdettäessä miettimään rangaistusasteikkoa. Ratkaisevaa kuitenkin on vain viestin tosiasiallinen sisältö, ei sen viestin ulkoisen suojauksen aste. Esimerkiksi ei ole välttämätöntä, että kirje on salaiseksi merkitty, vaan merkitystä on sillä, tiesikö rikoksentekijä rikokseen ryhtyessään sen sisältävän salaisuuksia, joita kirjeen lähettäjä on halunnut erityisesti suojella ulkopuolisilta. Tällaiset salaisuudet voivat olla niin ammattiin liittyviä kuin henkilökohtaisia.[116]

4.2.2.2 Tietoliikenteen häirintä

Rikoslain 38 luvun 5 §:ssä sääntelee tietoliikenteen häirinnästä. Sen mukaan:

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

[115] Helopuro, Perttula, Ristola 2009, s. 42.
[116] HE 94/1993 vp. s. 153.

Sääntö koskee postiliikennettä sekä tele- ja radioviestintää. Radiolaajuuksista ja telelaitteista annetun lain (16.11.2001/1015) 4 §:n 2 kohdan mukaan radioviestinnällä tarkoitetaan kaikkea radioaaltoja hyväksikäyttäen tapahtuvaa kirjoituksen, merkin, merkinannon, kuvan, äänen tai muussa muodossa olevan tiedon siirtoa, vastaanottoa tai lähettämistä. Säännöksen soveltamisalaa ei ole rajattu viestinnän sisällön perusteella, joten se soveltuu myös radioviestinnässä välitettävän elokuvan tai musiikkiohjelman lähettämisen häiritsemiseen.[117]

Tietoliikenteen häirintä voi tapahtua joko tietoliikenteessä käytetyn laitteen toimintaan fyysisesti puuttumalla tai sanomien lähettämistä tai vastaanottamista vaikeuttamalla. Säännöksessä ei ole mainittu tyhjentävästi tietoliikennettä häiritseviä tai estäviä tekotapoja, joten mahdollista on, että rikos tehdään myös muulla vastaavalla tavalla. Tekotavan ei välttämättä tarvitse olla teknisin keinoin toteutettu, vaan esimerkiksi tietoliikennettä hoitavan laitoksen virkailijan toiminnan estäminen voi olla vastaavaa tietoliikenteen häirintää. Teon pitää olla kuitenkin oikeudetonta. Tietoliikenteen häirintä on rangaistavaa vain tahallisena. Rikoksentekijän tulee tietää, että hän toiminnallaan estää tai häiritsee postiliikennettä tai tele- tai radioviestintää.[118]

Tietoliikenteen häirintä on törkeä, jos kyseessä on tietoliikenteen häirintä ja lisäksi jokin alla oleva ankaroittamisperuste täyttyy. Lisäksi teon on oltava kokonaisuutta arvostelleen törkeä. Rikoslain 38 luvun 6 §:n mukaan

> *Jos tietoliikenteen häirinnässä*
>
> *1) rikoksentekijä käyttää rikoksen tekemisessä hyväksi asemaansa teletoimintalaissa tarkoitetun yleistä teletoimintaa, kaapelilähetystoiminnasta annetun lain (307/87) mukaista kaapelilähetystoimintaa tai yleisradiotoimintaa harjoittavan laitoksen palveluksessa tai muuta erityistä luottamusasemaansa taikka*
>
> *2) rikoksella estetään tai häiritään hätäkutsujen radioviestintää tai muuta sellaista tele- tai radioviestintää, jota harjoitetaan ihmishengen turvaamiseksi,*
>
> *ja tietoliikenteen häirintä on myös kokonaisuutena arvostellen törkeä, rikoksentekijä on tuomittava törkeästä tietoliikenteen häirinnästä vankeuteen vähintään neljäksi kuukaudeksi ja enintään neljäksi vuodeksi.*

[117] HE 94/1993 vp. s. 153.
[118] HE 94/1993 vp. s. 153-154.

Yritys on rangaistava.

Ankaroittamisperusteita on kaksi rikoslain 38 luvun 6 §:n 1 momentin 1 - 2 kohdan mukaan. Ensimmäisellä ankaroittamisperusteella tarkoitetaan sitä, että rikoksentekijä käyttää hyväkseen asemaansa yleistä teletoimintaa tai yleisradiotoimintaa harjoittavan laitoksen palveluksessa. Toisella ankaroittamisperusteella tarkoitetaan sitä, että rikoksella estetään tai häiritään hätäkutsujen radioviestintää tai muuta sellaista tele- tai radioviestintää, jota harjoitetaan ihmishengen turvaamiseksi.

Tietoliikenteen häirintä voi vakavimmillaan aiheuttaa vakavaa vaaraa yhteiskunnan tärkeille toiminnoille, kuten yleiselle terveydenhuollolle, energiahuollolle tai maanpuolustukselle. Näissä tapauksissa voidaan soveltaa myös rikoslain 34 luvun 1 §:n 2 momentin mukaista säännöstä tuhotyöstä.[119]

Tietoliikenteen häirintä voi olla myös tilapäistä ja melko harmitonta. Tämän vuoksi on säädetty myös lakiin lieviä tekomuotoja tarkoittava säännös, jonka nojalla voidaan tuomita vain sakkoa. Rikoslain 7 §:n mukaan jos tietoliikenteen häirintä, huomioon ottaen aiheutetun häiriön laatu tai määrä taikka muut rikokseen liittyvät seikat, on kokonaisuutena arvostellen vähäinen, rikoksentekijä on tuomittava lievästä tietoliikenteen häirinnästä sakkoon. Yritys on rangaistava.

4.2.2.3 Tietojärjestelmän häirintä

Tietojärjestelmän häirintä kriminalisoitiin vuonna 2007 samalla, kun Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus eli niin sanottu tietoverkkorikossopimus saatettiin voimaan. Samalla lainsäädäntö saatettiin vastaamaan Euroopan Unionin tietojärjestelmiin kohdistuvista hyökkäyksistä annetun puitepäätöksen vaatimuksia.[120]

Rikoslain 38 luvun 7 a §:n mukaan

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

[119] HE 94/1993 vp. s. 154.
[120] HE 153/2006 vp. s. 120, Rautio 2010 s. 1042.

> *häiriötä, on tuomittava, jollei teosta muualla laissa säädetä ankarampaa tai yhtä ankaraa rangaistusta, tietojärjestelmän häirinnästä sakkoon tai vankeuteen enintään kahdeksi vuodeksi.*
>
> *Yritys on rangaistava.*

Säännöksen tarkoituksena on suojata tietojärjestelmiä virus- ja palvelunestohyökkäyksiltä. Säännös täydentää edellä kerrottua tietoliikenteen häirintää. Mutta eroaa siitä sillä tavalla, että kun tietoliikenteen häirinnässä kohteena on viestintä, tietojärjestelmän kohteena on järjestelmä. Lisäksi tietojärjestelmien häirintä merkitsee usein sähköisten viestien välittämisen häiritsemistä, joten useat tietojärjestelmän toimintaan kohdistuvat häirintäteot täyttävät samalla tietoliikenteen häirinnän tunnusmerkit.[121]

Säännösten keskinäinen soveltamisjärjestys määräytyy tietojärjestelmän häirintä -säännöksen toissijaisuuslausekkeen mukaisesti siten, että tietoliikenteen häirintä yleensä yhtä ankarasti rangaistavana syrjäyttää tietojärjestelmän häirinnän. Tietojärjestelmään voidaan kuitenkin kohdistaa myös sellaista häirintää, joka ei edes välillisesti liity viestien siirtoon, minkä vuoksi erillistä säännöstä on pidetty tarpeellisena.[122]

Häirinnän tarkoituksena tulee olla aiheuttaa toiselle haittaa tai vahinkoa. Vaaditaan siis erityistä tahallisuutta. Toisaalta teon tulee olla oikeudeton. Esimerkiksi loukatun suostumus poistaa rangaistavuuden.[123]

Tietojärjestelmän tekotapoja ovat datan syöttäminen, muuttaminen, siirtäminen, vahingoittaminen ja poistaminen. Pykälässä mainittu tekotapaluettelo on kattava, mutta ei tyhjentävä. Muukin niihin rinnastettava tapa tulee kysymykseen. Tekotavoille kuitenkin on yhteistä, että häiriö aiheutetaan joko kohteena olevan järjestelmän ulkopuolista dataa käyttämällä tai vahingoittamatta esimerkiksi ylikuormittamalla järjestelmää tai syöttämällä dataa, jolla on häiriötä aiheuttavia ominaisuuksia. Tyypillinen tekotapa on dataa tuhoavan tai muuttavan tietokoneviruksen saattaminen järjestelmään.[124]

Hajautetulla palvelunestohyökkäyksellä tarkoitetaan hyökkäystä, jossa hyökkäykseen käytetty ohjelma ensin asennetaan uhrien koneisiin, minkä jälkeen verkon eri osissa sijaitsevat hyökkäysohjelmat aktivoidaan samanaikaisesti suorittamaan varsinainen

---

[121] HE 153/2006 vp. s. 65.
[122] HE 153/2006 vp. s. 65.
[123] HE 153/2006 vp. s. 65.
[124] HE 153/2006 vp. s. 65.

hyökkäys ennalta määrättyyn kohteeseen. Hajautetun hyökkäyksen erityispiirre sen lisäksi, että sitä vastaan suojautuminen on vaikeaa, on se, että se altistaa hyökkäykseen tahattomasti osallistuvat välikädet aiheettomille rikosepäilyille.[125]

Rikoslain 38 luvun 7 a §:n 1 momentin mukaan tietojärjestelmän häirinnän seurauksena tulee olla tietojärjestelmän toiminnan estäminen tai vakavan häiriön aiheuttaminen järjestelmälle. Vakava häiriö on esimerkiksi järjestelmän toiminnan olennainen hidastuminen tai sen toimintavarmuuden olennainen heikkeneminen siten, että järjestelmää ei voida käyttää sen normaalin käyttötarkoituksen edellyttämällä tavalla.[126]

Törkeä tietojärjestelmän häirintä rikoslain 38 luvun 7 b §:n mukaan on seuraavaa:

> *Jos tietojärjestelmän häirinnässä*
>
> *1) aiheutetaan erityisen tuntuvaa haittaa tai taloudellista vahinkoa tai*
>
> *2) rikos tehdään erityisen suunnitelmallisesti*
>
> *ja tietojärjestelmän häirintä on myös kokonaisuutena arvostellen törkeä, rikoksentekijä on tuomittava törkeästä tietojärjestelmän häirinnästä vankeuteen vähintään neljäksi kuukaudeksi ja enintään neljäksi vuodeksi.*
>
> *Yritys on rangaistava.*

Tietojärjestelmän häirintä voi olla törkeä rikoslain 38 luvun 7 b §:n mukaan, jos sillä aiheutetaan erityisen tuntuvaa haittaa tai taloudellista vahinkoa tai rikos tehdään erityisen suunnitelmallisesti. Lisäksi edellytetään, että tietojärjestelmän häirintä on myös kokonaisuutena arvostellen törkeä.

Haitta viittaa muuhun kuin taloudelliseen vahinkoon. Tietojärjestelmän käytön estyminen tai olennainen heikkeneminen ei aina aiheuta ainakaan välitöntä taloudellista vahinkoa, vaan esimerkiksi hidastaa työn tai tehtävän suorittamista tai siirtää järjestelmän kautta tapahtuvien toimenpiteiden, kuten yhteydenottojen, hankintojen tai vastaavien toteuttamista. Erityisen tuntuvana voi pitää sellaista haittaa, joka on pitkäaikaista ja laajasti vaikuttavaa ja jonka poistaminen vaatii huomattavia ponnistuksia. Haitan tuntuvuuden pitää olla rikoksentekijän miellettävissä. Tietojärjestelmän käytön tilapäisestä

[125] HE 153/2006 vp. s. 66.
[126] HE 153/2006 vp. s. 65-66.

estymisestä aiheutuva satunnainen huomattavakaan haitta ei aina täytä tätä edellytystä.[127]

Taloudellinen vahinko viittaa tietojärjestelmän käytön estymisen tai häiriintymisen aiheuttamiin rahassa mitattaviin menetyksiin. Välittömiä kustannuksia voi aiheutua uuden järjestelmän hankinnasta, vanhan korjaamisesta tai huoltamisesta taikka varajärjestelmän vuokraamisesta. Vahinkoa voi syntyä myös tulojen menettämisen johdosta. Myös taloudellisen vahingon ja sen tuntuvuuden tulee olla rikoksentekijän miellettävissä.[128]

Tietojärjestelmän häirintä edellyttänee jokseenkin aina jonkinasteista suunnitelmallisuutta ja järjestelmän tuntemusta. Tämä tulee ottaa huomioon asetettaessa törkeän tekomuodon soveltamisessa tarkoitetun erityisen suunnitelmallisuuden kynnystä. Tehtyjen valmistelutoimenpiteiden tai ilmitulon estämiseksi tai rikoshyödyn salaamiseksi tehtyjen toimenpiteiden tulee olla poikkeuksellisen laajoja tai huomattavan monimutkaisia ainakin silloin, kun on kyse järjestelmässä tehdyistä toimenpiteistä. Esimerkkinä voidaan mainita niin sanottu hajautettu palvelunestohyökkäys.[129]

4.2.3 Tietomurto

Rikoslain 38 luvun 8 § mukaan tietomurrolla tarkoitetaan seuraavaa:

> *Joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja, taikka sellaisen järjestelmän erikseen suojattuun osaan, on tuomittava tietomurrosta sakkoon tai vankeuteen enintään yhdeksi vuodeksi.*
> *Tietomurrosta tuomitaan myös se, joka tietojärjestelmään tai sen osaan tunkeutumatta teknisen erikoislaitteen avulla oikeudettomasti ottaa selon 1 momentissa tarkoitetussa tietojärjestelmässä olevasta tiedosta.*
> *Yritys on rangaistava.*
> *Tätä pykälää sovelletaan ainoastaan tekoon, josta ei ole muualla laissa säädetty ankarampaa tai yhtä ankaraa rangaistusta.*

[127] HE 153/2006 vp. s. 66.
[128] HE 153/2006 vp. s. 66.
[129] HE 153/2006 vp. s. 66.

Tietomurto säännös täydentää tietojärjestelmien ja tietokonetyöskentelyn suojaa erityissäännöksenä. Säännös väistyy, jos teosta on muualla laissa säädetty yhtä ankara tai ankarampi rangaistus. Jos kysymyksessä on esimerkiksi yritysvakoilua varten tapahtuva tietojärjestelmään tunkeutuminen, säännökset syrjäytyvät.[130]

Säännökseen sisältyy kaksi eri kriminalisointia. Ensimmäinen koskee oikeudetonta tunkeutumista tietojärjestelmään tai sen erikseen suojattuun osaan. Yhteys tietojärjestelmään voidaan ottaa esimerkiksi modeemia käyttäen puhelinlinjan välityksellä. Kysymykseen voi tulla myös tilanne, jossa tekijällä on oikeus olla yhteydessä tietojärjestelmään, mutta hän tunkeutuu järjestelmän sellaiseen suojattuun osaan, johon hänellä ei ole oikeutta. Toinen taas turvaa tietokonetyöskentelyn yksityisyyttä sellaisissa tapauksissa, joissa ei ole kysymys salakuuntelusta tai -katselusta.[131] Tietojärjestelmään tunkeutumisella tarkoitetaan pääsyn hankkimista järjestelmässä varastoituihin, käsiteltyihin tai siirrettyihin tietoihin.[132]

Säännöksessä on kysymys automaattisesta tietojenkäsittelystä ja niin sanotusta datasiirrosta. Säännös koskee ainoastaan sellaisia järjestelmiä, joissa tietoja käsitellään, varastoidaan tai siirretään sähköisesti tai muulla vastaavalla teknisellä keinolla. Se ei koske manuaalisia tietojärjestelmiä.[133]

Teon rangaistavuuden edellytyksenä on se, että tunkeutuminen tapahtuu järjestelmän turvajärjestely[134] murtamalla. Turvajärjestely on murrettava jollakin rikoksentekijän toiminnalla eikä esimerkiksi turvajärjestelyn satunnainen epäkunto ja siitä johtuva ulkopuolisen pääsy järjestelmään kuulu säännöksen piiriin. Tunkeutumisen tulee olla tahallista eli tunkeutuja on tiedettävä tunkeutuvansa tietojärjestelmään tai sen osaan oikeudettomasti.[135]

Rikos täyttyy heti, kun tunnistuskontrolli on läpäisty. Jos turvajärjestely on monivaiheinen, edellytetään viimeisenkin vaiheen läpäisemistä. Sitä ennen on kyse tämän rikoksen yrityksestä. Tunkeutuminen ei edellytä, että tietojärjestelmässä olevia tietoja millään

[130] HE 94/1993 vp. s. 156.
[131] HE 94/1993 vp. s. 155.
[132] Pihlajamäki 2004, s. 124.
[133] HE 94/1993 vp. s. 155.
[134] Esimerkiksi tunnistuskontrollin murtaminen.
[135] HE 94/1993 vp. s. 155-156 ja Pihlajamäki 2004, s. 126.

tavalla käytetään, luetaan tai selataan. Jos rikos on edennyt tietojen käyttämiseen saakka, tekoon tulee soveltaa luvatonta käyttöä koskevia rikoslain 28 luvun säännöksiä.[136]

Tietomurrosta tuomitaan myös se, joka oikeudettomasti saa tietoonsa teknisen erikoisvälineen avulla tietojärjestelmässä olevasta tiedosta. Tällaista on esimerkiksi tiedon hankkiminen, jossa tietojärjestelmässä oleva tieto saadaan selville käyttämällä laitetta, joka tietojärjestelmästä lähtevän säteilyn perusteella pystyy selvittämään järjestelmässä käsiteltävän tiedon sisällön. Säännöstä voidaan soveltaa siirrettävänä olevan viestin sieppaamiseen, johon ei voida soveltaa viestintäsalaisuuden loukkausta koskevaa säännöstä, koska tiedonsiirto ei tapahdu televerkossa.[137]

Tietomurtosäännöksen tarkoituksena on suojata *Pihlajamäen* mukaan tietojenkäsittelyrauhaa hakkerien toiminnalta. Tietomurtosäännös on yhteydessä toiseen rikoslain säädökseen, nimittäin luvattomaan käyttöön. Rikoslain 28 luvun 7-9 §:t käsittelevät luvatonta käyttöä. Luvattomana käyttönä tarkoitetaan toisen irtaimen omaisuuden tai kiinteän koneen tai laitteen luvatonta käyttämistä. Jos järjestelmään tunkeutuja ei tyydy pelkkään sisäänpääsyyn vaan alkaa käyttää järjestelmää, tunnusmerkistö viittaa enemmän luvattomaan käyttöön kuin itse tietomurtoon[138]. *Pihlajamäen* mukaan tietomurtosäännös on tarkoitettu pitkälti toimimaan ennalta ehkäisevänä pelotteena, sillä jokainen käynti tietojärjestelmään jättää omat jälkensä.[139]

Ruotsissa tietomurtoa vastaava säännös löytyy brottsbalkenin (SFS 1962:700) 4. luvun (Om brott mot frihet och frid) 9 c §:stä:

> *9 c § Den som i annat fall än som sägs i 8 och 9 §§ olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling eller olovligen ändrar, utplånar, blockerar eller i register för in en sådan uppgift döms för dataintrång till böter eller fängelse i högst två år. Detsamma gäller den som olovligen genom någon annan liknande åtgärd allvarligt stör eller hindrar användningen av en sådan uppgift. Lag (2007:213).*

Luvun 10 §:n mukaan myös teon yritys ja valmistelu ovat rangaistavia ellei tekoa täytettynä olisi pidettävä vähäisenä. Tietomurtokriminalisointi on siis toissijainen.

---

[136] HE 94/1993 vp. s. 156.
[137] HE 94/1993 vp. s. 156.
[138] Rikoslain 28 luvun 9§:n 3 momentin mukaan luvattomana käyttönä ei pidetä kuitenkaan suojaamattoman langattoman verkkoyhteyden kautta muodostetun internet-yhteyden käyttämistä. Lakimuutos tuli voimaan 4.3.2011. Tämä on osoitus siitä, että toimintojen siirtyminen yhä enemmän verkkomaailmaan, tuo myös itse käyttäjälle vastuuta huolehtia paremmin tietoturvastaan.
[139] Pihlajamäki 2004, s. 131.

Tietomurron törkeää tekomuotoa koskeva säännös lisättiin rikoslain 38 lukuun vuonna 2007. Rikoslain 38 luvun 8 a §:n mukaan

> *Jos tietomurto tehdään*
>
> *1) osana 17 luvun 1 a §:n 4 momentissa tarkoitetun järjestäytyneen rikollisryhmän toimintaa tai*
>
> *2) erityisen suunnitelmallisesti ja tietomurto on myös kokonaisuutena arvostellen törkeä, rikoksentekijä on tuomittava törkeästä tietomurrosta sakkoon tai vankeuteen enintään kahdeksi vuodeksi.*
>
> *Yritys on rangaistava.*

Järjestäytyneellä rikollisryhmällä tarkoitetaan rikoslain 17:1 a 4:ssa vähintään kolmen hengen muodostamaa tietyn ajan koossa pysyvää rakenteeltaan jäsentynyttä yhteenliittymää. Ryhmä toimii yhteistuumin tehdäkseen rikoslain 17:1 a 1:ssa tarkoitettuja rikoksia eli rikoksia, joista on säädetty enimmäisrangaistus vähintään neljä vuotta vankeutta tai yhden tai useamman kiihottamisen kansanryhmää vastaan tai oikeudenkäytössä kuultavan uhkaamisen.

Ryhmän tulee olla järjestäytynyt, millä tarkoitetaan, että järjestäytyneisyydelle on jonkinasteinen työnjako ja hierarkia. Ryhmällä täytyy olla selvä johto ja johdolla käskyvalta ryhmän jäseniin nähden, jotka ovat hierarkiassa alempana. Järjestäytyneisyyteen kuuluu myös henkilöiden välinen työnjako.[140]

Törkeä tekomuoto tarkoittaa myös sitä, että teko tehdään erityisen suunnitelmallisesti. Sillä tarkoitetaan esimerkiksi varsinaista tekoa edeltäviä laajoja valmistelutoimenpiteitä sekä toimia teon jälkeen jälkien peittämiseksi.[141] Lisäksi teon on oltava kokonaisuutena arvostellen törkeä.

Korkein oikeus on vahvistanut 8.4.2003 hovioikeuden päätöksen, joka on puhututtanut tietokoneväkeä pitkään. Ratkaisussa (KKO 2003:36) A oli vuonna 1998 yrittänyt murtaa turvajärjestelyn tunkeutuakseen oikeudettomasti osuuspankin tietojärjestelmään. A oli suorittanut niin sanotun porttiskannauksen eli erityistä tietokoneohjelmaa käyttämällä skannannut läpi osuuskunnan internetin yhteydessä olevan verkon kaikki osoitteet

[140] HE 153/2006 vp. s. 67.
[141] HE 153/2006 vp. s. 67.

tarkoituksin löytää avoimia välityspalveluita. Skannaus ei ollut kuitenkaan läpäissyt osuuskunnan tietojärjestelmän palomuuria.[142]

Hovioikeus katsoi, että A oli tehnyt porttiskannauksen siinä tarkoituksessa, että hänellä oli tarkoitus tunkeutua tietojärjestelmään. A:n teko täytti siten tietomurron yrityksen tunnusmerkistön. Hovioikeuden mielestä A:ta voitiin pitää atk-alan asiantuntijana. A:n oli toiminnassaan täytynyt ottaa huomioon, että hän voi menettelyllään aiheuttaa suurtakin vahinkoa, vaikkei olisikaan ollut tietoinen siitä, kenen verkon hän skannasi. Näin ollen ei ollut aihetta sovitella korvauksia. Tekohetkellä 17-vuotias nuori tuomittiin sakkorangaistukseen ja 75 000 markan vahingonkorvaukseen siitä, että hän oli suorittanut porttiskannauksen Osuuspankin verkkoon.[143]

Noin 12 500 euron korvaukset ovat kova pala kenelle tahansa parikymppiselle nuorelle. Etenkin kun varsinainen rikos ei tunnu järin suurelta. Mutta laki suhtautuu tietoverkossa tapahtuviin rikoksiin tiukasti silloinkin, kun ne jäävät yrityksen tai pelkän uteliaan testaamisen asteelle. Päätös herättää myös kysymyksen syytetyn oikeusturvasta. Tietoverkossa tapahtuvat rikokset ovat usein vaikeita myös tuomareille, koska ne vaativat tekniikan asiantuntemusta.[144]

4.2.4 Suojauksen purkujärjestelmärikos ja menettämisseuraamus

Rikoslain 38 luvun 8b§:n mukaan

> *Joka eräiden suojauksen purkujärjestelmien kieltämisestä annetun lain (1117/2001) 3 §:ssä säädetyn kiellon vastaisesti ansiotarkoituksessa tai siten, että teko on omiaan aiheuttamaan huomattavaa haittaa tai vahinkoa suojatun palvelun tarjoajalle, valmistaa, tuo maahan, pitää kaupan, vuokraa tai levittää suojauksen purkujärjestelmää, mainostaa sitä taikka asentaa tai huoltaa sitä, on tuomittava, jollei teosta muualla laissa säädetä ankarampaa tai yhtä ankaraa rangaistusta, suojauksen purkujärjestelmärikoksesta sakkoon tai vankeuteen enintään yhdeksi vuodeksi.*

Eräiden suojauksen purkujärjestelmien kieltämisestä annetun lain (30.11.2001/1117) 2 §:n 2. momentin mukaan suojauksen purkujärjestelmässä tarkoitetaan sellaisia laitteita,

[142] KKO 2003:36
[143] KKO 2003:36
[144] Fredman, Järvinen 2003, s. 766.

tietokoneohjelmia, jonka tarkoituksen on poistaa televerkon avulla tarkoittavan palvelun erityisellä teknisellä järjestelmällä toteutettu suojaus. Laissa tarkoitettuja suojauksen purkujärjestelmiä ovat muun muassa maksutelevisiokanavan suojauksen purkava älykortti tai tietokoneohjelma, joka mahdollistaa pääsyn Internetissä tarjottavaan palveluun[145].

Suojauksen purkujärjestelmää koskevalla kiellolla tarkoitetaan suojauksen purkujärjestelmän oikeudetonta hallussapitoa, valmistusta, käyttöä, maahantuontia, vuokrausta, kaupanpitoa, levittämistä, huoltoa ja asentamista. Oikeudettomia ovat myös toimet, jotka suoritetaan ilman palvelun tarjoajan lupaa. Esimerkiksi palvelun teknisen suojauksen purkamiseen valmistetaan järjestelmä ilman, että palvelun tarjoaja on antanut siihen luvan.[146]

Oikeudettoman toiminnan ei tarvitse olla laajamittaista tai ammattimaisesti organisoitua, jotta se täyttäisi ansiotarkoitusvaatimuksen. Teon motiivina taloudellisen hyödyn hankkimistarkoitukseen on riittävä edellytys säännöksen soveltamiselle. Suojatun palvelun tarjoajalle voidaan aiheuttaa huomattavaa vahinkoa tai haittaa myös toimilla, joihin ei liity taloudellisen hyödyn hankkimistarkoitusta. Esimerkiksi Internetissä voidaan levittää suojauksen purkujärjestelmiä.[147]

Rikoslain 38 luvun 10 §:n mukaan suojauksen purkujärjestelmärikos on asianomistajarikos. Mutta vaikka asianomistaja ei ole ilmoittanut rikosta syytteeseen pantavaksi, niin virallinen syyttäjä saa nostaa syytteen erittäin tärkeän edun niin vaatiessa.

Rikoslain 38 luvun 11 §:n mukaan suojauksen purkujärjestelmä on tuomittava valtiolle menetetyksi. Muutoin, kuten rikoksella saadun hyödyn osalta, sovelletaan rikoslain 2 luvun 16 pykälää menettämisseuraamussäännöstä.

4.2.5 Henkilörekisteririkos

Henkilötietojen suoja on ihmisen perusoikeuksien, erityisesti yksityisyyden suojaa. Ja me puhumme henkilötietojen suojasta silloin, kun jokin henkilötieto, eli tieto, jonka

[145]HE 146/2000 vp. s.11.
[146]HE 146/2000 vp. s.11.
[147]HE 146/2000 vp. s.12.

avulla meidät voidaan yksilönä tunnistaa, on kiinnitetty jollekin alustalle.[148] Henkilötiedolla tarkoitetaan henkilötietolain 3 §:n mukaan kaikenlaisia luonnollista henkilöä tai hänen elinolosuhteitaan tai ominaisuuksiaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi.

Toinen tärkeä käsite on henkilörekisteri. Henkilötietolain 3 §:n mukaan henkilörekisterillä tarkoitetaan *" käyttötarkoituksensa vuoksi yhteenkuuluvista merkinnöistä muodostuvaa henkilötietoja sisältävää tietojoukkoa, jota käsitellään osin tai kokonaan automaattisen tietojenkäsittelyn avulla taikka joka on järjestetty kortistoksi, luetteloksi tai muulla näihin verrattavalla tavalla siten, että tiettyä henkilöä koskevat tiedot voidaan löytää helposti ja kohtuuttomitta kustannuksitta"*

Henkilörekisteririkoksen törkein rikosmuoto on rikoslaissa henkilörekisteririkoksena ja lievemmät sakkoihin johtavat henkilörekisteririkkomukset henkilötietolaissa. Rikosmuotojen jaottelu liittyy henkilörekisterilain muuttamiseen henkilötietolaiksi ja se aiheutti muutoksen rikoslain 38 luvun 9 §:ään vuonna 1999.

Rikoslain 38 luvun 9§:n mukaan:

> *Joka tahallaan tai törkeästä huolimattomuudesta*
>
> *1) käsittelee henkilötietoja vastoin henkilötietolain (523/1999) käyttötarkoitussidonnaisuutta, käsittelyn yleisiä edellytyksiä, henkilötietojen tarpeellisuutta tai virheettömyyttä, arkaluonteisia tietoja, henkilötunnusta tai henkilötietojen käsittelyä erityisiä tarkoituksia varten koskevia säännöksiä taikka rikkoo henkilötietojen käsittelyä koskevia erityissäännöksiä, (8.6.2001/480)*
>
> *2) antamalla rekisteröidylle väärän tai harhaanjohtavan tiedon estää tai yrittää estää rekisteröityä käyttämästä hänelle kuuluvaa tarkastusoikeutta tai*
>
> *3) siirtää henkilötietoja Euroopan unionin tai Euroopan talousalueen ulkopuolisiin valtioihin henkilötietolain 5 luvun vastaisesti*
>
> *ja siten loukkaa rekisteröidyn yksityisyyden suojaa tai aiheuttaa hänelle muuta vahinkoa tai olennaista haittaa, on tuomittava henkilörekisteririkoksesta sakkoon tai vankeuteen enintään yhdeksi vuodeksi.*

[148] Saarenpää 2011, s. 326.

Henkilörekisteririkoksen tekijänä on aina rekisterinpitäjä tai tämän edustaja. Teot ovat rangaistavia ainoastaan siinä tapauksessa, että ne on tehty tahallisesti. Jos teko tehdään törkeän huolimattomuuden johdosta, on se henkilörekisteririkkomus. Henkilörekisteririkoksen täyttymisen yleisenä edellytyksenä on se, että säännöksessä tarkoitetulla teolla loukataan rekisteröidyn yksityisyyden suojaa tai aiheutetaan hänelle muuta vahinkoa tai olennaista haittaa.[149]

Poroilan mukaan henkilörekisteriin kohdistuvissa henkilötietorikoksissa rikoksentekijät ovat usein työntekijöitä, jotka uteliaisuudesta katselevat työtehtäviin kuulumattomia tietoja. Poroilan tutkimusten mukaan[150] vuonna 2007 tietosuojavaltuutetulle tuli 35 rikoslausuntopyyntöä. Selvityksen kohteena olleissa asioissa käräjäoikeus oli antanut tuomion 20 jutussa, kun taas 12 tapauksessa syyttäjä oli tehnyt syyttämättäjättämispäätöksen. Syyttämättäjättämisen perusteena oli joko syyteoikeuden vanhentuminen tai puuttuva näyttö. Tuomio oli tullut siis yli puolessa tapauksista. Suurimmassa osassa tuomioista rikosnimikkeen oli henkilörekisteririkos.[151]

4.2.6 Syyteoikeus ja oikeushenkilön rangaistusvastuu

Rikoslain 38 luvun 10 §:n 1 momentin mukaan

> *Jos salassapitorikoksen tai salassapitorikkomuksen kohteena on yksityisen henkilökohtaisia tai taloudellisia oloja taikka elinkeinoa koskeva seikka, syyttäjä ei saa nostaa syytettä tästä teosta, ellei asianomistaja ilmoita sitä syytteeseen pantavaksi taikka ellei rikoksentekijä rikoksen tehdessään ole ollut yleistä posti- tai teletoimintaa harjoittavan laitoksen palveluksessa taikka erittäin tärkeä yleinen etu vaadi syytteen nostamista.*

Salassapitosäännöksillä suojataan sekä yksityisiä että julkisia intressejä. Koska salassapitoperusteet ovat hyvin vaihtelevia, myös salassapitorikoksen syyteoikeus on eriytettävä sen mukaan, minkä tyyppisiä etuja mikin salassapitovelvollisuus koskee. Salassapitorikoksista asianomistajarikoksia ovat useimmiten ne, joissa on kysymys yksityisen hen-

[149] HE 94/1993 vp. s.157.
[150] Poroila teki tietosuojavaltuutetun toimistossa selvityksen henkilörekisteriin kohdistuvissa rikosasioissa tietosuojavaltuutetulta vuonna 2007 pyydetyistä lausunnoista.
[151] Poroila 2009, s. 26-27.

kilökohtaisia tai taloudellisia oloja tai elinkeinoa koskevien salassapitovelvollisuuksien rikkomisesta. Valtion turvallisuuteen tai viranomaisen toimintaan liittyvät salassapitorikokset ovat virallisen syytteen alaisia.[152]

Rikoslain 38 luvun 10 §:n 2 momentin mukaan:

> *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.*

Asianomistaja rikokset ovat rikoksia, joihin tarvitaan aina asianomistajan lupa. Asianomistaja on ilmoittanut poliisille tai syyttäjälle vaativansa rikokseen syyllistyneelle rangaistusta. Jos asianomistaja peruuttaa vaatimuksensa, poliisi keskeyttää tutkinnan. Suurin osa rikoksista on kuitenkin niin sanotun virallisen syytteen alaisia. Tällä tarkoitetaan sitä, että poliisi voi tutkia niitä ja syyttäjä syyttää niistä, vaikka asianomistaja ei vaatisikaan niistä rangaistusta.[153]

Rikoslain 38 luvun 10 §:n 3 momentin mukaan:

> *Syyttäjän on ennen henkilörekisteriin kohdistuvaa salassapitorikosta, salassapitorikkomusta, viestintäsalaisuuden loukkausta, törkeää viestintäsalaisuuden loukkausta tai tietomurtoa taikka henkilörekisteririkosta koskevan syytteen nostamista kuultava tietosuojavaltuutettua. Tuomioistuimen on tällaista rikosta koskevaa asiaa käsitellessään varattava tietosuojavaltuutetulle tilaisuus tulla kuulluksi.*

Tällä halutaan varmistua siitä, että rikosprosessin toimijat saavat käyttöönsä sen tietosuoja-alan erityisosaamisen, jota tietosuojavaltuutetulla on. Apulaisvaltakunnan syyttäjä on ratkaisussaan 15.4.2008 todennut, *” että tietosuojavaltuutettua tulee aina kuulla henkilötietolain 41 §:n 2 momentin ja rikoslain 38 luvun 10 §:n 3 momentin tilanteissa*

[152] HE 94/1993 vp. s.158.
[153] http://poliisi.fi/poliisi%5Chome.nsf/pages/55A4688283395A67C2256B980043A39C?opendocument. Viitattu 3.8.2011.

syyteharkinnan yhteydessä, vaikka syyteharkinta johtaisikin seuraamusluonteiseen tai prosessuaaliseen syyttämättä jättämiseen".[154]

Rikoslain 38 luvun 12 §:n mukaan viestintäsalaisuuden loukkaukseen, törkeään viestintäsalaisuuden loukkaukseen, tietoliikenteen häirintään, törkeään tietoliikenteen häirintään, tietomurtoon, törkeään tietomurtoon, tietojärjestelmän häirintään ja törkeään tietojärjestelmän häirintään sovelletaan, mitä oikeushenkilön rangaistusvastuusta säädetään.

Rikoslain 9 luvun 1 § yhteisö, säätiö tai muu oikeushenkilö, jonka toiminnassa on tehty rikos, on syyttäjän vaatimuksesta tuomittava rikoksen johdosta yhteisösakkoon, jos se on rikoslain mukaan säädetty rikoksen seuraamukseksi. Kuitenkaan julkisen vallan käytössä tehtyyn rikokseen sovelletaan kuitenkin virkarikossäännöstöä.

Yhteisösakon tuomitsemiseksi vaaditaan, että oikeushenkilön toiminnassa on tehty konkreettinen rikos. Kysymykseen ei voi kuitenkaan tulla mikä tahansa rikos. Jotta yhteisösakko voidaan tuomita, lakitekstissä vaaditaan maininta siitä, että yhteisösakosta säädetyt säännöt koskevat tätä rikosta.[155]

Rikoslain 38 luvun 10 §:ää on muutettu hieman lakimuutoksella 13.5.2011/441. Syyttäjä- sanan edessä on ollut sana virallinen, mutta lakimuutoksen kautta, se on siitä poistettu. Lakitekstissä käsitteet eivät ole olleet yhtenäisiä ja varsinkin syyttäjiin viittaaminen vaihtelee. Uudistuksella on haluttu luoda yhtenäinen käytäntö, jossa syyttäjiin viitataan aina sanalla syyttäjä.[156] Kerron seuraavaksi lakimuutoksista, jotka ovat muuttaneet rikoslain 38 lukua vuoden 1995 lakimuutoksen jälkeen. Viimeisintä muutosta en kuitenkaan käsittele tämän enempää, koska lakimuutoksessa 13.5.2011/441 kyse oli vain yhden sanan poistamisesta lakitekstistä.

[154] Valtakunnansyyttäjäviraston ratkaisu 15.4.2008.
http://www.vksv.oikeus.fi/Etusivu/Ratkaisuja/Ratkaisuja2008/1208352670868. Viitattu 31.7.2011.
[155] Frände 2005, s. 404.
[156] HE 286/2010 vp. s. 11, 23.

5 RIKOSLAIN 38 LUKUUN LIITTYVÄT LAKIMUUTOKSET

5.1 Yleistä lakimuutoksista

Lait vanhentuvat tai tulevat ajan mittaan puutteellisiksi, joten voimassaolevia lakeja täytyy uudistaa. Lakimuutoksen kautta uudistettu laki vastaa paremmin yhteiskunnan tarpeita. Lisäksi lakimuutos tulee ajankohtaiseksi myös direktiivien kautta.

Direktiivit ovat Euroopan unionin jäsenvaltioille tarkoitettuja lainsäädäntöohjeita. Se ei suoraan vaikuta jäsenvaltioiden lainsäädäntöön, mutta jäsenvaltion lainsäädännön on täytettävä direktiivin vaatimukset. Jos lainsäädäntö täyttää direktiivin vaatimukset, ei lakia tarvitse muuttaa, mutta jos ei, niin silloin lakia muutetaan. Direktiivi on pantava täytäntöön eli implementoitava.[157]

Suomen perustuslain (11.6.1999/731) 6 luvussa säädetään lain säätämisestä. Kyseisen luvun 70 §:n mukaan lain säätäminen tulee vireille eduskunnassa hallituksen esityksellä tai kansanedustajan lakialoitteella. Eduskunnan työjärjestyksen (17.12.1999/40 v. 2000) 4 luvun 32 §:n mukaan lain käsittely alkaa eduskunnan täysistunnossa lähetekeskustelulla. Lähetekeskustelun päätyttyä eduskunta päättää puhemiesneuvoston ehdotuksesta, mihin valiokuntaan asia lähetetään.

Suomen perustuslain 6 luvun 72§:n ja eduskunnan työjärjestyksen 5 luvun 53§:n mukaan lakiehdotus otetaan asiaa valmistelleen valiokunnan annettua siitä mietintönsä eduskunnan täysistunnossa kahteen käsittelyyn. Lakiehdotuksen ensimmäisessä käsittelyssä esitellään valiokunnan mietintö ja käydään siitä yleiskeskustelu sekä päätetään lakiehdotuksen sisällöstä. Toisessa käsittelyssä, joka pidetään aikaisintaan kolmantena päivänä ensimmäisen käsittelyn päätyttyä, päätetään lakiehdotuksen hyväksymisestä tai hylkäämisestä. Sen sisältöön ei enää puututa.

Suomen perustuslain 6 luvun 77§:n mukaan eduskunnan hyväksymä laki on esiteltävä tasavallan presidentin vahvistettavaksi. Presidentin on päätettävä lain vahvistamisesta kolmen kuukauden kuluessa. Presidentti voi hankkia laista lausunnon korkeimmalta oikeudelta tai korkeimmalta hallinto-oikeudelta. Jollei presidentti vahvista lakia, se palautuu eduskunnan käsiteltäväksi. Jos eduskunta hyväksyy lain uudelleen asiasisällöl-

[157] Ojanen 2010, s. 42-43.

tään muuttamattomana, se tulee voimaan ilman vahvistusta. Lain katsotaan rauenneen, jos eduskunta ei ole sitä uudestaan hyväksynyt.

Suomen perustuslain 6 luvun 79§:n mukaan laki, joka on vahvistettu tai tulee voimaan ilman vahvistusta, on tasavallan presidentin allekirjoitettava ja asianomaisen ministerin varmennettava. Valtioneuvoston on tämän jälkeen viipymättä julkaistava laki Suomen säädöskokoelmassa. Laista tulee käydä ilmi, milloin se tulee voimaan. Erityisestä syystä laissa voidaan säätää, että sen voimaantuloajankohdasta säädetään asetuksella. Jollei lakia ole julkaistu viimeistään säädettynä voimaantuloajankohtana, se tulee voimaan julkaisemispäivänä.

Rikoslain 38 lukua on muutettu viisi kertaa sen jälkeen, kun siihen tehtiin perustavanlaatuinen muutos vuonna 1995.

5.2 Lakimuutos 525/1999

Ensimmäinen lakimuutos koski henkilörekisteririkosta. Hallituksen esityksen pohjalta eduskunta hyväksyi henkilötietolain, lain tietosuojalautakunnasta ja tietosuojavaltuutetusta annetun lain muuttamisesta, lain rikoslain 38 luvun 9§:n muuttamisesta sekä lain yleisten asiakirjain julkisuudesta annetun lain 18 a §:n muuttamisesta.[158]

Tietosuojalainsäädännön tarpeeseen hyväksyttiin henkilörekisterilaki vuonna 1987. Voimaan se tuli seuraavana vuonna. Henkilörekisterilain korvasi henkilötietolaki (22.4.1999/523), joka tuli voimaan 1.6.1999. Uusi laki on myös Euroopan henkilötietodirektiivin mukainen.

Tietosuojadirektiivin tarkoituksena on turvata yksilön perusoikeudet ja – vapaudet tietojenkäsittelyssä, mutta myös lainsäädäntöä harmonisoimalla turvata henkilötietojen vapaa liikkuvuus Euroopan unionin jäsenvaltioiden välillä.[159]

Samalla muutettiin myös henkilörekisteririkoksen tunnusmerkistöä ja tämä merkitsi myös lakimuutosta rikoslain 38 luvun 9§:ään. Hallintovaliokunta hyväksyi hallituksen esityksessä ehdotetun muutoksen rikoslain 38 luvun 9§:ään muutettuna. Hallintovalio-

[158] http://www.eduskunta.fi/valtiopaivaasiat/he+96/1998
[159] Euroopan parlamentin ja neuvoston direktiivi 95/46/EY 1 artikla.

kunta ehdotti eduskunnalle, että vakiintuneen kirjoitustavan mukaan käsitteen ”törkeä tuottamus” sijasta käytetään käsitettä ”törkeä huolimattomuus”. Eduskunta hyväksyi lakimuutoksen hallituksen esityksen pohjalta muutettuna.

Myös Ruotsissa Suomen tapaan uudistettiin henkilötietolaki, Personuppgifftslagen (PuL), vuonna 1998. Uusi laki vastasi henkilötietodirektiivin vaatimuksia. Sen tarkoituksena on suojella ihmisten yksityisyyttä, kun on kyse henkilötietojen käsittelystä.[160]

Henkilötietodirektiivi ei vastaa nykyajan vaatimuksia ja sitä ollaan muuttamassa. Kerron uudistamisesta tarkemmin luvussa 7.2.

5.3 Lakimuutos 531/2000

Hallituksen esityksen pohjalta eduskunta hyväksyi sekä lain rikoslain, että lain yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta annetun lain 18 §:n muuttamisesta. Eduskunta hyväksyi lait 9.6.2000 ja ne tulivat voimaan 1.10.2000.[161]

Hallituksen esityksessä ehdotettiin, että silloisen rikoslain 24 lukuun sijoitetut kotirauhan rikkomista, salakuuntelua ja salakatselua sekä rikoslain 27 lukuun sijoitetut kunnian ja yksityiselämän loukkaamista koskevat säännökset uudistettaisiin ja koottaisiin yksityisyyttä, rauhaa ja kunniaa koskevaksi rikoslain 24 luvuksi. Uudistuksella haluttiin nykyaikaistaa ja selkeyttää kotirauha- ja kunnianloukkaussäännökset sekä laajentaa yksityiselämän rikosoikeudellista suojaa.[162]

Lakimuutoksella haluttiin muun muassa täsmentää salakuuntelun ja viestintäsalaisuuden välistä rajaa. Ennen lakimuutosta viestintäsalaisuuden loukkauksena rangaistavaksi oli säädetty äänen kuuntelu sekä sen tallentaminen, jos se tapahtui salaa ja oikeudettomasti sekä kohdistui toisen henkilön puheeseen. Teon rangaistavuus ei riippunut siitä, missä puhuja oli, mutta jos se tapahtui kotirauhan suojaa nauttivalla alueella, tekoon sovellettiin salakuuntelua koskevaa rikoslain 24 luvun 3 b §:n säännöstä.[163]

---

[160] http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/. Viitattu 12.9.2011.
[161] http://www.eduskunta.fi/valtiopaivaasiat/he+184/1999. Viitattu 13.7.2011.
[162] HE 184/1999 vp. s. 1.
[163] HE 94/1993 vp. s. 149.

Muutoksen kautta rikoslain 24 luvun 5 §:stä tuli yleissäännös salakuuntelusta, joka kattaa kaikentyyppisen puheen ja keskustelun kuuntelun. Salakuuntelu kohdistuu puheviestintään, kun taas rikoslain 38 luvun 3 § käsittää sähköisesti tai muulla tavalla välitettävän suojatun viestin kuuntelemisen.[164] Salakuuntelu ei esityksen mukaan ole sidottu kotirauhan suojaamaan alueeseen, vaan kuunneltava voi oleskella missä tahansa. Tällä on haluttu suojata vielä enemmän ihmisten yksityiselämää. Salakuuntelun rangaistavuuden edellytyksenä on, ettei puhe ole tarkoitettu ulkopuolisten tietoon tai että puhujalla ei ole ollut syytä olettaa, että ulkopuoliset kuulisivat hänen puhettaan.[165] Viestintäsalaisuuden loukkauksena pidetään taas esimerkiksi suojatun radioliikenteen, kuten poliisiradioverkon, oikeudetonta kuuntelemista.[166]

5.4 Lakimuutos 1118/2001

Palvelujen tarjoaminen televerkon välityksellä, joiden vastaanottamiseen vaaditaan erityinen laite tai muu järjestelmä, oli kasvanut 1990-luvun lopussa niin suuriin mittoihin, että asiaan tarvittiin rikosoikeudellista sääntelyä. Esimerkkinä tästä voidaan mainita kaapelitelevisio- ja satelliittilähetykset, joiden vastaanottamiseen tarvitaan laite, joka muuntaa lähetyksen katsottavaan muotoon.[167]

Lakimuutoksella hallitus esitti eduskunnalle lakia tietoyhteiskunnan palvelujen suojasta. Lakiesitys hyväksyttiin kuitenkin nimellä laki eräiden suojauksen purkujärjestelmien kieltämisestä. Lakimuutoksen taustalla vaikuttaa Euroopan neuvoston ehdolliseen pääsyyn perustuvien tai ehdollisen pääsyn sisältävien palvelujen oikeussuojasta annettu direktiivi vuodelta 1998 (98/84/EY). Direktiivin tarkoituksena oli yhdenmukaistaa jäsenvaltioiden lainsäädäntöä suojattujen palveluiden ja suojattuihin palveluihin pääsyn mahdollistavien laitteiden ja tietokoneohjelmien osalta sekä lisäksi suojata maksullisia televisio- ja radiolähetyksiä ja etäpalveluita kuten esimerkiksi tilausmusiikin palveluita. Direktiivin tarkoituksen lisäksi oli edesauttaa sitä, että kukin palveluntarjoaja saa maksun tarjoamastaan palvelustaan.[168]

---

[164] HE 184/1999 vp. s. 25.
[165] HE 184/1999 vp. s. 14.
[166] HE 184/1999 vp. s. 25.
[167] HE 146/2000 vp. s. 3.
[168] HE 146/2000 vp. s. 4-5.

Ruotsissa pantiin täytäntöön ehdollisen pääsyn direktiivin edellyttämät muutokset, kun 1.5.2000 tuli voimaan laki (lag om förbud mot viss avkodningsutrustning SFS 2000:171).[169]

Eräiden suojauksen purkujärjestelmien kieltämisessä annetussa lakia (30.11.2001/1117) sovelletaan televerkon avulla tarjottavien tietoyhteiskunnan palvelujen suojaamiseen niiden suojauksen purkujärjestelmien oikeudetonta käyttöä vastaan. Lain 2 §:ssä määritellään se, mitä suojauksen purkujärjestelmällä tarkoitetaan. Suojauksen purkujärjestelmä on laite, tietokoneohjelma tai muu järjestelmä tai järjestelmän olennainen osa, jonka tarkoituksena on poistaa televerkon avulla tarjottavan palvelun erityisellä teknisellä järjestelmällä toteutettu suojaus.

Eräiden suojauksen purkujärjestelmien kieltämisessä annetun lain 3 §:n mukaan suojauksen purkujärjestelmän oikeudeton hallussapito, käyttö, valmistus, maahantuonti, kaupanpito, vuokraus, levittäminen, myynninedistäminen, asentaminen ja huolto on kiellety.

Edellä mainitun lain 6 §:n mukaan rangaistus suojauksen purkujärjestelmärikoksesta säädetään rikoslain 38 luvun 8 a §:ssä. Mutta joka muutoin kuin 6 §:n 1 momentissa mainitussa säännöksessä tarkoitetulla tavalla tahallaan rikkoo 3 §:ssä säädettyä kieltoa, tuomitaan, jollei teosta muualla laissa säädetä ankarampaa rangaistusta, suojauksen purkujärjestelmärikkomuksesta sakkoon.

Lain 6 §:n 3 momentin mukaan virallinen syyttäjä ei saa nostaa syytettä suojauksen purkujärjestelmärikkomuksesta, ellei asianomistaja ilmoita rikosta syytteeseen pantavaksi taikka ellei erittäin tärkeä yleinen etu vaadi syytteen nostamista.

Lakimuutoksella (1118/2001), joka vahvistettiin 30.11.2001, muutettiin rikoslain 38 luvun 10 §:n 2 momentti sekä lisättiin kyseiseen lukuun uusi 8 a ja 11 §:t. Lakia sovelletaan televerkon avulla tarjottavien tietoyhteiskunnan palvelujen suojaamiseen niiden suojauksen purkujärjestelmien oikeudetonta käyttöä vastaan.

[169] HE 146/2000 vp. s. 6.

5.5 Lakimuutos 540/2007

Viimeisin lakimuutos, joka toi isompia muutoksia rikoslain 38 lukuun, tapahtui vuonna 2007. Sen jälkeen rikoslain 38 luku on pysynyt muuttumattomana, ainoastaan jo aiemmin kertomani lakimuutos tapahtui toukokuussa 2011. Tämä lakimuutos koski vain rikoslain 38 luvun 10 §:ää.

Tietotekniikkarikollisuus on helposti rajat ylittävää rikollisuutta. Rikokset kun tapahtuvat internetin välityksellä, ei valtioiden rajoilla ole merkitystä. Tietotekniikkarikollisuus aiheuttaa lisäksi mittavia taloudellisia vahinkoja. Ilman laajaa kansainvälistä yhteistyötä ei rikollisuutta vastaan voida taistella. Tämä huomattiin myös Euroopan neuvostossa ja kyseessä oleva lakimuutos perustuu Euroopan neuvoston tietoverkkorikollisuutta koskevaan yleissopimukseen (Convention on Cybercrime), jäljempänä tietoverkkorikossopimus tai yleissopimus. Suomi allekirjoitti yleissopimuksen marraskuussa 2001.[170]

Yleissopimus on ensimmäinen velvoittava kansainvälinen tietotekniikkarikollisuutta koskeva sopimus. Yleissopimuksella ja sen kansallisella voimaansaattamisella pyritään suojelemaan paremmin yhteiskuntaa tietotekniikkarikollisuudelta sekä sen aiheuttamilta vahingoilta.[171] Sopimusvaltioille on tärkeää harjoittaa yhteistä rikospolitiikkaa, jonka päämääränä on suojella yhteiskuntaa tietoverkkorikollisuudelta lainsäädännön ja tehokkaan kansainvälisen yhteistyön avulla. Myös yhteistyö valtioiden ja yksityisten yritysten välillä on tarpeellista tietoverkkorikollisuuden torjumiseksi.[172]

Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus jakaantuu neljään eri lukuun. Ensimmäinen luku määrittelee käsitteiden käytön, toinen käsittelee niitä kansallisia toimenpiteitä, jotka sopimusvaltioiden on tehtävä. Kolmas luku käsittää kansainvälisen yhteistyön ja viimeinen luku loppumääräykset.[173]

Yleissopimuksen ensimmäinen luku määrittelee käsitteet. Sopimuksessa termillä tietojärjestelmä tarkoitetaan laitetta tai toisiinsa liitettyjä tai kytkettyjä laitteita. Näistä yksi

[170] Pihlajamäki 2007, s. 27-29.
[171] HE 153/2006 vp. s. 4.
[172] Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus (SopS 60/2007) Johdanto 4. ja 7. kappale.
[173] Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus (SopS 60/2007) Pääluvut I Luku käsitteiden käyttö, II luku kansalliset toimenpiteet, III luku kansainvälinen yhteistyö ja IV luku Loppumääräykset.

tai useampi on ohjelmoitu automaattista tietojenkäsittelyä varten. Termillä data tarkoitetaan tietojen, tosiseikkojen tai käsitteiden esitystä niin, että se soveltuu käsiteltäväksi tietojärjestelmässä. Palveluntarjoajalla tarkoitetaan joko julkista tai yksityistä yksikköä, joka tarjoaa palveluidensa käyttäjille mahdollisuuden tietojärjestelmän välityksellä tapahtuvaan viestintään tai muuta yksikköä, joka tallentaa tai käsittelee dataa edellä mainitun palveluntarjoajan tai palvelujen käyttäjien puolesta. Liikennetiedoilla taas tarkoitetaan tietojärjestelmän välityksellä siirrettyyn viestiin liittyvää dataa, jonka viestinsiirtoketjuun kuuluva tietoverkko on tuottanut ja josta ilmenee viestin alkuperä, määränpää, kellonaika, reitti, koko päivämäärä tai kesto.[174]

Yleissopimuksen turvin varmistettiin se, että kaikkien sopimusvaltioiden lainsäädäntö harmonisoituu. Toiseen lukuun on kirjattu kaikki ne kansalliset toimenpiteet, jotka valtioiden on tehtävä. Tietosuoja-lehdelle kirjoittamassaan artikkelissa *Pihlajamäki* kertoo, että Suomen tietotekniikkarikoksia koskeva sääntely on jatkuvasti ollut kansainvälisesti vertailtuna kattavaa, eikä yleissopimuksen voimaansaattaminenkaan merkitse mitään mullistavia uudistuksia[175]. Rikoslain muutokset laajensivat tietoverkkorikollisuuden soveltamisalaa sekä samalla kiristivät rangaistuksia.

Yleissopimuksen mukaisesti datasiirron ja tietojärjestelmien luottamuksellisuuteen, eheyteen ja käytettävyyteen kohdistuvat rikokset[176], tietokoneavusteiset rikokset[177], viestin sisältöön liittyvät rikokset[178] ja tekijänoikeusrikokset ja tekijänoikeuden lähioikeuksia koskevat rikokset[179] on kaikkien sopimusvaltioiden kriminalisoitava.[180] Myös edellä mainittujen rikosten tahallinen avunanto ja yllytys, kun teon tarkoituksena on aikaansaada rikoksen täyttyminen, on rangaistavaa. Lisäksi tahallinen yritys on myös rangaistavaa muutamissa rikoksissa.[181]

Oikeushenkilö voidaan asettaa vastuuseen yleissopimuksen mukaisesti rangaistavaksi säädetystä teosta, jonka luonnollinen henkilö on tehnyt oikeushenkilön hyväksi joko

---

[174] Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus (SopS 60/2007) 1. artikla.
[175] Pihlajamäki 2007, s. 27-29.
[176] Luvaton tunkeutuminen, viestintäsalaisuuden loukkaaminen, datan vahingoittaminen, tietojärjestelmän häirintä ja laitteiden väärinkäyttö.
[177] Tietokoneavusteinen väärennös ja tietokoneavusteinen petos
[178] Lapsipornografiaan liittyvät rikokset
[179] Tekijänoikeusrikokset ja tekijänoikeuden lähioikeuksia koskevat rikokset
[180] Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus (SopS 60/2007) 2-10. artikla.
[181] Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus (SopS 60/2007) 11. artikla 1. ja 2. kappale.

itsenäisesti tai oikeushenkilön nimissä, silloin kun asianomainen henkilö on oikeushenkilössä johtavassa asemassa, joka perustuu: a) valtuutukseen edustaa kyseistä oikeushenkilöä; b) valtuutukseen tehdä päätöksiä kyseisen oikeushenkilön puolesta; c) valtuutukseen harjoittaa oikeushenkilön sisäistä valvontaa.[182]

Oikeushenkilö voidaan asettaa vastuuseen myös silloin kun 1 kappaleessa tarkoitettu luonnollinen henkilö on laiminlyönyt valvonnan, ja kyseisen oikeushenkilön valtuuttaman luonnollisen henkilön on sen vuoksi ollut mahdollista tehdä tämän yleissopimuksen mukaisesti rangaistavaksi säädetty rikos kyseisen oikeushenkilön hyödyksi.[183]

Rikoslain 38 lukuun lisättiin 7 a § ja 7 b §:t ja 5 - 7 §:ssä yritys määrättiin rangaistavaksi. Säännökset täydentävät tietoliikenteen häirintää koskevia säännöksiä ja tarkoittavat tietojärjestelmän toiminnan oikeudetonta estämistä tai vakavan häiriön aiheuttamista tietojärjestelmälle.[184]

Tietoliikenteen häirintä säädettiin rikoslain 38 luvun 5 - 7 §:ien mukaan kolmeen eri kategoriaan: lievään tietoliikenteen häirintään, tietoliikenteen häirintään sekä törkeään tietoliikenteen häirintään. Tietoliikenteen häirinnällä tarkoitetaan ilkivaltaisessa tarkoituksessa lähetettyjä viestejä radiolaitteella tai televerkossa tai muuten estetään tai häiritään postiliikennettä tai radio- tai televiestintää. Tietoliikenteen häirintä muuttuu törkeäksi, jos rikoksentekijä on rikosta tehdessään käyttänyt hyväksi luottamusasemaansa tai muuta asemaansa tai rikoksella on estetty tai häiritty hätäkutsujen radioviestintää. Tietoliikenteen häirintä täytyy olla myös kokonaisuutena arvostellen törkeä.

Spammaus eli roskapostin lähettäminen tai keskustelupalstan häiriköinti ovat esimerkkejä tietoliikenteen häirinnästä.[185] Rikoslain 38 luvun 5-7 §:n mukaan häirinnästä on tuomittava sakkoon tai vankeuteen enintään kahdeksi vuodeksi ja törkeästä tietoliikenteen häirinnästä vankeuteen vähintään neljäksi kuukaudeksi ja enintään neljäksi vuodeksi. Yritys on rangaistava kummassakin tapauksessa kuin myös lievän tietoliikenteen häirinnän kohdalla. Yrityksen rangaistavuus lisättiin lakimuutoksella vuonna 2000.

[182] Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus (SopS 60/2007) 12. artikla 1. kappale.
[183] Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus (SopS 60/2007) 12. artikla 2. kappale.
[184] Pihlajamäki 2007, s. 27-29.
[185] Mäkinen 2006, s. 121

Rikoslain 38 luvun 7 §:n mukaan tietoliikenteen häirintä on lievää, jos aiheutetun häiriön määrä tai laatu tai muut rikokseen liittyvät seikat ovat kokonaisuutena arvostellen vähäisiä. Lievästä tietoliikenteen häirinnästä on tuomittava sakkoa.

Pykälät 7 a ja 7 b koskevat tietojärjestelmän häirintää ja törkeää tietoliikenteen häirintää. Tietojärjestelmän häirinnällä tarkoitetaan tekoa, jossa henkilö aiheuttaakseen toiselle haittaa tai taloudellista vahinkoa estää tietojärjestelmän toiminnan tai aiheuttaa sille vakavaa häiriötä. Tietojärjestelmän häirinnästä tuomitaan sakkoa tai vankeutta enintään kaksi vuotta. Teon yritys on rangaistava.

Mikäli tietojärjestelmän häirinnässä aiheutetaan erityisen tuntuvaa haittaa tai taloudellista vahinkoa tai mikäli rikos tehdään erityisen suunnitelmallisesti, ja tietojärjestelmän häirintä on myös kokonaisuutena arvostellen törkeä, katsotaan teko törkeäksi tietojärjestelmän häirinnäksi. Törkeästä tietojärjestelmän häirinnästä tuomitaan vankeutta neljästä kuukaudesta neljään vuoteen. Teon yritys on rangaistava.

Rikoslain 38 luvun 8 §:n mukaan tietomurrolla tarkoitetaan rikosta, jossa henkilö käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään. Tietomurrosta tuomitaan myös se, joka tietojärjestelmään tai sen osaan tunkeutumatta teknisen erikoislaitteen avulla oikeudettomasti ottaa selon edellä tarkoitetussa tietojärjestelmässä olevasta tiedosta. Tietomurrosta tuomitaan sakkoa tai vankeutta enintään yksi vuosi. Teon yritys on rangaistava.

Mikäli tietomurto tehdään osana järjestäytyneen rikollisryhmän toimintaa taikka erityisen suunnitelmallisesti ja tietomurto on myös kokonaisuutena arvostellen törkeä, katsotaan teko törkeäksi tietomurroksi. Vuonna 1995 säännöt löytyivät vain tietomurron osalta, mutta vuonna 2007 tietomurto sai rinnalleen myös rikoksen törkeämmän muodon, kun säädettiin törkeästä tietomurrosta. Törkeästä tietomurrosta tuomitaan sakkoa tai vankeutta enintään kaksi vuotta. Teon yritys on rangaistava.

Tavallisin tietomurron tekijä on hakkeri. Päästyään sisään järjestelmään hakkeri tutkii paikkoja, selaa tiedostoja, kopioi tiedostoja itselleen ja lukee sähköposteja. Tietojärjestelmään murtautuminen on rikos riippumatta siitä mikä on murtautujan tarkoitus tai mi-

ten helppoa se on ollut. [186] Mutta on muistettava, että tietomurron täyttyminen ei edellytä, millään tavalla kajotaan[187].

Tietoverkkorikosoikeussopimus velvoittaa sopimusvaltiot osallistumaan kansainväliseen rikosoikeudelliseen yhteistyöhön. Yleissopimuksessa sovitaan myös rikoksen johdosta tapatuvasta luovuttamisesta kuin keskinäisestä oikeusavustakin.[188]

Yleissopimuksen myötä muutettiin myös muitakin lakeja kuin rikoslakia. Pakkokeinolain (30.4.1987/450) 4 lukuun lisättiin uudet 4 a - 4 c §:t sekä 4 luvun 1 § ja 15 a §:n 1 momentti muutettiin. Muutokset koskivat data-käsitteen lisäämistä lakitekstiin. Esineen ja asiakirjan ohella nyt myös data voitiin takavarikoida. Tällä hetkellä pakkokeinolain 4 luku käsittää takavarikon, mutta uusi pakkokeinolaki on jo vahvistettu ja se tulee voimaan 1.1.2014. Pakkokeinolain myötä, myös laki kansainvälisestä oikeusavusta rikosasioissa kokee uudistuksen.

Samalla muutettiin myös lakia kansainvälisestä oikeusavusta rikosasioissa (5.1.1994/4). Lain 1 luvun §:n 1 momentin mukaan lakia sovelletaan kansainväliseen oikeusapuun rikosasiassa, jonka käsittely oikeusapua pyydettäessä kuuluu pyynnön esittäneen Suomen viranomaisen tai vieraan valtion viranomaisen toimivaltaan. Yleissopimuksen mukaan kyseessä olevan lain 15 §:ään lisättiin uusi 2 momentti, joka koski pakkokeinojen käytön rajoituksia. Jos oikeusapupyyntö tarkoittaa tai sen täyttäminen edellyttää pakkokeinolaissa tarkoitettujen pakkokeinojen käyttämistä, ei pakkokeinoja saa käyttää 1 momentin mukaan, jos se ei Suomen lain mukaan ole sallittua, jos pyynnön perusteena oleva teko olisi tehty Suomessa vastaavissa olosuhteissa. Mutta 2 momenttiin lisättiin kohta: mitä 1 momentissa säädetään, ei kuitenkaan koske pakkokeinolain 4 luvun 4 b:ssä tarkoitettua datan säilyttämismääräystä. Datan säilyttämismääräyksestä tuli uusi pakkokeino, jota voidaan tarvittaessa käyttää esitoimenpiteenä ennen muita dataan kohdistuvia pakkokeinoja. Kansainvälisestä oikeusavusta rikosasioissa annetun lain 23 §:n 1 momentti muutettiin siten, että siinä olevaan oikeusapupyynnön perusteella toimeenpantavissa olevien pakkokeinojen luetteloon lisättiin datan säilyttämisvelvollisuus.

Yleissopimus toi muutoksensa myös esitutkintalain (30.4.1987/449) 27 ja 28 §:ään. Lain 27 §:ään lisättiin uusi 2 momentti, jonka mukaan todistajalla, jolla on 1 momentis-

[186] Järvinen 2002, s. 294-295.
[187] HE 153/2006 vp. s. 14.
[188] Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus (SopS 60/2007) 23., 24. ja 25. artikla.

sa tarkoitettu ilmaisuvelvollisuus, on velvollisuus myös esittämään hallussaan olevan, esitutkinnan kannalta merkityksellisen asiakirjan tai muun todistusaineiston. Lain 28 §:ään ehdotettiin lisättävän uusi 2 momentti, jonka mukaan 1 momentin mukainen tuomioistuinkäsittely olisi käytettävissä myös silloin, kun todistaja kieltäytyy noudattamasta ehdotetun 27 §:n 2 momentin mukaista esittämisvelvollisuutta.

6 TIETO- JA VIESTINTÄRIKOKSET MUISSA RIKOSLAIN LUVUISSA

On muistettava, että tieto- ja viestintärikoksia on myös muissa rikoslain luvuissa. Jos rikos täyttää lisäksi tietotekniikkarikoksen tunnusmerkit, on se myös tieto- ja viestintärikos, vaikka se nimikkeeltään voi viitata myös muuhunkin. Esittelen seuraavaksi muutamia rikoslain säännöksiä, jotka voivat olla myös tieto- ja viestintärikoksia.

Rikoslain 28 luvun 7-9 §:t, jotka käsittelevät luvattoman käytön tunnusmerkistön. Toisen irtaimen omaisuuden tai kiinteän koneen tai laitteen luvaton käyttö on kielletty rikoslain 28 luvun 7 §:n mukaan. Luvatonta käyttöä ei kuitenkaan ole suojattoman langattoman tietoverkkoyhteyden kautta muodostetun internet-yhteyden käyttöä 7 §:n 3 momentin mukaan.

Yrityssalaisuuden rikkomisesta ja yrityssalaisuuden väärinkäytöstä on säädelty rikoslain 30 luvun 4-6 §:ssä. Rikoslain 30 luvun 4 §:n mukaan yritysvakoilun tunnusmerkistö täyttyy muun muassa silloin, kun oikeudettomasti hankitaan tietoa toiselle kuuluvasta yrityssalaisuudesta tunkeutumalla ulkopuolisilta suojattuun tietojärjestelmään tai käyttämällä teknistä erikoislaitetta ja tarkoituksena on oikeudettomasti ilmaista salaisuus tai oikeudettomasti käyttää sitä.

Myös väärennös (33 luvun 1-3 §:t), maksuvälinepetos (37 luvun 8-10 §:t), rahanpesu (32 luvun 6§) ja vahingonteko (35 luvun 1§:n 2-3 momentit) ovat tieto- ja viestintärikoksia, jos rikoksen tunnusmerkit täyttävät myös tietoverkkorikokselle asetetut vaatimukset.

Vaaran aiheuttaminen tietojenkäsittelylle (34 luvun 9 a §) sekä tietoverkkovälineen hallussapito (34 luvun 9 b §) ovat tieto- ja viestintärikoksia. Vaaran aiheuttamisella tietojenkäsittelylle tarkoitetaan rikoslain 34 luvun 9 a §:n mukaan sitä, että joka aiheuttaakseen haittaa tai vahinkoa tietojenkäsittelylle tai tieto- tai viestintäjärjestelmän toiminnalle tai turvallisuudelle joko tuomalla maahan, valmistavan, myyvän tai muuten levittävän tai asettavan saataville a) sellaisen laitteen tai tietokoneohjelman tai ohjelmakäskyjen sarjan, joka on suunniteltu tai muunnettu vaarantamaan tai vahingoittamaan tietojenkäsittelyä tai tieto- tai viestintäjärjestelmän toimintaa tai murtamaan tai purkamaan sähköisen viestinnän teknisen suojauksen tai tietojärjestelmän suojauksen tai b) tietojärjestelmän toiselle kuuluvan salasanan, pääsykoodin tai muun vastaavan tiedon tai levittää

tai asettaa saataville ohjeen 1 kohdassa tarkoitetun tietokoneohjelman tai ohjelmakäskyjen sarjan valmistamiseksi, on tuomittava, jollei teosta muualla laissa säädetä ankarampaa tai yhtä ankaraa rangaistusta, vaaran aiheuttamisesta tietojenkäsittelylle sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

Rikoslain 34 luvun 9 b §:n mukaan joka aiheuttaakseen haittaa tai vahinkoa tietojenkäsittelylle tai tieto- tai viestintäjärjestelmän toiminnalle tai turvallisuudelle pitää hallussaan 9 a §:n 1 kohdan a alakohdassa tarkoitettua laitetta, tietokoneohjelmaa tai ohjelmakäskyjen sarjaa taikka b alakohdassa tarkoitettua salasanaa, pääsykoodia tai muuta vastaavaa tietoa, on tuomittava tietoverkkorikosvälineen hallussapidosta sakkoon tai vankeuteen enintään kuudeksi kuukaudeksi.

Rikoslain 36 luvun 1 §:n 2 momentin mukaan petoksesta tuomitaan myös se, joka dataa syöttämällä, muuttamalla, tuhoamalla tai poistamalla taikka tietojärjestelmän toimintaan muuten puuttumalla saa aikaan tietojenkäsittelyn lopputuloksen vääristymisen ja siten aiheuttaa toiselle taloudellista vahinkoa.

7 TIETO- JA VIESTINTÄRIKOSTEN TULEVAISUUTTA

7.1 Rikoslain 38 luvun tulevaisuudesta

Tulevaisuudessa tietoteknisen kehityksen myötä säännöksiä tullaan muuttamaan, mutta uudistaminen ei tule tuottamaan valtavasti ongelmia, koska tieto- ja viestintärikokset on keskitetty samaan rikoslain lukuun, on luvun muuttaminen helpompaa, kuin jos kaikki rikosoikeudelliset säädökset olisivat rikoslain eri luvuissa.

Rikoslain 38 luku on noin 20 viime vuoden aikana saatu säänneltyä niin pitkälle, että se vastaa nykyajan vaatimuksia ainakin rikoslajien osalta. Rikoslajeja ei ainakaan tällä hetkellä olla lisäämässä tai poistamassa. Tunnusmerkistö tulee varmasti muuttumaan sitä mukaan, kun tieto- ja viestintälakeja muutetaan. Silloin myös rangaistussäännökset tarkentuvat vastaamaan lainsäädäntöä.

Tällä hetkellä suurin puheenaihe on mahdollisen identiteettilain säätäminen. Lain valmistelu on jo aloitettu, mutta vaatii vielä oman aikansa, ennen kuin se voidaan saattaa voimaan. Myös uusi henkilötietodirektiivi on tuomassa omat muutoksensa henkilötietolakiin ja sitä kautta myös rikoslain 38 luvun 9 §:ään. Uusi pakkokeinolaki sisältää myös yksityisyyteen sekä tietoturvaan liittyviä asioita.

7.2 Uusi pakkokeinolaki tulee heikentämään tietoturvaa sekä ihmisten yksityisyydensuojaa

Pakkokeinolaki sisältyy isoon esitutkinta-, pakkokeino- ja poliisilainsäädännön kokonaisuudistukseen. Eduskunta hyväksyi lain maaliskuussa ja voimaan se tulee 1.1.2014. Uusi pakkokeinolaki on herättänyt vilkasta keskustelua, jossa ovat osin menneet sekaisin julkiset ja salaiset pakkokeinot sekä operatiivisen tiedonhankinnan eri vaiheet. Uudessa säännöksessä poliisin toimivaltuudet on kirjoitettu auki entistä selkeämmin.[189]

[189] Rautvuori 2011, s. 5.

Verkkorikoksissa toimivaltuudet ovat olleet puutteelliset. Esimerkiksi tiedon oikeudetonta kaappaamista tietojärjestelmän sisältä ei ole Suomessa kriminalisoitu, vaikka Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus sitä Suomelta on edellyttänyt. Tämän vuoksi poliisi ei voi tutkia taloudellista hyötyä tavoittelevia identiteettirikoksia silloin, kun näyttö olisi vielä olemassa.[190]

Uusia toimivaltuuksia tulevassa pakkokeinolaissa (22.7.2011/806) ovat muun muassa laite-etsintä (pakkokeinolain 8 luvun 20 - 29 §:t) ja tekninen laitetarkkailu (pakkokeinolain 10 luvun 23 - 26 §:t). Laite-etsintä erotetaan kotietsinnästä. Nykyisin tietojärjestelmien etsintä suoritetaan kotietsintänä. Laite-etsintä kohdistetaan tietokoneessa, tietojärjestelmässä tai mobiililaitteessa etsintähetkellä olevaan tietoon. Näin poliisi voi sillä hankkia tietojärjestelmistä mitä tahansa dokumentteja, kuten esimerkiksi kirjanpitoasiakirjoja. Laite-etsinnän kynnys on sama kuin kotietsinnässä: tutkittavan rikoksen enimmäisrangaistus on oltava vähintään kuusi kuukautta. Laite-etsintä voidaan toteuttaa myös etäetsintänä. Kyseessä ovat tilanteet, joissa Suomen viranomaisten oikeudenkäyttöpiiriin kuuluvan epäillyn hallussa on aineistoa, joka sattuu sijaitsemaan kolmannessa maassa jonkin globaalin jätin levyfarmilla. [191]

Toinen uusi toimivaltuus koskee poliisille annettavaa oikeutta seurata tietokoneen toimintaa. Tämä on pakkokeinolain 10 luvun 23 §:n mukaan teknistä laitetarkkailua. Poliisi saa asentaa epäillyn epäilyn tietokoneelle ohjelmiston, joka kerää ja seuraa tietoja tietokoneen tai sen ohjelmiston toiminnasta. Teknistä laitetarkkailua saa käyttää, jos tutkittavan rikoksen enimmäisrangaistus on vähintään neljä vuotta vankeutta. Viestien tunnistamistietojen ja sisällön selvittäminen ei kuulu laite-etsintään tai laitetarkkailuun. Esimerkiksi viestinnän lokitietoja ei saa etsiä päätelaitteesta laite-etsinnällä, vaan ne on haettava televalvonnalla.[192] Käytännössä tekninen laitetarkkailu antaa poliisille oikeuden tehdä salaisen tietomurron.

Laite-etsintä on julkinen pakkokeino eli siitä on ilmoitettava laitteen haltijalle. Tekninen laitetarkkailu puolestaan on salainen pakkokeino, eli se tehdään kohteen tietämättä. Salaisissa pakkokeinoissa viestintään puuttumista päättää aina tuomioistuin pakkokeinolain 10 luvun 24 §:n mukaisesti.

[190] Rautvuori 2011, s. 5.
[191] Rautvuori 2011, s. 5-7.
[192] Rautvuori 2011, s. 6.

Julkisuudessa on arvosteltu teknistä laitetarkkailua puuttumiseksi ihmisten tietoturvaan ilman selkeitä perusteluita. Teknisessä laitetarkkailussahan poliisi saa seurata tietokoneen tai sen ohjelmiston toimintaa vakoiluohjelmiston avulla. Julkisuudessa on myös epäilty, että poliisin käyttämässä vakoiluohjelmistossa on tahallaan mahdollistettu tai epähuomiossa jäänyt takaportti, joka saattaisi avata ulkopuolisille pääsyn tutkinnan kohteena olevan tahon koneelle. Mutta tämä saattaa olla hätäilyä, poliisit tietoisia siitä, että, että heidän käyttämiensä ohjelmistojen tietoturvavaatimukset ovat korkeat.[193]

7.3 Uudistuva henkilötietodirektiivi

Henkilötietodirektiivi valmisteltiin 1980-luvun tietopohjalta 1990-luvun alkupuolella. Siksi sen ajantasaistamisen tarpeista on keskusteltu jo usean vuoden ajan.[194] Euroopan Unionissa ollaan parhaillaan uudistamassa 15 vuotta sitten hyväksyttyä henkilötietodirektiiviä. Vanhassa direktiivissä vahvistettiin kaksi Euroopan yhdentymiskehityksen vanhinta tavoitetta, jotka kumpikin ovat yhä päteviä. Ensinnäkin yksilön perusoikeuksien ja vapauksien ja erityisesti tietosuojaa koskevan perusoikeuksien suojelu ja toiseksi sisämarkkinoiden toteuttaminen eli henkilötietojen vapaa liikkuvuus. Koko ajan kehittyvä tietotekniikka on kuitenkin luonut uusia haasteita henkilötietojen suojeluun ja niihin olisi kyettävä vastaamaan.[195]

Valtaosa uudistustarpeista johtuu siitä, että yritysten liiketoiminta sanoin kuin yksityisten henkilöiden vapaa-ajallaan käyttämät palvelut ovat siirtyneet verkkoon. Uuden direktiivin keskeisenä tavoitteena on yksilön oikeuksien lujittaminen. Luonnollisten henkilöiden perusoikeuksia ja erityisesti oikeutta henkilötietojen suojaan on suojattava. Myös läpinäkyvyyttä on lisättävä rekisteröidyn kannalta. On tärkeää, että rekisterinpitäjät ilmoittavat rekisteröidylle selkeästi ja läpinäkyvällä tavalla siitä, miten heidän tietojaan on kerätty ja käsitelty ja kenen toimesta, kuinka kauan, mitä tarkoitusta varten ja mitkä ovat heidän oikeutensa siinä tapauksessa, että he haluavat tutustua näihin tietoihin ja tarpeen vaatiessa oikaista tai poistaa niitä. Nykyiset säännökset eivät ole kyllin katta-

[193] Rautvuori 2011, s. 6-7.
[194] Saarenpää 2011, s. 337.
[195] KOM(2010) 609, s. 2.

via. Erityisesti on pyrittävä suojaamaan lapsia, koska he eivät välttämättä ole hyvin perillä henkilötietojen käsittelyyn liittyvistä riskeistä, oikeuksista ja seurauksista.[196]

Yksi erityisesti verkkoympäristöön liittyvä haaste on vahvistaa rekisteröidyn oikeutta tulla unohdetuksi. Tämä liittyy siihen, että rekisteröidyn tiedot tuhotaan eikä niitä enää käsitellä sen jälkeen kun niitä ei enää tarvita laissa säädetyssä tarkoituksissa. Tällainen tilanne voi olla esimerkiksi silloin, kun rekisteröity peruu suostumuksensa, jonka perusteella tietoja on käsitelty tai tietojen sallittu säilytysaika on kulunut umpeen.[197]

Myös omien tietojen valvonnan mahdollisuutta on parannettava sekä lisättävä yleisön tietoutta henkilötietojen käsittelyyn liittyvissä asioissa.. Yksilön oikeuksien lujittamiseen liittyy myös suostumuksen antamista koskevien sääntöjen selkeyttäminen. Myös arkaluonteisia tietoja on suojattava entistä paremmin. Oikeussuojakeinoja ja seuraamuksia on tehostettava. Esimerkiksi komissiolla on arvioitavana seuraamuksia koskevien voimassa olevien säännöksien vahvistamistarve.[198] Toteutuessaan tämä tuo muutoksia myös rikoslain 38 luvun 9 §:ään.

Toisena keskeisenä tavoitteena on sisämarkkinaulottuvuuden lujittaminen. Euroopan Unioniin liittyy vahva sisämarkkinaulottuvuus. Tämä tarkoittaa sitä, että on tärkeää varmistaa henkilötietojen vapaa liikkuvuus jäsenvaltioissa sisämarkkinoiden puitteissa. Tärkeänä tavoitteena on myös rikosasioissa tehtävää poliisi- ja oikeudellista yhteistyötä koskevien tietosuojasääntöjen tarkistaminen. Kansainvälisiä tiedonsiirtoja koskevien sääntöjen selkeyttäminen ja yksinkertaistaminen tuo tietosuojan globaalia ulottuvuutta.[199]

Viimeisenä tavoitteen komission tiedonannossa on tietosuojasääntöjen täytäntöönpanon valvonnan tehostaminen institutionaalisia järjestelyjä lujittamalla. Tietosuojaviranomaisilla on tietosuojasääntöjen täytäntöönpanon valvonnassa keskeinen asema. Heidän asemaa ja toimivaltuuksia tulisi lujittaa, selkeyttää ja yhdenmukaistaa. Myös tietosuojaviranomaisten keskinäistä yhteistyötä tulisi lisätä.[200] Näillä seikoilla on merkitystä esi-

[196] KOM(2010) 609, s. 5-6.
[197] Talus 2011, s. 39.
[198] KOM(2010) 609, s. 7-10.
[199] KOM(2010) 609, s. 10-17.
[200] KOM(2010) 609, s. 17-18.

merkiksi tilanteissa, joissa on kyse valtioiden rajat ylittävistä kysymyksistä kuten silloin, kun monikansallinen yritys tarjoaa samaa palvelua useassa eri jäsenmaassa.[201]

7.4 Identiteettilaki

7.4.1 Identiteettivarkaudesta

Identiteettivarkaus on arkikielen ilmaus. Identiteettiä eli henkilöllisyyttä ei voi Suomen oikeuden mukaan varastaa, koska varkaus voi kohdistua vai irtaimeen omaisuuteen (rikoslain 28.luku).[202] Ennen vanhaan ihminen saattoi esiintyä vaikkapa naapurinaan varastamalla roskiksesta hänen henkilötietonsa. Nykyaikana henkilöllisyyden varastaminen on siirtynyt verkkoon ja nyt naapuri kätevästi nappaa nämä tiedot naapurinsa Facebook -profiilista. Identiteettivarkaus on uhrille henkisesti raskas kokemus ja sen kriminalisointia on vaadittu jo pitkään.[203]

Identiteetin varastaminen on yksinkertaisesti sitä, että joku ottaa luvatta toisen ihmisen identiteetin, tätä nykyä nimenomaan digitaalisen identiteetin ja esiintyy tämän avulla toisena. Yleisin syy varkauteen on käyttää toisen hyvää identiteettiä oman huonon identiteetin asemesta, jotta saisi erilaisia etuja, luottoa, luottokortteja, voisi varastaa rahaa uhrin tililtä, perustaa uusia tilejä, hankkia työtä, asunnon tai käyttää muulla tavalla uhrin hyvää nimeä. Väärän identiteetin esittäjä voi toimia pitkään uhrin tietämättä siitä mitään, aina tämä ei edes huomaa identiteettiään varastetun, hänellähän on edelleen nimensä ja tunnuksensa.[204]

Henkilöllisyysvarkaus on identiteettivarkauden osajoukko, jossa teko kohdistuu nimenomaan henkilöön ja jossa kerättävä tieto on henkilötieto. Tietoverkossa ”identiteetti” voi kuitenkin olla henkilötiedon lisäksi mikä tahansa tunniste, jota käytetään joko vain erottelemaan kokonaisuudet toisistaan tai osoittamaan, että 1) tunnisteen haltija on se, joksi hän itseään väittää tai että 2) tunnisteen haltijalla on oikeus päästä käsiksi tietoon tai

[201] Talus 2011, s. 40.
[202] Tavi 2011, s. 60.
[203] Männikkö 2010, s. 9.
[204] Heinonen 2001, s. 202.

palveluun, johon identiteetin todellisella haltijallakin on oikeus. Identiteettivarkauksilla aiheutetusta vahingosta ei ole saatavilla yhteismitallista tilastotietoa.[205]

Identiteettivarkaudet ovat tiiviisti kytköksissä kansainväliseen rikollisuuteen. Esimerkiksi internetissä palveluntarjoajat toimivat ympäri maailmaa, jolloin pelkällä kansallisella lainsäädännöllä voi olla vaikeaa puuttua nouseviin ongelmiin. Euroopan unionissa valmistellaan uutta eurooppalaista strategiaa ja lainsäädösehdotuksia identiteetin hallintaan liittyvissä kysymyksissä.[206]

7.4.2 Tarvitaanko identiteettilakia?

Kansainvälisesti, varsinkin Yhdysvalloissa, ovat muodostuneet vakavaksi ongelmaksi. Useissa maissa on jo ryhdytty toimenpiteisiin identiteettivarkauksien estämiseksi. Oletettavissa on, että tilanne heikkenee myös Suomessa, joten syytä on pohtia identiteettivarkauksien ennalta estäviä kansallisia ja kansainvälisiä toimia.[207]

Jo nyt Suomessa on tehty identiteettivarkauksia ja nykytilanteessa poliisi on usein voimaton niiden kohdalla. Usein käy niin, että kun identiteettivarkauden uhri tulee poliisiasemalle tekemään rikosilmoitusta, joudutaan toteamaan, ettei mitään ole tehtävissä lain keinoin.[208]

Ihmiset osallistuvat tietoverkon eri palveluihin, keskusteluryhmiin, peleihin ja vastaaviin vaihtelevista syistä. Digitaalinen identiteetti olipa se itse rakennettu ja hyväksytty tai muiden rakentama ja myös tunnustama, näyttelee osallistujille merkittävää osaa. Tietoverkon palveluissa ei useinkaan ole ketään takaamassa osapuolten esittämien identiteettien aitoutta, ei myöskään ole käytössä identiteettien luotettavuutta ilmaisevia standardeja eikä näillä tarkoiteta tässä henkilötunnusta.[209]

Identiteettivarkauden kriminalisointi on mielestäni välttämätöntä. Nykyinen lainsäädäntö ei ole pysynyt kehityksen mukana. Mutta samalla myös kansalaisten olisi oltava enemmän varuillaan siitä, mihin he tietojaan antavat.

---

[205] Henkilöllisyyden luomista koskeva hanke (identiteettiohjelma). Työryhmän loppuraportti 2010, s. 48.
[206] Tavi 2011, s. 60.
[207] Henkilöllisyyden luomista koskeva hanke (identiteettiohjelma). Työryhmän loppuraportti 2010, s. 15.
[208] Castrén 2010, s. 15.
[209] Heinonen 2001, s. 188.

Pelkkä kriminalisointi ei kuitenkaan riitä. Identiteettivarkauden torjuntaan ei ole yhtä ainoata keinoa. Kriminalisointikin on usein vain viimekätinen keino. Tästä johtuen tarvittaisiin toimintaohjelma siitä, miten henkilötietoja voitaisiin parhaiten suojata, estää niiden hyödyntäminen, puuttua ja katkaista luvaton käyttö sekä auttaa henkilöitä palautumaan tällaisesta tapahtumasta.[210] Identiteettivarkauksilla voidaan loukata useita eri perusoikeuksia, kuten oikeutta omaisuuden tai yksityiselämän suojaan. Myös tämän takia identiteettilaki olisi säädettävä.[211]

7.4.3 Identiteettiohjelma

Sisäasiainministeriö asetti 29.10.2008 hankkeen valtion vahvistaman henkilöllisyyden luomista koskevien menettelytapojen sekä henkilöllisyyttä koskevan lainsäädännön laatimiseksi. Hankkeessa laadittiin kansallinen identiteettiohjelma, joka sisältää kokonaisvaltaisen suunnitelman valtion tehtävistä henkilöllisyyden luomisessa yhteiskunnassa sekä keinoista, joilla valtio tulevaisuudessakin suojaa kansalaisten henkilöllisyyden sekä perinteisessä että sähköisessä toimintaympäristössä. Työryhmän toimikausi oli 28.10.2008 - 26.1.2011.[212]

Raportti on esiselvitys, jossa käytännön näkökulmasta tuodaan esiin suurimpia identiteettivarkauksiin liittyviä oikeusturvaongelmia. Työryhmä ei ota kantaa siihen, tulisiko identiteettivarkaus kriminalisoida. Pykälien mahdollinen laatiminen jätetään oikeusministeriön ja eduskunnan harteille. Aiheen tausta on hyvin laaja. Identiteettivarkaudet kun liittyvät rikosoikeuteen, tietojenvaihtoon ja perusoikeuksiin.[213] Työryhmä katsoi, että lainsäädäntö on jo pääosin kunnossa, koska identiteettitiedon käyttäminen väärin hyödyn hankkimiseksi tai kohteen vahingoittamiseksi on kriminalisoitu, samoin kuin toisena henkilönä esiintyminen. Mutta pohdittavaa kuitenkin riittää siinä, että pitäisikö yksityiselle toisena esiintyminen säätää rikokseksi ainakin tapauksissa, joissa henkilö rekis-

[210] Castrén 2010, s. 15.
[211] Henkilöllisyyden luomista koskeva hanke (identiteettiohjelma). Työryhmän loppuraportti 2010, s. 75.
[212] Henkilöllisyyden luomista koskeva hanke (identiteettiohjelma). Työryhmän loppuraportti 2010, s. 13.
[213] Castrén 2010, s. 15.

teröityy verkkopalveluun toisen nimissä tai hakee varmennetta yksityiseltä palveluntarjoajalta.[214]

Identiteettiohjelmassa kuvataan kattavasti henkilöllisyyden luomiseen liittyvä nykytila, kehitysnäkymät ja riskit sekä tuoda esille johtopäätökset ja toimenpidesuositukset. Kansainvälisesti identiteettivarkaudet ovat muodostuneet vakavaksi ongelmaksi.[215]

Useat maat ovat ryhtyneet mittaviin toimenpiteisiin identiteettivarkauksien estämiseksi. Oletettavissa on, että tilanne heikkenee myös Suomessa ja myös Suomessa on syytä pohtia identiteettivarkauksien ennalta estäviä kansallisia ja kansainvälisiä toimia. Työryhmän tehtävänä oli käytännönläheisesti kansalaisnäkökulmasta kartoittaa mahdollisia ongelmatilanteita koskien identiteettivarkautta, sen tutkimista ja uhrin asemaa. Usealta taholta on ehdotettu identiteettivarkauksien kriminalisointia, mutta tarkempaa analyysia kokonaisuudesta ei ole tehty. Raportissa on määritelty erilaisia tekotyyppejä ja tuotu esiin ongelmakohtia mahdollisten jatkotoimien pohjaksi ja tueksi. Lisäksi on pohdittu identiteettivarkauksien torjuntakeinoja. Uhrin asemaan on kiinnitetty erityistä huomiota.[216] Identiteettityöryhmä vaatiikin identiteettivarkauden uhreille lisää apua. Ensimmäisenä pitäisi laatia ohje varkauden jälkeisistä toimista[217].

Identiteettivarkauksien merkitys nousee jatkuvasti esille alan toimijoiden keskuudessa. Toistaiseksi niiden uhrien määrä ei ole ollut hälyttävän suuri, mutta seuraukset yksilötasolla voivat olla hyvinkin vakavia. Jatkossa identiteettivarkauksien määrä voi nousta huomattavastikin, ja siksi on tärkeää ryhtyä ripeisiin toimiin niiden ehkäisemiseksi ja seurausten minimoimiseksi. Erityisen tärkeää on sulkea lainsäädäntöön ja erilaisiin käytänteisiin liittyvät aukot, joita voidaan pyrkiä käyttämään hyväksi. Työryhmän loppupäätelmät siitä, että työtä on edelleen jatkettava, ovat siksi oikeaan osuvia.[218]

[214] Männikkö 2011, s. 31.
[215] Henkilöllisyyden luomista koskeva hanke (identiteettiohjelma). Työryhmän loppuraportti 2010, s. 15.
[216] Henkilöllisyyden luomista koskeva hanke (identiteettiohjelma). Työryhmän loppuraportti 2010, s. 15.
[217] Männikkö 2011, s. 31.
[218] Henkilöllisyyden luomista koskeva hanke (identiteettiohjelma). Työryhmän loppuraportti 2010, s. 112-113.

JOHTOPÄÄTÖKSET

Tietotekniikkarikos määritellään rangaistavaksi teoksi, jonka kohteena, välikappaleena tai tekoympäristönä on tietojärjestelmä siihen kuuluvine laitteineen ja jonka tekeminen ja / tai rikosprosessuaalinen käsittely välittömästi edellyttää tietoteknistä erityistietämystä. Tietotekniikkarikoksissa on rangaistavaa vain se, mikä on rangaistavaksi säädettyä

Tieto- ja viestintärikokset ovat hyvin kansainvälisiä rikoksia. Tästä johtuen kansainvälistä yhteistyötä on harjoitettu paljon ja työryhmät ovat esittäneet monenlaisia suosituksia ja lakien harmonisoimishankkeita.

Tieto- ja viestintärikoksia säätelee Suomen rikoslain 38 luku. Tieto- ja viestintärikoksia on myös muualla rikoslaissa, mutta kaikki uudet tietoteknisen kehityksen tuomat muutokset on koottu rikoslain 38 lukuun. Jos jo olemassa oleviin rikostunnusmerkkeihin on tullut uusia, tietotekniikkarikoksiin liittyviä muotoja, on järkevämpää ollut uudistaa jo olemassa olevia säädöksiä.

Tietoteknisen kehityksen ja direktiivien myötävaikutuksella on rikoslain 38 lukua uudistettu useita kertoja. Suurin muutos tapahtui vuonna 1995, kun tieto- ja viestintärikokset koottiin samaan lukuun. Suomessa ei haluttu lähteä rakentamaan uutta erillistä atk-lakia, vaan tieto- ja viestintärikokset koottiin jo olemassa olevaan rikoslakiin.

Sen jälkeen lukua on uudistettu viisi kertaa, lakimuutokset on vahvistettu vuosina 1999, 2000, 2001, 2007 ja 2011. Viimeisen lakimuutoksen jälkeen rikoslain 38 luku käsittää 12 §:ää.

Tieto- ja viestintärikosten määrä on noussut koko ajan. Vuonna 2010 rikosilmoituksia tehtiin rikoslain 38 luvun osalta 760 kappaletta. Mutta harmittavaa on huomata se, että samalla kun rikosten määrä on noussut, tuomiot yleensä ovat lieviä sakkorangaistuksia. Lisäksi epäillään, että tietotekniikkarikokset ovat piilorikollisuutta. Asianomistajat ovat varsin haluttomia ilmoittamaan rikoksista poliisille. Tämä johtuu taas siitä, että henkilö ei edes tiedä joutuneensa rikoksen uhriksi, ei haluta muiden tietävän yrityksen tietoturvaongelmista tai saatetaan olla sitä mieltä, että vaikka rötöstelijä saadaan kiinni, niin vahinkoa ei saada takaisin.

Tulevaisuudessa tietoteknisen kehityksen myötä säännöksiä tullaan muuttamaan, mutta uudistaminen ei tule tuottamaan valtavasti ongelmia, koska tieto- ja viestintärikokset on keskitetty samaan rikoslain lukuun, on luvun muuttaminen helpompaa, kuin jos kaikki rikosoikeudelliset säädökset olisivat rikoslain eri luvuissa.

Tällä hetkellä suurin puheenaihe on identiteettivarkauden kriminalisoiminen. Nykyajan lainsäädäntö ei ole ajan tasalla ja identiteettivarkaus ei ole kriminalisoitu. Nyt ollaan suunnittelemassa oma erityislainsäädäntö, joka kriminalisoisi identiteettivarkauden. Kyseessä on identiteettilain mahdollinen säätäminen.