SUOMALAISEN LAKIMIESYHDISTYKSEN JULKAISUJA
A-sarja N:o 258

Antti Pihlajamäki

TIETOJENKÄSITTELYRAUHAN RIKOSOIKEUDELLINEN SUOJA

Datarikoksia koskeva sääntely Suomen rikoslaissa

Tietojenkäsittelyrauhan rikosoikeudellinen suoja

SUOMALAISEN LAKIMIESYHDISTYKSEN JULKAISUJA
A-sarja N:o 258

Antti Pihlajamäki

Tietojenkäsittelyrauhan rikosoikeudellinen suoja

Datarikoksia koskeva sääntely Suomen rikoslaissa

Yliopistollinen väitöskirja, joka Helsingin yliopiston oikeustieteellisen tiedekunnan suostumuksella esitetään julkisesti tarkastettavaksi yliopiston päärakennuksen pienessä juhlasalissa perjantaina 1.10.2004 kello 12.

With an English Summary

SUOMALAINEN LAKIMIESYHDISTYS • HELSINKI

Tilausosoite
Suomalainen Lakimiesyhdistys
Kasarmikatu 23 A 17
00130 Helsinki
p. (09) 6120 300
f. (09) 604 668
sly@lakimies.org
www.lakimies.org

Verkkokirjan ISBN 978-951-855-530-1

ISSN 0356-7206
ISBN 951-855-233-9

Gummerus Kirjapaino Oy, Jyväskylä 2004

Aluksi

Tietotekniikkarikoksia koskeva tutkimustyö on osoittautunut varsin haastavaksi ja vaikeaksikin. Kun alkuvuodesta 1992 ryhdyin perehtymään atk-rikoksiin – niin kuin silloin sanottiin – oli tietotekninen ympäristö aivan toisenlainen kuin nykyään. Tietoverkot olivat vasta kehityksensä alussa, viruksia ja muita haittaohjelmia ei juuri tunnettu eikä sähköpostilla ollut sanottavaa merkitystä viestintävälineenä. Tavallisin tietojärjestelmä oli yksittäinen tietokone. Nykyään Internetistä on tullut verkkojen verkko, jolla on satoja miljoonia käyttäjiä ympäri maailman, haittaohjelmat tekevät tuhojaan ja sähköpostin käyttökelpoisuus on vaarantunut roskapostitulvan seurauksena. Tekninen kehitys on asettanut suuria haasteita lainsäätäjälle, jonka toiminnan seurauksena muun muassa kriminalisointien määrä on lisääntynyt ja lisääntyy. Oikeudenhoitoviranomaisten kyky seurata rikoksentekijöiden oivalluksia on kovalla koetuksella.

Kehityksen nopeudesta ja jatkuvuudesta johtuu, että tietotekniikkarikoksia koskevaa tutkimusta on mahdotonta saada koskaan täysin valmiiksi. Jossain kohdassa työ on katkaistava. Tämä työ on katkaistu helmikuun 2004 lopussa, jonka ajankohdan jälkeistä lainsäädäntöä ja käytäntöä ei ole enää otettu huomioon.

Väitöskirjatyön loppuun saattaminen ei koskaan voi olla yksin kirjoittajan ansiota. Työn etenemisen kannalta aivan välttämätöntä taloudellista tukea olen saanut *Jenny ja Antti Wihurin rahastolta, Aili ja Brynolf Honkasalon rahastolta, Suomen Kulttuurirahastolta, Kansleri Antti Tulenheimon muistorahastolta, sisäasiainministeriön poliisiosastolta* sekä *Valtakunnansyyttäjänvirastolta.* Kiitokset kuuluvat myös oikeustieteen tohtori *Matti Joutsenelle,* joka on tarkistanut englanninkielisen yhteenvedon kieliasun, ja *Suomalaiselle Lakimiesyhdistykselle,* joka on ottanut työn kustannettavakseen. Lisäksi työn aloittamiseen ja valmistumiseen ovat tavalla tai toisella myötävaikuttaneet lukuisat henkilöt, joista jokaista on mahdotonta tässä mainita. Kaikkia lämpimästi kiittäen haluan kuitenkin tuoda muutaman erikseen esille.

Ilman silloisen syyttäjäkollegani, nykyisen apulaisoikeuskansleri *Jaakko Jonkan* patistelua 1980- ja 1990-luvun taitteessa tuskin olisin koskaan ryhtynytkään jatkamaan 1970-luvulla lisensiaatintutkinnon suorittamiseen keskeytyneitä jatko-opintojani. Professori *Raimo Lahti* on työni ohjaajana osoittanut hämmästyttävää pitkämielisyyttä ja sinnikkyyttä, kun hän oman uskoni oltua jo moneen kertaan hiipumassa on yhä uudelleen ja uudelleen innostanut minua jatkamaan työtäni. Melkoista pitkämielisyyttä myös professori *Dan Frändeltä* ja professori *Martti Majaselta* on vaatinut esitarkastajan tehtävän lähes kym-

menvuotinen hoitaminen. Hyvän ystäväni ja työtoverini, nykyisen apulaisvaltakunnansyyttäjä *Jorma Kalskeen* ajoittain painostusta lähennellyt kannustaminen ei ole ollut vailla merkitystä. Keskusrikospoliisin entisen apulaispäällikön *Matti Tenhusen* kanssa käymäni kymmenet keskustelut yhteisillä matkoillamme eri puolilla Eurooppaa ovat olleet todella arvokkaita. Lainsäädäntöjohtaja *Jan Törnqvistin* myötävaikutuksella olen päässyt perehtymään ja osallistumaan tietotekniikkarikoksiin liittyvään lainvalmisteluun ja kansainväliseen yhteistyöhön. Lankoni, dosentti, valtiotieteen tohtori *Sampsa Saralehto* on kiitettävästi huolehtinut siitä, että työn keskeneräisyys ei ole päässyt unohtumaan. Dosentti, lääketieteen ja kirurgian tohtori *Martti Nurmen* erinomaiset kirurgin taidot ovat mahdollistaneet täysipainoisen paneutumiseni työn viimeistelyyn.

Läheinen ja tuloksellinen yhteistyö poliisin ja erityisesti keskusrikospoliisin tietotekniikkarikosryhmän kanssa on auttanut valtavasti käytännön ja teorian yhteensovittamisessa. Tärkeää on luonnollisesti ollut myös se, että tietotekniikkarikosten avainsyyttäjänä olen saanut hoitaa useita kiinnostavia tietotekniikkarikosjuttuja. Niin oikeussaleissa kuin niiden ulkopuolellakin on virinnyt antoisia keskusteluja sekä myötä- että vastapuolia edustaneiden lakimiesten ja muiden asiantuntijoiden kanssa.

Työtoverini Turun syyttäjänvirastossa ovat suhtautuneet kiitettävän ymmärtäväisesti niihin hankaluuksiin, joita tutkimustyöstä on esimerkiksi useina virkavapauksina virkani hoitamiselle aiheutunut.

Perheelle tämä nyt päättymässä oleva ajanjakso on usein ollut raskasta tai erittäin raskasta. Siitä huolimatta *Marjo-Riitta* ja *Antti-Veikko* ovat hämmästyttävää kärsivällisyyttä osoittaen monesti jaksaneet suhtautua työn valmistumiseen minua optimistisemmin ja pitäneet osaltaan huolta siitä, että luopumisajatukset ovat toistuvasti saaneet väistyä.

Turussa 4. kesäkuuta 2004

Antti Pihlajamäki

Sisällysluettelo

Lähteet

Aarnio, Aulis
Laintulkinnan teoria. Juva 1989.

Aikio, Annukka (toim.)
Uusi sivistyssanakirja. Keuruu 1974.

Angeles, Peter A.
The HarperCollins Dictionary of Philosophy. Second edition, New York 1992.

Anttila, Inkeri – Heinonen, Olavi
Rikosten lajit. Helsinki 1972.

Association Internationale de Droit Pénal
Recommendations of the XV International Congress on Penal Law on Computer Crimes and Other Crimes against Information Technology. Rio de Janeiro, Sept. 4–10, 1994. RIDP 1–2/1995. (AIDP:n päätöslauselma)

Bassiouni, M. Cherif
Draft Statute International Tribunal. Nouvelles Études Pénales 10, 1993.

Bigelow, Robert
Computer Security, Crime and Privacy in the USA – a Status Report. Part III. Computer Crime. The Computer Law and Security Report 1993:1.

Brenner, Susan W. – Goodman, Marc D.
Cybercrime: The Need to Harmonize National Penal and Procedural Laws (International Society for the Reform of Criminal Law 16th Annual Conference. Technology and its effects on Criminal Responsibility Security and Criminal Justice. Dec. 6–10, 2002).

Bright, Roy
Smart Cards: Principles, Practice, Applications. Chichester 1996.

Caelli, William – Longley, Dennis – Shain, Michael
Information Security Handbook. Stockton Press 1991.

Clarke, Susan – Crisp, Randy – Duncan, Michael
Counterfeit Card Fraud. RCMP Gazette Vol. 57, No. 10, 1995 s. 2 ss.

Council of Europe
Computer-related Crime: Recommendation no. R(89) on computer-related crime and final report of the European Committee on Crime Problems. Strasbourg 1989. (EN:n raportti 89)

Council of Europe
Final Activity Report and Recommendation concerning Problems of Criminal Procedural Law connected with Information Technology. Strasbourg 1995. (EN:n raportti 95)

Cornils, Karin
Internetissä tehtyjen rikosten paikallistaminen. Lakimies 1999 s. 705 ss.

Dolcini, E. – Marinucci, G – Pecorella, C.
Computer crimes and other crimes against information technology. Julkaisussa Introduction to the Debate by Centro Nazionale di Prevenzione e Difesa Sociale/CNPDS. Milano 1994. (Dolcini ym.)

Durham, Cole
The Emerging Structures of Criminal Information Law: Tracing the Contours of a New Paradigm. Report for the AIDP-Colloquium. RIDP 1–2/1993.

Euroopan komissio
Ehdotus neuvoston puitepäätökseksi rasismin ja muukalaisvihan vastaisesta toiminnasta. KOM(2001) 664 lopullinen.
Euroopan komissio
Ehdotus neuvoston puitepäätökseksi tietojärjestelmiin kohdistuvista hyökkäyksistä. KOM(2002) 173 lopullinen.
Euroopan komissio
Turvallisempaan tietoyhteiskuntaan tietojärjestelmien turvallisuutta parantamalla ja tietokonerikollisuutta ehkäisemällä. Tiedonanto neuvostolle, Euroopan parlamentille, talous- ja sosiaalikomitealle sekä alueiden komitealle. KOM (2001) 890 lopullinen.
Euroopan unionin neuvosto
Neuvoston puitepäätös 28.5.2001 muihin maksuvälineisiin kuin käteisrahaan liittyvien petosten ja väärennysten torjunnasta (2001/413/YOS)
European Communities
Council Decision in the Field of Security of Information Systems. 92/242/EEC.
Fites, Philip – Johnston, Peter – Kratz, Martin
The Computer Virus Crisis. New York 1989. (Fites ym.)
Frey, Silvia
Computerkriminalität in eigentums- und vermögensstrafrechtlicher Sicht. München 1987.
Frigerio, Claudio G.
The new Computer Virus Article in the Swiss Penal Law. 2nd International Conference on Computer Crime. INTERPOL. Lyon/France, May 9–10, 1996.
Frände, Dan
Allmän straffrätt. En introduktion. Helsingfors 1994. (Straffrätt)
Frände, Dan
Brottets grundelement. Helsingfors 1999. (Grundelement)
Greve, Vagn
Edb-strafferet. 2. rev. udg. København 1986. (Greve)
Greve, Vagn – Nielsen, Gorm Toftegaard – Jensen, Asbjørn
Kommenteret straffelov. Speciel del. 6. omarbejdede udgave, Gylling 1998. (Greve ym.)
Gutiérrez Francés, María Luz
Computer Crimes and Other Crimes against Information Technology in Spain. RIDP 1–2/1993.
Haft, Fritjof
Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG). Teil 2: Computerdelikte. NStZ 1987.
Hallituksen esitys n:o 63/1972 vp laiksi rikoslain täydentämiseksi eräillä yksityiselämän suojan loukkaamista koskevilla rangaistussäännöksillä. (HE 63/1972)
Hallituksen esitys n:o 49/1986 vp henkilörekisterilaiksi ja siihen liittyviksi laeiksi. (HE 49/1986)
Hallituksen esitys n:o 58/1988 vp virkarikoslainsäädännön uudistamisesta. (HE 58/1988)
Hallituksen esitys n:o 66/1988 vp rikoslainsäädännön kokonaisuudistuksen ensimmäisen vaiheen käsittäviksi rikoslain ja eräiden muiden lakien muutoksiksi. (HE 66/1988)
Hallituksen esitys n:o 40/1990 vp rikosten yhtymistä koskevan lainsäädännön uudistamiseksi. (HE 40/1990)
Hallituksen esitys n:o 161/1990 vp laeiksi yksinoikeudesta integroidun piirin piirimalliin sekä tekijänoikeuslain, oikeudesta valokuvaan annetun lain ja patentti- ja rekisterihallituksesta annetun lain muuttamisesta. (HE 161/1990)
Hallituksen esitys n:o 43/1991 vp yksilöiden suojelua henkilötietojen automaattisessa tietojenkäsittelyssä koskevan yleissopimuksen eräiden määräysten hyväksymisestä. (HE 43/1991)

Hallituksen esitys n:o 211/1992 vp laiksi tekijänoikeuslain ja tekijänoikeuslain muuttamisesta annetun lain voimaantulosäännöksen 2 momentin muuttamisesta. (HE 211/1992)
Hallituksen esitys n:o 61/1993 vp kansainvälistä oikeusapua rikosasioissa koskevaksi lainsäädännöksi. (HE 61/1993)
Hallituksen esitys n:o 94/1993 vp rikoslainsäädännön kokonaisuudistuksen toisen vaiheen käsittäviksi rikoslain ja eräiden muiden lakien muutoksiksi. (HE 94/1993)
Hallituksen esitys n:o 22/1994 vp telekuuntelua ja -valvontaa sekä teknistä tarkkailua koskevaksi lainsäädännöksi. (HE 22/1994)
Hallituksen esitys n:o 57/1994 poliisilaiksi ja eräiksi siihen liittyviksi laeiksi. (HE 57/1994)
Hallituksen esitys n:o 9/1995 vp laiksi pakkokeinolain 5 a luvun 2 §:n muuttamisesta. (HE 9/1995)
Hallituksen esitys n:o 42/1995 vp eräiden rikoslain kokonaisuudistuksen toiseen vaiheeseen liittyvien lakien muutoksiksi. (HE 42/1995)
Hallituksen esitys n:o 38/1997 vp laiksi rikoslain 37 luvun muuttamisesta. (HE 38/1997)
Hallituksen esitys n:o 4/1999 vp laiksi rikoslain muuttamisesta. (HE 4/1999)
Hallituksen esitys n:o 146/2000 vp laeiksi tietoyhteiskunnan palvelujen suojasta sekä rikoslain 38 luvun ja eräiden viestintälakien muuttamisesta. (HE 146/2000)
Hallituksen esitys n:o 44/2002 vp rikosoikeuden yleisiä oppeja koskevan lainsäädännön uudistamiseksi. (HE 44/2002)
Hallituksen esitys n:o 2/2003 vp laiksi rikoslain muuttamisesta. (HE 2/2003)
Hannula, Antti
RahaSampo. Tietovuodon tarina. Hämeenlinna 1989.
Hannula, Antti – Siilasmaa, Risto
Mikrojen tietoturva. Jyväskylä 1991.
Heinonen, Olavi – Koskinen, Pekka – Lappi-Seppälä, Tapio – Majanen, Martti – Nuotio, Kimmo – Nuutila, Ari-Matti – Rautio, Ilkka
Rikosoikeus. Oikeuden perusteokset. Toinen, uudistettu painos. Juva 2002. (viittaukset ao. kirjoittajan nimellä + Rikosoikeus)
Helminen, Klaus
Förundersökning och tvångsmedel. Helsingfors 1992.
Hilpinen, Risto
Mitä on tieto? ss. 13–37 teoksessa Filosofia. Käsitteellisen ajattelun perusteita (toim. Juha Räikkä). Kuopio 1997.
Hintikka, Kari
Tieto – neljäs tuotannontekijä. Tehtaasta televirtuaalisuuteen. Helsinki 1993.
Honkasalo, Brynolf
Suomen rikosoikeus. Erityinen osa II. Helsinki 1960. (Erityinen osa II)
Honkasalo, Brynolf
Suomen rikosoikeus. Erityinen osa I 2. Varallisuusrikokset. Helsinki 1964. (Erityinen osa I 2)
Honkasalo, Brynolf
Suomen rikosoikeus. Yleiset opit, ensimmäinen osa. Toinen painos, Helsinki 1965. (Yleiset opit I)
Honkasalo, Brynolf
Suomen rikosoikeus. Yleiset opit, toinen osa. Toinen painos, Helsinki 1967. (Yleiset opit II)
Hornby, A. S. – Gatenby, E. V. – Wakefield, H.
The Advanced Learner's Dictionary of Current English. Second edition, fourteenth impression, London 1970.
Jareborg, Nils
Brotten I. Stockholm 1984. (Brotten I)

Jareborg, Nils
Essays in Criminal Law. Helsingborg 1988. (Essays)
Jareborg, Nils
Computer Crimes and Other Crimes against Information Technology in Sweden. RIDP 1–2/1993. (RIDP 1–2/93)
Jokela, Antti – Lahti, Raimo – Mattila, Heikki E. S. (toim.)
Encyclopaedia Iuridica Fennica. Neljäs osa. Rikos- ja prosessioikeus. Helsinki 1995. (EIF IV)
Jonkka, Jaakko
Rikosasiain oikeudenkäyntimenettelyn uudistamisesta. Lakimies 1994 ss. 727–741.
Järvinen, Petteri
Internet. Verkkojen verkko. Opas PC-käyttäjälle. Juva 1995. (Opas)
Järvinen, Petteri
Windows 98. Käyttäjän käsikirja. Jyväskylä 1998. (Windows 98)
Järvinen, Petteri
Tietomurron yrityskin on rikos. Helsingin Sanomat 27.4.2003. (HeSa)
Järvinen, Petteri
Porttiskannaus voi käydä kalliiksi. Tietokone 6–7/2003. (Tietokone)
Jääskeläinen, Petri
Syyttäjä tuomarina. Vammala 1997.
Karvonen, Erkki
Yleisönosastokirjoitus. Helsingin Sanomat 25.4.2000.
Kaspersen, Henrik W. K.
Implementation of Recommendation No. R (89) 9 on computer-related crime. Amsterdam 1997.
Kiviniemi, Pekka
Oikeutetusta puuttumisesta luottamukselliseen viestiin. Sähköpostiviesti ja muut viestit. Turku 2000.
Kuopus, Jorma
Hallinnon lainalaisuus ja automatisoitu verohallinto: oikeustieteellinen tutkimus kansalaisen oikeusturvasta teknistyvässä valtionhallinnossa. Helsinki 1988.
Küchler, Markus
Dataintrång – Om personlig integritet och bevisfrågor. IRI-rapport 2000:1. Stockholm 2000.
Laakso, Seppo
Oikeudellisesta sääntelystä ja päätöksenteosta. Helsinki 1990.
Lahti, Raimo
Lainkonkurrenssista. Lakimies 1968, ss. 709–737. (LM 68)
Lahti, Raimo
Rikoslain kokonaisuudistuksen ensimmäinen vaihe: varallisuus- ja talousrikossäännökset I–III. Lakimies 1991, ss. 258–290, 873–901 ja 1168–1201. (LM 91)
Lahti, Raimo
Kansainvälistyvä rikosoikeus – ajankohtaisia kehityspiirteitä ja ongelmia. Teoksessa Asianajajan työkentältä. Helsinki 1994. (Kansainvälistyvä rikosoikeus)
Lahti, Raimo
Perusoikeusuudistus ja rikosoikeus. Lakimies 1996, ss. 930–939. (LM 96)
Lahti, Raimo
Rikoslain kokonaisuudistusta 30 vuotta – entä nyt? Lakimies 2001, ss. 718–725. (LM 01)
Laine, Timo
Yrityssalaisuusrikokset – totta vai tarua? Poliisipäällystön tutkinto nro 1. Poliisiammattikorkeakoulu 2000.

Lakivaliokunnan lausunto n:o 10/2001 vp hallituksen esityksestä laeiksi tietoyhteiskunnan palvelujen suojasta sekä rikoslain 38 luvun ja eräiden viestintälakien muuttamisesta. (LaVL 10/2001)

Lakivaliokunnan mietintö n:o 6/1990 vp rikoslainsäädännön kokonaisuudistuksen ensimmäisen vaiheen käsittäväksi rikoslain ja eräiden muiden lakien muutoksiksi. (LaVM 6/1990)

Lakivaliokunnan mietintö n:o 22/1994 vp rikoslainsäädännön kokonaisuudistuksen toisen vaiheen käsittäviksi rikoslain ja eräiden muiden lakien muutoksiksi. (LaVM 22/1994)

Lakivaliokunnan mietintö n:o 2/1999 vp hallituksen esityksestä laiksi rikoslain muuttamisesta. (LaVM 2/1999)

Lakivaliokunnan mietintö n:o 28/2002 vp hallituksen esityksestä rikosoikeuden yleisiä oppeja koskevan lainsäädännön uudistamiseksi. (LaVM 28/2002)

Lanzi, Alessio
Les crimes informatiques et d'autres crimes dans le domaine de la technolgie informatique en Italie. RIDP 1–2/1993.

Lappi-Seppälä, Tapio
ks. Heinonen ym., Rikosoikeus.

Lehtimaja, Lauri
Taloudellinen rikollisuus I (moniste). 1979. (Taloudellinen rikollisuus)

Lehtimaja, Lauri
Rikoslaki ja kansainvälinen kriminaalipolitiikka. Lakimies 1986 ss. 208–222. (LM 86)

Lehtimaja, Lauri
Eurooppalaisesta atk-rikospolitiikasta. Teoksessa Rikosoikeudellisia kirjoitelmia VI, Vammala 1989. (Atk-rikospolitiikasta)

Lehtonen, Asko
Veropetoksesta. Jyväskylä 1986. (Veropetos)

Lehtonen, Asko
Kriminalisering av tillverkning och spridning av datavirus. Nätets juridik ss. 44–52 (red. Ari Koivumaa). Nordisk årsbok i rättsinformatik 1999. (Datavirus)

Lehtonen, Asko
Straffrättslig jurisdiktion över Internet-brott. Lapplands universitet. Juridiska fakulteten. Rovaniemi 2001. (Jurisdiktion)

Liikennevaliokunnan mietintö n:o 8/2001 vp hallituksen esityksestä laeiksi tietoyhteiskunnan palvelujen suojasta sekä rikoslain 38 luvun ja eräiden viestintälakien muuttamisesta. (LiVM 8/2001)

Majanen, Martti
Ks. Heinonen ym., Rikosoikeus.

Martin, Elisabeth A. (toim.)
A Concise Dictionary of Law. Second edition. Oxford ym. 1990.

Matikkala, Jussi
Tahallisuuden alimmasta asteesta. Lakimies 1992 ss. 962–980. (LM 92)

Matikkala, Jussi
HIV-infektio, seksi ja rikosoikeudellinen vastuu. Helsinki 1995. (Vastuu)

Matikkala, Jussi
Näkökohtia rikosoikeuden yleisiä oppeja koskevan lainsäädännön uudistamiseksi annetusta HE 44/2002:sta. Rikosoikeudellisia kirjoituksia VII ss. 215–230. Vammala 2003. (Näkökohtia)

Möhrenschlager, Manfred
Computer Crimes and Other Crimes against Information Technology in Germany. RIDP 1–2/1993.

Niiniluoto, Ilkka
Informaatio, tieto ja yhteiskunta. Filosofinen käsiteanalyysi. 5., täydennetty painos. Helsinki 1996.

Nilsson, Hans G.
Databrottslighet – en europeisk angelägenhet. SvJT 1990. (SvJT 90)
Nilsson, Hans G.
The Activities of the Council of Europe in the Field of Computer Crime. Teoksessa Information Technology Crime. National Legislations and International Initiatives. Köln ym. 1994. (Activities)
Nuotio, Kimmo
Ks. Heinonen ym., Rikosoikeus.
Nuutila, Ari-Matti
Rikosoikeudellinen huolimattomuus. Jyväskylä 1996. (Huolimattomuus)
Nuutila, Ari-Matti
Rikoslain yleinen osa. Jyväskylä 1997. (Rikoslaki)
Nuutila, Ari-Matti
Ks. Heinonen ym., Rikosoikeus.
Nyblin, Klaus
Yrityssalaisuuksille dokumenttisuoja? Defensor Legis 1/2001.
Oftedal Broch, Lars
Kriminalitetens internasjonalisering. Nordisk tidsskrift for kriminalvidenskab 2/1994.
Oikeusministeriön työryhmämietintö 2003:6. Tietoverkkorikostyöryhmän mietintö. Helsinki 2003.
Oikeusministeriön lainvalmisteluosaston julkaisu 2/1991. Rikoslakiprojektin Suomen rikosoikeuden soveltamisalaa koskeva ehdotus. Helsinki 1991. (OLJ 2/1991)
Oikeusministeriön lainvalmisteluosaston julkaisu 1/1993. Rikosasioiden oikeudenkäyntimenettelyn uudistaminen: työryhmän mietintö. (OLJ 1/1993)
Oikeusministeriön lainvalmisteluosaston julkaisu 7/1994. Rauhan, yksityisyyden ja kunnian loukkaamisesta. Rikoslakiprojektin ehdotus. Helsinki 1994. (OLJ 7/1994)
Oikeusministeriön lainvalmisteluosaston julkaisu 5/2000. Rikosoikeuden yleisiä oppeja koskevat säännökset. Rikoslakiprojektin ehdotus. Helsinki 2000. (OLJ 5/2000)
Oikeuspoliittinen tutkimuslaitos
Rikollisuustilanne 1999. Rikollisuus ja seuraamusjärjestelmä tilastojen valossa. Helsinki 2000.
Organization for Economic Co-operation and Development
Computer-related Crime: Analysis of Legal Policy. Paris 1986. (OECD:n raportti)
Organization for Economic Co-operation and Development
Recommendation, Guidelines and Explanatory Memorandum for the Security of Information Systems. Paris 1992. (OECD:n tietoturvallisuusasiakirjat)
Pihlajamäki, Antti
Computer Crimes and Other Crimes against Information Technology in Finland. RIDP 1–2/1993. (RIDP 1–2/93)
Pihlajamäki, Antti
Tietotekniikkarikosten tutkintaan liittyvät ongelmat. Sisäasiainministeriön poliisiosaston julkaisu 8/1994. (Tutkinta)
Pihlajamäki, Antti
KKO 2003:58. Väärennys. KKO:n ratkaisut kommentein I 2003 (toim. Pekka Timonen), s. 415 ss. Helsinki 2003. (Kommentti)
Pihlanto, Pekka
Tiedon käsitettä hyvä ajatella oikein laajasti. Helsingin Sanomat 26.8.1995.
Piragoff, Donald K.
Computer Crimes and Other Crimes against Information Technology in Canada. RIDP 1–2/1993.

Popper, Karl
Objective Knowledge. An Evolutionary Approach. Oxford 1972.
Rautio, Ilkka
Rikoslain uudistus ja uusi oikeuskäytäntö, ATK-rikokset (koulutusmoniste). 1992.
Rautio, Ilkka
Ks. Heinonen ym., Rikosoikeus.
Rinnemaa, Tommi
Mydoom rikkoo leviämisennätyksiä. Tietoviikko 29.1.2004 s. 2.
Saarenpää, Ahti (toim.) – Pöysti, Tuomas (toim.) – Sarja, Mikko – Still, Viveca – Balboa-Alcoreza, Ruxandra
Tietoturvallisuus ja laki. Näkökohtia tietoturvallisuuden oikeudellisesta sääntelystä. Helsinki 1997. (Saarenpää ym.)
Saari, Juhani
Tietoturvallisuuden käsikirja. Keuruu 1988.
Schjølberg, Stein
Computers and Penal Legislation. 2. oppl., Oslo 1983.
Schmid, Niklaus
Das neue Computerstrafrecht. ZStrR 1995.
Schönke, Adolf – Schröder, Horst ym.
Strafgesetzbuch. Kommentar. 26., neu bearbeitete Auflage. München 2001. (Schönke – Schröder)
Scottish Law Commission
Report on Computer Crime (Scot Law Com No 106). Edinburgh 1987.
Selmer, Knut S.
Hva er ”data”? Lov og Rett 1995, s. 149 s.
Sieber, Ulrich
Informationstechnologie und Strafrechtsreform. Köln ym. 1985. (Strafrechtsreform)
Sieber, Ulrich
The International Handbook on Computer Crime. Chichester ym. 1986. (Handbook)
Sieber, Ulrich
Computer Crimes and Other Crimes against Information Technology. Commentary and Preparatory Questions for the Colloquium of the AIDP in Würzburg. RIDP 1–2/1993. (Commentary)
Sieber, Ulrich (toim.)
Information Technology Crime. National Legislations and International Initiatives. Köln ym. 1994. (Information Technology Crime)
Sieber, Ulrich
Internet Law I. Criminal Liability for the Transfer of Data in International Networks – New Challenges for the Internet. Parts I–IV, Computer Law & Security Report, Vol. 13 nos 3–6/1997; Part V, CLSR Vol. 14 no. 1/1998. (Internet Law)
Sieber, Ulrich
Legal Aspects of Computer-Related Crime in the Information Society – COMCRIME-Study. Versio 1.0, 1.1.1998. (COMCRIME-Study)
Silvander, Jan
Dator- och datarelaterade brott. Lund 2003.
Solarz, Artur
ADB och brott. Kriminalitetens utveckling i ett informationssamhälle. Stockholm 1987.
Statens offentliga utredningar 1983:50. Översyn av lagstiftningen om förmögenhetsbrott utom gäldenärsbrott. Stockholm 1983. (SOU 1983:50)

Statens offentliga utredningar 1992:110. Information och den nya InformationsTeknologin – straff- och processrättsliga frågor m.m. Betänkande av Datastraffrättsutredningen. Stockholm 1992. (SOU 1992:110)

Statens offentliga utredningar 1993:10. En ny datalag. Slutbetänkande av Datalagsutredningen. Malmö 1993. (SOU 1993:10)

Straffelovrådets betaenkning om datakriminalitet. Betaenkning nr. 1032. Kobenhavn 1985.

Sunde, Inger Marie
IKT-kriminalitet: etterforskingsmetoder og personvern. Nordisk Tidskrift for Kriminalvidenskab 3/2000.

Suomalaisen Kirjallisuuden Seura
Nykysuomen sanakirja, kolmas osa. Kuudes painos, Porvoo 1978.

Tapani, Jussi
KKO 1999:110. Maksuvälinepetoksen täyttymisen edellytykset. KKO:n ratkaisut kommentein II 1999 (toim. Pekka Timonen), s. 200 ss. Helsinki 2000. (Kommentti)

Tapani, Jussi
Tietäen vai tahtoen – tahallisuudesta velallisen rikoksissa. Turun yliopiston oikeustieteellinen tiedekunta 40 vuotta (toim. Timo Ahonen), s. 259 ss. Turku 2001. (Tahallisuudesta)

Tenhunen, Matti
Information Security and Strategies against Computer Crime. Esitelmä The INSIG Computer Crime Seminarissa 22.–23.10.1991 Luxembourgissa. (Information Security)

Tenhunen, Matti
The Legal Anatomy of Electronic Documents. Helsinki 1993. (Electronic Documents)

Tenhunen, Matti
Vastaus Euroopan neuvoston kyselyyn ”Questionnaire on Criminal Procedural Law Problems Connected with Use of Information Technology”, 1994. (Criminal Procedural Law)

Tenhunen, Matti
Legal Infrastructures and Malicious Code. A Comparative Law Analysis. Helsinki 1995. (Malicious Code)

Tietotekniikan liitto ry.
Atk-sanakirja. 10. uusittu painos, Jyväskylä 1999. (Atk-sanakirja)

Tolonen, Kari
Talousrikossäännösten tulkinta erityisesti velallisen rikoksissa. Poliisiammattikorkeakoulun tutkimuksia 9. Espoo 2000.

Tolvanen, Matti
KKO 2003:36. Tietomurto, yrityksen rangaistavuus ja rikokseen perustuva vahingonkorvaus. KKO:n ratkaisut kommentein I 2003 (toim. Pekka Timonen), s. 256 ss. Helsinki 2003.

Torikka, Mikko – Virta, Toni
Code Red aiheuttaa miljardituhoja. Tietoviikko 16.8.2001 s. 10.

Träskman, P. O.
Internationella brott och världsbrott. Teoksessa Europeisk rätt i utveckling. Helsingfors 1990.

Tuomi, Ilkka
Ei ainoastaan hakkerin käsikirja. Juva 1987.

Ufig, Alexander
Lexikon der philosophisen Begriffe. Gütersloh 1993.

Ulrich, Stein
Internationalt politisamarbeid. Nordisk tidsskrift for kriminalvidenskab 2/1994.

United Nations
Manual on the Prevention and Control of Computer-related Crime. International Review of Criminal Policy, Nos 43 and 44/1994. New York 1994. (UN Manual)

Wallich, Paul
Wire Pirates. Scientific American, March 1994, s. 72 ss.
Valtioneuvosto
Valtioneuvoston periaatepäätös tietoturvallisuuden kehittämisestä valtionhallinnossa. VM 1/73/93. (VN:n tietoturvallisuuspäätös)
Wasik, Martin
Law Reform Proposals on Computer Misuse. Crim.L.R. 1989. (Crim.L.R. 89)
Wasik, Martin
Computer Crimes and Other Crimes against Information Technology in the United Kingdom. RIDP 1–2/1993. (RIDP 1–2/93)
Vassilaki, Irini E.
Multimedia Crime – Emergence, Phenomena and Legal Questions of ”Metacomputer Crime”. Computer Law & Security Report Vol. 13 no 3. 1997.
Watkinson, John
The Art of Data Recording. Focal Press 1994.
Vento, Harri
Maksukyvyttömyys ja konkurssi rangaistavuuden edellytyksenä. Helsinki 1994.
Wiio, Osmo A.
Informaatiotekniikan ikä 30 000 vuotta? Tekniikan Maailma 5/2001, s. 79.
Vikatmaa, Juha
Erehdyksestä. Turku 1970.
Wise, Edward M.
Computer Crimes and Other Crimes against Information Technology in the United States. RIDP 1–2/1993.
Woltring, Herman
The Activities of the UN Crime Prevention and Criminal Justice Branch in the Field of Computer Crime. Teoksessa Information Technology Crime. National Legislations and International Initiatives. Köln ym. 1994.
Wranghult, Hans
Datakriminalitet. Hackers, insiders och datorstödd brottslighet. RPS rapport 1988:5.
Yamaguchi, Atsushi
Computer Crimes and Other Crimes against Information Technology in Japan. RIDP 1–2

I
YLEISTÄ

”Ajatus täydellisestä rikoksesta on vaarallisen kiehtova. Sitä on moni yrittänyt ja vielä useampi on yrityksessään pettynyt. Rikollisten ja poliisien kilpajuoksu päättyy useimmiten poliisien voittoon.

Rikoksia jää kuitenkin aina selvittämättä. Mittatappio on tosiasia myös rikostutkinnassa. Se panee yhä uudet ja uudet rikolliset koettamaan onneaan. Viimeksi kulunut vuosikymmen on antanut rikollisille pelottavan tehokkaan välineen täydellisen rikoksen toteuttamiseen. Uusi tietotekniikka on rajattomien mahdollisuuksien tekniikkaa – myös rikollisille.” (Pääkirjoitustoimittaja Keijo Himanen Helsingin Sanomissa 13.2.2001)

1 Johdanto

1.1 TUTKIMUKSEN MERKITYKSESTÄ JA TAVOITTEISTA

1.1.1 Tietotekniikka ja rikoslainsäädäntö

1.1.1.1 Yleistä

Valtioneuvoston periaatepäätös

Valtioneuvoston iltakoulussa tammikuun 18. päivänä 1995 hyväksytyissä suomalaisen tietoyhteiskunnan kehittämistä koskevissa periaatteissa[1] on asetettu tavoitteeksi, että Suomi on vuonna 2000 edelleen niin Euroopassa kuin maailmanlaajuisestikin johtavia tietoyhteiskuntia, jossa tieto- ja viestintäteollisuus on tärkeä elinkeino, jossa tietoyhteiskunnan tarjoamien palvelujen käyttömahdollisuudet ja perustaidot ovat kaikilla ja jossa tietotekniikan avulla on uudistettu elinkeinoelämän ja julkisen sektorin toimintatapoja ja rakenteita.

Yhtenä lukuisista osatavoitteista mainitaan, että tietoverkkojen toimivuuden ja turvallisuuden tulee pysyvästi olla sellaisella tasolla, että suurta luotettavuutta edellyttävien palvelujen kehittäminen on mahdollista. – Varsinaisia rikosoikeudellisia keinoja asetettujen tavoitteiden saavuttamiseksi ei periaatekannanotossa mainita, joskin huomiota saavat osakseen suojatun aineiston käyttöön ja tuottamiseen liittyvät ongelmat, salassapitolainsäädännön kehittäminen ja yhdenmukaistaminen sekä henkilörekisterilainsäädännön kehittäminen.

Tätä kirjoitettaessa on vuosi 2000 jo jäänyt taakse. Voidaan todeta, että asetetut tavoitteet näyttävät tulleen paljolti saavutetuiksi – Suomen asema tieto-

[1] Ks. Virallinen lehti 23.1.1995/9.

tekniikan alueella on tunnustettu ja erityisesti mobiilin viestinnän alueella Suomi on eittämättä yksi maailman huippumaista.

Periaatekannanoton mukaan tietoyhteiskunnalla tarkoitetaan ”yhteiskuntaa, jossa laajalti hyödynnetään tietoverkkoja ja tietotekniikkaa sekä tuotetaan runsaasti tieto- ja viestintäteollisuuden tuotteita ja palveluja ja jossa on monipuolinen sisältöteollisuus”.

Tällaisessa tietoyhteiskunnassa ei voida välttyä ongelmilta, joiden ratkaisemiseen tarvitaan rikosoikeuden keinoja. Yhtä lailla kuin tietoyhteiskunta on käsitteenä vielä jokseenkin uusi ja sisällöltään täsmentymätön muodostavat tietotekniikkaan kohdistuvat tai sen mahdollistamat rikokset uudehkon ja – ainakin ensivaikutelmaltaan – epämääräisen rikoskategorian.

Eduskunnan lakivaliokunta toteaa mietinnössään hallituksen esityksestä rikoslainsäädännön kokonaisuudistuksen toisen vaiheen käsittäviksi rikoslain ja eräiden muiden lakien muutoksiksi muun ohessa pitävänsä ”tärkeänä, että tietokonerikollisuuden kehitystä ja sen eri ilmenemismuotoja seurataan tarkoin kansainvälisessä yhteistyössä ja lainsäädäntöä uudistetaan tarvittaessa”.[2]

Yhdistyneiden Kansakuntien tietotekniikkarikoskäsikirja

Yhdistyneiden Kansakuntien vuonna 1994 julkaistussa tietotekniikkarikosten ehkäisemistä ja kontrolloimista koskevassa käsikirjassa todetaan kahdennenkymmenennen vuosisadan jälkipuoliskoa tultavan tulevaisuudessa tarkastelemaan informaatiovallankumouksen aikakautena, jolloin aikaisemmin mahdottomana pidetystä on tietoteknisen kehityksen myötä tullut mahdollista. Informaatiovallankumouksen eduista saavat nauttia niin liike-elämä, hallitukset kuin yksityisetkin. Yhä enenevässä määrin liike- ja talouselämä, teollisuus, sairaalat ja viranomaiset ovat tulleet riippuvaisiksi tietokoneista, jotka ovat mahdollistaneet suurten tietomäärien varastoimisen ja äärimmäisen nopean käsittelemisen maailmanlaajuisissakin tietoverkoissa.

Kuitenkin, todetaan käsikirjassa, tällä kehityksellä on myös kielteinen puolensa. Se on avannut ovet senlaatuiselle epäsosiaaliselle ja rikolliselle käyttäytymiselle, joka ei koskaan aikaisemmin olisi ollut mahdollista. Tietokonejärjestelmät tarjoavat uusia ja monimutkaisia mahdollisuuksia lain rikkomiseen ja ne luovat tilaisuuksia perinteisten rikosten tekemiseen uusilla menetelmillä. Yhteiskunta tukeutuu tietoteknisiin järjestelmiin jo lähes kaikilla elämänalueilla ilma-, raide- ja tieliikenteen valvonnasta terveydenhuoltoon ja kansallisen turvallisuuden ylläpitämiseen. Pienikin häiriö näiden järjestelmien toiminnassa voi aiheuttaa vaaran ihmishengille. Yhteiskunnan riippuvuudella tietojärjestelmistä on niin muodoin syvä inhimillinen ulottuvuus.

Suurten tietoverkkojen nopea transnationaalinen laajeneminen ja mahdolli-

---

[2] LaVM 22/1994.

suus päästä useisiin järjestelmiin tavallisia puhelinlinjoja pitkin lisää näiden järjestelmien haavoittuvuutta ja mahdollisuuksia väärinkäytöksiin tai rikolliseen toimintaan. Tietotekniikkarikokset voivat aiheuttaa paitsi suuria taloudellisia menetyksiä myös vakavia ihmisten turvallisuuteen kohdistuvia seurauksia.[3]

Kansainvälisen rikosoikeusyhdistyksen päätöslauselma

Kansainvälisen rikosoikeusyhdistyksen AIDP:n vuoden 1994 maailmankongressin päätöslauselmassa[4] todetaan muun muassa, että tiedon liikkuvuus kansainvälisessä televerkossa ja nykyaikaisessa informaatioyhteiskunnassa vallitsevat erittäin tiiviit vuorovaikutussuhteet tekevät kansainvälisen yhteistyön tietotekniikkarikosten ehkäisemisessä ja syytteeseen saattamisessa erityisen tärkeäksi.

Transnationaaliset tietotekniikkarikokset

Yksi tietotekniikkarikoksille ominainen piirre on se, että niiden vaikutukset hyvin helposti saattavat ulottua usean valtion alueelle. Rikoksentekijä voi vaivattomasti tietoverkkoja käyttäen ylittää valtioiden välisiä rajoja niin, että tosiasiallinen tekeminen voi tapahtua kaukana siitä maasta, jossa teon seuraus ilmenee. Erityisesti Internetin käytön räjähdysmäinen lisääntyminen aivan viime vuosina on oleellisesti muuttanut niitä mahdollisuuksia, joita tietotekniikka rikollisille tarjoaa. Internetin käyttäjiä lienee tätä nykyä satoja miljoonia ja Internet-verkko kattaa käytännössä koko maapallon – eihän Internet-yhteyden luomiseen tarvita muuta kuin verkkoyhteydet mahdollistava jonkin matkapuhelinverkon kuuluvuusalueella oleva matkapuhelin tai kannettava mikrotietokone ja kaikkialla toimiva satelliittipuhelin.

Tästä tietotekniikkarikosten *transnationaalisesta luonteesta*[5] on seurannut, että kansainväliset järjestöt ovat kiinnittäneet tietotekniikkarikoksiin erityistä huomiota. Jäljempänä osan I luvussa 2 selostetaan yksityiskohtaisemmin eri järjestöjen toimenpiteitä samoin kuin tietotekniikkarikosten transnationaalisesta luonteesta johtuvia ongelmia; joka tapauksessa muun muassa Taloudellisen yhteistyön ja kehityksen järjestössä OECD:ssä, Euroopan neuvostossa ja Yh-

---

[3] UN Manual, kohdat 1–4.

[4] Tietotekniikkarikoksia koskeva päätöslauselma, kohta 21.

[5] *Lehtimaja* (LM 86 s. 211) käyttää termiä *transnationaali* rikoksista, joita ei ole mahdollista paikallistaa yksiselitteisesti mihinkään valtioon. Tällaisen vierasperäisen sanan käyttäminen suomenkielisessä tekstissä on sinänsä arveluttavaa, mutta tässä tapauksessa samaa tarkoittavan suomenkielisen sanan löytäminen on vaikeaa. – Tietotekniikkarikosten on usein sanottu olevan luonteeltaan *kansainvälisiä* (international). Tämä ei kuitenkaan ole tyydyttävä luonnehdinta, sillä tietotekniikkarikokset eivät ole kansainvälisiä rikoksia siinä mielessä, mitä käsitteellä rikosoikeudessamme yleensä ymmärretään. Ks. esim. EIF IV, s. 131, jossa kansainvälisiksi rikoksiksi määritellään tietyt sellaiset kansainvälisen oikeuden loukkaukset, jotka ovat luonteeltaan erityisen törkeitä ja loukkaavat kansainvälisen valtioyhteisön perustavanlaatuisia etuja tai arvoja taikka

distyneissä Kansakunnissa on tehty laajoja selvitystöitä ja laadittu järjestöjen jäsenvaltioille suosituksia tietotekniikkarikoksia koskevan lainsäädännön yhdenmukaistamiseksi. Euroopan neuvostossa on menty vielä askel pitemmälle: maailman ensimmäinen tietotekniikkarikoksia koskeva yleissopimus on valmistunut ja onpa sopimukseen jo ehditty neuvotella ensimmäinen lisäpöytäkirjakin.

Tietotekniikka ja rikosoikeus

Niin Suomen kuin usean muunkin läntisen Euroopan valtion tietotekniikkarikoksia koskeva lainsäädäntö perustuu paljolti Euroopan neuvoston vuonna 1989 antamaan kriminalisointisuositukseen. Rikoslain kokonaisuudistuksen ensimmäisen vaiheen myötä vuoden 1991 alusta tuli voimaan joukko kriminalisointeja, joissa nimenomaan on kysymys tietotekniikkarikoksiksi luonnehdittavista menettelyistä. Tällaisia säännöksiä sisältyy myös uudistuksen toiseen vaiheeseen, joka on tullut voimaan syyskuun alusta 1995 lukien. Tämän jälkeen on meillä toteutettu joitakin osittaisuudistuksia, jotka ovat ensisijaisesti perustuneet tietotekniikan kehityksen asettamiin vaatimuksiin ja joiden tarkoittamia menettelyjä ei 1980-luvulla valmistellussa suosituksessa ole vielä osattu edes pitää kriminalisoimisen arvoisina.

Tietotekniikka ei suinkaan kohtaa rikosoikeutta vain varsinaisten tietotekniikkarikosten ollessa kysymyksessä: 1990-luvun jälkipuoliskolta alkaen on yhä suurempaa merkitystä rikosten selvittämisessä saanut niin sanottu *elektroninen todistusaineisto* eli elektronisessa muodossa erilaisille tietovälineille tallennettu tai tallentunut data, joka edustaa jotain rikoksen tekemiseen liittyvää ja rikoksen selvittämisen kannalta relevanttia informaatiota ja jota voi ilmetä oikeastaan minkä tahansa perinteisenkin rikoksen yhteydessä. Tällaisen todistusaineiston kerääminen, tulkitseminen ja selittäminen asettaa niin esitutkinta- ja syyttäjäviranomaiset kuin tuomaritkin kokonaan uudentyyppisten haasteiden eteen, sillä aineiston merkityksen ymmärtäminen edellyttää välttämättömästi ainakin jossain määrin tietotekniikan ymmärtämistä. Tähän taas ei päästä ilman koulutusta, jota poliisi- ja syyttäjälaitoksessa jo onkin järjestetty.

---

ihmisyyden vähimmäisvaatimuksia. Näihin tekoihin sovelletaan *universaaliperiaatetta,* jonka mukaan kansainvälisistä rikoksista rangaistaan tekopaikasta, tekijästä tai tekopaikan lainsäädännöstä riippumatta. Nämä rikoslain 1 luvun 7 §:ssä tarkoitetut rikokset on määritelty asetuksessa rikoslain 1 luvun 7 §:n soveltamisesta 727/1996 (ks. Heinonen ym., s. 116). – Sopivaa suomenkielistä sanaa englanninkielisten termien *transnational* tai *transborder* vastineeksi ei ole, joten käytän sanaa transnationaalinen kuvaamaan sitä tietotekniikkarikoksille ominaista piirrettä, että ne helposti ulottavat vaikutuksensa usean valtion alueelle; ”helposti valtioiden rajoja ylittävistä” rikoksista puhuminen olisi asiallisesta täsmällisyydestään huolimatta kömpelöä.

1.1.1.2 Lainsäädäntötekniikasta

Vaihtoehdoista

Lähdettäessä säätämään uudentyyppisiä rikoksia koskevia rangaistussäännöksiä on valittavana kaksi tietä: joko olemassa olevan, perinteisiä rikoksia koskevan säännöstön täydentäminen ja muokkaaminen vastaamaan uusia vaatimuksia tai sitten kokonaan uuden säännöstön luominen. Tietotekniikkarikosten osalta Suomessa on valittu edellinen vaihtoehto: tietojenkäsittelypetoksesta säädetään erehdyttämispetoksen yhteydessä, tietotekninen tallenne on saatettu väärennysrikoksen kelvolliseksi objektiksi määrittelemällä todistuskappaleen käsite riittävän laajaksi, tietokoneen ja -järjestelmän luvattomasta käyttämisestä voidaan rangaista luvatonta käyttöä koskevan säännöksen perusteella ja tietovahingon aiheuttaminen rinnastetaan tavalliseen vahingontekoon.

Valmistumassa oleva rikoslain kokonaisuudistus on epäilemättä toisaalta ollut omiaan edesauttamaan tällaisen vaihtoehdon valitsemista: teknisesti on ollut yksinkertaista laatia tunnusmerkistöt ja määritelmät sellaisiksi, että esimerkiksi Euroopan neuvoston kriminalisointisuosituksessa tarkoitettuja tekoja voidaan nyt meilläkin käsitellä rikoksina. Eri asia on, onko valittu vaihtoehto kuitenkaan tarkoituksenmukaisin ja onko se ollut omiaan johtamaan yksiselitteisiin ratkaisuihin, jotka ovat toimivia myös käytännön työssä: rikosten tutkinnassa, syyteharkinnassa ja tuomioistuinkäsittelyssä.[6]

Euroopan neuvoston vuonna 1985 asettamassa asiantuntijakomiteassa, joka valmisteli neuvoston kriminalisointisuosituksen, erottui kaksi eri linjaa. Vähemmistöön jääneen näkemyksen mukaan tietotekniikka olisi tullut määritellä kriminaalipolitiikassa kokonaan uudeksi elämänalueeksi ja yleinen luottamus tietotekniikkaan vastaavasti kokonaan uudeksi oikeushyväksi, joka olisi vaatinut omintakeisen sääntelyn.

Enemmistön mielestä taas automaattinen tietojenkäsittely oli ainoastaan uusi ilmiö, joka oli luonut eräitä uusia rikoksentekomahdollisuuksia ja uudenlaisen ympäristön useille perinteisille rikoksille, minkä vuoksi tietotekniikan kehitys olisi otettava huomioon nykyistä rikosoikeusjärjestelmää kehitettäessä järjestelmän osana eikä erillisenä ilmiönä.[7] Suomalaisessa lainsäädännössä on otettu

---

[6] HE 94/1993, s. 133: ”Nimenomaan automaattisen tietojenkäsittelyn ja uusien tiedonsiirtomuotojen yleistyminen on nostanut esiin tarpeen tarkastella tietoa ja tietoliikennettä omana kokonaisuutenaan myös rikosoikeudellisen sääntelyn kannalta. Automaattisen tietojenkäsittelyn sovellukset ja tietotyö ulottuvat nykyään lähes kaikkiin inhimillisiin toimintoihin ja niinpä siitä aiheutuvat vaatimukset on otettava huomioon kaikilla lainsäädäntölohkoilla. Kaikissa OECD-maissa, Yhdysvaltoja lukuun ottamatta, on katsottu, ettei tarvita erillistä atk-rikoslakia, vaan että niin sanottuihin atk-rikoksiinkin on mahdollisimman pitkälle sovellettava olemassa olevia rikossäännöksiä.”

[7] Lehtimaja, Atk-rikospolitiikasta, s. 263.

lähtökohdaksi juuri tämä viimeksi mainittu näkemys.[8]

On totta, että tietotekniikkarikoksiksi määriteltävien rangaistavien tekojen joukko *näyttää* varsin heterogeeniseltä – pelkkiä rikosnimikkeitä ajateltaessa on vaikeata nähdä yhteneväisyyksiä esimerkiksi petoksen, vahingonteon ja yritysvakoilun kesken. Tässä suhteessa on valittu lainsäädäntötekniikka epäilemättä tarkoituksenmukainen.

Euroopan neuvoston asiantuntijakomitean vähemmistön kannan hyväksyminen puolestaan saattaisi johtaa pitämään – ainakin jossain mielessä – perusteltuna, että tietotekniikkarikoksista säädettäisiin kootusti, yhdessä rikoslain luvussa (niin kuin säädetään esimerkiksi huumausainerikoksista) tai peräti omassa laissaan (niin kuin säädettiin huumausainerikoksista). Tällainen vaihtoehto on valittu muun muassa Yhdistyneessä kuningaskunnassa, jossa vuonna 1990 säädettiin yksinomaan tietotekniikkarikoksia koskeva *Computer Misuse Act.*

Suomen ratkaisusta

Suomessa ei kuitenkaan ole yleensä säädetty erikoisrikoslakeja – ja sikäli kuin niitä on ollut, on niistä pyritty pääsemään eroon. Tietotekniikkarikosten erottaminen niin selkeästi omaksi ryhmäkseen olisikin, ellei peräti mahdotonta, niin ainakin hyvin vaikeaa, kun rangaistussäännösten ensisijaiset suojeluobjektit kuitenkin ovat erilaisia: tietotekniikkaväärennys kohdistuu ”tavallisen” väärennyksen tavoin todistelun luotettavuuteen, tietovahingon aiheuttaminen ”tavallisen” vahingonteon tavoin omaisuuteen ja niin edelleen. Palaan kysymykseen tietotekniikkarikoksia koskevien kriminalisointien suojeluobjekteista jäljempänä tietotekniikkarikoksen käsitteen määrittelyn yhteydessä.

Suomessa valittu lainsäädäntötekniikka saattaa aiheuttaa käytännön lainsoveltamisessa ongelmia ainakin siinä suhteessa, että – niin kuin jäljempänä osassa II säännöksiä yksityiskohtaisesti käsiteltäessä tullaan havaitsemaan – tunnusmerkistöjen väliset rajat voivat ainakin näennäisesti olla hyvinkin epäselviä.

Lainkonkurrenssitilanteilta on tällöin mahdotonta kokonaan välttyä eivätkä nämä tilanteet aina ratkenne tavanomaisten ja yleisten sääntöjen – *lex specialis derogat legi generali, lex primaria derogat legi subsidiariae* – mukaisesti. Tällaisia tilanteita ei ole nähtävissä vain tietotekniikkarikoksiksi luettavien tekojen keskinäisessä suhteessa vaan myös tietotekniikkarikosten ja niin sanottujen perinteisten rikosten välillä.

Sovellettavan säännöksen valitseminen tapahtuu paljolti sen selvittämisellä, mikä on kulloisessakin tilanteessa suojeltava oikeushyvä – tietojenkäsittelyn loukkaamattomuuden eli niin sanotun tietojenkäsittelyrauhan *lisäksi* silloin, kun kysymyksessä on kahden tietotekniikkarikossäännöksen konkurrenssi. Lisäksi sovellettavan säännöksen valinnassa on huomattavan suuri merkitys sen

---

[8] Ks. HE 94/1993, s. 17 s.

selvittämisellä, mikä on ollut tekijän ensisijaisena tarkoituksena. Käsittelen tahallisuuteen liittyviä kysymyksiä tarkemmin jäljempänä osan II luvussa 6.

1.1.1.3 Tietotekniikkarikokset ja Suomen oikeus

Aineellinen rikosoikeus

Vaikka tietotekniikkarikoksia suoranaisesti koskevat rikosoikeudelliset säännöksemme jo tälläkin hetkellä ovat myös kansainvälisestä näkökulmasta tarkasteltuina hyvin ajan tasalla, aiheutuu tietotekniikan jatkuvasta ja nopeasta kehittymisestä yhä uusia kriminalisointien tarpeita. Jo nyt on sekä varsinkin OECD:n että myös Euroopan neuvoston suosituksissa havaittavissa selviä aukkoja, ja kun kansallinen lainsäädäntö niin Suomessa kuin muuallakin paljolti perustuu juuri näihin suosituksiin, ovat aukot siirtyneet myös kansallisiin rikoslakeihin. Tietotekniikkarikoksia koskevalle sääntelylle on nimittäin tyypillistä, että omaperäisiä kansallisia säännöksiä on vaikea löytää.

Tietotekniikkarikossäännösten soveltamiskäytäntö on Suomessa toistaiseksi ollut jokseenkin vähäistä. Tarkkaa tietoa tietotekniikkarikosten lukumäärästä ei ole saatavissa, toisaalta siksi, että viranomaisten käsittelemiä asioita ei tilastoida erikseen vaan esimerkiksi tietojenkäsittelypetokset sisältyvät tilastoissa petoksiin, toisaalta siksi, että tietotekniikkarikokset useassa tapauksessa jäävät kokonaan tulematta viranomaisten käsiteltäviksi.[9]

Viimeksi mainittuun on ainakin yhtenä syynä se, että asianomistajat eivät ole erityisen halukkaita paljastamaan järjestelmiensä haavoittuvuutta ja menettämään tämän seurauksena mainettaan – tämä ilmiö on havaittu yleismaailmallisesti. Toinen syy on ilmeisesti se, että luottamus viranomaiskoneiston kykyyn hoitaa ja käsitellä tämäntyyppistä rikollisuutta ei ole kovin korkealla tasolla – ja jotta viranomaiskoneisto voisi todistaa kykenevyytensä, se tarvitsisi juttuja hoitaakseen! Kolmanneksi on ilmeistä, että rikosten uhrit pelkäävät asioiden selvittämisen aiheuttavan niille huomattavan suuria kustannuksia.

Prosessioikeus

Prosessioikeuden alueella lainsäädäntömme ottaa tietoteknisen kehityksen asettamat vaatimukset huomioon selvästi huonommin kuin aineellisen rikosoikeuden alueella. Euroopan neuvoston raportissa[10] on kiinnitetty erityistä huomiota kolmeen tietoteknisessä ympäristössä tapahtuvaan näytön hankkimiseen ja esittämiseen liittyvään ongelmakokonaisuuteen: (1) pakkokeinojen käyttä-

---

[9] Timo Laineen yrityksiin kohdistuneita yrityssalaisuusrikoksia koskevasta tutkimuksesta on pääteltävissä, että vain pari prosenttia yrityksiin kohdistuneista yritysvakoiluista ja tietomurroista ilmoitetaan poliisille.

[10] EN:n raportti 89, s. 52 ss.

minen todisteiden hankkimiseksi; (2) rikosprosessissa tapahtuvaan henkilötietojen kokoamiseen, tallentamiseen ja yhdistämiseen liittyvät oikeudelliset kysymykset; sekä (3) tietoteknisistä tallenteista koostuvan näytön sallittavuus rikosprosessissa. Tässä tarkoitetaan muun muassa juuri edellä mainitun elektronisen todistusaineiston keräämiseen liittyviä kysymyksiä, jotka monessa kohdin ovat esitutkinta- ja pakkokeinolainsäädännössämme vailla nimenomaista sääntelyä.

Mainituista kolmesta ongelmakokonaisuudesta lähinnä ensimmäinen on relevantti Suomen oikeuden kannalta. Näytön sallittavuuteen liittyvät ongelmat koskettavat ensisijaisesti common law -maita; meillä sovellettava, joskin ihmisoikeusajattelun vahvistumisen myötä aikaisempaan verrattuna rajoittunut, vapaan todistusharkinnan periaate ei kuitenkaan samassa määrin todistusaineiston arvoa arvioitaessa anna merkitystä sille, onko tietynlaatuinen näyttö esimerkiksi hankittu sopimattomaksi katsottavalla tavalla.

AIDP:n vuoden 1994 kongressin päätöslauselmassa puututaan lähinnä esitutkintaan ja pakkokeinojen käyttämiseen liittyviin prosessuaalisiin kysymyksiin.[11] Lisäksi kiinnitetään huomiota tietoteknisten tallenteiden todisteina käyttämisen sallittavuuteen ja kehotetaan vähentämään tässä suhteessa ilmeneviä ongelmia lainsäädäntötoimilla.

Yhdistyneiden Kansakuntien käsikirjassa käsitellään prosessin osalta samoja kysymyksiä kuin Euroopan neuvoston instrumenteissakin.[12]

Tietotekniikkarikosten transnationaalinen luonne, jota on korostettu muun muassa Euroopan neuvoston raportissa, aiheuttaa kansainvälistä yhteistyötä edellyttäviä ongelmia niin esitutkinnassa, syytteeseenpanossa kuin oikeudenkäynnissäkin. Vaikka ongelmat ovat pääosin prosessuaalisia, on niiden ratkaisemisessa merkitystä myös rikosoikeudellisilla säännöksillä. Euroopan neuvosto on ollut aktiivinen tälläkin saralla: vuoden 1995 prosessioikeudellisessa suosituksessa R(95)13 on esitetty keskeisimmät tietotekniikkarikosten esitutkintaan, syyteharkintaan ja tuomioistuinkäsittelyyn samoin kuin elektronisen todistusaineiston keräämiseen liittyvät sääntelytarpeet. Juuri näiden kysymysten ratkaisemisessa on ollut pääpaino myös Euroopan neuvoston tietoverkkorikoskonvention valmistelussa, ja suurin osa sopimusmääräyksistä koskeekin prosessuaalisia kysymyksiä.

---

[11] Ks. päätöslauselma kohta 18, jossa mm. todetaan, että ”there should be clearly defined: (a) powers for conducting, search and seizure in an information technology environment, particularly in regard to the seizure of intangibles and the search of computer networks; (b) duties of active co-operation by victims, witnesses and other users of information technology, other than the suspect, (especially to make information available in a form usable for judicial purposes); and (c) powers to permit the interception of communications in or between computer systems, and to use the obtained evidence in court proceedings”.

[12] UN Manual, kohdat 148–175, joissa käsiteltävät teemat ovat (1) The coercive powers of prosecuting authorities, (2) Specific problems with personal data ja (3) Admissibility of computer-generated evidence.

Suomen oikeuden kannalta keskeiset ongelmatilanteet keskittynevät seuraaviin neljään ongelmakokonaisuuteen: (1) tuomiovaltaan liittyvät kysymykset; (2) kansainvälinen oikeusapu; (3) rikoksentekijän luovuttaminen; ja (4) tietoteknisessä ympäristössä olevan näytön hankkiminen ja esittäminen.

Näistä kokonaisuuksista kolme ensimmäistä nivoutuvat osittain yhteen ja johtuvat tietotekniikkarikollisuuden transnationaalisesta erityisluonteesta. Neljäs on seurausta lain säätämisen jälkeen tapahtuneesta tietotekniikan kehittymisestä (ja osaksi myös tietoteknisen kehityksen riittämättömästä ennakoimisesta lakia säädettäessä, tällainen ennakoiminen on kuitenkin tavattoman vaikea tehtävä).

Suomi ei pyrkinyt aktiivisesti implementoimaan Euroopan neuvoston prosessioikeudellista suositusta.[13] Euroopan neuvoston niin aineelliseen rikosoikeuteen kuin prosessioikeuteen kuuluvia määräyksiä sisältävän yleissopimuksen valtionsisäinen voimaan saattaminen on sen sijaan edennyt tehokkaasti ja oikeusministeriön joulukuussa 2002 asettama tietoverkkorikostyöryhmä[14] antoi tiiviin puolivuotisen työskentelyn jälkeen mietintönsä[15] kesäkuussa 2003. Mietintö oli lausuntokierroksella loppuvuodesta 2003 mutta hallituksen esityksen antamisajankohta ei ole vielä tarkkaan ennakoitavissa.

Myös Euroopan unionin piirissä käsiteltiin Euroopan neuvoston sopimusneuvottelujen aikoihin tietotekniikkarikollisuuteen liittyviä kysymyksiä.[16] Varsinainen velvoittavaan instrumenttiin johtava työ alkoi kuitenkin vasta konvention valmistuttua ja saattaa aikanaan johtaa joihinkin lainsäädäntötoimenpiteisiin.

---

[13] Suosituksen valmistuttua oikeusministeriössä tosin aloitti työskentelyn pakkokeinolainsäädännön uudistamista valmistellut työryhmä. Työryhmä jätti vuonna 2000 mietintönsä mutta totesi nimenomaan tietotekniikkarikoksiin liittyvien kysymysten osalta olevan syytä jäädä odottamaan EN:n tietoverkkorikoskonvention valmistumista.

[14] Tietoverkkorikostyöryhmään kuuluivat oikeusministeriön lainsäädäntöjohtaja Jan Törnqvist puheenjohtajana ja lainsäädäntöneuvos Riku Ahola sihteerinä sekä jäseninä tämän kirjoittajan lisäksi poliisiylitarkastaja Jouni Välkki sisäasiainministeriöstä, rikostarkastaja Ari Määttä keskusrikospoliisista, neuvotteleva virkamies Sanna Helopuro liikenne- ja viestintäministeriöstä, asianajaja Satu Tiirikka Suomen Asianajajaliitosta ja käräjätuomari Sirpa Ahola Helsingin käräjäoikeudesta.

[15] OM:n työryhmämietintö 2003:6.

[16] Näistä kysymyksistä keskusteltiin EY:n komission joulukuussa 1999 – huhtikuussa 2000 järjestämissä ”Creating a safer information society” -kokouksissa ja Ranskan puheenjohtajuuskauden alussa jopa näytti siltä, että EU:n piirissä jotain olisi ollut tapahtumassa. Näin ei kuitenkaan käynyt eikä edistystä tapahtunut Ruotsinkaan puheenjohtajuuskaudella alkuvuonna 2001. Tämä oli mielestäni ilman muuta järkevää ja edustin tällaista kantaa jo mainituissa kokouksissakin: ensin oli syytä katsoa, millaiseksi EN:n konventio lopulta muodostui, ja vasta sen jälkeen ryhtyä täyttämään aukkoja. Toinen asia on, että EU:n piirissä tehtävä työ saattaa lopulta johtaa konkreettisiin tuloksiin EN:n sopimusta nopeammin, sillä EN:n instrumentit eivät yleensä ole tulleet kovin nopeasti kansainvälisesti voimaan, kun taas esimerkiksi EU:n yhteinen toiminta saattaa olla hyvinkin pikaisesti kaikkien jäsenmaiden implementoima. Tanskan puheenjohtajuuskaudella loppuvuonna 2002 konkreettisiin toimenpiteisiin lopulta ryhdyttiin, kun komission ehdotusta verkkorikoksia koskevaksi puitepäätökseksi alettiin käsitellä neuvoston työryhmässä.

1.1.2 Tutkimuksen tavoitteet

1.1.2.1 Yleistä

Kuopus toteaa väitöskirjassaan, että osana tietotekniikan vaikutustutkimusta *oikeustieteen tehtäväksi* olisi nähtävä *ei* vain totutun *kontribuution vaan rakenteellisesti uuden tiedon tuottaminen* tietoyhteiskunnan murroksen hallitsemiseksi ja hahmottamiseksi. Edelleen Kuopuksen mukaan uusien ”atk-oikeudellisten normien” tuottamisen ohella on kiireellisesti arvioitava oikeustieteen metodien ja tietotekniikan vaatimusten sopivuutta keskenään. Uusia oikeudellisia ongelmia ei voida säädöstasollakaan hallita ilman perustutkimusta oikeustieteen mahdollisuuksista teknistyvässä yhteiskunnassa. Katson edellä lausutun soveltuvan hyvin pitkälti myös tähän tutkimukseen ja näin ollen voin Kuopuksen tavoin todeta tutkimukseni osaltaan kuuluvan laajasti ymmärretyn *tietotekniikan vaikutustutkimuksen alueeseen.*[17]

Tietotekniikkarikoksia koskevan rikosoikeudellisen tutkimuksen painopiste on luonnollisesti aineellisoikeudellisissa säännöksissä, toisaalta olemassa olevien säännösten sisällön selvittämisessä, toisaalta niiden kattavuuden kartoittamisessa ja mahdollisten uusien säännösten tarpeen selvittämisessä. Rikoslain kokonaisuudistus on sinänsä helpottanut tietotekniikkarikossäännösten sijoittamista rikoslakiin mutta muutamat myöhemmät erilliset lainsäädäntöhankkeet osoittavat selvästi, että kestävien ratkaisujen luominen juuri tietotekniikkarikosten kohdalla on, ellei suorastaan mahdotonta, niin ainakin hyvin vaikeaa. Sen selvittäminen, miten lainsäädäntötyössä on materiaalisesti onnistuttu – ottaen huomioon myös edellä lainsäädäntöteknisistä ratkaisuista lausuttu – on tämän tutkimuksen keskeisimpiä tavoitteita.

Oikeusnormissa katsotaan aina olevan kolme rakenneosaa: oikeustosiasia, pitämiselementti ja oikeusseuraamus.[18] Rikosoikeudellisen normin käyttökelpoisuus riippuu oleellisesti oikeustosiasiaosan selkeydestä ja yksiselitteisyydestä – mitä enemmän tulkinnanvaraisuutta tosiasiakuvaukseen sisältyy, sitä vaikeampaa on koko normin soveltaminen ja sitä arveluttavampaa on ottaa tällainen normi rankaisutoiminnan perusteeksi.

Tietotekniikkaan liittyvien oikeusnormien laatiminen ja soveltaminen edellyttää aina erityistietämystä, mutta rikosoikeudellisen normin tulisi kuitenkin olla niin muotoiltu, että erityistietämyksen osuus normin soveltamisessa loppujen lopuksi jää mahdollisimman vähäiseksi. Rikoslain ensisijaisilta soveltajilta – poliisilta, syyttäjiltä ja tuomareilta – ei tietenkään voida edellyttää kaikkien kysymykseen tulevien alojen erityistietämystä, joten normi on aina eräänlainen kompromissi, jonka tulisi myös antaa ymmärrettävässä muodossa olevaa informaatiota niille ihmisille, joiden käyttäytymistä se on tarkoitettu ohjaamaan.

---

[17] Kuopus, s. 15 s.
[18] Ks. esim. Aarnio, s. 66 ss.

1.1.2.2 Suomen voimassa oleva tietotekniikkarikoksia koskeva lainsäädäntö

Selvitän jäljempänä, miten meillä voimassa olevat tietotekniikkarikoksia koskevat säännökset täyttävät selkeyden ja yksiselitteisyyden vaatimukset ja tarkastelen myös, miten luontevasti ja johdonmukaisesti ne asettuvat osaksi rikosoikeudellista sääntelyjärjestelmäämme. Tutkimustehtävä on siis tavallaan kahtalainen: pääpaino on tulkintajuridiikassa, mutta tietotekniikkarikosten erityisluonteesta – mikä ei tarkoita niiden mystifioimista – aiheutuu tarvetta myös oikeuspoliittiseen tarkasteluun.

Tietoturvallisuuden ja tietojenkäsittelyrauhan takaamisessa rikosoikeuden keinot eivät voi olla ensisijaisen tärkeitä, sillä tietotekninen ympäristö asettaa perinteiseen maailmaan verrattuna täysin uudentyyppisiä haasteita: datan salamannopea liikkuminen ympäri maailmaa silmin nähtäviä jälkiä jättämättä edellyttää, että tietotekniikan välineitä – niin laitteita kuin ohjelmiakin – suunniteltaessa, valmistettaessa ja käytettäessä erilaisille turvallisuusnäkökohdille annetaan huomattavan suuri merkitys. Tietotekniikkarikoksista säädettäessä on usein voitu havaita monien tietotekniikan käyttäjien kyseenalaistavan sellaisten yksittäisten kriminalisointien tarpeellisuuden, jotka taas viranomaisten näkökulmasta ovat hyvinkin hyödyllisiä, sillä tietotekniikan käyttäminen helpottaa myös ns. perinteisten rikosten tekemistä ja rikosten jälkien salaamista.

Tietotekniikkarikoksen jäljempänä määriteltävä käsite kattaa paitsi rikoslain niin kutsutut data- ja informaatiorikokset eli tietojenkäsittelyrauhan loukkaukset myös eräitä immateriaalioikeuksien ja yksityisyyden suojan loukkauksia. Viimeksi mainittujen ottaminen mukaan tähän tutkimukseen ei ole perusteltua: tekijänoikeudelliset ja yksityisyyden suojaan liittyvät spesifiset kysymykset, joiden selvittämistä niihin liittyvien rangaistussäännösten tutkiminen välttämättä edellyttäisi, ensinnäkin poikkeavat siinä määrin varsinaisiin tietotekniikkarikoksiin liittyvistä ongelmista ja toiseksi ovat niin laaja-alaisia, että niiden liittäminen tähän tutkimukseen johtaisi liian laajaan ja epäyhtenäiseen lopputulokseen.

Myös data- ja informaatiorikokset eroavat luonteeltaan toisistaan. Eroa voidaan konkretisoida jäljempänä perusteltavalla näkemyksellä, jonka mukaan data on luonteeltaan lähinnä materiaalista, kun taas informaatio on ensisijaisesti immateriaalista. Data on informaatiota helpommin miellettävissä rikoksen objektiksi, ainakin ajateltaessa ns. perinteistä rikollisuutta.

Rikoslakiuudistuksen ensimmäisen vaiheen tietotekniikkakriminalisoinnit koskevat lähes poikkeuksitta juuri datarikoksia, kun taas toisen vaiheen rangaistussäännökset etupäässä koskevat informaatiorikoksia. Ne tietotekniikkarikokset, jotka ovat tämän tutkimuksen kohteena, ovat *datarikoksia;* jätän tarkoituksella käsittelemättä viestintään liittyvät teot eli lähinnä viestintäsalaisuuden loukkaukset ja tietoliikenteen häirinnän – en siksi, ettei niihin liittyisi *myös*

tietotekniikasta johtuvia ongelmia, vaan siksi, että niiden osalta ongelmat eivät ole ensi sijassa, eivätkä edes suurelta osin, tietoteknisiä. Julkisuudessa esimerkiksi viestintäsalaisuuden osalta on käyty keskustelua siitä, saako työnantaja lukea työntekijän sähköpostia; ongelmat ovat toisin sanoen paljolti keskittyneet viestintäsalaisuuden suojan ulottuvuuteen, joka ei ole *tietotekniikkarikoksia ajatellen* erityisen keskeinen kysymys (vaikka se muuten onkin mitä kiinnostavin ongelma ja epäilemättä ansaitsee tulla tutkituksi jossain muussa yhteydessä).

1.1.2.3 Tietotekniikkarikoksia koskeva kansainvälinen yhteistyö

Tietotekniikkarikoksia koskevan tutkimuksen alueella on harjoitettu poikkeuksellisen laajaa kansainvälistä yhteistyötä. Tähän on keskeisenä syynä edellä mainittu tietotekniikkarikollisuuden transnationaalinen luonne; on hyvin tärkeää, että kansalliset kriminalisoinnit ja menettelymuodot eri maissa mahdollisimman pitkälti vastaavat toisiaan. Erityisesti viime vuosina on Internetin[19] ja muiden tietoverkkojen[20] jatkuva laajeneminen tehnyt tietotekniikkarikoksista eräänlaisia maailmanrikoksia ja niiden käsitteleminen viranomaiskoneistossa saattaa poiketa olennaisesti niin sanottujen perinteisten rikosten käsittelemisestä.

Kansainvälinen oikeusyhteisö on ollut kaukaa viisas, kun se on aloittanut harmonisointityön ja ryhtynyt etsimään ratkaisuja tulevaisuuden ongelmiin jo hyvissä ajoin – jos nyt yhtäkkiä jouduttaisiin ilman minkäänlaisia keinoja kohtaamaan se tosiasia, että valtioiden välisillä rajoilla ei ole mitään merkitystä rikoksentekijöiden pidättelemisessä, saattaisivat seuraukset olla katastrofaaliset. Kysymys ei ole pelkästään tietotekniikkarikoksista vaan kaikista niistä rikoksista, joiden tekemisessä tietotekniikkaa ja erityisesti tietoverkkoja voidaan hyödyntää, ja tässä suhteessa tietoverkkojen antama tuki esimerkiksi kansainväliselle järjestäytyneelle rikollisuudelle voi olla pelottavankin suurta.[21]

Monen länsieurooppalaisen valtion kriminalisointitarpeet ovat heränneet juuri kansainvälisen yhteistyön tuloksista. Kansainvälisessä yhteistyössä näkyvät voimakkaina myös niiden valtioiden kansallisten lainsäädäntöjen vaikutuk-

---

[19] Atk-sanakirja, s. 50. Internet = tutkimus- ja yliopistopiireistä yleiseen käyttöön levinnyt kaikille avoin TCP/IP-käytäntöjä noudattavien tietoverkkojen ja yhdyskäytävien muodostama maailmanlaajuinen kokonaisuus.

[20] Atk-sanakirja, s. 211. Tietoverkko = tiedonsiirtoverkon ja siihen kytkettyjen atk-laitteiden ja ohjelmien muodostama kokonaisuus, joka välittää tietoa muuten kuin tavanomaisena puhelinliikenteenä sekä tarjoaa tiedonsiirtoon liittyviä palveluja kuten osoite-, muunnos- ja tietopalveluja.

[21] Internetiin liittyvistä rikoksista ks. esim. Cornils ja Wallich. Cornils käsittelee eri valtioiden toimivallan määräytymistä Internet-rikoksissa ja Wallich kuvaa Internetiä rikoksentekovälineenä ja -ympäristönä enemmän tekniseltä kannalta. Sieber (ks. Internet Law) puolestaan on useassa yhteydessä tutkinut Internetin välityksin liikuteltavaa sisällöltään laitonta aineistoa ja palveluntarjoajien rikosoikeudellista vastuuta tällaisen aineiston suhteen.

set, jotka tietotekniikkarikollisuuden tutkimuksessa ovat olleet edelläkävijän asemassa; tällaisia valtioita ovat ennen muuta Saksa, Kanada ja USA.

Koska tietotekniikkarikollisuuden tutkimus ja siihen liittyvä lainsäädäntö Suomessakin paljolti perustuu ulkomaiseen ja kansainväliseen tutkimukseen, on siihen perehdyttävä, jotta suomalaisen lainsäädännön lähtökohdat tulisivat helpommin ymmärrettäviksi. Kansainvälisen yhteistyön ja ulkomaisen sääntelyn erillinen kuvaaminen niinkin laveasti kuin jäljempänä tapahtuu, on tarpeellista tutkimuksen kokonaisuuden kannalta.

Tietotekniikkarikokset ovat – niin kuin osan I luku 2 osoittaa – viimeiset runsaat viisitoista vuotta olleet niin keskeisessä asemassa kansainvälisessä oikeusyhteisössä, että kansainvälisen näkökulman jättäminen vaille huomiota tai vain vähälle huomiolle antaisi tietotekniikkarikollisuusongelmasta todellisuutta vastaamattoman kokonaiskuvan.

Lisäksi on huomattava, että suomalaisten säännösten aineellinen sisältö on suuressa määrin, oikeastaan täysin, peräisin kansainvälisen tutkimuksen ja yhteistyön tuloksista, jotka näin ollen ainakin tosiasiallisesti siis ovat oikeuslähteenä lain esitöihin rinnastettavassa asemassa. Lainkäyttäjälle ne eivät tosin tarjoa samanlaista tulkinta-apua kuin suomalainen lainvalmisteluaineisto, mutta niiden merkitystä lain tavoitteita selvittävänä tulkintaperusteena ei tule väheksyä.[22]

Kansainvälisen yhteistyön seurauksena eri valtioiden kansalliset rikoslait ovat sisällöltään lähentyneet toisiaan. Niin kauan kuin valtioiden väliset rajat hankaloittivat usean valtion alueelle vaikutuksiaan ulottavien rikosten tekemistä, ei kovin pitkälle menevän harmonisoinnin tarvetta ollut.[23] Nyt tilanne on toinen. Esimerkiksi Euroopan neuvoston jäsenvaltioiden – ja eräiden muidenkin valtioiden – tietotekniikkarikoksia koskeva sääntely perustuu paljolti vuoden 1989 suositukseen ja tulee perustumaan vuoden 2001 yleissopimukseen. Kansallisen lainsäädäntötyön taustalla on vuosien yhteinen kansainvälinen työ ja yhteiset tavoitteet, mistä seuraa, että kansallisia säännöksiä tulkittaessa relevanttia apua saattaa olla saatavilla vieraasta valtiosta, jonka lainsäädäntöön samat periaatteet on implementoitu. Lainsäädäntöjen harmonisoiminen toisin sanoen johtaa oikeusvertailevan aineiston merkityksen lisääntymiseen.

1.1.2.4 Tietotekniikkarikokset ja prosessioikeus

Tietotekniikkarikollisuuden transnationaalisesta luonteesta johtuu ongelmia, jotka edellä selostetuin tavoin osaksi kuuluvat kansainvälisen rikosoikeuden mutta osaksi myös prosessioikeuden alaan. Nämä rikosten selvittämiseen ja

---

[22] Ks. Nilsson, SvJT 96, s. 549 ss., jossa Nilsson selvittää Euroopan neuvoston oikeudellisen työn eri muotojen merkitystä.

[23] Harmonisoinnin tarpeesta ks. Brenner – Goodman.

elektronisen todistusaineiston keräämiseen ja käsittelyyn liittyvät kysymykset muodostavat hyvin laajan ja Suomessa toistaiseksi melko tutkimattoman alueen, joka sinänsä olisi hyvinkin houkutteleva löytöretkeilyn kohde erityisesti *de lege ferenda* -mielessä.

Niin kuin edellä mainitsin, on tilanne sellainen, että esitutkinta- ja pakkokeinolainsäädäntöämme joudutaan Euroopan neuvoston yleissopimusta implementoitaessa remontoimaan. Yleissopimuksen tarkoituksena on esitutkintaa ja pakkokeinoja koskevilta osiltaan helpottaa kansainvälistä yhteistyötä lähinnä velvoittamalla sopimuspuolet säätämään sellaisista kansallisella tasolla käytettävistä pakkokeinoista, jotka mahdollistavat nopeamman menettelyn niin valtionsisäisessä prosessissa kuin oikeusapupyyntöihin vastattaessakin. Vaikka prosessioikeudelliset kysymykset eivät olekaan tämän tutkimuksen kohteena, käsittelen kuitenkin *de lege ferenda* -jaksossa lähinnä kuvailevasti niitä muutoksia, joita lainsäädäntöömme yleissopimuksen velvoittamana ehdotetaan tehtäväksi. Koska muutoksia on tulossa, tällä hetkellä voimassa olevan lain prosessuaalisten säännösten selvittelyllä ei tässä yhteydessä olisi kovinkaan pitkälle ulottuvaa merkitystä.[24]

1.1.2.5 Yhteenveto

Olen nyt rajannut tutkimuksen kohteeksi tietojenkäsittelyrauhan loukkaukset ja niistä erityisesti *datarikokset*. Rikoslain säännösten syntyhistorian samoin kuin säännösten sisällön ymmärtämisen helpottamiseksi tarkastelen kuitenkin ensiksi sekä tietotekniikkarikoksia koskevaa *kansainvälistä* yhteistyötä että tarpeellisin osin myös *ulkomaista* lainsäädäntöä ja tutkimusta – viimeksi mainittua tosin jokseenkin suppeasti ja pintapuolisesti, sillä kansainvälinen yhteistyö on siihen vaikuttanut yleisesti ottaen varsin samaan tapaan kuin Suomessakin eikä tarkastelulla näin ollen ole kovin suurta itsenäistä merkitystä varsinkaan, kun se osoittaa muissa maissa päädytyn kovin samanlaisiin ratkaisuihin.

Enimmillään runsaan 13 vuoden kokemusten jälkeen voidaan havaita rikoslakiin sen kokonaisuudistuksen yhteydessä liitettyjen säännösten olevan joissakin suhteissa puutteellisia tai ainakin vaikeasti tulkittavissa olevia. Aukkojen – joiden määrä teknisen kehityksen myötä on jatkuvasti vaarassa lisääntyä – täyttämiseksi, tulkintavaikeuksien vähentämiseksi sekä säännösten keskinäisen loogisuuden ja yhteensopivuuden parantamiseksi tulen esittämään eräitä *de lege ferenda* -kannanottoja.

Yhteenvedonomaisesti on jäljempänä olevan tutkimuksen rakenne tiivistettävissä seuraavasti: (1) tietotekniikkarikoksia koskeva kansainvälinen yhteistyö sekä ulkomainen tutkimus ja lainsäädäntö osan I luvussa 2.; (2) tietotekniikkarikokset ja erityisesti voimassa oleva datarikoksia koskeva sääntely osan

---

[24] Tätä selvittelyä olen tehnyt vuonna 1994 julkaistussa kirjasessani ”Tietotekniikkarikosten tutkintaan liittyvät ongelmat”. Tilanne ei tuosta ajasta ole sanottavasti muuttunut.

II luvuissa 2–5.; (3) tietotekniikkarikoksiin liittyviä tahallisuuskysymyksiä osan II luvussa 6.; sekä (4) tietotekniikkarikoksia koskevan voimassa olevan lainsäädännön arviointia ja siitä johtuvia ehdotuksia luvussa osan II luvussa 7.

Tutkimuksen keskeisen osan muodostavat osan II luvut 2–5 ja siinä puolestaan keskeisiä ovat kysymykset, miten lainsäädännössä on onnistuttu toteuttamaan valittu periaate perinteisten rikossäännösten täydentämisestä tietotekniset vaatimukset huomioon ottavilla elementeillä, miten selkeää ja yksiselitteistä sääntely on ja miten hyvin voimassaolevat tunnusmerkistöt kattavat sellaiset menettelyt, joita voidaan pitää ja joita tulee pitää moitittavina. Ongelmia on havaittavissa esimerkiksi eräiden tunnusmerkistöjen välisessä rajanvedossa, ja jäljempänä esitettävillä tulkinnoilla samoin kuin ehdotuksilla näiden ongelmien ratkaisemiseksi tulleekin olemaan välittömiä vaikutuksia säännösten soveltamiseen.

Näkökulmani ei välttämättä muodostu puhtaan akateemisen teoreettiseksi enkä yritä sitä sellaiseksi muodostaakaan, sillä olen päässyt kohtaamaan tietotekniikkarikoksiin liittyviä ongelmia kolmessa eri ominaisuudessa: paitsi tutkijana myös syyttäjänä ja lainvalmistelijana. Syyttäjänä ensisijainen kiinnostukseni kohde on tietysti säännösten sovellettavuus yksittäisiin rikosasioihin, ei niinkään niiden soveltuvuus koko rikosoikeudelliseen systematiikkaan. Lainvalmistelijana (johon rooliin luen paitsi toimintani oikeusministeriön lainvalmisteluosastolla myös osallistumiseni kansainvälisten instrumenttien luomiseen) minua kiinnostaa luonnollisesti myös säännösten käytännön toimivuus yksittäistapauksissa, mutta sen ohessa myös tietotekniikkarikoksia koskevan sääntelyn muodostaman kokonaisuuden loogisuus ja kattavuus.

Toivonkin tästä tutkimuksesta olevan hyötyä myös niille, jotka käytännössä joutuvat kohtaamaan tietotekniikkarikosten selvittämiseen liittyviä ongelmia: poliiseille, syyttäjille, tuomareille ja asianajajille. Tämä päämäärä on osaltaan sanellut ne tutkimuksen muotoon ja metodeihin liittyvät ratkaisut, jotka olen toteuttanut erityisesti osan II luvuissa 2–4. Joissain suhteissa kommentaarimaista muistuttava lähestymistapa ei toivottavasti peitä niitä muita tavoitteita, jotka edellä olen asettanut, mutta toivoakseni helpottaa kirjan käyttämistä myös eräänlaisena käsikirjana. Virassani olen joutunut havaitsemaan, että akateemiset opinnäytetyöt eivät aina ole parhaita mahdollisia apuneuvoja etsittäessä ratkaisuja käytännön ongelmatilanteisiin.

Yksittäisten rikossäännösten käsittelyssä en ole katsonut tarpeelliseksi niinkään käsitellä kuhunkin rikostyyppiin liittyviä *yleisiä* kysymyksiä vaan olen petoksen, maksuvälinepetoksen, väärennyksen, vahingonteon, luvattoman käytön ja yritysvakoilun kohdalla ensisijaisesti kiinnittänyt huomioni tietotekniikkaspesifisiin kysymyksiin. Näiden rikosten yleistä luonnetta on käsitelty oppija muissa kirjoissa sekä artikkeleissa eikä yleisillä näkökohdilla useimmissa tapauksissa ole merkitystä tekojen tietoteknistä ulottuvuutta – tietojenkäsittelyrauhan suojaa – arvioitaessa.

Rikossäännösten systematisointi tietojenkäsittelyrauhan eri osa-alueitten perusteella on ratkaisu, joka on muotoutunut lähinnä viime vuosina tapahtuneen kehityksen pohjalta. Yhteisen nimittäjän, *tietojenkäsittelyrauhan,* konstruointi kattavaksi suojeluobjektiksi on mielestäni jo tutkimustulos sinänsä: paitsi että se yhdistää itsessään erityyppiset yksittäiset kriminalisoinnit ja tällä tavoin muodostaa perusteen ryhmittelylle, sen käyttäminen myös helpottaa lain tarkoituksen selvittämistä. Tosin tietojenkäsittelyrauha nimenomaisesti mainittuna on lainvalmistelussa ollut melko harvoin käytetty käsite mutta – niin kuin jäljempänä havaitaan – juuri tietojenkäsittelyrauhan suojaamisesta kriminalisoinneissa on kysymys.

Tietotekniikkarikoksia koskevia korkeimman oikeuden ratkaisuja on tätä kirjoitettaessa olemassa kaksi, jotka molemmat ovat vuodelta 2003. Toinen niistä koskee tietomurtoa ja toinen väärennystä.[25] Niukka oikeuskäytäntö on siis toistaiseksi muodostunut pääasiassa alioikeuksissa ja vähäisessä määrin myös hovioikeuksissa.

Toisaalta tämä tilanne – ennakkotapausten vähäisyys – saattaa hankaloittaa tutkimusta. Toisaalta se kuitenkin pakottaa turvautumaan tulkinnassa muihin oikeuslähteisiin ja tätä kautta kenties löytämään sellaisia näkökulmia, joiden aukeamisen runsas oikeuskäytäntö olisi voinut kokonaan estää. Tästä syystä saattaakin lopulta tietotekniikkarikosten ollessa kysymyksessä oikeustieteen asema oikeuslähteenä korostua mm. oikeuskäytännön rinnalla.

Aarnio jakaa oikeuslähteet kolmeen ryhmään: vahvasti velvoittaviin, heikosti velvoittaviin ja sallittuihin oikeuslähteisiin.[26] Kansainvälisen yhteistyön aiheuttamasta lainsäädännön harmonisoinnista johtunutta oikeusvertailun merkityksen korostumista *Aarnio* ei teoksessaan ole ottanut huomioon eikä liioin kansainvälisten suositusten ja sopimusten asemaa mutta *Aarnion* ryhmittelyn perusteet huomioon ottaen voisi ajatella esimerkiksi kansainvälisen yleissopimuksen sijoittuvan heikosti velvoittavien ja sallittujen oikeuslähteiden välimaastoon.

Itse olen korostanut suojeluobjektin merkitystä säännösten tulkinnassa. Näin ollen ja kun soveltamiskäytäntö on toistaiseksi vähäistä, pyrin hakemaan johtoa tulkinnalle paitsi tietysti lain sanamuodosta, erityisesti *ratio legiksestä*, joka on tai jonka ainakin pitäisi olla johdettavissa lainvalmisteluaineistosta sekä myös tutkittavien säännösten taustalla olevasta kansainvälisestä materiaalista.

Huomattakoon, että puhtaasti tietotekniikkarikoksia käsittelevä oikeustie-

---

[25] KKO 2003:36 ja 58.

[26] Ks. Aarnio, s. 220 s., jossa oikeuslähteiden jako kolmeen ryhmään: (a) vahvasti velvoittavat eli laki ja maantapa, (b) heikosti velvoittavat eli ratio legis ja tuomioistuinratkaisut sekä (c) sallitut oikeuslähteet, jotka vahvistavat argumentaatiota mutta joiden sivuuttamisesta ei ole ennustettavia seurauksia; näitä ovat oikeusvertailevat ja oikeushistorialliset argumentit, oikeustiede, arvot ja arvoarvostelmat sekä teleologiset argumentit.

teellinen kirjallisuus on Suomessa käytännössä olematonta.[27] Tosin esimerkiksi yritysvakoilusta, joka kuuluu tietoteknisten elementtiensä osalta tässä tutkimuksessa käsiteltäviin kriminalisointeihin, on jonkin verran kirjoitettu[28] mutta pääpaino ei ole ollut tietotekniikkarikosominaisuudessa. Euroopassakaan ei viime vuosina ole julkaistu merkittäviä monografioita datarikosten osalta, mutta Internetin laittomia sisältöjä ja niihin liittyviä rikoksia on jonkin verran tutkittu. Vaikuttaa yleisesti ottaen siltä, että tässä suhteessa ollaan jollain lailla odottavalla kannalla, tai sitten rikosoikeustieteilijät vain jostain syystä suhtautuvat aihealueeseen varauksellisesti.

Ennen kuin on mahdollista siirtyä varsinaiseen oikeudelliseen tarkasteluun, on kuitenkin tehtävä selkoa eräistä käsitteistä, joilla jäljempänä tulen operoimaan. Seuraavan jakson laajahkolla filosofisella käsiteanalyysillä ei ole tarkoitus hakea vastausta esimerkiksi siihen vaikeaan kysymykseen, mitä tieto, data ja informaatio pohjimmiltaan ovat. Sen sijaan tarkoituksena on löytää noille käsitteille kullekin sellainen täsmällinen sisältö, että niitä voidaan käyttää selkeästi merkityksiltään toisistaan eroavina paitsi tässä tutkimuksessa myös yleensä tietotekniikkarikoksista puhuttaessa.

1.2 TUTKIMUKSEN KÄSITTEISTÄ JA METODEISTA

1.2.1 Yleistä

Rikosoikeuden yleisiä oppeja koskeva lainsäädäntö on uudistettu 1.1.2004 voimaan tulleella lailla 515/13.6.2003. Rikoslain uudessa 3 luvun 1 §:ssä säädetään laillisuusperiaatteesta: rikokseen syylliseksi saa katsoa vain sellaisen teon perusteella, joka tekohetkellä on laissa nimenomaan säädetty rangaistavaksi (1 mom.), ja rangaistuksen ja muun rikosoikeudellisen seuraamuksen on perustuttava lakiin (2 mom.). Vastaava laillisuusperiaate on jo aikaisemmin ilmaistu Suomen perustuslain (731/1999) 8 §:ssä ja se on kirjattu mm. Euroopan ihmisoikeussopimukseen (SopS 18–19/1990) sekä kansalaisoikeuksia ja poliittisia oikeuksia koskevaan kansainväliseen yleissopimukseen (SopS 7–8/1976).[29] Laillisuusperiaate asettaa tiettyjä rajoja säännösten tulkinnalle niitä sovellettaessa. Palaan tulkintaan liittyviin kysymyksiin tarkemmin jäljempänä tämän luvun jaksossa 1.2.3.3.

Oikeudellisia säännöksiä sovellettaessa on välttämätöntä ymmärtää, mitä niillä *tarkoitetaan,* mikä on niiden merkityssisältö. Useimmissa tilanteissa ei merkityksen selvittäminen aiheuta kovin suuria ongelmia, sillä laillisuusperi-

---

[27] Ks. kuitenkin esim. Hannula – Siilasmaa, s. 168 ss., jossa on jokseenkin hyvä, tosin suppeahko ja melko pinnallinen kuvaus kymmenen vuoden takaisesta ”atk-rikoksia” koskevasta sääntelystä.

[28] Erityisesti Klaus Nyblin on käsitellyt aihetta.

[29] Ks. Matikkala, Näkökohtia, s. 221 ss.

aatteesta johtuen lainsäätäjään on katsottava kohdistuvan vaatimus rikoslain sisällön täsmällisyydestä. Sekä rangaistuksella uhatun toiminnan kuvaus että teosta seuraava rangaistus on määriteltävä sellaisella tarkkuudella, että ihmiset voivat ennakolta tietää, mikä on rangaistavaa ja miten ankarasti.[30]

Säännös on saatettu kirjoittaa tavalla, joka vastaa yleiskielistä ilmaisua (esim. RL 35:1 ”Joka oikeudettomasti hävittää tai vahingoittaa toisen omaisuutta...”), tai sitten käsitteet, joiden voidaan olettaa olevan ainakin käyttöyhteydessään tulkinnanvaraisia, määritellään erityisissä määritelmäsäännöksissä (esim. RL 37:12). Toki on edellytettävä, että esimerkiksi käsitteen ”oikeudettomasti” sisältö vahingontekosäännöstä sovellettaessa on tutkittava tapauskohtaisesti, mutta tällöin ei ole kysymys säännöksen sanamuodon tulkinnasta vaan tosiasiallisen olotilan selvittämisestä, sillä oikeudettomuus on yleiskielinen termi, jolla on vahingontekorikoksen kysymyksessä ollen vakiintunut merkitys: ilman lupaa, vastoin kieltoa tai lupaan perustuva oikeus ylittäen.

Epäselvissä tulkintatilanteissa voidaan apua etsiä erilaisista oikeuslähteistä: lain sanamuodon lisäksi lain esitöistä, oikeuskäytännöstä, oikeustieteellisestä kirjallisuudesta jne.[31] Tällöin saatetaan kuitenkin joutua toteamaan lainvalmisteluaineiston olevan siinä määrin ikääntynyttä, että kysymyksessä olevaan tilanteeseen ei ratkaisua löydy – siitä yksinkertaisesta syystä, että tilannetta ei lakia säädettäessä ole voitu ottaa huomioon. Hyvä esimerkki on vanhan lain mukaisen asiakirjan käsitteen kattavuus suhteessa tietoteknisiin tallenteisiin.

Joillakin lainsäädännön alueilla on olemassa hyvin teknisiä ja yksityiskohtaisia säännöksiä. Tällaisia löytyy runsaasti esimerkiksi ajoneuvojen rakenteesta ja varusteista annetussa asetuksessa (1256/1992). Rikoslaissa on tämäntyyppisiä säännöksiä pyritty viime vuosiin saakka välttämään, joskin vaikuttaa siltä, että yhteiskunnan monimutkaistuminen ja monimuotoistuminen samoin kuin yhteiskunnan ja sen jäsenten erilaisten toimintojen jatkuva teknistyminen yhä enenevässä määrin edellyttää sanonnoilta ja ilmaisuilta entistä suurempaa täsmällisyyttä. Selvää on, että kovin yksityiskohtaiseen ja kasuistiseen sääntelyyn ei rikosoikeuden alueella voida mennä, mutta jollain tavoin olisi kyettävä järjestämään tilanne sellaiseksi, että normien merkityssisällön selvittäminen ei uusissakaan, jatkuvasti muuttuvissa olosuhteissa olisi kohtuuttoman vaikeaa – ei sille, jonka on normeja sovellettava, eikä varsinkaan sille, jonka edellytetään normeja noudattavan.[32] Palaan lain tulkintaan liittyviin kysymyksiin tarkemmin jäljempänä tämän luvun jaksossa 1.2.3.3.

Tietotekniikka on selkeästi jotain aivan muuta kuin juridiikkaa. Terminologia on teknistä ja matemaattista eikä sitä ole kehitetty tai tutkittu oikeudellisia tarpeita silmällä pitäen. Tietotekniikkaan liittyviä rikoksia koskevat säännökset puolestaan on koetettu sopeuttaa rikoslain systematiikkaan ja terminologiaan.

---

30 Ks. HE 44/2002, s. 29.
31 Ks. edellä jaksossa 1.1.2.5 lausuttu.
32 Siitä, mitä tulee säännellä ja miten yksityiskohtaisesti, ks. Matikkala, Näkökohtia, s. 217 s.

Säännökset ovat juristien laatimia ja lähtökohtana ovat olleet juristien tarpeet. Olen itse lainvalmistelutyöhön osallistuneena havainnut, miten vaikeaa on saada teknologi ymmärtämään juristin ajatuksia – ja luonnollisesti myös päinvastoin. Tavallisen tietotekniikan arkikäyttäjän käsitteistö taas poikkeaa niin juristin kuin tekniikan ammattilaisenkin käyttämästä kielestä.

Tietotekniikkarikosta ei ole lainsäädännössä määritelty. Käsite on kuitenkin yleisesti käytetty, niin meillä kuin muuallakin. Määritelty ei ole myöskään yleisesti käytettyjä käsitteitä tieto, data ja informaatio, ja myös tallenteen käsite jää rikoslain sanamuodon puitteissa epäselväksi. Yritän tässä luvussa antaa muun muassa näille käsitteille sellaiset täsmälliset sisällöt, joita hyväksi käyttämällä tietotekniikkarikoksia koskevien säännösten semanttiset tulkinnanvaraisuudet ainakin vähenisivät – kokonaan poistetuksi niitä ei koskaan saada.

Tällaisen menettelyn oikeutus näin tavallaan jälkikäteen – joidenkin säännösten kohdalla kymmenen vuotta niiden säätämisestä – tehtynä saatetaan ehkä pyrkiä kyseenalaistamaan. Katson kuitenkin, että tämä on paitsi oikeutettua myös tarpeellista: ensinnäkin vanhempien tietotekniikkarikossäännösten esitöissä nämä kysymykset ovat yleensä jääneet vaille riittävää huomiota ja toiseksi tietotekniikkarikoksia koskeva lainsäädäntöprosessi ei ole ollut yhtenäistä vaan on tapahtunut ikään kuin rikoslain kokonaisuudistuksen ohessa ilman, että tietotekniikkarikoksia koskaan olisi tarkasteltu yhtenä kokonaisuutena.

Sitä paitsi lähden käsitteiden täsmentämisessä siitä tarkoituksesta ja lainsäätäjän tahdosta, joka voimassa olevista säännöksistä ilmenee; kysymys on itse asiassa pyrkimyksestä löytää muutamia rikosoikeudellisen tietotekniikkaa koskevan sääntelyn yhteisistä nimittäjistä ja saattaa ne sellaiseen muotoon, että niistä voisi olla hyötyä paitsi voimassa olevaa sääntelyä sovellettaessa myös tulevaa sääntelyä kehitettäessä.

Yhteinen nimittäjä käsitteistön ohessa – tosin hieman toiselta kannalta – on tietotekniikkarikosten tietojenkäsittelyn luottamuksellisuudesta, eheydestä ja käytettävyydestä muodostuva suojeluobjekti, jota käsittelen tarkemmin tämän luvun lopussa jaksossa 1.2.3.4 Tietojenkäsittelyrauhan käsitettä ei lainsäädäntömme nimenomaisesti tunne, vaikkakin se on lainvalmistelun yhteydessä aika ajoin ollut esillä ja tällä tavoin saavuttanut jossain mielessä virallisesti hyväksytyn aseman. Käsitteen omaksuminen ja ottaminen tämän tutkimuksen keskeiseksi ideaksi saattaa sekin herättää arvostelua.

On kuitenkin syytä korostaa, että tietotekniikkarikokset on varsinkin kansainvälisesti jo pitkään nähty selkeästi yhtenä rikoskategoriana, jonka sisältö tosin on rajoiltaan jossain määrin epätäsmällinen mutta jossa mielestäni voidaan perustellusti todeta olevan muitakin yhteisiä elementtejä kuin vain tekoympäristöön ja tekotapoihin liittyvät seikat. Tietotekniikkarikokset liittyvät aina tavalla tai toisella tietojenkäsittelyprosessiin, jolle on usein ominaista tietynasteinen luottamuksellisuus ja yksityisyys.

Näiden arvojen loukkaaminen on eittämättä tietotekniikkarikosten yhteinen

elementti, olkoonkin, että niiden suojaaminen ei välttämättä ole tietotekniikkarikoksia koskevien kriminalisointien ensisijainen tehtävä.

1.2.2 Tieto, data ja informaatio

Lähdettäessä etsimään määritelmää *tietotekniikkarikoksen* käsitteelle on ensiksi selvitettävä eräiden muiden sanojen merkityssisältöjä. Jotta voitaisiin ymmärtää, mitä *tietotekniikalla* tarkoitetaan, on pyrittävä määrittelemään *tiedon* käsite; jotta tietotekniikkarikosten jäljempänä esitettävä jako data- ja informaatiorikoksiin tulisi selväksi, on käsitteille *data* ja *informaatio* annettava tarkempi sisältö.

1.2.2.1 Tieto

Yleistä

Sanan ”tieto” merkityssisältö on suomen kielessä hyvin laaja. Atk-sanakirja[33] määritteli esimerkiksi vielä vuoden 1991 painoksessaan tiedon jokseenkin yksinkertaisesti: tieto on ihmisen ajattelun kohde tai tulos ja sanaa käytetään yhteydestä riippuen sanojen data, informaatio, tietämys ja sanoma synonyyminä.[34] Niin kuin Atk-sanakirjan määritelmät yleensäkin on tämäkin määritelmä vuosien varrella täsmentynyt ja vuoden 1999 painoksessa[35] tiedon sanotaan olevan ”asia ihmisen ymmärtämänä tai vastaanottamana *(informaatio)* tai konkreettisessa esitysmuodossa ilmaistuna *(data)*”. Lisäksi todetaan sanan sisältävän myös merkitykset *tietämys* ja *sanoma*.[36]

Kun tarkastellaan esimerkiksi Atk-sanakirjan tarjoamia englanninkielisiä vastineita sanalle tieto, huomataan, miten kovin erilaisia käsitteitä käännetään yhdeksi ja samaksi suomen kielen sanaksi. Erään englannin sanakirjan[37] mukaan *data* on ”facts; things certainly known (and from which conclusions may be drawn)”, *information* toisaalta ”informing or being informed”, toisaalta ”sth. told, news or knowledge given”,[38] *knowledge* toisaalta synonyymi sanalle ”understanding”, toisaalta ”familiarity gained by experience; range of information” sekä lopuksi *message* ensinnäkin ”piece of news, or a request, sent to sb.”,

---

[33] Atk-sanakirja on Tietotekniikan liitto ry:n julkaisu. Kirjaa on julkaistu säännöllisesti vuodesta 1966 lähtien ja kymmenennen painoksen esipuheen mukaan teoksesta on kuluneen kolmannesvuosisadan aikana kehittynyt tietotekniikan käsitteistön ja termistön kiistaton auktoriteetti Suomessa. Kirja sisältää kaksi pääosaa: suomenkielisten hakusanojen mukaisen määritelmäosan sekä vieraskielisten termien käännöshakemistot.

[34] Määritelmää voidaan syystä pitää epäonnistuneena; niinpä Niiniluoto kysyykin, onko kinkku ”tietoa”, jos ajattelee joulukinkkua, ja onko ajattelun tuloksena syntyvä kinkun himo, päätös ostaa kinkku tai kinkun ostaminen ”tietoa”? Niiniluoto, s. 48.

[35] Atk-sanakirja, s. 202.

[36] Ulkomaisina vastineina mainitaan mm. englannin *data* ja *information,* ruotsin *data* ja *information* sekä saksan *Daten* ja *Information.*

[37] Hornby ym., s. 249.

[38] *Inform* määritellään ”give knowledge to”. Hornby ym., s. 506.

toiseksi synonyymi sanalle ”errand” ja kolmanneksi ”sth. announced by a prophet and said to be inspired; teaching”.

Nykysuomen sanakirja antaa hakusanalle ”tieto” lukuisia merkityksiä. Ensinnäkin sanaa voidaan käyttää merkityksessä ”jollakulla on tieto jostakin; joku tietää, on selvillä, tietoinen jostakin”. Sanaa voidaan toiseksi käyttää synonyyminä sanoille ”tietäminen” ja ”järki” sekä kolmanneksi sanojen ”tietoisuus” ja ”vakaumus” synonyyminä. Edelleen tieto voi olla ”tietämiseen perustuva käsitys jostakin; olettamus, otaksuma, arvelu, luulo, usko”. Tieto saattaa olla asia, seikka tai yksityiskohta, joka jostakin tiedetään, annetaan tai saadaan tietää, sekä tähän liittyen synonyymi sanoille ”ilmoitus”, ”tiedonanto”, ”tiedotus”, ”sana”, ”sanoma”, ”viesti”, ”uutinen”.

Tiedolla voidaan ymmärtää ”opetuksen, opintojen, tutkimusten, kokemuksen tms. tuloksena saatua henkistä pääomaa, kaiken sen summaa, mitä joku tietää tai mitä tiedetään jostakin, tuntemusta, tietoutta, tietämystä, oppia, viisautta”. Viimeisenä tieto-sanan käyttötarkoituksena sanakirjassa mainitaan käyttö yhdyssanojen jälkiosana, kun kysymys on tieteenhaarasta erityisesti koulun oppiaineena.

Kun vielä todetaan, että Atk-sanakirja määrittelee *datan* ”tiedoksi luettavassa, viestitettävässä tai käsiteltävässä muodossa” ja *informaation* ”datan ihmiselle tuottamaksi mielteeksi tai merkitykseksi”,[39] voidaan sanoa, että sanakirjojen antama apu ei ole kovin suuri yritettäessä luonnehtia tiedon käsitettä tietotekniikkarikoksen määrittelyn perustaksi.

Niiniluoto toteaakin suomen kielessä 1960-luvulta lähtien tapahtuneen käsitteellisen romahduksen: tieto voi nykyään merkitä melkein mitä tahansa.[40] Jos sanoja ”tieto” ja ”data” pidetään synonyymeinä, on *Niiniluodon* mukaan tästä tietojenkäsittelyoppiin sekä talous- ja hallintotieteisiin levinneestä valinnasta muun sekavuuden ohella seurauksena se, että tieto-sanan perinteelliseen merkitykseen liittyvä totuudenmukaisuuden vaatimus jää helposti tarkastelun ulkopuolelle: sopivaa vastinesanaa tälle vahvalle tiedon käsitteelle ei ole enää käytettävissä.[41]

Tieto ja totuus

Totuudenmukaisuuden vaatimuksella näyttäisi siis olevan erityistä merkitystä tiedon käsitettä selviteltäessä. *Niiniluoto* sanoo tieto-opin keskeisen ongelman olevan siinä, mitä lisäehtoja kognitiivisesti mielekkään, totuusarvon omaavan väitelauseen on täytettävä, jotta sitä voisi kutsua tiedoksi, ja käsittelee tässä yhteydessä *Platonin* klassista tiedon määritelmää, jonka mukaan tieto on (i) hyvin perusteltu (ii) tosi (iii) uskomus.[42] Määritelmän ehdoista (i) erottaa tiedon

---

[39] *Niiniluoto* toteaa tältä osin, että ”jos informaatiota on vain mielteenä ihmisen päässä, niin atk-alan ihmisten pitäisi pikaisesti lopettaa puhe informaation ’siirrosta’ viestintävälineiden avulla tai informaation ’käsittelystä’ ja ’tallentamisesta’ tietokoneissa”. Niiniluoto, s. 43 s.

[40] Niiniluoto, s. 48.

[41] Niiniluoto, s. 65.

[42] Niiniluoto, s. 57 ss.

pelkästä luulosta, (ii) erehdyksestä ja (iii) hypoteettisesta arvauksesta.

Koska ehtoa (iii) voidaan *Niiniluodon* käsityksen mukaan ehkä pitää vähiten merkityksellisenä (se liittyy traditionaaliseen ajatukseen, että tieto tai tietäminen on ihmisen mielen tila), voidaan klassinen määritelmä tiivistää seuraavasti: tieto on väitelauseiden sisältämää semanttista informaatiota, joka täyttää perusteluehdon (i) ja totuusehdon (ii).[43]

Klassista tiedon määritelmää on kritisoitu eri filosofisissa koulukunnissa erilaisin perustein; on katsottu, että tieto klassisen määritelmän mielessä ei ole ihmiselle mahdollista. *Niiniluodon* oma käsitys tiedon mahdollisuudesta edustaa ns. kriittistä tieteellistä realismia; sen mukaan voidaan kutsua ”tiedoksi” niitä väitteitä, joille on olemassa toistaiseksi paras perustelu – siitä huolimatta, että niiden totuutta saatetaan epäillä ja myös olla oikeassa tässä epäilyssä. Tämä fallibilistinen kanta[44] ei kuitenkaan *Niiniluodon* mukaan ole skeptisistinen, sillä uuden evidenssin sekä uusien käsitteiden ja teorioiden myötä tieto paranee lähestymällä totuutta.

Hintikka näkee totuudellisuuden eli asiaintilan vastaavuuden väitteen ja todellisuuden suhteen siksi elementiksi, joka tekee tiedosta tietoa. Tiedon totuudellisuus on kuitenkin pikemmin käsitejärjestelmään sidottu aiemmin oletettuun tietoon pohjautuva malli kuin absoluuttinen käsitys todellisuudesta.[45]

Hilpisen mukaan totuudellisuus on tiedon välttämätön tunnusmerkki eli välttämätön ehto. Erheelliset mielipiteet voisivat olla korkeintaan ”tietoa”, eivät tietoa: jos käsitys ei ole tosi, sitä ei voida tietää todeksi. Voidaan tosin puhua ”vääristä tiedoista”, mutta tällöin sanalla ’tieto’ tarkoitetaan vain *informaatiota,* so. väitettä, joka voi olla tosi tai epätosi.[46]

Lienee selvää, että suomalainen sanakirjamääritelmä käsitteelle ”tieto” on aivan liian laaja-alainen voidakseen tulla kysymykseen lähtökohtana tämän tutkimuksen käsitteistöä täsmennettäessä. Suhteessa tämän tutkimuksen kannalta merkityksellisiin lähikäsitteisiin sanalle ”tieto” tuntuisi ensisijaiselta merkitykseltä suomenkielinen vastine englannin kielen sanalle ”knowledge”. *The HarperCollins Dictionary of Philosophy*[47] antaa sanalle seuraavan määritelmän:

> **knowledge** 1. recognition of something. 2. familiarity or acquaintance with something from actual experience. 3. that which is learned. 4. clear perception of what is regarded as fact, truth, or duty. 5. information and/or learning that is preserved and continued by civilizations. 6. things held

---

43 Niiniluoto, s. 58.

44 Ks. esim. Popper, s. 265, jossa Popper esittää kaksi teesiä: ”(i) We are fallible, and prone to error; but we can learn from our mistakes. (ii) We cannot justify our theories, but we can rationally criticize them, and tentatively adopt those which seem best to withstand our criticism, and which have the greatest explanatory power.”

45 Hintikka, s. 2 s.

46 Hilpinen, s. 13 s.

47 Angeles, s. 156 ss.

> in conciousness (beliefs, ideas, facts, images, concepts, notions, opinions) that become justified in some way and thereby are regarded as true.

Määritelmä ei edellytä tiedolta missään sen merkityksessä absoluuttista totuudellisuutta. Tiedon totuudellisuuden absoluuttisuus tai relatiivisuus ei kuitenkaan ole olennainen kysymys silloin, kun tietoa tutkitaan rikoksen mahdollisena teko-objektina.

Epistemologisesti määritellyn tiedon on ylipäänsä hyvin vaikea kuvitella olevan rikosoikeudellisesti moitittavan menettelyn kohteena; kun rikoslain 36 luvun 1 §:n 2 momentissa puhutaan ”vääristä tiedoista”, eivät nämä ”tiedot” täytä totuudellisuuden vaatimusta sen paremmin tunnusmerkistön objektiivisen kuin subjektiivisenkaan puolen kannalta, koska ne ovat vääriä – ei-totuudellisia – niin suhteessa teon kohteena olevaan prosessiin kuin tekijän tietoisuuteenkin.

Tietysti tunnusmerkistönmukaisesti ”väärä” tieto saattaa jossain muussa tilanteessa tai suhteessa olla tosi; lainkohdan perustelujen mukaan väärän tiedon syöttämistä voisi olla esimerkiksi toiselle kuuluvan tunnistetiedon käyttäminen, ja epäilemättä tällainen tunnistetieto on tosi ja oikea silloin, kun sitä käyttää sen haltija, mutta silloin ei enää olekaan kysymyksessä tietojenkäsittelypetos. Tässä tarkoitettu vääryys on siis suhteellinen ominaisuus, joka riippuu kulloisestakin (käyttö)tilanteesta.

Edellä kuvatussa tilanteessa siis tiedolla tarkoitetaan jotain muuta kuin sanan ”knowledge” suomenkielistä vastinetta. Yleiskieltä käytettäessä on mahdollista puhua ”väärästä” ja ”oikeasta” tiedosta, koska tiedolta ei tuolloin edellytetä totuudellisuutta. Sen sijaan epistemologiseen tiedon käsitteeseen liitettynä epiteettipari ”väärä” ja ”oikea” tuntuu mahdottomalta; ainakin jos oikealla ymmärretään toden synonyymiä ja vastaavasti väärällä samaa kuin epätosi.

Professori *Pekka Pihlanto* kirjoittaa otsikon ”Tiedon käsitettä hyvä ajatella oikein laajasti”[48] alla mielipidekirjoituksessaan mm. seuraavasti:

> On hyvä tiedostaa, että kaikki tietoverkoissa esiintyvät tekstit, luvut, kuviot ja äänet ovat aluksi edustaneet ”vain” merkityksiä esittäjänsä tajunnassa. Näin ”tiedon” moninaisuus, suhteellisuus ja mahdollinen subjektiivisuus tulee asianmukaisesti huomioon otetuksi. Jokainen viesti tulee tulkituksi vastaanottajan tajunnassa subjektiivisella, asianomaisen maailmankuvan ja tilanteen säätelemällä tavalla, eikä välttämättä niin kuin lähettäjä oletti.
>
> Edellä esitetty käsitys, jota voitaisiin kutsua humanistiseksi tietokäsitykseksi, ei pyri vähättelemään eksaktin tosiasiatiedon merkitystä. Tarkoitukseni on vain muistuttaa tiedon ja tietämisen inhimillisestä ulottuvuudesta ja siten sen suhteellisuudesta. – – Saattaa olla, että tietoverkko-

[48] Ks. Pihlanto.

> jen eräs vaikutus tulee olemaan juuri tietokäsityksen laajeneminen ja henkilökohtaistuminen.

Pihlannon kirjoitus osaltaan osoittaa, miten vaikean tehtävän eteen joudutaan yritettäessä sopeuttaa yleiskieleen perustuvaa käsitteistöä rikosoikeudelliseen sanastoon, jossa tulkinnanvaraisuuksia ei oikeastaan saisi olla lainkaan. Suomen Akatemian tutkija *Erkki Karvosen* mielipide[49] osaltaan kuvaa tätä ongelmaa. Hänen mukaansa ”suurin ongelma tiedosta ja informaatiosta keskusteltaessa on se, että arkipuheen ja teknologisen puheen määritelmät ’informaation’ käsitteelle ovat aivan erilaiset. Keskusteluun tulee sekaannuksia, kun sanaa käyttävät keskustelijat luulevat puhuvansa samasta asiasta, vaikka tosiasiassa viittaavatkin aivan eri asioihin.”

Tiedon käsitteen merkityssisältö jää loppujen lopuksi rajoiltaan siinä määrin epäselväksi, että yksin tällä käsitteellä ei pystytä tehokkaasti operoimaan. Sen vuoksi on tutkittava, miten ”data” ja ”informaatio” käsitteinä suhtautuvat ”tietoon”.

1.2.2.2 Data

Laajassa ruotsalaisessa komiteanmietinnössä *Information och den nya InformationsTeknologin* on seuraava määritelmä:

> *Data i informationsteknisk mening* är representationen av fakta, begrepp eller instruktioner i en form lämpad för överföring, tolkning eller bearbetning utförd av människor eller av automatiska hjälpmedel. Genom denna inriktning på själva representationen av information har begreppet data givits en konkret betydelse.[50]

Mietinnössä todetaan edelleen, että määritelmä ei koske yksinomaan automaattista tietojenkäsittelyä eikä siis myöskään tarkoita, että datan (representationen av informationen) tulisi olla tietokoneella käsiteltävissä olevassa muodossa; määritelmä kattaa myös tilanteet, joissa informaatiota edustaa visuaalisesti luettavissa oleva kirjoitus.

Silvander on samalla kannalla sanoessaan että käsitteellä data ”avses representation av fakta, begrepp eller instruktioner lämpade för överföring eller bearbetning via ett tekniskt hjälpmedel”.[51]

Rikoslain kokonaisuudistuksen ensimmäistä vaihetta koskevan hallituksen esityksen 35 luvun 1 §:n perusteluissa datan todetaan tarkoittavan tiedon asiasisältöä viestittäviä merkkejä.[52] Datalla on siis tässä suunnilleen sama merkitys

---

[49] Ks. Karvonen.
[50] SOU 1992:110, s. 83.
[51] Silvander, s. 120.
[52] HE 66/88, s. 125. Ks. myös Lahti, LM 91, s. 882 s.

kuin ruotsalaisen mietinnön määritelmässä, eikä data näin ymmärrettynä tarkoita pelkästään automaattiseen tietojenkäsittelyyn soveltuvia merkkejä.

Edellä on jo esitetty Atk-sanakirjan määritelmä, jonka mukaan data on tieto luettavassa, viestitettävässä tai käsiteltävässä muodossa. Määritelmä tarkoittanee samaa kuin edellä kuvatutkin, mutta on tulkinnanvaraisempi. Jos tiedon asiasisältö välitetään analogisessa muodossa esimerkiksi puhelin- tai radioviestinnän keinoin, onko puhe silloin dataa? Sehän on asian esitys viestitettävässä ja ehkä myös käsittelykelpoisessa muodossa. Muuttuuko tilanne – ja jos, niin miten – kun puhe välittyykin esimerkiksi ISDN-tekniikkaa[53] käytettäessä digitaalisessa eli pelkästään numeroista koostuvassa (numeerisessa) muodossa? Entäpä sitten puhe suoraan ihmiseltä toiselle ilman muita (teknisiä) apuvälineitä kuin väliaine, jossa ääniaallot liikkuvat? Tai puhe ihmiseltä toiselle, kun informaatio siirtyy ääniaaltoina mutta apuvälineitä käytetään lähettämisessä (megafoni) ja / tai vastaanottamisessa (kuulokoje)?

Niiniluoto esittää käsitehierarkian, jossa informaatio on laajempi yläkäsite, tieto taas sen suppeampi erikoistapaus, johon liittyy jonkinlainen menestyksen, totuudenmukaisuuden ja perusteltavuuden lisäehto.[54] Informaation osalta voidaan erottaa ei-kielellinen informaatio, informaatiota kantavat merkit tai merkkijonot eli data sekä kielellisen informaation syntaktinen, semanttinen ja pragmaattinen taso. Näin siis *Niiniluotokin* näkee datan nimenomaan informaation kantajana, joka käsitys vastaa niin suomalaisten kuin ruotsalaistenkin rikoslainvalmistelijoiden näkemyksiä.

Kun datan kantasana on latinankielen *dare* eli antaa, on datan suomennokseksi suositeltu sanaa *anne.* Sanalla ja sen johdannaisilla on *Niiniluodon* mukaan se etu, että ne eivät ole harhaanjohtavalla tavalla päällekkäisiä minkään perinteisen käsitteen kanssa: vaikka ”data” käännetään sanalla ”tieto”, käänteinen ei päde; filosofien tieto-oppi ei ole ”dataoppia” eikä tietokilpailu ole ”datakilpailu”.[55]

Jälleen siis huomataan tieto-sanan ensyklopedisen merkityksen laaja-alaisuudesta aiheutuvan semanttisia ongelmia; vaikka koneellisesti käsitellään nimenomaan dataa, puhutaan Suomessa tietojenkäsittelylaitteella[56] tapahtuvasta tietojenkäsittelystä. Yleensäkin tietoteknisten (ruots. datatekniska) termien kysymyksessä ollessa on sana ”data” käännetty sanalla ”tieto”.

Datan käsitettä on – erityisesti yleissopimuksen soveltamista ajatellen – pyritty selventämään Euroopan neuvoston tietoverkkorikoskonventiossa. Yleissopimuksen 1 artiklan b kohdassa on seuraava määritelmä:

---

[53] Atk-sanakirja, s. 51. ISDN (Integrated Services Digital Network) = useita tiedonsiirtopalveluja tarjoavan numeerista tiedonsiirtotekniikkaa käyttävän verkon määritys.

[54] Niiniluoto, s. 18 ss.

[55] Niiniluoto, s. 29.

[56] Atk-sanakirjan (s. 203) mukaan tietojenkäsittelylaite on englanniksi *data processor,* ruotsiksi *databehandlingsenhet* t. *-hanterare* ja saksaksi *Datenverarbeitungsanlage.*

> ”Data” tarkoittaa sellaisessa muodossa olevien tosiseikkojen, tietojen tai käsitteiden esitystä, että se soveltuu käsiteltäväksi tietojärjestelmässä, mukaan lukien ohjelmat, joiden avulla tietojärjestelmä pystyy suorittamaan jonkin toiminnon.[57]

Määritelmä on jokseenkin samansisältöinen kuin esimerkiksi edellä esitetty ruotsalainen määritelmä. Yleissopimuksen selitysmuistion kohdassa 26 lausutaan vielä seuraavaa:

> The definition of computer data builds upon the ISO-definition of data. This definition contains the terms ”suitable for processing”. This means that data is put in such a form that it can be directly processed by the computer system. In order to make clear that data in this Convention has to be understood as data in electronic or other directly processable form, the notion ”computer data” is introduced. Computer data that is automatically processed may be the target of one of the criminal offences defined in this Convention as well as the object of the application of one of the investigative measures defined by this Convention.

1.2.2.3 Informaatio

Yleistä

Ruotsalaisessa lainvalmistelussa on tutkittu myös sanan ”informaatio” (information) sisältöä seuraavalla tavalla:

> I vanligt språkbruk brukar man beteckna som *information* ett meddelande som uttrycker ett sakförhållande, har ett syfte eller utlöser ett agerande. Information sägs öka mottagarens kunskap, minska hans osäkerhet eller möjliggöra ett agerande. Ett meddelande övergår till att bli information antingen genom en direkt tolkning av människor eller genom en indirekt tolkning efter en förberedande maskinell bearbetning. – – Information omfattar alltså sammanfattningsvis ett meddelande i förening med dess betydelse för mottagaren.[58]

Lainsäätäjän kannalta todetaan merkitykselliseksi eron tekeminen oikean (sann) ja aidon (äkta) informaation välillä; edellisellä tarkoitetaan oikeita tietoja sisältävää informaatiota, jälkimmäisellä informaatiota, joka, sisältääpä se oikeita tai vääriä tietoja, on peräisin siltä, joka on tietojen antajaksi ilmoitettu. Sekaantumisen vaaraa aiheuttaa, että sanaa väärä (falsk) käytetään sekä oikean että aidon vastakohtana.

---

[57] ”Computer data” means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.

[58] SOU 1992:110, s. 81.

Koska sanalla ”tieto” ei ole ruotsin kielessä yhtä laajamerkityksistä vastinetta, ei mietinnöstä juuri löydy apua tiedon ja informaation väliseen rajanvetoon.[59] Suomalaisessa lainvalmistelussa kysymystä ei ole syvällisesti käsitelty. Rikoslain kokonaisuudistuksen toista vaihetta koskevassa hallituksen esityksessä lausutaan ehdotetun 38 luvun perusteluissa tiedosta, datasta ja informaatiosta seuraavasti:

> Jo suomen kielen sana *tieto* on monimerkityksinen ja voi yhtä hyvin viitata tietoon informaationa kuin kuvata tietämystä yleensä tai sitten tarkoittaa ainoastaan niin sanottua ”dataa”. *Datalla* puolestaan useimmiten tarkoitetaan asian säännönmukaista esitystä viestitettävässä tai käsittelykelpoisessa muodossa, toisin sanoen data kuvaa tietoja esittäviä merkkejä. Tiedossa informaationa taas on kysymys itse tiedon sisällöstä.[60]

Datan määritelmä edellä olevassa lainauksessa on otettu suoraan Atk-sanakirjan vanhemmista painoksista, joissa informaatio määriteltiin nykyversion tavoin datan ihmiselle tuottamaksi mielteeksi tai merkitykseksi. Viimeksi mainittu määritelmä on liian epämääräinen: data (esimerkiksi paperiarkilla oleva käsin kirjoitettu teksti) voi tuottaa lukijalleen täysin tekstin sisällöstä riippumattoman mielteen (”onpa huono käsiala!”). Tällöin voidaan tietysti kysyä, mitä sanalla ”mielle” tässä yhteydessä ymmärretään, mutta kysymyksen ratkaisemisyritys herättäisi todennäköisesti loputtomasti uusia vastaavanlaisia kysymyksiä eikä johtaisi yksiselitteiseen lopputulokseen.

Tähän yhteyteen sopii hyvin *Selmerin* mielipide:

> ”Informasjon” kan ikke lagres eller overføres. Informasjon oppstår først i ett menneskes (eller et dyrs!) bevisshet når dette noe som er ”data” blir sett, hørt, ført eller på noen måte brakt innenfor rekkevidde av sanseapparatet. Data kan være bokstaver, streker og farger i et bilde, fakter, lyd, lys, elektromagnetiske impulser, spor i et elektronisk lagringsmedium. Data er alt som – dersom man bare har de riktige innretninger for å skape sanseinntrykk – kan føre til at et levende vesen får en bestemt, tilsiktet informasjon.[61]

Edellä lausuttua on mielenkiintoista verrata *Silvanderin* näkemykseen:

---

[59] Ks. kuitenkin SOU 1992:110, s. 82: ”I någon mån har vi använt begreppet *uppgift.* Detta ord brukar ofta användas synonymt med information men tilläggs inte sällan en föga urskiljbar begränsning till att avse information endast i något visst hänseende om något viss föremål eller förlopp. Av det anförda framgår emellertid att såväl information som uppgift är abstrakta begrepp.”

[60] HE 94/93, s. 132. Ks. myös Lahti, LM 91, s. 882 s.

[61] Selmer, s. 149 s.

> Även om data är en representation av uppgifter i maskinläsbar form är det fortfarande information som överförs.[62]

Toki *Silvanderkin* korostaa informaation subjektiivista luonnetta sanoessaan, että ”en fysisk persons subjektiva uppfattning av informationens innehåll kan omfattas av begreppet”.[63]

Informaatio tietona

Informaation käsitteen epistemologinen selvittely johtaa ainakin näennäisesti erilaisiin päätelmiin kuin yleiskielen pohjalta tapahtuva tutkiminen. Kun yleiskielessä voidaan puhua ”tiedosta informaationa”, näyttääkin siltä, että tietoteoreettisesti tämä ei ole mahdollista; sen sijaan voidaan kyllä puhua ”informaatiosta tietona”. Edellä on mainittu *Niiniluodon* käsitehierarkia, jossa informaatio on yläkäsite ja tieto sen suppeampi erikoistapaus.

Karvosen[64] mukaan arkipuheessa informaatio ja tieto suhtautuvat toisiinsa niin, että tieto on kuvausta maailman tiloista ja informaatio on tämän kuvauksen siirtämistä toisille viestimällä. Insinöörin kannalta viestien sisällön ja merkityksen kysymykset ovat yhdentekeviä, kun taas arkimerkityksessä juuri sisältö on olennaisinta.

Vaikka *Hintikkakin* edellä esitetyin tavoin näkee totuudellisuuden elementiksi, joka lopulta tekee tiedosta tietoa, käsittää hän informaation tiedon alalajiksi, ”suppeaksi” tiedoksi.[65] *Hintikka* toteaa informaatio-sanaan useimmiten törmättävän tilanteissa, joissa lähettäjä rajaa annettavan tiedon näkökulmaa, määrää ja laatua eri tarkoituksissa, ja tällöin informaation ja tiedon ero olisi se osuus, joka jää puuttumaan annetun ja todellisen tiedon välillä. Datan *Hintikka* puolestaan katsoo informaatiota vielä rajoitetummaksi tietoainekseksi; täysin käsitejärjestelmästään irrotetuksi raakatiedoksi tai tiedon osaksi.

Esitetyt näkemykset – jotka tosin perustunevat yleiskielen pohjalta tapahtuvaan tulkintaan – ovat mielestäni kritiikille alttiita. *Hintikankin* käsitys annetun ja todellisen tiedon erosta johtaa lopulta pitämään todellista tietoa annettua tietoa suppeampana käsitteenä – olkoonpa ensin mainitun totuudellisuus sitten relatiivista tai absoluuttista, subjektiivista tai objektiivista – koska periaatteessa väite voi olla tosi ainoastaan yhdenlaisena, epätosi taas äärettömän monessa muodossa. Jälkimmäisissäkin tilanteissa lause aina sisältää informaatiota, jonka olemassaoloa ei tarvitse altistaa totuudellisuuden kritiikille ja jonka tieto-ominaisuutta ei siten testata.

Datan näkeminen informaation alakäsitteeksi sen sijaan on mielestäni paremmin sopusoinnussa edellä datasta lausutun kanssa, joskin puhuminen *tiedon*

---

[62] Silvander, s. 120.
[63] Silvander, s. 92.
[64] Ks. Karvonen.
[65] Hintikka, s. 7 s.

osasta tai raaka*tiedosta* on jälleen harhaanjohtavaa, kun muistetaan tiedon olemukselta edellytettävä totuudellisuus. Informaation kantajana data voi olla myös tiedon kantaja, mutta se ei ole sitä välttämättömästi.

Näen datan olemukseen kuuluvan tietynlaisen oikeellisuuden: vaikka sen edustama informaatio ei täyttäisikään totuudellisuuden kriteeriä, voi data edustaa tuota informaatiota vain ollessaan oikeaa suhteessa esimerkiksi informaation sisältävän väitelauseen sisältöön.

Datan oikeellisuudella on rikosoikeudellista merkitystä; väärennysrikoksen kohteeksi joutunut data antaa kantamastaan (lähettäjän) informaatiosta väärän kuvan vastaanottajalle, vaikka informaation absoluuttinen totuusarvo ei rikoksen johdosta muuttuisikaan.[66]

Informaation lajeista

Niiniluoto erottaa toisistaan (1) ei-kielellisen eli fysikaalisen informaation, (2) datan sekä (3) kielellisen informaation. *Fysikaalisesta informaatiosta* on kysymys, kun informaation käsitettä käytetään ilmaisemaan aineellisten systeemien järjestyneisyyttä, organisaatiotasoa tai monimutkaisuutta, jolloin systeemit voivat kuulua joko elottomaan tai elolliseen luontoon. Käsitettä voidaan käyttää myös ilmaisemaan ihmisen suunnittelemien ja rakentamien artefaktien kompleksisuutta.[67]

Kielellinen informaatio -käsite lähtee *Niiniluodon* mukaan oletuksesta, että informaatiolla täytyy olla kantaja eli aineellinen olio, tapahtuma tai prosessi, joka kykenee tietyissä olosuhteissa välittämään tai tallentamaan viestejä. Laajassa mielessä informaation kantajia voidaan kutsua merkeiksi[68] ja merkkijärjestelmiä kieliksi.[69] Edellä kuvatuin tavoin *datalla* ymmärretään juuri informaatiota kantavia merkkejä tai merkkijonoja (tai yleiskielisesti: tietoa esittäviä merkkejä).

Niiniluoto erottaa kielellisen informaation osalta kolme tasoa: syntaktisen, semanttisen ja pragmaattisen.

Syntaktista[70] *informaatiota* kuvatessaan[71] *Niiniluoto* viittaa *Shannonin* tilastolliseen kommunikaatioteoriaan, jossa perusongelmana on ”jossakin pisteessä

---

[66] Jos esimerkiksi lauseen ”Suomen vankiloissa on enemmän lapsivankeja kuin naisvankeja” sisältämä informaatio datan manipuloinnin seurauksena muuttuu muotoon ”Suomen vankiloissa on enemmän lapsivankeja kuin miesvankeja”, pysyy väitteen sisältämän informaation suhde (lähes absoluuttiseksi katsottavaan) totuuteen ennallaan, mutta datan muuttaminen (merkkien n, a ja i muuttaminen merkeiksi m, i ja e) saa aikaan sen, että lähetetty informaatio ei välity vastaanottajalle lähettäjän tarkoittamassa muodossa. Itse informaatioon ei ole kajottu. Kummankaan väitelauseen sisältämä informaatio ei ole tietoa.

[67] Niiniluoto, s. 18 ss.

[68] Atk-sanakirjan (s. 110) mukaan merkki on pienin tiedon esityksen alkio, jolla yksinään voi olla merkitystä.

[69] Niiniluoto, s. 23 ss.

[70] Sanan *syntaktinen* kantasanana on kreikan kielen sana *syntaksis,* joka tarkoittaa yhteenliittämistä, järjestystä ja rakennetta.

[71] Niiniluoto, s. 30 ss.

valitun viestin reprodusointi eksaktisti tai approksimatiivisesti jossain toisessa pisteessä".

Shannon erottaa selvästi toisistaan kanavassa kulkevan merkeistä muodostuvan viestin ja kanavan välittämän informaation. Tilastollisen kommunikaatioteorian lähtökohtana olevan syntaktisen informaatiokäsitteen mukaan viestin informaatiomäärä riippuu ainoastaan siitä, kuinka usein ko. viestien muodostamaa merkkijonoa tilastollisesti katsoen syötetään kanavaan.[72] *Niiniluoto* korostaa, että syntaktisina olioina merkeillä ei ole informaatioarvoa ennen kuin ne esiintyvät säännönmukaisilla frekvensseillä jossakin kommunikaatiosysteemissä, ja tässä mielessä syntaktinen informaatio on tietyntyyppisten merkkien relationaalinen ominaisuus.

Semanttisen[73] *informaation"*käsitettä selvitellessään[74] *Niiniluoto* lainaa *Bar-Hilleliä,* joka valittaa tilastollisen informaatioteorian johtaneen kestämättömiin spekulaatioihin, koska aina ei ole osattu erottaa toisistaan kahta asiaa: termillä "informaatio" voidaan tarkoittaa joko merkkijonoa tai merkkijonon ilmaisemaa viestiä; vastaavasti "informaation määrällä" voidaan tarkoittaa itse merkkijonon esiintymisen harvinaisuutta tai merkkijonon ilmaisemien asioiden esiintymisen harvinaisuutta. Näistä vaihtoehdoista edellinen liittyy *Shannonin* syntaktiseen, jälkimmäinen semanttiseen informaation käsitteeseen.

Esimerkkinä käsitteiden erosta *Bar-Hillel* mainitsee lauseet

1) vihollinen hyökkäsi aamulla
   ja
2) vihollinen hyökkäsi pataljoonan voimalla klo 5.30.

Jos p_1 ja p_2 tarkoittavat lauseiden (1) ja (2) esiintymistiheyttä jossain sotilaallisessa viestintäkanavassa ja jos p_1 on suurempi kuin p_2, niin tilastollisen kommunikaatioteorian mielessä (1) on informatiivisempi viesti kuin (2). Sen sijaan semanttisen informaation teorian kannalta (2) on informatiivisempi kuin (1), koska se sanoo sisällöllisesti enemmän.

---

[72] Ks. Karvonen, jonka mielestä Shannon on ensisijaisesti syypää teknisen puheen kummalliseen tapaan käyttää sanaa "informaatio"; puhelininsinööri Shannonille viestinnän keskeinen ongelma oli se, miten saada yhdessä paikassa tuotettu bittien joukko toistetuksi mahdollisimman virheettömästi toisessa pisteessä. Karvosen mukaan tällä tasolla tarkasteltuna on aivan sama, ovatko nuo toistettavat bitit merkityksetöntä siansaksaa, pornokuvia, musiikkiesitys, ohjelmanpätkä vaiko maailman mullistavin tieteellinen artikkeli. Karvosen mielestä ei ole järkevää kutsua "tiedoksi" kaikkea tuota bittimuodossa siirrettyä ja toistettua materiaalia. – Olen tässä lopputuloksessa Karvosen kanssa samaa mieltä mutta eri perustein: merkityksetön siansaksa ei ole tietoa missään olosuhteissa kun taas tieteellinen artikkeli sitä (yleensä) on. Tiedon kriteeri on kuitenkin sen totuudellisuus, kysymys tiedosta ei ratkea järkevyyden (tarkoituksenmukaisuuden) perusteella.

[73] Sanan *semanttinen* kantasanana on kreikan *sema,* merkki, josta johtuu sana *semainein,* merkitä.

[74] Niiniluoto, s. 36 ss.

Niiniluoto korostaa muun muassa, että semanttisen informaation käsite on erotettava klassisesta tiedon käsitteestä (tieto on hyvin perusteltu tosi uskomus), koska lauseen informatiivisuus on täysin neutraali suhteessa lauseen totuusarvoon. Syntaktisessa informaation käsitteessä ei kiinnitetä huomiota sellaisiin semanttisiin käsitteisiin kuin totuus ja epätotuus, mutta myös semanttisessa informaation teoriassa väitelauseen informaatiosisältö ja lauseen sisältämän informaation määrä ovat riippumattomia lauseen totuudesta ja epätotuudesta.

Niiniluoto viittaa *Popperin* tieteenfilosofian perusoivallukseen, jonka mukaan totuus ja informaatiosisältö ovat vastakkaisiin suuntiin vetäviä tieteen tavoitteita: totuuden vaatimus olisi helppo toteuttaa triviaalisti ehdottamalla loogisesti heikkoja, epäinformatiivisia ja todennäköisiä teorioita, kun taas rohkeus informatiivisten hypoteesien esittämisessä merkitsee epätodennäköisyyttä, riskiä totuuden suhteen.

Semanttinen informaatio eroaa *Niiniluodon* mukaan[75] *pragmaattisesta*[76] *informaatiosta* siinä, että se ei sellaisenaan välttämättä liity kommunikaatioon, kun taas viimeksi mainitun osalta on kysymys nimenomaan henkilöihin relativisoidusta informaation käsitteestä.

Niiniluoto kirjoittaa, että hyvin yleisessä mielessä pragmaattisella informaatiolla tarkoitetaan henkilö- ja kulttuurisidonnaista merkityksellisyyttä tai merkittävyyttä. Jos ajatellaan nimenomaan informaation yksilöllistä merkitystä, päädytäänkin jo lähelle Atk-sanakirjan edellä esitettyä informaation määritelmää: informaatio on datan ihmiselle tuottama mielle tai merkitys.

Edellä informaatiosta ja sen lajeista sanottu kuitenkin osoittaa, että Atk-sanakirjan määritelmä on paitsi epämääräinen myös kovin yksipuolinen: tietotekniikkarikosten kannalta ajatellen informaatiota ei voida rajoittaa tarkoittamaan ainoastaan vastaanottajan mielteitä, vaan merkityksellistä on myös lähettäjän informaatio.

Tämä oikeuttaisi vielä näkemään tutkimuksen kannalta keskeisenä informaation lajina pragmaattisen informaation, mutta ajateltaessa esimerkiksi vahingontekorikoksen objektina kysymykseen tulevaa ”datan” käsitteen ulkopuolelle jäävää ”tallennettua tietoa”, ollaan jo tekemisissä paitsi pragmaattisen myös semanttisen informaation kanssa – ja ehkä ennen muuta viimeksi mainitun, sillä tallennettu informaatio ei välttämättä ainakaan välittömästi relativisoidu henkilöihin eikä välttämättä sellaisenaan liity kommunikointiin.

Niiniluoto toteaa semanttisen ja pragmaattisen informaation erottamisen toisistaan olevan varsin ongelmallista ja väittää ainakin semanttisen informaation määrän tutkimisen kuuluvan loogisen pragmatiikan alaan.

---

[75] Niiniluoto, s. 40 s.

[76] Kreikan sanasta *pragma,* teko, johtuu sana *pragmatiko, pragmaattinen*, jolla ymmärretään asioihin perehtynyttä, viisasta, kokenutta. Filosofisessa mielessä *pragmatismilla* tarkoitetaan suuntausta, joka pitää toimintaa tiedon edellytyksenä ja päämääränä.

Immateriaalinen informaatio

Ennen kuin lopullinen tämän tutkimuksen tarpeita palveleva informaation käsitteen määritteleminen on mahdollista, on vielä tutkittava informaation luonnetta, sitä, mitä informaatio on.[77]

Ruotsalaisessa lainvalmistelussa on pohdittu informaation olemusta seuraavasti:

> Viktigt är att hålla isär information och informationsbärare. Information är något immateriellt medan informationsbärare är fysiska föremål. Data är något däremellan. De ger en fysisk representation av information men de är inte påtagliga; de har som vi ofta återkommer till en kvasimateriell karaktär.[78]

Ja edelleen, väärennysrikoksia käsiteltäessä:

> Pappersurkunderna är materiella objekt, saker, medan digitalt representerade uppgifter inte med vanligt språkbruk kan beskrivas som materiella objekt.[79]

Datastraffrättsutredningen on siis ottanut lähtökohdakseen ajatuksen, että informaatio on luonteeltaan immateriaalista, data kvasimateriaalista, siis jotakin aineellisen ja aineettoman väliin jäävää – aiemmin esitetyn määritelmän mukaan ”representationen av information”, mikä ei tarkoittaisi samaa kuin ”informationsbärare”.[80] Näiden ilmaisujen merkityssisältöä enemmälti pohtimatta totean, että datan luonnehtiminen joksikin kvasimateriaaliseksi ei tunnu ensinnäkään tarpeelliselta eikä toiseksi myöskään perustellulta. Jako aineelliseen ja aineettomaan on riittävä eikä kolmannen kategorian luomisella saavuteta mitään; päinvastoin sillä aiheutetaan sekaannusta.

Olkoonpa data tietokoneella käsiteltävissä olevaa tai ilmetköön se asiakirjalle kirjoitettuina, sellaisinaan luettavissa olevina merkkeinä, on se luonteeltaan materiaalista. Esimerkiksi tietokonelevykkeellä tai koneen kiintolevyllä dataa ovat tietyssä järjestyksessä olevat rautahiukkaset, paperiasiakirjalla sille käsin tai koneellisesti kirjoitetut tai painetut kirjainmerkit.

Informaationkaan immateriaalista luonnetta ei voida pitää itsestäänselvyytenä. *Niiniluoto* esittelee erilaisia näkemyksiä, esimerkiksi *Brillouinin* fysikaali-

---

77 Tästä Niiniluoto, s. 43 ss.

78 SOU 1992:110, s. 156.

79 SOU 1992:110, s. 261.

80 Ajattelutapa tuntuu edelleen olevan Ruotsissa vallalla, sillä esimerkiksi Silvander, s. 169, nimenomaan toteaa, että ”de digitala tecken som representerar lagrade data inte har fysisk substans”. Tämä on tosin mielestäni ristiriidassa sen Silvanderin (s. 120) lausuman kanssa, että data on ”representationen av fakta, begrepp eller instruktioner”; mielestäni tämä tarkoittaa sitä, että juuri digitaaliset merkit ovat dataa, eivät sen edustajia. Joka tapauksessa tuntuu vaikealta kuvitella, ettei *merkillä* – oli se sitten digitaalinen tai muun tyyppinen – olisi fyysistä substanssia.

nen informaatiokäsite termodynamiikan negentropiana tekee informaatiosta fysikaalisen suureen, joka liittyy materiaalisten järjestelmien makrotilojen muutokseen. Vastakkaista ajattelutapaa edustaa muiden ohessa Atk-sanakirjan määritelmä, jonka mukaan informaatio on datan ihmiselle tuottama mielle tai merkitys. *Klausin* ja *Buhrin* mukaan informaatio ei ole ainetta eikä aineellisten kappaleiden ominaisuus, vaan aineellisten kappaleiden ominaisuuksien ominaisuus.[81]

Popper erottaa tietoa (knowledge) objektiivisessa mielessä tutkiessaan kolme eri maailmaa: fysikaalisen maailman (maailma 1), tietoisten kokemustemme maailman (maailma 2) sekä kirjojen, kirjastojen, tietokonemuistien ja vastaavien loogisten sisältöjen maailman (maailma 3).[82] *Popperin* jaottelua seuraten *Niiniluoto* erottaa ontologiassa kolme todellisuuden piiriä: maailman 1, johon kuuluvat ajassa ja avaruudessa esiintyvät fysikaaliset objektit, tapahtumat ja prosessit, aine ja energia, epäorgaaninen ja orgaaninen luonto; maailman 2 eli yksilöllisen tajunnan tilat, mentaaliset tapahtumat, psyyke; ja maailman 3, joka muodostuu ihmisen sosiaalisen toiminnan kautta syntyneistä kulttuuriesineistä, artefakteista ja abstraktioista, kulttuurista ja yhteiskunnasta. Tämän jälkeen *Niiniluoto* paikallistaa eri informaation lajit seuraavasti:[83]

> Fysikaalinen informaatio, materian järjestys eli negentropia, kuuluu maailmaan 1. Myös kielellisten merkkien, merkkijonojen tai datan esiintymät fysikaalisina objekteina – aikaan ja paikkaan sidottuina, puhuttuina, kirjoitettuina tai muulla tavoin tuotettuina – kuuluvat maailmaan 1.
>
> Esimerkiksi tälle sivulle painetut kirjainmerkit ovat maailman 1 olioita. Sen sijaan mielessäni ollut ajatus, jota kirjoittamani lauseet yrittävät ilmaista, samoin kuin lukijan mielessä syntyvät ajatukset, ovat maailman 2 tapahtumia. Pragmaattinen informaatio subjektiivisessa mielessä kuuluu siten maailmaan 2.
>
> Semanttinen informaatio – sanojen ilmaisemat käsitteet, väitelauseiden ilmaisemat propositiot, lauseiden pois sulkemien mahdollisten asiantilojen joukot – on parhaiten ymmärrettävissä abstraktiseksi maailma 3:n osaksi. Semanttinen informaatio edellyttää symbolifunktiota, ihmisen luomaa merkityksellistä kieltä, mutta muutoin se on objektiivis-

---

[81] Tätä puhetapaa Niiniluoto ei pidä kaikissa suhteissa täysin luontevana. Ks. s. 47: ”Esimerkiksi paloautot ovat punaisia, ja punainen on väri; siis ’on väri’ on fysikaalisten objektien ominaisuuksien ominaisuus. Toisaalta ’olla värillinen’ on fysikaalisten objektien ominaisuus, joka niillä on sen kautta, että niillä on eräs toinen ominaisuus, kuten punaisuus. Koska yksityiset merkit ovat tietyssä tilanteessa informaation kantajia sen kautta, että ne ovat tiettyä tyyppiä, ominaisuus ’olla informatiivinen’ on analoginen pikemminkin ominaisuuden ’olla värillinen’ kuin ’olla väri’ kanssa.”

[82] Popper, s. 74: ”We can call the physical world ’world 1’, the world of our conscious experiences ’world 2’, and the world of the logical *contents* of books, libraries, computer memories, and suchlike ’world 3’.”

[83] Niiniluoto, s. 45 ss.

ta, yksilöllisestä ihmismielestä riippumatonta. Samaan tapaan pragmaattinen informaatio, kun se perustuu jonkin kulttuurin piirissä vallitseviin intersubjektiivisiin merkityksiin ja merkittävyyden arvioihin, on osa ihmisen luomasta todellisuudesta, maailma 3:sta.

Lopputulos

Edellä lainattua soveltaen voidaan väittää, että data on materiaalista, kun taas kielellinen informaatio tämän tutkimuksen kannalta – eli siis semanttinen ja pragmaattinen informaatio – on immateriaalista. Fysikaalisella informaatiolla sen paremmin kuin kielellisen informaation lajeista syntaktisella informaatiolla ei ole nähtävissä olennaista merkitystä tietotekniikkarikoksista puhuttaessa.

On tietysti mahdollista katsoa myös maailma 3 ihmisen luomana materiaaliseksi,[84] mutta tällä ei nähdäkseni saavuteta mitään oleellista: vaikka maailmassa 3 oleva ihmisen aiheuttama materian järjestys[85] olisikin informaationa fysikaalista, on se informaatio, jota tässä tutkimuksessa käsitellään, kielellistä informaatiota, jota ei ole pidettävä sen paremmin materiaalisena kuin kvasimateriaalisenakaan.

Kaiken edellä kirjoitetun perusteella voitaisiin jo pyrkiä täsmentämään yhdyssanojen tieto-, informaatio- ja datatekniikka samoin kuin sanojen tieto-, informaatio- ja datateknologia alkuosien sisältöjä. Ennen siihen ryhtymistä on kuitenkin syytä tarkastella mainittujen sanojen loppuosien merkityksiä.

1.2.2.4 Tekniikka ja teknologia

Niin tekniikan kuin teknologiankin kantasanana on kreikan kielen sana *tekhne,*[86] taito; teknologian kantasanana on lisäksi kreikan *logos,*[87] tieto. Uudesta sivistyssanakirjasta voidaan lukea seuraavanlaiset määritelmät:

---

[84] Ks. Angeles, s. 83 hakusanan *emergent* kohdalla: ”– – The mind (consciousness, awareness) is regarded as a new quality that emerges when certain neural processes become organized in a specific way; change the organization of these physical structures, and another quality (mind) will emerge.”

[85] Ks. Niiniluoto, s. 48.

[86] Ks. Angeles, s. 308: ”techne (Greek, art, skill, craft, cunning of hand, technique, a trade, handiwork, a system or method of making or doing something) – – 1. the very general meaning of *techne,* especially as found in Aristotle, refers to anything deliberately created by humans in contrast to anything not humanly created. – – 2. a less general meaning of *techne* refers to handiwork, a craft, a technique, or a skill. – – 3. specifically, *techne* refers to the knowledge of *how* to do or make things (as opposed to *why* things are the way they are); *how* to achieve a desired end or *how* to produce something. – – 4. *techne* also refers to the rational, professional knowledge of the *rules of procedure* involved in making or doing things. – –”

[87] Ks. Angeles, s. 172: ”logos (Greek, speech, discourse, thought, reason, word, meaning, study of, the account of, the science of, the underlying reasons for why a thing is what it is, the principles and methods used to explain phenomena in a particular discipline, those features in a thing that make it intelligible to us, the rationale of a thing). – –”

> *tekniikka,* teoreettisten tietojen käytännöllinen hyväksikäyttö aineellisen tuotantoelämän piirissä, teoreettisvoittoisena sama kuin teknologia, insinööritieteet; laajemmassa merkityksessä yl. tarkoituksenmukaisten ja (työtä) säästävien menetelmien tuntemus ja käyttö tai käyttötaito.
>
> *teknologia,* niiden tieteiden yhteisnimitys, jotka käsittelevät teknisiä järjestelmiä ja menetelmiä; oppi työmenetelmistä, joita käyttäen raaka-aineita muokataan jalostustuotteiksi.[88]

Ruotsin *Datastraffrättsutredningen* on selvittelytyössään päätynyt käyttämään käsitettä *informaatioteknologia* (informationsteknologin), johon se lukee sekä automaattisen tietojenkäsittelyn (ADB, automatisk databehandling) että televiestinnän; enää ei ole mahdollista kohdistaa päähuomiota yksin automaattiseen tietojenkäsittelyyn, koska myös dataviestintä on tullut yhtä tärkeäksi. *Datastraffrättsutredningen* tosin toteaa kattavan termin keksimisen olevan vaikeaa.[89]

Sana teknologia olisi suomennettavissa sananmukaisesti *taitotiedoksi,* taitoon kohdistuvaksi tiedoksi, jolloin ollaan lähellä englannin *know how'n* epäonnistuneelta kuulostavaa mutta valitettavan vakiintunutta käännöstä *tietotaito*[90] (joka sananmukaisesti tarkoittaa tietoon kohdistuvaa taitoa; tällainen käsite tuntuu mahdottomalta). Hyvin lähellä äsken mainittuja on vielä *osaamisen* käsite.

Niiniluoto pitää tärkeänä pelkän osaamisen ja *know how'n* – taitoa koskevan tiedon – erottamista toisistaan. Taitotieto poikkeaa hänen mukaansa pelkästä osaamisesta tai taidosta siinä, että se on kielellisesti ilmaistavissa lauseina, jotka koskevat jonkin taidon harjoituksen tehokkainta tapaa; siten taitotieto on propositionaalisen tiedon erikoinen laji, joka ilmaisee keinojen ja tavoitteiden suhteita koskevaa välineellistä tietoa. Tällaisten lauseiden yleinen muoto on

> Jos haluat A:ta ja uskot olevasi tilanteessa B, sinun pitää (kannattaa) tehdä X!

Niiniluoto näkee tällaisen *teknisen normin* taitotiedon perusmuodoksi.[91]

Atk-sanakirjan määritelmistä ei ole oleellista apua nyt puheena olevaa käsitteistöä täsmennettäessä. Sanakirjan määritelmä sanalle "teknologia" on seuraava: "Tekniikan tutkiminen tai opettaminen. Merkitystä 'tekninen välineistö ja osaaminen' vastaa suomen sana *tekniikka."* Informaatioteknologian kohdalla viitataan tietotekniikkaan. Ja lopuksi tietotekniikan määritelmä: "Tiedon automaattisen käsittelyn ja siirron välineet ja menetelmät sekä niiden käytön osaaminen."[92]

---

[88] Aikio, s. 595.
[89] SOU 1992:110 s. 75.
[90] Atk-sanakirjassa, s. 210, tosin on hakusana "tietotaito", mutta sen kohdalla todetaan: "Ei suositella. Suomen sanoja ovat taito, osaaminen."
[91] Niiniluoto, s. 54 s.
[92] Atk-sanakirjan (s. 210) mukaan *tietotekniikka* on englanniksi *information technology,* ranskaksi *informatique* tai *telematique* ja ruotsiksi *datateknik* tai *informationsteknik.*

Tässä yhteydessä on mielenkiintoista todeta, mitä viestinnän emeritusprofessori *Osmo A. Wiio* ymmärtää tietotekniikalla:[93]

> Tietokoneeni esimuoto (mikrotietokone) syntyi 1970-luvun puolivälissä, itse tietokoneen keksimisen ajankohdasta kuitenkin riidellään. Tässä joukko ensimmäisiä tietokoneita: ENIAC (1946), Harvard Mark 1 (1944), Colossus-kone ja Alan Turing (1943), Konrad Zuse (1931) ja Charles Babbage (1835).
>
> Oikeastaan tietokone ei ole mikään ”tietotekniikan” mittari! Tietotekniikkaa on mikä tahansa tekniikka, jolla tietoa tuotetaan, tallennetaan ja/tai siirretään. Siten mukaan on otettava esimerkiksi lennätin (Chappe 1793, Morse 1837), puhelin (Bell 1876), kirjoituskone (Mill 1714), laskukone (Pascal 1642) ja helmitaulu (noin 3000 eKr.).

Ehkäpä tämä hieman helpottaa suhtautumista koko tietotekniikkarikosongelmaan, edesauttaa sen sijoittamista historiallisiin puitteisiin ja vähentää tarvetta turhaan mystifiointiin.

1.2.2.5 Tallenne

Jotta data ja erityisesti immateriaalinen informaatio voisivat tulla kysymykseen esimerkiksi rikoksen kohteena tai elektronisena todistusaineistona, on niiden oltava kiinnitettynä johonkin. Tämän selventämiseksi on tarkasteltava tallenteen käsitettä.

Atk-sanakirjan mukaan[94] tallenne on ”tieto tai joukko tietoja tallennettuna, esimerkiksi paperille, magneettinauhalle tai tietokoneen muistiin”. Tämä määritelmä on jo huomattavasti täsmällisempi kuin esimerkiksi vuoden 1991 painoksen määritelmä, jonka mukaan tallenne oli ”taltio ja siihen tallennettu tieto”, *taltio* puolestaan ”rajallinen määrä tietovälineitä, joita käsitellään yhtenä kokonaisuutena. Esimerkiksi asiakirjamappi, levyke, levykkö, magneettinauha”.

Nykyinenkään määritelmä parantuneesta täsmällisyydestään huolimatta ei sellaisenaan sovellu juridiseen kielenkäyttöön (johon sitä ei ole ensisijaisesti tarkoitettukaan). Tallenne määriteltynä ”tiedoksi tallennettuna” on liian epämääräinen käsite.

Ruotsissa on *Küchler* käsitellyt tallenne-käsitettä tietomurron kriminalisoivan Brottsbalkenin 4 luvun 9 c §:n kannalta. Hän toteaa – viitaten vuodelta 1973 olevaan ehdotukseen ”Förslag till ändringar i tryckfrihetsförordningen mm” (1973:33) – mm. seuraavaa:[95]

---

93 Wiio, TM 5/2001.
94 Atk-sanakirja, s. 191.
95 Küchler, s. 20 s.

> Med upptagning avses själva informationsinnehållet, dvs. de uppgifter som fixerats på någon form av datamedium och som antingen finns eller kan matas in i en datamaskin och som är läsbara endast med ADB-teknik. Vidare bör varje uppgift som hämtas från ett och samma datamedium ses som en särskild upptagning. En uppgift som matas in i en datamaskin och som i samma stund blir visuellt läsbar, bör inte falla under begreppet upptagning för ADB.

Küchlerin esittämässä määritelmässä on käsitykseni mukaan oikein kiinnitetty huomiota tietojen (uppgifter) kiinnittämiseen tietovälineelle. Täytyy muistaa, että kysymyksessä on nimenomaan ”upptagning för ADB”, jolle käsitteelle voidaan hyvin asettaa lisäkvalifikaatioita (läsbar endast med ADB-teknik).[96] Yleisempänä oikeudellisena terminä näkisin tallenteen voivan lähinnä merkitä *tietovälineelle kiinnitetyn datan ja datan edustaman informaation* muodostamaa kokonaisuutta.[97] Tallenteen käsitteessä *täytyy* näkyä sekä datan että informaation osuus: informaatio ei konkretisoidu teknisin keinoin tapahtuvaa käsittelemistä varten ilman dataa ja toisaalta sellaisella datalla, joka ei edusta jotain (järjellistä) informaatiota, vain harvoin voi olla itsenäistä merkitystä.

Tietovälineellä[98] (data carrier, datamedium, Datenträger) ymmärrän tässä yhteydessä mitä tahansa esinettä, jolle data voidaan kiinnittää; näitä ovat tietokoneiden kiintolevyt, tietokonelevykkeet ja -nauhat sekä CD-levyt aivan samoin kuin paperiarkitkin. Toisinaan on käytetty poronkorvaa havainnollistamaan dokumentin ja tallenteen käsitettä, mihin tarkoitukseen poronkorva epäilemättä hyvin sopiikin, sillä sitä on varmasti pidettävä yhtenä vanhimmista suomalaisista tallenteista: poronkorva itsessään on tietoväline, jolle määrätynlainen kuvio leikkaamalla ”kiinnitetään” dataa, joka puolestaan edustaa informaatiota siitä, kenelle poro kuuluu.[99]

Mikäli datan kiinnittäminen ja datan edustaman informaation selvittäminen edellyttää tietoteknisiä toimenpiteitä, kysymyksessä on tietotekninen tai automaattiseen tietojenkäsittelyyn soveltuva rikoslain 33 luvun 6 §:ssäkin tarkoitettu tallenne.

---

[96] Silvanderkin tutkii tallenteen käsitettä (s. 114 ss.) mutta tyytyy lähinnä viittaamaan lainvalmisteluasiakirjoissa esitettyihin näkemyksiin. Silvanderin mielestä myös tietokoneohjelmaa on pidettävä tallenteena.

[97] Ks. Pihlajamäki, Tutkinta, s. 31, jossa jo vuonna 1994 olen esittänyt vastaavanlaisen tallenteen määritelmän. Katso myös HE 38/97, s. 4, jossa tallenteen käsitteelle annetaan sama sisältö. Yhtäläisyys johtuu osaksi siitä, että olen kirjoittanut myös HE:n tekstin.

[98] Atk-sanakirjan (s. 211) mukaan tietoväline on ”aines tai fysikaalinen ilmiö, jota voidaan käyttää tiedon esittämiseen”. Tämäkin määritelmä on liian epämääräinen juridisiin tarkoituksiin.

[99] Tallenneproblematiikkaa ja erityisesti tallenteen kestävyyttä sivuaa Wiio (TM 5/2001): ”Tutkijat voivat tänään lukea alkuperäisiä saveen piirrettyjä sumerien asiakirjoja. Mahdollinen tulipalo on vain tehnyt savitauluista entistä kestävämpiä. Miten säilyvät meidän filmimme, nauhamme, magneettilevykkeemme tai CD-romppumme? Huonosti! – Paperi on oikeastaan säilyvin tallenne. Tosin paperia on paremmin tai huonommin säilyvää laatua, paperi palaa helposti ja kosteus vaurioittaa sitä. Magneettilevykkeet saattavat mennä pilalle muutamassa vuodessa, filmit muutamassa vuosikymmenessä. CD-levyihin saattaa ilmestyä virheitä muutamassa vuodessa. Savikirjoitukset kestävät siis 8000–5000 vuotta!”

1.2.2.6 Yhteenveto

Yleis- ja juridiseen kielenkäyttöön ovat vakiintumassa sanat *tietotekniikka* ja *tietotekniikkarikos.* Niin kuin edellä jo useaan kertaan on havaittu, on tietosanan yleiskielinen merkityssisältö tavattoman laaja, ja tässä mielessä tietotekniikka-sana voisi samoin saada hyvin erilaisia merkityksiä, joista useimmat eivät olisi millään tavoin relevantteja tämän tutkimuksen kannalta.

Käytän kuitenkin jäljempänä juuri näitä termejä nimenomaan niiden vakiintuneisuuden vuoksi; kuitenkin niin, että *tietotekniikalla* asiallisesti tarkoitetaan joko *datatekniikkaa* tai *informaatiotekniikkaa,* jolloin jälkimmäinen ymmärretään yläkäsitteeksi.

Tältä pohjalta voidaan tehdä jako toisaalta *datarikoksiin* ja toisaalta *informaatiorikoksiin.* Mahdollisia olisivat myös termit datatekniikkarikos ja informaatiotekniikkarikos, mutta niiden ero ei nähdäkseni ole yhtä selkeä, mikäli informaatiotekniikka hyväksytään yläkäsitteeksi datatekniikkaan nähden; datan ja informaation erottaminen toisistaan on helpommin tehtävissä.

Informaatiolla tarkoitan tässä yhteydessä kielellistä informaatiota ja sen lajeista ennen muuta semanttista ja pragmaattista informaatiota; lauseen sisältöä sellaisena, miksi laatija on sen tarkoittanut, tai sellaisena, minä vastaanottaja sen ymmärtää. Dataa puolestaan ovat ne merkit, jotka kantavat sanotunlaista informaatiota.

Määritelmät ovat lähellä rikoslain kokonaisuudistuksen toista vaihetta tarkoittavassa hallituksen esityksessä olevia; kuitenkin niin, että kun esityksessä puhutaan informaatiosta ”tiedon sisältönä”, ei tätä käsitystä voida hyväksyä. Informaatio käyttämässäni merkityksessä on lauseen (viestin, sanoman tms.) immateriaalinen sisältö ja *se* saattaa joissakin tilanteissa olla tietoakin.

Koska tietotekniikkaan liittyvä suomenkielinen termistö on täysin vakiintuneesti johdettu tieto-sanasta, ei tässäkään yhteydessä ole aiheellista ryhtyä esimerkiksi tietojenkäsittelyn asemesta puhumaan datankäsittelystä, josta itse asiassa on kysymys; *Kuopus* on nähdäkseni osunut lähes asian ytimeen, kun hän katsoo automaattisessa tietojenkäsittelyssä käsiteltävän tietoa eli *informaatiota datana* (kursivointi tässä).[100]

Kuopuksen näkemys on täysin hyväksyttävissä silloin, kun ajatellaan pelkästään datan muokkaamista; toisaalta voidaan kuitenkin ajatella datalla olevan vain välinearvoa käsittelyn tosiasiallisesti kuitenkin kohdistuessa informaatioon. Joka tapauksessa tämän tutkimuksen kohteena olevia rikoksia ovat *tietotekniikkarikokset,* jotka voidaan jakaa toisaalta *data-* ja toisaalta *informaatiorikoksiin.*

---

[100] Kuopus, s. 13.

1.2.3 Tietotekniikkarikos

1.2.3.1 Käsitteen muotoutumisesta

Rikos-käsitettä voitaneen pitää siinä määrin notorisena, että sen määritteleminen on tässä yhteydessä sivuutettavissa toteamalla rikoksen olevan laissa rangaistavaksi määrätty teko tai tunnusmerkistönmukaisesti oikeudenvastainen teko, joka osoittaa tekijässään syyllisyyttä.[101] Tietotekniikkarikos sen sijaan ei käsitteenä ole lainkaan yhtä selkeä.

Suomen kielessä on aiemmin käytetty tietotekniikkarikos-sanan asemesta sanoja atk-rikos, tietokonerikos ja tietokoneavusteinen rikos. Esimerkiksi englanninkielisiä termejä ovat *computer crime, computer-related crime* sekä *information tecnology crime* ja ruotsinkielisiä *datorbrott, datorrelaterade brott, adb-brott* sekä *informationsteknologibrott.* Ranskassa samaa tarkoittaa *crime t. délit informatique* ja saksalaiset käyttävät sanaa *Computerstraftat.*

Termit ovat siis osaksi erilaisia: toisaalta ne viittaavat tietokoneeseen, toisaalta joko dataan tai informaatioon.[102] Aivan uudet ulottuvuudet myös rikosnimitykselle on kuitenkin tuonut Internetin käytön räjähdyksenomainen laajeneminen: *crimes in cyberspace* tai *cyber-crimes* olivat esimerkiksi vuonna 1997 työskentelynsä aloittaneen Euroopan neuvoston työryhmän pohdinnan kohteena ja cyber-crimea koskee myös Euroopan komission huhtikuussa 2002 julkaisema puitepäätösehdotus.[103]

Paitsi tietotekniikkarikosten alueella yleensä on myös itse käsitteen määrittelemiseksi tehty aktiivista kansainvälistä yhteistyötä. Yleisesti hyväksyttyä määritelmää ei kuitenkaan ole onnistuttu kehittämään, vaikkakin useita samansuuntaisia luonnehdintoja on esitetty.

Euroopan neuvosto ja OECD

Euroopan neuvoston vuoden 1989 tietotekniikkarikosraportissa on siinäkin todettu, ettei edellä tarkoitettua määritelmää käsitteille *computer crime* ja *computer-related crime* ole olemassa, mutta esimerkinomaisesti raportissa on luonnehdittu tietotekniikkarikoksen olevan

> ”any illegal action in which a computer is a tool or object of the crime; in other words, any crime, the means or purpose of which is to influence the function of a computer” tai ”any incident associated with computer

---

[101] Rikoksen käsitteestä ks. esim. Nuutila, Rikoslaki, s. 1. Ks. myös HE 44/2002, s. 9 s., jossa esitetään mm. molemmat tekstissä mainitut rikoksen käsitteet.

[102] AIDP:n vuoden 1994 kongressin yhtenä teemana oli englanniksi *Computer Crimes and Other Crimes related to Information Technology,* ranskaksi *Les crimes informatiques et d’autres crimes dans le domaine de la technologie informatique* sekä saksaksi *Computerkriminalität und andere Delikte im Bereich der Informationstechnik.*

[103] Atk-sanakirjan englanti–suomi-hakemistossa (s. 267) tarjotaan ”cybercrimen” suomenkieliseksi vastineeksi sanaa ”verkkorikos”. Tätä ei ole pidettävä ollenkaan huonona vaihtoehtona.

> technology in which a victim suffered or could have suffered loss and a perpetrator by intention made or could have made gain".[104]

Taloudellisen yhteistyön ja kehityksen järjestön OECD:n vuoden 1986 raportissa käytetyn työmääritelmän mukaan *computer-related crime* on

> "any illegal, unethical or unauthorized behaviour relating to automatic processing and the transmission of data".[105]

Tietotekniikan osuus on edellä olevissa määritelmissä kuvattu eri tavoin. Yksityiskohtaisin luonnehdinta on Euroopan neuvoston edellisessä määritelmässä, jossa edellytetään tietokoneen olevan joko tekoväline tai teko-objekti. Laajimmat mahdollisuudet tietotekniikan osuuden huomioon ottamiselle antaa Euroopan neuvoston jälkimmäinen määritelmä, joka edellyttää teolta ainoastaan liittymistä tietotekniikkaan. Näiden väliin jää OECD:n käyttämä määritelmä; se edellyttää teon liittyvän automaattiseen datan käsittelyyn ja siirtoon. Sekä Euroopan neuvoston edellisen että OECD:n määritelmän mukaan teon on oltava laiton, kun taas Euroopan neuvoston jälkimmäisessä määritelmässä kiinnitetään erityistä huomiota vahingoittamis- tai hyötymistarkoitukseen.

Määritelmien soveltaminen saattaa johtaa erilaisiin lopputuloksiin, niin arvovaltaisten tahojen esittämiä kuin ne ovatkin. Huomattakoon kuitenkin, että sen paremmin OECD kuin Euroopan neuvostokaan eivät ole pyrkineetkään autoritaariseen käsitteen määrittelemiseen.

Viime vuosien nopea tekninen kehitys on aiheuttanut sen, että tietotekniikkarikosten ohella ja yhä useammin myös niiden asemesta on käytetty termiä "verkkorikos" (cybercrime). Euroopan neuvoston verkkorikoskonventiossa käsitettä ei ole määritelty mutta yleissopimuksen valmistelleen asiantuntijakomitean (PC-CY) marraskuussa 1996 asettaessaan Euroopan kriminaalipoliittinen komitea CDPC totesi mm. seuraavaa:[106]

> By connecting to communication and information services users create a kind of common space, called "cyber-space", which is used for legitimate purposes but may also be the subject of misuse. These "cyber-space offences" are either committed against the integrity, availability, and confidentiality of computer systems and telecommunication networks or they consist of the use of such networks of their services to commit traditional offences. The transborder character of such offences, e.g. when committed through the Internet, is in conflict with the territoriality of national law enforcement authorities.

---

104 EN:n raportti 89, s. 9.
105 OECD:n raportti, s. 6.
106 Päätös CDPC/103/211196.

Suomi

Suomessa ei tietotekniikkarikoksen käsitteen määrittelemiseksi ole nähty paljonkaan vaivaa. *Lehtimajan* mukaan atk-rikoksiksi kutsutaan sellaisia rikoksia, joiden kohteena, välikappaleena tai tekoympäristönä on atk-järjestelmä siihen kuuluvine laitteineen.[107]

Vaikka tietotekniikkarikoksen käsite – jäljempänä esitettävin tavoin – asiallisesti on sisällytetty suomalaiseen rikoslainsäädäntöön, ei lainvalmistelussa ennen 1990-luvun loppua ole paneuduttu käsitteen täsmentämiseen yleisellä tasolla, vaan lähtökohdaksi on otettu Euroopan neuvoston raporttiin liittyvä, jäljempänä yksityiskohtaisesti käsiteltävä kriminalisointisuositus tekotapaluetteloineen.[108]

Atk-sanakirja käyttää termiä *atk-rikos* ja määrittelee sen rikokseksi, rikkomukseksi, väärinkäytökseksi tai vahingonteoksi, joka kohdistuu tietojärjestelmään tai sen tietoihin tai muutoin tehdään tietotekniikkaa käyttäen.[109] Kirjassa on myös hakusana *tietokonerikos,* johon ei liity määritelmää; lisäksi kirjaan on otettu hakusanat *atk-petos, atk-sabotaasi, atk-vakoilu, atk-väärennys, tietorikos* ja *tietosuojarikos;* näiden määritelmät muistuttavat suurelta osin Euroopan neuvoston vastaavia suositustekstejä. Jossain määrin outona pidän sitä, että Atk-sanakirjasta kokonaan puuttuu hakusana ”tietotekniikkarikos”, vaikka termi on rikosoikeuden puolella ollut lähes yksinomaisessa käytössä jo kohta kymmenen vuotta.

Edellä mainitsin verkkorikoksen käsitteen. Lähellä tätä on *Lehtosen* määritelmän mukainen Internet-rikos:[110]

> Med Internet-brott avses sådana brott vars objekt eller handlingsmedel är Internet-nätverket samt anordningar, system och tjänster och vars utförande förutsätter att de används samt vilka är stadgade som straffbar i någon stats lagar.

Ulkomainen kirjallisuus

Ulkomaisesta oikeustieteellisestä kirjallisuudesta on löydettävissä useita määritelmiä, joskin monet tutkijat ovat tyytyneet käsittelemään aihetta pitäen lähtökohtanaan OECD:n ja Euroopan neuvoston raporteissa esitettyä. Niinpä *Sieber* yhdeksi alan perusteoksista luettavissa olevassa kirjassaan ”The International

---

[107] Lehtimaja, Atk-rikospolitiikasta, s. 260.

[108] Ks. esim. HE 94/1993, s. 17 ss., jossa esityksen yleisperustelujen 6. jakso on otsikoitu ”Suomen oikeus ja Euroopan neuvoston tietokonerikossäännöksiä koskevat suositukset”. Huomattakoon, että HE:ssä käytetty termi on ”tietokonerikos”.

[109] Atk-sanakirjan (s. 18) tarjoamia ulkomaisia vastineita atk-rikokselle ovat englannin *computer crime,* ranskan *délit informatique* ja ruotsin *databrott.*

[110] Lehtonen, Jurisdiktion, s. 4.

Handbook on Computer Crime" lähtee tietotekniikkarikoksia luokitellessaan OECD:n määritelmästä. Sieber jakaa tietotekniikkarikokset kolmeen pääryhmään: tietotekniikkaan liittyvät taloudelliset rikokset (computer-related economic crimes), tietotekniikkaa käyttäen tehdyt yksilön oikeuksien loukkaukset (computer-related offences against personal rights) sekä yksilötasoa laajemmalle ulottuvien intressien tietotekniikka-avusteiset loukkaukset (computer-related offences against superindividual interests).[111]

Saksalaiset oikeustieteilijät ovat edellä *Sieberin* lisäksi esittäneet useita tietotekniikkarikoksen määritelmiä. *Silvia Frey,* joka väitöskirjassaan esittelee mm. *Mühlenin, Tiedemannin* ja *Sieberin* näkemyksiä, antaa käsitteelle seuraavanlaisen sisällön:

> Der Begriff der "Computerkriminalität" ist deshalb auf diejenigen kriminellen Verhaltensweisen zu beschränken, die ohne Computertechnik in vergleichbarer Form nicht zu verwirklichen sind, also auf computerspezifische Delikte. Der Täter nutzt gerade die besonderen technischen Möglichkeiten der EDV für seine Zwecke aus, vor allem durch missbräuchliche Einwirkung auf den EDV-Prozess selbst.[112]

Ruotsissa, jonka *Datalagen* vuodelta 1973 eräässä mielessä on edelläkävijä tietotekniikkarikosten kriminalisoinnin alueella, eivät oikeustieteilijät ole suomalaisia innokkaammin kehittäneet määritelmää tietotekniikkarikoksen käsitteelle.

Polisöverintendent *Hans Wranghult,* joka vuosina 1987–88 on tutkinut tietotekniikkarikollisuutta USA:ssa Stanford Research Institutessa (SRI-International), jakaa tietotekniikkarikokset toisaalta tietokonerikoksiin (datorbrott) ja toisaalta tietokoneavusteisiin rikoksiin (datorrelaterade brott), jolloin edellisillä tarkoitetaan joko tietojärjestelmään kohdistuneita tai tietojärjestelmää apuna käyttäen tehtyjä rikoksia, joiden tekijä on käyttänyt hyväkseen perehtyneisyyttään tietotekniikkaan yleensä tai erityisesti kysymyksessä olevaan järjestelmään, ja jälkimmäisillä muita tietotekniikkaan liittyviä rikoksia. "Datakriminalitet" on molemmat rikoslajit kattava yläkäsite.[113]

Tanskalainen *Vagn Greve* luokittelee tietotekniikkarikollisuuden samaan tapaan kuin *Wranghultkin*: varsinaiseen atk-rikollisuuteen (den egentlige edb-

---

[111] Sieber, Handbook, s. 3: "Up to the present three main groups of computer crime (falling within the OECD definition) have been revealed: computer-related economic crimes such as computer fraud, computer espionage, and computer sabotage; computer-related offences against personal rights, especially against the citizens' right to privacy, and computer-related offences against superindividual interests such as offences against national security, control of transborder data flow, integrity of computer-based procedures and data-communication networks, or democratic legitimation of computer-based parliamentary decisions."

[112] Frey, s. 5 ss.

[113] Wranghult, s. 9.

kriminalitet) ja atk-avusteiseen rikollisuuteen (kriminalitet ved hjaelp af edb). *Greve* myös toteaa, että ero näiden kahden välillä ei ole selvä.[114]

Norjalainen *Stein Schjølberg,* joka *Wranghultin* tavoin on tehnyt tietotekniikkarikoksia koskevaa tutkimusta SRI-Internationalissa, hyväksyy Yhdysvaltain oikeusministeriön manuaalissa vuodelta 1979 esitetyn määritelmän, jonka mukaan tietotekniikkarikos (computer crime) on ”any illegal act for which knowledge of computer technology is essential for its perpetration (investigation or prosecution)”.[115] *Schjølberg* korostaa, että jokainen yhteys rikoksen ja tietokoneen välillä ei suinkaan tee rikoksesta tietotekniikkarikosta.[116] Hän jakaa tietotekniikkarikokset kahteen pääkategoriaan: rikoksiin, joissa tietokone on tekoväline, ja rikoksiin, jotka kohdistuvat tietokoneeseen.

Norjan Økokrimin tietotekniikkarikosyksikön johtaja, førstestatsadvokat *Inger Marie Sunde* on tyytynyt melko yleiseen määrittelyyn:[117]

> Med ”IKT-kriminalitet” menes kriminalitetsformer som er relatert til bruk av informasjons- og kommunikasjonsteknologi. Begrepet dekker nye kriminalitetsformer som datainnbrudd og skadeverk via kommunikasjonsnett. Det dekker også alle type kriminalitet hvor man tar beslag i elektroniske bevis. Eksempelvis faller narkotikasaker hvor det tas beslag i siktedes e-post og saker om spredning av barnepornografi via internett, i den siste kategorien.

Sunden käsitys tietotekniikkarikosten ulottuvuudesta tuntuu olevan varsin laaja ja heijastelee nykyaikaisen verkkopoliisin toimenkuvaa, johon yhtä lailla kuin ”perinteisten” tietotekniikkarikosten tutkiminen kuuluu myös lähes minkä tahansa rikostyypin yhteydessä mahdollisesti esiintyvän elektronisen todistusaineiston selvittäminen.

Ruotsalainen *Jan Silvander* ei tuoreessa väitöskirjassaan ”Dator- och datarelaterade brott” pyrikään määrittelemään tietotekniikkarikoksen käsitettä vaan tekee työn nimestäkin ilmenevän jaottelun. ”Datorrelaterade brott” tarkoittaa tekoja, jotka ”är riktade mot en datoranläggning och de installationer som utnyttjas för informationsöverföring” ja ”datarelaterade brott” puolestaan ”riktas mot infor-

---

[114] Greve, s. 16: ”Den egentlige edb-kriminalitet er rettet direkte mod selve edb-systemet (datamat, programmel, lagrede data og transmissionsledninger m.m.).” ja s. 61: ”Under II behandlede jeg de tilfaelde, hvor beskyttelsesinteressen (og angrebsobjektet) i det vaesentlige var knyttet til edb-systemet som sådant eller til en del af dette. I naervaerende afsnit III er det kun angrebsobjektet eller midlet, som er et edb-anlaeg.”

[115] Schjølberg, s. 4 s.

[116] Schjølberg käsittelee myös rikoslajin nimikettä: ”Computer abuse, computer fraud, computer-related crime, computer-assisted crime, and computer crime are among terms used to identify this category of criminal activity, depending on the purposes of the descriptions. In the recent years, however, *computer crime* is regarded as the simplest, broadest and most widely accepted term in the criminal justice community and in public.” Ibid. s. 3.

[117] Sunde, s. 275.

mation i olika former".[118] Tällä tavoin määritellyt tekotavat mahtuvat hyvin esimerkiksi *Sunden* määritelmään ja vastaavat periaatteessa edellä esittämääni jakoa data- ja informaatiorikoksiin, joskin hieman harhaanjohtavalta tuntuu, että nimenomaan "datarelaterade" rikokset ovat asiallisesti informaatiorikoksia.

Interpol, RCMP ja YK

International Criminal Police Organization (ICPO-Interpol) laajensi edellä esitettyä USA:n oikeusministeriön manuaalin määritelmää 1981 pidetyssä seminaarissa siten, että tietotekniikkarikoksiksi katsottiin "any illegal act for which knowledge of computer technology is essential for its perpetration, investigation, prosecution or sentencing".[119] Kaikkia edellä esitettyjä määritelmiä monipuolisempi on Ruotsin valtuuskunnan toisessa pohjoismaisessa talousrikoskonferenssissa 1983 esittämä, jonka mukaan tietotekniikkarikos on rikos, joka on kohdistunut tietojärjestelmään tai tehty sitä käyttäen ja jota tehdessään rikoksentekijä on käyttänyt hyväkseen tietoteknistä tietämystään tai perehtyneisyyttään asianomaiseen järjestelmään.[120]

Kanadan kuninkaallisen ratsupoliisin eli *Royal Canadian Mounted Policen (RCMP*) piirissä on tehty merkittävää tietotekniikkarikoksiin liittyvää selvittelytyötä. RCMP:n tietoturvallisuusohjeissa vuodelta 1989 annetun määritelmän mukaan tietotekniikkarikos on "criminal activity aimed at any function of a computer system and includes data stored within or generated by a computer system that is used to assist in the commission of a criminal offence".[121]

Yhdistyneiden Kansakuntien lokakuussa 1992 järjestämässä asiantuntijakokouksessa valmistellussa tietotekniikkarikoskäsikirjassakaan ei pyritä esittämään tietotekniikkarikoksen määritelmää, vaan tyydytään viittaamaan OECD:n ja Euroopan neuvoston raportteihin. Huomionarvoista on kuitenkin käsikirjassa korostettu käsitteiden "computer misuse" ja "computer abuse" välinen ero, jolloin edellisellä ymmärretään sellaista tietokoneen tai -järjestelmän väärinkäyttämistä, jota ei voida lukea rikosoikeudellisessa mielessä tekijän syyksi tahallisena menettelynä, ja jälkimmäisellä taas tahallista oikeudenvastaista väärinkäyttämistä.[122]

---

[118] Silvander, s. 30.

[119] Tenhunen, Information Security, s. 1.

[120] Tenhunen, Information Security, s. 2, jossa englanninkielinen versio määritelmästä: "A computer crime is a crime which was committed against or by means of a computer system by someone who, in the commission of the crime, used his knowledge of computer technology or his acquaintance with the system in question."

[121] Tenhunen, Information Security, s. 2.

[122] UN Manual, kohta 24: "The terms 'computer misuse' and 'computer abuse' are also used frequently, but they have significantly different implications. Criminal law recognizes the concepts of unlawful or fraudulent intent and of claim of right; thus, any criminal laws that relate to computer crime would need to distinguish between accidental misuse of a computer system, negligent misuse of a computer system and intended, unauthorized access to or misuse of a computer system, amounting to computer abuse. Annoying behaviour must be distinguished from criminal behaviour in law."

Suomen kielessä ei termille ”computer misuse” ole olemassa vakiintunutta vastinetta; joskus on käytetty sanaa ”tietokoneväärinkäytös”, joka nyt käyttöön otettua ”tietotekniikkarikosta” mukaillen olisi korvattavissa vaikkapa sanalla ”tietotekniikkaväärinkäytös” tai ”tietotekninen väärinkäytös”. Erottelulla on sinänsä merkitystä myös Suomen oikeutta ajatellen: rikosoikeuden keinot eivät ole eivätkä saa olla ainoat eivätkä edes ensisijaiset keinot tietotekniikkarikosten torjunnassa, ja niin muodoin hyvin suuri osa tietoteknisistä väärinkäytöksistä jää rangaistavuuden alueen ulkopuolelle. Näin on pääsääntöisesti asianlaita tuottamuksellisten tekomuotojen kohdalla.

1.2.3.2 Oma määritelmäni

Edellä esitetyt määritelmät ovat kolmentyyppisiä. Niissä on ensinnäkin saatettu korostaa tietokoneen ja -järjestelmän asemaa rikoksen tekovälineenä, -objektina tai -ympäristönä. Toisaalta määritelmissä on tuotu esiin rikoksen tekemisessä, tutkimisessa, syytteeseenpanossa ja tuomitsemisessa vaadittava tietotekninen asiantuntemus. Kolmanneksi on esitetty määritelmiä, joissa molemmat mainitut elementit ovat edustettuina.

On selvää, että ensin mainitun tyyppiset määritelmät eivät aina johda tyydyttäviin tuloksiin. Vaikka mikrotietokoneen anastamisen kohteena on tietokone, ei varkaus ole tietotekniikkarikos. Murhasta ei tule tietotekniikkarikosta, vaikka se tehtäisiin esimerkiksi muuttamalla automaattisen tietojenkäsittelyn avulla ylläpidettyjä sairaalan potilastiedostoja seurauksin, että potilas väärää lääkettä saatuaan menehtyy – tosin kuvatussa tilanteessa on murhan *ohessa* syyllistytty tietotekniikkarikokseen.[123]

Vaatimus tietotekniikan tuntemuksesta on edellistä yksiselitteisempi tunnusmerkki. Kuitenkaan ei ole kysymys tietotekniikkarikoksesta, kun hyvin tietotekniikkaan perehtynyt kauppias syyllistyy perehtyneisyyttään hyväksikäyttäen petokseen erehdyttämällä asiakkaansa ostamaan mikrotietokoneen, jonka ominaisuudet eivät lainkaan vastaa kauppiaan lupaamia.

Ollakseen käyttökelpoinen täytyy tietotekniikkarikoksen määritelmän sisältää molemmat elementit: sekä rikoksen tietotekninen tekoympäristö että rikoksen tekemisen tai selvittämisen edellyttämä tietotekninen asiantuntemus. Näistä lähtökohdista ja edellä esitettyjä määritelmiä yhdistäen olen esittänyt seuraavan määritelmän:

---

[123] On kuitenkin tärkeää muistaa, että myös tällaisten rikosten selvittämisessä saattaa olla hyvin suuri merkitys ns. elektronisella todistusaineistolla, jota nykyään voi esiintyä lähes minkä tahansa ns. perinteisenkin rikoksen tutkinnassa. Tämä tavallaan hämärtää rajaa tietotekniikkarikosten ja muiden rikosten välillä mutta toisaalta korostaa jäljempänä käsiteltävän tietotekniikkarikosten yhteisen suojeluobjektin merkitystä rikoskategorian määrittelyssä.

> *Tietotekniikkarikos on rangaistava teko, jonka kohteena, välikappaleena tai tekoympäristönä on tietojärjestelmä siihen kuuluvine laitteineen ja jonka tekeminen ja/tai rikosprosessuaalinen käsitteleminen välttämättömästi edellyttää tietoteknistä tietämystä.*[124]

Määritelmä on toisaalta riittävän suppea rajaamaan käsitteen ulkopuolelle rikokset, joissa tietojärjestelmä tai siihen kuuluvat laitteet tavalla tai toisella tosin ovat mukana mutta joissa niillä ei teon oikeudellisen arvioinnin kannalta ole olennaista ja itsenäistä merkitystä. Toisaalta määritelmä on tarpeeksi kattava, jotta paitsi rikoslain data- ja informaatiorikokset myös tietokoneohjelmien ja integroitujen piirien piirimallien tekijänoikeuksiin kohdistuvat rikokset mahtuvat käsitteen piiriin. Määritelmä on kuitenkin edellä esitettyä *Sunden* näkemystä suppeampi sikäli, että mikä tahansa rikos, jonka selvittely saattaa edellyttää elektronisen todistusaineiston tutkimusta (esimerkiksi kirjanpitorikos tai veropetos), ei välttämättä ole määritelmässä tarkoitettu tietotekniikkarikos.

Tietojärjestelmällä määritelmän tarkoittamassa mielessä voidaan ymmärtää samaa kuin rikoslain 38 luvun 8 §:n tietomurtoa ja 34 luvun 9 a §:n vaaran aiheuttamista tietojenkäsittelylle koskevissa säännöksissä: tietojärjestelmällä tarkoitetaan järjestelmää, jossa tietoja käsitellään, varastoidaan tai siirretään sähköisesti tai muulla vastaavalla teknisellä keinolla.[125] Tietojärjestelmällä ei tarkoiteta yksinomaan useiden laitteiden tietojenkäsittely- ja siirtolaitteiden muodostamaa verkostoa, vaan yksittäinenkin tietokone voi muodostaa kysymyksessä olevan järjestelmän.[126]

---

[124] Pihlajamäki, Tutkinta. Alun perin määritelmässäni tosin edellytettiin ”tietoteknistä *erityis*tietämystä” mutta kymmenessä vuodessa ihmisten tietotekninen osaaminen on siinä määrin lisääntynyt, että aikanaan erityistietämykseksi ajateltu osaaminen ei enää ole vain harvojen hallitsemaa.

[125] HE 94/1993, s. 155.

[126] HE 4/1999, s. 8. Euroopan neuvoston verkkorikoskonvention selitysmuistiossa selvennetään ”computer systemin” ja ”networkin” käsitteitä seuraavasti:

23. A computer system under the Convention is a device consisting of hardware and software developed for automatic processing of digital data. It may include input, output, and storage facilities. It may stand alone or be connected in a network with other similar devices ”Automatic” means without direct human intervention, ”processing of data” means that data in the computer system is operated by executing a computer program. A ”computer program” is a set of instructions that can be executed by the computer to achieve the intended result. A computer can run different programs. A computer system usually consists of different devices, to be distinguished as the processor or central processing unit, and peripherals. A ”peripheral” is a device that performs certain specific functions in interaction with the processing unit, such as a printer, video screen, CD reader/writer or other storage device.

24. A network is an interconnection between two or more computer systems. The connections may be earthbound (e.g., wire or cable), wireless (e.g., radio, infrared, or satellite), or both. A network may be geographically limited to a small area (local area networks) or may span a large area (wide area networks), and such networks may themselves be interconnected. The Internet is a global network consisting of many interconnected networks, all using the same protocols. Other types of networks exist, whether or not connected to the Internet, able to communicate computer data among computer systems. Computer systems may be connected to the network as endpoints

1.2.3.3 Säännösten tulkinnasta

Tietoteknisessä ympäristössä tehtyyn moitittavalta vaikuttavaan menettelyyn soveltuvan rangaistussäännöksen löytäminen voi osoittautua vaikeaksi nähdäkseni lähinnä kahdesta syystä: joko soveltuvaa säännöstä yksinkertaisesti ei tunnu olevan olemassa tai sitten olemassa olevan, sinänsä soveltuvalta vaikuttavan säännöksen tunnusmerkistö ei täysin vastaa tosiasiallista tapahtumainkulkua.

Ensin mainitussa tilanteessa on olemassa *lainaukko* – lain soveltaja ei säännöksen puuttuessa tiedä, onko menettely sallittua vai kiellettyä. Oikeudellisessa ratkaisutoiminnassa ei ongelmaa kuitenkaan voida sivuuttaa, sillä ratkaisijalla on epäselvissäkin tapauksissa ratkaisupakko.[127]

Analogia ja laventava tulkinta

Analogiasta yleensä tai sen suhteesta sallittuun tulkintaan ei meillä ole nimenomaisesti säädetty ennen 1.1.2004 voimaan tullutta rikoslain yleisten oppien uudistamista koskevaa lainsäädäntöä. Palaan uudistukseen hieman jäljempänä.

Aarnion mukaan aukon täyttäminen on läheisessä yhteydessä *analogian* käsitteeseen; koska oikeusideologia rakentuu vahvasti yleistettävyyden ajatukselle eli ajatukselle, että samankaltaisia tapauksia on kohdeltava samalla tavalla, on aukon täyttäminen olennaisten samankaltaisuuksien etsimistä, analogian hyväksi käyttöä.[128]

Tulkintametodina hyvin lähellä analogiaa ja siitä joskus vaikeasti erotettavissa on *laventava tulkinta,* lakitekstin soveltaminen sen luonnollisen merkityssisällön ulkopuolelle.[129] Aukkoa voi pyrkiä täyttämään myös laventavan tulkinnan avulla, joskin tällöin lienee kysymyksessä lähinnä aukon supistaminen laajentamalla lain soveltamisalaa.

---

or as a means to assist in communication on the network. What is essential is that data is exchanged over the network.

Tässä yhteydessä on myös mielenkiintoista havaita, miten laveaksi Atk-sanakirja (s. 204) määrittelee tietojärjestelmän:

1. Ihmisistä, tietojenkäsittelylaitteista, tiedonsiirtolaitteista ja ohjelmista koostuva järjestelmä, jonka tarkoitus on tietoja käsittelemällä tehostaa tai helpottaa jotakin toimintaa tai tehdä toiminta mahdolliseksi.

2. Abstrakti systeemi, jonka muodostavat tiedot ja niiden käsittelysäännöt.

127 Vrt. esim. Laakso, s. 145 ss. ja Aarnio, s. 171 ss., jossa Aarnio ryhmittelee aukkoja mm. alkuperäisiin ja jälkiperäisiin, avoimiin ja kätkettyihin sekä aitoihin ja epäaitoihin.

128 Aarnio, s. 173. Aarnion mukaan osaksi juuri tätä kautta lainkäyttö ja oikeustiede kehittävät oikeutta, jatkavat siitä, mihin oikeuden luominen on lainsäätäjältä jäänyt.

129 Ks. Aarnio, s. 258 ja Laakso, s. 151 ss. Molemmat tekevät eron analogian ja laventavan tulkinnan välille, mutta molemmat myös toteavat, että rajanveto on vaikeaa; Laakson mukaan monesti on lähinnä makuasia, kumpaan kategoriaan tietty tulkinta sijoitetaan. Aarnio taas toteaa, että ”vain *periaatteessa, ei* käytännössä, on mahdollista sanoa: tämä on laventavan tulkinnan ääriraja, tästä eteenpäin alkaa analogia”. Ks. myös Honkasalo, Yleiset opit I, s. 45, jossa esitetyn mielipiteen mukaan varsinaisen tulkinnan alaan kuuluu säännöksen sanamuodon rajoissa tapahtuva soveltaminen, kun taas analogia on lain sanamuodosta vapautunutta soveltamista, laista ilmenevien oikeusajatusten käyttämistä esiintyvien oikeustapausten ratkaisemisessa.

Rikosoikeudellisessa lainkäytössä ongelmallista ei ole niinkään se, kutsutaanko aukon täyttämismetodia analogiapäättelyksi vai laajentavaksi tulkinnaksi. Ongelmana on sen sijaan se, onko aukon täyttäminen ylipäänsä sallittua.

Rikosoikeudessa noudatetaan *analogiakieltoa,* joka *Fränden* mukaan perustuu ajatukselle, että lakitekstiä tulee ymmärtää ja tulkita normaalilla kielitaidolla.[130] *Nuutila* katsoo analogiakiellon seuraavan hallitusmuodon, Euroopan ihmisoikeussopimuksen sekä kansalais- ja poliittisia oikeuksia koskevan yleissopimuksen määräyksistä. Hänen mukaansa laillisuusperiaate ei ainoastaan vaadi, että asiasta on säädetty laissa, vaan se vaatii myös tietynlaista säännösten tulkintaa.[131] *Honkasalo* oli vielä toisella kannalla, kun hän katsoi, että lainanalogia *in malam partem* on sallittava; oikeusanalogian sallimiseen nähden hän sen sijaan asettui kielteiselle kannalle.[132]

Lainaukon täyttämistä ajatellen lähtökohtana siis on, että täyttämiseen analogian tai laventavan tulkinnan keinoin on suhtauduttava kielteisesti, joskaan rajanveto sallittuun tulkintaan nähden ei aina ole ongelmatonta. *Lahti* esimerkiksi toteaa, että legaliteettiperiaatteen kasvaneesta merkityksestä huolimatta rikosoikeudessamme ei ole voimassa yleistä (vahvaa) tulkintaperiaatetta, jonka mukaan rikosoikeudellisia säännöksiä olisi tulkittava suppeasti (supistavasti), syytetylle edullisella tavalla.[133]

Koska kuitenkin esimerkiksi tietokoneviruksen valmistamista ei ennen vuotta 1999 ollut kriminalisoitu, ei valmistajaa siis yleensä voitu rangaista (ainakaan pelkästä valmistamisesta), vaikka hänen valmistamansa virus levitessään saattoikin aiheuttaa samankaltaisia ja yhtä vaarallisia seurauksia kuin ne teot, joiden valmistelu on kriminalisoitu rikoslain 34 luvun 9 §:ssä.

Tilanne on kuitenkin toinen, kun joudutaan harkitsemaan olemassa olevan säännöksen soveltamisalan laajentamista sellaiseen tekoon, joka ainoastaan joiltakin osin näyttää jättävän täyttämättä säännöksessä asetetun objektiivisen tunnusmerkistön. Suhteessa oikeustieteelliseen ja ehkä nimenomaan rikosoikeudelliseen terminologiaan on tietotekninen suomenkielinen käsitteistö muotoutunut täysin itsenäisesti. Kieliopillisen tulkinnan periaatteiden mukaan tulkittavalle ilmaisulle ei tulisi ilman riittäviä perusteita antaa yleisestä kielen-

---

130 Frände, Straffrätt, s. 54 s.

131 Nuutila, Rikoslaki, s. 56 ss.

132 Honkasalo, Yleiset opit I, s. 49. Honkasalon mukaan ”nykyaikaista oikeuskäsitystä voidaan tuskin saada vakuuttuneeksi siitä, että tuomarin orjallinen sitoutuneisuus lain sanamuotoon olisi välttämätön yksilön turvaamiseksi valtiovallan taholta tapahtuvaa väärinkäyttöä vastaan. Se näkee pikemminkin vaaran liiallisessa muodollisuudessa, joka estää oikeuden toteutumasta samanlaisissa tapauksissa samalla tavalla.” *Lainanalogialla* Honkasalo tarkoittaa säännöksen soveltamista tapaukseen, johon se ei sanamuotonsa puolesta sovellu, mutta johon säännöksen perustana oleva ratio vaatii sitä sovellettavaksi. *Oikeusanalogia* pyrkii saamaan selville ne yleiset periaatteet, joiden ilmauksia positiiviset säännökset ovat, voidakseen soveltaa niitä käytännössä esiintyvään tapaukseen. Mts. 45 s.

133 Lahti, LM 1996, s. 937

käytöstä poikkeavaa merkitystä[134] – miten on meneteltävä silloin, kun lakitekstin yleiskielinen ilmaisu ei ole riittävän täsmällinen tai yksiselitteinen, jotta sen perusteella voitaisiin riidattomasti arvioida tietyn rikoslain säännöksen soveltuvuutta todellisessa tilanteessa?

Frände toteaa, että rikosoikeus ei aina tyydy pelkästään yleiskielen merkityksiin. Usein keskeisille juridisille käsitteille annetaan yleiskielestä poikkeava juridistekninen määritelmä. Analogiakielto ei suinkaan estä sellaista menettelyä edellyttäen, että kysymys on vakiintuneesta teknisestä kielenkäytöstä.[135]

Tietotekniikkarikoksia koskevissa rangaistussäännöksissä käytetään tietotekniikan alueella kehittyneitä (juridisteknisiä) termejä. Nämä eivät – niin kuin jäljempänä havaitaan – aina ole merkityssisällöltään niin yksiselitteisiä, että ongelmilta voitaisiin välttyä. Kysymyksessä ei suinkaan ole tietotekniikkarikossäännöksille ominainen piirre; jos nyt joudutaan miettimään, mikä itse asiassa on ”automaattiseen tietojenkäsittelyyn soveltuva tallenne”, niin ei aikaisemminkaan ongelmitta kyetty aina toteamaan, mitä ”asiakirjalla” oli ymmärrettävä.

Nuutilan mukaan väärennyskriminalisoinnissa tarkoitettu ”asiakirjan” tai ”todistuskappaleen” merkityssisältö voi poiketa jossain määrin normaalikielestä. Lainkohdan *systemaattisessa* tulkinnassa voidaan esimerkiksi arvioida koko sitä rikoslain lukua kokonaisuudessaan, jonka alaisesta rikoksesta on puhe. Tulkinnassa voidaan nojautua *lainopillisiin* teorioihin. Oikeussäännöksiä on luettava myös *historiallisissa yhteyksissään.*[136]

Hyvä esimerkki *Nuutilan* mainitseman todistuskappaleen merkityssisällön tulkinnasta on jäljempänä osassa II väärennystä koskevassa jaksossa 3.1. tarkemmin käsiteltävä korkeimman oikeuden ratkaisu 2003:58, jossa väärennyksen kohteena olleen älykortin mikropiirin ei katsottu voivan tulla kysymykseen rikoslain 33 luvun 6 §:ssä tarkoitettuna todistuskappaleena, jota olisi käytetty tai voitu käyttää oikeudellisesti merkityksellisenä todisteena. Ratkaisu perustuu ilmeisesti väärennyskriminalisointien ensisijaisen suojeluobjektin eli todistelun luotettavuuden korostamiseen eikä rikoslain 33 luvun määritelmäsäännöksessä todistuskappaleelle annettu juridistekninen merkityssisältö ole korkeimman oikeuden mielestä vastannut konkreettista asiaintilaa.

Tulkintatilanne voi muodostua hyvinkin vaikeaksi, jos lainsäätäjä tietoisesti käyttää yleiskielessä vakiintuneen merkityksen saanutta termiä yleiskielestä poikkeavassa merkityksessä mutta jättää sen merkityssisällön laissa määrittelemättä. Tietomurtoa koskevassa rikoslain 38 luvun 8 §:n 1 momentissa käytetään ilmaisua ”turvajärjestelyn muuten murtamalla” ja säännöksen perusteluissa[137]

---

134 Aarnio, s. 256.
135 Frände, Straffrätt, s. 55.
136 Nuutila, Rikoslaki, s. 57.
137 HE 94/1993, s. 155.

taas todetaan murtamisella tarkoitettavan turvajärjestelyn läpäisyn luvattomuutta ilmaisevaa kielikuvaa. Korkein oikeus on ratkaisussaan 2003:36 nimenomaisesti viitannut tähän perusteluissa lausuttuun ja siitä johtamaansa säännöksen tarkoitukseen katsoessaan ns. porttiskannauksen voivan toteuttaa tietomurron yrityksen tunnusmerkistön, vaikkei skannauksella sinänsä murtamisen (yleiskielisen merkityksen) kanssa mitään tekemistä olekaan. Käsittelen tätäkin ratkaisua tarkemmin osan II luvun 2 jaksossa 2.1.1.

Analogiakielto siis sisältyy 1.1.2004 voimaan tulleeseen rikoslain yleisten oppien uudistukseen ja se on ilmaistu laillisuusperiaatteesta säätävässä rikoslain 3 luvun 1 §:n 1 momentissa sanomalla, että rikokseen syylliseksi saa katsoa vain sellaisen teon perusteella, joka tekohetkellä on laissa *nimenomaan* säädetty rangaistavaksi. Säännöksen perusteluissa[138] todetaan lainsäätäjän käyttämien käsitteiden vaativan aina tulkintaa, koska lainsäätäjä käyttää tyyppikäsitteitä. Analogiasta sanotaan olevan kysymys, kun normia sovelletaan tapaukseen, johon se ei lain sanamuodon yleiskielisessä tai erikseen määritellyssä juridisteknisessä merkityksessä sovellu mutta jota tapausta kuitenkin voidaan pitää jossakin suhteessa samanlaisena taikka rinnasteisena.

Tulkinnasta analogian vastakohtana on perustelujen mukaan kysymys, kun merkityssisältö vahvistetaan lain sanamuodon puitteissa; lainkäyttäjä ei saa edetä sanamuodon ulkopuolelle. Sanamuodon sallimia rajoja määriteltäessä yhtenä lähtökohtana voidaan pitää termien yleiskielistä merkitystä, mutta usein laissa joudutaan myös käyttämään käsitteitä, joiden sisältöä on tarkennettu antamalla niille juridistekninen sisältö. Sallittua tulkintaa sanotaan olevan toisaalta sellainen lain soveltaminen, joka perustuu termeille annettuun normaalikielen mukaiseen merkitykseen, ja toisaalta sellaisen soveltamisen, jonka perusteena on termeille oikeustieteessä, lakien esitöissä taikka mielummin itse laissa vahvistettu juridistekninen merkityssisältö.[139]

Kysymyksen sallitun tulkinnan ja kielletyn analogian rajoista todetaan palautuvan osittain ennakoitavuuskysymykseen ja siihen, miten määräytyy yleisessä tulkintakäytännössä ennakoitavissa oleva merkitys.

Kansainväliset asiakirjat tulkinnan lähteinä

Tietotekniikkarikokset ovat erityisasemassa useimpiin muihin rikoslajeihin nähden sikäli, että muun muassa Suomessa aloite niitä koskevien kriminalisoin-

---

[138] HE 44/2002, s. 34. Ks. myös Matikkala, Näkökohtia, erityisesti s. 226 ss., jossa hän kommentoi (ja kritisoi) hallituksen esitystä.

[139] Viimeksi mainitun osalta *Matikkala* toteaa, että ”(o)lisi siis ilmeisesti sallittua antaa lain termille y (normaalikielisen merkityksen ulkopuolellekin menevä) esitöissä tai jopa oikeustieteessä ’vahvistettu’ juridistekninen merkityssisältö. Mahtaako näissä oloissa olla syytä puhua laillisuusperiaatteesta edes kvalifioimattomassa ’laissa säädetty’ -merkityksessä, puhumattakaan ilmaisusta ’laissa nimenomaan säädetty rangaistavaksi’?” Ks. Matikkala, Näkökohtia, s. 226 s.

tien laatimiseksi on yleensä tullut kansainväliseltä kentältä, josta suomalainen lainsäätäjä on saanut myös mallit näille kriminalisoinneille. Suomen tietotekniikkarikoksia koskeva lainsäädäntö perustuu valtaosaltaan Euroopan neuvoston vuoden 1989 suositukseen; oikeastaan ainut omintakeisempi säännöstö on rikoslain 37 luvun maksuvälinepetosta koskeva sääntely ja jossain määrin omaan kansalliseen ideointiin perustuu myös 34 luvun 9 a §:n säännös vaaran aiheuttamisesta tietojenkäsittelylle.

Tietenkin tietotekniikkarikoksia koskeva lainsäädäntö on *kansallista* lainsäädäntöä – ainakin toistaiseksi, sillä Euroopan unionin piirissä ei jäsenmaita velvoittavia instrumentteja ole vielä olemassa, joskin valmisteilla olevasta puitepäätöksestä sellainen ajan mittaan muodostunee. Olemassa oleva sääntely perustuu siis kotimaiseen lainvalmisteluun ja kotimaiset lain esityöt ovat näin ollen käytettävissä tulkinnan lähteinä.

Kuitenkin mielestäni myös kansainväliselle aineistolle on juuri tietotekniikkarikosten kysymyksessä ollessa annettava tässä suhteessa merkitystä. Euroopan neuvoston vuoden 1989 suosituksen perusteluosassa on analysoitu eri rikostyyppien peruselementtejä sellaisella syvällisyydellä, johon vastaavia menettelyjä koskeva suomalainen lainvalmistelu ei yllä. Varsin syvällinen ja perusteellinen on myös Euroopan neuvoston verkkorikoskonvention selitysmuistio, ja kun sopimus aikanaan implementoidaan Suomen oikeuteen, on johdonmukaista ja järkevää, että mahdollisissa tulkintatilanteissa voidaan hyödyntää myös useiden valtioiden huippueksperttien neljän vuoden työn aikana dokumentoituja kannanottoja.

In dubio mitius

Täsmennettäessä moniselitteisiksi tai epätäsmällisiksi osoittautuvien käsitteiden merkityssisältöä on turvauduttava tulkintaan. Myös tällöin voidaan joutua käyttämään analogiapäättelyä tai laventavaa tulkintaa. Rikosoikeudellisen lainkäytön yhteydessä on katsottu olevan voimassa niin kutsuttu *in dubio mitius* -periaate, jonka mukaan laintulkintatilanteissa lakia on sovellettava sen tulkinnan mukaisesti, joka johtaa vastaajan kannalta lievempään lopputulokseen.[140]

Silloin, kun tulkintateitse joudutaan etsimään sisältöä uudelle normistolle ja kun lain esityöt tai oikeuskäytäntö eivät tarjoa tulkinnalle riittäviä välineitä, olisi mielestäni väärin kategorisesti päätöksenteon jokaisella tasolla ratkaista tulkintatilanteet vastaajalle edullisemmalla tavalla. Tällainen periaate johtaisi väistämättä siihen, että laki lopulta saisi sisällön, joka ei vastaisi sen paremmin lainsäätäjän tahtoa kuin yleistä oikeustajuakaan. Tässä suhteessa olen samaa mieltä kuin *Jonkka,* joka puolestaan yhtyy *Jareborgin* näkemykseen *in dubio*

---

[140] OLJ 1/93, s. 25 s.

mitius -periaatteesta eräänlaisena viimeisenä tulkintaperiaatteena, johon tulee turvautua vasta muutoin ratkaisemattomassa tasapainotilanteessa.[141]

Niin kauan kuin yleiskielestä poikkeavaakin tulkintaa käyttämällä voidaan perustellusti löytää lain tarkoituksen kanssa sopusoinnussa oleva kanta, tulee se hyväksyä, vaikka lainkäyttötilanteessa päädyttäisiinkin vastaajalle epäedullisempaan lopputulokseen.

Syyttämättä jättäminen vai syyte?

Sitä paitsi käsitykseni mukaan mainitun ratkaisemattoman tasapainotilanteen ollessa kysymyksessä ei sen olemassaolon toteamista (ja *in dubio mitius* -periaatteen soveltamista) tulisi hyväksyä hierarkkisesti kovin alhaisella oikeudellisen päätöksenteon tasolla – ei ainakaan silloin, jos kysymys on vähänkin merkittävämmästä tulkintaongelmasta. Poliisin tutkinnanlopettamispäätös tai syyttäjän syyttämättäjättämispäätös ovat tällaisissa tilanteissa kovin huonoja prejudikaatteja verrattuna käräjäoikeudenkin ratkaisuun saati sitten mahdollisesti saatavilla olevaan hovioikeuden tai ehkä jopa korkeimman oikeuden ratkaisuun.

Jääskeläinen on väitöskirjassaan käsitellyt kysymystä oikeuskysymysten ratkaisemisesta syyttäjän päätöksellä ja toteaa muun muassa, että ”lain soveltamiseen liittyvien kysymysten kuulumista tuomioistuimille, viime kädessä korkeimmalle oikeudelle, korostaa korkeimman oikeuden rooli ennakkopäätöstuomioistuimena, jonka tehtävänä on juuri antaa lain soveltamiseen liittyviä, oikeuskäytännön yhtenäisyyttä ohjaavia arvovaltaisia tulkintakannanottoja. Tähän kuvaan sopii huonosti se, että epäselviä oikeuskysymyksiä ratkaistaan syyttäjien päätöksillä, joista saattaa myös muodostua ’oikeuskäytäntöä’, joka ei ole syntynyt tuomioistuimessa, kuten perustuslain tuomiovallan käyttöä koskevien normien mukaan pitäisi”.[142]

Erityisesti tietotekniikkarikosten ollessa kysymyksessä voi hyvin kuvitella olevan olemassa keskimääräistä enemmän tarvetta tietoiseen ennakkopäätösten hakemiseen (ylemmistä) tuomioistuimista, sillä sovellettavat säännökset ovat toisaalta sen verran uusia, että niitä koskeva soveltamiskäytäntö on kovin vähäistä, ja toisaalta sen verran vanhoja teknisen kehityksen huimaan nopeuteen nähden, että niiden sanamuoto ei kaikilta osin enää yksiselitteisesti ole sovitettavissa yhteen ympäröivän todellisuuden kanssa. Erityisesti viimeksi mainitussa tilanteessa on ”ei näyttöä” tai ”ei rikos” -perusteista päätöstä syyttämättä

---

[141] Jonkka, s. 736 s., Jareborg, Brotten I, s. 96. Ks. Myös Lahti, LM 96, s. 935.

[142] Jääskeläinen, s. 255. – On kuitenkin muistettava, että syyttäjille on tosiasiassa siirretty huomattava määrä aikaisemmin tuomioistuimille kuulunutta valtaa, kun syyttäjät rangaistusmääräysmenettelyssä ratkaisevat lopullisesti moninkertaisen määrän asioita tuomioistuinten ratkaisemiin verrattuina. Voidaan tietysti väittää, että ne kannanotot ja linjaukset, joita syyttäjät ratkaisukäytännössään tekevät, koskevat vain vähäpätöisiä asioita, mutta tosiasia on kuitenkin esimerkiksi se, että RL 10 luvun menettämisseuraamusta koskevia säännöksiä sovelletaan rangaistusmääräysmenettelyssä huomattavan usein ja että tämä soveltaminen varmasti luo tiettyä käytäntöä.

jättämisestä usein pidettävä varsin epätyydyttävänä ratkaisuna, selvästi syytteen hylkäävää hovioikeuden tuomiota huonompana.

1.2.3.4 Tietojenkäsittelyrauha tietotekniikkarikosten suojeluobjektina

Tietotekniikkarikoksen määritelmän mukaisilla teoilla on havaittavissa yksi yhteinen nimittäjä: koska niiden kohteena, välikappaleena tai tekoympäristönä on tietojärjestelmä siihen kuuluvine laitteineen, ne kaikki loukkaavat luonteeltaan jossain määrin kotirauhaan rinnastettavissa olevaa niin sanottua *tietojenkäsittelyrauhaa,* josta on käytetty myös nimitystä *pax computationis.* Muita, suunnilleen samaa tarkoittavia termejä ovat esimerkiksi *luottamus tietotekniikkaan* tai *tietojenkäsittelyn luottamuksellisuus.*[143]

Suomen lainsäädäntö ei nimenomaisesti tunne tietojenkäsittelyrauhan käsitettä, mutta sitä on käytetty lainvalmistelussa: ensimmäisen kerran rikoslain kokonaisuudistuksen toisen vaiheen yhteydessä tietomurtoa koskevan säännöksen perusteluissa,[144] joissa on todettu säännöksellä pyrittävän turvaamaan toisaalta niin sanottua *tietokonerauhaa* eli tietojärjestelmiä ulkopuolista tunkeutumista vastaan ja toisaalta tietokonetyöskentelyn yksityisyyttä sellaista ulkopuolista tarkkailua vastaan, jossa ei ole kysymys salakuuntelusta tai -katselusta, ja toisen kerran niin kutsutun tietokoneviruksen valmistamisen ja levittämisen kriminalisoimista koskevassa hallituksen esityksessä,[145] jossa käsitettä on selvitetty perusteellisemmin.

Esityksessä todetaan seuraavaa:

> Tietoturvallisuus on tavoitetila, jossa tiedot, järjestelmät ja palvelut saavat asianmukaista suojaa niin normaali- kuin poikkeusoloissakin lainsäädännön ja muiden toimenpiteiden avulla niiden luottamuksellisuuteen, eheyteen ja käytettävyyteen kohdistuvia laitteisto- ja ohjelmistovioista, luonnontapahtumista tai tahallisista, tuottamuksellisista ja tapaturmaisista inhimillisistä teoista johtuvia uhkia ja vahinkoja vastaan.
>
> Tietotekniikkarikosten suojeluobjekti on ilmaistu esimerkiksi Alankomaiden lainsäädännössä termillä ”tietojenkäsittelyrauha” ja oikeuskirjallisuudessa esiintyy myös latinankielinen ”Pax Computationis”, joka kuvaa yhdellä ilmaisulla sen, mitä esimerkiksi Yhdistyneiden Kansakuntien tietotekniikkarikoskäsikirja, OECD:n, Euroopan neuvoston ja Suomen valtioneuvoston tietoturvallisuuspäätökset selittävät tarkemmin kolmen peruskäsitteen eli luottamuksellisuuden (Confidentiality), eheyden (Integrity) ja käytettävyyden (Availability) avulla.[146]

---

[143] Tietojenkäsittelyrauhan käsite esiintyy mm. EN:n vuoden 1989 raportissa (s. 38) muodossa *computer domicile* (tietomurtoa koskevan suosituksen ensisijaiseksi suojeluobjektiksi mainitaan ”the inviolability of the computer domicile”).

[144] HE 94/1993.

[145] HE 4/1999.

[146] Ks. VN:n tietoturvallisuuspäätös ja OECD:n tietoturvallisuusasiakirjat. Vrt. myös EY:n neuvoston tietoturvallisuuspäätös.

Tällä tavoin määriteltynä tietojenkäsittelyrauhan käsite on mielestäni hyvin pitkälti rinnastettavissa kotirauhaan, joka rinnastus ehkä osaltaan myös konkretisoi käsitettä. Kotirauhan suojaa nauttiva alue ja tietojenkäsittelytapahtuma on suojattu ulkopuolista puuttumista vastaan. Asukas tai käyttäjä voi itse luoda teknisiä suojamekanismeja (lukot, salasanat), jotka tietyissä kriittisissä tilanteissa erikseen valtuutetuilla henkilöillä on lupa ohittaa (asunto-osakeyhtiön isännöitsijä, järjestelmän pääkäyttäjä). Lainsäätäjä on omalta osaltaan pyrkinyt turvaamaan näitä oikeushyviä kriminalisoimalla kotirauhan rikkomisen samoin kuin tietomurron, luvattoman käytön, tietovahingon aiheuttamisen, tietojenkäsittelypetoksen, väärennyksen ja vaaran aiheuttamisen tietojenkäsittelylle, jotka kaikki viimeksi mainitut ovat tietojenkäsittelyrauhan rikkomista.

Tietoturvallisuus käsitteenä on huomattavasti tietojenkäsittelyrauhaa laajempi ja sitä toteutetaan moniin eri oikeudenaloihin – erityisesti hallinto- ja siviilioikeuteen – kuuluvalla sääntelyllä.[147] Kaikki tietoturvallisuuden loukkauksia koskevat rangaistussäännökset eivät suinkaan turvaa tietojenkäsittelyrauhaa. Tietoturvallisuusrikokset voidaan jakaa kolmeen luokkaan:[148] (1) rikokset, joiden tunnusmerkistöön kuuluu tietoturvallisuusvelvollisuuden laiminlyönti, (2) rikokset, jotka kohdistuvat tieto- ja viestintäjärjestelmiin tai itse tietoon, sekä (3) rikokset, joiden tunnusmerkistöön kuuluu informaation oikeudeton julkistaminen tai levittäminen.

Näistä kategorioista keskimmäinen, tieto- ja viestintäjärjestelmiin tai tietoon kohdistuvat rikokset, käsittää tämän tutkimuksen kohteena olevat tietojenkäsittelyrauhaa loukkaavat tietotekniikkarikokset.

Vaikka tietojenkäsittelyrauha siis on vain yksi tietoturvallisuuden useista ilmenemismuodoista, on sitä perusteltua lähestyä tietojen luottamuksellisuuden, eheyden ja käytettävyyden käsitteiden avulla, kunhan muistetaan pitää näiden käsitteiden ulottuvuus vain rikosoikeudellisena.

Valtioneuvoston periaatepäätöksessä tietoturvallisuuden kehittämisestä valtionhallinnossa määritellään edellä mainitut kolme peruskäsitettä seuraavasti:[149]

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

---

147 Ks. esim. Saarenpää ym., s. 3.
148 Saarenpää ym., s. LIX.
149 Ks. myös Saarenpää ym., s. 56 ss.

Hyvin samantapaiset määritelmät ovat luettavissa myös OECD:n tietoturvallisuusperiaatteisiin liittyvästä perustelumuistiosta:

> Security of information systems is the protection of availability, confidentiality and integrity. Availability is the characteristic of information systems being accessible and usable on a timely basis in the required manner. Confidentiality is the characteristic of data and information being disclosed only to authorised persons, entities and processes at authorised times and in the authorised manner. Integrity is the characteristic of data and information being accurate and complete and the preservation of accuracy and completeness. The relative priority and significance of availability, confidentiality and integrity vary according to the information system.

Erityyppiset teot kohdistuvat tietojenkäsittelyrauhan eri osa-alueisiin eri tavoin. Tietomurto vaarantaa erityisesti tietojenkäsittelyn luottamuksellisuuden: se, että joku on päässyt tunkeutumaan järjestelmään, osoittaa, että järjestelmän suojauksessa on ollut aukko, ja jättää epävarmuuden siitä, onko järjestelmä murtautumisen jälkeen enää ennallaan ja ovatko järjestelmän tiedot säilyttäneet luottamuksellisuutensa.[150] Luvaton käyttö kohdistuu samoin ensisijaisesti luottamuksellisuuteen mutta loukkaa sen ohessa käytettävyyttä: siltä osin kuin järjestelmän sisältämät tiedot ovat rikoksentekijän käytössä, ei oikea omistaja tai laillinen haltija yleensä voi niitä käyttää.

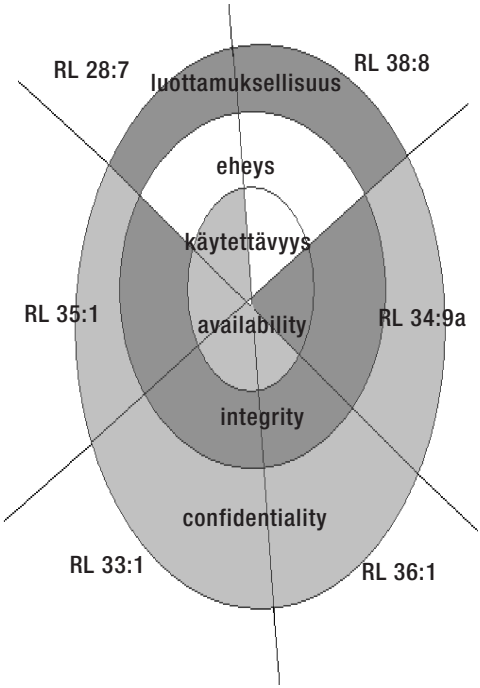
Petos, väärennys ja vahingonteko puolestaan kohdistuvat ensisijaisesti tietojen eheyteen: tekojen tunnusmerkistöön kuuluu tavalla tai toisella (tai tarkoituksessa tai toisessa) datan muuttaminen, jolloin sen eheys kärsii. Samalla nämä teot kuitenkin loukkaavat myös tietojen luottamuksellisuutta ja käytettävyyttä.

Vaaran aiheuttaminen tietojenkäsittelylle kohdistuu ennen muuta niin tietojen eheyteen kuin käytettävyyteenkin: vahingollisen ohjelman leviäminen saattaa tuhota järjestelmän sisältämät tiedot ja estää järjestelmän käyttämisen siihen oikeutetulta. Koska se loukkaa näiden ohella myös tietojen luottamuksellisuutta, on se mainituista rikoksista laajimmin tietojenkäsittelyrauhaa vaarantava.

Seuraava koulutuskäyttöön kehittelemäni kuvio havainnollistaa sitä, miten eräät rikostyypit loukkaavat tietojenkäsittelyrauhan eri osa-alueita. Siinä tietojenkäsittelyrauhaa kuvaa ympyränomainen kuvio, joka on jaettu luottamuksellisuutta, eheyttä ja käytettävyyttä kuvaaviin kehiin sekä eräitä tietotekniikkarikoksia vastaaviin sektoreihin. Mitä tummempaa väriä yksittäisen rikoslajin sektoriin jäävässä kehän osassa on käytetty, sen vakavammasta loukkauksen asteesta on kysymys.

---

[150] Asia voidaan toki nähdä paljon yksinkertaisemminkin. Esimerkiksi Küchler (s. 20) toteaa käsitellessään Ruotsin Brottsbalkenin 4 luvun 9 c §:ää yksiselitteisesti, että ”skyddsobjektet i den straffrättsliga bestämmelsen om dataintrång är upptagning för ADB”. Näinkin kysymystä voidaan toki lähestyä, mutta tällöin tietotekniikkarikos-käsitteelle on vaikeampi löytää yhteismitallisuutta.



Tietojenkäsittelyrauhan käsitteen olemassaolon hyväksymisestä seuraa, että tietotekniikkarikoksia koskevilla rangaistussäännöksillä voidaan katsoa suojeltavan yhtä yhteistä oikeushyvää, mikä puolestaan käsitykseni mukaan oikeuttaa tarkastelemaan tietotekniikkarikoksia yhtenä erillisenä ja itsenäisenä rikoskategoriana.

Vento on väitöskirjassaan käsitellyt laajasti suojeluobjektia rikosoikeudessa.[151] Tässä yhteydessä ei ole syytä lähteä yksityiskohtaisesti tutkimaan suojeluobjektin ja oikeushyvän käsitteiden sisällön muotoutumista; tietotekniikkarikoksia ajatellen voidaan hyvin yhtyä siihen *Vennon* näkemykseen, että oikeushyvän käsitteen sisältö ja rajat eivät määräydy pelkästään lain perusteella vaan myös lain käytännön sovellutuksista sosiaalisessa todellisuudessa. Oikeushyvän määrittely tapahtuu kahdella tasolla, toisaalta laissa ja toisaalta todellisuudessa ja sen tulkinnan kautta.[152]

Vaikka siis tietotekniikkarikoksia koskevilla säännöksillä ei *nimenomaisesti* mainiten suojata tietojenkäsittelyrauhaa, *käytännössä* myös tämä oikeushyvä saa suojaa – ja yksinomaan juuri näiden säännösten kautta.

---

[151] Vento, s. 104 ss.
[152] Vento, s. 119.

Edellä olen todennut tietotekniikkarikoksia koskevien kriminalisointien ensisijaisten suojeluobjektien olevan erilaisia sen mukaan, minkä perinteisen rikostunnusmerkistön laajennuksesta on kysymys. Tietojenkäsittelyrauha suojeluobjektina on siis selkeästi toissijainen *lukuun ottamatta* tietomurtoa ja vaaran aiheuttamista tietojenkäsittelylle eikä sille muita kuin näitä säännöksiä koskevissa lain esitöissä ole annettu olennaista merkitystä. Ajatus tällaisesta oikeushyvästä on kuitenkin jo paljon aikaisemminkin – muun muassa Euroopan neuvoston asiantuntijakomitean vähemmistössä – noussut esiin ja sillä voi jäljempänä havaittavin tavoin olla käytännöllistäkin merkitystä eräiden rajanveto-ongelmien ratkaisemisessa.[153]

Kun jäljempänä käsittelen yksittäisiä tietotekniikkarikoksia koskevia kriminalisointeja, teen sen käyttämällä hyväksi tässä omaksumaani tietojenkäsittelyrauhan ja sen eri osa-alueiden käsitettä. Ryhmittely osan II luvuissa 2–4 perustuu toisaalta siihen, mitä osa-aluetta kulloinenkin teko ensisijaisesti loukkaa, toisaalta siihen, miten voimakasta loukkaaminen on.

1.2.3.5 Euroopan neuvoston suositus Suomen lainsäädännön perustana

Tietotekniikkarikosten jako edellä kuvatuin tavoin kolmeen ryhmään – data- ja informaatiorikoksiin, immateriaalioikeuksien loukkauksiin ja yksityisyyden suojan loukkauksiin – perustuu paljolti Euroopan neuvoston raporttiin ja siihen liittyvään kriminalisointisuositukseen, joka on ollut lainsäätäjän ohjeena paitsi Suomessa myös useassa muussa maassa tietotekniikkarikoksia koskevia kriminalisointeja kehiteltäessä. On muistettava, että raportti ja suositus ovat jo runsaasti yli kymmenen vuoden ikäisiä ja että nykyään eletään aivan toisenlaisessa tietoteknisessä ympäristössä kuin 1980-luvulla. Siitä huolimatta tietotekniikkarikoksen peruskaava on säilynyt ennallaan – oikeudeton tunkeutuminen järjestelmään ja sitä mahdollisesti seuraavat muut oikeudettomat dataan kohdistuvat toimet – joten Euroopan neuvostossa raporttia ja suositusta laadittaessa tehdyllä mittavalla selvitystyöllä on yhä edelleen suuri merkitys.

Suositus, jota käsitellään yksityiskohtaisesti jäljempänä, käsittää kaksi listaa: minimilistan (minimum list of offences necessary for a uniform criminal policy on legislation concerning computer-related crime), johon otettujen tekojen kriminalisoinnin tarpeesta valtiot olivat yksimielisiä, ja valinnaislistan (optional list), jossa mainittujen tekojen kriminalisoimista pidettiin ainakin harkinnan

---

[153] Vento esittelee (s. 107 ss.) eräitä näkemyksiä oikeushyvän käsitteen merkityksestä ja sisällöstä ottamatta kuitenkaan itse kysymykseen kantaa. Vento mainitsee *Jescheckin* käsityksen, jonka mukaan oikeushyvä tarkoittaa eri asiaa kuin *ratio legis,* vaikka oikeushyvä onkin tunnusmerkistön tulkinnassa ensisijainen lähde. Oikeushyvä on itsenäinen käsite, jolla on reaalinen sisältö. Muutoin ei olisi mahdollista, että oikeushyvä voisi olla tunnusmerkistön sisällön tulkinta-apuväline tai rangaistussäännöksen rajoittaja.

arvoisena mutta joiden osalta ei saavutettu yksimielisyyttä.[154] Minimilistan tekoja ovat (1) tietojenkäsittelypetos (computer fraud), (2) tietotekniikkavääärennys (computer forgery), (3) datan tai ohjelmiston vahingoittaminen (damage to computer data or computer programmes), (4) tietotekniikkasabotaasi (computer sabotage), (5) luvaton järjestelmään tunkeutuminen (unauthorised access), (6) luvaton viestin sieppaaminen (unauthorised interception), (7) luvaton kappaleiden valmistaminen suojatusta tietokoneohjelmasta (unauthorised reproduction of a protected computer programme) ja (8) luvaton kappaleiden valmistaminen integroidun piirin piirimallista (unauthorised reproduction of a topography). Valinnaislistan tekoja ovat (9) datan tai ohjelmiston muuttaminen (alteration of computer data or computer programmes), (10) tietokonevakoilu (computer espionage), (11) tietokoneen luvaton käyttö (unauthorised use of a computer) ja (12) suojatun tietokoneohjelman luvaton käyttö (unauthorised use of a protected computer programme).

Suosituksen tarkoittamista teoista ovat data- ja informaatiorikoksia ainakin useimmissa tapauksissa tietojenkäsittelypetos ja -väärennys, datan tai ohjelmiston vahingoittaminen, tietotekniikkasabotaasi, luvaton järjestelmään tunkeutuminen, luvaton viestin sieppaaminen, datan tai ohjelmiston muuttaminen, tietokonevakoilu sekä tietokoneen luvaton käyttö. Luvattomat kappaleiden valmistamiset suojatusta tietokoneohjelmasta ja integroidun piirin piirimallista samoin kuin suojatun tietokoneohjelman luvaton käyttö kuuluvat immateriaalioikeuksien loukkausten ryhmään, kun taas yksityisyyden suojaa voidaan loukata luvattomalla järjestelmään tunkeutumisella ja osin myös tietokonevakoilulla.

---

[154] Ks. EN:n raportti 89, s. 80 s.

2 Kansainvälisestä yhteistyöstä ja ulkomaisesta sääntelystä

2.1 KANSAINVÄLISESTÄ YHTEISTYÖSTÄ JA TUTKIMUKSESTA

2.1.1 Yleistä

Johdantojaksossa on jo useaan kertaan viitattu tietotekniikkarikosten transnationaaliseen luonteeseen. Itse asiassa tietotekniikkarikosten vaikutukset saattavat ulottua usean valtion alueelle selvästi helpommin kuin minkään muun rikoslajin kohdalla. Valtioiden rajat ovat televerkkojen välityksin ylitettävissä vaivattomasti ja nopeasti. Lähes jokapäiväisiä ovat nykyään sellaiset uutiset, jollainen oli esimerkiksi luettavissa Helsingin Sanomista 18.2.2004:

> Hakkeri hyökkäsi taannoin Yhdysvaltain Etelämantereella olevan tutkimusaseman tietokoneen kimppuun. Liittovaltion poliisi FBI jäljitti hyökkäyksen Pittsburghin esikaupungissa Yhdysvalloissa olevaan tietokoneeseen. Varsinaiset tekijät löydettiin kuitenkin Romanian pääkaupungista Bukarestista.

Niin kuin tämäkin tapahtuma osoittaa, tietotekniikkarikoksen tekijän tosiasiallinen toiminta jonkin valtion alueella saattaa lähes välittömästi aiheuttaa toisessa valtiossa, jopa toisella mantereella ilmenevän seurauksen. Välttämättä seurauksen ei tarvitse ilmetä vain *yhdessä* toisessa maassa tai *yhdellä* toisella mantereella: mahdollisia seurauksen ilmenemispaikkoja voi periaatteessa olla yhtä monta kuin Internetiin yhteydessä olevia työasemia. Näin ollen osa niistä rikosoikeudellisista keinoista, joilla pyritään ehkäisemään ja kontrolloimaan tietotekniikkarikollisuutta, kuuluu tyypillisesti *kansainvälisen rikosoikeuden* alaan.

Lahden mukaan kansainvälinen rikosoikeus on oikeudenalajaottelussa luettavissa osaksi niin hyvin kansainvälistä oikeutta kuin (kansallista, valtionsisäistä) rikosoikeutta (jolloin rikosoikeudella ymmärretään niin aineellisten kuin menettelyllistenkin oikeusnormien muodostamaa kokonaisuutta, rikos- ja rikosprosessioikeutta).[155]

Tietotekniikkarikokset eivät ole ennen Euroopan neuvoston tietoverkkorikosyleissopimusta olleet sellaisia kansainvälisiä rikoksia (eli ns. kansainoikeus- tai maailmanrikoksia),[156] joiden ehkäiseminen ja kontrolloiminen perus-

---

[155] Lahti, Kansainvälistyvä rikosoikeus, s. 186 s.

[156] Tällaisia rikoksia esimerkiksi Bassiouni (s. 40) toteaa olevan 24 eri kategoriaa.

tuisi valtioiden välisiin kahden- tai monenvälisiin sopimuksiin tai tapahtuisi ylivaltiollisten orgaanien – esimerkiksi kansainvälisen rikostuomioistuimen – toimesta. Tällaisten kansainvälisoikeudellisesti velvoittavien sopimusten on sanottu olevan kansainvälisen kriminaalipolitiikan *kovaa arsenaalia.*[157]

Kun tällaiseen kovaan arsenaaliin on turvauduttu esimerkiksi taistelussa huumausainerikollisuutta vastaan, on tietotekniikkarikollisuutta torjuttaessa aikaisemmin tyydytty niin sanottuun *pehmeään arsenaaliin.*[158] Niin Yhdistyneiden Kansakuntien piirissä kuin alueellisissa elimissäkin hyväksytyt julistukset ja suositukset eivät tosin ole olleet kansainvälisoikeudellisesti valtioita velvoittavia, mutta niillä on nähtävä olevan moraalista ja poliittista sitovuutta erityisesti niiden puolesta äänestäneiden valtioiden kohdalla.

On ymmärrettävää, että tällainen pehmeä arsenaali soveltuu – ainakin monenvälisissä suhteissa – kovaa paremmin sisällöltään niinkin epämääräisen rikollisuuslajin torjuntaan kuin tietotekniikkarikollisuus on. Kun tietotekniikkarikoksiksi luokiteltavat teot useimmiten ovat jonkin ns. perinteisen rikoksen modifikaatioita, saa niitä koskeva valtionsisäinen sääntely sisältönsä paljolti kansallisen rikoslain muusta sisällöstä ja on niin muodoin kansallisen perinteen sitomaa. Tällaisessa tilanteessa on vaikea kuvitella, että esimerkiksi tietoteknisen väärennyksen kriminalisoimista tarkoittavassa monenkeskisessä valtiosopimuksessa kaikkia sen osapuolia tyydyttävällä tavalla voitaisiin yksiselitteisesti luonnehtia se menettely, joka sopijapuolten tulisi säätää rangaistavaksi (ja tällaiset vaikeudet nousivatkin monessa kohdin selvästi esille esimerkiksi Euroopan neuvoston tietoverkkorikosyleissopimusta neuvoteltaessa).

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

Tietotekniikkarikoksia koskevan kansainvälisen yhteistyön tärkeimmäksi tavoitteeksi on noussut eri valtioissa voimassa olevan kansallisen rikoslainsäädännön saattaminen mahdollisimman yhdenmukaiseksi niin, että samantapaiset menettelyt olisivat kriminalisoituja. Näin voitaisiin minimoida se mahdollisuus, että jostain valtiosta muodostuisi tietotekniikkarikosten tekijöille sellainen paratiisi *(data paradise)* tai suojasatama *(computer crime haven),* jossa rikollista toimintaa olisi mahdollista harjoittaa kaikessa rauhassa ilman pelkoa asianomaisen valtion viranomaisten puuttumisesta toimintaan.[159] Tällaisten

---

[157] Ks. Lehtimaja, LM 86, s. 209 ja Lahti, Kansainvälistyvä rikosoikeus, s. 189 ss.

[158] Lahti, Kansainvälistyvä rikosoikeus, s. 191 s.

[159] Ks. esim. UN Manual, kohta 244. Lehtimaja (LM 86, s. 212) puhuu *kriminaalikeitaista* tai *valkamista* eli maista, joista käsin voidaan laillisesti harjoittaa muissa maissa kriminalisoitua toimintaa välittömästi muihin maihin ulottuvin vaikutuksin, ja mainitsee esimerkkeinä verokeitaat ja tietokeitaat.

dataparatiisien kehittyminen tulee teknisesti yhä helpommaksi maailmanlaajuisten tietoverkkojen kehittyessä ja tiedonsiirtotekniikoiden parantuessa ja niitä on mahdollista perustaa jopa millekään valtiolle kuulumattomille alueille. Yhä useammissa valtioissa, joista joissakin rikosoikeudellisen lainsäädännön taso saattaa olla hyvin vaatimaton, on olemassa asian- ja ajanmukaiset tekniset edellytykset rikollisen toiminnan harjoittamiselle.

Lainsäädäntöjen harmonisointi saattaa olla myös edellytyksenä keskinäisen oikeusavun antamiselle tai rikoksentekijän luovuttamiselle; usein toimenpiteen onnistuminen vaatii menettelyn kriminalisoimista kummassakin menettelyn osapuolena olevassa valtiossa.[160]

Paitsi aineellisen rikosoikeuden harmonisointi on kansainvälisen yhteistyön kohteena ollut myös prosessuaalisten säännösten yhdenmukaistaminen. Tietotekniikkarikosten tutkinta ja viime vuosina yhä merkittävämpään asemaan tulleen elektronisen todistusaineiston kokoaminen esimerkiksi edellyttävät sellaisten pakkokeinojen käyttämistä, joita koskevat menettelymuodot ovat vain vaivoin sovitettavissa perinteistä etsintää tai takavarikkoa koskeviin säännöksiin. Lisäksi on viime aikoina ilmennyt tarvetta aivan uudenlaisillekin pakkokeinoille, sillä esimerkiksi todisteena relevantti tietojärjestelmään tallennettu data on tarpeen vaatiessa helppoa hävittää erittäin nopeasti ja näin ollen mahdollisuus vieraassa valtiossa olevan datan nopean säilyttämisen järjestämiseen voisi olla hyvin käyttökelpoinen.

Tietotekniikkarikoksiin liittyvää tutkimus- ja selvitystyötä on tehty useissa kansainvälisissä järjestöissä. Seuraavassa tarkastellaan lähemmin Taloudellisen yhteistyön ja kehityksen järjestön OECD:n, Euroopan neuvoston, Yhdistyneiden Kansakuntien, Kansainvälisen rikosoikeusyhdistyksen AIDP:n ja Euroopan unionin toimintaa.[161] Tarkastelutapa on suurelta osin kuvaileva, mutta osan II luvuissa 2–4 tullaan tarpeellisilta osin tarkemmin palaamaan aineellista rikosoikeutta koskeviin suositusten ja päätöslauselmien kohtiin.

Saattaa vaikuttaa siltä, että tässä jaksossa tarpeettomasti toistetaan samoja asioita. En pidä tällaista toistoa kuitenkaan tarpeettomana: järjestöjen työssä on nähtävissä selvä kehitys suunnan ollessa toisaalta yleisistä periaatteellisista

---

[160] Ks. esim. AIDP:n päätöslauselma kohta 22.

[161] Mainittujen järjestöjen lisäksi on tietotekniikkarikoksia käsitelty mm. Kansainvälisessä kauppakamarissa ICC:ssä (Computer-related Crime and Criminal Law: an International Business View 1988) ja Kansainvälisessä rikospoliisijärjestössä Interpolissa, jossa vuodesta 1990 on toiminut erityinen tietoteknisessä ympäristössä tehtyjä rikoksia koskevia kysymyksiä käsittelevä työryhmä. Kansainvälisen syyttäjäyhdistyksen (International Association of Prosecutors, IAP) vuoden 1999 maailmankongressissa Pekingissä oli ”Fraud in Internet” yhtenä pääteemana. Teollisuusmaiden ns. G8-ryhmä on asettanut High-Tech Crimeä tutkivan työryhmän, jonka työn tuloksena on jo mm. luotu ns. 24/7-verkosto eli 24 tuntia vuorokaudessa, seitsemän päivää viikossa avoinna olevien kontaktipisteiden verkosto kansainvälisen oikeusavun saamisen helpottamiseksi.

lausumista kohti yksityiskohtaisempia kannanottoja ja toisaalta koko tietotekniikkarikollisuusongelman osalta ylipäänsä kansallisesta, valtionsisäisestä ilmiöstä yhä selkeämmin kohti näkemystä koko kansainvälisen oikeusyhteisön toimenpiteitä edellyttävästä uhkakuvasta. Järjestöjen työn kuvauksessa piirtyy samalla kuva tietotekniikkarikosoikeuden lyhyestä historiasta alkaen sellaisen 30 vuoden takaisen rikollisen menettelyn käsittelystä, jonka keskipisteenä oli yleensä vain yksittäinen tietokone, ja päätyen – toistaiseksi – uuden vuosituhannen alun verkkorikollisuuteen, jossa yksi rikollinen teko saattaa koskettaa tuhansia työasemia kymmenissä valtioissa.

Järjestöjen kannanottoihin kuuluu myös paljon sellaista, joka ei välittömästi liity tämän tutkimuksen aihepiiriin mutta on silti syytä tuoda esille, jotta lukijalle muodostuisi kokonaiskuva niistä tavoitteista, jotka kansainvälisessä yhteistyössä on havaittu tärkeiksi; prosessioikeudelliset kysymykset samoin kuin kansainväliseen rikosoikeuteen kuuluvat ongelmat ovat nekin tietotekniikkarikosten kohdalla hyvin spesifisiä ja liittyvät läheisesti aineelliseen rikosoikeuteen. Mikäli tällaiset kannanotot kaipaavat kommentteja Suomen oikeuden kannalta, esitän ne tässä luvussa. Lisäksi käsittelen lyhyesti Euroopan neuvoston tietoverkkorikosyleissopimuksen rikosprosessioikeuden alaan kuuluvia määräyksiä niiden implementoimisen kannalta *de lege ferenda* -jaksossa.

2.1.2 Taloudellisen yhteistyön ja kehityksen järjestö OECD

OECD:n toimenkuvassa ei rikosoikeudellisilla kysymyksillä ole mikään erityisen keskeinen osuus, joskin aika ajoin järjestö on tuottanut lähes puhtaasti rikosoikeudellisiksi luonnehdittavia instrumentteja.[162] On kuitenkin selvää, että tietotekniikan merkitys maailmantaloudessa on suuri, niin myönteisessä kuin kielteisessäkin mielessä. Tämä oli jo nähtävissä 1980-luvun alkupuolella (joskaan tulevien vuosien kehitystä ei ehkä osattu oikealla tavalla ennakoida) ja niinpä OECD:n tieto- ja viestintäpoliittinen komitea ICCP (Committee for Information, Computer and Communications Policy) asetti vuonna 1984 *ad hoc* -asiantuntijatyöryhmän tutkimaan mahdollisuuksia harmonisoida jäsenmaiden rikoslainsäädäntöä tietotekniikkarikosten alueella. Työryhmän laatima raportti julkaistiin vuonna 1986[163] ja on nimeltään ”Computer-related Crime: Analysis of Legal Policy”.

---

[162] Merkittävimpänä tällaisista instrumenteista voidaan pitää 15.2.1999 kansainvälisesti voimaan tullutta yleissopimusta kansainvälisissä liikesuhteissa tapahtuvan ulkomaalaiseen virkamieheen kohdistuvan lahjonnan torjumisesta.

[163] Työryhmässä olivat edustettuina Yhdysvallat, Itävalta, Belgia, Kanada, Tanska, Suomi (Lauri Lehtimaja), Ranska, Saksan Liittotasavalta, Italia, Alankomaat, Norja, Portugali, Ruotsi, Sveitsi ja Yhdistynyt kuningaskunta. Luettelo työryhmään kuuluneista henkilöistä on raportin liitteenä.

Raportti jakaantuu johdantoon, neljään kappaleeseen ja johtopäätösosaan. Johdannossa todetaan raportilla olevan kolme tarkoitusta: (1) helpottaa jäsenvaltioita vaihtamaan informaatiota omaksumistaan tavoista suhtautua tietotekniikkarikoksiin; (2) tarkastella yleistä kehitystä ja jäsenvaltioiden toimenpiteitä; sekä (3) yrittää saavuttaa yhteisymmärrys niin tietotekniikkarikoksesta itsestään käsitteenä kuin mahdollisuuksista puuttua siihen lainsäädännöllä.[164] Tietotekniikkarikoksen määritelmää ei raportissa ole yritettykään luoda.

Ensimmäinen kappale käsittelee tietotekniikkarikoksiin liittyvän lainsäädäntöpolitiikan päälinjoja (main lines of legislative policy in response to computer-related crime), toinen kappale sisältää analyysin tietotekniikkarikosten erityispiirteistä (analysis of the specific and unique aspects of computer-related crime), kolmas analyysin aineellisesta rikosoikeudesta ja ehdotuksia lainsäädäntöpolitiikaksi (analysis of substantive penal law and suggestions for legal policy) ja viimeisessä kappaleessa käsitellään tietotekniikkarikoksiin liittyviä kansainvälisiä näkökohtia (international aspects of computer-related crime).

Raportin ensimmäisessä kappaleessa jaotellaan jäsenvaltiot harjoittamansa lainsäädäntöpolitiikan perusteella kahteen pääryhmään:165 ensimmäiseen kuuluneissa valtioissa[166] ei tietotekniikkarikosten ole katsottu edellyttävän mitään erityisiä uusia toimenpiteitä eikä ole havaittu aiheelliseksi tehdä eroa toisaalta informaation ylipäänsä ja toisaalta tietoteknisen (computerised) informaation välillä. Tietokone on yksinkertaisesti katsottu sellaisen rikoksen tekovälineeksi, johon jo olemassa olevilla kriminalisoinneilla voidaan puuttua.

Toiseen ryhmään kuuluneissa valtioissa[167] sen sijaan on lainsäädännölliset toimenpiteet nähty aiheellisiksi; toisaalta joko niin, että voimassa olevan lain säännöksiä täydennetään vastaamaan uusia rikoksen tekomuotoja, tai toisaalta niin, että luodaan uusia tietotekniset vaatimukset huomioon ottavia kriminalisointeja. Molempia metodeja voidaan käyttää myös yhdessä.

Raportissa selvitetään, mikä on ollut tilanne kussakin jäsenvaltiossa; nämä tiedot ovat tällä hetkellä jo suurelta osin vanhentuneita.

Voidaan siis havaita, että oikeastaan tietotekniikkarikoksia koskevan kansainvälisen yhteistyön ensivaiheista alkaen on ilmennyt mielipiteiden jakautumista sen suhteen, miten tietotekniikkarikoksia tulisi lainsäädännössä käsitellä, ja että tuo jakautuminen juontaa juurensa valtioiden lainsäädäntökäytännöstä.

---

[164] Ks. OECD:n raportti s. 7: ”It aims: a) To make it easier for Member countries to exchange information about how they are approaching computer-related crime; b) To observe the main evolution and trends of measures taken by Member countries in approaching computer-related crime; c) To try to reach a common understanding both of computer-related crime itself and how the law can deal with it.”

[165] OECD:n raportti s. 12 s.

[166] Näitä ovat raportin valmistuessa olleet Belgia, Islanti ja Japani.

[167] Australia, Itävalta, Kanada, Tanska, Suomi, Ranska, Saksan Liittotasavalta, Kreikka, Italia, Alankomaat, Norja, Portugali, Ruotsi, Sveitsi, Yhdistynyt kuningaskunta ja Yhdysvallat.

Toisen kappaleen analyysi keskittyy kolmeen kysymykseen: (1) muuttavatko tietokoneet siinä määrin sitä teknologista ja sosiologista ympäristöä, jossa niitä otetaan käyttöön, että uudet säännökset tai jopa uusi lainsäädäntö on välttämätöntä; (2) mitä sellaisia erityisiä kysymyksiä uuden teknologian käyttöönoton myötä on noussut esille, joita voimassa olevan lain säännökset eivät ole säännelleet tai eivät voi säännellä; sekä (3) mille intresseille on annettava ensisijaisesti suojaa havaittuja lainsäädännöllisiä aukkoja täytettäessä ja millaisia sosiaalisia seurauksia tässä tarkoituksessa tehtävillä päätöksillä tulevaisuudessa saattaa olla.[168]

Kysymyksenasettelua nyt tarkasteltaessa voidaan mainiosti havaita, millainen muutos runsaan viidentoista vuoden aikana on tapahtunut. Nykyään käytävän keskustelun kannalta mainitut kysymykset ovat käyneet paljolti merkityksettömiksi: tietotekniikan kehitys on kymmenessä vuodessa ollut niin nopeaa, että uuden lainsäädännön tarpeellisuutta ei aseteta kysymyksenalaiseksi. Lainsäädännöllisiä aukkoja toki syntyy jatkuvasti ja jatkuvasti saattaa ilmetä myös uusia suojaa kaipaavia intressejä, joten tältä osin kysymyksenasetteluilla on yhä relevanssia.

Raportin kolmannen kappaleen analyysissa tarkastellaan lähemmin tietotekniikkarikostyyppejä ja niiden suhdetta perinteiseen rikosoikeudelliseen sääntelyyn. Tarkastelun kohteena ovat tietojenkäsittelypetos (fraud by computer manipulation),[169] tietokonevakoilu ja tietokoneohjelmien tekijänoikeuksiin kohdistuvat loukkaukset (computer espionage and programme piracy),[170] tietokone-sabotaasi (computer sabotage),[171] tietokoneen luvaton käyttö (unauthorised use of computers)[172] ja luvaton tunkeutuminen tietojärjestelmään eli ns. tietomurto (unauthorised access: protecting the integrity of computer systems).[173]

Kunkin rikostyypin kohdalla käsitellään perinteisen lainsäädännön sovellettavuuteen liittyviä ongelmia sekä eri jäsenvaltiossa mahdollisesti jo voimassa olevaa tai suunniteltua lainsäädäntöä. Lisäksi esitetään ehdotuksia lainsäädäntöpolitiikaksi, ja näiden ehdotusten perusteella lopuksi suositus siitä, mitä menettelyjä jäsenvaltioiden tulisi pyrkiä kriminalisoimaan.[174]

---

168 Ks. OECD:n raportti s. 23 ss.
169 OECD:n raportti s. 30 ss.
170 OECD:n raportti s. 40 ss.
171 OECD:n raportti s. 54 ss.
172 OECD:n raportti s. 56 ss.
173 OECD:n raportti s. 60 ss.
174 OECD:n raportti s. 64 s. "…it might be highly recommendable that all Member countries consider the following list of acts which could constitute a common denominator between the different approaches…"

Suosituksessa kuvataan viisi erilaista tekotapaa:[175]

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

Kolmessa ensimmäisessä suosituksessa rinnastetaan toisiinsa teko-objekteina *data* ja *ohjelmisto,* jolloin jälkimmäisellä tarkoitettaneen pelkkien yksittäisten ohjelmien ohella näiden muodostamaa kokonaisuutta, niin kutsuttua *softwarea.* Edellä olen määritellyt datan materiaaliseksi; ohjelmista ja ohjelmistosta puhuttaessa tarkoitetaan nähdäkseni jotakin tallenteeseen rinnastettavaa eli datan ja informaation muodostamaa kokonaisuutta. Näin ollen suositukset tarkoittavat paitsi dataan myös datan kantamaan informaatioon kohdistuvien tekojen kriminalisoimista.

Suositusteksti on jäljempänä käsiteltävään Euroopan neuvoston suositukseen verrattuna melko yksilöimätöntä; sellaisenaan suositus toisaalta on jokseenkin kattava eikä sen tarkoituksena ole ollutkaan muu kuin suuntaviivojen antaminen kansallisille lainsäätäjille. Joka tapauksessa OECD:n raportti suosituksineen on antanut hyvän pohjan Euroopan neuvostossa tehdylle työlle.

---

[175] OECD:n raportti s. 64 s.:

a) The input, alteration, erasure and/or suppression of computer data and/or computer programmes made wilfully with the intent to commit an illegal transfer of funds or of another thing of value;

b) The input, alteration, erasure and/or suppression of computer data and /or computer programmes made wilfully with the intent to commit a forgery;

c) The input, alteration, erasure and/or suppression of computer data and/or computer programmes, or other interference with computer systems, made wilfully with the intent to hinder the functioning of a computer and/or telecommunication system;

d) The infringement of the exclusive right of the owner of a protected computer programme with the intent to exploit commercially the programme and put it on the market;

e) The access to or interception of a computer and/or telecommunication system made knowingly and without the authorisation of the person responsible for the system, either (i) by infringement of security measures or (ii) for other dishonest or harmful intentions.

2.1.3 Euroopan neuvosto

2.1.3.1 PC-R-CC

Tietotekniikkarikoksia oli Euroopan neuvostossa käsitelty – tosin suppeasti – jo 1970-luvulta lähtien.[176] Osaksi OECD:n työn seurauksena asetettiin vuonna 1985 asiantuntijakomitea (Select Committee of Experts on Computer-related Crime, PC-R-CC),[177] joka aloitti työnsä samana vuonna ja päätti sen maaliskuussa 1989. Euroopan neuvoston kriminaalipoliittinen komitea (European Committee on Crime Problems, CDPC) hyväksyi PC-R-CC:n raportin ja siihen liittyvän suositusluonnoksen kesäkuussa 1989 ja saman vuoden joulukuussa neuvoston ministerikomitea hyväksyi suosituksen. Suositus ja raportti on julkaistu vuonna 1990 nimellä ”Recommendation No. R(89)9 on Computer-related Crime and Final Report of the European Committee on Crime Problems”.[178]

PC-R-CC:n toiminnasta

Asiantuntijakomitea aloitti työnsä tarkoituksenaan (a) tutkia tietotekniikkarikollisuuteen liittyviä ongelmia (i) analysoimalla aikaisempien tutkimusten valossa tietotekniikkarikollisuuden eri muotoja (petosta, vakoilua, sabotaasia ja väärinkäyttöä); (ii) tutkimalla, missä laajuudessa lainsäädäntöön tulisi sisällyttää tällaisen rikollisuuden uusia muotoja, samoin kuin kehittämällä suuntaviivoja kansallista sääntelyä, yhteistä terminologiaa, turvallisuutta ja ehkäisykeinoja varten; sekä (iii) tutkimalla, miten laajalti eurooppalaiset yleissopimukset rikosoikeuden alalla mahdollistavat taistelun uusimuotoista rikollisuutta vastaan, ja tarvittaessa esittämällä ehdotuksia voimassa olevien yleissopimusten täydentämiseksi, sekä (b) laatia raportti.[179]

Myöskään Euroopan neuvoston asiantuntijakomitea ei esittänyt tietotekniikkarikoksen määritelmää, vaan katsoi käsitteen saavan sisältönsä raporttiin liittyvässä suosituksessa kuvatuista tekotavoista.[180]

---

176 Ks. Lehtimaja, Atk-rikospolitiikasta s. 261.

177 Komiteassa olivat EN:n jäsenmaista edustettuina Itävalta, Tanska, Ranska, Saksan Liittotasavalta, Kreikka, Italia, Luxemburg, Alankomaat, Norja, Portugali, Espanja, Ruotsi ja Sveitsi. Tarkkailijoina komitean työhön osallistuivat Kanada, Suomi, Japani, Yhdysvallat, EY, OECD ja UNSDSRI. Tieteellisinä asiantuntijoina toimivat *B. de Schutter, P. Poelmans* ja *U. Sieber.* Henkilöt komiteassa olivat pitkälti samoja kuin OECD:n *ad hoc* -asiantuntijatyöryhmässä; Suomea edusti *Lauri Lehtimaja.* Ks. EN:n raportti 89, s. 5.

178 *Hans G. Nilsson,* joka toimi asiantuntijakomitean sihteerinä, on kertonut raportista artikkelissaan SvJT 90, ss. 142–149.

179 Ks. EN:n raportti 89, s. 5 s.

180 EN:n raportti 89, s. 9: ”Computer-related crime is, as the term is used by the Committee, simply then reduced to the offences enumerated and defined in the guidelines for national legislatures, which will leave it open for the various states to adapt this ’definition’ to its own legal system and historical traditions, taking into account the offences on the minimum and optional list.”

Raportti jakautuu viiteen osaan: (1) yleisiä kysymyksiä, (2) kriminalisointisuositukset kansallisille lainsäätäjille, (3) prosessuaalisia kysymyksiä, (4) kansainvälisiä näkökohtia ja (5) muita näkökohtia.

Lauri Lehtimaja on kuvannut komitean työskentelyä seuraavasti:

> Atk-rikoskomiteassa erottui jo heti alussa, puheenjohtajaa valittaessa, kaksi eri linjaa: oltiin eri mieltä siitä, heiluttaako häntä koiraa vai koira häntää. Ensimmäisen eli ns. *mystifiointilinjan* mukaan tietotekniikka oli kriminaalipolitiikassa määriteltävä kokonaan uudeksi elämänalueeksi ja yleinen luottamus tietotekniikkaan vastaavasti kokonaan uudeksi oikeushyväksi, joka vaati aivan omintakeisen sääntelynsä. Toisen eli ns. *perinteisen linjan* mukaan taas atk oli ainoastaan uusi ilmiö, joka oli luonut eräitä uusia rikoksentekomahdollisuuksia sekä uudenlaisen ympäristön monille perinteisille rikoksille. Siksi uuden tietotekniikan tosiasiat oli otettava huomioon nykyistä rikosoikeusjärjestelmää vuosi- ja peruskorjattaessa. Komitean puheenjohtajuudesta kilpailivat mystifiointilinjaa ajanut *Italia* sekä perinteistä linjaa puoltanut *Saksan Liittotasavalta.* Vaalin voitti jälkimmäinen, mistä ainakin pohjoismaat olivat tyytyväisiä.[181]

Perinteisen linjan saavuttama voitto näkyy itse raportissa ja siihen liittyvässä suosituksessa ja niiden kautta muun muassa Suomessa valitussa lainsäädäntötekniikassa.

Komitean työn tuloksessa on selkeästi nähtävissä yhtenä peruslähtökohtana olleen rikosoikeuden *toissijaisuuden periaate* (principle of subsidiarity). Raportin mukaan[182] se, että tietotekniikan käyttö synnyttää uusia suojaa kaipaavia intressejä, ei välttämättä edellytä, että suojaa annettaisiin rikosoikeuden keinoin tai että olisi välttämätöntä laatia uusia rikosoikeudellisia säännöksiä. Rikosoikeuden keinoja tulisi käyttää vasta muiden kysymykseen tulevien keinojen osoittauduttua riittämättömiksi. Rikoslain olisi oltava toissijainen toisaalta suhteessa ei-oikeudellisiin järjestelyihin, toisaalta suhteessa siviili- ja hallinto-oikeudelliseen sääntelyyn.

Ylikriminalisointien välttämiseksi raportissa nähdään tärkeäksi tutkia, mitkä oikeudelliset intressit – oikeushyvät – voivat vaarantua tietotekniikan väärinkäytön seurauksena.[183] Toisaalta on nähtävissä, että tietojenkäsittelyprosessia eri komponentteineen käytetään vain *välineenä* rikollisessa menettelyssä. Tällaisessa tapauksessa on tosin mahdollista, että välineen käyttäminen antaa rikokselle kokonaan uuden ulottuvuuden – esimerkiksi niin, ettei tekoa olisi ollut lainkaan mahdollista tehdä perinteisiä keinoja käyttämällä – mutta tosiasiassa kysymyksessä on vain uusi rikoksentekoväline.

---

[181] Lehtimaja, Atk-rikospolitiikasta, s. 263.
[182] EN:n raportti 89, s. 17 ss., ks. myös Lehtimaja, Atk-rikospolitiikasta, s. 264.
[183] EN:n raportti 89, s. 15 s.

Toisaalta kuitenkin tietokoneiden käytön lisääntyminen on luonut tilanteita, joissa täysin uudentyyppiset oikeushyvät vaativat oikeudellista suojaa. Tällaisina itsenäisinä suojaa vaativina intresseinä voidaan pitää esimerkiksi informaation oikeellisuutta ja tietojenkäsittelyjärjestelmän toiminnan luotettavuutta.[184]

Niin sanottuun perinteiseen rikollisuuteen verrattuna tietotekniikkarikollisuudella on kokonaan toisentyyppisiä kohteita; erityisesti silloin, kun teko kohdistuu tallennettuun tai siirrettävään dataan taikka tietojärjestelmiin. Tällaisia tekoja ovat esimerkiksi tallennetun datan hävittäminen tai muuttaminen, tietokonejärjestelmän toimintaan puuttuminen taikka tallennetun datan luvaton paljastaminen tai käyttäminen. Kun teko kohdistuu dataan ja sen kantamaan informaatioon, on teon viimekätisenä kohteena klassisen rikollisen teon aineellisesta objektista poiketen jotain aineetonta.

PC-R-CC:n aineellisoikeudelliset suositukset

Yleisten kriminaalipoliittisten pohdintojen jälkeen komitea päätyy kansallisille lainsäätäjille annettaviin kriminalisointisuosituksiin.[185] Suositus jakaantuu kahteen listaan: *minimilistaan* (minimum list of offences necessary for a uniform criminal policy on legislation concerning computer-related crime), johon otettujen tekojen kriminalisoinnin tarpeesta komiteassa oltiin yksimielisiä, ja *valinnaislistaan* (optional list), jossa mainittujen tekojen kriminalisoimista pidettiin ainakin harkinnan arvoisena.

Minimilistan suositukset ovat seuraavanlaiset:[186]

1. *Tietokonepetos.*[187] Sellainen datan tai ohjelmiston syöttäminen, muuttaminen, hävittäminen tai käytön estäminen taikka muu tietojenkäsittelyn lopputulokseen vaikuttava tietojenkäsittelytapahtumiin puuttuminen, joka aiheuttaa toiselle omaisuuden menetyksen tai taloudellista vahinkoa, kun teon tarkoituksena on hankkia itselle tai toiselle laitonta taloudellista hyötyä (tai vaihtoehtoisesti: kun teon tarkoituksena on laittomasti riistää toiselta tämän omaisuutta).

---

[184] Luvussa I.1.2.3.4. on jo käsitelty tätä kotirauhaa muistuttavaa suojeluobjektia, *tietojenkäsittelyrauhaa* (computer domicile tai pax computationis).

[185] EN:n raportti 89, s. 24 ss.

[186] Suomenkieliset käännökset ovat *Lehtimajan,* ks. Atk-rikospolitiikasta, s. 268 s. Englanninkieliset suositustekstit ovat näin kuuluvat (EN:n raportti 89, s. 80 s.):

1. *Computer fraud*. The input, alteration, erasure or suppression of computer data or computer programmes, or other interference with the course of data processing, that influences the result of data processing thereby causing economic or possessory loss of property of another person *with the intent of procuring an unlawful economic gain for himself or for another person.

*alternative draft: with the intent unlawfully deprive that person of his property

2. *Computer forgery*. The input, alteration, erasure or suppression of computer data or computer programmes, or other interference with the course of data processing, in a manner or such conditions, as prescribed by national law, that it would constitute the offence of forgery if it had been committed with respect to a traditional object of such an offence.

2. *Tietokonevääärennys.*[188] Datan tai ohjelmiston syöttäminen, muuttaminen, hävittäminen tai käytön estäminen taikka muu tietojenkäsittelyyn puuttuminen sellaisella tavalla ja sellaisissa olosuhteissa, että tekoa kansallisen lainsäädännön nojalla olisi pidettävä väärennysrikoksena, jos sen kohteena olisi ollut väärennysrikoksen perinteinen teko-objekti (”asiakirja” tms.).
3. *Datan tai ohjelmiston vahingoittaminen.* Datan tai ohjelmiston oikeudeton hävittäminen, vahingoittaminen, huonontaminen tai käytön estäminen.
4. *Tietokonesabotaasi.*[189] Sellainen datan tai ohjelmiston syöttäminen, muuttaminen, hävittäminen tai käytön estäminen taikka tietokonejärjestelmiin puuttuminen, jonka tarkoituksena on estää tietokone- tai televiestintäjärjestelmän toiminta.
5. *Luvaton järjestelmään tunkeutuminen.* Oikeudeton tunkeutuminen tietojärjestelmään tai tietokoneverkkoon, kun teko on tapahtunut turvajärjestelyjä murtamalla.
6. *Luvaton viestin sieppaaminen.* Tietokonejärjestelmässä välitettävien taikka siihen tulevien tai siitä menevien viestien sieppaaminen, kun teko on tapahtunut oikeudettomasti ja teknisiä apuvälineitä hyväksi käyttäen.
7. *Luvaton kappaleiden valmistaminen suojatusta tietokoneohjelmasta.* Oikeudeton kappaleiden valmistaminen lailla suojatusta tietokoneohjelmasta taikka sellaisen ohjelman oikeudetta tapahtuva levittäminen tai yleisön saataviin saattaminen.
8. *Luvaton kappaleiden valmistaminen integroidun piirin piirimallista.* Oikeudeton kappaleiden valmistaminen integroidun piirin lailla suojatusta piirimallista taikka piirimallin tai sen perusteella valmistettujen puolijohdetuotteiden oikeudetta tapahtuva kaupallinen käyttö tai sellaista käyttöä varten oikeudetta tapahtuva maahantuonti.

---

3. *Damage to computer data or computer programmes*. The erasure, damaging, deterioration or suppression of computer data or computer programmes without right.

4. *Computer sabotage*. The input, alteration, erasure or suppression of computer data or computer programmes, or interference with computer systems, with the intent to hinder the functioning of a computer or a telecommunications system.

5. *Unauthorised access*. The access without right to a computer system or network by infringing security measures.

6. *Unauthorised interception*. The interception, made without right and by technical means, of communications to, from or within a computer system or network.

7. *Unauthorised reproduction of a protected computer programme*. The reproduction, distribution or communication to the public without right of a computer programme which is protected by law.

8. *Unauthorised reproduction of a topography*. The reproduction without right of a topography, protected by law, of a semi-conductor product, or the commercial exploitation or the importation for that purpose, done without right, of a topography or of a semi-conductor product manufactured by using the topography.

[187] Pidän parempana rikosnimikkeenä *tietotekniikka-* tai *tietojenkäsittelypetosta.*

[188] Vastaavasti *tietotekniikka-* tai *tietotekninen väärennys.*

[189] *Tietotekniikka-* tai *tietojenkäsittelysabotaasi* olisi johdonmukainen rikosnimike.

Valinnaislistalla on neljä tekomuotoa:[190]

9. *Datan tai ohjelmiston muuttaminen.* Oikeudettomasti tapahtuva datan tai ohjelmiston muuttaminen.
10. *Tietokonevakoilu.* Sopimattomin keinoin tapahtuva ammatti- tai yrityssalaisuuden hankinta taikka sellaisen salaisuuden luvaton ilmaiseminen, luovuttaminen tai käyttäminen, kun teon tarkoituksena on aiheuttaa taloudellista vahinkoa salaisuuden lailliselle haltijalle taikka hankkia laitonta taloudellista hyötyä itselle tai toiselle.
11. *Tietokoneen luvaton käyttö.* Sellainen tietokonejärjestelmän tai -verkoston oikeudeton käyttö,
    a) johon tekijä ryhtyy hyväksyen mielessään sen huomattavan riskin, että teosta aiheutuu vahinkoa järjestelmän käyttöön oikeutetulle henkilölle taikka haittaa itse järjestelmälle tai sen toiminnalle, taikka
    b) joka tapahtuu tarkoituksin aiheuttaa vahinkoa järjestelmän käyttöön oikeutetulle henkilölle taikka haittaa itse järjestelmälle tai sen toiminnalle, taikka
    c) josta aiheutuu vahinkoa järjestelmän käyttöön oikeutetulle henkilölle taikka haittaa itse järjestelmälle tai sen toiminnalle.
12. *Suojatun tietokoneohjelman luvaton käyttö.* Lailla suojatusta tietokoneohjelmasta oikeudettomasti valmistettujen kappaleiden oikeudeton käyttö, kun se tapahtuu tarkoituksin hankkia laitonta taloudellista hyötyä joko itselle tai toiselle taikka oikeudenhaltijan vahingoittamiseksi.

Suositukset ovat yksityiskohtaisesti perusteltuja; palaan niin suositusteksteihin kuin perusteluihinkin tarpeellisilta osin jäljempänä yksittäisiä tietotekniikkarikoksia käsitellessäni. Suosituksen merkitys kansallisille lainsäätäjille on ollut huomattava niin Suomessa[191] kuin ulkomaillakin ja suositukselle asetettu har-

---

[190] EN:n raportti 89, s. 81:

9. *Alteration of computer data or computer programmes.* The alteration of computer data or computer programmes without right.

10. *Computer espionage*. The acquisition by improper means or the disclosure, transfer or use of a trade or commercial secret without right or any other legal justification, with intent either to cause economic loss to the person entitled to the secret or to obtain an unlawful economic advantage for oneself or a third person.

11. *Unauthorised use of a computer*. The use of a computer system or network without right, that either:

(a) is made with the acceptance of a significant risk of loss being caused to the person entitled to use the system or harm to the system or its functioning, or

(b) is made with the intent to cause loss to the person entitled to use the system or harm to the system or its functioning, or

(c) causes loss to the person entitled to use the system or harm to the system or its functioning.

12. *Unauthorised use of a protected computer programme*. The use without right of a computer programme which is protected by law and which has been reproduced without right, with the intent, either to procure an unlawful economic gain for himself or for another person or to cause harm to the holder of the right.

[191] Ks. esim. HE 94/93, s. 18 ss., jossa jakso ”Suomen tietokonerikossäännösten ja Euroopan neuvoston tietokonerikoskomitean suositusten vertailu”.

monisointitavoite on epäilemättä monessa suhteessa toteutunut. Kuitenkin suositus on jo eräiltä osin vanhentunut sikäli, että uusia kriminalisointitarpeita on ilmennyt. Näihin on kiinnitetty huomiota myös myöhemmässä kansainvälisessä yhteistyössä.[192]

PC-R-CC:n prosessioikeudellisia kannanottoja

Euroopan neuvoston raportissa käsitellään myös prosessuaalisia kysymyksiä.[193] Käsittelyn tarkoituksena on kansainvälisen keskustelun käynnistäminen eikä niinkään ratkaisujen löytäminen, ja tässä mielessä komitea on keskittynyt seuraaviin kolmeen ongelmaryhmään:

1) viranomaisten mahdollisuudet pakkokeinojen käyttämiseen todistusaineiston hankkimiseksi;
2) rikosprosessissa tapahtuvaan henkilötietojen keräämiseen, tallettamiseen ja yhdistämiseen liittyvät oikeudelliset ongelmat; sekä
3) tietoteknisistä tallenteista koostuvan todistusaineiston hyväksyttävyys tuomioistuinkäsittelyssä.

Mainituista ongelmista kaikki eivät ole suomalaisittain keskeisiä. Meillä suurimman ongelman muodostaa pakkokeinojen käyttö, sillä pakkokeinolainsäädäntömme ei sisällä erityissäännöksiä tietoteknisessä ympäristössä suoritettavan etsinnän tai takavarikon osalta. Henkilötietojen käsitteleminen rikosprosessin yhteydessä ei aiheuta Suomessa ongelmia, eikä suurempia vaikeuksia synny myöskään todistusaineiston hyväksyttävyyden suhteen; tämä ongelma koskettaa lähinnä *common law* -maita.[194]

Vuoden 1989 raportin neljännessä jaksossa käsitellään kansainvälisiä kysymyksiä.[195] Näistä nousevat erityisesti esille (1) tuomiovaltaan liittyvät ongelmat, jotka aiheutuvat tietotekniikkarikosten valtioiden välisiä rajoja ylittävästä (transfrontier) luonteesta ja (2) eurooppalaisten rikosoikeudellisten yleissopimusten sovellettavuus tietotekniikkarikosten kohdalla. Viimeksi mainituista käsitellään laajemmin rikoksen johdosta tapahtuvaa luovuttamista ja keskinäistä oikeusapua rikosasioissa koskevia eurooppalaisia yleissopimuksia, joihin

---

[192] Ks. esim. AIDP:n päätöslauselma kohta 10: "…other types of abuses that are not included expressly in the lists, such as trafficking in wrongfully obtained computer passwords and other information about means of obtaining unauthorized access to computer systems, and the distribution of viruses or similar programs, should also be considered as candidates for criminalization…"

[193] EN:n raportti 89, s. 52 ss.

[194] Nämä ongelmat eivät ole meilläkään täysin vailla merkitystä. Jos tietotekniikkarikos on tehty esimerkiksi sekä Suomessa että Englannissa ja rikosprosessuaalinen käsittely tapahtuu Englannissa, saattaa syntyä ongelmia Suomessa hankitun näytön hyväksyttävyydestä englantilaisessa tuomioistuimessa. Tällaiset vaikeudet ovat voitettavissa prosessuaalisten säännösten harmonisoimisella tai prosessia koskevilla kansainvälisillä sopimuksilla.

[195] EN:n raportti 89, s. 63 ss.

Suomi on liittynyt, sekä syytteen siirtämistä koskevaa eurooppalaista yleissopimusta.

Tuomiovallan suhteen aiheuttavat raportin mukaan ongelmia alueperiaate ja siihen liittyen kysymys exterritoriaalisen tuomiovallan laajuudesta. Monenvälisistä järjestelmistä toimivaltaristiriitojen hallitsemiseksi raportissa tuodaan esille muun muassa lainsäädäntöjen harmonisointi, syytteiden siirrot ja keskinäinen oikeusapu rikosasioissa.

Tässä yhteydessä raportissa käsitellään vielä erikseen ”suoran tunkeutumisen” (direct penetration) ongelmaa, joka syntyy nykytekniikan suomista mahdollisuuksista televerkon välityksin päästä käsiksi toisessa valtiossa tallennettuna olevaan dataan. Usean valtion alueella tehdyksi katsottavan tietotekniikkarikoksen tutkinnassa saattaa tutkintaa suorittavan valtion viranomaisille olla varsin tärkeää mahdollisimman nopeasti päästä käsiksi dataan, joka voi olla tallennettuna toisessa valtiossa olevaan tietojärjestelmään; todisteena merkityksellistä informaatiota edustavan datan muuttaminen tai hävittäminen käy esimerkiksi rikoksesta epäillyltä hyvin helposti.

Toisen valtion viranomaisen toimesta tapahtuva suora tunkeutuminen toisessa valtiossa olevaan järjestelmään tutkinnallisessa tarkoituksessa on varsin lähellä valtion suvereniteetin loukkaamista; joissakin oikeudellisissa järjestelmissä saattaa myös tällä tavoin hankitun todistusaineiston hyväksyttävyys olla kyseenalaista.

Todistusaineiston hyväksyttävyyden suhteen raportissa erotetaan erilaisia suoran tunkeutumisen tilanteita. Poliisi saattaa kotietsintää suoritettaessa löytää päätteen, jonka näytössä näkyy ulkomailla tallennettuna olevaa informaatiota. Etsinnän suorittaja voi olla joko tietoinen tai tietämätön siitä, että informaatio on tallennettu ulkomaille. Mahdollinen on myös tilanne, että poliisi omia päätteitään käyttäen tunkeutuu tiedostoon, jonka sisältämän tiedon tietää olevan tallennettuna ulkomailla.

Tällaisista ja muista vastaavista tilanteista syntyvien ongelmien vähentämiseksi komitea on erityisesti pohtinut sitä, olisiko sellaiseen suoraan tunkeutumiseen, johon keskinäistä oikeusapua rikosasioissa koskevan eurooppalaisen yleissopimuksen säännökset eivät *a priori* sovellu, voitava poikkeuksellisissa olosuhteissa ja erittäin tiukoin ehdoin oikeuttaa. Näitä kysymyksiä on kehitelty edelleen myöhempinä vuosina niin PC-PC:n kuin PC-CY:nkin työssä.

PC-R-CC ja tietoturvallisuus

Erillisenä kysymyksenä raportissa käsitellään turvallisuus- ja ehkäisemiskeinoja (security and prevention measures).[196] Tässä yhteydessä korostetaan jälleen sitä, että rikosoikeudelliset keinot eivät saa olla ensisijaisia, vaan ennen kaikkea

[196] EN:n raportti 89, s. 72 ss.

on pyrittävä kehittämään tietoturvallisuutta.[197] Komitea esittää seuraavan työmääritelmän tietoturvallisuuden keinoille:[198]

> Mikä tahansa sellainen tietotekniikkaa hyödyntävän organisaation johdon toiminta, jonka tarkoituksena on ehkäistä, paljastaa tai torjua hyökkäyksiä tai uhkia, jotka kohdistuvat järjestelmän vapaaseen ja yksinomaiseen käyttöön, järjestelmän häiriöttömään toimintaan tai sen koskemattomuuteen ja luotettavuuteen, pyrkimyksenä saavuttaa tasapaino turvallisuustoimenpiteistä koituvien kustannusten ja tavoitellun riskien vähenemisasteen välillä.

Määritelmän todetaan kattavan sekä aktiivisen toiminnan (actions) että tekemättä jättämisen (omissions), sekä aineelliset (material) että aineettomat keinot (non-material means) samoin kuin henkilöstöön liittyvät (personnel) ja muodolliset keinot (formal means); viimeksi mainituista mainitaan esimerkkeinä vakuutussopimukset sekä yleisesti kaikki oikeudelliset ja organisatoriset turvajärjestelyt.

Komitea pitää välttämättömänä sitä, että Euroopan neuvoston jäsenvaltiot ryhtyvät toimenpiteisiin tietoturvallisuuden parantamiseksi. Esimerkkeinä tällaisista toimenpiteistä mainitaan muiden muassa asianomaisten henkilöstöryhmien (opettajien, virkamiesten ja poliisien) koulutuksellisten valmiuksien parantaminen sekä tietokoneiden valmistajien ja käyttäjien oikeudellinen velvoittaminen ottamaan huomioon ainakin tietty tietoturvallisuuden vähimmäistaso.

> Tietoturvallisuuden merkityksen korostaminen on sopusoinnussa komitean painottaman rikosoikeuden toissijaisuuden periaatteen kanssa. Tietoturvallisuuden alueella Suomen kannalta merkittävimmät kansainväliset asiakirjat ovat maaliskuussa 1992 hyväksytty Euroopan yhteisöjen neuvoston tietoturvallisuuspäätös sekä marraskuussa 1992 hyväksytyt OECD:n neuvoston tietoturvallisuussuositus, tietoturvallisuusperiaatteet ja perustelumuistio.
>
> Euroopan unionin neuvosto on 7.4.1995 antanut suosituksen yleisistä tietotekniikan turvallisuuden arviointiperusteista (95/144/EY). Suositus ei ole jäsenmaita juridisesti sitova; sen tarkoituksena on toisaalta parantaa valmistettavien tietotekniikkatuotteiden turvallisuusominaisuuksia, toisaalta tarjota tuotteiden ja palvelujen käyttäjille arviointiperusteita, joita voidaan käyttää tarjouspyyntö- ja hankintatilanteissa.[199]

---

[197] Komitea käyttää tässä termiä ”computer security”, johon toteaa kuuluvan muutakin kuin komitean käsittelemät rikosoikeudelliset aspektit; komitea viittaa myös termiin ”information security”, jolle on – ainakin tässä yhteydessä – annettavissa sama sisältö.

[198] ”Any kind of action or means deployed by the management of a computerised organisation to prevent, detect, withstand or react to attacks on and threats to the free and exclusive availability of a system or its undisturbed functioning or on its integrity and its confidentiality, seeking to balance the cost of the security measure against and desired degree of reduction of the risk.” EN:n raportti 89, s. 72.

[199] VvM:n hallinnon kehittämisosaston kirje VM 9/73/95/7.9.1995.

Suomessa valtioneuvosto on 4.2.1993 tehnyt periaatepäätöksen tietoturvallisuuden kehittämisestä valtionhallinnossa. Kehittämispäätös koskee ministeriöitä, virastoja ja laitoksia sekä näiden ulkopuolisilta hankkimia tietohallintopalveluja; lisäksi päätöksen periaatteita suositellaan noudatettavaksi myös valtionhallinnon ja muiden organisaatioiden (mm. kunnallishallinnon yksiköt, yritykset ja yhteisöt) välisessä tietoteknisessä yhteistyössä ja tiedonsiirrossa sekä valtion uusimuotoisten liikelaitosten ja valtionyhtiöiden tietoturvallisuustyössä.[200]

Näiden viranomaisten toimintaan liittyvien tietoturvallisuusnormistojen ohessa on aivan oma merkityksensä liike- ja yritysmaailmassa toteutetuilla tietoturvallisuustoimenpiteillä, joihin ei tässä yhteydessä kuitenkaan ole aiheellista puuttua.[201]

Tietotekniikkarikosten uhrit

Toisena erilliskysymyksenä käsitellään tietotekniikkarikosten uhrien asema (computer-related victimisation).[202] Rikoksen uhrin asema ylipäänsä on ollut Euroopan neuvoston erityisen huomion kohteena 1970-luvun loppupuolelta lähtien.

Raportin mukaan useissa maissa tehdyt tutkimukset osoittavat tietotekniikkarikosten kohdistuneen pääasiassa pankki- ja vakuutusaloihin sekä julkishallinnon organisaatioihin ja yksiköihin. Raportissa todetaan se nykyään jo notoriseksi katsottava tosiseikka, että tietotekniikkarikosten kohteeksi joutuneet ovat haluttomia ilmoittamaan rikoksista viranomaisille, minkä vuoksi on syytä olettaa tietotekniikkarikosten todellisen määrän olevan huomattavasti viranomaisten tietoon tullutta suurempi. Ilmoittamishaluttomuus muodostaa vakavan ongelman taistelussa tietotekniikkarikollisuutta vastaan, sillä yhteistyö asianomistajien kanssa on ensiarvoisen tärkeää pyrittäessä tukahduttamaan puheena olevaa rikollisuutta.

Ilmoittamishaluttomuuden syinä nähdään mm. pelko siitä, että julkisuuden seurauksena yleisö menettää luottamuksensa asianomaiseen organisaatioon, jolloin taloudelliset menetykset saattavat nousta rikoksen välittömästi aiheuttamia suuremmiksi; julkisuus saattaa aiheuttaa myös organisaation johdon kasvojen menetyksen. Toisaalta rikoksen käsittelystä sinänsä saattaa aiheutua merkittävää ajanhukkaa, minkä lisäksi rikoksen uhrit saattavat suhtautua varauksella rikostutkinnasta ja syytteeseenpanosta vastaavien viranomaisten asiantuntemukseen.

---

[200] Ks. myös valtiovarainministeriön valtionhallinnossa noudatettavan atk-turvapolitiikan määrittelyä varten 31.5.1991 asettaman työryhmän 26.6.1992 antama mietintö, VvM 6/1992. Työryhmän asiantuntijana ja sihteerinä toimi *Matti Tenhunen,* joka sittemmin on koonnut yhdeksi niteeksi valtioneuvoston, EY:n ja OECD:n tietoturvallisuuspäätökset sekä suomen- että englanninkielisinä versioina, VvM 5/1993.

[201] Ks. esim. Saari.

[202] EN:n raportti 89, s. 74 ss.

Komitea on pohtinut erilaisia keinoja asianomistajien kanssa käytävän yhteistyön tehostamiseksi. Radikaaleimpana ratkaisuna on esitetty lakisääteisen velvollisuuden asettaminen organisaatioiden johdolle ilmoittaa poliisille kaikista tietojärjestelmiin kohdistuneista laittomista teoista, mutta useimpien valtioiden oikeudellisia traditioita vastaamattomana tällainen vaihtoehto on hylätty.

Lievempänä vaihtoehtona voisi tulla kysymykseen velvollisuus ilmoittaa puheena olevista tapauksista jollekin valvontaelimelle samaan tapaan kuin Yhdysvalloissa, jossa *Bank Protection Act* asettaa pankeille sanktioidun velvollisuuden ilmoittaa pankkiviranomaisille kaikista petoksista samoin kuin 1 000 US$:ia suuremmista selittämättömistä tappioista. Toisaalta tällaista velvollisuutta ei voida ulottaa koskemaan kaikkia tietotekniikkarikoksia eikä myöskään rajoittaa ainoastaan tietotekniikkarikoksia koskevaksi. Koska tällainen ilmoittamisvelvollisuuskin joissakin tapauksissa saattaisi soveltua huonosti eri valtioiden oikeusjärjestyksiin, ei komitea suoranaisesti suosittele sen käyttöönottamista mutta esittää vaihtoehtoa harkittavaksi.

Yksityisyyden suoja

Tietotekniikkarikoksiin on kansainvälisessä yhteistyössä läheisesti liittynyt kysymys yksityisyyden suojasta, ja yksityisyyden suojan tietotekniikka-avusteisia loukkauksia käsitellään raportissa kolmantena erilliskysymyksenä.[203] Tältä osin komitea esittää kuusi perusperiaatetta, jotka pääpiirteissään ovat seuraavanlaiset:

1) Yksityisyyden suojelu nykyaikaisen tietotekniikan keinoin tapahtuvia loukkauksia vastaan on erityisen tärkeää. Suojelun on kuitenkin perustuttava ensisijassa hallinto- ja siviilioikeudelliseen sääntelyyn rikosoikeuden keinojen tullessa kysymykseen ainoastaan äärimmäisissä tapauksissa (ultima ratio -periaate).
2) Rikosoikeudellisten säännösten on oltava täsmällisiä ja tyhjentäviä; avoimia yleislausekkeita on vältettävä (rikoslain sanamuodon täsmällisyyden periaate).
3) Rangaistavat menettelyt on kuvattava mahdollisimman selkeästi asianomaisissa rangaistussäännöksissä. Viittaustekniikan liiallista käyttöä on vältettävä (selvyysperiaate).
4) Erilaisia yksityisyyden tietotekniikka-avusteisia loukkauksia ei tule kriminalisoida yhdellä laaja-alaisella säännöksellä. Kriminalisoinnit on eroteltava ottaen huomioon loukattava intressi, loukkaava teko sekä tekijän asema ja hänen tarkoituksensa (erotteluperiaate).
5) Tietotekniikka-avusteisten yksityisyyden loukkausten tulisi periaatteessa olla rangaistavia vain tahallisesti tehtyinä (tahallisuusperiaate).
6) Vähäisempien tietotekniikka-avusteisten yksityisyyden loukkausten ei tulisi olla virallisen syytteen alaisia tekoja (asianomistajaperiaate).

---

[203] EN:n raportti 89, s. 77 ss.

Komitea toivoo, että nämä periaatteet muodostaisivat perustan vastaiselle tietotekniikka-avusteisia yksityisyyden loukkauksia koskevalle työlle ja että ne auttaisivat luomaan riittävää rikosoikeudellista järjestelmää automaattisen tietojenkäsittelyn alueelle.

PC-R-CC:n raportin suurin merkitys on epäilemättä sen kriminalisointisuosituksessa. Suosituksen vaikutus näkyy usean valtion lainsäädännössä ja esimerkiksi Yhdistyneiden Kansakuntien ja AIDP:n piirissä tehdyn tietotekniikkarikoksia koskevan työn lähtökohdat ovat – niin kuin jäljempänä havaitaan – suurelta osin juuri puheena olevassa suosituksessa.

2.1.3.2 PC-PC

Euroopan neuvosto asetti vuonna 1991 asiantuntijakomitean selvittämään tietotekniikkarikoksiin liittyviä prosessioikeudellisia kysymyksiä.[204] Komitean tehtäväksi annettiin tutkia Euroopan neuvoston tietotekniikkarikossuosituksen R(89)9 samoin kuin kirjallisia todistuksia sekä asiakirjajäljenteiden ja tietoteknisten tallenteiden hyväksyttävyyttä koskevan harmonisointisuosituksen R(81)20[205] pohjalta seuraavia kysymyksiä:[206]

---

[204] Committee of Experts on Procedural Law Problems connected with Computer Crime (PC-PC). Komiteassa olivat edustettuina EN:n jäsenvaltioista Belgia, Kypros, Suomi (edustajana *Matti Tenhunen),* Ranska, Saksa, Kreikka, Unkari, Italia, Alankomaat, Norja, Portugali, Ruotsi, Sveitsi, Turkki ja Yhdistynyt kuningaskunta. Tarkkailijoina komitean työhön osallistuivat EU:n komissio, Kanada, Yhdysvallat sekä Interpol.

[205] Harmonisation of laws relating to the requirement of written proof and to the admissibility of reproductions of documents and recordings on computers, s. 6, jossa seuraavat suositukset:

I.1. Governments of the member states whose laws require proof for transactions whose value is greater than the minimum amount fixed by law:

a. to study the possibility of abolishing this requirement;

b. to provide that in all those cases where written proof is still required a written form will be necessary only for transactions whose value is equal to or greater than a sum, in national currency, corresponding to at least 728 drawing rights as defined by the International Monetary Fund at the moment when the state implements this recommendation;

c. to consider, in the light of the economic situation, the advisability of revising the sum mentioned in *b* above at least every five years from the date of the adoption of this recommendation.

2. Paragraph 1 does not affect the cases where national requires a written form for the validity of the transaction.

II. Governments of all member states:

to fix a period nor exceeding ten years as the period of compulsory preservation of books and documents which commercial undertakings must preserve pursuant to national law.

III. Governments of all member states: to make their law concerning reproductions of documents by microfilming and recordings on computers conform to the rules contained in the appendix to this recommendation or, if no such law exists, to introduce legislation conforming to these rules.

[206] Ks. Nilsson, Activities, s. 580.

1) pakkokeinojen käyttö teknologisessa ympäristössä, kotikäyntejä, tele-kuuntelua ja tietokoneiden salakuuntelua sekä etsintää ja takavarikkoa tietoteknisessä ympäristössä koskevien rikosprosessuaalisten säännösten pohjalta mukaan lukien mahdollisuus rikoksesta epäillyn aktiiviseen yhteistyöhön esitutkinnassa;
2) tietojenkäsittelyaineistosta ohjelmat mukaan lukien koostuvan todistusaineiston sallittavuus ja luotettavuus; komitean on lisäksi tutkittava elektronisen asiakirjan määritelmää;
3) erityiset prosessioikeudelliset kysymykset, jotka liittyvät uuden teknologian käyttöön sekä uusiin rikoksentekomuotoihin kuten ”virusten”, ”loogisten pommien” ja ”matojen” valmistamiseen; syyttäjien ja poliisin kouluttaminen erityisesti teknisissä kysymyksissä tämäntyyppistä rikollisuutta vastaan käytävän taistelun tehostamiseksi;
4) kansainvälinen yhteistyö tietotekniikkarikosten tutkinnassa.

Komitean työ päättyi keväällä 1995, jolloin komitea sai valmiiksi raporttinsa ja siihen liittyvän suositusluonnoksen. Euroopan neuvoston ministerikomitea on hyväksynyt raportin ja suosituksen syyskuun 7. päivänä 1995.[207]

Raportissa käsitellään elektronisessa muodossa olevaa dataa rikostutkinnan kohteena ja asetetaan kysymyksenalaiseksi se, onko viranomaisilla käytettävissään vastaavia keinoja todistusaineiston hankkimiseksi tietoverkkoihin ja -järjestelmiin kohdistuneista rikoksista verrattuna tilanteisiin, joissa on kysymys konkreettisiin ja aineellisiin objekteihin kohdistuneista rikoksista ja niiden tutkinnasta. Tosiasiallisesti tällainen tietokoneeseen tallennetun datan edustama informaatio on todistusaineiston uusi muoto, jonka hankkiminen ja käyttäminen edellyttää uusia ja erityisiä säännöksiä.[208]

Suositus sisältää kahdeksantoista yksittäistä säännössuositusta, jotka kohdistuvat seitsemään pääalueeseen: (1) etsintä ja takavarikko, (2) tekninen tarkkailu, (3) velvollisuudet yhteistyöhön tutkintaviranomaisten kanssa, (4) elektroninen todistusaineisto, (5) salaustekniikan käyttö, (6) tutkimus, tilastointi ja koulutus sekä (7) kansainvälinen yhteistyö.

2.1.3.3 PC-CY

Huhtikuussa 1997 piti ensimmäisen kokouksensa CDPC:n marraskuussa 1996 tekemällä päätöksellä asetettu uusi asiantuntijakomitea, niin kutsuttu *Cybercrime-työryhmä* (Committee of Experts on Crime in Cyber-space, PC-CY), jonka toimeksiantonsa mukaan tuli valmistella sitova instrumentti eli kansainvälinen yleissopimus PC-R-CC:n ja PC-PC:n suositusten pohjalta ottaen erityi-

---

[207] Final Activity Report and Recommendation Concerning Problems of Criminal Procedural Law Connected with Information Technology, R(95)13.
[208] Raportti, kohta 16.

sesti huomioon tietoverkkojen kehittyminen ja laajeneminen.[209] CDPC:n päätöksessä komitean asettamista perusteltiin mm. seuraavasti:[210]

> ”The fast developments in the field of information technology have a direct bearing on all sections of modern society. The integration of telecommunication and information systems, enabling the storage and transmission, regardless of distance, of all kinds of communication opens a whole range of new possibilities. These developments were boosted by the emergence of information super-highways and networks, including the Internet, through which virtually anybody will be able to have access to any electronic information service irrespective of where in the world he is located. By connecting to communication and information services users create a kind of common space, called ’cyber-space’, which is used for legitimate purposes but may also be the subject of misuse. These ’cyber-space offences’ are either committed against the integrity, availability, and confidentiality of computer systems and telecommunication networks or they consist of the use of such networks of their services to commit traditional offences. The transborder character of such offences, e.g. when committed through the Internet, is in conflict with the territoriality of national law enforcement authorities.
>
> The criminal law must therefore keep abreast of these technological developements, which offer highly sophisticated opportunities for misusing facilities of the cyber-space and causing damage to legitimate interests. Given the cross-border nature of information networks, a concerted international effort is needed to deal with such misuse. Whilst Recommendation No. (89) 9 resulted in the approximation of national concepts regarding certain forms of computer misuse, only a binding international instrument can ensure the necessary efficiency in the fight against these new phenomena. In the framework of such an instrument, in addition to measures of international co-operation, questions of substantive and procedural law, as well as matters that are closely connected with the use of information technology should be addressed.”

Komitean alkuperäinen toimeksianto kesti vuoden 1999 loppuun mutta ajan osoittauduttua riittämättömäksi toimikautta jatkettiin vielä vuodella.[211] Tämäkään ei aivan riittänyt, sillä komitean viimeisessä kokouksessa joulukuussa 2000 jouduttiin toteamaan, että ratkaisemattomia kysymyksiä oli vielä jäljellä.

---

[209] Suomi osallistui PC-CY:n työskentelyyn alusta saakka edustajinaan tämän kirjoittaja ja varsinkin työn alkuvaiheessa myös Keskusrikospoliisin silloinen apulaispäällikkö Matti Tenhunen, joka jatkoi osallistumistaan työryhmän työskentelyyn jonkin aikaa vielä kesällä 1999 tapahtuneen eläkkeelle siirtymisensä jälkeenkin.

[210] Päätös CDPC/103/211196.

[211] PC-CY kokoontui toiminta-aikanaan kymmeneen täysistuntoon. Lisäksi PC-CY:n asettama ns. Drafting Group eli kaikille PC-CY:n jäsenille avoin alatyöryhmä kokoontui 15 kertaa. Varsinainen artiklojen kirjoittaminen tapahtui Drafting Groupissa, täysistunnoissa keskusteltiin ja päätettiin enemmänkin linjakysymyksistä, joskin tietysti yksityiskohdistakin päättäminen muodollisesti kuului täysistunnon toimivaltaan.

CDPC asettikin kevätkaudeksi 2001 suppean alatyöryhmän viimeistelemään sopimustekstiä ja laatimaan selitysmuistiota. Sitä paitsi Euroopan neuvoston parlamentaarinen yleiskokous antoi lausuntonsa sopimusluonnoksesta vasta vuoden 2001 puolella, ja myös tämän lausunnon mahdollisesti aiheuttamat muutokset sopimustekstiin kuuluivat alatyöryhmän toimeksiantoon. Sopimusluonnos hyväksyttiin[212] kesäkuussa 2001 CDPC:n 50. täysistunnossa,[213] minkä jälkeen sopimus hyväksyttiin alkusyksystä 2001 ministerikomiteassa ja avattiin allekirjoitettavaksi 22.–23.11.2001 Budapestissa Euroopan neuvoston ja Unkarin hallituksen järjestämässä konferenssissa. Suomi allekirjoitti sopimuksen heti ensimmäisten joukossa.[214]

Yleissopimusluonnos julkistettiin pääosiltaan keväällä 2000 tarkoituksena saada yleisöltä kommentteja.[215] Näitä saatiinkin todella paljon. Yleissopimuksen työnimenä oli ”Convention on Cybercrime”, joka jäi myös sen lopulliseksi englanninkieliseksi nimeksi – nimeen ei tosin oltu PC-CY:ssä erityisen tyytyväisiä mutta parempaakaan ei keksitty. Suomenkieliseksi nimeksi näyttää tulevan ”Tietoverkkorikollisuutta koskeva yleissopimus”.

Yleissopimuksesta on tehty avoin kaikille valtioille. Tämä lähtökohta on tietysti asettanut ylimääräisiä vaatimuksia sopimuksen sisällölle verrattuna siihen tilanteeseen, että sopimusteksti olisi luotu vain Euroopan neuvoston jäsenmaita varten; näillähän on esimerkiksi jo olemassa valmiit instrumentit kansainvälisen oikeusavun antamiseksi ja rikoksentekijän luovuttamiseksi. Euroopan neuvoston ulkopuolisista maista PC-CY:n työhön osallistuivat hyvin aktiivisesti USA, Kanada ja Japani ja olikin havaittavissa, että joissakin kysymyksissä oli erityisesti angloamerikkalaisen ja mannereurooppalaisen oikeusjärjestyksen yhteensovittaminen melkoisen vaikeaa.

PC-CY:n yksityiskohtaiset tehtävät oli toimeksiannossa määritelty seuraavasti:

---

[212] Sopimusluonnos hyväksyttiin yksimielisesti lukuun ottamatta ns. liittovaltiolauseketta, federal clausea, joka sallisi osavaltiolainsäädännön tietyissä tilanteissa poikkeavan sopimuksen määräyksistä, olkoonkin, että liittovaltio sinänsä olisi sopimuksen ratifioinut. Ensisijaisesti Ranskan vastustuksen johdosta tämän USA:n erittäin tärkeänä pitämän kysymyksen ratkaisu siirtyi ministerikomiteaan.

[213] CDPC:n kokouksessa päätettiin asettaa uusi komitea, PC-RX, valmistelemaan verkkorikoskonventioon lisäpöytäkirjaa tietoverkkojen välityksin tapahtuvan rasismiin ja muukalaisvihaan yllyttämisen kriminalisoimisesta. Kysymyksessä on ns. sisältörikos, joka ei kuulu tämän tutkimuksen alaan.

[214] Suomen puolesta allekirjoittajana toimi oikeusministeri Johannes Koskinen. Suomen valtuuskuntaan kuuluivat lisäksi suurlähettiläs Hannu Halinen Suomen Unkarin suurlähetystöstä, lähetystöneuvos Pekka Voutilainen Suomen pysyvästä edustustosta Strasbourgista sekä tämän kirjoittaja.

[215] Sopimusteksti on luettavissa esimerkiksi osoitteessa http://conventions.coe.int.

i. Examine, in the light of Recommendations No R (89) 9 on computer-related crime and No R (95) 13 concerning problems of criminal procedural law connected with information technology, in particular the following subjects:
ii. cyber-space offences, in particular those committed through the use of telecommunication networks, e.g. the Internet, such as illegal money transactions, offering illegal services, violation of copyright, as well as those which violate human dignity and the protection of minors;
iii. other substantive criminal law issues where a common approach may be necessary for the purposes of international co-operation such as definitions, sanctions and responsibility of the actors in cyber-space, including Internet service providers;
iv. the use, including the possibility of transborder use, and the applicability of coercive powers in a technological environment, e.g. interception of telecommunications and electronic surveillance of information networks, e.g. via the Internet, search and seizure in information-processing systems (including Internet sites), rendering illegal material inaccessible and requiring service providers to comply with special obligations, taking into account the problems caused by particular measures of information security, e.g. encryption;
v. the question of jurisdiction in relation to information technology offences, e.g. to determine the place where the offence was committed (*locus delicti*) and which law should accordingly apply, including the problem of *ne bis idem* in the case of multiple jurisdictions and the question how to solve positive jurisdiction conflicts and how to avoid negative jurisdiction conflicts;
vi. questions of international co-operation in the investigation of cyber-space offences, in close co-operation with the Committee of Experts on the Operation of European Conventions in the Penal Field (PC-OC).

Yleissopimus käsittää johdannon lisäksi neljä lukua: (I) *Käsitteiden käyttö;* (II) *Kansalliset toimenpiteet;* (III) *Kansainvälinen yhteistyö;* ja (IV) *Loppumääräykset.* Pääpaino sopimuksessa on prosessuaalisissa säännöksissä (ml. esitutkinta ja pakkokeinojen käyttäminen) ja kansainvälisessä yhteistyössä. Sopimukseen sisältyy kuitenkin useita myös tämän tutkimuksen kannalta merkityksellisiä aineellista rikosoikeutta koskevia määräyksiä. Käsittelen tässä yhteydessä vain näitä; prosessioikeudelliset samoin kuin kansainväliseen yhteistyöhön liittyvät määräykset jätän tämän tutkimuksen ulkopuolelle lukuun ottamatta niiden pääpiirteittäistä kuvailemista *de lege ferenda* -jaksossa. Palaan määräyksiin tarpeellisilta osin yksityiskohtaisemmin jäljempänä kolmannessa luvussa yksittäisiä rikostyyppejä käsiteltäessä mutta esitän tässä niiden sisällön pääpiirteissään.

Sopimuksen toisen luvun ensimmäisen jakson *(Rikosoikeuden aineelliset säännökset)* ensimmäinen osasto *(Datasiirron ja tietojärjestelmien luottamuksellisuuteen, eheyteen ja käytettävyyteen kohdistuvat rikokset)* sisältää artiklois-

sa 2–6 määräyksiä kaikkein keskeisimmistä tietotekniikkarikoksista, jotka kohdistuvat juuri tietotekniikkarikosten yhteiseen suojeluobjektiin: luottamuksellisuuden, eheyden ja käytettävyyden yhdessä muodostamaan tietojenkäsittelyrauhaan.

Artiklassa 2 velvoitetaan sopimusvaltiot kriminalisoimaan *luvaton tunkeutuminen (Illegal access),* artikla 3 koskee *viestintäsalaisuuden loukkaamista (Illegal interception),* artikla 4 *datan vahingoittamista (Data interference),* artikla 5 *tietojärjestelmän häirintää (System interference)* ja artikla 6 eräiden *välineiden väärinkäyttöä (Misuse of devices).*

Nämä kriminalisoinnit on meillä jo pääpiirteissään toteutettu lukuun ottamatta artiklassa 6 tarkoitettua menettelyä. Sama ajattelu on tosin havaittavissa vasta hiljattain kumotusta vanhasta rikoslain 44 luvun 19 §:stä, jossa kriminalisoitiin tiirikan hallussapito, samoin kuin nykyään voimassa olevasta 28 luvun 12a §:stä (400/2002): tässähän on kysymys eräänlaisesta elektronisten murtovälineiden hallussapidon ja levittämisen kriminalisoimisesta, sillä säännöksessä puhutaan välineestä (ml. tietokoneohjelma), joka on suunniteltu tai muunnettu erityisesti artikloissa 2–5 tarkoitettujen tekojen tekemiseen. Lisäksi näihin välineisiin luetaan salasanat, käyttäjätunnukset ja muu vastaava data, jota käyttämällä tietojärjestelmään on mahdollista oikeudettomasti tunkeutua. Kysymyksessä on siis eräänlainen tietoteknisessä ympäristössä käytettävän tiirikan kriminalisointivelvoite, jonka implementoiminen edellyttää Suomessa lain muuttamista.

Toisen osaston *(Tietokoneavusteiset rikokset)* artikloissa 7 ja 8 on määräykset *tietokoneavusteisesta väärennyksestä (Computer-related forgery)* ja *tietokoneavusteisesta petoksesta (Computer-related fraud),* joissa tarkoitetut menettelyt on Suomen rikoslaissa kriminalisoitu.

Kolmas osasto *(Viestin sisältöön liittyvät rikokset)* sisältää vain yhden artiklan. Artikla 9 koskee lapsipornografian tuottamista, tarjoamista, levittämistä, hankkimista ja hallussapitoa. PC-CY:ssä harkittiin kylläkin eräiden muiden sisältöön liittyvien rikosten mukaan ottamista konventioon; tällaisia olivat mm. rasismiin ja terrorismiin yllyttäminen. Yhdysvaltalainen käsitys sananvapaudesta perusoikeutena poikkesi kuitenkin siinä määrin eurooppalaisista näkemyksistä, että yksimielisyyttä ei saavutettu.

Suomessa ei lapsipornografia-artikla edellytä lainsäädäntötoimia muuten kuin sikäli, että sopimuksen mukaan lapsi tulee määritellä käyttämällä kiinteää ikärajaa, joka ei saa olla 16 vuotta alhaisempi. Suomi vastusti tällaisen kiinteän ikärajan käyttöön ottamista, sillä käsitykseni mukaan siitä saattaa seurata suuria ongelmia lapsipornografiarikosten selvittämisessä: jotta voitaisiin tietää, onko esimerkiksi jokin kuvamateriaali lapsipornografiaa, olisi kyettävä selvittämään kuvan ottamisen ajankohta ja kuvassa esiintyvän henkilön ikä kuvan ottamishetkellä. Suomen perustelut eivät kuitenkaan tehonneet ja nähtäväksi jää, miten ongelmat aikanaan ratkaistaan. Artikla on tarkoitus implementoida samanaikai-

sesti Euroopan unionin lapsipornografiaa koskevan puitepäätöksen voimaan saattamisen kanssa. Asiaa koskeva työryhmämietintö on jo ollut helmikuussa 2004 päättyneellä lausuntokierroksella ja mietinnössä ehdotetaan otettavaksi käyttöön 18 vuoden ikäraja, jota mm. Euroopan unionin puitepäätös edellyttää.

Neljäs osasto *(Tekijänoikeusrikokset ja tekijänoikeuden lähioikeuksia koskevat rikokset)* käsittää sekin vain yhden artiklan, jossa velvoitetaan kriminalisoimaan immateriaalioikeuksien tietojärjestelmän välityksin tapahtuneet loukkaukset. Koska Suomen lainsäädäntö ei näiltä osin ole mitenkään välinesidonnaista, vastaavat voimassa olevat säännöksemme yleissopimuksen 10 artiklaa.

Viidennessä osastossa *(Osallisuus, yhteisövastuu ja sanktiot)* käsitellään yritystä, yllytystä ja avunantoa (artikla 11), yhteisövastuuta (artikla 12) ja seuraamuksia (artikla 13). Yrityksen osalta sopimus merkitsisi meillä lähinnä sitä, että vahingonteon yritys tulisi kriminalisoida, joskin yrityksen rangaistavuuden suhteen on mahdollista tehdä varauma. Yhteisövastuu on sopimuksessa ulotettu varsin laajalle eli koskemaan kaikkia sopimuksessa mainittuja rikoksia, joten tältä osin lainmuutoksia joudutaan meillä tekemään.

Yleissopimuksen varsinainen ydin on sen prosessioikeudellisissa ja kansainvälistä yhteistyötä koskevissa säännöksissä, joiden implementoiminen Suomen lainsäädäntöön tulee aiheuttamaan jonkin verran työtä. Alkuperäisistä tavoitteista jouduttiin vuosien mittaan tinkimään ja esimerkiksi esitutkintaviranomaisen mahdollisuutta suorittaa ns. rajat ylittävä etsintä (transborder search) vain ilmoittamalla siitä jälkikäteen kohdevaltiolle ei sopimukseen loppujen lopuksi tullut; menettely koettiin siinä määrin ongelmalliseksi valtioiden suvereenisuuden kannalta.

Kuitenkin yleissopimus sisältää lukuisia eri maiden viranomaisten keskinäisiä menettelymuotoja nopeuttavia ja yksinkertaistavia määräyksiä, joiden käyttöön ottaminen aikanaan epäilemättä suuressa määrin tulee helpottamaan useiden valtioiden alueella tehtyjen tietotekniikkarikosten tutkintaa ja syytteeseenpanoa.

Yleissopimus on koettu kansainvälisesti erittäin tärkeäksi ja sen valmisteluun osallistuminen oli usealle valtiolle hyvin korkealle priorisoitu tehtävä. Myös Euroopan oikeusministerit ilmaisivat kahdesti nimenomaisen tukensa PC-CY:n työlle: ministerien 21. konferenssissa Prahassa kesäkuussa 1997[216] sekä 23. konferenssissa Lontoossa kesäkuussa 2000.[217]

2.1.3.4 PC-RX

Joulukuussa 2001 kokoontui ensimmäiseen istuntoonsa uusi komitea PC-RX, Committee of Experts on the criminalisation of acts of a racist and xenophobic nature committed through computer systems, jonka tehtävänä oli luonnostella

---

[216] Konferenssin päätöslauselma nro 1.
[217] Päätöslauselma nro 3.

tietoverkkorikosyleissopimuksen ensimmäinen lisäpöytäkirja.[218] Koska yleissopimusta neuvoteltaessa ei saavutettu yksimielisyyttä siitä tavasta, jolla rasistisia ja muukalaisvihamielisiä tekoja olisi pitänyt käsitellä, ja kun niiden huomioon ottaminen kuitenkin koettiin yleisesti ja erityisesti Ranskan mielestä tärkeäksi, päädyttiin lisäpöytäkirjan käyttämiseen. Komitea kokoontui kevättalven 2002 aikana neljä kertaa ja sen työn lopputulos hyväksyttiin CDPC:n yleiskokouksessa kesäkuussa 2002. Ministerineuvoston hyväksyttyä lisäpöytäkirjan loppuvuonna 2002 se avattiin allekirjoitettavaksi tammikuussa 2003, jolloin myös Suomi sen allekirjoitti.

Lisäpöytäkirja velvoittaa tietoverkkojen välityksin tapahtuvan rasistisen ja muukalaisvastaisen aineiston levittämisen sekä rasismiin ja muukalaisvastaisuuteen perustuvan uhkaamisen ja loukkaamisen kriminalisoimiseen. Lisäksi pöytäkirjassa on määräys, joka edellyttää joukkotuhonnan tai ihmisyyttä vastaan tehtyjen rikosten[219] vähättelemisen tai hyväksymisen[220] kriminalisoimista.

Asiallisesti pöytäkirja ei suurestikaan eroa Euroopan komission tekemästä ehdotuksesta puitepäätökseksi rasismin ja muukalaisvihan vastaisesta toiminnasta.[221] Erona on kuitenkin se, että puitepäätösehdotus ei ole rajoitettu koskemaan tietoverkkoja hyväksi käyttäen tehtyjä rikoksia, vaikka korostaakin niiden merkitystä. Tätä helmikuussa 2004 kirjoitettaessa on puitepäätösehdotuksen käsittely Euroopan unionin neuvoston aineellisen rikosoikeuden työryhmässä vielä kesken.

2.1.4 Yhdistyneet Kansakunnat

Yhdistyneiden Kansakuntien sihteeristön yhteydessä toimiva kriminaalipoliittinen yksikkö (Crime Prevention and Criminal Justice Branch of the United Nations), jonka työ 1980-luvun alusta on keskittynyt niin kutsuttuun valkokaulusrikollisuuteen (white collar crime) ja vallan väärinkäyttöön (abuse of power), on runsaat kymmenen vuotta sitten ryhtynyt kiinnittämään erityistä huomiota tietotekniikan lisääntyvään käyttöön rikosten ehkäisemisessä ja kontrolloimisessa ja tämän myötä myös tietotekniikkarikosten ehkäisemiseen ja syytteeseen saattamiseen.[222]

---

218 Tämän kirjoittaja toimi Suomen edustajana komiteassa.

219 Art. 8: ”genocide or crimes against humanity, as defined by international law and recognised as such by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 April 1945, or of any other international court, established by relevant international instruments and whose jurisdiction is recognised by that Party.”

220 ”… denial, gross minimisation, approval or justification…”

221 KOM(2001)664.

222 Woltring, s. 603.

2.1.4.1 Kahdeksas kriminaalipoliittinen kongressi

Havannassa 1990 järjestetyssä Yhdistyneiden Kansakuntien kahdeksannessa kriminaalipoliittisessa kongressissa (the Eighth U.N. Congress on the Prevention of Crime and the Treatment of Offenders) olivat tietotekniikkarikokset (computer-related crimes) yhtenä teemana ja kongressin päätöslauselmassa edellytetään jäsenvaltioiden tehostavan toimenpiteitään taistelussa tietotekniikkarikollisuutta vastaan seuraavasti:[223]

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

Päätöslauselma myös edellyttää Yhdistyneiden Kansakuntien toimenpiteitä sellaisten ohjeiden ja standardien kehittämiseksi ja levittämiseksi, jotka ovat avuksi jäsenvaltiolle tietotekniikkarikosten kontrolloimisessa. Lisäksi päätöslauselma velvoittaa Yhdistyneet Kansakunnat edelleen kehittämään tutkimusta ja analysointia, jotta jäsenvaltiot vastaisuudessa voivat löytää uusia keinoja tietotekniikkarikosten käsittelemiseksi. Erityisesti päätöslauselmassa suositellaan *ad hoc* -asiantuntijakokouksen järjestämistä käsittelemään edellä mainittuja kysymyksiä. Tällainen kokous pidettiin Würzburgissa Saksassa lokakuussa 1992.[224]

2.1.4.2 Tietotekniikkarikoskäsikirja

Würzburgin kokouksessa käsiteltiin Kanadan oikeusministeriössä valmisteltua luonnosta Yhdistyneiden Kansakuntien tietotekniikkarikoksia koskevaksi käsi-

---

[223] UN Manual kohdat 16–19.

[224] Suomen edustajana kokouksessa oli tämän kirjoittaja. Lisäksi Suomesta kokoukseen osallistuivat *Raimo Lahti* ja *Matti Tenhunen.*

kirjaksi.[225] Lopullinen käsikirja (United Nations Manual on the Prevention and Control of Computer-related Crime) julkaistiin vuonna 1994.[226] Käsikirjassa määritellään sen tarkoitus seuraavasti:[227]

> The purpose of this Manual is to assist in developing a common framework for understanding the implications of computer-related crime for the entire world. Accordingly, it advises Member States of the nature of the problem, the inadequacies of current laws and the various solutions or proposals for action that have been recommended throughout the world. The Manual is not intended to be a comprehensive dissertation on computerrelated crime or on the legal problems inherent in addressing such crime. It does not mandate that particular courses of action should be taken, as would an international standard or guideline. Rather, the Manual seeks to be a working document, a blueprint for action, which Member States, faced with this new criminality, may use to better understand the problem, to become aware of some of the solutions that have been recommended, to develope their own response to the problem and to foster international cooperation. The Manual also identifies other sources of information to which Member States may turn to obtain more detailed information on a particular issue.

Yhdistyneiden Kansakuntien käsikirja siis poikkeaa sekä OECD:n että Euroopan neuvoston raporteista sikäli, että siinä ei anneta jäsenvaltioille minkäänlaisia lainsäädäntösuosituksia eikä edellytetä jäsenvaltioilta erityisiä toimenpiteitä.

Käsikirja jakaantuu johdantoon ja seitsemään lukuun. Johdannon jälkeen ensimmäisessä luvussa käsitellään tietotekniikkarikosta ilmiönä, toisessa ja kolmannessa luvussa käsitellään aineellista rikosoikeutta, ensin datan ja informaation haltijan suojan ja sitten yksityisyyden suojan kannalta, ja neljäs luku koskee prosessioikeudellisia kysymyksiä. Viidennessä luvussa käsitellään rikosten ehkäisemistä tietoteknisessä ympäristössä ja kuudes luku koskee kansainvälistä yhteistyötä. Würzburgin kokous ei juuri puuttunut näihin hyvin valmisteltuihin jaksoihin vaan keskittyi seitsemänteen lukuun, johon päätöslauselman luonteisesti on kirjattu johtopäätökset.

Käsikirjassa ei yritetä määritellä tietotekniikkarikoksen (computer crime tai computer-related crime) käsitettä. Käsitteen todetaan kattavan toisaalta joukon sellaisia rikollisia menettelyjä, jotka ovat luonteeltaan perinteisiä ja maailmanlaajuisesti rikosoikeudellisesti sanktioituja (varkaus, petos, väärennys, vahingonteko), toisaalta sellaisia uusia tietotekniikan luomia väärinkäytöksiä, joita olisi mahdollista tai joita pitäisi tarkastella rikoksina.[228]

---

[225] Käsikirjan kirjoittajina toimivat *Donald Piragoff, Larissa Easson* ja *John Neilly* Kanadasta, *Ulrich Sieber* Saksasta ja *Bart De Schutter* Belgiasta.
[226] International Review of Criminal Policy 43–44/1994.
[227] UN Manual, Preface.
[228] UN Manual, kohdat 20–26.

Esimerkkeinä tyypillisistä tietotekniikkarikoksista mainitaan tietojenkäsittelypetos (fraud by computer manipulation), tietotekniikkaväärennys (computer forgery), datan tai ohjelmiston vahingoittaminen tai muuttaminen (damage to or modification of computer data or programmes), tietomurto (unauthorised access to computer systems and services) ja luvaton kappaleiden valmistaminen suojatusta tietokoneohjelmasta (unauthorized reproduction of legally protected computer programmes).

Käsiteltäessä aineellista rikosoikeutta datan ja informaation haltijan suojan kannalta[229] käsikirjassa tehdään ero toisaalta informaation yksinomaiseen käyttöön (exclusive use of information) ja toisaalta datan koskemattomuuteen ja oikeellisuuteen (integrity and correctness of data) kohdistuvien rikosten välillä ja esitellään kansallisten lainsäädäntöjen kehittymistä mainittujen tekojen kriminalisoimisessa. Lisäksi selvitetään rikoslain kansainvälisiä harmonisointipyrkimyksiä kuvaamalla OECD:n, Euroopan neuvoston ja Yhdistyneiden Kansakuntien toimenpiteitä. Samaan tapaan käsitellään yksityisyyden rikosoikeudellista suojaa.[230]

Edellä mainittu erottelu dataan ja informaatioon kohdistuvien tekojen välillä vastaa pitkälti Suomessakin jossain määrin omaksuttua tietotekniikkarikosten jakoa toisaalta data- ja toisaalta informaatiorikoksiin. Käsikirjassa luetaan informaatiorikosten ryhmään myös immateriaalioikeuksiin kohdistuneet loukkaukset; tällainen luokittelu saattaa tuntua vieraalta, mutta jos ajatellaan vaikkapa tietokoneohjelman tekijänoikeuteen kohdistunutta loukkausta, lienee teossa asiallisesti kysymys enemmän immateriaaliseen informaatioon kuin materiaaliseksi katsottavaan dataan kohdistuvasta teosta.

Prosessioikeudellisista kysymyksistä[231] nousevat käsikirjassakin keskeisimmiksi pakkokeinojen käyttäminen (coercive powers of prosecuting authorities), henkilötietoihin liittyvät erityiset ongelmat (specific problems with personal data), tietoteknisen näytön hyväksyttävyys (admissibility of computer-generated evidence) sekä kansainvälinen harmonisointiyhteistyö, jonka todetaan jo alkaneen kaikilla kolmella edellä mainitulla ongelma-alueella.[232]

---

229 UN Manual, kohdat 84–126.

230 UN Manual, kohdat 127–145.

231 UN Manual, kohdat 146–184.

232 *Pakkokeinojen käytön* osalta käsikirjassa viitataan ns. Euroopan ihmisoikeussopimuksen (Yleissopimus ihmisoikeuksien ja perusvapauksien turvaamiseksi, Convention for the Protection of Human Rights and Fundamental Freedoms; Suomessa L 438/90, A 439/90) 8 artiklaan, joka kuuluu seuraavasti:

”1. Jokaisella on oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa ja kirjeenvaihtoonsa kohdistuvaa kunnioitusta.

2. Viranomaiset eivät saa puuttua tämän oikeuden käyttämiseen, paitsi silloin kun laki sen sallii ja se on demokraattisessa yhteiskunnassa välttämätöntä kansallisen ja yleisen turvallisuuden tai maan taloudellisen hyvinvoinnin vuoksi, tai epäjärjestyksen ja rikollisuuden estämiseksi, terveyden tai moraalin suojaamiseksi, tai muiden henkilöiden oikeuksien ja vapauksien turvaamiseksi.” (Teksti julkaistu SopS:ssa 19/90)

Tietotekniikkarikosten ehkäisemiseen tähtäävistä toimenpiteistä käsitellään viidennessä luvussa ensiksi tietoturvallisuuden lisäämistä. Tässä yhteydessä tietoturvallisuuden on katsottu muodostuvan seitsemästä eri osa-alueesta:[233]

1) hallinnollinen ja organisatorinen tietoturvallisuus (administrative and organizational security);
2) henkilöstöturvallisuus (personnel security);
3) fyysinen turvallisuus (physical security);
4) tietoliikenneturvallisuus (communications-electronic security);
5) laitteisto- ja ohjelmistoturvallisuus (hardware and software security);
6) käyttöturvallisuus (operations security); sekä
7) sattumanvaraissuunnittelu (contingency planning).[234]

Lainsäädännön kehittäminen ja lainkäyttäjien koulutus nähdään toisena keinona ehkäistä tietotekniikkarikollisuuden lisääntymistä. Tietotekniikan tuntemusta olisi lisättävä kaikilla lainkäyttösektoreilla ja erityisesti koulutuksen tulisi tähdätä seuraaviin yleisiin päämääriin:

1) lain perusteellinen tuntemus ja sen myötä kyky erottaa toisistaan siviili- ja rikosoikeudelliset vääryydet;
2) teknologian perusteellinen tuntemus;
3) niiden keinojen perusteellinen hallinta, joita käyttämällä todistusaineistoa voidaan hankkia ja säilyttää sekä esittää oikeudelle;

Artikla soveltuu Euroopan ihmisoikeustuomioistuimen käytännön mukaan mm. tilanteisiin, joissa on kysymys viranomaisten suorittamasta teleliikenteen valvonnasta tai kuuntelusta.

Henkilötietoihin liittyvien ongelmien osalta mainitaan Euroopan neuvoston toimenpiteet, joiden tuloksena on mm. syntynyt ns. tietosuojasopimus (Yksilöiden suojelua henkilötietojen automaattisessa tietojenkäsittelyssä koskeva yleissopimus, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data; Suomessa L 269/92, A 270/92, teksti julkaistu SopS:ssa 36/92). Sopimuksen 9 artikla antaa viranomaisille eräitä valtuuksia, kun kysymyksessä on valtiollisen tai yleisen turvallisuuden suojaaminen tai rikosten ehkäiseminen.

Tietoteknisen näytön hyväksyttävyyden osalta viitataan edellä jo mainittuun Euroopan neuvoston harmonisointisuositukseen R(81)20 (Harmonisation of laws relating to the requirement of written proof and to the admissibility of reproductions of documents and recordings on computers). Kysymystä on käsitelty myös CCC:ssä (Customs Cooperation Council) ja UNCITRAL:ssa (U.N. Commission on International Trade Law), minkä lisäksi Euroopan Yhteisöissä on tutkittu asiaa lähinnä liiketoimiin liittyvän näytön kannalta. Erityisesti rikosoikeuden alalta tuodaan esiin PC-R-CC:n suositukset ja YK:n kahdeksannen kriminaalipoliittisen kongressin päätöslauselma.

[233] Vrt. valtioneuvoston periaatepäätös tietoturvallisuuden kehittämisestä valtionhallinnossa 4.2.1993.

[234] Termi ”Contingency Planning” saattaa kaivata lisäselvitystä. Näin käsikirjan kohdassa 209: ”Every EDP system has been developed to perform some type of service or to fulfil a role. The plans for achieving the goals associated with that role are, in most instances, based on normal operating conditions. However, no amount of precautionary work can preclude the occurrence of situations that produce unexpected disruptions in routing operations. Contingency planning is therefore a basic requirement in the EDP security program, regardless of the sensitivity of the information processed or the size of the installation providing the service.”

4) tietotekniikkarikollisuuden kansainvälisen luonteen aiheuttamien ongelmien tuntemus; sekä
5) sekä rikoksesta epäillyn että rikoksen uhrin oikeuksien perusteellinen tuntemus.[235]

Ilman yhteistyötä tietotekniikkarikoksen uhrin ja viranomaisten välillä keinot tietotekniikkarikosten vähentämiseksi voivat olla ainoastaan osittain tehokkaita; yhteistyön tehostamisen keinojen osalta käsikirjassa viitataan edellä käsiteltyihin PC-R-CC:n näkemyksiin.

Viimeisenä tietotekniikkarikollisuuden ehkäisemisen keinona luvussa käsitellään tietojenkäsittelyetiikkaa (computer ethics), jollaisen tarpeellisuus todetaan ilmeiseksi mutta jollaista ei vielä ole kehittynyt – ”hyvästä tietojenkäsittelytavasta” tosin puhutaan, mutta käsitteen sisältö on täsmentymätön toisin kuin esimerkiksi ”hyvän kirjanpitotavan” tai ”hyvän asianajotavan” merkityssisältö.

Tietotekniikkaan ja sen käyttöön liittyvät erityiset eettiset ongelmat johtuvat tietokoneiden erityispiirteistä ja niistä toiminnoista, joihin tietokoneita käytetään. Tietojenkäsittelyetiikan kehittäminen edellyttää kaikkien nykyaikaisen yhteiskunnan sektorien toimenpiteitä niin paikallisilla, kansallisilla kuin kansainvälisilläkin tasoilla, joskin lopullinen hyöty (ultimate benefit) koituu koko ihmiskunnan hyväksi.

Kuudennessa luvussa[236] käsiteltävät kansainväliseen yhteistyöhön liittyvät kysymykset koskevat lähinnä prosessuaalista menettelyä. Yhteistyön tarpeellisuutta ja välttämättömyyttä perustellaan mm. seuraavasti:

> The international element in the commission of computer crime creates new problems and challenges for the law. Systems may be accessed in one country, the data manipulated in another and the consequences felt in a third country. Hackers can physically operate in one country, move electronically across the world from one network to another and easily access databases on a different continent. The result of this ability is that different sovereignities, jurisdictions, laws and rules will come into play. More than in any other transnational crime, the speed, mobility, flexibility, significance and value of electronic transactions profoundly challenge the existing rules of international criminal law.[237]

Ongelmien ratkaisemiseksi kansainvälisen yhteisön olisi erityisesti pyrittävä (1) maksimoimaan kansakuntien välinen yhteistyö sen selvittämiseksi, millai-

---

[235] An appropriate training program would, therefore, impart a thorough understanding in five areas: (1) the difference between a civil and a criminal wrong; (2) the technology; (3) proper means of obtaining and preserving evidence and of presenting it before the courts; (4) the intricacies of the international nature of the problem; (5) the rights and privileges of the accused and the victim. Käsikirjan kohdat 214–220.

[236] UN Manual, kohdat 239–288.

[237] UN Manual, kohta 241.

sia valtavien taloudellisten vahinkojen mahdollisuuksia ja millaisia uhkia yksityisyydelle ja muille yksilöiden perusarvoille valtioiden rajoja ylittävät elektroniset transaktiot saattavat luoda; (2) maailmanlaajuiseen suojaan sellaisia dataparatiiseja tai tietotekniikkarikossatamia vastaan, joihin tietotekniikkarikolliset voivat paeta tai joista käsin he voivat toimia; sekä (3) sellaiseen lailliseen yhteistyöjärjestelmään, joka ottaa huomioon yhtäältä kansainvälisen kaupan ja muiden suhteiden asettamat edellytykset sekä toisaalta yksilöiden oikeudet ja vapaudet.

Erityisistä kansainvälistä yhteistyötä edellyttävistä ongelmista käsitellään ensiksi *tuomiovaltaan* liittyviä kysymyksiä. Kun valtioiden rajoja ylittäneen tietotekniikkarikoksen tekopaikkaa määritellään, saattaa usea eri valtio katsoa olevansa kompetentti käsittelemään rikosta. Lopullista forumia etsittäessä joudutaan soveltamaan sellaisia yleisiä rikosoikeudellisia periaatteita kuin *non bis in idem*- tai *lex mitior* -sääntöjä sekä ottamaan huomioon yleisesti hyväksytty, valtion suvereenisuudesta johtuva alueperiaate.

Tekopaikan määritteleminen voi kuitenkin olla hankalaa: toisaalta yhden teon tekopaikaksi voidaan katsoa niin tosiasiallisen tekemisen kuin seurauksen tosiasiallisen ilmenemisenkin paikka; toisaalta *common law* -maissa sovellettavan doktriinin mukaan tekopaikaksi katsotaan se paikka, jossa teon vaikutukset oli tarkoitettu ilmenemään tai jossa ne tosiasiallisesti ilmenivät.

Positiivisten toimivaltaristiriitojen ratkaisemiseksi valtioiden tulisi (1) luoda nimenomainen järjestys tuomiovallan kriteereille; (2) kehittää mekanismi valtioiden välisille neuvotteluille toimivaltakysymysten ratkaisemiseksi; sekä (3) järjestää yhteistyö ylikansallisten tietotekniikkarikosten tutkimista, syytteeseenpanoa ja rankaisemista varten.

Lisäksi edellytetään exterritoriaalisen tuomiovallan osalta analysoitavan (1) aktiivista kansallisuusperiaatetta (active nationality principle), joka perustuu rikoksesta epäillyn kansallisuuteen; (2) passiivista kansallisuusperiaatetta (passive personality principle), joka puolestaan perustuu uhrin kansallisuuteen; (3) suojeluperiaatetta (protection principle), jonka perusteena ovat valtion intressit; sekä (4) yleismaailmallisten arvojen suojeluun perustuvaa universaaliperiaatetta (universality principle).

Esitutkintaan liittyy kysymys maasta toiseen tapahtuvasta tietojärjestelmiin kohdistuvasta etsinnästä. Perinteiset esitutkintaviranomaisten yhteistyömuodot ovat varsin aikaa vieviä, kun taas tietoteknisessä ympäristössä tehdyn rikoksen tutkinnan täytyy olla nopeaa ja tehokasta toimintaa. Suoran tunkeutumisen (direct penetration) rajoittamaton hyväksyminen merkitsisi kuitenkin valtioiden suvereenisuuden loukkaamista, joten valtioiden tulisi pyrkiä saamaan aikaan sopimuksia, joissa suora tunkeutuminen sallittaisiin mutta vain poikkeustilanteissa.[238]

---

[238] Vrt. edellä EN:n yhteydessä lausuttu.

Myös keskinäisen oikeusavun, luovuttamismenettelyn sekä syytteiden siirtomenettelyn kehittäminen helpottavat valtioiden rajoja ylittäneiden tietotekniikkarikosten käsittelyä. Nämä ongelma-alueet on kansainvälisesti – ainakin eurooppalaisesti – säännelty yleissopimuksilla eivätkä tietotekniikkarikokset näissä suhteissa ole missään erityisasemassa, vaan niihin liittyvät ongelmat ratkeavat yleisten sääntöjen mukaan.

Käsikirjan seitsemäs luku[239] sisältää päätöslauselmanomaiset johtopäätökset, jotka laadittiin Würzburgin kokouksessa.

Ottaen huomioon tele- ja tietoliikenteen kansainvälisen laajuuden, useiden tietotekniikkarikosten valtioiden välisiä rajoja ylittävän luonteen ja tämänhetkisten kansainvälisen yhteistyön keinojen rajallisuuden edellytetään käsikirjassa järjestelmällisiä kansainvälisiä pyrkimyksiä ongelmien selvittämiseen. Määrittelemällä tietotekniikkarikoksen käsite tai ainakin saavuttamalla yksimielisyys siitä, mitä käsite sisältää, samoin kuin harmonisoimalla prosessuaaliset säännökset sanktioiden toteuttamiseksi saavutettaisiin useita etuja:

a) Monikansallisten tietoverkkojen yleistymisen myötä näiden verkkojen haavoittuvuus lisääntyy ja luo mahdollisuuksia niihin kohdistuviin transnationaaleihin väärinkäytöksiin; järjestelmällistä kansainvälistä yhteistyötä voi tapahtua vain, jos on olemassa yhteisymmärrys siitä, mikä on tietotekniikkarikos tai mikä sen tulisi olla;
b) Kansainvälisen kaupan laajeneminen synnyttää tarvetta lainsäädäntöön, jolla turvataan taloudellisia etuja ja taloudellista toimintaa. Myös henkilötietojen käsittelyn automatisoituminen aiheuttaa vastaavasti tarvetta oikeudelliseen suojeluun niin kansallisella kuin kansainväliselläkin tasolla, varsinkin kun yksityisyyden suojaamisen merkitys on kasvanut;
c) Kansainvälinen lainsäädäntöjen harmonisointi lisää monikansallisten tietotekniikan hyödyntäjien mahdollisuuksia ennakoida tietojärjestelmien väärinkäyttämisen seuraamuksia, mikä edistää kansainvälisten investointimarkkinoiden luotettavuutta ja vakautta;
d) Siinä määrin kuin rikosoikeus synnyttää positiivisia käyttäytymisnormeja ja toteuttaa kasvatus- ja ehkäisytavoitteita, rikoslakien harmonisointi helpottaa kansainvälisten, tietokoneiden käyttämiseen liittyvien normien luomista;
e) Harmonisointi voi auttaa poistamaan erilaisia esteitä informaation vapaalta liikkumiselta ja teknologian siirrolta;
f) Niin rikos- kuin muidenkin lakien harmonisointi voi edistää yhtäläisten kilpailuedellytysten kehittymistä. Puutteellinen tietokoneohjelmien, teknologian ja liikesalaisuuksien suoja joissakin maissa saattaa johtaa jotkin yritykset menettelemään niissä tavalla, jota muualla pidettäisiin vilpillisenä kilpailuna;
g) Tehokkaampi harmonisointi voi estää tiettyjä valtioita muodostumasta ns. suojasatamiksi, joista käsin kansainvälisiä tietotekniikkari-

[239] UN Manual, kohdat 289–296.

koksia on mahdollista tehdä joutumatta rangaistusseuraamusten kohteeksi;

h) Harmonisointi helpottaa eri valtioiden viranomaisten tehokasta lakien soveltamista, koska se saa aikaan yhteisymmärryksen siitä, minkä tyyppinen menettely konstituoi rikoksen ylipäänsä ja tietotekniikkarikoksen erityisesti;
i) Aineellisen lainsäädännön harmonisointi helpottaa rikoksentekijän luovuttamismenettelyä, sillä luovutussopimukset yleensä edellyttävät kaksoiskriminalisointeja;
j) Harmonisointi helpottaa keskinäistä oikeusapumenettelyä, koska joissakin oikeusapusopimuksissa myös edellytetään kaksoiskriminalisointeja. Vaikkei tällaista edellytystä olisikaan, yhteneväinen käsitys siitä, mikä konstituoi rikoksen, edesauttaa oikeusavun antamista.
k) Aineellisen rikosoikeuden harmonisointi helpottaa tutkintaan liittyvän prosessuaalisen lainsäädännön harmonisoimista.

Tietotekniikkarikollisuuteen kohdistuvaa yhteistyötä edellytetään kehitettävän niin kansallisella kuin kansainväliselläkin tasolla. Kansallisella tasolla suositellaan perustettavaksi työryhmiä, joissa olisivat edustettuina hallitus, teollisuus ja tieteellinen tutkimus, käsittelemään keskeisiä kysymyksiä tutkimalla käytäntöä sekä analysoimalla kansallista tilannetta ja lainsäädäntöä.

Kansainvälisellä tasolla mainitaan esimerkkeinä niistä toimenpiteistä, joihin vastaisuudessa olisi aiheellista ryhtyä

a) tietotekniikkarikoksiin liittyvän aineellisen ja prosessioikeudellisen lainsäädännön vertaileva analysoiminen alueellisissa työryhmissä tai yhteisöissä;
b) pyrkiminen alueen valtioiden aineellisen ja prosessuaalisen lainsäädännön harmonisointiin laatimalla ohjeita, mallilakeja tai sopimuksia;
c) seuraavien kysymysten käsitteleminen neuvoteltaessa tai tarkistettaessa luovutusta, keskinäistä oikeusapua tai syytteiden siirtoa koskevia sopimuksia, ottamalla kuitenkin huomioon ihmisoikeudet mukaan lukien oikeus yksityisyyteen sekä valtioiden suvereenisuus:
   i) juridisen perustan varmistaminen valtioiden välisiä rajoja ylittäneen tietotekniikkarikoksen syytteeseen saattamiselle sekä mekanismien omaksuminen tuomiovaltaan liittyvien konfliktien ratkaisemiseksi;
   ii) velvoittaminen tekijöiden luovuttamiseen tai heidän syytteeseen saattamiseensa; sekä
   iii) keskinäisen oikeusavun helpottaminen erityisesti täytäntöönpanon, rajoja ylittävän etsinnän ja takavarikon sekä tietoliikenteen valvonnan ja seurannan suhteen.

Äsken lausuttu osoittaa myös Yhdistyneissä Kansakunnissa omaksutun sen ajatuksen, että alueellisella yhteistyöllä on mahdollista saavuttaa yleismaail-

mallista yhteistyötä tehokkaammin näkyviä tuloksia.[240] Tällaista alueellista yhteistyötä edustavat juuri edellä käsitellyt OECD:n ja Euroopan neuvoston puitteissa tehdyt toimenpiteet samoin kuin jäljempänä selostettavat toistaiseksi jokseenkin vähäiset Euroopan unionin toimet.

Johtopäätösjakson lopussa todetaan, että turvallisuuden lisäämisen ja rikosten ehkäisykeinojen on kehityttävä teknologian mukana. Käsikirja päättyy lakoniseen ja velvoittavaan toteamukseen: *"The time to act is now."*

Yhdistyneiden Kansakuntien käsikirja on ensimmäinen maailmanlaajuisen järjestön analyysi tietotekniikkarikollisuudesta ja sellaisena varsin tärkeä askel yleismaailmallisessa taistelussa tätä rikollisuuden lajia vastaan. Huomattava on, että käsikirja erityisesti materiaalisten kysymysten osalta tukeutuu paljolti Euroopan neuvoston vuoden 1989 raporttiin, mikä korostaa PC-R-CC:n työn merkittävyyttä.

2.1.4.3 Kymmenes kriminaalipoliittinen kongressi

Tietotekniikkarikokset olivat esillä myös toukokuussa 1995 Kairossa järjestetyssä yhdeksännessä kriminaalipoliittisessa kongressissa, tosin jokseenkin vaatimattomasti. Tilanne oli toinen viittä vuotta myöhemmin, huhtikuussa 2000 Wienissä, jolloin kymmenennessä kriminaalipoliittisessa kongressissa järjestettiin hyvin valmisteltu päivän mittainen cyber-crime-seminaari.[241]

Seminaari keskittyi tietoverkkorikosten esitutkintaan ja oli toteutukseltaan hyvin mielenkiintoinen, eräänlainen oikeustapausharjoitus, jossa maailman johtavat asiantuntijat ottivat kantaa tutkinnallisesti ongelmallisiin kysymyksiin. Seminaari ei antanut Suomelle varsinaisesti mitään uutta, mutta tietynlaiseksi anniksi on luettava sen havaitseminen, että Suomessa tietotekniikkarikosten tutkinta ilmeisestikin oli ja on aivan kansainvälisellä huipputasolla: ne tutkinnan keinot, joita esimerkiksi Yhdistyneen kuningaskunnan ja Yhdysvaltojen tietotekniikkarikostutkijat seminaarissa esittelivät, olivat lähes poikkeuksetta käytössä myös Suomessa. Useille Aasian, Afrikan ja Etelä-Amerikan valtioille seminaarin anti sen sijaan oli epäilemättä hyvin suuri.

---

[240] AIDP:n syksyn 1994 kongressissa oli yhtenä teemana kansainvälisen rikosoikeuden alueellistuminen; ao. päätöslauselman kohta 2: "Institutional arrangements for co-operation in criminal matters and other forms of legal co-operation should be incorporated into the activities of regional organizations which have been established for the development of closer co-operation within the region concerned in economic matters, the improvement of the freedom of movement of persons, goods and capital or for other forms of development of the region. Such legal co-operation should not only be directed towards the economic objectives of the regional organization, but also towards the general interests of each participating State." – RIDP:ssä 1–2/1994 ovat Rion kongressia tämän teeman osalta valmistelleen syyskuussa 1992 Helsingissä pidetyn kollokvion asiakirjat mukaan lukien kansalliset raportit. – Ks. myös Lahti, Kansainvälistyvä rikosoikeus, s. 192 ss.

[241] Suomesta seminaariin osallistuivat tämän kirjoittaja ja keskusrikospoliisin tietotekniikkarikosryhmän silloinen vetäjä, rikoskomisario Juha Härkönen.

2.1.5 Kansainvälinen rikosoikeusyhdistys AIDP

Kansainvälinen rikosoikeusyhdistys (L'Association Internationale de Droit Pénal, AIDP, the International Association of Penal Law, IAPL) on perustettu Pariisissa vuonna 1924, mutta sen juuret ovat *von Lisztin, van Hamelin ja Prinsin* vuonna 1889 Wienissä perustamassa Kansainvälisessä rikosoikeusunionissa. Ranskankielisestä nimestään johdetulla lyhenteellä AIDP yleisimmin tunnettu järjestö on maailman tärkein rikosoikeustieteilijöiden yhdistys, johon kuuluu yli 3 000 jäsentä noin 70 maasta. Yhdistys on ei-hallitustenvälinen järjestö (non-governmental organisation, ngo), joka on akkreditoitu Yhdistyneisiin Kansakuntiin, Euroopan neuvostoon ja Amerikan valtioiden järjestöön OAS:ään.

AIDP järjesti syyskuussa 1994 Rio de Janeirossa viidennentoista kansainvälisen rikosoikeuskongressin, jossa yhtenä neljästä teemasta olivat tietotekniikkarikokset (computer crimes and other crimes against information technology).[242] Lokakuussa 1992 AIDP järjesti Würzburgissa kongressia valmistelevan kollokvion, jossa mm. laadittiin ehdotus kongressin päätöslauselmaksi kansallisten raporttien pohjalta.[243]

Kollokvion yhteydessä järjestivät sekä Euroopan yhteisöt että – jo edellä mainituin tavoin – Yhdistyneet Kansakunnat omat konferenssinsa.[244] Würzburgin kollokvio on erittäin merkityksellinen siinä suhteessa, että kansalliset raportit, joita kollokvioon saapui kaikkiaan 29 maasta, muodostavat kattavan selvityksen tietotekniikkarikosten alueella tuohon mennessä tapahtuneesta kehityksestä ja lainsäädännöstä.

Raportit perustuvat professori *Ulrich Sieberin* laatimaan kommentaariin ja kyselyyn,[245] joka koski viittä eri osa-aluetta, nimittäin (1) empiiristä analyysiä, (2) yleistä oikeudellista kehitystä, (3) aineellista rikosoikeutta, (4) prosessioikeutta ja (5) kansainvälisiä ongelmia. Yleisraportin kollokviosta laati professori *Cole Durham.*[246]

Durham näkee, että rikosoikeudessa on noussut esiin uusi paradigma: kompleksisen keskinäisen riippuvuuden malli (the pattern of complex interdependence).[247] Luonteenomaista tälle uudelle ajattelutavalle on se kompleksisuus,

---

[242] Muina teemoina olivat ympäristörikokset, ihmisoikeuksien suojelu rikosprosessissa ja rikosoikeuden kansainvälistyminen. Tämän kirjoittaja osallistui tietotekniikkarikoksia käsitelleen jaoston työskentelyyn. Kongressin osanottajat edustivat 62 maata.

[243] Tämän kirjoittaja toimi kollokviossa Suomen raportöörinä. Kansalliset raportit on julkaistu RIDP:ssä n:o 1–2/1993, Suomen raportti s. 275 ss. Kaikkiaan kollokvioon osallistui edustajia 28 valtiosta.

[244] Ks. Sieberin toimittama Information Technology Crime, johon on koottu sekä kollokvion että konferenssien asiakirjat.

[245] Sieber, Commentary (englanninkielinen alkuperäisversio).

[246] RIDP 1–2/1993, s. 79 ss.

[247] "My major contention in this General Report is that we are witnessing the emergence of a fundamentally new pattern of criminality exemplified by criminal information law that I call the 'pattern of complex interdependence'." Durham, s. 86.

joka syntyy informaatioyhteiskunnassa elävien ihmisten yhä monimutkaisemmista ja yhä enemmän toisistaan riippuvista intresseistä. Paradigman merkityksen lisääntyminen on väistämätöntä, koska riippuvuus tietotekniikasta ja telekommunikaatiosta kasvaa, mikä puolestaan lisää ihmisten keskinäistä riippuvaisuutta toisistaan.[248]

Analysoituaan kansallisissa raporteissa esiin tulleita näkemyksiä *Durham* lopuksi toteaa analyysin vahvistavan hypoteesin, joka on kehittynyt alkaen siitä, että uusi tieto- ja telekommunikaatioteknologia on synnyttänyt rikosoikeudessa paradigman muutoksen. Kun substantiiviset eroavuudet vielä erottavat erilaiset oikeudelliset järjestelmät toisistaan, harmonisointipyrkimykset ja kokemukset uuden teknologian aiheuttamista ongelmista johtavat kohti merkittävää yhdentymistä.[249]

Würzburgin kollokviossa tehty työ oli perustana Riossa käydyille keskusteluille, joiden tuloksena kongressi hyväksyi 28-kohtaisen päätöslauselman.[250]

Päätöslauselma jakaantuu kuuteen jaksoon seuraavasti:

1) ei-rikosoikeudelliset ehkäisykeinot (*non-penal preventive measures*; kohdat 1–2);
2) aineellinen rikosoikeus (*substantive criminal law*; kohdat 3–11);
3) erityiset yksityisyyden suojaan liittyvät kysymykset (*specific issues of privacy protection*; kohdat 12–15);
4) prosessioikeus (*procedural law*; kohdat 16–20);
5) kansainvälinen yhteistyö (*international co-operation*; kohdat 21–23); sekä
6) tulevaisuuden työ (*future work*; kohdat 24–28).

Ei-rikosoikeudellisten keinojen sijoittamisella päätöslauselman ensimmäiseksi jaksoksi haluttiin korostaa näiden keinojen ensisijaisuutta suhteessa rikosoikeudellisiin keinoihin, joita tulisi käyttää ainoastaan *ultima rationa.* Tällaisina keinoina mainitaan muiden muassa vapaaehtoisten turvajärjestelyjen lisääminen tietokoneiden käyttäjien keskuudessa yleensä samoin kuin pakollisiin turvajärjestelyihin velvoittaminen tietyillä arkaluonteisilla sektoreilla, hallitusten toimesta tapahtuva tietoturvallisuuslainsäädännön, -politiikan ja -ohjeiston luominen ja käyttöön ottaminen, tietoturvallisuuden kehittäminen tietotekniikkaa hyödyntävissä yrityksissä ja tietotekniikkateollisuudessa, tietojenkäsittely-

---

248 Durham, s. 87.

249 Durham, s. 116 s.

250 Päätöslauselmaehdotuksesta käytyä keskustelua edelsi joukko eräiden Latinalaisen Amerikan maiden edustajien puheenvuoroja, joissa voimakkaasti kritisoitiin tällaisen rikollisuuden lajin ottamista kongressin yhdeksi teemaksi. Puheenvuoroissa tuotiin esille se erilainen merkitys, joka rikoslailla on vasta diktatuureista vapautuneissa valtioissa verrattuna esimerkiksi Pohjois-Amerikan ja Länsi-Euroopan valtioihin; myös korostettiin sitä, että valtaosa ko. maiden asukkaista ei edes tiedä, mikä tietokone on, saati sitten käyttäisi sitä rikoksentekovälineenä.

etiikan luominen ja kehittäminen, ammatillisten standardien kehittäminen tietojenkäsittelyteollisuudessa, viranomaisten ja rikosten uhrien yhteistyön edistäminen erityisesti tietotekniikkarikoksista ilmoittamisen suhteen sekä rikostutkintaa, syyteharkintaa ja tuomitsemistointa suorittavien henkilöiden kouluttaminen.

Aineellisen rikosoikeuden osalta tietotekniikka-avusteisten väärinkäytösten todetaan vaikuttavan niin tietotekniikkaan liittyviin taloudellisiin kuin yksityisyyteenkin liittyviin intresseihin joko niin, että tietojenkäsittelyä komponentteineen käytetään välineenä perinteisten arvojen loukkaamisessa, tai niin, että tietojenkäsittely on suorastaan väärinkäytösten objektina. Sikäli kuin tällöin loukataan tai vaarannetaan perinteisiä arvoja, voivat uudet tekotavat paljastaa aukkoja perinteisessä rikoslaissa.

Toisaalta tietotekniikan kehittyminen synnyttää uusia oikeudellista suojelua kaipaavia intressejä. Ellei perinteinen rikoslaki ole riittävä, on joko täydennettävä olemassa olevia säännöksiä tai kehitettävä uusia, mikäli ei-rikosoikeudelliset keinot eivät riitä. Muutoksia ja uusia säännöksiä hyväksyttäessä on kiinnitettävä huomiota säännösten täsmällisyyteen ja selkeyteen sekä tekojen objektiiviseen kuvaamiseen. Ylikriminalisointeja on vältettävä ja pyrittävä rajaamaan rikosoikeudellinen vastuu ainoastaan tahallisiin tekoihin liittyväksi.[251]

Päätöslauselmassa korostetaan OECD:n ja Euroopan neuvoston työn tärkeää merkitystä kriminalisoinnin kohteeksi suositeltavien menettelytapojen täsmentämisessä. Euroopan neuvoston suosituksessa luetellut teot hyväksytään sellaisinaan kriminalisointisuosituksen kohteiksi, kuitenkin niin, että vuoden 1989 jälkeen tapahtunut rikollisuuden lisääntymisen, informaatioaikakauden immateriaalisten intressien arvojen merkittävyyden ja potentiaalisten vahinkojen suuruuden vuoksi suositellaan myös Euroopan neuvoston suosituksen valinnaislistalla kuvattujen tekojen kriminalisoimista.

Lisäksi ehdotetaan eräiden Euroopan neuvoston suosituksen teonkuvausten täsmentämistä ja selkeyttämistä sekä myös muutamien suosituksessa mainitsemattomien tekojen kriminalisoimisen harkitsemista. Tällaisina uusina kriminalisoinnin kohteina mainitaan liikennöinti laittomasti hankituilla käyttäjätunnuksilla tai salasanoilla, muun tiedon hankkiminen luvattoman tietojärjestelmään tunkeutumisen keinoista sekä virusten ja vastaavien ohjelmien levittäminen. Erityisesti virusten, matojen ja muiden samankaltaisten ohjelmien aiheuttaman suuren vahingonvaaran vuoksi suositellaan tällaisiin vahingollisiin ohjelmiin kohdistuvaa tieteellistä keskustelua ja tutkimusta.

Yksityisyyden suojalle kehittyvä tietotekniikka luo uusia vaaroja. Suojelun merkitystä näissä olosuhteissa on korostettava ottaen kuitenkin huomioon yhteiskunnan tiedon vapaaseen kulkuun ja leviämiseen kohdistuvat intressit. Yk-

---

[251] Päätöslauselman kohdat 3–7.

sityisyyteen liittyviin intresseihin kuuluu myös kansalaisen oikeus päästä käsiksi niihin tietoihin, joita muut ovat hänestä koonneet.

Yksityisyyden suojelussa ei-rikosoikeudellisille keinoille on annettava etusija, erityisesti silloin, kun osapuolet ovat keskenään sopimussuhteessa. Rikosoikeudellisia säännöksiä tulee soveltaa vain silloin, kun siviilioikeudellinen tai tietosuojalainsäädäntö ei tarjoa riittäviä keinoja. Erityisesti rikosoikeudellisten säännösten tulee

- olla sovellettavissa vain vakavissa tapauksissa, varsinkin kun kysymyksessä ovat erittäin arkaluonteiset tiedot tai perinteisesti lailla suojattu luottamuksellinen informaatio;
- olla määritelty selkeästi ja täsmällisesti sen asemesta, että käytetään avoimia tai yleisiä lausekkeita, erityisesti suhteessa aineelliseen yksityisyyden suojaa tarkoittavaan lainsäädäntöön;
- määritellä rangaistavien tekojen törkeysasteet ja niiltä edellytettävä moitittavuus;
- olla ensisijaisesti rajoitettu koskemaan tahallisia tekoja; ja
- antaa syyttäjäviranomaisille mahdollisuus teon tyypistä riippuen ottaa huomioon asianomistajan syytteen nostamista koskevat toiveet.

Tulevaisuudessa edellytetään ryhdyttävän toimenpiteisiin niiden nimenomaisten tekojen määrittelemiseksi, jotka olisi kriminalisoitava. Päätöslauselmassa mainitaan tällaisina mahdollisina kriminalisointikohteina tahalliset salassapitovelvollisuuden loukkaukset sekä sellaiset vakavat henkilötietojen oikeudettoman kokoamisen, käytön, siirtämisen tai muuttamisen muodot, jotka vaarantavat henkilökohtaisia oikeuksia.

Prosessioikeuden osalta todetaan niin varsinaisten tietotekniikkarikosten kuin perinteisempienkin tietoteknisessä ympäristössä tehtyjen rikosten tutkinnan edellyttävän, että esitutkinta- ja syyttäjäviranomaisilla on käytettävissään riittävät pakkokeinot. Väärinkäytösten välttämiseksi kaikkien ihmisoikeuksia rajoittavien viranomaisten toimenpiteiden on perustuttava kansainvälisten ihmisoikeusstandardien kanssa sopusoinnussa oleviin selkeästi määriteltyihin lain säännöksiin. Ottaen huomioon tällaiset yleiset periaatteet tulisi selkeästi määritellä

a) oikeus etsinnän ja takavarikon suorittamiseen tieto-teknisessä ympäristössä, erityisesti ottaen huomioon aineettomaan kohdistuva takavarikko ja tietoverkossa tapahtuva etsintä;
b) asianomistajien, todistajien ja muiden tietotekniikan käyttäjien (epäiltyä lukuun ottamatta) velvollisuus aktiiviseen yhteistyöhön (erityisesti informaation saattamiseksi sellaiseen muotoon, että se on käytettävissä oikeudellisiin tarkoituksiin); ja
c) oikeus tietojärjestelmän sisäisen tai järjestelmien välisen tietoliikenteen seuraamiseen sekä näin hankitun todistusaineiston käyttö tuomioistuinmenettelyssä.

Tiedon liikkuvuus kansainvälisessä televerkostossa ja nykyaikaisen tietoyhteiskunnan erittäin tiiviit vuorovaikutussuhteet tekevät *kansainvälisen yhteistyön* tietotekniikkarikosten ehkäisemisessä ja syytteeseensaattamisessa erityisen tärkeäksi.

Kun tietyt kansainvälisen yhteistyön muodot (rikoksentekijän luovuttaminen ja myös keskinäinen oikeusapu) saattavat edellyttää kaksoisrangaistavuutta ja kun voimassa oleva laki saattaa rajoittaa joidenkin valtioiden mahdollisuuksia avun antamiseen, sekä aineellisen lain harmonisointi että riittävien pakkokeinojen mahdollistaminen edesauttaisivat tehokasta kansainvälistä yhteistyötä. Lisäksi yhteistyö nähdään tarpeelliseksi kehitettäessä

a) kansainvälisiä standardeja tietojärjestelmien turvallisuudelle;
b) riittäviä keinoja tuomiovaltaan liittyvien ongelmien ratkaisemiseksi, kun kysymyksessä ovat valtioiden välisiä rajoja ylittävät tai muuten kansainväliset tietotekniikkarikokset; sekä
c) kansainvälisiä uuden tietoteknologian huomioon ottavia, tietotekniikkarikosten tutkintaa tehostavia sopimuksia, mukaan lukien sopimukset rajoja ylittävästä etsinnästä ja takavarikosta tietoverkoissa samoin kuin muut kansainvälisen yhteistyön muodot, unohtamatta kuitenkaan yksilöiden perusoikeuksien ja -vapauksien suojelua.

Tulevaisuudessa tehtävän työn osalta korostetaan edellä mainittujen tavoitteiden saavuttamiseksi tapahtuvaa tieteellisten yhteisöjen, viranomaisten, tietotekniikan ammattilaisten sekä kansainvälisten järjestöjen toimenpiteitä esitettyjen suositusten voimaan saattamiseksi ja jatkuvaa sellaisten rikosten ehkäisemiskeinojen hyväksymistä, jotka vastaavat informaatiotekniikan uusiin haasteisiin.

Akateemisen ja tiedeyhteisön samoin kuin hallitusten on huolehdittava jatkuvasta tietotekniikkarikoksia koskevasta tutkimuksesta, jonka tulee erityisesti kohdistua tietotekniikkarikosten tekotapoihin ja niillä aiheutettujen vahinkojen määrään samoin kuin tekijöiden erityispiirteisiin. Myös on tutkittava niitä vaihtoehtoja, jotka mahdollistavat rikosoikeudellisten keinojen käyttämisen *ultima rationa.*

Poliisi- ja syyttäjäviranomaisten tulee niin kansallisella kuin kansainväliselläkin tasolla tehostaa taistelua tietotekniikkarikollisuutta vastaan ja koordinoida toimenpiteitään tehokkaan globaalisen suojan aikaansaamiseksi. Laitteistoja ohjelmistovalmistajien sekä kuluttajien yhteenliittymien olisi osallistuttava tietotekniikkarikoksista käytävään keskusteluun.

Edellä on jokseenkin pääpiirteittäisesti selostettu AIDP:n Rion kongressin tietotekniikkarikoksia koskevan päätöslauselman sisältöä. Myös tämä päätöslauselma perustuu paljolti Euroopan neuvoston raporttiin ja tällä tavoin osaltaan korostaa PC-R-CC:n työn merkitystä tietotekniikkarikoksia koskevan kansainvälisen yhteistyön suunnan osoittajana. Kuitenkin verrattaessa AIDP:n pää-

töslauselmaa Euroopan neuvoston raporttiin ja siinä esitettyihin suosituksiin voidaan ajattelutavassa havaita viidessä vuodessa tapahtuneen selvää kehitystä, joka on suoraan verrannollinen teknologiassa tapahtuneeseen kehitykseen.

Kun Euroopan neuvosto asettaa vielä etusijalle kansalliset – tosin kansainväliseen tasoon vaikutuksensa ulottavat – toimenpiteet, on AIDP:n päätöslauselma hengeltään hyvin kansainvälinen ja globaalisen yhteistyön merkitystä korostava unohtamatta kuitenkaan valtionsisäisen lainsäädäntötoiminnan tärkeyttä.

2.1.6 Euroopan unioni

2.1.6.1 COMCRIME-projekti

Euroopan unionissa ei sanottavasti pohdittu tietotekniikkarikollisuutta ennen vuotta 1996, jolloin komissio käynnisti ns. COMCRIME-projektin. Siinä kartoitettiin Würzburgin yliopistolta ostetussa tutkimuksessa tietotekniikkarikoksia koskevan lainsäädännön tila unionin jäsenvaltioissa sekä eräissä sen ulkopuolisissa maissa eli Kanadassa, Japanissa ja Yhdysvalloissa. Projektin toteutus tapahtui paljolti AIDP:n edellä selostettuun työhön tukeutuen ja samojen henkilöiden toimesta.[252]

Tutkimus perustui – AIDP:n selvityksen tavoin – kansallisiin raportteihin, joiden pohjalta professori *Sieber* on laatinut perusteellisen yleisraportin,[253] johon palaan soveltuvin osin jäljempänä. Kansalliset raportit on myös tarkoitus julkaista, joko painettuna tai verkkoversiona.[254] Lisäksi projektiin kuuluu tietotekniikkarikoksia koskevaa lainsäädäntöä sisältävän Internet-pohjaisen, jatkuvasti päivitettävän tietopankin luominen; tämäkin on vielä keskeneräisessä vaiheessa. Huhtikuussa 1998 komissio esitteli tutkimuksen tulokset Euroopan unionin neuvostolle.

2.1.6.2 Komission tiedonanto

Lokakuussa 1999 Tampereella pidetyssä Eurooppa-neuvoston kokouksessa päätettiin, että myös huipputekniikkaan liittyvälle rikollisuudelle tulisi kehittää yhteiset tunnusmerkistöt ja seuraamukset. Tampereen kokouksen päätelmien toteuttamiseksi komission tietoyhteiskunta- ja oikeus- ja sisäasiain pääosastot järjestivät joulukuun 1999 ja huhtikuun 2000 välisenä aikana kolme kokousta teemalla ”Creating a Safer Information Society”. Kokouksissa oli edustettuina

---

[252] Käytännön toteutuksesta vastasivat silloinen Würzburgin (nyttemmin Münchenin) yliopiston professori *Ulrich Sieber* aineellisen rikosoikeuden osalta ja Amsterdamin Vriej-yliopiston professori *Henrik Kaspersen*, joista jälkimmäinen on toiminut myös Euroopan neuvoston PC-CY-komitean puheenjohtajana. Suomen puolesta projektiin osallistui tämän kirjoittaja.

[253] ”Legal Aspects of Computer-Related Crime in the Information Society – COMCRIME-Study”; versio 1.0 (Volume 1 – General Report) on julkaistu tammikuussa 1998. Ajantasaistettua versiota varten on kerätty tietoa vuoden 2000 kuluessa mutta se ei ole vielä ilmestynyt.

[254] Alkuvuoteen 2004 mennessä niitä ei ollut julkaistu.

lähinnä jäsenvaltioiden lainkäyttöviranomaisia, mutta erityisesti viimeisessä kokouksessa paikalla oli myös yksityisen sektorin eli verkkopalveluiden tarjoajien sekä laitteisto- ja ohjelmistoteollisuuden edustajia.[255]

Kokouksissa käytyjen keskustelujen perusteella komissio on laatinut neuvostolle, Euroopan parlamentille, talous- ja sosiaalikomitealle sekä alueiden komitealle tiedonannon ”Turvallisempaan tietoyhteiskuntaan tietojärjestelmien turvallisuutta parantamalla ja tietokonerikollisuutta[256] ehkäisemällä”.[257]

Tiedonannon jaksossa ”Päätelmät ja ehdotukset” todetaan tietotekniikkarikollisuuden ehkäisemisen ja tehokkaan torjunnan edellyttävän ensinnäkin muun muassa, että

– käytettävissä on ennalta ehkäisevää tekniikkaa;
– turvallisuusriskit tiedostetaan ja osataan torjua;
– käytössä on riittävät aineelliset ja prosessioikeudelliset säännöt, jotka koskevat sekä kansallista että kansainvälistä rikollisuutta;
– koulutettuja lainvalvontaviranomaisia on riittävästi ja heillä on käytössään asianmukaiset välineet;
– kaikkien toimijoiden (käyttäjien, kuluttajien, alan yritysten sekä lainvalvonta- ja tietosuojaviranomaisten) yhteistyötä tehostetaan;
– alan yritysten ja yhteisön johdolla toteutettavia aloitteita jatketaan; sekä että
– tutkimus- ja kehitystoiminnan saavutukset ja mahdollisuudet hyödynnetään mahdollisimman tehokkaasti.

Varsinaisina säädösehdotuksina komissio esittää seuraavat ehdotukset:

– ehdotus lapsipornografiarikoksia koskevan jäsenvaltioiden lainsäädännön lähentämisestä;
– ehdotus rikosoikeuden aineellisten sääntöjen lähentämisestä entisestään huipputekniikkaan liittyvän rikollisuuden osalta; tässä mainitaan erityisesti tietojärjestelmään murtautuminen ja ruuhkauttamishyökkäyksiin liittyvät rikokset[258] ja niiden ohella myös Internetissä esiintyvä rasistinen ja muukalaisvastainen toiminta samoin kuin huumeiden Internet-kauppa; sekä

---

[255] Suomea kokouksissa edusti tämän kirjoittaja; viimeisessä kokouksessa oli mukana myös Karoliina Rasi-Hedberg Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry:stä.

[256] Tiedonannon virallisessa suomennoksessa todellakin käytetään sanaa ”tietokonerikollisuus”. On muistettava, että EU-käännösten juridiseen täsmällisyyteen ja käytettyjen sanojen asianmukaisuuteen on syytä suhtautua tietyllä varauksellisuudella: tosiasiallisesti todistusvoimaisin teksti on yleensä englanninkielistä ja vaikka englanniksi vielä jossain määrin käytetäänkin termiä ”computer crime”, on sen täysin vakiintunut suomenkielinen vastine ”tietotekniikkarikos”. Käytän itse tätä viimeksi mainittua sanaa tässä(kin) yhteydessä tiedonannon sisältöä kuvaillessani.

[257] Asiakirja KOM(2000) 890 lopullinen.

[258] Otan osaksi takaisin sen, mitä sanoin edellä EU-käännöksistä: ruuhkauttamishyökkäys ei ole ollenkaan huono sana kuvaamaan menettelyä, joka englanniksi tunnetaan nimellä ”spamming” ja jota Suomessa on kutsuttu spammaukseksi tai spämmäykseksi. Kysymyksessä on esimerkiksi ns. roskapostin lähettäminen eli lukumääräisesti tai kooltaan poikkeavan suurten sähköpostisanomien lähettäminen puhtaasti ilkivaltaisessa tarkoituksessa.

– ehdotus vastavuoroisen tunnustamisen periaatteen soveltamisesta ennen oikeudenkäyntiä annettuihin määräyksiin ja vähintään kahta jäsenvaltiota koskevien tietotekniikkarikostutkimusten helpottamiseksi.

Lisäksi komissio arvioi tarvetta toteuttaa teleliikennetietojen säilyttämisen osalta lainsäädännöllisiä ja muita toimenpiteitä perustettavaksi ehdottamansa Euroopan unionin keskustelufoorumin tulosten perusteella ja muita osapuolia kuultuaan.

Muilla osa-alueilla komissio ehdottaa seuraavia toimenpiteitä:

– komissio perustaa unionin keskustelufoorumin, jolla se toimii puheenjohtajana ja jolla lainvalvontaviranomaiset, palveluntarjoajat, verkko-operaattorit, kuluttajaryhmät ja tietosuojaviranomaiset pyrkivät tehostamaan yhteistyötään unionin tasolla tuomalla yleiseen tietoisuuteen Internetiä käyttävien rikollisten aiheuttamat riskit, edistämällä tietotekniikan turvallisuuden kannalta parhaita käytäntöjä, kehittämällä tehokkaita rikoksentorjuntavälineitä ja -keinoja tietotekniikkarikollisuuden kitkemiseksi sekä edistämällä ennakkovaroitus- ja kriisinhallintajärjestelmien jatkokehittelyä;[259]
– komissio edistää edelleen turvallisuutta ja luottamusta *e*Europe-aloitteen, Internet-toimintasuunnitelman, IST-ohjelman ja seuraavan TTK-puiteohjelman avulla;
– komissio edistää nykyisten ohjelmien avulla uusia hankkeita, joilla tuetaan lainvalvontaviranomaisille annettavaa koulutusta huipputekniikkaan liittyvää rikollisuutta koskevissa asioissa ja edistetään tietotekniikkarikosten jälkien tutkimista; sekä
– komissio tutkii mahdollisuuksia parantaa COMCRIME-tutkimuksen yhteydessä laaditun kansalliset lait käsittävän tietokannan sisältöä ja käynnistää tutkimuksen, jonka tarkoituksena on aiempaa paremmin selvittää jäsenvaltioissa harjoitettavan tietotekniikkarikollisuuden luonne ja laajuus.

Lisäksi komissio pyrkii edelleen aktiivisesti koordinoimaan tietoverkkorikollisuutta koskevia jäsenvaltioiden kannanottoja Euroopan neuvostossa[260],

---

[259] Tässä tarkoituksessa komissio järjesti marraskuussa 2001 ensimmäisen ”EU-forum on Cyber-crime”-konferenssin, joka kokosi kolmattasataa asiantuntijaa paitsi EU-maista myös hakijamaista ja muistakin EU:n ulkopuolisista valtioista keskustelemaan tunnistamistietojen (traffic data) säilyttämisvelvollisuudesta. Keskusteluissa erottui kolme eri rintamaa: lainkäyttäjät (law enforcement), palveluntarjoajat sekä yksityisyyden suojan puolestapuhujat, joista ensin mainitut olivat säilyttämisvelvollisuuden kannalla, operaattorit periaatteessa kannattivat mutta olivat huolissaan kuluista ja viimeksi mainitut vastustivat.

[260] Euroopan neuvoston verkkorikoskonventioneuvotteluja silmällä pitäen Brysselissä tehtiin Saksan puheenjohtajuuskaudella yksi yhteinen kanta, joka oli jokseenkin yleisluonteinen. Suomen kaudella tällaista ei yritetty, sillä neuvottelujen silloisessa vaiheessa tähän ei nähty tarvetta. Portugalin puheenjohtajuuskaudella yksityiskohtaisempaa yhteistä kantaa yritettiin tehdä siinä onnistumatta; syynä oli aivan liian nopea aikataulu. Ranskan kaudella käytiin koordinaatiokeskusteluja mutta yhteisen kannan syntymisestä ei ollut puhettakaan; viimeisessä PC-CY:n kokouksessa Ranska esiintyi aivan omilla linjoillaan ja osaltaan vaikutti käyttäytymisellään siihen, että PC-CY ei saanut työtään valmiiksi. Ranskan sooloilu jatkui CDPC:n kokouksessa kesäkuussa 2001.

G8-maiden kokouksissa ja muissa kansainvälisissä yhteyksissä.[261]

2.1.6.3 Komission puitepäätösehdotus

Huhtikuussa 2002 komissio antoi ehdotuksen neuvoston puitepäätökseksi tietojärjestelmiin kohdistuvista hyökkäyksistä.[262] Ehdotuksen mukaan kriminalisoitavia menettelyjä olisivat tietomurto (illegal access to information systems) ja tietojärjestelmän häirintä (illegal interference with information systems). Ehdotetussa muodossaan puitepäätös ei menisi juurikaan Euroopan neuvoston yleissopimusta pidemmälle eikä sillä ilmeisesti olisi sellaisia vaikutuksia Suomen oikeuteen, jotka edellyttäisivät yleissopimuksen implementoimista pitemmälle meneviä lainmuutoksia. Tätä helmikuussa 2004 kirjoitettaessa puitepäätöksen työryhmäkäsittely unionin neuvostossa on vielä kesken.

2.1.7 Kokoavia huomioita kansainvälisestä yhteistyöstä ja sen merkityksestä

Monessa yhteydessä on jo tullut selväksi se, että erityisesti Euroopan neuvoston vuoden 1989 suosituksen merkitys suomalaiselle lainsäädännölle on ollut suuri. Ei kuitenkaan sovi väheksyä muissakaan järjestöissä tehtyä työtä, sillä itse asiassa kysymyksessä on ollut sama jatkuva prosessi. Syynä on yksinkertaisesti se, että työhön osallistuneiden henkilöiden ydinjoukko on pysynyt pitkään samana: erityisesti *Ulrich Sieber* ja *Manfred Möhrenschlager* Saksasta, *H.W.K. Kaspersen* Alankomaista, *Donald Piragoff* Kanadasta ja *Martha Stansell-Gamm* Yhdysvalloista sekä *Matti Tenhunen* Suomesta ovat olleet merkittävillä panoksilla mukana vaikuttamassa useimpiin edellä selostettuihin hankkeisiin, eikä tällainen henkilöllinen jatkuvuus tietenkään voi olla vaikuttamatta siihen, millaiseksi kulloinenkin työ muodostuu – olkoonkin, että toimeksiannot tietysti aina ovat erilaisia eikä työn substanssi aina ole sama.

1980-luvun puolivälissä, kun OECD:n asiantuntijatyöryhmä suoritti toimeksiantoaan, oli tietotekniikkarikos käsitteenä varsin uusi ja outo. Tähän nähden – jälkiviisaus on aina helppoa – työryhmä onnistui erittäin hyvin kartoittamaan keskeisimmät tietotekniikkarikollisuuteen liittyvät ongelmat. OECD:n suositus

---

[261] Kesäkuussa 2001 komissio järjesti asiantuntijakokouksen, jonka perusteella päätettiin Belgian puheenjohtajuuskaudella vuoden 2001 jälkipuoliskolla ryhtyä unionin neuvoston alaisessa työryhmässä valmistelemaan tietotekniikkarikoksia koskevaa instrumenttia. Näin ei kuitenkaan tapahtunut.

[262] KOM(2002) 173 lopullinen. Englanniksi asiakirjan nimi on ”Proposal for a Council framework decision on attacks against information systems”. Ehdotuksen julkaistu suomenkielinen versio on malliesimerkki epäonnistuneesta EU-käännöksestä. Suomen- ja englanninkieliset versiot poikkeavat toisistaan oleellisissa kohdin ja kun ehdotus lienee valmisteltu englanninkielisen version pohjalta, voidaan suomenkielistä versiota pitää virheellisenä.

jäi luonnollisesti ylimalkaiseksi ja pääpiirteittäiseksi mutta voidaan kyllä perustellusti sanoa, että tuokin suositus on Suomen lainsäädäntöön implementoitu, sillä Euroopan neuvoston vuoden 1989 suositus on selvä OECD:n suosituksen huomattavasti pitemmälle viety kehitelmä.

AIDP:n vuoden 1994 kongressin päätöslauselma perustuu pääosin Euroopan neuvoston suositukseen, joskin sitä on hieman täydennetty viiden vuoden kuluessa tapahtuneen teknisen kehityksen johdosta. Syksyn 1992 Würzburgin konferenssissa, jonka yhteydessä järjestettiin AIDP:n kongressin päätöslauselmaa valmisteleva kollokvio, valmisteltiin Yhdistyneiden Kansakuntien tietotekniikkarikoskirjan teksti, joka näin muodoin heijastelee hyvin pitkälti samoja näkemyksiä kuin AIDP:n päätöslauselma – ja OECD:n ja Euroopan neuvoston suositukset.

Euroopan unionin kohdalla tilanne on hieman erilainen. Ensinnäkään unioni ei ole kovin pitkään työskennellyt muiden kuin yhteisön taloudellisiin etuihin liittyvien rikosoikeudellisten kysymysten parissa ja toiseksi tietotekniikkarikoksiin liittyvä työ on alkanut laittomiin sisältöihin liittyvistä ongelmista. Varsinaisia tietojenkäsittelyrauhaa loukkaavia rikoksia koskevia kysymyksiä ei toistaiseksi ole käsitelty muuten kuin keskustelemalla siitä, olisiko joihinkin toimenpiteisiin aihetta, ja antamalla edellä mainittu ehdotus puitepäätökseksi.

Nyt kun unionissa on ryhdytty laatimaan jäsenvaltioita velvoittavia instrumentteja, on oletettavissa tai ainakin mahdollista, että niiden määräykset tulevat menemään olemassa olevien instrumenttien säännöksiä pitemmälle, sillä kaikki unionin jäsenvaltiot ovat jäseninä niin OECD:ssä ja Yhdistyneissä Kansakunnissa kuin Euroopan neuvostossakin, joissa voimaan saatetut suositukset ja määräykset näin ollen koskevat unionin jäsenvaltioita jo sellaisinaan. Kuitenkin yksi keskusteluissa esille tullut syy esimerkiksi puitepäätösten tarpeellisuudelle on se, että Euroopan neuvoston yleissopimusten voimaan saattaminen kestää yleensä sangen kauan, kun taas unionin jäsenvaltiot voidaan velvoittaa implementoimaan puitepäätökset hyvinkin nopeasti. Näin ollen puitepäätösmenettelyä käyttämällä tärkeimmät määräykset ovat saatettavissa voimaan huomattavasti nopeammin kuin tyytymällä odottamaan Euroopan neuvoston yleissopimuksen implementoimisia ja voimaan tulemisen ehdoksi asetetun ratifiointien määrän saavuttamista.

Maailmanlaajuisesti ehdottomasti merkittävintä työtä on äsken sanotusta huolimatta joka tapauksessa tähän mennessä tehty Euroopan neuvostossa, jonka verkkorikoskonventio on kaikille valtioille avoin. Yhdistyneet Kansakunnat ei toistaiseksi ole nähnyt tarpeelliseksi ryhtyä laatimaan sopimusta. Euroopan tasolla Euroopan neuvostossa tehtyä työtä tulevat ennen pitkää täydentämään Euroopan unionissa tehtävät toimenpiteet, joiden ulottuvuus ei tietenkään ole alueellisesti yhtä laaja (mutta saattaa toki lähivuosina laajeta unionin laajetessa, tuskin kuitenkaan kovin pitkälle yli Euroopan rajojen).

Suomi on tunnetusti tunnollinen kansainvälisten suositusten ja sopimusten noudattaja ja näin on laita myös tähänastisten tietotekniikkarikossuositusten

kohdalla. Suomen rikoslaki on osoittautunut hyvin joustavaksi, eikä Euroopan neuvoston verkkorikoskonventionkaan implementointi näytä edellyttävän kovin monia muutoksia lainsäädäntöömme ainakaan aineellisen rikoslain osalta. Tähän on epäilemättä yhtenä syynä se, että Euroopan neuvoston vuoden 1989 suositusta on meillä noudatettu erinomaisen hyvin ja, kuten sanottu, tietotekniikkarikoksen peruskaava on 30 vuoden ajan pysynyt ennallaan: oikeudeton tunkeutuminen tietojärjestelmään ja tunkeutumista mahdollisesti seuraavat muut oikeudettomat toimet.

2.2 ERÄIDEN VALTIOIDEN LAINSÄÄDÄNNÖSTÄ

Suomessa on ryhdytty tietotekniikkarikoksia koskeviin lainsäädäntöhankkeisiin 1980-luvun jälkipuoliskolla. Edellisellä vuosikymmenellä virinnyt kiinnostus tietotekniikkarikoksia koskevaan tutkimukseen on saanut aikaan sen, että useissa läntisen Euroopan valtioissa lainsäädännöllinen tilanne on hyvin samankaltainen: joko kriminalisoinnit ovat varsin uusia tai sitten niitä parhaillaan valmistellaan. Suomella ei ole mitään syytä hävetä vertailussa muihin valtioihin: tietotekniikkarikoksia koskeva lainsäädäntömme on maailman kattavimpiin kuuluvaa ja kriminalisoinnit vastaavat hyvin edellä käsiteltyjä kansainvälisiä lainsäädäntösuosituksia.

Tässä jaksossa tarkastelen lähemmin tietotekniikkarikoksia koskevaa sääntelyä Ruotsissa, Tanskassa, Saksassa ja Yhdistyneessä kuningaskunnassa. Lopuksi esitän ylimalkaisen katsauksen eräiden muiden valtioiden tilanteisiin.

Ruotsi ja Tanska on valittu tarkastelun kohteeksi pohjoismaiden edustajina, Saksa sen merkityksen vuoksi, joka saksalaisella rikosoikeustieteellä on ollut suomalaiseen, ja Yhdistynyt kuningaskunta muista poikkeavan oikeusjärjestelmän edustajana. Ruotsissa, Tanskassa ja Saksassa on valittu samankaltainen lainsäädäntötekniikka kuin meilläkin, sen sijaan Britanniassa on päädytty toisenlaiseen vaihtoehtoon.

2.2.1 Ruotsi

Ruotsin *datalagen* vuodelta 1973 (1973:289) oli yksi maailman ensimmäisistä nykyaikaisen tietotekniikan käyttöön ja myös väärinkäyttöön kohdistuvista sääntelyhankkeista.[263] Sen päätarkoituksena oli estää sellaisten henkilötietojen tietoteknisin keinoin tapahtuva tallentaminen, joiden käyttäminen saattaisi vaarantaa asianomaisen henkilön yksityisyyttä.[264] Materiaaliselta sisällöltään suo-

[263] Ks. Jareborg, RIDP 1–2/93, s. 575.
[264] Solarz, s. 49 ss. ja SOU 1993:10, s. 319.

malaista henkilötietolakia muistuttavan lain tietotekniikkarikosten kannalta merkityksellinen säännös oli sen tietomurtoa *(dataintrång)* koskeva 21 § (SFS 1986:122), joka nyttemmin on korvattu samansisältöisellä, 24.10.1998 voimaan tulleella *brottsbalkenin* neljännen luvun (Om brott mot frihet och frid) 9 c §:llä:

> Den som i annat fall som sägs i 8 och 9 §§ olovligen bereder sig tillgång till upptagning för automatisk databehandling eller olovligen ändrar eller utplånar eller i register för in sådan upptagning döms för *dataintrång* till böter eller fängelse i högst två år. Med upptagning avses härvid även uppgifter som är under befordran via elektroniskt eller annat liknande hjälpmedel för att användas för automatisk databehandling.

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

Kun *datalagen* kokonaisuudessaan tarkoitti suojata yksilön loukkaamattomuutta, annettiin 21 §:ssä määräyksiä, jotka oli tarkoitettu sovellettaviksi myös muihin kuin henkilötietoja sisältäviin tiedostoihin. *Solarz* asettikin kysymyksenalaiseksi sen, oliko soveliasta antaa lain yhdelle säännökselle sellainen sovellettavuuden ala, joka ulottui paljon laajemmalle kuin *datalagenin* muutoin säännöstämiin yksityisyyden suojaan liittyviin kysymyksiin.[265]

Tietomurtokriminalisointi on toissijainen, ja usein tunnusmerkistön mukainen teko toteuttaa jonkin muun *brottsbalkenissa* tarkoitetun rikoksen tunnusmerkistön – esimerkiksi varkauden, petoksen, vahingonteon, luvattoman käytön tai telesalaisuuden rikkomisen.[266] *Brottsbalkeniin* tietotekniikkarikoksia koskevia säännöksiä lisättiin vuonna 1986 (SFS 1986:122–123); säännösten syntymiseen vaikutti muun muassa se, että Ruotsi oli edustettuna OECD:n vuoden 1986 raporttia laatineessa työryhmässä,[267] joskin tuolloinen varallisuusrikoksia koskenut lainuudistus paljolti perustui jo huomattavasti aikaisemmin aloitettuun selvitystyöhön.[268]

Vuoden 1986 lainuudistuksen jälkeen *brottsbalkenissa* on säännökset tietojenkäsittelypetoksesta,[269] luottamusaseman väärinkäytöstä[270] ja luvattomasta

---

[265] Solarz, s. 55.
[266] Jareborg, RIDP 1–2/93, s. 577.
[267] Solarz, s. 41.
[268] Ks. SOU 1983:50, erit. s. 169 ss.
[269] BrB 9:1.2 (SFS 1986:123): För bedrägeri döms också den som genom att lämna oriktig eller ofullständig uppgift, genom att ändra i program eller upptagning eller på annat sätt olovligen påverkar resultatet av en automatisk informationsbehandling eller någon annan liknande automatisk process, så att det innebär vinning för gärningsmannen och skada för någon annan.
[270] BrB 10:5.1 (SFS 1986:123): Om någon, som på grund av förtroende ställning fått till uppgift att för någon annan sköta ekonomisk angelägenhet eller självständigt handha kvalificerad teknisk uppgift eller övervaka skötseln av sådan angelägenhet eller uppgift, missbrukar sin förtroendeställning och därigenom skadar huvudmannen, döms han för *trolöshet mot huvudman* till böter eller fängelse i högst två år. Vad som har sagts nu gäller inte, om gärningen är belagd med straff enligt 1–3 paragrafer.

käytöstä.[271] Väärennystä koskevassa säännöksessä (14:1) ei nimenomaisesti mainita tietoteknistä tallennetta kelvollisena teko-objektina, mutta käytännössä asiakirjan (urkund) käsitettä on tulkittu laajasti.[272]

Varsinkin petosta ja luvatonta käyttöä koskevat säännökset muistuttavat suuresti Suomessa vuoden 1991 alusta voimaan tulleita vastaavia säännöksiä. Perusproblematiikka on ollut sama; niinpä luvattoman käytön osalta aikaisempi säännös edellytti teko-objektin olevan tekijän hallussa.[273] Tästä vaatimuksesta luopumalla mahdollistettiin rankaiseminen ”tietokoneajan varastamisesta”.

Voimassa oleva ruotsalainen tietotekniikkarikoksia koskeva sääntely on siis varsin niukkaa – sinänsä nämä harvat voimassa olevat säännökset ovat iästään huolimatta hyvin ajan tasalla. Lainsäädännön täydentämis- ja uudistamishankkeet ovat kuitenkin olleet jo pitkään vireillä. Oikeusministeriö asetti vuonna 1989 asiantuntijaelimen selvittämään toisaalta data- ja teletekniikan kehitykseen liittyviä rikos- ja prosessioikeudellisia kysymyksiä, toisaalta vastaavia muiden viranomaisten selvitys- ja kontrollitoimintaan liittyviä kysymyksiä.

Työryhmä, joka otti nimekseen *Datastraffrättsutredningen,* sai joulukuussa 1992 valmiiksi laajan ja perusteellisen loppumietintönsä *Information och den nya InformationsTeknologin – straff- och processrättsliga frågor m.m.* (SOU 1992:110).

Toteutuessaan mietinnössä esitetyt ehdotukset olisivat merkinneet osaksi varsin pitkälle meneviä tietotekniikan käyttöön liittyviä kriminalisointeja – sellaisissakin yhteyksissä, joihin niitä ei ole kovinkaan helppoa kuvitella. Tällainen on esimerkiksi laitonta uhkausta *(olaga hot)* koskeva ehdotus (4:5), jonka mukaan laittomasta uhkauksesta olisi kysymys myös silloin, kun uhka ”avser angrepp på data för automatisk informationsbehandling”. Keskeisimpiä muista ehdotetuista kriminalisoinneista[274] ovat tietomurto *(informationsintrång, 4:8),* tietovahingon aiheuttaminen (*dataskadegörelse, 12:1.1),* sabotaasi *(sabotage, 13:4), tietokoneviruk-sen* valmistaminen tai levittäminen *(framställande eller spridande av datavirus, 13:7a)* sekä väärennys[275] *(dokumentförfalskning, 14:1).* Näyttää kuitenkin siltä, että mietintö sellaisenaan ei johda lainsäädäntötoimiin.

---

[271] BrB 10:7.1 (SFS 1986:123): Om någon olovligen brukar någon annans sak och därigenom vållar skada eller olägenhet, döms han för *olovligt brukande* till böter eller fängelse i högst sex månader.

[272] SOU 1992:110, s. 249 ss.; ks. myös Jareborg, RIDP 1–2/93, s. 588 s.

[273] Solarz, s. 47 s., Jareborg, RIDP 1–2/93, s. 584 s.

[274] SOU 1992:110, s. 15 ss.

[275] Väärennyksen osalta uudistus tarkoittaisi lähinnä teko-objektin määritelmän muuttamista: ”Med dokument avses i detta kapitel en skriftlig originalhandling eller en bestämd mängd data för automatisk informationsbehandling, om det är möjligt att fastställa att innehållet härrör från den som framstår som utställare. Som dokument anses också legitimationskort, biljett och dylikt bevismärke.”

Ruotsin voimassa oleva lainsäädäntö ei siis vastaa kansainvälisiä suosituksia kuin joiltakin osin, mutta *Datastraffrättsutredningenin* ehdotusten joskus ehkä toteuduttua – muodossa tai toisessa – on Ruotsissa voimassa nykyaikainen ja kansainväliset vaatimukset hyvin huomioon ottava tietotekniikkarikoslainsäädäntö.[276]

2.2.2 Tanska

Tietotekniikkarikoksiin kohdistuva lainvalmistelu alkoi Tanskassa maaliskuussa 1984 oikeusministeriön pyydettyä *straffelovrådetilta* lausuntoa siitä, miten tyydyttävästi tuolloin voimassa olleet *straffelovenin* asianomaiset säännökset soveltuivat elektroniseen tietojenkäsittelyyn liittyviin tekomuotoihin. Vuotta myöhemmin *straffelovrådet* sai valmiiksi mietintönsä,[277] johon liittyi myös ehdotus uusiksi säännöksiksi.[278] Ehdotus johti lainsäädäntötoimiin ja laki, jolla eräitä *straffelovenin* pykäliä muutettiin, annettiin jo kesäkuussa 1985 (Lov om aendring af straffeloven nr. 229/6.6.1985).

Tanskan rikoslaissa on nyt tietotekniikkarikoksiksi katsottavia menettelyjä kriminalisoivia säännöksiä, jotka koskevat sabotaasia,[279] viestintäsalaisuuden rikkomista ja yritysvakoilua[280] ja tietojenkäsittelypetosta.[281] Lisäksi 280 §:n säännös luottamusaseman väärinkäyttämisestä *(mandatsvig)* ja 284 §:n säännös kätkemisrikoksesta *(haeleri;* säännöksessä mainitaan yhtenä kysymykseen tulevista esirikoksista myös *databedrageri)* voivat liittyä tietotekniikkarikok-

---

[276] Professori H.W.K. Kaspersen, joka on toiminut myös PC-CY:n puheenjohtajana, on tehnyt 1997 valmistuneen tutkimuksen EN:n vuoden 1989 suosituksen implementoinnista. Ainakin tämän tutkimuksen pohjana olleeseen kyselyyn vastatessaan Ruotsi on ilmoittanut, että ehdotukset hyvin todennäköisesti aikanaan tulevat voimaan.

[277] Straffelovrådets betaenkning om datakriminalitet (nr. 1032/1985).

[278] Strl.bet.1985, s. 76 ss.

[279] 193 § ”Den, som på retsstridig måde fremkalder omfattende forstyrrelse i driften af almindelige samfaerdselmidler, offentlig postbesorgelse, telegraf- eller telefonanlaeg, radio- eller fjernsynsanlaeg, databehandlingsanlaeg eller anlaeg, der tjener til almindelig forsyning med vand, gas, elektrisk strom eller varme, straffes med haefte eller med faengsel indtil 4 år eller under formildende omstaendigheder med bode. (Stk. 1.) Begås forbrydelsen uagtsomt, er straffen bode eller haefte. (Stk. 2.)”

[280] 263 §: ”– – Med bode, haefte eller faengsel indtil 6 måneder straffes den, som uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et anlaeg til elektronisk databehandling. (Stk. 2.) Begås de i stk. 1 eller 2 naevnte forhold med forsaet til at skaffe sig eller gore sig bekendt med oplysninger om en virksomheds erhvervshemmeligheder eller under andre saerlig skaerpende omstaendigheder, kan straffen stige til faengsel indtil 2 år. (Stk. 3.)” Ks. myös 264 §.

[281] 279 a §: ”For databedrageri straffes den, som for derigennem at skaffe sig eller andre uberettiget vinding retstridigt aendrer, tilfojer eller sletter oplysninger eller programmer til elektronisk databehandling eller i ovrigt retsstridigt soger at påvirke resultatet af sådan databehandling.”

siin. Muiden muassa *databedragerin* ja *mandatsvigin* erityisen törkeiden tekomuotojen varalta säädetään 286 §:ssä aina kahdeksaan vuoteen vankeutta ulottuva rangaistusasteikko.

Tanskan rikoslaissa on siis nimenomaisesti tietotekninen kehitys huomioon ottaen säädetty sabotaasista ja viestintärikoksesta,[282] tietojenkäsittelypetoksesta[283] sekä osin myös yritysvakoilusta. Sabotaasi-, viestintärikos- ja petossäännökset muistuttavat sisällöltään vastaavia suomalaisia säännöksiä.

Tietoteknistä väärennystä ei Tanskassa ole erikseen kriminalisoitu. *Greve* toteaa, että niin syötettävän, tallennetun kuin tulostetunkin datan osalta saattaa tulla rangaistavaksi dataan kohdistuva vahingoittaminen, muuttaminen tai jäljentäminen;[284] sovellettavia säännöksiä voivat tuolloin olla edellä käsiteltyjen lisäksi muiden muassa 291 §:n vahingontekosäännös[285] ja 171 §:n asiakirjaväärennystä koskeva säännös.[286]

Luvatonta käyttöä ei Tanskan rikoslaissa ole kriminalisoitu. Dataan kohdistuva luvaton käyttö saattaa tulla rangaistavaksi erityislainsäädäntöön sisältyvien säännösten nojalla.[287]

Tanskalainen tietotekniikkarikoksia koskeva sääntely on siis jokseenkin niukkaa ja uudistamispaineita on olemassa. *Greve* on muun muassa todennut, että tietoteknisen väärennyksen *(datafalsk)* kriminalisoimista erikseen olisi harkittava.[288] Tanskassa onkin ryhdytty valmistelemaan laajempaa tietotekniikkarikoksiin liittyvän lainsäädännön tarkistamista.

2.2.3 Saksa

Saksan Liittotasavallassa tietotekniikkarikoksia koskeva lainsäädäntö alkoi kehittyä tietosuojan alueella.[289] Ensimmäinen tietosuojasäädös annettiin Hessenin

---

[282] Ks. Greve, s. 57 ss., Greve ym., s. 180 ss. ja s. 284 ss.

[283] Ks. Greve, s. 65 ss., Greve ym., s. 365 ss.

[284] Greve, s. 44 ss.

[285] Teon kohteena tulee kysymykseen ”ting, der tillhorer en anden” ja tekotapoina ”odelaegger, bekadiger eller bortskaffer”. Tietoteknisen tallenteen katsominen kelvolliseksi teko-objektiksi edellyttänee laventavaa tulkintaa.

[286] *Dokumentfalsk;* säännöksen toisen momentin mukaan ”ved dokument forstås en skriftlig med betegnelse af udstederen forsynet tilkendegivelse, der enten fremtraeder som bestemt til at tjene som bevis eller bliver benyttet som bevis for en rettighed, en forpligtelse eller en befrielse for en sådan”. Määritelmä ei siis sisällä nimenomaista mainintaa tietoteknisen tallenteen asemasta lainkohdassa tarkoitettuna dokumenttina eikä Tanskassa tältä osin ole lähdetty laventavan tulkinnan tielle; vrt. Greve ym., s. 135 s.

[287] Ks. Greve, s. 61 ss., jossa mainitaan *love om private registre* sekä *love om offentlige myndigheders registre.*

[288] Greve, s. 87. Greve tosin tuntuu pitävän tanskalaista sääntelyä melko kattavana, mutta on otettava huomioon, että hänen nämä mielipiteensä ovat vuodelta 1986.

[289] Möhrenschlager, s. 332 ss.

osavaltiossa lokakuussa 1970; liittovaltion lainsäädäntöön tietosuojalaki säädettiin vuonna 1977. Varsinaista tietotekniikkarikoksia koskevaa säännöstöä säädettiin erityisesti kuitenkin vasta 1980-luvun keskivaiheilla; erityisen tärkeä tässä suhteessa oli *2. Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG),* joka säädettiin 15.5.1986 ja jolla lisättiin *Strafgesetzbuchiin (StGB)* säännökset tietojenkäsittelypetoksesta, todistuskappaleena relevantin datan väärentämisestä, tietokonevakoilusta, datan muuttamisesta ja tietokonesabotaasista.[290] Saksan Demokraattisen Tasavallan rikoslakiin tuli tietotekniikkarikossäännöksiä vuonna 1989; nämä kuitenkin kumottiin Saksojen yhdistyessä lokakuun 3. päivänä 1990.

Tietojenkäsittelypetoksesta *(Computerbetrug)* säädetään StGB:n 263 a §:ssä; säännös muistuttaa suomalaista petossäännöstä ja sen mukaan rangaistaan henkilöä, joka hankkiakseen itselleen hyötyä vahingoittaa toisen omaisuutta vaikuttamalla tietojenkäsittelyn lopputulokseen erilaisin säännöksessä kuvatuin keinoin.[291] Perustunnusmerkistön mukaisesta teosta säädetty rangaistus on sakkoa tai enintään viisi vuotta vankeutta. *Möhrenschlager* pitää säännöstä epätäsmällisenä ja tulkinnanvaraisena sekä näkee ongelmalliseksi säännöksen sovellettavuuden suomalaiseen maksuvälinepetokseen rinnastettaviin tekoihin.[292]

StGB:n 269 §:ssä on erityinen väärennyssäännös *(Fälschung beweiserheblicher Daten).* Säännös suojaa niin kutsuttuja elektronisia asiakirjoja väärennysteoilta antamalla niille todistuskappaleina saman suojan kuin perinteisillekin asiakirjoille.[293]

Tietokonevakoilusta *(Ausspähen von Daten)* on säännös StGB:n 202 a §:ssä; vakoiluun syyllistyy se, joka oikeudettomasti hankkii itselleen tai toiselle tietoja, jotka eivät ole hänelle tarkoitettuja ja jotka on erityisesti ulkopuolisilta suojattu.[294] Tietojärjestelmään tunkeutumista ei Saksassa ole yleisesti kriminalisoitu, mutta tietokonevakoilusäännöksessä tarkoitettu menettely kohdistuessaan ulkopuolisilta suojattuun tiedostoon – ”die gegen unberechtigten Zugang besonders gesichert sind” – voi helposti toteuttaa myös tietomurroksi katsottavan menettelyn tunnusmerkistön.[295]

---

290 Ks. Sieber, Strafrechtsreform, s. 31 ss.

291 ”– – das Vermögen eines anderen dadurch beschädigt, dass er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programmes, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung der Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflusst – – ”. Ks. Haft, s. 7 s. ja Sieber, Strafrechtsreform, s. 37 ss.

292 Möhrenschlager, s. 342 s.

293 ”– – beweiserhebliche Daten so speichert oder verändert, dass bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde oder derart gepeicherte oder veränderte Daten Gebraucht – –”. Ks. Haft, s. 8 s., Sieber, Strafrechtsreform, s. 43 ss. ja Möhrenschlager, s. 343 s.

294 ”– – wer unbefugt Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft – –”. Ks. Haft, s. 9 s.

295 Möhrenschlager, s. 338 s.

Vahingontekotyyppinen menettely kriminalisoidaan 303a §:ssä *(Datenveränderung)*[296] ja tietokonesabotaasi *(Computersabotage)*[297] 303 b §:ssä.[298] Säännöksillä on tietovahingon aiheuttaminen erotettu esinevahingon aiheuttamisesta.

Tietojärjestelmän luvatonta käyttöä Saksassa ei ole kriminalisoitu, vaikkakin 2. WiKG:iä säädettäessä kriminalisoimista kannattaneita ajatuksia esitettiin. Yhtenä syynä kriminalisoimatta jättämiseen on saksalainen käsitys, jonka mukaan omaisuuden käyttäminen ei – määrättyjä poikkeuksia lukuun ottamatta – perusta rikosoikeudellista vastuuta.[299]

Edellä kuvatut lähinnä datarikoksia koskeviksi luokiteltavat säännökset ovat iästään huolimatta nykyaikaisia ja jokseenkin hyvin kansainvälisiä suosituksia vastaavia. Näiden lisäksi Saksassa on kriminalisoitu tietokoneohjelmien tekijänoikeuksiin kohdistuvat loukkaukset lisäyksillä tekijänoikeuslakiin vuonna 1985 ja 1991.[300] Myös yksinoikeus integroidun piirin piirimalliin on suojattu rikosoikeudellisesti vuonna 1986.[301]

Vaikka sääntely Saksassa muuten onkin hyvin kattavaa, ei varsinaisista informaatiorikoksista ole säädetty niin, että niissä nimenomaisesti olisi otettu huomioon tietoteknisten elementtien asettamia erityisvaatimuksia.[302]

2.2.4 Yhdistynyt kuningaskunta

Kun Ruotsissa, Tanskassa ja Saksassa on tietotekniikkarikoksia koskeva sääntely toteutettu samoin kuin Suomessakin olemassa olleita säännöksiä muokkaamalla ja täydentämällä niitä joillakin uusilla normeilla, on Britanniassa päädytty olennaisesti toisenlaisiin ratkaisuihin. Englannissa on säädetty erityinen tietotekniikkarikoksia koskeva *Computer Misuse Act,* joka tuli voimaan 29.8.1990. Tätä ennen ei Englannissa ollut erityisesti tietotekniikkarikoksia koskevia kriminalisointeja; joissakin tapauksissa voitiin soveltaa vuodelta 1981 olevaa *Forgery and Counterfeiting Actia.*

Computer Misuse Actin taustalla on *Scottish Law Commissionin* vuodelta 1987 oleva tietotekniikkarikoksia koskeva raportti,[303] joka muun muassa sisäl-

---

296 ”– – Daten löscht, unterdrückt, unbrauchbar macht oder verändert – –”.

297 ”– – eine Datenverarbeitung, die für einen fremden Betieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, dass er eine Datenveränderung begeht oder eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert – –”.

298 Haft, s. 10, Möhrenschlager, s. 344 s.

299 Möhrenschlager, s. 345 s.

300 Möhrenschlager, s. 340.

301 Möhrenschlager, s. 341.

302 Möhrenschlager, s. 335.

303 Scot Law Com No 106.

tää ehdotuksen tietotekniikkarikoslaiksi. Skotlantilaista raporttia seuraten *Law Commission for England and Wales* valmisti oman raporttinsa,[304] jonka pohjalta *Computer Misuse Act* sitten säädettiin.

Computer Misuse Actissa on kaiken kaikkiaan vain kolme rangaistussäännöstä, jotka on kirjoitettu jokseenkin avoimiksi ja yleisiksi. *Act* ei sisällä määritelmiä, sillä *Law Commission* katsoi, että teknologinen kehitys kuitenkin johtaisi määritelmien vanhentumiseen. Määrittelemisen ongelma jää niin muodoin lainkäyttäjän huoleksi.[305]

Actin ensimmäinen pykälä sisältää tietomurtoa koskevan perussäännöksen (”Basic Hacking Offence”).[306] Säännöksen mukaan rangaistaan sitä, joka nimenomaisena tarkoituksenaan oikeudettomasti tunkeutua mihin tahansa ohjelmistoon tai tiedostoon saa tietokoneen suorittamaan minkä tahansa toiminnon.

Teon kohteena ei tarvitse olla mikään tietty tai tietynlainen taikka tietyssä tietokoneessa oleva ohjelmisto tai tiedosto. Teko voi täyttyä hyvin varhaisessa vaiheessa; rangaistavuus ei edellytä, että tekijä onnistuu tunkeutumisyrityksessään, kunhan vain järjestelmä on ryhtynyt tunnistamaan tunkeutujaa. *Law Commissionin* mukaan jo ”knocking on the door of the computer” on rangaistavaa. – Säännöstä voidaan soveltaa ainoastaan *magistrates' courtissa.* [307]

Toisessa pykälässä säädetään kvalifioidusta tietomurrosta (”Ulterior Hacking Offence”).[308] Säännöksen sovellettavuus riippuu tekijän tarkoituksesta: mikäli hänellä tehdessään 1 §:ssä kuvattua tekoa on ollut aikomuksena tehdä

---

[304] Report No 186, Computer Misuse, 1989, Cm. 819, HMSO, 1989; ks. Wasik, Crim.L.R. 89, s. 257 ja RIDP 1–2/93, s. 628.

[305] Ks. Wasik, RIDP 1–2/93 s. 631.

[306] (1) A person is guilty of an offence if (a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer; (b) the access he intends to secure is unauthorised; and (c) he knows at the time when he causes the computer to perform the function that that is the case. (2) The intent a person has to have to commit an offence under this section need not be directed at (a) any particular program or data; (a) a program or data of any particular kind; or (c) a program or data held in any particular computer. (3) A person guilty of an offence under this section shall be liable on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale or to both.

[307] Wasik, RIDP 1–2/93 s. 632 s.

[308] (1) A person is guilty of an offence under this section if he commits an offence under section 1 above with intent (a) to commit an offence to which this section applies; or (b) to facilitate the commission of such an offence (whether by himself or by any other person); and the offence he intends to commit or facilitate is referred to below in this section as the further offence. (2) This section applies to offences (a) for which the sentence is fixed by law; or (b) for which a person of twentyone years of age may be sentenced to imprisonment for a term of five years. (3) It is immaterial for the purposes of this section whether the further offence is to be committed on the same occasion as the unauthorised access offence or on any further occasion. (4) A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is impossible. (5) A person guilty of an offence under this section shall be liable (a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; and (b) on conviction on indictment, to imprisonmet for a term not exceeding five years or to a fine or to both.

rikos, josta saattaa seurata viiden vuoden vankeusrangaistus (esimerkiksi petos), arvioidaan menettely toisen pykälän perusteella. Asiaan ei tuolloin vaikuta, onko tekijä tehnyt aikomansa törkeämmän teon tai onko aiottu teko ylipäänsä ollut mahdollinen tehdä. Merkitystä ei ole myöskään sillä, onko tietomurto ja muu teko tehty samanaikaisesti. – Kvalifioitua tietomurtoa voidaan käsitellä joko *magistrates' courtissa* tai *Crown Courtissa* sen mukaan, kuinka törkeän rikoksen tekijä on aikonut tehdä.[309]

Kolmannen pykälän laaja-alainen säännös koskee aineiston oikeudetonta muuttamista ("Unauthorised Modification of Computer Material").[310] Säännöksen tunnusmerkistö on jokseenkin kattava: kaikenlainen tallennetun tiedon muuttaminen on sen perusteella rangaistavissa, kunhan teko on tapahtunut tahallisesti ja tietoisena teon oikeudettomuudesta – näin ollen esimerkiksi virusten ja muiden vahingollisten ohjelmien levittäminen on katsottavissa säännöksen tarkoittamaksi modifioimiseksi. – Lainkohdassa tarkoitettuja rikoksia voidaan niiden vakavuusasteesta riippuen käsitellä joko *Crown Courtissa* tai *magistrates' courtissa.* [311]

Tietosuojan alueella Yhdistyneessä kuningaskunnassa on nähty tärkeämmäksi ohjata ja säännellä käyttäytymistä kuin turvautua rankaisullisiin sanktioihin.[312]

Tekijänoikeuksiin kohdistuvista loukkauksista voi seurata rangaistus yleensä vain silloin, kun teolla tavoitellaan kaupallisia päämääriä; *Copyright, Designs and Patents Actin* rangaistussäännös ei sovellu esimerkiksi yksityistä käyttöä varten tapahtuvaan tietokoneohjelman kopiointiin.[313]

---

309 Wasik, RIDP 1–2/93 s. 634 s.

310 (1) A person is guilty of an offence if (a) he does an act which causes an un-authorised modification of the contents of any computer; and (b) at the time when he does the act he has the requisite intent end the requisite knowledge. (2) For the purposes of subsection (1)(b) above the requisite intent is an intent to cause a modification of the contents of any computer and by so doing (a) to impair the operation of any computer; (b) to prevent or hinder access to any program or data held in any computer; or (c) to impair the operation of any such program or the reliability of any such data. (3) The intent need not be directed at (a) any particular computer; (b) any particular program or data or a program or data of any particular kind; or (c) any particular modification or a modification of any particular kind. (4) For the purposes of subsection (1)(b) above the requisite knowledge is knowledge that any modification he intends to cause is unauthorised. (5) It is immaterial for the purposes of this section whether an unauthorised modification or any intended effect of it of a kind mentioned in subsection (2) above is, or is intended to be, permanent or merely temporary. (6) For the purposes of the Criminal Damage Act 1971 a modification of the contents of a computer shall not be regarded as damaging any computer or computer storage medium unless its effect on that computer or computer storage medium impairs its physical condition. (7) A person guilty of an offence under this section shall be liable (a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; and (b) on conviction on indictment, to imprisonment for a term not exceeding five years or to fine or to both.

311 Wasik, RIDP 1–2/93, s. 635 ss.

312 Wasik, RIDP 1–2/93, s. 637 s.

313 Wasik, RIDP 1–2/93, s. 638.

Varsinaisten datarikosten kohdalla Britanniassa on siis voimassa kattavat kriminalisoinnit sisältävä säännöstö, joka joiltakin osin saattaa olla sovellettavissa myös informaation vapaaseen liikkuvuuteen kohdistuviin rikoksiin; informaatiorikosten osalta sääntelyä kuitenkin voi – ainakin suomalaisittain – pitää puutteellisena. Joka tapauksessa *Computer Misuse Act* on hyvin mielenkiintoinen säädös, joka taustallaan olevasta oikeusjärjestelmästä irrotettunakin erityislaadullaan voisi antaa ajattelemisen aihetta myös mannereurooppalaisille lainsäätäjille.

2.2.5 Tilanne eräissä muissa valtioissa

Tarkastelen vielä varsin pääpiirteisesti eräiden tietotekniikkarikosten sääntelyn suhteen edistyksellisten valtioiden lainsäädäntöä. Sveitsin ja Italian asianomainen lainsäädäntö on melko uutta, kun taas Yhdysvalloissa sillä on jo pitkä traditio.

2.2.5.1 Sveitsi

Sveitsissä saatiin kesäkuussa 1994 päätökseen omaisuus- ja asiakirjarikosoikeutta koskeva lainuudistus, johon sisältyy myös muutamia tietotekniikkarikoksia tarkoittavia kriminalisointeja ja niihin liittyviä säännöksiä.[314] Asiakirjan käsite on laajennettu tarkoittamaan myös tietoteknistä tallennetta *(Datenträger),* joten tällainen tallenne voi tulla kysymykseen väärennysrikoksen kohteena.

Immateriaalinen tieto voi olla varkaustyyppisen teon kohteena (Art. 143, *Unbefugte Datenbeschaffung).* Tietomurto *(Unbefugtes Eindringen in ein Datenverarbeitungssystem)* säädetään rangaistavaksi 143bis artiklassa. Tietovahingon aiheuttamista *(Datenbeschädigung)* koskeva 144bis artikla kriminalisoi 1 momentissaan sabotaasinomaisen vahingonteon ja 2 momentti säätää rangaistavaksi vahingollisten ohjelmien valmistamisen ja levittämisen. Tietojenkäsittelypetoksesta *(Betrügerischer Missbrauch einer Datenverarbeitungsanlage)* säädetään 147 artiklassa. Myös luvaton käyttö – tietokoneajan anastaminen – on rangaistavaa (Art. 150, *Erschleichen einer Leistung).*

Sveitsiläiset säännökset kattavat hyvin Euroopan neuvoston datarikoksia koskevat suositukset ja menevät niitä pitemmällekin säätäessään vahingollisten ohjelmien valmistamisesta ja levittämisestä.

---

[314] Schmid, ZStrR 1/1995, s. 23 ss.

2.2.5.2 Italia

Italian rikoslakia muutettiin 23.12.1993 annetulla lailla, jolla *codice penaleen* lisättiin lukuisia tietotekniikkarikossäännöksiä.[315]

Tietotekniset tallenteet *(documenti informatici)* nauttivat 491 *bis* artiklan nojalla samanlaista suojaa kuin perinteisetkin asiakirjat. Tietojenkäsittelypetoksesta *(frode informatica)* säädetään 640 *ter artiklassa*. Tietomurto *(accesso abusivo ad un sistema informatico o telematico)* kriminalisoidaan 615 *ter* artiklassa. Mielenkiintoisia ja toistaiseksi vielä kansainvälisesti harvinaisia ovat kriminalisoinnit artikloissa 615 *quater* ja 615 *quinques:* ensin mainitussa säädetään käyttäjätunnusten tai vastaavien oikeudettomasta hankkimisesta ja levittämisestä *(detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici)* ja jälkimmäisessä tuholaisohjelmien levittämisestä *(diffusione di programmi diretti a danneggiare o interrompere un sistema informatico).*

Mainittujen datarikoksia tarkoittavien säännösten lisäksi *codice penalessa* on joukko informaatiorikossäännöksiä, joista tässä mainittakoon luvatonta viestin sieppaamista koskeva 617 *quater* artiklan säännös *(intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche).*

Tietotekniikkaan liittyvien immateriaalioikeuksien rikosoikeudellista suojaa tehostettiin tekijänoikeuslain *(legge n. 633/1941, protezione del diritto d'autore e di altri diritti connessi al suo esercizio)* muutoksella joulukuussa 1992; integroitujen piirien piirimallit olivat suojattuja jo aikaisemmin *(legge n. 70/ 1989, norme per la tutela giuridica delle topografie dei prodotti a semiconduttori).*

Italiassa on tietoisesti ainakin toistaiseksi pidättäydytty kriminalisoimasta tietovahingon aiheuttamista ja tietokoneen luvatonta käyttöä. Kokonaisuudessaan Italian tietotekniikkarikossääntelyä on pidettävä varsin ajanmukaisena, osin jopa hyvinkin edistyksellisenä.

2.2.5.3 Yhdysvallat

Kun Sveitsissä ja Italiassa on säädetty tietotekniikkarikoksista mannereurooppalaiseen tapaan pääasiassa täydentämällä ja modifioimalla perinteisiä rikossäännöksiä, muistuttaa USA:ssa noudatettu menettely enemmän brittiläistä. Kuitenkin erona viimeksi mainittuun on case law'n huomattavan suuri merkitys verrattuna säädännäiseen oikeuteen. Lisäksi on huomattava, että Yhdysvaltain liittovaltio-ominaisuus vaikuttaa rikoslainsäädäntöön aivan toisella tavalla kuin esimerkiksi Saksassa; liittovaltion lainsäädäntö jättää osavaltioille monessa suhteessa runsaasti harkintavaltaa.

---

[315] Dolcini ym., s. 21 ss.

Niin kuin monessa muussakin maassa, on tietotekniikkarikoksia koskeva sääntely Yhdysvalloissa alkanut yksityisyyden suojan alueella; ensimmäisiä liittovaltion säädöksiä olivat *Fair Credit Reporting Act* vuodelta 1970 ja – merkitykseltään edellistä tärkeämpi – *Privacy Act* vuodelta 1974. Varsinaisten tietotekniikkarikosten kohdalla sääntely alkoi osavaltiotasolla; ensimmäiset erilliset lait säädettiin Floridassa ja Arizonassa vuonna 1978.

Nämä – niin kuin useat myöhemmätkin säädökset – perustuivat paljolti liittovaltion lakiehdotukseen vuodelta 1977. Ehdotus ei tullut sellaisenaan hyväksytyksi, joskin sen pohjalta säädettiin vuonna 1984 *Computer Fraud and Misuse Act,* jota vuonna 1986 olennaisesti laajennettiin.[316] Immateriaalioikeuksien rikosoikeudellinen suoja laajeni kattamaan tietokoneohjelmat vuoden 1976 *Copyright Actiin* vuonna 1980 tehdyllä lisäyksellä.[317]

Computer Fraud and Misuse Actin soveltamisala on sikäli rajoitettu, että siinä tarkoitetut rikokset loukkaavat vain liittovaltion hallinnon intressejä. Lain nojalla voidaan rangaista valtion turvallisuutta vaarantavassa tarkoituksessa tapahtuneesta kvalifioidun tiedon hankkimisesta sekä eräiden rahoitus- ja luottotietojen hankkimisesta, eräistä valtionsisäiseen ja ulkomaankauppaan liittyvistä menettelyistä samoin kuin liittovaltion hallinnon tietokoneissa olevaan informaatioon kohdistuvista vahingontekotyyppisistä rikoksista.[318]

Niin sanottuihin varsinaisiin datarikoksiin luettavista teoista – tietojenkäsittelypetos, väärennys yms. – ei liittovaltion tasolla ole yleisesti säädetty; näiden osalta rangaistavuus perustuu paitsi osavaltiolainsäädäntöön myös paljolti *case law'hin.*

2.2.6 Johtopäätöksiä

Edellä esitetyt katsaukset vieraiden valtioiden lainsäädäntöihin osoittavat selvästi, että vaikka yksittäiset lainsäädännölliset ratkaisut saattavat poiketa toisistaan selvästikin, ovat kriminalisointien kohteena olevat menettelyt hyvin samankaltaisia. Tämä selittyy ymmärtääkseni hyvin suurelta osin juuri kansainvälisen yhteistyön tiiviydellä – tietotekniikkaan liittyvien väärinkäytösten osalta ei ainakaan joka suhteessa ole olemassa sellaista yleisesti koettua moraalista moitittavuutta, jonka ansiosta juuri kukaan ei kyseenalaista esimerkiksi tahallisen tappamisen kriminalisoimisen oikeutetusta ja perusteltavuutta.

Euroopan neuvoston yleissopimus tulee epäilemättä entisestään yhdenmukaistamaan muun muassa juuri edellä käsiteltyjen valtioiden lainsäädäntöä.

---

316 18 United States Code § 1030.
317 Ks. Wise, s. 655 ss.
318 Bigelow, s. 16 s.

Jotta tämä tutkimus olisi ollut mahdollista jossain vaiheessa saada edes jollain lailla valmiiksi, en ole ryhtynyt selvittämään, onko – ja jos, niin miten – yleissopimusta näissä maissa ryhdytty implementoimaan.

Käsittääkseni voidaan perustellusti ennakoida, että tietotekniikan käyttöön liittyvät väärinkäytökset aletaan yleisesti kokea yhä uhkaavammiksi, kun yhteiskunnan toimintojen rakentuminen tietoteknisten sovellusten varaan jatkuvasti lisääntyy ja esimerkiksi yksityisyyden suojan loukkaamisen mahdollisuudet lisääntyvät ja monimuotoistuvat. Tällöin myös kuilu kehittyneiden sivistysvaltioiden ja kehitysvaltioiden välillä tulee laajenemaan: toisaalta tietysti siksi, että ensin mainituissa on lähtökohtaisesti suurempi riski joutua väärinkäytösten kohteeksi, mutta toisaalta myös siksi, että niissä on oleellisesti paremmat mahdollisuudet paitsi teknisin myös muun muassa rikoslain keinoin vastata uusiin haasteisiin.

Tällä hetkellä voitaneen karkeasti arvioida, että Länsi-Euroopan ja Pohjois-Amerikan valtiot samoin kuin ainakin Australia, Uusi-Seelanti ja Japani ovat rikoslainsäädäntöjensä sisältöjen ja tehokkuuden suhteen jotakuinkin samalla tasolla.

II
TIETOJENKÄSITTELYRAUHAA LOUKKAAVAT RIKOKSET

1 Yleistä

Tietotekniikkarikoksia koskevilla kriminalisoinneilla suojataan osan I luvussa 1.2.3.4 tarkemmin selostetuin tavoin tietoturvallisuuden kolmea eri osa-aluetta eli tietojen luottamuksellisuutta (confidentiality), eheyttä (integrity) ja käytettävyyttä (availability), joista yhdessä voidaan käyttää nimitystä tietojenkäsittelyrauha (pax computationis).[1]

Tarkasteltaessa lähemmin varsinaisia datarikoksia eli tietojenkäsittelypetosta, tietoteknistä väärennystä, tietovahingon aiheuttamista, luvatonta käyttöä, tietomurtoa ja vaaran aiheuttamista tietojenkäsittelylle koskevia kriminalisointeja sekä soveltuvin osin myös yritysvakoilua ja maksuvälinepetosta koskevia säännöksiä voidaan havaita niiden itse asiassa suojaavan tietoturvallisuuden eri elementtejä sen mukaan, missä vaiheessa ja millä tavoin kunkin rikoksen tunnusmerkistö täyttyy.

Tietomurto täyttyy aikaisimmassa vaiheessa ja sen täyttymiselle asetetaan muutenkin alhaisimmat vaatimukset. Tietomurtoa koskeva säännös suojaa ennen kaikkea tietojen luottamuksellisuutta: tiedot ovat vain niiden käyttöön oikeutettujen saatavissa. *Yritysvakoilussa* on kysymys kvalifioidusta tietomurrosta, jonka suojeluobjektina on myös tietojen – yrityssalaisuuksien – luottamuksellisuus.

Sama suojeluobjekti on *luvattomalla käytöllä,* jonka täyttymisaste on edellä mainituista rikoksista toiseksi alhaisin. Tunnusmerkistön täyttyminen ei edellytä pitemmälle menevää kajoamista tietoihin, vaan pelkkä järjestelmän käyttäminen riittää. Tätä kautta luvattoman käytön kriminalisoimisella suojataan kuitenkin myös tietojen käytettävyyttä, sillä luvaton käyttäminen saattaa muodostaa esteen tai ainakin haitan oikeutetulle tietojen käyttämiselle.

Tietojenkäsittelypetos, tietotekninen väärennys ja tietovahingon aiheuttaminen puolestaan ovat tekoja, jotka suoranaisesti kohdistuvat dataan ja vaikuttavat myös datan edustaman informaation sisältöön. Näitä tekoja koskevat kriminalisoinnit suojaavat paitsi osaltaan tietojen luottamuksellisuutta ja käytettävyyttä ennen kaikkea tietojen eheyttä. *Maksuvälinepetos* on tietojenkäsittelypetoksen erityistyyppi, jota koskevalla kriminalisoinnilla on haluttu antaa maksuliikenteen häiriöttömyydelle ja luotettavuudelle erityistä rikosoikeudellista suojaa.

Vaaran aiheuttaminen tietojenkäsittelylle poikkeaa luonteeltaan muista tässä mainituista teoista, sillä rikos voi täyttyä, vaikkei sen kohteena olevaan tietojenkäsittelyyn olisi vielä varsinaisesti millään tavoin puututtu. Säännöksessä tarkoitettu vahingollinen tai haitallinen ohjelma tai ohjelmakäskyjen sarja saattaa

---

[1] Anglosaksisessa kielenkäytössä on jokseenkin yleinen termi ”cia-crimes”, joka viittaa juuri puheena oleviin tietoturvallisuuden osa-alueisiin kohdistuviin loukkauksiin.

joutuessaan kosketuksiin tietojenkäsittelyn kanssa luonteestaan riippuen loukata kaikkia tietoturvallisuuden elementtejä, joskin ensisijaisesti mahdollinen loukkaus kohdistunee tietojen eheyteen ja käytettävyyteen: niin sanottu virusohjelma voi toisaalta saada aikaan informaation muuttumisen tai häviämisen, toisaalta se voi estää järjestelmän oikeutetun käyttämisen tai haitata sitä.

Kaikille tässä mainituille rikoksille on siis ominaista, että ne loukkaavat tai voivat loukata yhtä tai useampaa tietoturvallisuuden kolmesta peruselementistä ja että ne kaikki tällä tavoin kohdistuvat tietojenkäsittelyrauhaan. Lisäksi niille on tyypillistä, että tämä loukkaaminen tapahtuu datan käsittelemisellä tai datan vaarantamisella; informaation muuttumisesta mahdollisesti aiheutuva haitta tai vahinko on sikäli välillistä, että sitä välttämättömästi edellyttää informaatiota edustavan datan jonkinasteinen muuttuminen tai pahimmassa tapauksessa täydellinen tuhoutuminen.

Käsittelen seuraavassa erikseen kutakin edellä mainittua rikosta niiden täyttymiselle asetettavan tietojenkäsittelyrauhan loukkauksen vakavuuden mukaisessa järjestyksessä alkaen lievimmästä eli tietomurrosta sekä yhdestä tietomurron erityistapauksesta eli yritysvakoilusta. Seuraavana vuorossa on luvaton käyttö ja sen jälkeen tietotekninen väärennys, tietojenkäsittelypetos ja sen erityismuoto maksuvälinepetos sekä tietovahingon aiheuttaminen. Väärennyksen, petoksen ja vahingonteon keskinäinen järjestys tässä yhteydessä määräytyy sillä perusteella, että väärennyksen ja petoksen ensisijainen suojeluobjekti on muu kuin tietojenkäsittelyrauha. Vaaran aiheuttaminen tietojenkäsittelylle jää tässä tarkastelussa viimeiseksi johtuen sen muista poikkeavasta luonteesta.

Edellä osassa I luvussa 1.1.2.5 selostetut tavoitteet ja syyt ovat määränneet jäljempänä seuraavan esityksen muodon eli sen, että ensin esitän kysymyksessä olevan säännöksen, sitten selostan säännöksen syntymiseen johtaneita syitä, käsittelen erityisiä tietotekniikkaspesifisiä ongelmia ja tarvittaessa myös rikoslajin yleisiä elementtejä ja lopuksi mahdollisuuksien mukaan selvitän säännöksen soveltamiskäytäntöä. Kommentoin myös osan I luvussa 2.1 selostettuja kansainvälisiä instrumentteja sikäli kuin niillä on merkitystä säännösten tulkinnan kannalta.

Yksittäisten tunnusmerkistöjen läpikäymisen jälkeen käsittelen kokoavasti niiden keskinäisiä suhteita koskevia kysymyksiä ja analysoin tarkemmin tietotekniikkarikoksiin liittyvää tahallisuusproblematiikkaa. Osan lopussa esitän vielä kokoavia arvioita samoin kuin ehdotuksia säädettävää lakia silmällä pitäen.

2 Tietojen luottamuksellisuutta loukkaavat teot

2.1 OIKEUDETON TUNKEUTUMINEN TIETOJÄRJESTELMÄÄN

2.1.1 Tietomurto (RL 38:8)

Rikoslain 38 luvun 8 §:ssä on seuraava tietomurtoa koskeva säännös:

> 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.

Ennen rikoslain nykyisen 38 luvun säätämistä voimassa olleista säännöksistä on nyt kysymyksessä oleva säännös asiallisesti korvannut henkilörekisterilain 45 §:n henkilörekisteriin tunkeutumista koskeneen säännöksen (sellaisena kuin se oli laissa 471/1987), joka ennen tietomurron kriminalisoimista oli ainoa luvatonta tietojärjestelmään tunkeutumista sellaisenaan koskenut kriminalisointi.

Tietomurto on asianomistajarikos, josta virallinen syyttäjä saa ilman asianomistajan ilmoitustakin nostaa syytteen, jos rikoksentekijä rikoksen tehdessään on ollut yleistä posti- tai teletoimintaa harjoittavan laitoksen palveluksessa tai jos erittäin tärkeä yleinen etu vaatii syytteen nostamista (RL 38 luku 10 § 2 mom.). Näistä edellytyksistä tietomurtoon voi yleensä soveltua vain jälkimmäinen; ensin mainittu soveltuu etupäässä viestintäsalaisuuden loukkaukseen, josta myös säädetään rikoslain 38 luvussa.

Tietomurtoa koskevalla säännöksellä pyritään perustelujen[2] mukaan turvaamaan toisaalta niin sanottua tietokonerauhaa[3] eli tietojärjestelmiä ulkopuolista

---

[2] HE 94/1993, s. 155 ss.

[3] Perusteluissa käytetyn termin ”tietokonerauha” voidaan siis nyttemmin katsoa korvautuneen käsitteellä ”tietojenkäsittelyrauha”.

tunkeutumista vastaan ja toisaalta tietokonetyöskentelyn yksityisyyttä sellaista ulkopuolista tarkkailua vastaan, jossa ei ole kysymys salakuuntelusta tai -katselusta.

Ensimmäisessä momentissa tietojärjestelmällä – jolla yleensä ymmärretään tietyssä organisaatiossa käytettävää tietojenkäsittely- ja siirtolaitteiden muodostamaa verkostoa – tarkoitetaan nimenomaan sellaisia tietojärjestelmiä, joissa tietoja käsitellään, varastoidaan tai siirretään sähköisesti tai muulla vastaavalla teknisellä keinolla; käsin pidettyjä tietojärjestelmiä säännös ei koske.[4]

Murtautuminen ja murtovälineet

Tietojärjestelmään tunkeutumisella tarkoitetaan pääsyn hankkimista järjestelmässä käsiteltyihin, varastoituihin tai siirrettyihin tietoihin; pääsy voidaan siis hankkia joko tietokoneen muistissa olevaan tai tiedonsiirtolinjaa pitkin siirrettävään tietoon.

Teon rangaistavuuden edellytyksenä olevan turvajärjestelyn – josta säännöksessä mainitaan esimerkkinä käyttäjätunnus – murtamisen on tapahduttava jollakin rikoksentekijän nimenomaisella toimella. Säännöksessä ei edellytetä tunkeutumisen tapahtuvan mitenkään järjestelmällisesti, vaan sattumaltakin onnistunut koodin keksiminen riittää, mikäli tekijän tarkoituksena on oikeudeton tietojärjestelmään tunkeutuminen. Oikean käyttäjätunnuksen tai muun tunnistuskontrollikeinon tiedoksisaantitapa on rikoksen täyttymisen kannalta merkityksetön. Huomattava on, että säännöksen perustelujen ja nyttemmin myös oikeuskäytännön mukaan jo pelkkä tiedon hankkiminen esimerkiksi käyttäjätunnus-salasanapareista toteuttaa tietomurron yrityksen, mikäli hankkiminen tapahtuu tietomurron tekemisen tarkoituksessa.

Tiedon hankkiminen käyttäjätunnuksesta vilpillisin keinoin tai käyttäjätunnusten ja salasanojen levittäminen (password swapping, trafficking in passwords) oli keskustelun kohteena AIDP:n sekä syksyn 1992 kollokviossa että syksyn 1994 maailmankongressissa. Kollokviossa ehdotetun mukaisesti kongressi päätyi suosittelemaan myös tämän menettelyn kriminalisoimisen harkitsemista.[5]

---

[4] Tietojärjestelmästä tietomurron kohteena ks. esim. Rautio, Rikosoikeus, s. 1220 s.

[5] Ks. kongressin ao. päätöslauselman kohta 10: ”Furthermore, it is suggested that some of the definitions in the Council of Europe lists – such as the offence of unauthorized access – may need further clarification and refinement in the light of advances in information technology and changing perceptions of criminality. For the same reasons, other types of abuses that are not included expressly in the lists, such as trafficking in wrongfully obtained computer passwords and other information about means of obtaining unauthorized access to computer systems, and the distribution of viruses or similar programs, should also be considered as candidates for criminalization, in accord with national legal traditions and culture and with reference to the applicability of existing laws.”

Yhdysvalloissa on jo pitkään ollut olemassa lainsäädäntöä, jolla ”password swapping” on kriminalisoitu. Title 18 Section 1030 (a)(6) of the United States Code esimerkiksi säätää rangaistavaksi ”whoever – – knowingly and with intent to defraud traffics – – in any password or similar information through which a computer may be accessed without authorisation”. Kalifornian lain mukaan rangaistaan sitä, joka ”knowingly and without permission provides or assists in providing a means of accessing a computer” [Californian Penal Code, Section 502 (c)(6)].[6]

Tietotekniset tiirikat

Kansainvälinen yhteistyö onkin nykyisellään johtanut velvollisuuteen kriminalisoida salasanojen ja käyttäjätunnusten levittäminen. Euroopan neuvoston tietoverkkorikoskonvention 6 artiklan otsikko on *välineiden väärinkäyttö (Misuse of Devices)* ja itse artikla on näin kuuluva:

1. Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin säätääkseen kansallisen lainsäädäntönsä mukaisesti rangaistavaksi seuraavat tahalliset ja oikeudettomat teot:

a) seuraavien tuottaminen, myynti, hankkiminen, tuonti, levittäminen tai muu saataville asettaminen:
   i) väline, mukaan luettuna tietokoneohjelma, joka on suunniteltu tai muutettu ensisijaisesti tämän yleissopimuksen 2–5 artiklan mukaisesti rangaistavaksi säädettyjen rikosten tekemistä varten;
   ii) tietojärjestelmän salasana tai käyttäjätunnus tai muu vastaava tieto, joka mahdollistaa pääsyn tietojärjestelmään tai sen osaan, tarkoituksin, että sitä käytetään tämän yleissopimuksen 2–5 artiklan mukaisesti rangaistaviksi säädettyjen rikosten tekemiseen;

b) tämän kappaleen a kohdan i tai ii alakohdassa tarkoitetun tuotteen hallussapito tarkoituksin käyttää sitä 2–5 artiklan mukaisesti rangaistaviksi säädettyjen rikosten tekemiseen. Sopimuspuoli voi asettaa rikosvastuun syntymisen edellytykseksi sen, että tekijän hallussa on useita tällaisia tuotteita.

2. Tämän artiklan määräysten ei katsota perustavan rikosvastuuta muun muassa silloin, kun tämän artiklan 1 kappaleessa tarkoitetun tuotannon, myynnin, hankkimisen, tuonnin, levittämisen tai muun saataville asettamisen tarkoituksena ei ole tehdä tämän yleissopimuksen 2–5 artiklan mukaisesti rangaistavaksi säädettyä rikosta, vaan tietojärjestelmän luvallinen testaus tai suojelu.[7]

---

[6] Ks. Sieber, COMCRIME-Study, III.B.1, alav. 113.

[7] Artiklan toinen kohta voi vaikuttaa omituiselta ja itsestään selvältä. Sen tarkoitus onkin olla puhdas ”PR-clause”, sillä 6 artikla kirvoitti ehkä kaikkein kärkevimmät kommentit yleisöltä, kun sopimusluonnos keväällä 2000 julkistettiin. Ohjelmistoteollisuus mm. katsoi, että sinänsä lailliset järjestelmien testaukseen ja suojaukseen käytettävät ohjelmat tulisivat nyt laittomiksi. Siksi toisessa kohdassa sanotaan oikeastaan sama kuin ensimmäisessäkin, joskin käyttäen ehkä kansantajuisempaa lähtökohtaa kertomalla, mikä menettely ei ole rikollista.

3. Kukin sopimuspuoli voi tehdä varauman, jonka mukaan se ei sovella tämän artiklan 1 kappaletta, edellyttäen kuitenkin, että varauma ei koske tämän artiklan 1 kappaleen a kohdan ii alakohdassa tarkoitettujen tuotteiden myyntiä, levittämistä tai muuten saataville asettamista.[8]

Artiklan 1 kappaleen a kohdan ii alakohdassa siis tarkoitetaan nimenomaan tietojärjestelmään tunkeutumiseen käytettäviä ”tiirikoita”, joiden myymisen, levittämisen ja saataville asettamisen kriminalisoimisen suhteen ei artiklan kolmannen kohdan mukaan varaumaa ole mahdollista tehdä. Tällainen kriminalisointi Suomen rikoslaista toistaiseksi puuttuu.

Asiallisestihan tällainen erillinen kriminalisointi merkitsisi tietojärjestelmään tunkeutumisen – ja myös monen muun edellä mainitun ja jäljempänä käsiteltävän rikoksen – tietyntyyppisen valmistelun kriminalisoimista, joka on hyvinkin perusteltua, kun ajatellaan tietojenkäsittelyrauhan loukkausten potentiaalista vaarallisuutta ja vahingollisuutta. Palaan asiaan *de lege ferenda* -jaksossa.

Tunkeutumisen oikeudettomuus

Tietojärjestelmään tunkeutumisen on oltava tahallista; tunkeutujan on tiedettävä tunkeutuvansa tietojärjestelmään tai sen osaan oikeudettomasti. Oikeudettomuus voi tarkoittaa oikeuden täydellistä puuttumista; tällöin tekijänä tulee kysymykseen lähinnä joku täysin ulkopuolinen henkilö. Toisaalta oikeudettomuus voi ilmetä laillisen oikeuden ylittämisenä. Esimerkiksi yrityksen tai laitoksen tietojärjestelmään on voitu määritellä erilaisia käyttäjätasoja, joille pää-

---

[8] 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law when committed intentionally and without right:

a. the production, sale, procurement for use, import, distribution or otherwise making available of:

i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2–5:

ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing any of the offences established in Articles 2–5; and

b. the possession of an item referred to in paragraphs (a)(1) or (2) above, with intent that it be used for the purpose of committing any of the offences established in Articles 2–5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2. This Article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this Article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer

3. Each Party may reserve the right not to apply paragraph 1 of this Article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1(a)(2).

sy on eri henkilöille sallittu erilaisin perustein. Tällöin henkilöllä voi sinänsä olla oikeus käyttää tietojärjestelmää, mutta oikeudeton tunkeutuminen ylemmälle käyttäjätasolle edellyttää turvajärjestelyn murtamista.[9]

Tekijä voi tunkeutumisyrityksessään käyttää paitsi oikeudettomasti tietoonsa hankkimiaan[10] käyttäjätunnuksia ja salasanoja myös käyttää nimenomaan salasanojen selvittämiseen suunniteltua erityistä tietokoneohjelmaa tai sitten hän voi sattumanvaraisesti erilaisia salasanavaihtoehtoja kokeilemalla pyrkiä läpäisemään kontrollin. Mahdollisuus oikean salasanan löytämiseen voi varsinkin viimeksi mainitussa tilanteessa olla häviävän pieni. Tällä ei kuitenkaan pitäisi olla ratkaisevaa merkitystä tekijän rikollisen tahdon arvioinnissa; tarkoituksena on joka tapauksessa kontrollin läpäiseminen.

Alioikeuskäytännössä tosin aikanaan ainakin joskus katsottiin itselle kuulumattoman pankkikortin tunnusluvun arvaamisen tai sattumanvaraisen keksimisen olevan niin epätodennäköistä, että rahannostoyritysten ei katsottu edenneen edes kelvollisen rikoksen yrityksen asteelle. Tämä ongelma on kuitenkin nyt saanut toistaiseksi ratkaisunsa, kun korkeimman oikeuden maksuvälinepetosta koskevassa ratkaisussa 1999:110 (ään.) katsottiin edellä kuvatun kaltaisessa tilanteessa maksuvälinepetoksen täyttyneen, vaikkakin todettiin, että todennäköisyys varojen nostamisen onnistumiselle on erittäin pieni.[11]

Tapaus tosin koskee nimenomaan maksuvälinepetosta eikä siitä välttämättä voi tehdä kovin pitkälle meneviä johtopäätöksiä tietomurron tunnusmerkistön täyttymisen suhteen. *Jussi Tapani* on tapausta kommentoidessaan kysynyt, suojellaanko maksuliikenteen varmuutta ja turvallisuutta liian järein keinoin, jos teon rangaistavuudelta ei edellytetä, että se voi edes jollakin tavoin vaarantaa säännöksen taustalla olevaa oikeushyvää, ja todennut korkeimman oikeuden siirtäneen kelvottoman yrityksen problematiikan maksuvälinepetoksen tunnusmerkistön tulkintaongelmaksi.[12]

Olen itse usein pyrkinyt havainnollistamaan tietomurtoa asuntomurron avulla – vaikka rikoslaki ei tunne asuntomurto-nimistä rikosta, on käsitteen sisältö maallikoillekin (tai nimenomaan maallikolle) yleensä selvä. Suojauksen murtaen tapahtuva tietojärjestelmään tunkeutuminen on rinnastettavissa oven lukituksen

---

[9] Ks. myös Rautio, Rikosoikeus, s. 1221.

[10] Käyttäjätunnuksia ja salasanoja voi kerätä mm. erityisillä verkonkuunteluohjelmilla, niin sanotuilla sniffereillä. Verkonkuunteluohjelmat eivät sinänsä ole laittomia mutta jos ne muutetaan sellaisiksi, että ne kuuntelevat vain kunkin otetun yhteyden alun ja tallentavat tuolloin lähetettävät käyttäjätunnuksen ja salasanan, on kysymyksessä jo yksinomaan rikollista menettelyä varten valmistettu ohjelma, jonka käyttäminen voi kvalifioida viestintäsalaisuuden loukkauksen törkeäksi.

[11] Käräjäoikeus ja hovioikeus olivat katsoneet, ettei rahan nostoyrityksestä rikoksen täyttymiseen ollut ollut huomattavaa vaaraa, koska todennäköisyys teon onnistumiseen oli ollut hyvin pieni. Yksi oikeusneuvoksista oli samalla kannalla.

[12] Tapani, Kommentti, s. 202. Ks. myös Tolvanen, s. 260.

väkivaltaiseen avaamiseen samoin kuin siihen tilanteeseen, että lukko avataan siihen kuuluvilla avaimilla, joiden käyttämiseen avaajalla ei ole oikeutta.[13]

Tietomurron yrityksestä on kysymys silloin, kun järjestelmään yritetään tunkeutua käyttämällä sellaisia murtovälineitä tai käyttäjätunnus–salasana-pareja, joilla suojaus on mahdollista saada murretuksi; vastaavasti asuntomurron yrityksestä on kysymys silloin, kun tiirikkaa, muuta murtovälinettä tai oikeudettomasti hallussa pidettyä avainta käyttäen yritetään avata asunnon ovi.

Kun sitten mietitään edellä mainittuun pankkikortin tunnuslukuun rinnastettavan salasanan arvaamisen yrityksen rangaistavuutta, on tilanne mielestäni asuntomurtoon verrattuna erilainen. Salasanan käyttäminenhän vastaa asuntoon kuuluvan avaimen käyttämistä ja asunnon oven lukosta on suoraan nähtävissä, että tietyn malliset avaimet eivät yksinkertaisesti voi lukkoa avata: Abloy-avain ei Boda-lukkoon mahdu. Tietojärjestelmästä tätä ei pysty etukäteen havaitsemaan ja niinpä on mahdollista, että salasana voi aivan yhtä hyvin olla muotoa aBcdEfgH, 1KL5&/156 tai mikä muu tahansa yhdistelmä, mistä seuraa, että salasanan arvaajalla on *teoreettinen* mahdollisuus osua oikeaan. Mahdollisuus on ehkä häviävän pieni mutta kuitenkin se *on* olemassa.

Tietomurron yrityskin on joka tapauksessa rangaistavaa ja jos tekijä on salasanoja kokeillut siinä tarkoituksessa, että tietojärjestelmän portti lopulta aukeaa, on hänellä riittävä tahallisuus. Sitä paitsi salasanojen kokeilua ilman tällaista tarkoitusta on vaikea kenenkään kuvitella pelkäksi huvikseen tekevän.

Usein salasanojen arvaaminenkaan ei ole kovin vaikeaa: käytäntö on osoittanut, että ihmisten mielikuvitus salasanojen keksimisessä on melko rajoittunut ja että salasanoja myös vaihdetaan kovin harvoin. Sitä paitsi ne ovat usein löydettävissä hyvin helposti; useat säilyttävät salasanojaan esimerkiksi näppäimistönsä alla. Ongelmana on vielä se, että joissakin organisaatioissa – esimerkiksi oikeushallinnossa – käyttäjätunnus määräytyy tietyn kaavan mukaan eikä sitä niin ollen tarvitse lähteä suuritöisesti selvittämään.

On siis erittäin tärkeää paitsi se, että järjestelmät sinänsä ovat huolella rakennettuja ja ylläpidettyjä, myös se, että käyttäjät muistavat vastuunsa. Jos käyttäjätunnus on kenen tahansa selvitettävissä ja salasanana on puolison nimi, ei tietomurtorikoksen välttämättä ole katsottava tapahtuneen ilman uhrin sellaista myötävaikutusta, joka on jo lähellä konkludenttista suostumusta!

Tietomurron tunnusmerkistön täyttymiskynnyksen mataluuden puolesta puhuu korkeimman oikeuden tuore ratkaisu 2003:36, jota selostan hieman jäljempänä tietomurtorikoksiin liittyvää oikeuskäytäntöä kuvaillessani.

---

[13] Samaa rinnastusta käyttää Järvinenkin; ks. Järvinen, Tietokone ja HeSa.

Teon täyttyminen

Säännöksessä tarkoitetulle menettelylle on ominaista se, että tietojärjestelmään tunkeutumisella tai tunkeutumisyrityksellä ei edellytetä olevan mitään erityistä pelkkää tunkeutumistarkoitusta pidemmälle menevää tarkoitusta. Tietojärjestelmän luonne ja käyttötarkoitus ovat rikoksen täyttymisen kannalta merkityksettömiä seikkoja.

Rikos täyttyy heti tunnistuskontrollin tultua läpäistyksi. Mikäli turvajärjestely on monivaiheinen, on viimeinenkin vaihe läpäistävä. Muussa tapauksessa teko jää rangaistavan yrityksen asteelle. Välttämättä ei edellytetä, että turvajärjestelyn murtamisen jälkeen on siirrytty pois koneen käyttöjärjestelmästä. Myöskään ei edellytetä, että tietojärjestelmässä olevia tietoja millään tavalla käytetään tai että niitä edes luetaan tai selataan.

Jäljempänä käsitellään tarkemmin kysymystä luvattoman käytön ja sen yrityksen tunnusmerkistöjen täyttymisvaiheesta. Tietomurtoa koskevan säännöksen perusteluissa otetaan kysymykseen nimenomainen kanta toteamalla, että jos rikos on edennyt tietojen käyttämiseen saakka, tekoon tulee soveltaa luvatonta käyttöä koskevia säännöksiä. Luvattomana käyttönä ei kuitenkaan vielä pidetä sitä, että hakkeri tunkeutumisellaan saa esimerkiksi tunkeutumisen kohteena olevan tietokoneen käyttöjärjestelmän toimimaan, vaan tällaisiin tekoihin soveltuu tietomurtosäännös, mikäli turvajärjestely onnistutaan murtamaan.

Tietomurron rangaistusasteikkona on sakkoa tai vankeutta enintään yksi vuosi eli asteikko on sama kuin luvattomassa käytössä. Kolmannen momentin mukaan tietomurron yritys on rangaistava. Perustelujen mukaan rangaistavaa on jo yrittää selvittää tietojärjestelmää suojaava käyttäjätunnus tai murtaa muu turvajärjestely, jos teko tehdään tarkoituksin tunkeutua oikeudettomasti tietojärjestelmään.

Tietomurto ja luvaton käyttö

Neljännen momentin mukaan tietomurtoa koskeva säännös on toissijainen; suhteesta luvattomaan käyttöön perusteluissa todetaan luvatonta käyttöä koskevan säännöksen olevan sovellettavissa siinä tapauksessa, että tietojärjestelmään tunkeutuja käyttää tietojärjestelmää jollakin sille ominaisella tavalla.[14] Jos tällainen aikomus on näytettävissä toteen jo tunkeutumisen tapahtuessa, kysymys voisi olla luvattoman käytön yrityksestä.[15]

---

[14] Tähän perusteluissa esitettyyn näkemykseen on Vaasan hovioikeus suhtautunut varauksellisesti tavalla, jota selostetaan jäljempänä ns. TCB-jutun luvatonta käyttöä koskevan osan yhteydessä.

[15] Ks. Rautio, Rikosoikeus, s. 1220, jossa Rautio toteaa, että tietojärjestelmään ”tunkeutumisen kriminalisointi sellaisenaan ei kovin merkittävästi laajenna rangaistavuuden alaa, jos luvaton käyttö on laajasti rangaistavaa, kuten Suomen rikoslaissa. Tietojärjestelmään tunkeutumisen erillisen kriminalisoinnin merkitys kuitenkin korostuu, jos myös tämän rikoksen yritys säädetään rangaistavaksi. Silloin on mahdollista tutkia rikoksina jo yrityksiä tunkeutua suojattuun tietojärjestelmään.”

Perustelujen viimeksi lainattu toteamus luvattoman käytön yrityksen ja tietomurron keskinäisestä suhteesta ei ole johdonmukainen. Asiallisesti luvattoman käytön yritystä merkitsevä teko voinee useinkin toteuttaa täytetyn tietomurron tunnusmerkistön. Tällaisessa tilanteessa tekijän syyksi on luettava täytetty tietomurto, koska luvattoman käytön yrityksen rangaistusasteikko on lievempi eikä neljännen momentin toissijaisuussäännös siis sovellu.[16]

Muutenkin tietomurron ja luvattoman käytön keskinäinen suhde vaikuttaa ongelmalliselta. Jos tekijällä on jo tunkeutumisyritykseen ryhtyessään aikomus käyttää teon kohteena olevaa järjestelmää ja jos teko jää yritysasteelle, on kysymyksessä ilmeisestikin luvattoman käytön eikä tietomurron yritys. Tämän pohtimisella ei ole suurempaa merkitystä, sillä rangaistusasteikot ovat samat. Saattaa toki olla, että tietomurto etenee yritysasteelle jo sellaisilla toimilla, jotka luvattoman käytön suhteen voitaisiin vielä katsoa valmistelutyyppisiksi teoiksi, mutta erottelun käytännön merkitys jää joka tapauksessa varsin vähäiseksi. Palaan tähän rajanveto-ongelmaan jäljempänä luvatonta käyttöä käsiteltäessä.

Silvander esittää hieman erikoisen tulkinnan Suomen lainsäädännöstä tietomurron ja luvattoman käytön keskinäisen suhteen osalta.[17] Hän toteaa Suomessa (samoin kuin Tanskassa ja Norjassa) olevan mahdotonta katsoa tietomurtoa (dataintrång) luvattomaksi käytöksi (tillgreppsbrott) siitä syystä, että luvattoman käytön kohteella on oltava fyysinen substanssi. Tämä käsitys poikkeaa selvästi paitsi omastani ymmärtääkseni myös lainsäätäjän näkemyksestä: järjestelmään tunkeutumista seurannut järjestelmän luvaton käyttäminen on juuri sellaista menettelyä, joka on haluttu saada luvattoman käytön kriminalisoinnin piiriin

Jos kysymyksessä on tietojärjestelmään tunkeutumisen käsittävä yritysasteelle jäänyt viestintäsalaisuuden loukkaus, on tilanne sama kuin luvattoman käytön suhteen. Jos taas tunkeutuminen on tapahtunut tarkoituksin tehdä yritysvakoiluna, väärennyksenä tai petoksena syyksi luettava rikos, joka ei kuitenkaan ole edennyt tunkeutumista pitemmälle, on tekoa arvosteltava mainittujen rikosten rangaistavana yrityksenä. Koska vahingonteon yritystä ei ole säädetty rangaistavaksi, on vahingoittamistarkoituksin tapahtuneessa tietojärjestelmään tunkeutumisessa kysymys tietomurrosta, ellei vahinkoa ole ehditty aiheuttaa.

Tietomurtosäännöksen toisen momentin mukaan tuomitaan tietomurrosta myös se, joka tietojärjestelmään tai sen osaan tunkeutumatta teknisen erikoislaitteen avulla oikeudettomasti ottaa selon tietojärjestelmässä olevasta tiedosta. Perustelujen mukaan säännöksellä tarkoitetaan esimerkiksi sellaista tiedon hankkimista, jossa tietojärjestelmässä oleva tieto saadaan selville käyttämällä laitetta, joka tietojärjestelmästä lähtevän säteilyn perusteella pystyy selvittä-

---

[16] Lakivaliokunta on mm. Suomen kaupunginviskaaliyhdistys ry:n kiinnitettyä lausunnossaan asiaan huomiota päätynyt mietinnössään toteamaan perustelujen olevan tältä osin virheelliset. LaVM 22/94, s. 18.

[17] Ks. Silvander, s. 258.

mään järjestelmässä käsiteltävän tiedon sisällön; näin ollen säännös soveltuu myös sellaiseen siirrettävänä olevan viestin sieppaamiseen, johon viestintäsalaisuuden loukkausta koskeva säännös ei sovellu esimerkiksi sen vuoksi, että tiedonsiirto ei tapahdu televerkossa.[18]

Tietomurtosäännös käytännössä

Tietomurtosäännöksen ensisijaisena tarkoituksena on suojata tietojenkäsittelyrauhaa hakkerien – tai oikeammin krakkerien[19] – toiminnalta. Nähtäväksi jää, kuinka laajaksi säännöksen soveltamisala muodostuu; ellei järjestelmään tunkeutuja tyydy pelkkään sisäänpääsyyn vaan alkaa tavalla tai toisella käyttää järjestelmää, muuttuu teko joksikin muuksi, vähintäänkin luvattomaksi käytöksi. Tuntuu todennäköiseltä, että useimmille tunkeutujille pelkkä turvajärjestelyn murtaminen ei riitä. Tätä osoittaa sekin, että vuoden 1996 loppuun mennessä poliisin tutkittavaksi ei ollut tullut yhtään yksinomaan tietomurtoa koskevaa juttua ja sen jälkeiseltäkin ajalta alioikeusratkaisuja on vain muutama.[20]

Toisaalta säännös lienee hyvin pitkälti tarkoitettu toimimaan ennalta ehkäisevänä pelotteena – tosiasiahan on, että jokainen käynti tietojärjestelmässä ja jokainen tunkeutumisyritys jättää jälkiä ja tekijä on ainakin periaatteessa jäljitettävissä. Sitä paitsi poliisin kannalta säännös on erittäin käyttökelpoinen: tietojärjestelmään kohdistuneessa tunkeutumisen tai sen yrityksen käsittäneessä teossa on lähes poikkeuksetta kysymys ainakin tietomurron yrityksestä ja näin ollen tutkinnalle on aina olemassa selkeä lähtökohta. Vaikka epäiltäisiinkin luvatonta käyttöä, viestintäsalaisuuden loukkausta tai vahingontekoa, ei tuomittavaa rangaistusta ajatellen olisi välttämätöntä uhrata tutkintaresursseja enempien yksityiskohtien selvittämiseen, jos tietomurrosta on saatavissa täysi näyttö. Kysyä tietysti sopii, miten järkevä tällainen tilanne on. Palaan näihin kysymyksiin käytännön esimerkkien valossa jäljempänä luvatonta käyttöä käsitellessäni.

Omassa syyttäjäntoimessani olen käsitellyt joitakin tietomurtoa koskevia juttuja.[21] Näistä seuraavassa muutama esimerkki:

---

[18] Kysymyksestä Ruotsin oikeuden kannalta ks. Silvander, s. 247.

[19] Hakkerin ja krakkerin käsitteistä lisää jäljempänä luvattoman käytön yhteydessä.

[20] Ks. Rikollisuustilanne 2000, josta ilmenee (s. 305), että vuonna 1998 yleisissä alioikeuksissa käsiteltiin kaksi tietomurtojuttua, seuraavana vuonna kolme ja vuonna 2000 vain yksi. Absoluuttiluvut ovat siis varsin pieniä mutta esimerkiksi vuoden 2000 juttu oli huomattavan laaja. Rikollisuustilanne 2001 -kirja ei sisällä vastaavaa tietoa vuodelta 2001 mutta juttujen määrässä ei ole tapahtunut oleellista muutosta. Rikollisuustilanne 2002 -teoksesta ei kysymyksessä olevia tietoja myöskään ilmene mutta tiedän tietomurtojuttuja jonkin verran aikaisempaa enemmän esiintyneen.

[21] Mahdollisuus saada tällaisia juttuja käsiteltäväksi oman toimialueen ulkopuoleltakin on tarjoutunut syyttäjälaitoksen ns. avainsyyttäjäjärjestelmän myötä: tietotekniikkarikokset on yksi rikoslajeista, joihin on määrätty avainsyyttäjiä eli syyttäjiä, jotka ovat velvollisia perehtymään aiheeseensa keskivertosyyttäjää syvällisemmin ja konsultoimaan muita syyttäjiä samoin kuin tarvittaessa valtakunnansyyttäjän määräyksestä hoitamaan syyttäjäntehtäviä missä tahansa valtakunnan alueella. Tietotekniikkarikosten avainsyyttäjänä toimii lisäkseni Nokian johtava kihlakunnansyyttäjä Mika Mäkinen ja Valtakunnansyyttäjänvirastossa toimintaamme ohjaa ja koordinoi valtionsyyttäjä Jarmo Rautakoski.

> A oli 5.12.1997 Turussa käyttäen hänelle kuulumatonta käyttäjätunnusta ja salasanaa oikeudettomasti tunkeutunut B Oy:n tietojärjestelmään. A oli 2.12.1997 vieraillessaan B Oy:n tietojärjestelmässä työnantajansa käyttäjätunnusta ja salasanaa oikeutetusti käyttäen kopioinut yhtiön salasanatiedoston, minkä jälkeen oli ns. hakkeriohjelmaa käyttämällä saanut selvitetyksi kaksi salasanaa, joista toisen avulla oli tehnyt edellä selostetun tunkeutumisen. Vieraan käyttäjätunnuksen ja salasanan avulla A:lla olisi ollut mahdollisuus käyttää tietojärjestelmää tavalla, johon ainoastaan käyttäjätunnuksen ja salasanan haltijalla oli oikeus.[22]

Juttu oli alun perin tutkittu viestintäsalaisuuden loukkauksena, koska epäiltiin A:n lukeneen B Oy:n asiakkaiden sähköposteja, mutta näyttöä siitä, että A järjestelmään päästyään olisi siellä jotain tehnyt, ei esitutkinnassa saatu. A itse kertoi oikeudessa tarkoituksenaan olleen vain turvallisuusaukkojen paljastamisen. A tuomittiin tietomurrosta lievään sakkorangaistukseen.

Jos A:n menettely olisi käsittänyt vain salasanatiedoston kopioimisen (hän ei esimerkiksi olisi kyennyt käyttämällään ohjelmalla selvittämään yhtään salasanaa), olisi kysymyksessä joka tapauksessa ollut tietomurron yrityksenä rangaistava teko, sillä myöhempää tunkeutumistarkoitusta varten tehty kopiointi on katsottava valmisteluvaiheesta jo yritysasteelle edenneeksi tietomurroksi. Salasanat ovat tiedostona olleet A:n hallussa.

Porttiskannausjuttu

Tärkeään korkeimman oikeuden ennakkopäätökseen johti seuraava tapaus:

> C oli syytteen mukaan 23.11.1998 Helsingissä yrittänyt murtaa turvajärjestelyn tunkeutuakseen oikeudettomasti OPK-Osuuskunnan tietojärjestelmään. C oli suorittanut niin sanotun porttiskannauksen eli erityistä tietokoneohjelmaa käyttämällä skannannut läpi osuuskunnan internetiin yhteydessä olevan verkon kaikki osoitteet tarkoituksin löytää avoimia välityspalvelimia. Skannaus ei ollut läpäissyt osuuskunnan tietojärjestelmän palomuuria. Mikäli C olisi löytänyt avoimen välityspalvelimen, olisi hän sitä kautta kyennyt saamaan jatkoyhteyden internetiin niin, että yhteys olisi näyttänyt tulleen tästä välityspalvelimesta. Vaadin C:lle rangaistusta tietomurron yrityksestä.

Turun käräjäoikeus[23] hylkäsi syytteen, koska ei katsonut selvitetyksi, että juuri C olisi tehnyt kysymyksessä olevan porttiskannauksen.[24]

---

[22] Dnro R 98/704.

[23] Turun käräjäoikeus siksi, että C oli turkulainen ja oli toiminut kotonaan ollutta tietokonetta käyttämällä. Verkon välityksin tehdyissä laajemmissa tietomurtojutuissa ei laillisista tuomioistuimista yleensä ole pulaa, joskin toistaiseksi jutut on yleensä käsitelty vastaajan kotipaikan eli tosiasiallisen toimimispaikan tuomioistuimessa.

[24] C oli samalla kertaa syytteessä myös tietoliikenteen häirinnästä. Hän oli tunkeutunut puhelinpalveluja tarjonneen Turun Puhelin Oy:n palvelimelle ja häirinnyt televiestintää siirtämällä ilki-

C:n syyllisyyden puolesta puhunut näyttö oli sinänsä (mielestäni) vahva ottaen vielä huomioon, että hän esitutkinnassa oli itse asiassa myöntänyt menetelleensä syytteessä selostetuin tavoin. Tästä myöntämiseksi tulkittavissa olleesta kannanotosta olikin johtunut, että esitutkinnassa ei ollut hankittu televalvontatietoja. Oikeudessa C kiisti syytteessä kuvatun menettelyn ja piti mahdollisena, että joku muu joko oli väärentänyt hänen IP-osoitteensa, käyttänyt hänen tietokonettaan tai käyttänyt hänen tietokoneellaan ollutta välityspalvelinta.

Valitin asiasta Turun hovioikeuteen, joka päätyi toiseen lopputulokseen kuin käräjäoikeus ja tuomitsi C:n tietomurron yrityksestä sakkorangaistukseen.[25] Hovioikeuden päätöksen perustelut ansaitsevat tulla osittain siteeratuiksi:

> On riidatonta, että kysymyksessä oleva yhteys oli tullut C:n koneen IP-osoitteella. – – Hän ei kuitenkaan tiennyt, että olisi skannannut pankin verkon. Joku muu oli saattanut väärentää IP-osoitteen ja tehdä porttiskannauksen siten, että oli näyttänyt siltä, että yhteys oli tullut C:n koneelta.
>
> (Todistajien) K:n ja P:n kertomuksista ilmeni, että jos joku muu olisi tehnyt porttiskannauksen C:n väittämällä tavalla, vastaus olisi kuitenkin tullut C:lle eikä porttiskannauksen tekijälle. Porttiskannaus olisi tuolloin ollut tekijälleen hyödytön. K:n ja etenkin P:n kertomuksista ilmeni kyllä myös, että sinänsä on mahdollista, että mahdollinen osoitteen väärentäjä olisi voinut toimia siten, että hän olisi saanut vastauksen itselleen. P:n kertomuksesta ilmeni kuitenkin, että hänen käsityksensä mukaan tuollainen toiminta olisi kuitenkin vaatinut niin suurta osaamista, ettei ole uskottavaa, että niin taitava henkilö olisi yrittänyt hankkia haluamiaan tietoja tässä tapauksessa käytetyllä menetelmällä.
>
> P:n kertomuksesta ilmeni myös, että väärennetystä osoitteesta olisi todennäköisesti jäänyt jälkiä C:n käyttämän verkkopalveluyhtiön palvelimelle ja että luvattomasta käyttämisestä olisi jäänyt jälkiä C:n tietokoneelle. Verkkopalveluyhtiö oli P:n pyynnöstä sittemmin tutkinut asiaa eikä merkkejä väärennetyn osoitteen käyttämisestä ollut löytynyt. P on kollegansa kanssa tutkinut C:n kovalevyn kopiot eikä jälkiä luvattomasta tunkeutumisesta ollut löytynyt.
>
> P:n kertomuksesta ilmeni kuitenkin myös, ettei näillä uusillakaan tutkimuksilla kuitenkaan voinut kokonaan pois sulkea osoitteen väärentämisen mahdollisuutta.
>
> Asian tutkinnassa on jätetty selvittämättä, mistä puhelinnumerosta yhteys oli tullut. Tuo seikka olisi ollut selvitettävissä tutkinnassa. Lisäksi C:n koneella on ollut myös sellainen ohjelma, jonka välityksellä joku ulkopuolinen olisi voinut toimia. Kun osoitteen väärentäminen on mah-

---

valtaisessa tarkoituksessa palvelimelle useita satoja kuvatiedostoja, jotka olivat sisältäneet pääasiassa pornografista kuvamateriaalia. C:n siirtämien tiedostojen koko oli yhteensä ollut useita kymmeniä megatavuja. Tällaisen kuvamateriaalin löytyminen yhtiön palvelimelta vaikutti huonontavasti yhtiön maineeseen ja myös ruuhkautti palvelimen tiedon kuvien olemassaolosta levittyä nuoren yleisön piiriin. Tästä tietoliikenteen häirinnästä C tuomittiin sakkorangaistukseen.

[25] Turun HO tuomio nro 1304 4.6.2001.

> dollista ja kun C esitutkinnassa oli kertonut, että hänen konettaan on hakkeroitu siten, että on yritetty selvittää salasanatiedostoja, on tutkinta suoritettu puutteellisesti, kun puhelinnumero on jätetty selvittämättä. Se, ettei puhelinnumero ole tiedossa, on syytettä vastaan puhuva seikka.
>
> Asiassa on mahdollista, että joku muu on tehnyt teon C:n väittämällä tavalla. Kuitenkin tuomitsemiseen riittävä näyttö on vahvimmillaankin perimmältään vain todennäköisyysnäyttöä. Ehdottoman varman totuuden selvittäminen on yleensä mahdotonta. Kysymys on siitä, mitä pidetään uskottavana.
>
> K:n ja P:n kertomuksista on pääteltävissä, että on epätodennäköistä, että yhteys olisi tullut muualta kuin C:n koneelta. C:llä on ollut koneellaan sellainen ohjelmisto, jolla kyseinen teko on voitu tehdä ja hän on kertonut myös tehneensä joskus kyseisen kaltaisia porttiskannauksia. Tämän tapauksen olosuhteissa ei ole syytettä vastaan puhuvasta seikasta huolimatta uskottavaa, että yhteys olisi tullut jostakin muualta kuin C:n koneelta.

Päätöksessä ei ole mielenkiintoista niinkään se, että siinä todetaan porttiskannauksen toteuttavan tietomurron yrityksen tunnusmerkistön, joskin tälläkin lopputuloksella oli toki relevanssia asian myöhemmän käsittelyn kannalta. Tosin tätä kysymystä ei käräjäoikeudessa sen paremmin kuin hovioikeudessakaan juuri käsitelty, painopiste oli syyllisyyden tueksi esitetyn näytön arvioinnissa.

Erityisen tyytyväinen olen syyttäjänä siihen tapaan, jolla hovioikeus asetti tuomitsemiskynnyksen: käsitykseni mukaan verkkorikoksissa on usein yksinkertaisesti mahdotonta löytää absoluuttisen varmaa lopputulosta. Kun C hovioikeudessa jatkuvasti toisti, että se ja se on *mahdollista,* päädyin itse – kieltämättä epäasiallisesti – sanomaan, että mahdollistahan toki on sekin, että jokin avaruusolio on käyttänyt osuuskunnan tietokonetta ja skannannut D:n tietojärjestelmän mutta että se yksinkertaisesti ei ole uskottavaa. *Tätä* ei hovioikeuskaan pitänyt uskottavana.

C sai korkeimmalta oikeudelta valitusluvan ja korkein oikeus antoi tuomionsa 8.4.2003.[26] Tuomiossa ei muutettu hovioikeuden tuomion lopputulosta.

C oli vaatinut ensisijaisesti tietomurron yrityksiä koskevien syytteiden samoin kuin vahingonkorvausvaatimusten hylkäämistä ja joka tapauksessa vahingonkorvausten sovittelemista.

Korkein oikeus joutui tavallaan ensimmäisenä oikeusasteena ottamaan nimenomaisesti kantaa porttiskannauksen rikosoikeudelliseen luonteeseen. Korkein oikeus, joka tuomiossaan hyväksyy hovioikeudessa suoritetun näytön arvioinnin, perustelee porttiskannauksen katsomista tietomurron yritykseksi mm. seuraavalla tavalla:

---

[26] KKO 2003:36, dnro R2001/678.

> C on katsonut, ettei hän ole voinut syyllistyä tietomurron yritykseen, koska skannauksella ei yritetä tunkeutua järjestelmään väkisin vaan pelkästään todeta avoimet palvelut. Järjestelmään pääseminen tällä tavoin ei myöskään edellytä turvajärjestelyjen murtamista, koska se ei edellytä minkään salaisen tunnuksen tai tiedon käyttämistä.
>
> Kuten [rikoslain 38 luvun 8 §:ää] koskevassa hallituksen esityksessä todetaan, järjestelmään tunkeutumiselle ei edellytetä mitään erityistä tarkoitusta. Säännös soveltuu siten myös urheilumielessä tapahtuvaan tunkeutumiseen. Tietomurron yrityksen rangaistavuus taas on tarkoitettu helpottamaan puuttumista tietojärjestelmien luotettavuuden ja turvallisuuden[27] kannalta huolestuttavaan käyttäjätunnusten tai muiden turvajärjestelyjen järjestelmälliseen selvittämiseen. Rangaistavaksi on saatettu jo se, että tekijä yrittää selvittää tietojärjestelmää turvaavan käyttäjätunnuksen tai murtaa muun turvajärjestelyn, jos teko tehdään tarkoituksella tunkeutua oikeudettomasti tietojärjestelmään. Ilmaisua murtaa on käytetty säännöksessä kielikuvana ilmaisemaan sitä, että turvajärjestelyn läpäisyn täytyy olla luvatonta.
>
> – –
>
> Porttiskannausohjelmalla on näin ollen mahdollista järjestelmällisesti selvittää tietojärjestelmän mahdollisia aukkoja ja sen heikkoja kohtia. Toimenpiteen avulla kyetään saamaan tietoja, jotka mahdollistavat myös luvattoman pääsyn kohteena olevaan järjestelmään. Ohjelmaa käyttämällä hankitun tiedon avulla voidaan siten laissa tarkoitetuin tavoin murtaa tietojärjestelmän turvajärjestely. Kuten lain esitöissä todetaan jo se, että yrittää hankkia tällaisen luvattoman pääsyn järjestelmään mahdollistavan tiedon, on rangaistavaa, jos se tehdään tarkoituksella oikeudettomasti tunkeutua tietojärjestelmään.
>
> – –
>
> Kun kyseessä olevan tietojärjestelmän skannaaminen on ollut järjestelmällistä eikä ole uskottavaa, että tällaisen skannauksen kautta saatavalla tiedolla olisi ollut C:lle käyttöä muussa tarkoituksessa kuin luvattomasti tietojärjestelmään pyrittäessä, Korkein oikeus katsoo, että C on suorittanut skannauksen tarkoituksin sen kautta saatavan tiedon avulla tunkeutua tietojärjestelmään. Näin ollen C on syyllistynyt hovioikeuden hänen syykseen lukemaan osuuskunnan tietojärjestelmään kohdistuneeseen tietomurron yritykseen.

Korkeimman oikeuden ratkaisulla saattaa olla arvaamattoman kauaskantoisia seurauksia, sillä porttiskannaus on nykyään yleistynyt valtavasti verrattuna C:n rikoksen tekoaikaan eli vuoteen 1998. Ei liene liioittelua väittää, että tällä tavoin tehtyjä tietomurron yrityksiä tapahtuu yksin Suomessa päivittäin ainakin satoja mutta todennäköisesti jopa tuhansia. Tosin valtaosa yrityksistä jää uhreilta huomaamatta kilpistyessään järjestelmien palomuureihin ja huomatuistakin suurin osa jää tulematta viranomaisten tietoon.

---

[27] Eli tietojenkäsittelyrauhan (tekijän huom.).

Korkein oikeus on ratkaisussaan katsonut rangaistavaksi yritykseksi menettelyn, joka asiallisesti tuntuisi olevan varsin lähellä valmistelua. *Tolvanen* on tapausta kommentoidessaan kiinnittänyt huomiota siihen, että korkein oikeus ei ole tässä tapauksessa lainkaan pohtinut yrityksen kelvollisuuden ongelmaa, ja lausuu tältä osin mm. seuraavasti:[28]

> Kelvollinen yritys on silloin, kun voidaan sanoa oikeushyvälle aiheutuneen täytäntöönpanotoimesta konkreettisen vaaran. Täydentävänä kriteerinä on se, että konkreettinen vaara on jäänyt aiheutumatta satunnaisesta syystä. Korkein oikeus ei ole ottanut kantaa, miten todennäköistä osuuskunnan niin sanotun palomuurin läpäisy olisi ollut. Tapauksesta on pääteltävissä, että KKO piti sitä kuitenkin mahdollisena. Olisi kuitenkin ollut paikallaan pohtia, miten todennäköistä tietojärjestelmään pääsyn mahdollistavan tiedon saanti oli juuri tässä tapauksessa.
>
> Voidaan tietysti ajatella, että tietomurron yritys on puhdas tekorikos, jossa konkreettisen vaaran tai ylipäätään vaaran kriteeristä on luovuttu. Korkein oikeus on tulkinnut maksuvälinepetoksen tunnusmerkistöä juuri näin.

Tolvanen kuvailee lyhyesti edellä käsiteltyä ratkaisua KKO 1999:110 ja toteaa lopuksi, että ”todennäköisyys päästä palomuurin läpi lienee olennaisesti suurempi kuin mahdollisuus arvata toisen henkilön pankkikortin salainen tunnusluku niillä kahdella tai kolmella kerralla, jotka automaatti sallii ennen kortin jäämistä automaattiin”. Näin varmasti on, sillä palomuurin läpäiseviä tietojärjestelmään tunkeutumisia sentään tapahtuu, kun taas ainakaan minun tiedossani ei ole, että joku olisi onnistunut puhtaalla arvauksella käyttämään toiselle kuuluvaa pankkikorttia.

Vantaan hakkerijuttu

Helsingin käräjäoikeus antoi 5.12.2003 lainvoimaiseksi jääneen tuomion,[29] jossa kahden nuoren tekijän suorittamien skannausten kohteiksi joutuneiden järjestelmien haltijoita oli liki 200 000 eri puolilla maailmaa. Uhrien henkilöllisyys oli kyetty selvittämään vain vähäisiltä osin (eikä henkilöllisyyksiä edes ollut yritetty laajalti selvittää; tämä rajaus tehtiin heti tutkinnan alkuvaiheessa), vaikkakin kaikkien skannattujen järjestelmien IP-osoitteet olivat tiedossa, ja vain muutama kymmenen oli esittänyt rangaistusvaatimuksia. Katsoin rikoslain 38 luvun 10 §:n 2 momentin – ja epäiltyjen luvattomien käyttöjen osalta 28 luvun 15 §:n 1 momentin – perusteella erittäin tärkeän yleisen edun tässä

---

[28] Tolvanen, s. 259 s.

[29] Helsingin KO osasto 4/3 5.12.2003 nro 03/11655. Juttu on julkisuudessa tunnettu ns. ”Vantaan hakkerijuttuna”, koska tutkintapyyntö tehtiin tammikuussa 2002 Vantaan poliisilaitokselle, joka jutun myös tutki. Tämän kirjoittaja määrättiin jutun syyttäjäksi heti tutkinnan alkuvaiheessa.

tapauksessa vaativan syytteen nostamista myös niiden asianomistajien osalta, joista ainoa tieto on heidän järjestelmiensä IP-osoite.

Käräjäoikeus hyväksyi tämän näkemyksen ja lausui tältä osin lyhyesti seuraavaa:

> Huomioon ottaen vastaajien rikollisen toiminnan laajuus ja todistaja T:n kertomus toiminnan merkittävyydestä on rikoslain 28 luvun 15 § 1 momentissa ja 38 luvun 10 § 2 momentissa tarkoitettu erittäin tärkeä yleinen etu syytteen nostamiselle kaikkien syytekohtien osalta ollut olemassa.

Tämä ei kuitenkaan merkinnyt sitä, että vastaajat olisi tuomittu 200 000 asianomistajaan kohdistuneesta tietomurron yrityksestä. Korkeimman oikeuden edellä käsitellystä ratkaisusta keskusteltiin oikeudenkäynnin aikana ja vastaajat katsoivat, että tässä tapauksessa, kun porttiskannauksella ensin oli ainoastaan haettu tietoturva-aukon sisältäviä järjestelmiä ja vasta näiden löydyttyä oli toista ohjelmaa käyttäen yritetty tunkeutua ja joissakin tapauksissa tunkeuduttu itse järjestelmiin, skannaaminen olisi katsottava ainoastaan tietomurron yrityksen valmisteluksi. Itsekin asetuin varovaisesti samalle kannalle.

Käräjäoikeus oli lopulta myös samaa mieltä ja lausui perusteluissa seuraavaa:

> Lain esitöiden mukaan jo se, että yrittää hankkia luvattoman pääsyn järjestelmään mahdollistavan tiedon on rangaistavaa, jos se tehdään tarkoituksella oikeudettomasti tunkeutua tietojärjestelmään.
>
> Huomioon ottaen vastaajien kertomus käyttämästään tekniikasta sekä todistajan kertomus porttiskannauksesta sekä varsinaisen murron edellyttämistä manuaalisista jatkotoimenpiteistä käräjäoikeus toteaa porttiskannauksen käsiteltävässä tapauksessa olleen pääsääntöisesti luonteeltaan rikosoikeudellisesti rankaisematonta rikoksen valmistelua. Porttiskannauksen luonnetta valmistelevana toimena käsiteltävänä olevassa tapauksessa tukee skannattujen kohteiden lukuisuus.
>
> Vastaajat ovat myöntäneet skannanneensa syytteessä esitetyssä laajuudessa tarkoituksella etsiä mahdollisia kiinnostavia murtokohteita. Kukin kohde on skannauksen jälkeen valikoitu erikseen manuaalisen murtamisen kannalta välttämättömien jatkotoimenpiteiden kohteeksi. Murretuksi valikoituja kohteita on ollut vain murto-osa skannatuista kohteista.
>
> Käräjäoikeus katsoo, edellä esitetyt kertomukset huomioiden, jääneen näyttämättä vastaajien syyllistyneen syytekohdissa 1 ja 2 myöntämäänsä laajempaan tietomurron yritykseen. Vastaajien tarkoituksena ei ole näytetty olleen oikeudettomasti tunkeutua kaikkiin niihin lukuisiin tietojärjestelmiin, joista porttiskannaus oli vastaajille tietoa antanut.

Toinen vastaajista tuomittiin tietomurron yrityksestä, tietomurrosta, luvattomasta käytöstä ja tietoliikenteen häirinnästä 50 päivän ehdolliseen vankeusrangaistukseen. Toiselle vastaajista luettiin mainittujen tekojen lisäksi syyksi myös

vaaran aiheuttaminen tietojenkäsittelylle[30] ja hänet tuomittiin kolmen kuukauden ehdolliseen vankeusrangaistukseen. Vahingonkorvauksia tuomittiin kaikkiaan n. 18 000 euroa ja asianomistajien oikeudenkäyntikuluja kertyi korvattavaksi n. 3 500 euroa.

Helsingin käräjäoikeus otti siis selkeästi korkeimman oikeuden näkemyksestä poikkeavan kannan, jota kuitenkin käsitykseni mukaan voidaan tämän laajuisessa jutussa pitää varsin perusteltuna. Vastaajien olisi ollut käytännössä täysin mahdotonta edes yrittää murtautua kaikkiin niihin vajaaseen 200 000 järjestelmään, joiden haavoittuvuudesta he skannauksella olivat hankkineet tiedon – jos yhteen murtautumisyritykseen / murtautumiseen käyttäisi aikaa viisi minuuttia, vaatisi 200 000 järjestelmän läpikäyminen lähes kahden vuoden *tauottoman* työn; jos päivittäinen hakkerointiaika olisi kahdeksan tuntia ja toimintaa tapahtuisi *joka* päivä, veisi operaatio siis aikaa kuutisen vuotta.

Korvauksista

On syytä kiinnittää huomiota yhteen kumpaankin edellä käsiteltyyn tapaukseen liittyvään rikosoikeudelliselta moitittavuudeltaan sinänsä jokseenkin vähäisille tietomurtojutuille ominaiseen piirteeseen: asianomistajien korvausvaatimukset saattavat nousta hyvin korkeiksi, sillä ryhtymättä laajoihin tarkastus- ja uudelleenasennustoimiin on mahdotonta saada varmuutta siitä, ettei syyllisen menettelystä ole järjestelmälle aiheutunut vahinkoa. Tietojen luottamuksellisuus, yksi tietojenkäsittelyrauhan olennaisista osa-alueista, on menetetty.

Korkeimpaan oikeuteen päätyneessä porttiskannaustapauksessa asianomistajan korvausvaatimukset nousivat noin neljännesmiljoonaan markkaan, ja tämä johtaa helposti ajatukset siihen, että vastaajan oikeudenkäynnissä esittämä muuttunut käsitys syyllisyydestään olisikin johtunut ensisijassa pyrkimyksestä välttää vahingonkorvaukset eikä niinkään rangaistuksen pelosta. Hovioikeus velvoitti C:n korvaamaan asianomistajataholle aiheuttamistaan vahingoista yhteensä 75 000 markkaa ja oikeudenkäyntikuluista 17 950 markkaa, mikä sekin on kieltämättä paljon verrattuna 1 400 markan sakkorangaistukseen. C:n korvattaviksi tulleet asianomistajien oikeudenkäyntikulut korkeimmassa oikeudessa olivat 500 euroa.

Korkeimman oikeuden ratkaisu on mielenkiintoinen myös vahingonkorvauksia koskevilta osiltaan. C:hän oli toissijaisesti vaatinut korvauksia soviteltaviksi. Korkein oikeus lausuu asiasta mm. seuraavaa:

> – – C:n vetoamista seikoista hänen ikänsä ja varallisuusolonsa puoltavat korvausten sovittelemista. Harkintaperusteita ovat kuitenkin myös C:n kehitystaso, teon laatu ja muut tekoon liittyvät olosuhteet.

---

[30] Selostan juttua tältä osin tarkemmin jäljempänä käsitellessäni vaaran aiheuttamista tietojenkäsittelylle.

> C on nuoresta iästään huolimatta kokenut tietokonealan harrastaja ja hän on tahallaan yrittänyt tunkeutua toisen tietojärjestelmään. Sillä, että hän ei ole tiennyt kohteena olevan juuri osuuskunnan tietojärjestelmä, ei ole tässä suhteessa merkitystä. C:n on täytynyt kokemuksensa ja tietojensa perusteella ymmärtää, että jo pelkkä tunkeutuminen tietojärjestelmään aiheuttaa vahinkoa, vaikka tietojärjestelmän tietoja ei tunkeutumisen yhteydessä kopioida, muuteta tai hävitetä. Sanottu koskee myös tietojärjestelmään tunkeutumisen yritystä. Vahinko ilmenee tietoturvallisuuskustannusten nousuna, joista keskeisimpiä ovat turvajärjestelyjen uudistaminen, tietoturvallisuusjärjestelmän lisääntynyt valvontatarve ja sen selvittäminen, onko ilmi tullut tietojärjestelmään tunkeutuminen ollut harmitonta vai onko tietojärjestelmää vahingoitettu, muutettu tai kopioitu.
>
> Tässä tapauksessa osuuskunnalle tietojärjestelmän omistajana ja yhtiölle tietojärjestelmän hoitajana rikoksen selvittämiseen käytetyn henkilökunnan palkoista ja ulkopuolisten asiantuntijoiden käyttämisestä aiheutuneet kustannukset ovat tyypillisesti ja ennalta-arvattavasti tietojärjestelmään tunkeutumisesta tai sen yrittämisestä aiheutuvaa vahinkoa, jonka C on velvollinen korvaamaan.
>
> Ottaen huomioon tietoturvallisuuden tärkeyden, teon tahallisuuden ja laadun sekä sen, että C teon tehdessään on kyennyt ymmärtämään siitä aiheutuvan vahingonvaaran, Korkein oikeus katsoo, ettei vahingonkorvauksia ole perusteltua tässä tapauksessa sovitella.

Arvostettu tietotekniikka-asiantuntija, diplomi-insinööri *Petteri Järvinen* on jokseenkin kriittisesti kommentoinut korkeimman oikeuden ratkaisua sen korvausvelvollisuutta koskevalta osalta.[31] *Järvisen* mukaan pankin kaltaisen organisaation tulisi joka tapauksessa huolehtia tietoturvastaan. Päätöksen soveltaminen reaalimaailmaan merkitsisi hänen mukaansa sitä, että pankki voisi vaatia korvauksia henkilöiltä, jotka tarttuvat pankin oveen iltaisin ja viikonloppuisin.

Korkeimman oikeuden kanta on kieltämättä tiukka, mutta oman käsitykseni mukaan se ottaa juuri oikealla tavalla huomioon reaalimaailman ja tietoteknisen ympäristön oleellisimmat erot. *Järvisen* vertausta käyttääkseni: jos joku illalla oven kautta tunkeutuu pankkiin, jää tunkeutumisesta niin selvät jäljet, että tunkeutumisen havaitseminen ei edellytä kustannuksia aiheuttavia lisätöitä. Vaikka ovi olisikin jäänyt auki ja pankkiin olisi ollut vaivatonta tulla, olisi silti jokseenkin helppoa havaita, onko pankkisalissa tehty jotain sopimatonta.

Tietojärjestelmään tunkeutumisesta ei ainakaan osaavan murtautujan jäljiltä välttämättä juurikaan jälkiä jää. Sen havaitseminen, onko jotain pankin tietojärjestelmässä olevaa dataa kenties muutettu, on jo hyvin vaikeaa ja suuritöistä. Lainsäätäjä ei ole tosin kriminalisoinut tietomurtoa erityisen ankarasti mutta on toisaalta säännöksen perusteluista havaittavin tavoin asettanut yrityksen täyttymiskynnyksen varsin matalaksi ja tällä tavoin ilmaissut haluavansa kohdella

---

[31] Ks. Järvinen, Tietokone ja HeSa. Ks. myös Tolvanen, s. 259, jossa lievempää kritiikkiä.

tietojärjestelmään murtautujaa toisella tavalla kuin autovarasta tai asuntomurron tekijää.

On tietysti totta, että tietojärjestelmien haltijoilla on vastuunsa järjestelmien tietoturvallisuuden tasosta. Oikeuskäytäntöä siitä, miten turvallisuusjärjestelyjen laiminlyöminen vaikuttaisi korvausvelvollisuuteen, ei toistaiseksi ole, mutta tuntuu siltä, että laiminlyönnin pitäisi olla melkoisen huomattava, jotta se voisi vaikuttaa korvauksia alentavasti.

Tietyllä tavalla poikkeukselliseksi C:n tapauksen tekee vielä se, että asianomistaja, joka on suuri pankkitoimintaa harjoittava osuuskunta, oli ylipäänsä tehnyt rikosilmoituksen. Valtaosa tämän tyyppisiin asianomistajiin kohdistuneista tietomurtorikoksista jää tutkimatta, koska virallista tutkintapyyntöä ei tehdä, olkoonkin, että asianomistajat usein ovat yhteydessä poliisiin havaittuaan järjestelmissään asiaan kuulumatonta liikehdintää.

Tietomurron ja luvattoman käytön välinen rajanveto oli esillä myös niin sanotussa TCB-jutussa eli Suomen tähän mennessä laajimmassa tuomioistuimessa käsitellyssä tietotekniikkarikosasiassa, jossa toimin valtakunnansyyttäjän määräyksestä syyttäjänä ja josta Jyväskylän käräjäoikeus antoi tuomionsa 22.2.2001. Vaasan hovioikeus käsitteli asian vastaajan ja syyttäjän valitettua ja antoi tuomionsa 18.6.2002.[32] Hovioikeuden ratkaisu jäi lainvoimaiseksi sillä korkein oikeus ei myöntänyt syytetylle valituslupaa. Selostan tätä juttua jäljempänä erityisesti luvattoman käytön yhteydessä.

EN ja tietomurto

Euroopan neuvoston minimilistalla on luvatonta järjestelmään tunkeutumista (unauthorised access) koskeva suositus, jota 38 luvun 8 §:n säännös vastaa. Euroopan neuvoston tietoverkkorikosyleissopimuksen 2 artikla sisältää myös tietomurtoa koskevan säännöksen:

> *Luvaton tunkeutuminen.* Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin säätääkseen tahallisen ja oikeudettoman tietojärjestelmään tai sen osaan tunkeutumisen kansallisen lainsäädäntönsä mukaisesti rangaistavaksi teoksi. Sopimuspuoli voi asettaa rangaistavuuden edellytykseksi sen, että rikos on tehty turvajärjestelyt murtamalla, tarkoituksin päästä käsiksi dataan tai muuta epärehellistä tarkoitusta varten tai että se liittyy tietojärjestelmään, joka on kytketty toiseen tietojärjestelmään.[33]

---

[32] Vaasan HO 18.6.2002 nro 745 (dnro R 01/533).

[33] *Illegal Access.* Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law when committed intentionally the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Artikla ei aiheuta meillä tarvetta lainmuutoksiin. Artiklan loppuosan kvalifiointimahdollisuudet on otettu tekstiin helpottamaan eräiden valtioiden implementointityötä; esimerkiksi mahdollisuus vaatia tunkeutumisen kohteena olevan tietojärjestelmän olemista kytkettynä toiseen tietojärjestelmään lisättiin Japanin toivomuksesta, jottei Japanin tarvitsisi kriminalisoida yksittäiseen tietokoneeseen *(stand-alone computer)* kohdistuvaa tietomurtoa. Yleissopimuksessa tietojärjestelmän käsite on ymmärretty laajasti: se tarkoittaa yhtä lailla yksittäistä sylimikroa kuin Internetiäkin.[34]

2.1.2 Yritysvakoilu (RL 30:4)

Vuoden 1991 alusta tuli rikoslakiin yritysvakoilun kriminalisoiva säännös, jossa osaltaan on muun ohessa kysymys myös tietomurrosta eli oikeudettomasta tietojärjestelmään tunkeutumisesta:

> Joka oikeudettomasti hankkii tiedon toiselle kuuluvasta yrityssalaisuudesta
> 1) tunkeutumalla ulkopuolisilta suljettuun paikkaan taikka ulkopuolisilta suojattuun tietojärjestelmään,
> 2) hankkimalla haltuunsa tai jäljentämällä asiakirjan tai muun tallenteen taikka muulla siihen rinnastettavalla tavalla tai
> 3) käyttämällä teknistä erikoislaitetta tarkoituksin oikeudettomasti ilmaista tällainen salaisuus tai oikeudettomasti käyttää sitä, on tuomittava, jollei teosta ole muualla laissa säädetty ankarampaa rangaistusta, *yritysvakoilusta sakkoon* tai vankeuteen enintään kahdeksi vuodeksi.
> Yritys on rangaistava.

Rikoslain 30 luvun 4 §:n yritysvakoilusäännökseen liittyvät läheisesti myös yrityssalaisuuden rikkomista ja yrityssalaisuuden väärinkäyttöä koskevat 5 ja 6 §:n säännökset,[35] joista ensimmäinen tarkoittaa hyödynhankkimis-, hyödyt-

---

[34] Artikla 1 kohta a: ”Tietojärjestelmä” tarkoittaa laitetta tai toisiinsa kytkettyjä tai liitettyjä laitteita, joista yksi tai useampi on ohjelmoitu automaattista tietojenkäsittelyä varten.

[35] RL 30:5: (24.8.1990/769) Joka hankkiakseen itselleen tai toiselle taloudellista hyötyä tai toista vahingoittaakseen oikeudettomasti ilmaisee toiselle kuuluvan yrityssalaisuuden tai oikeudettomasti käyttää tällaista yrityssalaisuutta, jonka hän on saanut tietoonsa (1) ollessaan toisen palveluksessa, (2) toimiessaan yhteisön tai säätiön hallintoneuvoston tai hallituksen jäsenenä, toimitusjohtajana, tilintarkastajana tai selvitysmiehenä taikka niihin rinnastettavassa tehtävässä; (3) suorittaessaan tehtävää toisen puolesta tai muuten luottamuksellisessa liikesuhteessa tai (4) yrityksen saneerausmenettelyn yhteydessä, on tuomittava, jollei teosta ole muualla laissa säädetty ankarampaa rangaistusta, yrityssalaisuuden rikkomisesta sakkoon tai vankeuteen enintään kahdeksi vuodeksi. (1 mom., 25.1.1993/54) Tämä pykälä ei koske tekoa, johon 1 momentin 1 kohdassa tarkoitettu henkilö on ryhtynyt palvelusaikansa päätyttyä (2 mom.).

RL 30:6: (24.8.1990/769) Joka oikeudettomasti (1) käyttää tässä laissa rangaistavaksi säädetyllä teolla tietoon saatua tai ilmaistua toiselle kuuluvaa yrityssalaisuutta elinkeinotoiminnassa taikka (2) hankkiakseen itselleen tai toiselle taloudellista hyötyä ilmaisee tällaisen salaisuuden, on tuomittava yrityssalaisuuden väärinkäytöstä sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

tämis- tai vahingoittamistarkoituksessa tapahtuvaa toiselle kuuluvan määrätyn luottamuksellisen aseman perusteella tietoon saadun yrityssalaisuuden oikeudetonta ilmaisemista tai käyttämistä ja jälkimmäinen ylipäänsä rangaistavalla teolla tietoon saadun tai ilmaistun toiselle kuuluvan yrityssalaisuuden oikeudetonta käyttämistä tai ilmaisemista.

Kahdennentoista pykälän mukaan niin yritysvakoilu kuin yrityssalaisuuden rikkominen ja väärinkäyttökin ovat asianomistajarikoksia, ellei erittäin tärkeä yleinen etu vaadi syytteen nostamista.

Yritysvakoilussa on siis kysymys oikeudettomasta tiedon hankkimisesta toiselle kuuluvasta yrityssalaisuudesta. Oikeudettomalla menettelyllä voidaan ymmärtää joko ilman lupaa tai lupaan perustuva oikeus ylittäen tapahtuvaa toimintaa;[36] lainkohdan perusteluissa[37] ei oikeudettomuuden käsitettä tarkemmin ole käsitelty. Perustelujen mukaan ”tekijänä voisi tulla kysymykseen paitsi yrityksen ulkopuolinen myös sen palveluksessa oleva henkilö, jos hänen toimenkuvaansa ei kuulu tiedon saaminen työnantajan yrityssalaisuuksista”. Lähtökohtaisesti voitaneen katsoa, että yrityksen ulkopuolinen henkilö tarvitsee aina luvan voidakseen saada tietoa yrityssalaisuuksista.

Yrityssalaisuus

Yrityssalaisuuden käsitettä on määritelty rikoslain 30 luvun 11 §:ssä. Tämän jokseenkin avoimen määritelmän mukaan yrityssalaisuudella tarkoitetaan liike- tai ammattisalaisuutta taikka muuta vastaavaa elinkeinotoimintaa koskevaa tietoa, jonka elinkeinonharjoittaja pitää salassa ja jonka ilmaiseminen olisi omiaan aiheuttamaan vahinkoa joko hänelle tai toiselle elinkeinonharjoittajalle, joka on uskonut tiedon hänelle.[38]

Määritelmäsäännöksen perustelujen mukaan[39] yrityssalaisuuden tunnusmerkkejä ovat ”tiedon haltijan salassapitotahto ja salassapitointressi sekä tiedon tosiasiallinen salassapito”. Myös tiedon kanssa tekemisiin joutuvan henkilön on miellettävä tieto salaisuudeksi. Tiedon on oltava myös objektiivisesti arvioiden ainakin jossain määrin merkityksellinen elinkeinotoiminnan kannalta, vaikkakin lainkohta jättää salaisuuselementin arvioinnin paljolti riippumaan tiedon haltijan subjektiivisesta käsityksestä.

Käytännössä tiedon yrityssalaisuus-ominaisuutta on jouduttu muutaman kerran pohtimaan tapauksissa, joissa on hankittu tietoa yrityksen asiakastiedoista.

---

[36] Ks. Nyblin, s. 91, jossa Nyblinin mukaan oikeudettomuusedellytyksen täyttymisen arvioinnissa tulee antaa merkitystä myös hyvän liiketavan toteutumista edistäville tulkinnoille sekä työoikeudelliselle lojaliteettivelvoitteelle. Nyblinin mielestä lähtökohtaolettamus on, että lojaliteettivelvoitteen vastainen menettely voi myös rikosoikeudellisesti merkityksellisellä tavalla olla oikeudetonta.

[37] HE 66/1988 s. 83 ss.

[38] Ks. tästä myös Rautio, Rikosoikeus, s. 1044 s.

[39] HE 66/1988 s. 92 s.

Tällaisten tilanteiden osalta on mahdotonta esittää mitään yleistä sääntöä; kysymyksessä olevan elinkeinotoiminnan laadusta ja laajuudesta jää pitkälti riippumaan se, miten merkityksellistä asiakastietojen salassapito on elinkeinotoiminnan kannalta. Tässä suhteessa asiaan vaikuttaa käsitykseni mukaan oleellisesti ainakin se, kuinka yleisesti harjoitetusta elinkeinotoiminnasta on kysymys: päivittäistavarakauppaa harjoittavan kauppaliikkeen kanta-asiakasrekisteri tuskin muodostaa sellaista yrityssalaisuutta, jonka joutumista vilpillisinkään keinoin kilpailevan liikkeenharjoittajan haltuun voitaisiin pitää yritysvakoiluna, mutta mitä spesifisemmille elinkeinotoiminnan alueille siirrytään ja mitä rajoitetumpi on potentiaalinen asiakaskunta, sitä helpompaa on katsoa asiakkaita koskevat tiedot paitsi elinkeinonharjoittajan subjektiivisesta näkökulmasta myös objektiivisesti arvioiden merkityksellisiksi elinkeinotoiminnan harjoittajan kannalta.

Oikeudettomuus

Tekijän täytyy toimia tarkoituksin oikeudettomasti ilmaista haltuunsa saamansa yrityssalaisuus tai oikeudettomasti käyttää sitä. Yritysvakoilusäännöksen perustelujen mukaan tällainen ilmaiseminen voi tarkoittaa joko salaisuuden julkistamista tai sen luovuttamista toiselle, useimmiten sen myymistä välittäjälle tai kilpailevalle yritykselle.[40]

Laissa ei ole säännöksiä siitä, milloin yrityssalaisuudeksi katsottavan tiedon saa ilmaista; esimerkkinä oikeudettomasta menettelystä mainitaan perusteluissa taloudellisen hyödyn hankkiminen yrityssalaisuuden haltijan kustannuksella. Loogiselta joka tapauksessa tuntuu, että se, joka on oikeudettomasti hankkinut tiedon, ei myöskään ole oikeutettu sitä ilmaisemaan, sillä tiedon leviäminen edelleen on epäilemättä suurempi loukkaus tiedon oikean haltijan intressejä kohtaan kuin tiedon päätyminen vain yhden henkilön haltuun, ellei tämä itse ryhdy aktiivisesti käyttämään hyväkseen hankkimaansa tietoa.[41]

Huomattava on, että pelkkä ilmaisemis*tarkoitus* riittää tunnusmerkistön täyttymiseen; vaikka suunniteltu tietojen luovuttaminen tekijästä riippumattomastakin syystä jäisi toteutumatta, on hän kuitenkin menetellyt yritysvakoilusäännöksessä tarkoitetulla tavalla. Tilanne on sama, jos tekijällä itsellään olisi ollut tarkoitus käyttää hankkimiaan tietoja, mutta tämä ei syystä tai toisesta ole onnistunut. Tietojen toteutunut luovuttaminen tai käyttäminen on tiedot hankkineen tekijän kohdalla rankaisematon jälkiteko.[42]

---

[40] Ks. Rautio, Rikosoikeus, s. 1046.

[41] Rangaistavuuden alan ulkopuolelle on tarkoitettu kuitenkin jäämään sellaiset teot, joissa tekijä sinänsä oikeudettomasti hankkii tiedon toisen yrityssalaisuudesta mutta jossa tekijällä kuitenkin on oikeusjärjestyksen hyväksymä syy tiedon ilmaisemiselle, esimerkiksi yhteiskunnallisesti merkittävän epäkohdan paljastaminen. HE 66/1988, s. 84. Ks. myös Nyblin, s. 91.

[42] Nyblin, s. 79.

Tietojärjestelmään tunkeutuminen

Yritysvakoilusäännöksen 1 momentin 1 kohdan mukaan yhtenä tekotapana tulee kysymykseen tunkeutuminen ulkopuolisilta suojattuun tietojärjestelmään. Lainkohdan perustelujen mukaan[43] tunkeutumisella tässä tarkoitetussa mielessä on ymmärrettävä pääsyn hankkimista tietojärjestelmään hakkerin keinoin esimerkiksi tietokonetta, modeemia ja puhelinta käyttämällä.[44]

Tietojärjestelmällä tarkoitetaan erilaisia tietojenkäsittelylaitteita ja niiden välisiä tiedonsiirtoyhteyksiä. Tietojärjestelmän tulee olla ulkopuolisilta suojattu, jolloin tunkeutuminen edellyttää jonkin turvajärjestelyn murtamista tai käyttäjäkontrollin läpäisemistä samalla tavoin kuin henkilörekisterilain 45 §:ssä on säädetty; viimeksi mainittu lainkohta on tosin tietomurtosäännöksen tultua voimaan muutettu, joten viittaus tulee nykyään asiallisesti ymmärtää viittaukseksi rikoslain 38 luvun 8 §:ään. Tietojärjestelmään tunkeutumista olen jo edellä käsitellyt.

Tallenteen jäljentäminen

Momentin 2 kohdassa mainitaan tiedonhankkimiskeinona asiakirjan tai muun tallenteen jäljentäminen tai siihen rinnastettava tapa.[45] Tältä osin säännös sai muotonsa lakivaliokunnassa, jonka mietinnön[46] mukaan asiakirjan jäljentämiseen on rinnastettava tiedon sisältävän tallenteen luvaton haltuun saaminen; näin menetellen yrityssalaisuuden kaikki hankkimistavat voidaan arvostella saman säännöksen nojalla.[47]

Lakivaliokunta ei ole mitenkään määritellyt tallenteen käsitettä, mutta ilmeistä on, valiokunnan mietinnön syntyajankohta huomioon ottaen, että kovin pitkälle meneviä sähköisen tiedonsiirron ja -tallentamisen muotoja ei ole ajateltu; ensi sijassa noihin aikoihin – runsaat kymmenen vuotta sitten – sähköisesti tallennettu tieto siirrettiin paikasta toiseen siirtämällä tallenteen sisältävä levyke.[48]

Ei kuitenkaan liene estettä antaa käsitteelle tässäkin sama sisältö kuin osan I luvussa 1.2.2.5 olen määritellyt: tallenne on tietovälineelle kiinnitetyn datan ja datan edustaman informaation muodostama kokonaisuus. Näin määritellyn tallenteen hankkiminen on yksiselitteisesti käsitettävissä: esimerkiksi tietokonelevykkeen anastaminen on lainkohdassa tarkoitettua haltuunsa hankkimista. Tallenteen jäljentämisestä puhuminen ei ole aivan yhtä selkeää; asiallisestihan kysymyksessä on datan jäljentäminen.

---

[43] HE 66/1988, s. 83 s.
[44] Ks. myös Rautio, Rikosoikeus, s. 1045.
[45] Rautio, Rikosoikeus, s. 1045.
[46] LaVM 6/1990 s. 11.
[47] HE:een liittyvässä ehdotuksessa kysymyksessä oleva 4 §:n 1 momentin 2 kohta oli seuraavanlainen: ”2) jäljentämällä asiakirjan tai muulla siihen rinnastettavalla tavalla”.
[48] Ks. myös Nyblin, s. 87.

Tallenteen ollessa esimerkiksi asiakirja saadaan vaikkapa valokopiotekniikkaa käyttämällä aikaan tallenteen näköisjäljennös, mutta tietoteknisen tallenteen kohdalla ei tällaisesta välttämättä ole kysymys: tietokoneen kiintolevyltä levykkeelle tai nauhalle suoritettu datan kopiointi ei tuota jäljennöstä tallenteesta vaan ainoastaan *osasta* sitä – datasta ja datan kantamasta informaatiosta. Tallenne voidaan kylläkin jäljentää lähes kokonaisuudessaan – esimerkiksi poliisin käytössä olevilla laitteilla ja ohjelmilla voidaan tietokoneen kiintolevyn sisällöstä saada identtinen kopio.

Käytännössä ei puheena oleva semanttinen epätäsmällisyys tuottane ylitsekäymättömiä vaikeuksia, sillä selvää on, ettei lainkohdassa voida tarkoittaa identtisen kopion tuottamista koko tallenteesta; käsin ruutupaperille tehty jäljentämisen kohteena olevan sisällön uudelleen merkitseminen voi varmasti merkitä säännöksessä tarkoitettua jäljentämistä. Näin ollen tässä on kysymys nimenomaan informaation, *sisällön,* jäljentämisestä.

Tilanne on sama ajateltaessa kehittyneempiä sähköisen tiedonsiirron muotoja. Informaatio voidaan tietoverkkoja pitkin siirtää työasemasta toiseen, jolloin jälkimmäiseen koneeseen muodostuu alkuperäistä vastaavan informaation sisältävä tallenne.

Yritysvakoilun suhde muihin rikoksiin

Ensimmäisessä kohdassa tarkoitettu tunkeutuminen tietojärjestelmään merkitsee tosiasiallisesti myös sekä tietomurron että luvattoman käytön tunnusmerkistöjen toteutumista; tietomurtoa koskeva säännös on kuitenkin toissijainen ja syrjäytyy yritysvakoilun tunnusmerkistön täytyttyä. Tilanne on sama yritysvakoilun jäädessä – tietojärjestelmään tunkeutumisen tosin jo tapahduttua – kuitenkin yritysasteelle.

Tiedon hankkiminen yrityssalaisuudesta tarkoittaa itse asiassa yrityssalaisuuden sisältämään informaatioon kohdistuvaa anastustyyppistä rikosta, jonka seurauksena alkuperäinen informaatio joko jää oikealle haltijalleen tai siirtyy yksinomaan rikoksentekijän haltuun. Tekoa ei kuitenkaan voida arvioida rikoslain 28 luvun säännösten perusteella, sillä varkautta koskevan säännöksen perustelujen mukaan[49] varkausrikoksen kohteena olevaan irtaimeen omaisuuteen ei lueta niin sanottua aineetonta eli henkistä omaisuutta, esimerkiksi yrityssalaisuuksia.[50]

---

[49] HE 66/1988, s. 34.

[50] Asia ei ollut lainsäädäntövaiheessa niin yksinkertainen kuin miltä se nyt näyttää. Vielä hallituksen esityksessä (HE 66/1988, s. 84 s.) lähdettiin siitä, että tekijän luvattomasti hankkiessa haltuunsa yrityssalaisuuksia sisältävän tallenteen tekoon sovellettaisiin RL 28 luvun säännöksiä. Tällöin tekijä olisi voitu tuomita myös törkeästä anastusrikoksesta, jos tallenteen anastamisella haltuun saadun yrityssalaisuuden arvo olisi ollut suuri. Lakivaliokunta kuitenkin totesi (LaVM 6/1990, s. 11) mietinnössään, että yrityssalaisuuden kaikki hankkimistavat tulisi voida arvioida saman yritysvakoilusäännöksen nojalla.

Informaatio ei siis sinänsä voi olla anastusrikoksen objektina, mutta toisaalta tilanteissa, joissa informaation ohella anastetaan sinänsä arvokas tietoväline,[51] jolle informaatiota edustava data on kiinnitetty, tulee teko käsitykseni mukaan arvioitavaksi paitsi 30 luvun myös 28 luvun säännösten pohjalta.[52]

Ajatellaanpa asiaa kahden kärjistetyn esimerkin valossa. A tietää, että X Oy:llä on hallussaan yrityssalaisuus, jonka A haluaa saada haltuunsa.

1. A murtautuu yöllä X Oy:n toimitiloihin ja anastaa kymmenen kannettavaa tietokonetta, joista johonkin hän tietää yritysalaisuuden olevan tallennettuna. Anastetun omaisuuden arvo on yhteensä 40 000 euroa.
2. A vierailee päivällä X Oy:n toimitiloissa ja näkee yhdellä työpöydällä tietokonelevykkeen, jolle on kirjoitettu ”yrityssalaisuus”. A panee 50 sentin arvoisen levykkeen taskuunsa ja poistuu toimitiloista yrityssalaisuus hallussaan.

Ensimmäisessä tilanteessa A on oikeudettomasti hankkinut tiedon toiselle kuuluvasta yrityssalaisuudesta tunkeutumalla ulkopuolisilta suljettuun paikkaan. Toisessa tilanteessa A on saavuttanut saman päämäärän hankkimalla haltuunsa yrityssalaisuuden sisältäneen tallenteen. Ensimmäisessä tilanteessa A on yritysvakoilun ohessa syyllistynyt törkeän varkauden tunnusmerkistön toteuttavaan tekoon, jälkimmäisessä tapauksessa A:n menettely toteuttaa näpistyksen tunnusmerkistön.

Jos X Oy ei halua vaatia A:lle lainkaan rangaistusta, jää jälkimmäinen teko kokonaan rankaisematta mutta ensimmäisen teon osalta A tuomitaan törkeästä varkaudesta. Jos taas X Oy vaatii A:lle rangaistusta yritysvakoilusta, voidaan A tuomita jälkimmäisen teon osalta tästä rikoksesta mutta ensimmäinen teko on käsitykseni mukaan luettava A:n syyksi sekä yritysvakoiluna että anastusrikoksena.[53]

Sammon tietovuoto

Kysymystä informaatiosta anastusrikoksen objektina on sivuttu aikanaan suurtakin julkisuutta saavuttaneessa, tosin vanhan lain mukaan ratkaistussa niin kutsutussa Sammon tietovuoto -jutussa, jossa oli kysymys paitsi tiedon (oikeammin informaation) asemasta anastusrikoksen kohteena myös tietovälineelle kiinnitetyn tiedon (informaation) merkityksestä tietovälineeseen kohdistunutta anastusrikosta kvalifioivana tekijänä.[54]

---

[51] Ks. Silvander, s. 150, josaa hän jakaa tietovälineet (textbärare) kolmeen kategoriaan: 1) textbärare som har ett inbyggt värde, 2) textbärare som har ett bakomliggande värde och 3) textbärare som endast fungerar som bärare av en lagrad upptagning.

[52] Ks. myös LaVM 6/1990 s. 11.

[53] Ks. Silvander, s. 277 s., jossa hän Ruotsin oikeuden kannalta kysymystä tutkittuaan päätyy siihen, että kysymyksessä voi olla sekä yritysvakoilu- että varkausrikos.

[54] Ks. Hannula.

> Raastuvanoikeuden ja hovioikeuden mukaan syytettynä ollut vakuutusyhtiön atk-operaattori, joka oli luvattomasti siirtänyt tietoja yhtiön asiakasrekisteristä yhtiön omistamille magneettinauhoille ja luovuttanut nauhat tietoineen edelleen, oli syyllistynyt vain varkauksia ja toisen irtaimen omaisuuden luvatonta käyttämistä käsittävään jatkettuun rikokseen, josta raastuvanoikeus harkitsi oikeaksi seuraamukseksi viisikymmentä päiväsakkoa. Varkaudet olivat kohdistuneet nimenomaan nauhoihin eivätkä 73 000 vakuutusyhtiön asiakkaan nimi- ja osoitetietoihin. Hovioikeus lausui perusteluissaan muun muassa, että ”anastusrikoksen kohteena voi olla vain sellainen tietoväline tietoineen, jonka tiedot on tietovälineen omistajan tieten tai suostumuksin ennen anastuksen tapahtumista kiinnitetty tietovälineelle”.[55]

Ryhtymättä tässä pohtimaan kysymystä, onko vakuutusyhtiön asiakasrekisteriä pidettävä 30 luvun 4 §:ssä tarkoitettuna yrityssalaisuutena, voidaan kuitenkin todeta, että kuvatun kaltaisen menettelyn kohdistuessa informaatioon, joka *koskee* yrityssalaisuutta, se olisi luettava tekijänsä syyksi yhtiön tietokoneen luvattomana käyttönä, yhtiön nauhojen anastamisena sekä yrityssalaisuuteen kohdistuvana yritysvakoiluna 30 luvun 4 §:n 1 momentin 2 kohdan perusteella.

Mikäli informaatio taas ei koskisi yrityssalaisuutta eikä nauttisi suojaa minkään muunkaan säännöksen perusteella, teko toteuttaisi luvattoman käytön ja anastusrikoksen tunnusmerkistöt, mahdollisesti jopa kvalifioitujenkin tekomuotojen osalta, joskin nimenomaan tällaisessa tapauksessa varkauden ja kavalluksen nykyään voimassa olevat ankaroittamisperusteet lienevät jokseenkin vaikeasti sovellettavissa. Rikoslain 28 luvun 2 §:n perusteista voisi sovellettavaksi ajatella ainoastaan kohtaa 2 eli rikoksen uhrille tämän olot huomioon ottaen erityisen tuntuvan vahingon syntymistä ja sama olisi tilanne myös 5 §:n perusteiden osalta.

Eräs käytännön tapaus

Mielenkiintoinen tapaus, jossa jouduttiin pohtimaan paitsi yrityssalaisuus-ominaisuuden myös eräiden muiden tunnusmerkistötekijöiden täyttymistä, käsiteltiin muutama vuosi sitten Helsingin käräjäoikeudessa ja myöhemmin Helsingin hovioikeudessa:

> Helsingin kaupunginviskaali oli vaatinut A:lle rangaistusta ensisijaisesti yritysvakoilusta ja toissijaisesti luvattomasta käytöstä, koska A oli 8.–11.3.1996 Helsingissä irtisanouduttuaan B Oy:n toimitusjohtajan asemasta oikeudettomasti hankkinut tiedon B Oy:lle kuuluneesta yrityssalaisuudesta tunkeutumalla yhtiön ulkopuolisilta suojattuun tietojärjestelmään yhtiön tietojärjestelmän ulkopuolelta tietokoneen ja modeemin

---

[55] Turun HO p. n:o 1674/1990. KKO ei myöntänyt asiassa syyttäjän ja asianomistajan pyytämää valituslupaa.

avulla käyttäen hyväkseen käyttäjätunnusta, joka hänelle oli annettu yhtiön toimitusjohtajana, ja kopioinut yhtiön tiedostoista yhtiön myynti- ja asiakastiedot eli ns. Sales Power -tietokannan, tarkoituksin oikeudettomasti luovuttaa tietokanta käytettäväksi toisen yhtiön toiminnassa.

A kiisti syytteet. Yritysvakoilun osalta hän ensinnäkin katsoi, etteivät hänen kopioimansa tiedot olleet yrityssalaisuuksia. Lisäksi hän katsoi olleensa toimitusjohtajana oikeutettu tiedot kopioimaan, sillä vaikka hän oli allekirjoittanut ja päivännyt irtisanoutumisilmoituksensa ennen kopioimista, oli ilmoitus tullut B Oy:n tietoon vasta kopioimisen tapahduttua. Lisäksi C Oy, jolle toimitettaviksi tiedot oli kopioitu, olisi muutenkin ollut sopimuksen perusteella oikeutettu saamaan haltuunsa A:n kopioimat tiedot.

Usean käsittelykerran jälkeen Helsingin käräjäoikeus antoi asiassa tuomion 7.5.1997 (dnro R 96/4548) ja tuomitsi A:n yritysvakoilusta yhden vuoden ja viiden kuukauden ehdolliseen vankeusrangaistukseen sekä velvoitti A:n mm. suorittamaan B Oy:n konkurssipesälle vahingonkorvausta 6,4 miljoonaa markkaa. Laajoissa perusteluissaan käräjäoikeus mm. totesi, että huomioon ottaen A:n irtisanoutumisilmoitus sisältöineen ja A:n asema yhtiössä oli A irtisanoutunut yhtiöstä ilmoituksen allekirjoittamispäivästä lukien eikä hänellä enää ollut käyttöoikeutta kysymyksessä olleeseen tietokantaan. Edelleen käräjäoikeus lausui, että jos kysymyksessä olleet tiedot olisivat A:n kertomin tavoin olleet saatavissa erilaisista julkisista lähteistä, ei A:lla olisi ollut mitään tarvetta kopioida niitä irtisanoutumisensa jälkeen varsinkaan, jos niillä ei olisi ollut mitään merkitystä A:lle itselleen ja samalla alalla toimiville hänen intressipiiriinsä kuuluville yhtiöille. Asiassa oli käräjäoikeuden mukaan selvitetty, että tiedostot olivat sisältäneet kapealla kansainvälisellä alueella toimineen yrityksen elinkeinotoimintaa koskevaa tietoa, joka on kokonaisuutena ollut salassa pidettävää, tosiasiassa ulkopuoliselta suojattavaa tietoa, jonka ilmaiseminen olisi ollut omiaan aiheuttamaan taloudellista vahinkoa B Oy:lle. Tiedoston arvo oli ollut erityisen arvokasta niille henkilöille, jotka olivat aikaisemmin palvelleet kyseisellä toimialalla ja jotka olivat käynnistämässä vastaavaa ainutlaatuista liiketoimintaa. – Käräjäoikeus nimenomaisesti hylkäsi syyttäjän toissijaisen luvatonta käyttöä koskeneen syytevaatimuksen.

A valitti Helsingin hovioikeuteen ja vaati syytteen ja korvausvaatimusten hylkäämistä. Syyttäjä valitti myös vaatien rangaistuksen korottamista. Lisäksi A:n avustajana toiminut asianajaja vaati valtion varoista maksetun palkkion korottamista.

Helsingin hovioikeus antoi tuomionsa 18.8.1998 (nro 2424) ja hylkäsi syytteen. Perustelut eivät olleet pitkät (kursivoinnit tässä):

”A:lla oli työsuhteensa kestäessä toimitusjohtajan asemassaan pääsy syytteessä tarkoitettuihin tiedostoihin. Jutussa *ei ole väitetty*, että tiedostoissa olevat *tiedot olisivat muuttuneet* millään mainittavalla tavalla hänen *irtisanoutumispäivänsä aikana tai sitä ennen*.

A oli toimittanut ajan tasalla olevan version tiedostoista D:lle, jolla on *tietoja toimitettaessa ollut oikeus saada käyttöönsä nuo tiedot*.

Näin ollen A *ei ole* rikoslain 30 luvun 4 §:n tarkoittamin tavoin *oikeudettomasti hankkinut tietoa* toiselle kuuluvasta yrityssalaisuudesta

tarkoituksin oikeudettomasti ilmaista se. Sen vuoksi syyte ja sen nojalla esitetyt vaatimukset on hylättävä."

B Oy:n konkurssipesä haki korkeimmalta oikeudelta valituslupaa, jota ei myönnetty.

Tapaukseen liittyy useita yritysvakoilun tunnusmerkistöön liittyviä kysymyksiä. A:lla oli toimessaan ollut oikeus päästä yhtiön tietojärjestelmään ja kaikkiin siinä oleviin tiedostoihin, mutta hänen irtisanoutumisestaan oli seurannut tuon oikeuden menettäminen. A oli siis oikeudettomasti hankkinut haltuunsa saamansa tiedot. Hän oli tunkeutunut tietojärjestelmään hallussaan olleita käyttäjätunnusta ja salasanaa käyttäen, joiden käyttämistä ei yhtiön toimenpitein vielä ollut estetty.

A:n oli kuitenkin täytynyt ymmärtää, että hänellä ei ollut enää ollut oikeutta päästä tietojärjestelmään, joten hänen menettelynsä on ollut lainkohdassa tarkoitettua tunkeutumista ulkopuolisilta suojattuun tietojärjestelmään; tämä menettely puolestaan täyttää myös tietomurron tunnusmerkistön. Samoin täyttyy luvattoman käytön tunnusmerkistö.

A:lla oli ollut rangaistavuuden edellytyksenä oleva tarkoitus ilmaista oikeudettomasti haltuunsa saamansa tiedot, joiden tässä tapauksessa voidaan katsoa olleen yrityssalaisuuksia. A:n menettely siis täyttää paitsi tietomurron ja luvattoman käytön myös yritysvakoilun tunnusmerkistön. Tämän kaiken pitäisi vaikuttaa aivan selvältä.

Hovioikeuden tuomio on kuitenkin mielestäni omituinen ja on hyvin vaikeaa – suorastaan mahdotonta – ymmärtää, miten hovioikeus on lausumillaan perusteilla voinut päätyä esittämäänsä lopputulokseen.

Tuomiossa ei oteta kantaa siihen keskeiseen kysymykseen, olivatko ko. tiedot yrityssalaisuuksia; ilmeisesti tätä ei hovioikeudessa ole pidetty riitaisena. Tuomiossa ei myöskään oteta kantaa A:n oikeuteen tunkeutua yrityksen tietojärjestelmään irtisanoutumisensa jälkeen eikä liioin A:n oikeuteen ilmaista yrityssalaisuus. Ainoat seikat, joilla lopputulosta perustellaan, ovat se, että A:lla työsuhteensa kestäessä oli pääsy tiedostoihin, että ei ollut väitetty tietojen millään mainittavalla tavalla muuttuneen irtisanoutumispäivän aikana tai sitä ennen (!) ja että D:llä oli tietoja toimitettaessa ollut oikeus saada tiedot käyttöönsä. *Tämän vuoksi* hovioikeus siis katsoi selvitetyksi, ettei A ollut oikeudettomasti hankkinut tietoa toiselle kuuluvasta yrityssalaisuudesta tarkoituksin oikeudettomasti ilmaista se.

Hovioikeuden ajatuksenkulkua on vaikea seurata. Vailla merkitystä pitäisi olla sen, onko A:lla työsuhteensa kestäessä ollut pääsy tiedostoihin. Oikeus pääsyyn on joka tapauksessa lakannut työsuhteen päättyessä, jolloin A:sta on tullut yrityksen ulkopuolinen henkilö. – Omituista on myös vetoaminen siihen, ettei ollut väitetty tietojen muuttuneen A:n irtisanoutumispäivän aikana tai sitä ennen. Selvähän on, että tiedot *ovat* ennen A:n irtisanoutumispäivää muuttuneet ties kuinka monta kertaa myynti- ja asiakastietoja päivitettäessä. Jos hovi-

oikeuden tuomio on kirjoitusvirheen johdosta saanut toisen sisällön ja tosiasiassa onkin tarkoitettu tietojen muuttumista irtisanomispäivän *jälkeen,* ei tälläkään voi olla mitään merkitystä: yrityssalaisuus pysyy yrityssalaisuutena, vaikka joku yrityksestä irtisanoutuisikin.

Merkitystä ei ole silläkään, onko D:llä sinänsä ollut oikeus saada tiedot käyttöönsä. Oleellista on se, että A:lla ei irtisanoutumisensa jälkeen ole ollut oikeutta luovuttaa oikeudettomasti hankkimiaan B Oy:lle kuuluvia yrityssalaisuuksia. Ainoa, joka on ollut oikeutettu määräämään yrityssalaisuuksien luovuttamisesta, on B Oy yrityssalaisuuksien haltijana.

Ei voi välttyä siltä ajatukselta, että hovioikeus on jollain lailla sekoittanut rikoslain 30 luvun 4 ja 5 §:t keskenään. Yrityssalaisuuden rikkomisesta ei nimittäin tuolloin voimassa olleen lain mukaan voitu tuomita rangaistukseen sellaista, joka oli saanut yrityssalaisuuden tietoonsa ollessaan toisen palveluksessa mutta ilmaissut yrityssalaisuuden vasta palvelusaikansa päätyttyä. *Jos* hovioikeus olisikin katsonut, että A:n irtisanoutuminen ei vielä ollut tullut tehokkaaksi ja hän olisikin saanut tiedot haltuunsa työsuhteensa kestäessä, olisi syytteen hylkäävä lopputulos ollut – rikoslain 30 luvun 5 §:n 2 momentin perusteella – lainmukainen.[56] Hovioikeuden tuomion perusteluissa ei kuitenkaan millään tavoin viitata rikoslain 30 luvun 5 §:ään.

Yritysvakoilu kansainvälisissä instrumenteissa

Yritysvakoilua, yrityssalaisuuden rikkomista ja yrityssalaisuuden väärinkäyttöä koskevat rikoslain 30 luvun säännökset vastaavat omalta osaltaan yhdessä Euroopan neuvoston valinnaislistan tietokonevakoilua koskevaa sanamuodoltaan väljähköä suositusta.[57] Suosituksen perusteluissa[58] viitataan automaattisen tietojenkäsittelyn suomiin mahdollisuuksiin hankkia tietoja yritys- ja ammattisalaisuuksista (trade and commercial secrets) ja hyödyntää niitä, minkä vuoksi esillä olevan kaltaista kriminalisointia pidetään perusteltuna; suositus on kuitenkin sijoitettu valinnaislistalle, koska yrityssalaisuuksien rikosoikeudelli-

---

[56] Lainmukaisuus ei tässä merkitse välttämättä oikeudenmukaisuutta. Lainsäädännöllinen tilanne oli koettu ongelmalliseksi ja 1.4.2003 voimaan tulleella lailla rikoslain muuttamisesta (61/2003) on rikoslain 30 luvun 5 §:n 2 momentti muutettu kuulumaan seuraavasti: ”Tämä pykälä ei koske tekoa, johon 1 momentin 1 kohdassa tarkoitettu henkilö on ryhtynyt kahden vuoden kuluttua palvelusaikansa päättymisestä.”

[57] Sopimattomin keinoin tapahtuva ammatti- tai yrityssalaisuuden hankinta taikka sellaisen salaisuuden luvaton ilmaiseminen, luovuttaminen tai käyttäminen, kun teon tarkoituksena on aiheuttaa taloudellista vahinkoa salaisuuden lailliselle haltijalle taikka hankkia laitonta taloudellista hyötyä itselle tai toiselle.

[58] EN:n raportti 89, s. 45 ss., jossa mm. ”The need for increased protection is undisputed today. – – The trend towards better civil and criminal law protection of trade secrets in the last twenty years has been a result of the increasing importance of economically valuable ’information’ in the development of science, technology and industry, being especially reflected in the increasing use of data storage and processing.”

nen suojelu ei kovin läheisesti kuulu perinteiseen tietotekniikkarikosten piiriin ja kun jäsenvaltioiden keskuudessa oli ollut erimielisyyttä niistä kriminaalipoliittisista toimenpiteistä, joihin yrityssalaisuuksien suojaamiseksi ylipäänsä olisi aihetta ryhtyä.

Yleinen mielipide yritysvakoilun kriminalisoimisen tarpeellisuudesta lienee kuitenkin jonkin verran muuttunut sitten Euroopan neuvoston raportin laatimisen, sillä *Durham* kirjoittaa AIDP:n kollokvion yleisraportissaan, että vaikka yrityssalaisuuksien suojaamista siviilioikeudellisin keinoin voidaankin perustella, ”there is growing consensus that the violation of trade secrets or ’computer espionage’ should be subjected to criminal sanctions”, ja viittaa tässä yhteydessä paitsi Suomen myös Ranskan, Saksan, Kreikan, Italian, Luxemburgin ja Turkin kansallisiin raportteihin.[59]

Yritysvakoilu tietotekniikkarikoksena

Edellä on käsitelty yritysvakoilua ja siihen liittyviä tekoja vain siltä osin kuin niiden tunnusmerkistönmukaiset menettelyt toteuttavat myös tietotekniikkarikoksen tunnusmerkistön. Yritysvakoilussa yleisesti ottaen tietotekniikkarikoselementti ei ole erityisen keskeinen, ja niin muodoin yritysvakoilu tietotekniikkarikoksena poikkeaa olennaisesti jäljempänä käsiteltävistä tietoteknisestä väärennyksestä, tietovahingon aiheuttamisesta ja tietojenkäsittelypetoksesta, joissa tietojenkäsittelyyn puuttuminen – tavalla tai toisella – on olennainen tunnusmerkistötekijä ja joissa tietojenkäsittelyrauhan asema suojeluobjektina on keskeisempi.

Tässä yhteydessä ei ole syytä tarkemmin paneutua liike- ja ammattisalaisuuksien suojaan sinänsä, mutta vuoden 1991 alusta voimaan tulleen uuden sääntelyn taustalla olleita ajatuksia kuvatkoon seuraava sitaatti rikoslain 30 luvun perusteluista:[60]

> Kiristynyt kilpailu, yritysten ja markkinoiden kansainvälistyminen sekä niin sanotun strategisen yritysajattelun korostuminen ovat lisänneet elinkeinotoiminnassa tarvittavan taitotiedon[61] kysyntää ja taloudellista arvoa. Kysymys ei ole pelkästään tuotteisiin ja tuotekehittelyyn liittyvästä osaamisesta vaan yritystoiminnan niin sanotuista aineettomista investoinneista kokonaisuudessaan. Erityisen näkyvää tämä kehitys on ollut aloilla, missä itse tieto ja tietämys ovat yritystoiminnan varsinaisena kohteena. Toisaalta tietotekniikan uudet keinot ovat mahdollistaneet uusia tiedonhankintatapoja. Tietovuodot ovat käyneet entistä todennäköisemmiksi mutta samalla entistä vaikeammiksi jäljittää. Tämä kehitys on aiheuttanut monissa maissa tarpeen tarkistaa liike- ja ammattisalaisuuksien lakisääteistä suojaa.

---

[59] Durham, s. 104.
[60] HE 66/1988, s. 76.
[61] On syytä kiinnittää huomiota know how’n oikean suomenkielisen vastineen eli taitotiedon käyttämiseen!

2.2 LUVATON KÄYTTÖ (RL 28:7)

Luvatonta käyttöä koskeva rikoslain 28 luvun 7 §:n rangaistussäännös sai nykyisen muotonsa lailla 769/1990:

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

Luvattoman käytön törkeä ja lievä tekomuoto on kriminalisoitu luvun 8 ja 9 §:ssä.[62] Luvaton käyttö on luvun 15 §:n 1 momentin mukaan kaikissa muodoissaan asianomistajarikos, ellei erittäin tärkeä yleinen etu vaadi syytteen nostamista. Säännöksillä korvattiin 38 luvussa olleet luvatonta käyttämistä koskenut 6 §:n 1 momentin sekä luvatonta ja omavaltaista käyttöönottamista koskenut 6 a §:n säännös.[63]

Luvatonta käyttöä koskeva säännös poikkeaa muista tietotekniikkarikoksia koskevista säännöksistä siinä, että se on luonteeltaan yleinen: tietotekniikkarikoselementtiä ei ole kirjoitettu näkyviin tunnusmerkistöön ja niinpä säännöstä voidaan tarkastella tietotekniikkarikossäännöksenä ainoastaan silloin, kun säännöstä sovelletaan tietotekniikkarikoksen määritelmässä esitetyt kriteerit täyttävään tekoon.

Säännöksen syntyhistoriasta

Tietotekniikkarikosten kannalta luvatonta käyttöä koskevassa säännöksessä on olennaista se, että siinä on luovuttu vaatimasta luvattomasti käytettävän omai-

---

[62] RL 28:8: Jos luvattomassa käytössä (1) tavoitellaan huomattavaa taloudellista hyötyä tai (2) aiheutetaan rikoksen uhrille tämän olot huomioon ottaen erityisen tuntuvaa vahinkoa tai haittaa ja luvaton käyttö on myös kokonaisuutena arvostellen törkeä, rikoksentekijä on tuomittava törkeästä luvattomasta käytöstä sakkoon tai vankeuteen enintään kahdeksi vuodeksi. (1 mom.) Yritys on rangaistava. (2 mom.)

RL 28:9: Jos luvaton käyttö, huomioon ottaen se, että rikos ei ole omiaan aiheuttamaan merkittävää vahinkoa tai haittaa, tai muut rikokseen liittyvät seikat, on kokonaisuutena arvostellen vähäinen, rikoksentekijä on tuomittava lievästä luvattomasta käytöstä sakkoon.

[63] RL 38:6.1 (397/1937): Joka luvattomasti itse tahi toisen kautta käyttää huostassaan olevaa irtainta omaisuutta, mikä ei ole hänen omaansa, rangaistakoon sakolla.

RL 38:6 a.1 (223/1964): Joka ilman laillista oikeutta toisen hallusta ottaa käyttöönsä toisen irtainta omaisuutta taikka käyttää sellaista omaisuutta tietäen sen mainitulla tavalla toisen hallusta otetuksi, tuomittakoon, jollei teosta ole muualla laissa säädetty ankarampaa rangaistusta, luvattomasta käyttöönottamisesta sakkoon tai enintään kahdeksi vuodeksi vankeuteen.

RL 38:6 a.2 ja 3 koskivat moottoriajoneuvon luvatonta käyttöönottamista ja sen yritystä.

RL 38:6 a.4: Jos 1 tai 2 momentissa tarkoitettua rikosta on sen johdosta, että käyttämisestä ei ole aiheutunut mitään vahinkoa eikä vaaraa, taikka rikoksen tapahtuessa vallinneiden olosuhteiden perusteella muutoin pidettävä vähäisenä, tuomittakoon syyllinen omavaltaisesta käyttöönottamisesta sakkoon.

suuden olemista käyttäjän hallussa, mikä aikaisemman lain mukaan oli rangaistavuuden edellytyksenä. Luvatonta käyttämistä koskeneessa säännöksessä edellytettiin rikoksentekijän käyttävän *huostassaan olevaa* irtainta omaisuutta ja luvaton käyttöönotto oli kysymyksessä kun rikoksentekijä *toisen hallusta otti käyttöönsä* mainitunlaista omaisuutta.[64]

> Käytännössä vanhan lain soveltumattomuus tietotekniikkarikoksiin tuli erityisen selvästi esille aikanaan suurta huomiota herättäneessä[65] ns. Espoon hakkerijutussa, joka jäi hovioikeuden päätöksen varaan.[66] Jutussa oli kysymys tietokoneen luvattomasta käyttöönottamisesta; syytetyt olivat käyttäneet tietokonetta puhelimen ja modeemin välityksellä pääsemällä tietojärjestelmiin eri käyttäjätunnuksin ja salasanoin. Päätöksen perustelujen mukaan tietokoneiden tällainen käyttö ei ollut estänyt niiden omistajaa tai muita niiden käyttöön oikeutettuja käyttämästä samanaikaisesti tietokoneita eivätkä syytetyt siten olleet ottaneet tietokoneita asianomistajan hallusta omaan käyttöönsä. Syytteet luvattomasta käyttöönottamisesta hylättiin mutta syytetyt velvoitettiin suorittamaan asianomistajille korvausta käytön aiheuttamista kustannuksista.

Päätöstä voidaan perustellusti arvostella ja kysyä, eikö voimassa ollutta lakia sallitulla tavalla tulkiten olisi voitu päätyä toisenkinlaiseen lopputulokseen. Kiistatonta on, että luvatta käytetyt tietokoneet eivät fyysisesti olleet käyttäjiensä hallussa, mutta yhtä kiistatonta on, että he niitä luvattomasti käyttivät. Kysymys on siis siitä, oliko käyttämistointa edeltänyt käyttöönottaminen tuolloin voimassa olleen rikoslain 38 luvun 6a §:n 1 momentin tarkoittamassa mielessä.

Päätöksen perusteluista ilmenee ajatus, että käyttöönottamisen seurauksena on omaisuuden omistajan tai muun käyttämiseen oikeutetun *täysin* menetettävä mahdollisuutensa käyttämiseen; tässä tapauksessa omistajan on ollut mahdol-

---

[64] Tilanne muuttui kuvatun kaltaiseksi muutettaessa rikoslain 38 luvun 6 §:ää lailla 223/1964. Aikaisempi pykälän toinen momentti (397/1937) kuului: ”Jos joku muuten luvattomasti käyttää toiselle kuuluvaa irtainta omaisuutta, rangaistakoon sakolla tai vankeudella enintään kuudeksi kuukaudeksi. Jos luvattomasta käyttämisestä on ollut erikoista vahinkoa tai vaaraa taikka jos asianhaarat muuten ovat erittäin raskauttavat, olkoon rangaistus vankeutta enintään kaksi vuotta.” – Lähtökohdat säännöksen laatimiselle ovat kuitenkin olleet täysin toiset kuin nykyään, sillä toisen momentin sanamuoto viittaa ensisijaisesti juuri luvattoman käyttöönottamisen tilanteeseen (HE 89/1937). Honkasalo tosin kirjoittaa 2 momentissa edellytetyn luvattoman käytön voivan toteutua myös esinettä toisen hallinnasta ottamatta ja mainitsee esimerkkinä tilanteen, jossa jotkut henkilöt ovat yön aikana luvattomasti painaneet julistuksia toisen hallinnassa olevalla painokoneella tai käyttäneet toisen hallinnassa olevaa elokuvakonetta. (Erityinen osa I.2 s. 86 s.) Vuoden 1937 säännös olisi itse asiassa ollut hyvin helposti sovellettavissa myös tietotekniikkarikokseksi katsottavaan luvattomaan käyttöön.

[65] Tiedotusvälineiden mielenkiinnon jutussa herätti ennen muuta se, että nuoret, luvattomasta käytöstä epäillyt rikoksentekijät pidettiin tutkinnan aikana pidätettyinä tuolloin voimassa olleen lain salliman enimmäisajan.

[66] HelHO 15.5.1990 n:o 1106. Sekä syyttäjä että syytetyt hakivat KKO:lta valituslupaa, jota ei kuitenkaan myönnetty (KKO 18.10.1990).

lista käyttää tietokonetta huolimatta järjestelmässä operoineesta hakkerista. Tosiasia kuitenkin on, että *siltä osin kuin järjestelmä on ollut hakkerin käytössä, se on ollut omistajan käyttömahdollisuuksien ulkopuolella* – oli hakkerin käytössä ollut osa koneen kapasiteetista sitten kuinka minimaalinen tahansa.

Syytettyjen tuomitseminen luvattomasta käyttöönottamisesta olisi nähdäkseni ollut täysin voimassa olleen lain kirjaimen mukainen ratkaisu – lain hengestä tai lainsäätäjän tahdosta ei tässä tapauksessa olisi ollut johtoa löydettävissä, koska tilannetta ei lakia säädettäessä ollut osattu ennalta ajatella. Tosiasiahan tilanteessa on ollut, että luvattoman käytön ensisijaisena kohteena ei suinkaan ollut tieto*kone* vaan tieto*järjestelmä,* vaikka juttua käsiteltäessä lähtökohtana on koko ajan tavallaan erheellisesti ollut tietokoneen luvaton käyttö.

Voimassa olevan lain esityöt ilmentävät tuomioistuinten omaksumaa kantaa. Luvattoman käytön käsite ei ole täysin selkeä silloin, kun puhutaan tietoteknisessä ympäristössä tehdyistä teoista. Lainsäätäjä lienee ajatellut ensisijaisesti juuri edellä kuvatun hakkerijutun tapaista menettelyä mainitessaan 28 luvun perusteluissa esimerkkinä 7 §:n soveltamistilanteista toisen omistaman tietokoneen luvattoman käyttämisen puhelinlinjan välityksellä huolimatta siitä, että tietokoneen fyysistä haltuunottoa ei ole tapahtunut.[67] Myös asianomaisen pykälän perusteluissa nimenomaan todetaan rangaistavuuden alan laajenevan esimerkiksi sellaisiin ”atk-hakkereihin”, jotka puhelinlinjan välityksellä tunkeutuvat toisen tietokonejärjestelmään ja käyttävät sitä luvattomasti eli ”varastavat tietokoneaikaa”[68] – tässä siis puhutaan aivan oikein tietojärjestelmän luvattomasta käyttämisestä.[69]

Edellä lausuttu osaltaan osoittaa selkeästi, miten tärkeää on täsmällisyys termien käytössä. Tieto*järjestelmä* tarkoittaa jotakin muuta kuin tieto*kone*. Tietokone voi olla osa tietojärjestelmää tai se voi yksinäänkin muodostaa tietojärjestelmän, mutta tietojärjestelmään saattaa kuulua ja useimmiten kuuluu myös muita koneita ja tiedonsiirtokanavia sekä dataa, jotka kaikki yhdessä tai erikseen voivat olla luvattoman käytön kohteena. Pienen tietojärjestelmän kohdalla konkreettinen haltuunotto voi olla mahdollista mutta mitä suuremmasta

---

[67] HE 66/1988, s. 31. Fyysisellä haltuunotolla tarkoitettaneen siis esineen haltuun ottamista niin, että sen omistaja (vast.) kokonaan estyy sitä käyttämästä.

[68] HE 66/1988, s. 43. Käytetty termi ”tietokoneajan varastaminen” kuvaa sitä suhtautumista, joka on vielä varsin yleinen yritettäessä sovittaa rikosoikeudellisia säännöksiä vastaamaan tietoteknistä todellisuutta. Kysymyksessä ei ole katsottava olevan mihinkään immateriaaliseen (aikaan) kohdistuva teko vaan teko, joka täysin konkreettisesti rajoittaa tai ainakin vaarantaa tietokoneen omistajan mahdollisuuksia käyttää konettaan siksi, että joku toinen käyttää sitä samanaikaisesti.

[69] Ks. myös Lappi-Seppälä, Rikosoikeus, s. 976.

järjestelmästä on kysymys, sitä vaikeammaksi koko järjestelmän haltuun- ja käyttöönotto muuttuu.[70]

Asianomistajan hallinnoima data voi fyysisesti sijaita aivan muualla kuin asianomistajan tietokoneen kiintolevyllä – se voi olla esimerkiksi jollain sellaisella vaikkapa toisella puolella maapalloa sijaitsevalla palvelimella, jonka käyttäminen sinänsä ei ole luvatonta; luvatonta vain on käyttää sitä dataa, jonka asianomistaja on esimerkiksi suojannut tavalla tai toisella. Hyvä esimerkki tällaisesta tilanteesta on jonkun henkilön Internet-kotisivu. Se ei suinkaan sijaitse asianomaisen henkilön koti-PC:ssä vaan jonkin Internet-palvelujen tarjoajan palvelimella.[71]

Hakkeri / krakkeri

Tässä yhteydessä on syytä hieman lähemmin tarkastella ”hakkerin” (hacker) käsitettä, jota niin rikoslain esitöissä kuin yleisessä kielenkäytössäkin jokseenkin kritiikittömästi käytetään kuvaamaan tietotekniikkarikoksiin ja niistä erityisesti tietomurtoon ja luvattomaan käyttöön syyllistyviä henkilöitä; sanalla toisin sanoen on yleisessä kielenkäytössä selkeästi kielteinen arvovaraus. Tietotekniikan harrastajat ja ammattilaiset kuitenkin ainakin joskus käyttävät sanaa erilaisessa merkityksessä. Niinpä esimerkiksi Atk-sanakirjan mukaan hakkeri on ”innokas tietokoneharrastaja”, joskin ”sana on myös saanut kielteisen lisämerkityksen tietokonejärjestelmiin murtautuja”.[72] Erityisesti oikeudettomiin tunkeutumisiin erikoistunutta hakkeria kutsutaan yleensä ”krakkeriksi” (cracker). Tietokonealan ihmiset tuntuvat halukkaasti tekevän selvän eron näiden kahden termin välille.

Yhdenmukaisesti lain esitöiden kanssa tulen jäljempänä käyttämään termiä ”hakkeri” silloin, kun puhe on järjestelmään tunkeutuneesta rikoksentekijästä, mutta tällä en suinkaan tarkoita leimata kaikkia hakkeriksi itseään kutsuvia tai muiden hakkereina pitämiä rikollisiksi – onhan henkilöautolla rattijuopumukseen syyllistyvä autoilijakin yhtä lailla autoilija kuin autoa selvin päin kuljettavat.[73]

---

[70] Silvander, s. 147, on sitä mieltä, että etäkäyttötilanteessa (gärning som sker på distans) ei ole kysymys tietokoneen luvattomasta käytöstä vaan teko-objektina on tällöin tietokoneohjelma. Tämä on tietysti tavallaan totta mutta tietojärjestelmän katsominen teko-objektiksi käsitykseni mukaan poistaa tämän tulkintaongelman. Silvanderin oman käsitteistön puitteissa ohjelman katsominen teko-objektiksi merkitsee sitä, että luvaton käyttö ei olekaan ”datorrelaterad” vaan ”datarelaterad”. Ks. myös 352, jossa Silvander toteaa olevan ”tveksamt om man kan säga att det är en dator i fysisk bemärkelse som brukas”.

[71] Tällaiset Internet-palvelimet tarjoavat erinomaisen tilaisuuden informaation kätkemiseen. Internet-yhteyden tilaaja yleensä saa palveluntarjoajalta käyttöönsä jopa useita megatavuja levytilaa, jonka olemassaolon selvittäminen ei esimerkiksi rikostutkinnassa aina ole helppoa.

[72] Atk-sanakirja, s. 41 s. Ks. myös Saari, s. 43 ss.

[73] Luvattomat tunkeutumiset ja käytöt ovat saaneet alkunsa Yhdysvalloissa 1950-luvulla alkaneesta ”Phone Phreak” -liikkeestä. Phreakit ohjailivat äänisignaalein puhelinverkkoa ja kykenivät näin välttämään puhelinmaksuja. Ks. Saari, s. 45 ss. ja Tuomi, s. 16 ss. Puhelinjärjestelmiin liittyvät eräät suurimpia vahinkoja aiheuttaneet luvattoman käytön tapaukset nykyäänkin. Maaliskuussa 1987 FBI ja Secret Service pidättivät New Yorkissa l8 henkilöä, jotka olivat soittaneet puheluja matkapuhelimilla, joita oli teknisesti muuteltu niin, että laskutus kohdistui muihin

Käyttäminen

Luvattomalla käytöllä on usein tarkoitettu teon kohteen käyttämistä sille tyypillisellä tavalla, jolloin tietojärjestelmän kysymyksessä ollessa järjestelmän luvatonta käyttöä olisi vasta siihen tunkeutumista seurannut käyttäminen. Tällä kannalla on ollut nimenomaan lainsäätäjä, sillä rikoslain kokonaisuudistuksen toista vaihetta tarkoittavassa hallituksen esityksessä todetaan ehdotetun tietomurtoa koskevan säännöksen perusteluissa, että luvattomana käyttönä ei vielä pidetä hakkerin tunkeutumisellaan aikaansaamaa tietokoneen käyttöjärjestelmän käynnistymistä.[74]

Tällainen näkemys on jokseenkin vaikea hyväksyä, sillä tietojärjestelmäähän käytetään jo siinä vaiheessa, kun järjestelmään pyrkijä yrittää läpäistä järjestelmää suojaavan kontrollin ja järjestelmä yrittää tunnistaa tulijan. Järjestelmä *käynnistyy* jo tuossa vaiheessa ja tunkeutuja saa aikaan yhden järjestelmään oleellisesti kuuluvan osan toimimisen juuri sille tyypillisellä tavalla.

Niin kuin edellä todettiin, perustelujenkin mukaan rangaistavuuden ala tahdottiin laajentaa ”tietokoneajan varastamiseen” – tosiasiassa ”tietokoneaikaa” alkaa kulua heti, kun prosessori alkaa toimia, eikä sillä, mitä järjestelmä kulloinkin tekee, ole välttämättä yhtään mitään merkitystä järjestelmän oikean haltijan kannalta: tunkeutujan käyttämä osa järjestelmän kapasiteetista – ”tietokoneaika” – on joka tapauksessa oikean haltijan käyttömahdollisuuksien ulkopuolella olkoonpa kysymyksessä sitten turvajärjestelmän kuormittaminen tunkeutumisyrityksillä tai onnistunutta tunkeutumista seurannut pasianssipeli.

Jos rikoksen täyttymisaste kuitenkin hyväksytään lainsäätäjän esittämän kaltaiseksi, pitäisi järjestelmään pyrkiminen joka tapauksessa katsoa luvattoman käytön yritykseksi, mikäli tekijän lopullinen aikomus on ollut järjestelmän käyttäminen. Tästä seuraa jo edellä käsiteltyjä ongelmia suhteessa 38 luvun 8 §:n tietomurtoon, jota tarkoittava tunnusmerkistö voi täyttyä jo luvattoman käytön yrityksellä, josta on säädetty samanlaiset rangaistusuhat kuin luvattomasta käytöstäkin ja jonka yritys myös on rangaistava.

---

tilaajiin. Samanaikaisesti otettiin kiinni seitsemän muuta henkilöä, jotka olivat tehneet muutokset puhelimiin ja myyneet niitä. – Muutokset olivat koskeneet matkapuhelinten tunnusnumeroita, jotka ohjasivat puheluiden laskutusta. Numerot oli tallennettu puhelinkojeisiin muistilastuihin ja voitiin vaihtaa asentamalla kojeisiin uusi lastu, johon oli ohjelmoitu toinen numero. Joka soitolla välittyi tunnusnumero automaattisesti tietokoneelle, joka hoiti laskutuksen saamansa numeron perusteella. – On arvioitu, että (vuonna 1987) newyorkilainen matkapuhelinyhtiö kärsi kuukaudessa 40 000 dollarin tappiot tämäntyyppisen rikollisuuden johdosta. Koko USA:ssa arvioitiin vuosittaisten tappioiden nousevan kolmeen miljoonaan dollariin. – FBI:n mukaan edellä kerrottu tapaus oli ensimmäinen, jossa päästiin puuttumaan tämän tyyppiseen rikollisuuteen. Puuttumisen mahdollisti uusi tekninen varustus. Ks. Wranghult, s. 23. – Kysyä sopii, millaisia menetykset ovat nyt, lähes kymmenen vuotta myöhemmin, kun matkapuhelinten määrä niin USA:ssa kuin muuallakin on valtavasti lisääntynyt. Toisaalta lienevät suojausmekanismitkin nykyään huomattavasti kehittyneempiä.

[74] HE 94/1993, s. 156. Vrt. kuitenkin jäljempänä selostettava Vaasan HO:n tuomio 18.6.2002, jossa HO kritisoi tätä kannanottoa.

Mikä sitten on se ”tyypillinen tapa”, jolla tietojärjestelmää voitaisiin käyttää? Esimerkiksi jäljempänä selostettavassa TCB-jutussa käräjäoikeus katsoi, että tiettyjen ohjelmien asentaminen tietojärjestelmiin ei ollut järjestelmien käyttämistä niille tyypillisellä tavalla. Olin – ja olen – tältä osin voimakkaasti eri mieltä (samoin kuin Vaasan hovioikeuskin tässä tapauksessa jäljempänä selostettavin tavoin), sillä käsitykseni mukaan ei voida edellyttää, että yksittäistä järjestelmää on käytettävä vain juuri siihen tarkoitukseen, johon se on suunniteltu. Riittävää täytyy olla, että järjestelmää käytetään siten kuin tietojärjestelmiä *yleensä* voidaan käyttää – paitsi selaamalla ja lukemalla tiedostoja myös asentamalla uusia ohjelmia ja muuttamalla tiedostoja. Jos rikoksentekijä tunkeutuu toiselle kuuluvaan tietojärjestelmään ja asentaa siihen jonkin ohjelman, jota käyttämällä hän myöhemmin voi suorittaa sellaisia toimintoja (vaikkapa porttiskannauksia), joita järjestelmässä aikaisemmin ei ollut mahdollista tehdä, hän mielestäni epäilemättä syyllistyy tämän järjestelmän luvattomaan käyttämiseen. Tietojärjestelmän käyttämiselle on nimenomaan tyypillistä, että siihen asennetaan ohjelmia ja että siinä olevia tiedostoja muutetaan.

Ulkomaisia käsityksiä

Ulkomaisessa oikeustieteellisessä kirjallisuudessa ei luvatonta käyttöä ole juurikaan tarkasteltu sen tietotekniikkarikos-ominaisuuden kannalta – ei varsinkaan niin, että olisi pohdittu tunnusmerkistön täyttymisvaiheeseen liittyvää problematiikkaa. Useissa maissa ei ole lainkaan tehty sellaista eroa kuin meillä luvattoman käytön ja tietomurron välillä, mihin on syynä se, että ajatus irtaimen omaisuuden luvattomasta käytöstä *(furtum usus) on* ollut traditiolle vieras.[75]

Nilsson on seurauksiltaan rinnastanut järjestelmään tunkeutumisen yrittämisen luvattomaan käyttöön. Hän toteaa[76] sen tosiasian, että hakkeri on *yrittänyt tunkeutua* (kursivointi tässä) järjestelmään, maksavan yrityksille suuria summia, koska ne eivät ehkä tarkalleen tiedä, kuinka pitkälle järjestelmään hakkeri on päässyt ja onko hän onnistunut pääsemään käsiksi arkaluonteiseen informaatioon.

Luvattoman käytön tunnusmerkistön mahdollisimman aikaisen täyttymisen puolesta tuntuu puhuvan myös *Piragoff* nähdessään yhdeksi luvattoman käytön kriminalisoimisella saavutettavaksi eduksi sen, että näin menetellen voidaan tekijä saada vastuuseen jo ennen kuin hän ehtii syyllistyä muihin suurempaa vahinkoa aiheuttaviin tekoihin.[77]

---

[75] Näin esimerkiksi Italiassa, Ranskassa, Saksassa ja Yhdistyneessä kuningaskunnassa. Ks. Sieber, COMCRIME-Study, III.B.1.
[76] Nilsson, Activities, s. 578 s.
[77] Piragoff, s. 224.

Käyttäminen ja EN:n suositus

Äsken esitettyjen, tunnusmerkistön varhaisen täyttymisen puolesta puhuvien näkemysten – joihin olen valmis yhtymään – lisäksi luvattoman käytön käsitteelle voidaan hakea johtoa Euroopan neuvoston raportista. Tietokoneen luvatonta käyttöä koskeva suositus on valinnaislistalla.[78] Rikoslain 28 luvun 7 §:n säännös poikkeaa suosituksesta paitsi yleisyydessään myös siinä suhteessa, että vahingon tai haitan aiheutumista taikka vahingon tai haitan aiheuttamistarkoitusta ei rikoslaissa nimenomaisesti edellytetä.

Luvattomasta käytöstä aiheutuva suoranainen vahinko saattaa jäädä hyvinkin vähäiseksi ainakin tapauksissa, joissa kysymyksessä on vain vierailu järjestelmässä; tällaiset teot voidaankin yleensä käsitellä lievinä luvattomina käyttöinä. Toisaalta kuitenkin tietojärjestelmään tunkeutuminen ja sitä seurannut käyttäminen merkitsevät sitä, että tietojen luottamuksellisuus on kadonnut: asianomistaja ei voi ilman joskus hyvinkin mittavia selvittelytoimenpiteitä saada selville, mitä järjestelmässä on tapahtunut, ja tällaiset selvittelytoimet vievät aikaa ja rahaa. Näin ollen sinänsä vähäinenkin luvaton käyttö saattaa aiheuttaa asianomistajille varsin merkittäviä taloudellisia menetyksiä.

Euroopan neuvoston raportissa lausutaan termiin ”käyttö” liittyen muun muassa seuraavaa:[79]

> ”Käyttämisen” käsitettä itsessään voidaan tulkita laajasti; teonkuvausta on rajoitettu lisäedellytyksillä. Tekijän on täytynyt toimia oikeudettomasti. Tämä vaatimus täyttyy, kun tekijä on toiminut täysin luvatta tai kun hän on ylittänyt lupaan perustuvan oikeutensa. Se, voidaanko käyttäminen luonnehtia oikeudettomaksi vai ei, ratkeaa useimmissa tapauksissa siviilioikeudellisten säännösten perusteella. – –

Rajoitukset kolmessa eri vaihtoehdossa ovat kahdentyyppisiä. Niissä on kysymys järjestelmän käyttämiseen oikeutetulle (mahdollisesti) aiheutuvasta taloudellisesta menetyksestä ja järjestelmän toiminnalle (mahdollisesti) aiheutuvasta (huomattavaan määrään nousevasta) vahingosta. Tietokoneen luvattoman käyttämisen vaarallisimpiin muotoihin voidaan puuttua näiden rajoitusten puitteissa. Suositus sallii valinnan ahtaamman, todellisen menetyksen tai haitan syntymistä edellyttävän vaihtoehdon ja laajempien vaihtoehtojen välillä. Jälkimmäiset edellyttävät joko sitä, että luvattomalla käytöllä aiheutetaan menetyksen tai

---

[78] Sellainen tietokonejärjestelmän tai -verkoston oikeudeton käyttö, (a) johon tekijä ryhtyy hyväksyen mielessään sen huomattavan riskin, että teosta aiheutuu vahinkoa järjestelmän käyttöön oikeutetulle henkilölle taikka haittaa itse järjestelmälle tai sen toiminnalle, taikka (b) joka tapahtuu tarkoituksin aiheuttaa vahinkoa järjestelmän käyttöön oikeutetulle henkilölle taikka haittaa itse järjestelmälle tai sen toiminnalle, taikka (c) josta aiheutuu vahinkoa järjestelmän käyttöön oikeutetulle henkilölle taikka haittaa itse järjestelmälle tai sen toiminnalle.

[79] EN:n raportti 89, s. 49 ss.

vahingon vaara tai että tekijällä ainakin on ollut tarkoituksena menetyksen tai vahingon vaaran aiheuttaminen. Myös eri vaihtoehtojen yhdistelmät ovat mahdollisia.

Suosituksen tarkoittamat suojeluobjektit ovat kahdenlaisia: toisaalta tahdotaan suojata asianomistajan taloudellisia intressejä, toisaalta yleisemmin tietoturvallisuutta ja järjestelmien toimivuutta. Suomalaisen säännöksen perustelut viittaavat lähinnä siihen, että rangaistavan menettelyn alan nimenomaisella laajentamisella käsittämään nyt puheena olevan tyyppiset tilanteet on ensisijaisesti haluttu saada hakkerit rikosvastuuseen korostamatta mitenkään erityisesti pyrkimystä tehostaa tietoturvallisuutta ja tietojärjestelmien toimintaa tai edes suojata asianomistajan taloudellisia etuja, mikä taas tuntuu olleen ensisijaisena lähtökohtana Euroopan neuvoston suosituksessa.

Ensisijaisesti luvattoman käytön kriminalisoimisen suojeluobjektina on nähtävissä omistajan oikeus omistamansa esineen yksinomaiseen ja häiriöttömään käyttämiseen – tietojärjestelmän kysymyksessä ollessa edellä sanotuin tavoin tietojen luottamuksellisuuden ohella niiden käytettävyys. Kun luvattoman käytön olemukseen kuitenkin kuuluu – päätellen kvalifioitua ja privilegioitua tekomuotoa koskevista tunnusmerkistöistä – ainakin mahdollisuus vahingon syntymiseen, ei rikoslakimme säännös sittenkään ole niin kaukana suosituksessa tarjotuista vaihtoehdoista kuin ensilukemalta saattaisi vaikuttaa.

Käytön luvattomuus

Luvatonta käyttöä koskevan säännöksen perusteluissa ei käsitellä tarkemmin ”luvattomuuden” käsitettä. Tietoteknisessä ympäristössä käytön luvattomuus voi ilmetä ehkä moninaisemmissa muodoissa kuin ajateltaessa esineen käyttöä yleensä, sillä selkeästi havaittavissa olevien ulkonaisten esteiden lisäksi oikeutta käyttämiseen saattavat määritellä ja rajata esimerkiksi tekijänoikeudelliset näkökohdat ja lisenssisopimusten määräykset.

Luvattomuus itsessään on tietysti objektiivinen tunnusmerkistöntekijä, jonka määrittelemisen pitäisi olla aina yksiselitteisesti tehtävissä. Jo yleiskielen mukaan luvatonta käyttämistä on luonnollisesti käyttäminen täysin ilman lupaa tai vastoin nimenomaista kieltoa. Luvatonta käyttöä voi olla myös käyttäminen sellaisissa olosuhteissa, joissa tekijän on täytynyt ymmärtää, että hänellä ei millään perusteella ole ollut oikeutta minkäänlaiseen käyttämiseen. Lisäksi sellainen käyttäminen, joka lähtökohtaisesti on oikeutettua mutta jossain vaiheessa ylittää sallitun rajat, voi nimenomaan tietojärjestelmän ollessa kysymyksessä tulla arvioitavaksi luvattomana käyttönä.

Esimerkiksi tietojärjestelmään, jolla on useita käyttäjiä, on saatettu määritellä erilaisia käyttäjätasoja, joille pääseminen on rajoitettu vaikkapa kytkemällä käyttöoikeudet eri käyttäjätunnuksiin. Yrityksessä työskentelevä henkilö, jonka tehtäviin ei kuulu yrityksen liikesalaisuuksiksi luokiteltavien tietojen käsittely,

saattaa saada – aktiivisen toimintansa seurauksena tai sattumalta – tietoonsa sellaisen käyttäjätunnuksen, joka oikeuttaa pääsyyn liikesalaisuuksia sisältäviin tiedostoihin. Jos henkilö ymmärtää, että hänellä ei ole oikeutta käyttää tuota käyttäjätunnusta ja että hänellä ei ole oikeutta käyttää niitä tietoja, joihin käyttäjätunnus mahdollistaa pääsyn, hän epäilyksittä toimii luvattomasti, olkoonkin, että itse tietojärjestelmän käyttäminen sinänsä olisi hänen työtehtäviinsä kuuluvana toimintana ollut täysin luvallista.

Luvaton käyttö on rangaistavaa vain tahallisesti tehtynä. Tietojärjestelmän luvattomassa käytössä tahallisuuden on ennen muuta käsitettävä tietoisuus käytön oikeudettomuudesta: siitä, että käyttäminen on kiellettyä tai että se edellyttää nimenomaista lupaa, tai siitä, että käyttäjä toimii ylittäen hänellä olevat tai hänelle myönnetyt oikeudet. Lisäksi on edellytettävä, että käyttäjä ymmärtää *käyttävänsä* tietojärjestelmää – jos tekijän tarkoituksena on ollut pelkästään tunkeutua tietojärjestelmään aikomattakaan mennä sen pidemmälle mutta hän kuitenkin osaamattomuuttaan tai varomattomuuttaan saa aikaan objektiivisesti tietojärjestelmän käyttämiseksi katsottavan tapahtuman, ei ole perusteltua syytä tuomita häntä rangaistukseen luvattomasta käytöstä (ellei sitten hyväksytä edellä esittämääni ajatusta siitä, että itse asiassa jo järjestelmään tunkeutumisen yrittäminen olisi katsottava luvattomaksi käytöksi).

Tietojärjestelmissä liikkuva henkilö saattaa tahtomattaan joutua tilanteeseen, jossa hän huomaakin olevansa sellaisessa järjestelmässä tai järjestelmän osassa, johon hänellä ei ollut oikeutta mennä. Syynä tällaiseen saattaa olla esimerkiksi inhimillinen erehtyminen tai sitten jokin järjestelmän ominaisuus. Kun henkilö huomaa joutuneensa puheena olevaan tilanteeseen, tulisi hänen rikosoikeudellisesta vastuusta vapautuakseen välittömästi poistua. Jos hän tultuaan tietoiseksi oleskelunsa oikeudettomuudesta jatkaa järjestelmän käyttämistä, hän syyllistyy luvattomaan käyttöön.

Eräitä käytännön ratkaisuja

Uudempaa (joskin tietotekniikkarikoksen kysymyksessä ollen ehkä jo hieman vanhaksikin katsottavissa olevaa) oikeuskäytäntöä hyvin tyypilliseksi katsottavan tietoteknisessä ympäristössä tapahtuneen luvattoman käytön osalta edustaa Espoon käräjäoikeudessa käsitelty, 30.5.1996 päättynyt juttu.[80]

> Luvattomasta käytöstä 30 päiväsakkoon tuomittu henkilö oli käyttämällä työsuhteensa kestäessä tietoonsa saamaansa yhtiön toimitusjohtajan käyttäjätunnusta tunkeutunut yhtiön palveluksesta erottuaan yhtiön sähköpostijärjestelmään, joka kylläkin oli periaatteessa kaikille avoin, mutta johon oli määritelty erilaisia käyttäjätasoja. Toimitusjohtajan käyttäjä-

[80] Dnro R 96/1209.

> tunnus oikeutti pääsyyn ylimmälle tasolle. Täysin selväksi asiaa käsiteltäessä ei tullut, mitä vastaaja loppujen lopuksi oli järjestelmässä tehnyt, mutta vaikutti ilmeiseltä, että hän enimmillään lähes tunnin mittaisten vierailujensa aikana oli onnistunut siirtymään sähköpostisovelluksesta käyttöjärjestelmätasolle, asentanut järjestelmään niin kutsuttuja takaportteja, joiden kautta hänellä myöhemmin oli mahdollisuus kenenkään huomaamatta palata järjestelmään, ja saanut useampia kertoja aikaan järjestelmän niin sanotun kaatumisen, mistä puolestaan oli asianomistajalle aiheutunut huomattavia kustannuksia.

Käräjäoikeuden päätöksen perustelut ovat kiinnostavat mm. siltä osin kuin niissä käsitellään ”käyttämisen” käsitettä. Käräjäoikeus lausuu muun ohessa seuraavaa:

> Tietojärjestelmän käyttämisellä ei voida käräjäoikeuden käsityksen mukaan katsoa tarkoitettavan vain tietojärjestelmän hyödyntämistä, joka ilmenisi järjestelmässä olevien tietojen ATK-teknisenä tai mekaanisena jäljentämisenä. Mikäli vain järjestelmään sisältyvien tietojen hyödyntäminen olisi luvattomana käyttönä rangaistavaa, jäisi luvattoman käytön ala tietojärjestelmän käyttämisen suhteen erittäin ahtaaksi ja käytön dokumentoiminen olisi vaikeaa. Lainsäätäjän tarkoitus on ollut kriminalisoida kunkin objektin tyypilliset luvattomat käyttämiset. Tietojärjestelmän *luvaton käyttäminen ilmenee tyypillisesti tietojen selaamisena ja lukemisena.* (Kursivointi tässä.)

Käräjäoikeuden perusteluihin on sinänsä helppo yhtyä, vaikka niissä toisaalta sanotaankin sellaista, joka aikaisemmin lausutun perusteella vaikuttaa jopa itsestäänselvyydeltä, ja vaikka niissä nimenomaista kantaa ottamatta asetetaankin rikoksen täyttymisajankohdalle mielestäni liian pitkälle meneviä edellytyksiä, sillä – niin kuin edellä olen sanonut – oma käsitykseni on, että luvaton käyttö alkaa jo huomattavasti tietojen selaamista ja lukemista aikaisemmassa vaiheessa. Selvää kuitenkin on, että tietojen *hyödyntämistä ei missään tapauksessa* pidä edellyttää.

Puheena oleva tapaus herätti jossain määrin mielenkiintoa alan asiantuntijoiden keskuudessa, sillä kysymyksessä ollut yhtiö toimii virustorjunta-alalla. Käräjäoikeuden päätös jäi lainvoimaiseksi.

Horjuvuus luvatonta käyttöä koskevan säännöksen soveltamisalan laajuudesta käy selville kahdesta alioikeusratkaisusta:

> Oulun käräjäoikeus tuomitsi A:n syytteen mukaisesti *tietomurrosta* 50 päiväsakkoon, kun tämä ”oli 18.8.–19.10.1998, muutettuaan Oulun yliopiston tiloissa olleen pankkiyhteysmikron käynnistystiedostoa niin, että hän oli saanut itselleen järjestelmän ylläpitäjän oikeudet, ja asennettuaan laitteeseen erityisen yliopiston ATK-verkkoa käyttävien käyttäjätunnuksia ja salasanoja tallentavan kuunteluohjelman, käyttämällä kuunteluohjelman avulla saamiaan hänelle kuulumattomia käyttäjätunnuksia

> oikeudettomasti tunkeutunut tietojärjestelmiin, joissa sähköisesti käsitellään, varastoidaan ja siirretään tietoja.
>
> A oli 10–15 kertaa kuukaudessa ottanut kotoaan modeemilla yhteyttä mainittuun pankkiyhteysmikroon tarkoituksenaan päästä teollaan hyödyntämään yliopiston nopeita internetyhteyksiä. Hän ei ollut käyttänyt tietojärjestelmiä muutoin niille ominaisella tavalla.
>
> Loki- ja hallintatietojen mukaan A oli saanut kuunteluohjelmalla haltuunsa 132 käyttäjätunnusta salasanoineen. Yksi käyttäjätunnuksista oli ollut Oulun yliopiston maksuliikennejärjestelmän ylläpitäjän ja yksi Valtion teknillisen tutkimuskeskuksen extranet-palvelinta käyttävien tutkimusyksiköiden tunnus."[81]

Tässä tapauksessa on mielestäni tyydytty liian "helppoon" ratkaisuun, kun on lähdetty vaatimaan rangaistusta vain tietomurrosta. Yksin käynnistystiedoston muuttaminen ja kuunteluohjelman asentaminen järjestelmään jo nähdäkseni toteuttaa järjestelmän käyttämisen vaatimuksen, sillä järjestelmässä olevien tiedostojen muuttaminen ja ohjelmien asentaminen järjestelmään on mielestäni tietojärjestelmän käyttämistä sille varsin tyypillisellä tavalla, ja kuunteluohjelman käyttämisellä on saattanut toteutua myös viestintäsalaisuuden loukkauksen tunnusmerkistö, mikäli käyttäjätunnus–salasana-pareja sisältävien datasiirtojen katsotaan olevan viestintäsalaisuuden suojaa nauttivia viestejä (niin kuin olen jäljempänä selostettavassa ns. TCB-jutussa katsonut ja niin kuin myös Jyväskylän käräjäoikeus ja Vaasan hovioikeus katsoivat). Jälleen tosin on huomattava, että välttämättä tällä erottelulla ei rangaistusta ajatellen ole olennaista merkitystä, ellei sitten kuunteluohjelman käyttäminen automaattisesti kvalifioi viestintäsalaisuuden loukkausta törkeäksi.

> Samantapaisesta teosta oli kysymys Turun käräjäoikeudessa, jossa B tuomittiin syytteen mukaan 20 päiväsakkoon *luvattomasta käytöstä,* koska hän oli 1.11.–31.12.1998 "efter att med hjälp av speciella datorprogram ha inhämtat uppgifter om användaridentifikationer och lösenord tillhörande [tillsammans 13 målsäganden], genom att olovligen utnyttja dessa identifieringsmetoder upprepade gånger obehörigen trängt in i ett datasystem tillhörande Åbo Akademi och olovligen brukat detta system för att skaffa sig tillträde till Internet på de verkliga lösenordinnehavarnas kostnad".[82]

Olin itse syyttäjänä jutussa, joten ratkaisu vastaa luonnollisesti omaa ajatteluani; tuomitun menettely eroaa Oulun tapauksesta siinä, että käyttäjätunnuksia ja salasanoja ei ollut hankittu käyttämällä kuunteluohjelmaa, joten asiassa ei noussut esille kysymys mahdollisesta viestintäsalaisuuden loukkauksesta. Luvattoman käytön katsottiin kohdistuneen sekä Åbo Akademin järjestelmään

---

[81] Dnro R 99/1886.
[82] Dnro R 00/561.

että asianomaisten henkilöiden tunnuksiin, joten asianomistajien piiri oli Oulun juttuun verrattuna laajempi.

Asianomistajat luvattomassa käytössä

Tässä suhteessa onkin tietysti olennaista merkitystä sillä, katsotaanko menettelyn toteuttavan tietomurron vai luvattoman käytön tunnusmerkistön, joskin prosessiekonomiset syyt pakottavat kuitenkin laajemmissa jutuissa miettimään salasanojen ja käyttäjätunnusten haltijoiden prosessuaalista asemaa ainakin silloin, kun ei ole syytä epäillä heille aiheutuneen vahinkoa, sillä rikoksentekijän hallusta saattaa löytyä satoja tai tuhansia käyttäjätunnus–salasana-pareja ja näiden haltijoiden käsitteleminen asianomistajina esitutkinnassa ja oikeudenkäynnissä ei yksinkertaisesti olisi järkevää, olletikin kun heille yleensä ei ole voinut aiheutua mitään konkreettista vahinkoa. Tosin selostetussa Åbo Akademin tapauksessa asianomistajiksi katsotuille oli syntynyt vahinkoa tai ainakin vahingon vaaraa sikäli, että Åbo Akademi laskutti heitä myös B:n käyttämistä Internet-yhteyksistä. Summat olivat kuitenkin hyvin pieniä, 20–30 markkaa, ja useimmat eivät olleet laskua tältä osin maksaneetkaan sovittuaan siitä Åbo Akademin kanssa.

Asianomistaja-ominaisuutta arvioitaessa on lisäksi otettava huomioon, että esitutkinta saattaisi tällaisissa tapauksissa venyä tavalla, joka johtaisi syyteoikeuden vanhentumiseen; tietomurron, luvattoman käytön ja viestintäsalaisuuden loukkauksenkin perustekomuotojen vanhenemisaika on vain kaksi vuotta. Laajoissa jutuissa nämä vanhenemisajat ovat epäilemättä muutenkin liian lyhyitä, sillä hakkerin mahdollisesti ympäri maailmaa kulkeneiden reittien selvittäminen ei ole aina kovinkaan helppoa.

TCB-juttu

Suomen tähän mennessä laajimmaksi katsottava[83] tutkittu ja tuomioistuimessa käsitelty tietotekniikkarikosjuttu sai yleisesti tunnetun kutsumanimensä rikoksentekijän käyttämästä nimimerkistä TCB. Juttu lähti selviämään keväällä 1998 muutaman asianomistajan tehtyä keskusrikospoliisille tutkintapyyntöjä tietojärjestelmissään havaitsemiensa luvattomien vierailujen johdosta. Tutkinnassa päästiin pian perille siitä, mistä hyökkäykset olivat lähtöisin, ja lopulta selvisi, että epäilty P oli luvattomasti tunkeutunut useaan sataan Suomessa ja ulkomailla sijainneeseen tietojärjestelmään. Jäätyään kiinni P ryhtyi hyvin yhteistyökykyiseksi ja selvitti esitutkinnassa tekemisensä oletettavasti varsin tarkkaan.

---

[83] Edellä tietomurron yhteydessä selostettu ns. Vantaan hakkerijuttu tosin oli asianomistajien määrällä mitattuna selvästikin TCB-juttua ”laajempi” mutta ottaen huomioon vastaajien järjestelmissä tekemät toimet ja asianomistajille aiheutuneet vahingot voidaan perustellusti pitää TCB-juttua merkittävämpänä tapauksena.

P oli käyttämällä toisaalta työnantajansa ja toisaalta oppilaitoksensa palvelimia siirtynyt verkossa järjestelmistä edelleen toisiin hankittuaan haltuunsa suuren määrän käyttäjätunnus–salasana-pareja. Hän oli asentanut järjestelmiin niin sanottuja takaportteja, jotka mahdollistivat myöhemmin huomaamattoman pääsyn järjestelmiin, hankkinut pääkäyttäjän oikeuksia, jolloin hän periaatteessa pystyi täysin kontrolloimaan valtaamaansa järjestelmää, ja myös lukenut ihmisten sähköposteja.

Sellaisia suomalaisia asianomistajia, jotka vaativat P:lle rangaistusta, oli lopulta kaikkiaan 137; ulkomailla tehtyjä tekoja ei tutkinnassa pyrittykään tarkkaan selvittämään vaan tyydyttiin ainoastaan informoimaan ulkomaisia viranomaisia eikä asianomistajina myöskään käsitelty P:n hallusta löydettyjen käyttäjätunnus–salasana-parien oikeita haltijoita. Jos tällaista ratkaisua ei olisi tehty, olisi asianomistajien määrä kasvanut jopa useisiin tuhansiin, mistä olisi taas tutkinnalle aiheutunut huomattavia hankaluuksia.

Esitutkinta valmistui ja saapui Turun syyttäjänvirastoon tammikuun lopulla 2000 ja haastehakemus lähti Jyväskylän käräjäoikeuteen toukokuun toisena päivänä. Oikeudenkäynti alkoi elokuussa, jolloin järjestettiin ensimmäinen valmisteluistunto. Toinen valmisteluistunto pidettiin lokakuussa 2000 ja nelipäiväinen pääkäsittely tammikuussa 2001. Käräjäoikeus antoi tuomionsa 22.2.2001.[84] Vaasan hovioikeus antoi P:n ja syyttäjän valitusten johdosta tuomionsa 18.6.2002.[85] järjestettyään sitä ennen kolmipäiväisen pääkäsittelyn huhtikuussa 2002.

Ensimmäisessä valmisteluistunnossa vaadin P:lle rangaistusta (1) luvattomasta käytöstä, (2) törkeästä luvattomasta käytöstä, (3) vahingonteosta, (4) törkeästä viestintäsalaisuuden loukkauksesta ja samoin (5) törkeästä viestintäsalaisuuden loukkauksesta, koska

> P oli 1.9.1997–1.7.1998 Jyväskylässä käyttämällä lupaan perustuvan oikeutensa ylittäen työnantajansa A Oy:n tietojärjestelmää sekä luvattomasti Jyväskylän ammattikorkeakoulun tietojärjestelmää, johon oli hänelle kuulumatonta käyttäjätunnusta käyttäen oikeudettomasti tunkeutunut, ottanut näiden tietojärjestelmien välityksellä yhteyksiä [84 asianomistajan] tietojärjestelmiin ja
>
> 1. käyttämällä hänelle kuulumattomia käyttäjätunnuksia ja salasanoja oikeudettomasti tunkeutunut mainittujen asianomistajien tietojärjestelmiin, joita oli luvattomasti käyttänyt siirtymiseen järjestelmästä toiseen sekä jäljempänä syytekohdissa 3–5 selostettavaan toimintaan;
>
> 2. kohdassa 1 selostetulla luvattomalla käyttämisellä aiheuttanut [viidelle asianomistajalle] näiden olot huomioon ottaen erityisen tuntuvaa haittaa tunkeutumisen seurauksena tehtyjen selvittelytoimenpiteiden

[84] Tuomio nro 10357, dnro R 00/687.
[85] Tuomio nro 745, dnro R 01/533.

aiheuttamana lisätyönä sekä näistä toimenpiteistä johtuneista käyttökatkoksista aiheutuneena työajan menetyksenä sekä käyttäjille ja asiakkaille tarkoitettujen palveluiden estymisenä;

3. edellä kerrottujen käyttämisten yhteydessä oikeudettomasti turmellut ja salannut [50 asianomistajan] tietojärjestelmiin tallennettuja tietoja asentamalla niin kutsuttuja takaporttiohjelmia ja muuttamalla olemassa olleita ohjelmia tällaisiksi samoin kuin poistamalla järjestelmien keräämiä lokitietoja; sekä

4. tietoverkossa tapahtuvaa liikennettä kuuntelemaan suunniteltuja ja muunnettuja tietojenkäsittelyohjelmia käyttämällä oikeudettomasti hankkinut tietoja [31 asianomistajan] tietojärjestelmien kautta liikkuneista datasiirroista tarkoituksin kerätä itselleen käyttäjätunnuksia ja salasanoja.

5. Lisäksi P oli 14.11.1997–20.6.1998 Jyväskylässä, saatuaan syytekohdissa 1–4 kerrotuin tavoin eli tietojärjestelmiin tunkeuduttuaan tietoverkossa tapahtuvaa liikennettä kuuntelemaan suunniteltuja tai muunnettuja tietojenkäsittelyohjelmia käyttämällä haltuunsa toisille kuuluvia käyttäjätunnuksia tai salasanoja, joko välittömästi niitä hyödyntäen tai saatuaan niitä käyttämällä itselleen järjestelmien pääkäyttäjän oikeudet, tällä tavoin suojauksen murtaen tunkeutunut useaan sähköpostilaatikkoon ja oikeudettomasti hankkinut tietoja niihin tallennetuista [54 asianomistajan] lähettämistä ja vastaanottamista ulkopuolisilta suojatuista viesteistä.

Kohdan 2 luvatonta käyttämistä ja kohtien 4 ja 5 viestintäsalaisuuksien loukkauksia oli, huomioon ottaen niiden laajamittaisuus ja järjestelmällisyys, pidettävä kokonaisuutena arvostellen törkeinä.

Kaiken kaikkiaan 17 asianomistajaa esitti P:lle korvausvaatimuksia, joiden yhteismäärä alkuvaiheessa nousi noin 800 000 markkaan.

P kiisti luvattoman käytön mutta myönsi järjestelmään tunkeutumisen eräiden asianomistajien kohdalla. Samoin hän kiisti muutaman asianomistajan kohdalla järjestelmään tunkeutumisen mutta myönsi hankkineensa itselleen ja pitäneensä hallussaan näihin järjestelmiin pääsyn mahdollistaneita käyttäjätunnus–salasana-pareja. Esitin tämän vuoksi vaihtoehtoiset syytteet tietomurrosta 49 asianomistajan ja vielä tietomurron yrityksestä 10 asianomistajan kohdalla.

P kiisti lisäksi syyllistyneensä törkeään luvattomaan käyttöön katsoen, ettei kvalifiointiperusteita ollut olemassa. Vahingontekoon P kiisti syyllistyneensä sillä perusteella, ettei hän syytekohdassa kerrotulla menettelyllään ollut turmellut eikä salannut tietoja. Myös viestintäsalaisuuden loukkaukset P kiisti, syytekohdan 4 siksi, että menettelyn kohteena ei ollut televiesti, tunnistetieto tai muu sellainen tieto, jota rikoslain 38 luvussa tarkoitetaan, vaan sellainen etäkäyttötieto, joka ei nauti viestintäsalaisuuden suojaa. P katsoi myös muun muassa, että yksittäisten tietokoneiden liittämistä yhteen verkossa ei voida pitää televerkkona, vaikka niiden väliset yhteydet järjestettäisiin yleisen televerkon välityksellä. Syytekohdan 5 osalta P totesi, etteivät sähköpostiviestit ole olleet

ulkopuolisilta suojattuja Internet-verkossa liikkuessaan ja että vasta 1.7.1999 voimaan tulleella niin kutsutulla teletoiminnan tietoturvalailla (565/1999)[86] oli ratkaistu yksiselitteisesti epäselvyys siitä, koskeeko viestintäsalaisuuden suoja muitakin kuin salattuja sähköpostiviestejä.[87]

Käräjäoikeus tuomitsi P:n 53 asianomistajaan kohdistuneesta luvattomasta käytöstä, 22 asianomistajaan kohdistuneesta tietomurrosta, yhdeksään asianomistajaan kohdistuneesta tietomurron yrityksestä, 30 asianomistajaan kohdistuneesta törkeästä viestintäsalaisuuden loukkauksesta (syytekohta 4) ja 52 asianomistajaan kohdistuneesta törkeästä viestintäsalaisuuden loukkauksesta (syytekohta 5) yhteiseen viiden kuukauden ehdolliseen vankeusrangaistukseen. P velvoitettiin suorittamaan asianomistajille vahingonkorvauksia ja oikeudenkäyntikulujen korvauksia yhteensä noin 450 000 markkaa. Käräjäoikeus hylkäsi syytteet törkeästä luvattomasta käytöstä ja vahingonteosta.

TCB-jutussa ei jouduttu – onneksi – P:n jäljittämistä lukuun ottamatta kovinkaan paljon hakemaan näyttöä elektronisen todistusaineiston perusteella; jos näin olisi jouduttu menettelemään, olisi juttu todennäköisesti päässyt suurelta osin vanhenemaan. P:n yhteistyöhalukkuus tutkintavaiheessa oli jutun käsittelyn kannalta varsin merkityksellistä ja vaikutti epäilemättä rangaistuksen mittaamiseenkin.

Syyteharkintavaiheessa vaikutti siltä, että jutussa on kaksi lain soveltamisen kannalta mielenkiintoista kysymystä: syytteessä vahingonteoksi kuvatun menettelyn ja vahingonteon tunnusmerkistön vastaavuus sekä syytekohdassa 4 tarkoitettujen datasiirtojen luonne viestintäsalaisuuden suojaa nauttivina viesteinä. Oikeudenkäynnin aikana jossain määrin yllättävästi nousivat keskeisiksi kysymyksiksi myös tietomurron ja luvattoman käytön välinen suhde sekä syytekohdassa 5 tarkoitetun sähköpostin nauttiman suojan ulottuvuus. En käsittele tässä viestintäsalaisuuden loukkauksiin liittyviä ongelmia ja vahingontekoa koskeviin kysymyksiin palaan jäljempänä vahingontekoa muutoin käsiteltäessä.

Syyte oli alun perin laadittu luvattoman käytön teonkuvauksen osalta ehkä liian suppeaksi mutta tästä ei loppujen lopuksi ollut mitään haittaa, sillä seuraamuksen ja asianomistajien korvausvaatimusten toteutumisen kannalta ei ollut merkitystä sillä, olivatko syyksiluetut teot luvattomia käyttöjä vai tietomurtoja tai luvattoman käytön vai tietomurron yrityksiä. Ne menettelyt, jotka alun alkaen olin katsonut luvattomaksi käytöksi, luettiin joka tapauksessa *rikoksina* P:n syyksi.

---

[86] Laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta 22.4.1999/565; HE 85/1998.

[87] Tässä yhteydessä en puutu kovin yksityiskohtaisesti syytekohdissa 4 ja 5 tarkoitettuihin viestintäsalaisuuden loukkauksiin, sillä osassa I selostetuin tavoin jätän viestintään liittyvät rikokset tämän tutkimuksen ulkopuolelle. Tämä ei merkitse sitä, etteivätkö TCB-jutun viestintäsalaisuuden loukkauksiin liittyvät kysymykset olisi erityisen mielenkiintoisia ja näin ollen ansaitsisi tarkempaa kommentointia jossain muussa yhteydessä.

Käräjäoikeus on perustellut luvatonta käyttöä koskevaa syyksilukemista seuraavasti:

> Edellä lain esitöistä lausutusta on pääteltävä, että siltä osin kuin tietojärjestelmää on käytetty siirtymiseen siitä toiseen järjestelmään, kysymys on ollut sen luvattomasta käytöstä. Sen sijaan menettelyssä siltä osin kuin syytteessä on viitattu sen 3-kohtaan, kysymys ei ole ollut tietojärjestelmien tarjoamien palvelujen käytöstä, vaan pikemminkin niitä ylläpitäviin käyttöjärjestelmiin taikka vastaaviin ohjelmiin kohdistuvista toimista. HE:stä 94/1993 ei ole suoraan pääteltävissä, onko näihin ohjelmiin kohdistuvia toimia pidettävä järjestelmän käyttämisenä. Tältä osin esityksessä luvattomana käyttönä ei ole vielä pidetty sitä, että tunkeutuja saa esimerkiksi kohteena olevan tietokoneen käyttöjärjestelmän toimimaan. Kuitenkin lakiesityksen mukaan tietomurtona pidettävä tunkeutuminen ei edellytä, että tietojärjestelmässä olevia tietoja millään tavalla käytetään tai niitä edes luetaan tai selataan. Rikos on täyttynyt heti, kun tunnistuskontrolli on läpäisty. Jos rikos on edennyt tietojen käyttämiseen saakka, tekoon esityksen mukaan tulee soveltaa luvatonta käyttöä koskevia säännöksiä. Näin ollen käräjäoikeus katsoo, että säännöstä on esityksessä lausutun perusteella tulkittava niin, että tietojärjestelmän käyttämisenä on myös pidettävä sitä ylläpitäviin ohjelmiin kohdistuneita toimia, kuten tässä tapauksessa tietojärjestelmään kuulumattomien ohjelmien asentamista, olemassa olevien ohjelmien muuttamista ja järjestelmässä olevien tiedostojen poistamista. Sen sijaan syytteen 4 ja 5 -kohdissa mainittua menettelyä ei ole pidettävä tietojärjestelmien käyttämisenä niille ominaisella tavalla ja siten 1-kohdan mukaisena luvattomana käyttönä.

Niin kuin edellä olen lausunut, hallituksen esityksessä teon täyttymisasteesta sanottu on mielestäni liian pitkälle vietyä. Se lienee vaikuttanutkin siihen, että käräjäoikeus tuntuu olleen turhan varovainen pohtiessaan käyttöjärjestelmää ylläpitäviin ohjelmiin kohdistuneen käytön luonnetta.

Valituksessani katsoin, että myös kohdissa 4 ja 5 selostettu menettely eli tiedon hankkiminen asianomistajien tietojärjestelmissä liikkuneista datasiirroista asentamalla järjestelmiin uusia verkonkuunteluohjelmia, olemassa olevien ohjelmien muuttaminen ja järjestelmään tallennetun datan sisällön selvittäminen oli tietojärjestelmän käyttämistä juuri sille ominaisella tavalla ja siten myös luvatonta käyttöä. Mainittakoon, että P:kin oli samaa mieltä, joskin katsoi kysymyksessä olleen tietomurtojen rangaistavan valmistelun.

Vaasan hovioikeus lausui perusteluissaan tältä osin seuraavaa:

> Käräjäoikeus on osittain hylännyt tuomiolauselman kohtaa 1.1 koskevan syytteen sillä perusteella, ettei 4 ja 5 -kohdissa mainittua menettelyä ole pidettävä tietojärjestelmien käyttönä niille ominaisella tavalla. Myös syyttäjän mukaan menettelyn lukeminen P:n syyksi luvattomana käyttönä edellyttää tietojärjestelmän käyttämistä sille ominaisella tavalla. Syyt-

> täjä on perustanut tämän rikoslain 28 luvun 7 §:n säännöksen tulkintaa koskevan käsityksensä eri yhteydessä säädetyn tietomurtoa koskevan rikoslain 38 luvun 8 §:n esitöissä (HE 94/1993 vp. s. 140 ja erityisesti s. 156) esitettyyn kannanottoon.
>
> Luvatonta käyttöä koskevan rikoslain 28 luvun 7 §:n sanamuoto ei rajaa rangaistavan käyttäytymisen alaa vain siihen, että rikoksen kohteena olevaa omaisuutta käytetään sille ominaisella tavalla. Myös lainkohdan esitöistä (HE 66/1988 vp. s. 43) ja oikeuskäytännöstä (KKO 1998:25) on pääteltävissä, että luvattoman käytön kriminalisoimisella suojataan omistajalle kuuluvaa oikeutta päättää esineen käytöstä riippumatta esineen tyypillisestä käyttötarkoituksesta. Lainkohdan soveltamisala on siten varsin laaja. Myöhemmän lainsäädännön esitöissä esitetty kannanotto ei anna aihetta tietojärjestelmien kohdalla lainkohdan suppeampaan tulkintaan. Sitä paitsi hovioikeus katsoo, että uusien ohjelmien asentaminen tietojärjestelmiin, olemassa olevien ohjelmien muuttaminen ja järjestelmään tallennetun datan sisällön selvittäminen on etenkin tietoteknisestä näkökulmasta tarkasteltuna tietojärjestelmien käyttämistä niille ominaisella tavalla.
>
> Käräjäoikeuden tuomion syyksilukemista muutetaan edellä selostetun perusteella siten, että myös kohdissa 4 ja 5 kuvattu menettely luetaan P:n syyksi kohdassa 1.1 luvattomana käyttönä.

Hovioikeuden kanta on mielestäni oikea ensinnäkin siinä, että tietojärjestelmän käyttäminen sille ominaisella tavalla tulkitaan laajasti, ja toiseksi siinä, että luvatonta käyttöä koskevaa säännöstä ylipäänsä tulkitaan laajasti. Tosin kysymyksessä oleva menettely mielestäni joka tapauksessa oli tietojärjestelmän käyttämistä sille ominaisella tavalla.

Hylätessään syytekohdan 2 syytteen törkeästä luvattomasta käytöstä käräjäoikeus ensin lausuu seuraavasti:

> Törkeää luvatonta käyttöä koskeva RL 28 luvun 8 §:n säännös on lisätty HE:n 66/1988 eduskuntakäsittelyn aikana lakivaliokunnan mietintöön (LaVM 6/1990). Mietinnöstä käy ilmi, että säännöksellä on tarkoitettu mahdollistaa ankara suhtautuminen luvattomaan käyttöön, jossa käytön kohteen arvo sinänsä ei ole suuri, mutta käytöstä aiheutuu esineen omistajalle huomattavaa vahinkoa tai haittaa. Lisäksi säännökseen sisältyvällä ilmaisulla ”aiheutetaan rikoksen uhrille tämän olot huomioon ottaen erityisen tuntuvaa” näytettäisiin mietinnön perustelujen mukaan tarkoitetun, että vahinko tai haitta on arvioitava suhteessa rikoksen kohteen taloudelliseen asemaan tai tämän muihin vastaaviin olosuhteisiin.

Tämän jälkeen käräjäoikeus referoi syytteen ja vahingonkorvausvaatimusten tueksi esitettyä todistelua ja jatkaa:

> Siten todistelu osoittaa, että P:n toiminnasta on aiheutunut syytteen 2-kohdassa mainituille asianomistajille sinänsä määrällisesti huomattavaa vahinkoa ja haittaa. Edelleen todistelun mukaan, kun P on ollut

> tietotekniikka-alaa tunteva ja hänen toimintansa on ollut pitkäaikaista ja järjestelmällistä, P:n on lain edellyttämin tavoin täytynyt mieltää nämä menettelynsä seuraukset. Kuitenkin 2-kohdan asianomistajista muut paitsi B Oy ovat opetusministeriön alaisia yhteiskunnallisesti merkittäviä yhteisöjä, joiden toiminnan rahoitus tapahtuu valtion varoista. Näin ollen, kun niille P:n menettelystä aiheutunutta taloudellista menetystä arvioidaan tuosta lähtökohdasta, vahinko ei ole ollut näiden asianomistajien oloihin nähden erityisen tuntuvaa.

Hain muutosta myös tältä osin, sillä syytteen mukaan luvaton käyttö kvalifioitui pelkästään asianomistajien *toiminnalle aiheutuneen haitan* perusteella täysin riippumatta *taloudellisen vahingon* määrästä, joka ei omasta mielestänikään näiden valtion rahoittamien laitosten kohdalla ollut niiden oloihin nähden erityisen tuntuvaa. Oma tulkintani toiminnallisen haitan merkityksestä perustuu lain sanamuotoon ja käsitteiden ”haitta” ja ”vahinko” erilaiseen merkityssisältöön, jota on käsitelty uudemman tietotekniikkarikoksia koskevan lainsäädännön perusteluissakin.[88] Hovioikeus päätyi samaan lopputulokseen ja totesi mm. seuraavaa:

> Lainkohdan ”rikoksen uhrille tämän olot huomioon ottaen erityisen tuntuvaa” – ilmaisulla viitataan sinänsä rikoksen uhrin taloudellisiin ja muihin olosuhteisiin. Lainkohdan sanamuodolla on kuitenkin tarkoitettu saattaa ankaramman rikosvastuun piiriin myös ne tilanteet, joissa aiheutunut vahinko tai haitta ei ole sinällään kovin suuri mutta josta on esimerkiksi uhrin vähävaraisuudesta johtuen aiheutunut hänelle huomattavaa vahinkoa tai haittaa (LaVM 6/1990 vp. s. 8 ja HE 66/1988 vp. s. 37). Tähän tarkoitukseen nähden ei rikoksen uhrin hyvälle taloudelliselle asemalle voida antaa ratkaisevaa merkitystä. Muussa tapauksessa ei esimerkiksi valtioon tai sen virastoihin ja laitoksiin kohdistuvaa luvatonta käyttöä voitaisi katsoa törkeäksi muutoin kuin erittäin harvinaisissa tilanteissa. Lainsäätäjän ei voida katsoa tarkoittaneen tätä.
> – –
> Hovioikeus toteaa kuitenkin tässä vaiheessa rikosoikeudellisesta näkökulmasta, että haittaa, joka on ilmennyt selvittelytoimenpiteiden aiheuttamana lisätyönä sekä käyttökatkoksista aiheutuneena työajan menetyksenä ja palveluiden estymisenä, on pidettävä erityisen tuntuvana. Toisin kuin käräjäoikeus on katsonut, hovioikeus pitää [neljälle asianomistajalle] aiheutunutta haittaa myös näiden olot huomioon ottaen erityisen tuntuvana. Luvaton käyttö on sen järjestelmällisyys ja laajamittaisuus huomioon ottaen myös kokonaisuutena arvostellen törkeä.

---

[88] Ks. HE 4/1999, jossa RL 34:9a:n perusteluissa lausutaan seuraavasti: ”Haitalla tarkoitetaan paitsi suoranaista, esimerkiksi tiedostojen häviämisenä tai muuttumisena syntyvää vahinkoa myös mitä tahansa muuta sellaista vaikutusta tieto- tai telejärjestelmän toimintaan, joka jollain tavalla loukkaa järjestelmän haltijan tai muun sen käyttöön oikeutetun oikeutta järjestelmän käyttöön eli niin sanottua tietojenkäsittelyrauhaa. Tällaisena haittana voisi siis tulla kysymykseen esimerkiksi viruksen saastuttaman järjestelmän toiminnan hidastuminen tai se tosiasiallinen tilanne, että levytila, jonka virus on vallannut, ei ole järjestelmän käyttöön oikeutetun käytettävissä.”

Hovioikeus muutti päätöstä myös sikäli, että se katsoi kaiken luvattomana käyttönä P:n viaksi luetun menettelyn yhdeksi törkeäksi luvattomaksi käytöksi. Tältä osin hovioikeus lausui mm. seuraavasti:

> Rikosten yhtymissäännösten uudistamista koskeneen lain esitöiden mukaan teko, jota luonnollisen katsantokannan mukaan on pidettävä yhtenä tekona, tulisi aikaisempaa useammin katsoa yhdeksi eikä useammaksi rikokseksi (LaVM 15/1990 vp. s. 3 ja HE 84/1980 vp. s. 8). Korkein oikeus on oikeuskäytännössään todennut, että sen kysymyksen ratkaiseminen, onko kyseessä yksi vai useampi rikos, on jäänyt oikeustieteen ja oikeuskäytännön varaan. Harkittaessa tätä kysymystä on kiinnitettävä huomiota siihen, minkälaisen ajallisen ja toiminnallisen kokonaisuuden yksittäiset teot muodostavat (esimerkiksi KKO 1996:41, KKO 1996:42 ja KKO 1994:67).
> – –
> Yhteenvetona hovioikeus toteaa, että P:n teot muodostavat luonnollisen katsantokannan mukaan sellaisen yhtenäisen ajallisen ja toiminnallisen kokonaisuuden, ettei kohdissa 1.1 ja 2 selostettuja tekoja ole pidettävä eri rikoksina vaan P:n menettely tulee arvioitavaksi kokonaisuudessaan pelkästään kohdassa 1.1.

Hovioikeus siis vahvisti sen jo aikaisemmin alioikeuskäytännössä hyväksytyn käsityksen, että useisiin tietojärjestelmiin kohdistunut rikollinen menettely muodostaa yhden kokonaisuuden, joka tulee lukea tekijän syyksi yhtenä rikoksena. Hovioikeus korotti P:lle tuomitun ehdollisen vankeusrangaistuksen viidestä seitsemään kuukauteen eikä muuttanut käräjäoikeuden asianomistajille maksettavaksi tuomitsemia vahingonkorvauksia. P tuomittiin korvaamaan asianomistajien oikeudenkäyntikuluja hovioikeudessa noin 20 000 euroa.

TCB-jutulla on merkitystä paitsi joiltain osin tärkeänä ennakkotapauksena myös siinä, että se konkreettisesti osoitti, miten haavoittuvia tietojärjestelmät saattavat olla silloin, kun osaava rikoksentekijä on asialla. Käytännössä useat jutun asianomistajista ja varmasti monet muutkin järjestelmien ylläpitäjät ovat jutun paljastumisen jälkeen parantaneet järjestelmiensä tietoturvallisuuden tasoa. P:n ansioksi on luettava se, ettei hän käyttänyt esimerkiksi saamiaan pääkäyttäjien oikeuksia tavalla, johon hänellä olisi ollut mahdollisuus – jos kysymyksessä olisi ollut todella pahansuopa krakkeri, olisi hän kyennyt aiheuttamaan asianomistajille todella korvaamattomia vahinkoja (esimerkiksi tuhoamalla kaiken Helsingin yliopistoon tietojärjestelmiin tallennetun tiedon), joiden arvoa ei rahassa olisi ollut mahdollista mitata.

Luvattoman käytön suhde muihin rikoksiin

Edellä on luvattomana käyttönä pääasiallisesti tarkasteltu tietojärjestelmään tunkeutumista seurannutta järjestelmään kohdistunutta luvatonta käyttöä. Tieto*koneen* luvaton käyttö voi toki tapahtua paljon yksinkertaisemminkin: työn-

tekijä saattaa luvatta tai lupaan perustuvan oikeutensa ylittäen käyttää työnantajansa tietokonetta ja siinä olevaa ohjelmaa esimerkiksi omien tekstiensä käsittelyyn ryhtymättä kuitenkaan esimerkiksi selaamaan sellaisia tiedostoja, joihin pääsyyn hänellä ei ole oikeutta.

Tällainen luvaton käyttö ei olennaisesti eroa minkä tahansa muun esineen käytöstä ja voidaankin kysyä, onko kysymyksessä enää lainkaan mikään erityinen tietotekniikkarikos.[89] Käyttäminen tosin edellyttää ainakin jonkinasteista tietoa tietotekniikasta, koska siinä koneen ohella käytetään myös ohjelmistoa tai järjestelmää, jollainen käyttäminen kylläkin nykypäivänä alkaa kuulua jo ainakin nuorempien henkilöiden perusvalmiuksiin. Euroopan neuvoston suosituksen voidaan tulkita kattavan tällaisetkin tilanteet, mutta olisin silti valmis rajaamaan tällaiset teot esittämäni tietotekniikkarikoksen määritelmän ulkopuolelle.

Tietotekniikkarikosten kohdalla Suomessa valittu sääntelytapa aiheuttaa sen, että tunnusmerkistöjen väliset rajat jäävät monessa kohdin epätäsmällisiksi ja että lainkonkurrenssitilanteilta ei voida välttyä. Rikoslain 30 luvun 4 §:n yritysvakoilu, 33 luvun tietotekniseen tallenteeseen kohdistuvat väärennykset, 35 luvun 1 §:n 2 momentin tietovahingon aiheuttaminen ja 36 luvun 1 §:n 2 momentin tietojenkäsittelypetos samoin kuin 38 luvun 8 §:n tietomurto käsittänevät yleensä tosiasiallisesti myös luvattoman käytön. Tällaisessa tilanteessa tietomurtosäännös nimenomaisen määräyksen perusteella väistyy ja luvaton käyttö puolestaan sisältyy yritysvakoiluun, väärennykseen ja petokseen.

Sen sijaan luvattoman käytön ja vahingonteon suhde ei ole yhtä selvä: molemmista rikoksista on säädetty samanlaiset rangaistusuhat eikä vahingonteon yritystä ole kriminalisoitu. Mielestäni on oikein katsoa, että tietojärjestelmää luvattomasti käyttäen aikaansaatu tallennetun tiedon vahingoittuminen on luettava tekijänsä syyksi sekä luvattomana käyttönä että vahingontekona, vaikkakin rikoslain 35 luvun 5 §:n säännöksen mukaan vahingontekoa koskeva säännös sinänsä on toissijainen. Tällaisessa tilanteessa mielestäni ensin toteutuu luvaton käyttö ja vasta sen jälkeen, erikseen, vahingonteko.

Luvatonta käyttöä ja vahingontekoa koskevat rangaistussäännökset ovat syntyneet tyystin erilaisten oikeushyvien suojaamiseksi. Tietojärjestelmän luvattoman käytön kriminalisoinnilla suojataan paitsi tietojen luottamuksellisuutta myös järjestelmän käyttöön oikeutetun oikeutta järjestelmän yksinomaiseen ja häiriöttömään käyttämiseen eli tietojärjestelmän *käytettävyyttä.* Tietojärjestelmään kohdistuneen vahingonteon kriminalisoiminen puolestaan antaa suojaa järjestelmän *eheydelle* ja *luottamuksellisuudelle.*

Olkoonkin, että luvattoman käytön *yhteydessä* voidaan toteuttaa useitakin muita rikostunnusmerkistöjä, se ei kuitenkaan ole edellytyksenä luvattoman

---

[89] Ks. myös Silvander, s. 144.

käytön tunnusmerkistön täyttymiselle: luvaton käyttö on siinä mielessä itsenäinen rikos. Vahingonteko on jotakin, joka menee luvatonta käyttämistä *pitemmälle* ja loukkaa tietotekniikkarikosten yhteistä suojeluobjektia eli tietojenkäsittelyrauhaa huomattavasti pelkkää luvatonta käyttämistä enemmän.

Luvaton käyttö voi *ilmetä* vahingontekorikoksen tunnusmerkistön toteuttavana menettelynä (niin kuin henkilöauton luvaton käyttö voi *ilmetä* törkeänä liikenneturvallisuuden vaarantamisena) mutta koska teoilla on eri kohteet, ei niitä voida katsoa samaksi teoksi rikoslain 35 luvun 5 §:n mielessä. Jos lähtökohtaisesti katsottaisiin, että rikoslain 35 luvun 1 §:n 2 momentissa tarkoitettu menettely syrjäytyisi luvattoman käytön tieltä, on hyvin vaikea enää kuvitella tilannetta, jossa lainkohtaa ylipäänsä voitaisiin soveltaa: tallennetun datan hävittäminen, turmeleminen, kätkeminen tai salaaminen on poikkeuksetta tietojärjestelmän käyttämistä ja jos menettely on oikeudetonta, sen täytynee olla rikoslain 28 luvun 7 §:ssä tarkoitetuin tavoin myös luvatonta.

Lainvalmisteluaineistosta ei tähän ongelmaan löydy yksiselitteistä ratkaisua, tosin hallituksen esityksessä 66/1988 puhutaan rikoslain 35 luvun 5 §:n perusteluissa ”vahingonteon luonteisista teoista” niinä tekoina, joita koskevat kriminalisoinnit etupäässä syrjäyttäisivät ko. lainkohdan. Luvatonta käyttöä ei voitane pitää vahingonteon luonteisena tekona, ei sen paremmin tekotavaltaan kuin suojeluobjektiltaankaan. TCB-jutussa jouduttiin käsittelemään myös tätä kysymystä, johon palaan tarkemmin jäljempänä vahingontekoa käsiteltäessä.

Vahingonteon jäädessä yritysasteelle mutta luvattoman käytön tunnusmerkistön täyttyessä voidaan tekoa arvioida ainoastaan luvattomana käyttönä. Konkurrenssitilanteisiin liittyviin ongelmiin palataan tarkemmin jäljempänä.[90]

[90] Luvattoman käytön konkurrenssitilanteista yleisemmin ks. Lappi-Seppälä, Rikosoikeus, s. 977.

3 Tietojen eheyttä loukkaavat teot

3.1 VÄÄRENNYS (RL 33:1)

Myös väärennysrikoksia koskeva rikoslain 33 luku uudistettiin lailla 769/1990. Perustekomuoto säädetään rangaistavaksi 1 §:ssä:

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

Väärennyksen yrityksen kriminalisoiva toinen momentti lisättiin pykälään 1.7.2003 voimaan tulleella lailla 514/2003.[91] Kvalifioitua ja privilegioitua tekomuotoa koskevat säännökset ovat luvun 2 ja 3 §:ssä.[92] Väärennys on kaikissa muodoissaan virallisen syytteen alainen rikos.

Tietotekniikkarikosten kannalta merkityksellinen on luvun kuudennen pykälän määritelmäsäännös:

> *Todistuskappaleena* pidetään tässä laissa asiakirjaa ja sen näköisjäljennöstä, merkkiä, leimaa, rekisterikilpeä, ääni- ja kuvatallennetta, piirturin, laskimen tai muun vastaavan teknisen laitteen tuottamaa tallennetta sekä automaattiseen tietojenkäsittelyyn soveltuvaa tallennetta, jos sitä käytetään tai voidaan käyttää oikeudellisesti merkityksellisenä todisteena oikeuksista, velvoitteista tai tosiasioista.
>
> Todistuskappale on väärä, jos se todisteena käytettäessä on omiaan antamaan erehdyttävän kuvan alkuperästään tai antajansa henkilöllisyydestä.
>
> Todistuskappale on väärennetty, jos sen sisältöä on oikeudettomasti muutettu jonkin todistelun kannalta merkityksellisen tiedon osalta.

Vanhat rikoslain väärennysrikoksia koskevat säännökset oli sijoitettu pääasiassa rikoslain 36 lukuun yhdessä petosrikosten kanssa, mutta myös muualla laissa oli runsaasti tunnusmerkistöjä, joihin sisältyi väärennysrikoksille ominaisia

[91] HE 2/2003.

[92] RL 33:2: Jos väärennyksessä (1) rikoksen kohteena oleva todistuskappale on yleiseltä kannalta tärkeä viranomaisen säilyttämä arkistoasiakirja tai viranomaisen pitämä yleinen rekisteri taikka jos todistuskappale on todistusarvoltaan muuten erityisen merkityksellinen tai (2) rikoksentekijä käyttää väärennysrikosten tekemistä varten hankittua teknistä laitteistoa taikka muuten toimii erityisen suunnitelmallisesti ja väärennys on myös kokonaisuutena arvostellen törkeä, rikoksentekijä on tuomittava törkeästä väärennyksestä vankeuteen vähintään neljäksi kuukaudeksi ja enintään neljäksi vuodeksi.

RL 33:3: Jos väärennys, huomioon ottaen todistuskappaleen laatu tai muut rikokseen liittyvät seikat, on kokonaisuutena arvostellen vähäinen, rikoksen tekijä on tuomittava lievästä väärennyksestä sakkoon.

elementtejä. Säännökset olivat säilyneet samanlaisina rikoslain säätämisestä lähtien eivätkä ne enää vastanneet nykyajan vaatimuksia.[93]

Säännösten taustasta

Epäkohta oli muun ohessa se, että väärennysrikosten tunnusmerkistöön kuului yleensä väärennetyn tai väärän asiakirjan käyttäminen; pelkkä väärentämistoimi sinänsä oli vain poikkeuksellisesti kriminalisoitu. Käyttämisvaatimus johti väärennyksen ja petoksen välisen rajanvedon hämärtymiseen erityisesti sellaisissa vaihdantatilanteissa, joissa asiakirjan antajan henkilöllisyydellä oli toisarvoinen merkitys. Väärien tai väärennettyjen asiakirjojen valmistaminen ja hallussapito jäivät yleensä sellaisinaan rankaisematta, olipa niiden käyttötarkoituksen laittomuus miten ilmeistä tahansa. Vanhoissa säännöksissä tehtiin vielä ero yleisen ja yksityisen asiakirjan välillä.[94]

Uusien säännösten mukaan väärennyksen rangaistavuuden edellytyksenä ei enää ole väärän tai väärennetyn todistuskappaleen käyttäminen, mutta käyttäminen mainitaan kolmantena tekotapana väärän todistuskappaleen valmistamisen ja aidon todistuskappaleen väärentämisen rinnalla.[95]

---

[93] Aikaisemman sääntelyn epäkohdista ks. myös HE 66/1988, s. 110.

[94] Yleisten asiakirjain väärentämisestä säädettiin 3 ja 4 §:ssä:

36:3: Joka, hankkiakseen itselleen tai toiselle hyötyä taikka toista vahingoittaakseen, valmistaa väärän tai väärentää oikeuden tahi muun viranomaisen tuomiokirjan tai alkuperäisen pöytäkirjan, tilikirjan, kirkonkirjan, henkikirjan, (maarekisterin) taikka muun sellaisen asiakirjan, joka on yleiseksi hyödyksi ja ojennukseksi, rangaistakoon (kuritushuoneella) vähintään yhdeksi ja enintään kuudeksi vuodeksi tai, jos asianhaarat ovat erittäin lieventävät, vankeudella vähintään kahdeksi kuukaudeksi, (sekä menettäköön sitä paitsi kansalaisluottamuksensa). Jos hän väärää tai väärennettyä asiakirjaa käytti, tuomittakoon (kuritushuoneeseen) vähintään kahdeksi ja enintään kahdeksaksi vuodeksi tai, jos asianhaarat ovat erittäin lieventävät, vankeuteen vähintään kuudeksi kuukaudeksi, (sekä lisäksi kansalaisluottamuksensa menettäneeksi). (1 mom.) Jos rikos tehtiin ilman mainittua aikomusta, olkoon rangaistus vankeutta. (2 mom.)

36:4: Jos joku on väärentänyt yleisen asiakirjan, jonka julkinen virasto tahi virkamies on antanut, taikka sellaisen asiakirjan valmistanut väärin, ja jos hän sitä käyttää hankkiaksensa itselleen tai toiselle hyötyä taikka toista vahingoittaakseen; rangaistakoon (kuritushuoneella) vähintään yhdeksi ja enintään neljäksi vuodeksi (ja menettäköön kansalaisluottamuksensa), taikka, jos asianhaarat ovat erittäin lieventävät, vankeudella korkeintaan kahdeksi vuodeksi taikka sakolla. (1 mom.) Jos väärä asiakirja on matkapassi, mainetodistus, taikka muu senkaltainen todistus; tuomittakoon vankeutta korkeintaan yksi vuosi taikka sakkoa. (2 mom.)

Yksityisen asiakirjan väärentämisestä säädettiin seuraavasti:

36:5: Joka valmistaa väärän taikka väärentää kauppakirjan, testamentin, välikirjan, velkakirjan, vekselin, kuitin, kaupanpitokirjan, taikka muun sellaisen yksityisen asiakirjan, ja sitä käyttää, hankkiaksensa itselleen tai toiselle hyötyä taikka toista vahingoittaakseen, rangaistakoon (kuritushuoneella) korkeintaan neljäksi vuodeksi (ja menettäköön kansalaisluottamuksensa) taikka, jos asianhaarat ovat erittäin lieventävät, tahi jos asiakirja on päästökirja, yksityisen antama mainetodistus, tahi muu senkaltainen todistus, vankeudella korkeintaan kuudeksi kuukaudeksi taikka (enintään viidensadan markan) sakolla.

Kuudennessa pykälässä kriminalisoitiin väärän asiakirjan käyttäminen sekä 10–12 §:ssä veroja muihin merkkeihin ja leimoihin kohdistuneet väärennykset.

[95] Ks. HE 66/1988, s. 110 s.

Tulkintaongelmista

Vaikka vanhoja väärennyssäännöksiä monessa suhteessa tulkittiinkin joustavasti, ei niitä kuitenkaan saatu sopeutumaan teknologian kehittymisen myötä syntyneisiin uusiin informaation tallentamisen muotoihin. Kun aikaisemmin asiakirjan muotoon tallennettua informaatiota yleensä on edustanut selvästi *nähtävissä oleva* data, toisin sanoen paperille painetut tai muuten kiinnitetyt kirjainmerkit, joista datan kantama informaatio on ainakin suuremmitta vaikeuksitta luettavissa, voi data nykyään olla tietokonenauhalla tai levykkeellä rautahiukkasina taikka CD-levyllä[96] painaumina, jolloin informaation selvittäminen ei ilman teknisiä apuvälineitä onnistu.

On kuitenkin huomattava, että yhtä lailla kuin jokin ihmisen käyttämä kieli on sopimukseen perustuva merkkien järjestelmä, jonka tulkitseminen järjestelmän logiikkaa tuntematta on mahdotonta, myös tietovälineeseen kiinnitetyn datan on ollakseen mielekästä aina oltava järjestetty tietyllä sopimukseen perustuvalla tavalla. Näin systeemin tuntevan on mahdollista selvittää myös tällaisen datan kantama informaatio, vaikka merkkijonoa ei olisikaan translitteroitu esimerkiksi latinalaisista kirjainmerkeistä muodostuvaksi merkkijonoksi (ja tätä mahdollisesti edelleen muokattu vaikkapa suomenkielisiksi sanoiksi ja lauseiksi).

Asiallisesti ei siis pitäisi olla eroa siinä, onko informaatio luettavissa paperilta vai onko se löydettävissä tietokonelevykkeeltä tai muulta tietotekniseltä tallennusvälineeltä. Merkitystä ei pitäisi olla informaation kantajan koolla: lukijasta riippuen saattaa jo normaalikokoisen kirjoitetun tekstin kantaman informaation selvittäminen edellyttää optisten apuvälineiden käyttämistä puhumattakaan mikrofilmillä olevasta tekstistä – missä vaiheessa data muuttuisi niin pieneksi, että enää ei olisi kysymys asiakirjasta? Tietokonelevykkeen rautahiukkaset saadaan tehokasta elektronimikroskooppia käyttäen näkyviin niin selvästi, että niiden järjestys on luettavissa, ja tuolloin systeemin tuntevan lukijan on mahdollista myös selvittää niiden kantama informaatio.

Käytännön kannanottoja

Vaikka olen edellä pyrkinyt osoittamaan tietoteknisen tallenteen kelvanneen asiakirjaksi siinä kuin perinteisen paperiasiakirjankin ja paljolti vain näennäisten ongelmien olleen ratkaistavissa tulkintateitse, ei näin käytännössä tapahtunut. Totta on, että rikosoikeudessa analogiapäättely on johdantoluvussa tarkemmin esitetyin tavoin katsottu kielletyksi,[97] ja laventavaankin tulkintaan ainakin

---

[96] ”CD-levystä” puhuminen on hieman huonoa kielenkäyttöä sillä kysymyksessähän on itse asiassa ”Compact Disc -levy” eli ”kompakti levy -levy”. Koska ilmaisu ”CD-levy” on kuitenkin täysin yleiseen kielenkäyttöön vakiintunut, en ole sitä tässä korvannut ilmaisulla ”C-levy”.

[97] Ks. Frände, Straffrätt, s. 50 ss. ja Aarnio, s. 246 s.

syylliseksi epäillylle epäedullisella tavalla on suhtauduttu tietyllä varovaisuudella mutta näinkin vanhan lainsäädännön ollessa kysymyksessä olen sitä mieltä, että seuraava korkeimman oikeuden kannanotto on ellei suorastaan virheellinen niin ainakin perustellusti kritisoitavissa:

> KKO 1985 II 60: Yhtiön luottopäällikkö oli antanut syöttää kirjanpitoa suorittavalle tietokoneelle erästä yhtiön asiakasta koskevan väärän tilimerkinnän. Koska *tietokoneen muistiin sähköisesti, magneettisesti tai muulla tavoin näkymättömään muotoon taltioidut tiedostot eivät ole RL 36 luvun 5 pykälässä tarkoitettuja asiakirjoja* (kursivointi tässä), teko ei toteuttanut yksityisen asiakirjan väärentämistä. Sitä vastoin luottopäällikkö, joka oli tietojenkäsittelyjärjestelmää välikappaleenaan käyttäen erehdyttänyt yhtiön sekä myöntämään tavaraluottoa että luovuttamaan tavaraa tuolle asiakkaalle, tuomittiin petoksesta. (Ään.)

Tapausselosteen sanamuodon mukaan korkein oikeus on pitänyt *asiakirjan kriteerinä* sitä, onko tiedosto tallennettu näkyvään vai näkymättömään muotoon. Epäselväksi jää, mihin korkein oikeus on asettanut näkyvän ja näkymättömän välisen rajan ja millaisten kriteerien avulla rajaa ylipäänsä on pyritty määrittelemään. Uskallan epäillä, että itse asiassa näkyvän ja näkymättömän välisen rajan sijainnista ei juurikaan ole keskusteltu.

Myös korkein hallinto-oikeus oli muutamaa vuotta aikaisemmin asettunut suppean tulkinnan kannalle:

> KHO 1981 II 1: Automaattista tietojenkäsittelyä varten laadittu magneettinauhalla oleva tiedosto ei ollut yleisten asiakirjain julkisuudesta annetun lain 2 pykälän 1 momentissa tarkoitettu yleinen asiakirja, josta voitiin antaa jäljennös tai ote. Kun tällaisestakin tiedostosta oli mahdollista eräin edellytyksin antaa tietoja verotuslain 132 pykälän 5 ja 6 momentin nojalla verohallituksen luvalla, asia palautettiin verohallitukselle.

Tässä ratkaisussa ei ole edellä mainitun korkeimman oikeuden päätöksessä selostetuin tavoin otettu kantaa datan kokoon ja luettavuuteen. Yleisten asiakirjain julkisuudesta annetun lain 1.1.1988 voimaan tulleella muutoksella rinnastettiin tekniset tallenteet asiakirjoihin.[98] Sama lopputulos olisi epäilemättä ollut saavutettavissa laajentavalla tulkinnalla (jonka käyttö ei tässä nimenomaisessa hallintolainkäyttöön liittyneessä tapauksessa olisi edes ollut sillä tavoin rajoitettua kuin rikosoikeudessa).

---

[98] AsiakJulkL 22§ (30.4.1987/472): Mitä tässä laissa säädetään yleisestä asiakirjasta, koskee myös viranomaisen laatimaa ja antamaa sekä sille lähetettyä tai annettua lävistämällä, magnetoimalla tai muulla näihin verrattavalla tavalla aikaansaatua tallennetta, joka on tarkoitettu luettavaksi, kuunneltavaksi tai muutoin ymmärrettäväksi teknisin apuvälinein ja joka on viranomaisen hallussa (tekninen tallenne).

Eräissä maissa on tulkinnan mahdollisuuksiin suhtauduttu toisin.[99] Ruotsissa voimassa olevan väärennysrikos-säännöksen (BrB 14:1) käsitettä ”urkund” on myös tulkittu laajasti. Ratkaisussa NJA 1987 B 8 Högsta Domstolen katsoi tiettyä maksuinformaatiota sisältänyttä magneettinauhaa voitavan pitää asiakirjana.[100]

Laki yleisten asiakirjain julkisuudesta on nyttemmin kumottu 1.12.1999 voimaan tulleella lailla viranomaisten toiminnan julkisuudesta (621/1999), jonka 5 §:ssä on mielenkiintoinen asiakirjan määritelmä:

> *Asiakirjalla* tarkoitetaan tässä laissa kirjallisen ja kuvallisen esityksen lisäksi sellaista käyttönsä vuoksi yhteen kuuluviksi tarkoitetuista merkeistä muodostuvaa tiettyä kohdetta tai asiaa koskevaa viestiä, joka on saatavissa selville vain automaattisen tietojenkäsittelyn tai äänen- ja kuvantoistolaitteiden taikka muiden apuvälineiden avulla.

Määritelmä on sikäli onnistunut, että se ei puhu näkyvästä ja näkymättömästä vaan hyväksyy asiakirjoiksi kaikki sellaiset tallenteet, joiden sisältö on selvitettävissä, joko apuvälineitä käyttämällä tai niitä ilman.

Honkasalo ja asiakirja

Edellä lausutun jälkeen on mielenkiintoista lukea, mitä *Honkasalo* on kirjoittanut väärennysrikoksen teko-objektiksi kelpaavasta asiakirjasta (kursivoinnit tässä):[101]

> Laissa ei ole kuitenkaan käsitettä määritelty, vaan lainsäätäjä on jättänyt kysymyksen lainkäyttäjän ratkaistavaksi. Yleisestä oikeuskäsityksestä, vaikkei siltä voidakaan evätä kaikkea merkitystä tässäkään suhteessa, ei voida riittävää ohjetta saada, joten pakostakin on turvauduttava rikosoikeustieteelliseen erittelyyn – – . Tieteisopissa lähdetään yleisesti siitä, että objektin ollakseen asiakirja tulee ilmaista jokin ajatus. Ajatuksen ilmaiseminen tapahtuu yleisimmin käytännössä olevin kirjoitusmerkein, mutta se voi tapahtua myös pikakirjoitusmerkein, *vieläpä salakirjoitus-*

---

[99] Näin esimerkiksi Alankomaissa, Israelissa, Itävallassa ja Ranskassa. Ks. Sieber, COMCRIME-Study, III.B.4.

[100] Ruotsissakin on ehdotettu uutta määritelmän sisältävää väärennysrikossäännöstä (BrB 14:1, ks. SOU 1992:110 s. 22 s.): ”Den som, genom att skriva annan, verklig eller diktad, persons namn eller genom att falskeligen förskaffa sig annans underskrift eller annorledes, framställer falskt dokument eller falskeligen ändrar eller utfyller äkta dokument, döms, om åtgärden innebär fara för bevishänseende för dokumentförfalskning till fängelse i högst två år. (1 mom.) Med dokument avses i detta kapitel en skriftlig originalhandling eller en bestämd mängd data för automatisk informationsbehandling, om det är möjligt att fastställa att innehållet härrör från den som framstår som utställare. Som dokument anses också legitimationskort, biljett och dylikt bevismärke. (2 mom.)”

[101] Honkasalo, Erityinen osa II, s. 181 ss.

> *merkein, jos viimeksi mainitut merkit ovat, vaikkeikään yleisesti, jonkin henkilöryhmän tunnettavissa ja tulkittavissa.* – –
>
> Asiakirjaan kuuluu välttämättömästi alusta, jossa ajatus on ilmaistu. *Yhdentekevää on, mitä ainetta alusta on.* Tavallisimmin se on paperia, mutta alustana tulevat myös esim. pergamentti, nahka, kangas, puu tai kivi kysymykseen. Edellytyksenä kuitenkin on, että *ajatus on alustaan kiinteästi yhdistetty.* – – Kiinteän yhdistämisen kautta alustaan on ajatukselle annettu määrätynlainen pysyvyys.
>
> Jokainen kiinteästi alustaan yhdistetty pysyväksi tarkoitettu ajatus ei kuitenkaan ole asiakirja. Siihen vaaditaan lisäksi, että *sitä voidaan käyttää todistuksena oikeuselämässä.* Välttämätöntä ei ole, että se yksinään käy täydestä todistuksesta, kunhan se vain, vaikkapa yhdessä muiden tosiasiain kanssa, vaikuttaa vakaumuksen syntymiseen.

Honkasalo ei siteerattua tekstiä kirjoittaessaan tietenkään ole pohtinut tietoteknisen tallenteen suhdetta asiakirjaan, joten hänen mielipiteistään ei ole mahdollista tehdä suoranaisia johtopäätöksiä. Jos kuitenkin tutkitaan tallenteen asiakirja-ominaisuutta *Honkasalon* esittämien kriteerien pohjalta, on hyvin lähellä ajatus, että tietoväline, jolle kiinnitetty data kantaa jotakin todistuksena merkityksellistä informaatiota, on asiakirja.[102]

Todistuskappale

Rikoslain 33 luvun 6 §:n määritelmäsäännöksellä on pyritty ratkaisemaan aikaisempaa lakia sovellettaessa ilmenneet tulkintaongelmat, kun *automaattiseen tietojenkäsittelyyn soveltuva tallenne* on nimenomaisesti mainittu yhtenä väärennyksen teko-objekteista. *Tallenteen* käsitettä on jo selvitetty edellä osan I jaksossa 1.2.2.5.

Määritelmäsäännöksen perustelujen[103] mukaan todistuskappaleen määritelmä on tarkoitettu tyhjentäväksi; jos tietotekniikan kehittyessä otetaan käyttöön uudentyyppisiä tiedontallennuksen muotoja, on todistuskappaleen määritelmää tarkistettava. Automaattiseen tietojenkäsittelyyn soveltuvilla tallenteilla tarkoitetaan perustelujen mukaan konekielisiä tallenteita, jotka on saatu aikaan lävistämällä, magnetoimalla, erilaisin optisin keinoin tai muilla teknisillä menetelmillä. Tieto on niissä tallennettu näkymättömään muotoon nauhalle, rummulle, levylle, kasetille tai muulle vastaavalle tietovälineelle. Tarvittaessa se voidaan tulostaa selväkieliseksi esimerkiksi paperille, näyttöpäätteelle tai mikrofilmille.[104]

Todistuskappaleen määritelmä on jo ehtinyt osoittautua käytännössä riittämättömäksi:

---

[102] Ks. myös Anttila-Heinonen, s. 37: ”Asiakirja on tavallisesti paperialustalla oleva kirjoitusteksti, josta allekirjoituksesta tai asiayhteydestä ilmenee asiakirjan antaja. Alustan ei välttämättä tarvitse olla paperia. Asiakirjan sisältämä ajatus tai selitys voi olla ilmaistu tavallisesta kielenkäytöstä poikkeavastikin. Asiakirjan antajan ei tarvitse olla nimenomaisesti ilmaistu asiakirjassa. Jos asiakirjan antaja ei selviä asiayhteydestäkään, ei asiakirjalla ole merkitystä todistuskappaleena. Tällöin asiakirja ei ole kelvollinen myöskään väärennyksen teko-objektiksi.”

[103] HE 66/1988, s. 117 ss.

[104] Ks. myös Nuotio, Rikosoikeus, s. 1099.

> Helsingin kaupunginviskaali jätti loppukesästä 1996 perusteella ”ei rikos” -syytteen nostamatta sellaisia väärennyksestä epäiltyjä vastaan, jotka olivat valmistaneet puhelukortteja muistuttavia niin sanottuja sirukortteja. Kortteihin sisällytetty prosessori oli konstruoitu niin, että se ensinnäkin erehdytti puhelinkojeen tunnistamaan kortissa olevan puheaikaa jäljellä sadan markan arvosta. Edelleen puhelinkoje luuli, että soitettaessa kului kortille muka ladattua rahaa puheluaikaa vastaavasti, mutta käyttäjän poistaessa kortin kojeesta olikin jäljellä oleva saldo edelleen alkuperäiset sata markkaa. Syyttäjän mukaan tällainen kortti ei voinut olla ”automaattiseen tietojenkäsittelyyn soveltuva tallenne”. Tämän ja muiden vastaavanlaisten tapausten seurauksena rikoslakia muutettiin – ei tosin todistuskappaleen vaan maksuvälineen määritelmän osalta. Mainittakoon kuitenkin, että käytäntö tällaisten väärien puhelukorttien osalta oli ollut horjuvaa; esimerkiksi Tampereella oli vastaavanlaisesta teosta syytetty ja tuomittu väärennyssäännöksen perusteella.[105]

Itse olisin vaikeuksitta tamperelaisen linjan mukaisesti saanut edellä tarkoitetun sirukortin mahtumaan esittämäni tallenteen käsitteen piiriin. Prosessorissa, joka itse asiassa on pieni tietojärjestelmä, oli tietovälineelle kiinnitettyä dataa, joka puolestaan edusti informaatiota siitä, että puheluaikaa on olemassa. Kortti on ollut väärä, koska se käytettäessä on käyttäytynyt kojeeseen päin samalla tavoin kuin oikea, kortin antamiseen oikeutetun antama kortti.

Puheena oleva tallenteen käsite ei kuitenkaan toistaiseksi tuottane suurempia vaikeuksia käytännön lainsoveltamisessa. Perusteluissa kiinnittää kuitenkin huomiota se, että – edellä käsitellyn korkeimman oikeuden ratkaisun tapaan – niissäkin puhutaan ”näkymättömään muotoon” tallennetusta tiedosta pyrkimättäkään mitenkään konkretisoimaan näkyvän ja näkymättömän välistä rajaa. Tosiasiallisesti ei rajanvedon ongelmallisuudella enää ole merkitystä määritelmän kattaessa niin ”näkyvät” kuin ”näkymättömätkin” todistuskappaleet, mutta periaatteelliselta kannalta asiaa tarkastellen ei tällaisilla tulkinnanvaraisilla käsitteillä operoimista voi varauksitta hyväksyä.

Vääryysominaisuus

Jos itse todistuskappaleen määritelmä ei suurempia tulkintaongelmia aiheutakaan, saattaa niitä syntyä määritelmäsäännöksen sisältämästä vääryysominaisuuden määrittelystä. Kun säännöksen mukaan todistuskappale on väärä, milloin se on todisteena käytettäessä omiaan antamaan erehdyttävän kuvan alkupe-

---

[105] Tampereen käräjäoikeuden 42. osaston tuomio 5.2.1997 dnro R 96/2865. Tekijä oli paitsi käyttänyt tällaisia väärennettyjä kortteja myös hankkinut käyttämisellä hyvät ansiot: hän oli avannut palvelupuhelinnumeron, johon soittamisesta hänelle koitui tuloja 13,60 markan minuuttitaksan mukaan, ja kun soitot tehtiin väärennetyillä korteilla, ei soittajalta rahaa kulunut. Kaiken kaikkiaan tuloja kertyi 35 000 markkaa ja menettelystä rangaistiin yhdeksän kuukauden ehdollisella vankeusrangaistuksella. Syyksiluetut rikokset olivat väärennys ja törkeä petos. Vastaaja oli myöntänyt syyllisyytensä eikä käräjäoikeuden tuomiosta valitettu.

rästään tai antajansa henkilöllisyydestä, jää tässä suhteessa varsinkin tietoteknisten tallenteiden osalta harkinnanvaraisuutta.

Säännöksen perustelujen mukaan[106] automaattisen tietojenkäsittelyn kautta syntyneellä tulosteella ei useinkaan ole muuta antajaa kuin se tietojenkäsittelytapahtuma, jonka avulla tuloste on saatu aikaan. Riippuu tilanteesta ja mahdollisesti erikseen annetuista määräyksistä, miten tarkasti tällaisen tulosteen alkuperätiedot (esimerkiksi päiväys, ajo ja ohjelmointi) on yksilöitävä, jotta tallenne saisi todistusarvoa ja jotta sitä voitaisiin pitää säännöksessä tarkoitettuna todistuskappaleena. Jos alkuperätiedot ovat omiaan antamaan tallenteen syntyhistoriasta erehdyttävän kuvan, tallennetta on pidettävä vääränä todistuskappaleena.[107]

Perusteluissa on täydellisesti sekoitettu keskenään käsitteet *tallenne* ja *tuloste,* mistä on ollut seurauksena selvää epäjohdonmukaisuutta. Todistuskappaleen määritelmän mukaan *todistuskappaleena pidetään tallennetta,* ei tallenteesta tehtyä tulostetta. Tällainen tuloste paperille tai jopa monitorille tehtynä toki saattaa myös olla todistuskappale (jos esimerkiksi tekstinkäsittelyohjelmalla laadittu kauppakirja, joka on tallennettu Word-tiedostoksi kauppakirja.doc, tulostetaan ja asianmukaisesti allekirjoitetaan), mutta se ei silloin ole enää automaattiseen tietojenkäsittelyyn soveltuva tallenne vaan – ainakin useimmiten – asiakirja. Entäpä jos kauppakirja on olemassa ainoastaan digitaalisesti allekirjoitettuna tiedostona, jota ei ole tarkoituskaan tulostaa kuin ehkä hetkittäin näytölle?

Tulosteen perusteella on kylläkin joskus mahdollista asettaa tallenteen oikeaperäisyys kysymyksenalaiseksi ja tulosteesta voi joskus olla suurellakin todennäköisyydellä pääteltävissä, että tallenne on väärä, mutta koska näin ei voi aina olla, on todistuskappaleeksi kelvollisen tallenteen mahdollinen vääryys voitava löytää tallenteesta itsestään – niin kuin edellä mainitussa ruotsalaisessa säännösehdotuksessa lausutaan, ”om det är möjligt att fastställa att innehållet härrör från den som framstår som utställare”.[108]

---

[106] HE 66/1988, s. 120.

[107] Nuotio (Rikosoikeus, s. 1101 ss.) käsittelee vääryysominaisuutta lähinnä hallituksen esityksen pohjalta eikä erityisesti ota erikseen huomioon tietoteknisiä tallenteita väärennyksen objekteina. Nuotio kirjoittaa seuraavasti: ”Esimerkiksi atk-tulosteen todistusarvo voi olla olennaisesti kiinni siitä, millaisia alkuperätietoja tulosteeseen tulostuu. Tulosteen todistusarvo määräytyy kuitenkin pitkälle tilannekohtaisesti. Tallenne on väärä todistuskappale, jos alkuperätiedot yleisesti ottaen antavat tallenteen synnystä erehdyttävän kuvan.” – Tässäkin on käsitykseni mukaan aiheettomasti sekoitettu toisiinsa tuloste ja tallenne. Todistuskappale on nimenomaan tallenne, tuloste on ainoastaan tallenteen visuaalinen esitys.

[108] Ks. SOU 1992:110, s. 258 ss., jossa todetaan mm. seuraavaa: ”Vid automatiska uppteckningar går det knappast att finna någon annan utställare än själva maskinen. Manipulationerna består därvid i att materialiseringarna oriktigt framstår som fullständigt framställda av en viss typ av apparat. Det är inte naturligt att då tala om en person som utställare. Kravet på att en utställare skall finnas angiven kan när det gäller utdata möjligen anses uppfyllt genom att den fysiska eller juridiska person eller den myndighet som står som garant för t.ex. en utskrift finns angiven i denna eller genom att ursprunget är allmänt känt. I detta sammanhang kan erinras exempelvis om ADB-framställda gravationsbevis eller kontoutdrag från en bank avseende ett motbokslöst konto.”

Kotimaisia mielipiteitä

Lehtimajan näkemyksen mukaan tietokoneen tuottaman tallenteen aitouden kriteeri on se, onko tallenne syntynyt laitteen normaalin toimintaprosessin tuloksena ilman laitteeseen kohdistettua manipulointia.[109] Periaatteessa näin varmasti on, mutta lausuma kaipaisi selvennystä ainakin siltä osin, mitä tarkoitetaan ”tietokoneen tuottamalla tallenteella”; tallennehan on kuitenkin alun perin jonkun ihmisen tuottaman ajatuksen – informaation – ja sitä kantavan tietovälineelle kiinnitetyn datan muodostama kokonaisuus, jota tietokone ei sellaisenaan voi tuottaa, vaikka koneet nykyään jo kovin ”älykkäitä” ovatkin.

On muistettava, että mitä kehittyneinkin tietokone on vain laskin, joka ei (onneksi) kykene itsenäiseen ajatteluun vaan toimii ihmisen sille laatimien ja siihen asentamien ohjeiden eli ohjelmien ja ohjelmakäskyjen perusteella, jotka voivat toimia vasta ihmisen kytkettyä virran tietokoneeseen ja käynnistettyä ohjelman. Usein nämä ohjelmat toki tekevät hyvin pitkälle automatisoituja toimia, mikä helposti saattaa antaa sen kuvan, että ne tekisivät niitä ”itse” – puhutaan esimerkiksi koneiden välisestä viestinnästä, jollaista tosiasiassa ei kuitenkaan ole olemassa.

Lisäksi *Lehtimajan* näkemys on rajoittunut sikäli, että manipuloinnin kohteena ei suinkaan aina välttämättä ole laite – ainakin sanan käyttäminen johtaa ajatukset helposti yksittäiseen tietokoneeseen ja siihen kohdistuneeseen menettelyyn. Tekijä saattaa päästä käsiksi tallenteeseen modeemia ja puhelinlinjoja käyttämällä ja kieltämättä lopuksi yleensä tavallaan operoi tallenteen sisältävällä koneella, mutta nykyaikaista terminologiaa vastaisi ehkä paremmin tietojärjestelmästä kuin laitteesta puhuminen.[110]

Lahti katsoo edellä käsiteltyä korkeimman oikeuden ratkaisua 1985 II 60 kommentoidessaan, että tapauksessa ei siinä tarkoitetun tulosteen eikä sitä vastaavan tallenteen alkuperän oikeellisuuden loukkaamiseen riitä se, että niiden perustana olevat tietokoneeseen syötetyt tilitiedot ovat virheellisiä,[111] ja näin sanoessaan tekee siis eron tallenteen ja tulos-teen välille.

Rautio näkemys on, että määritelmäsäännöksenkin sanamuodon valossa on ratkaisevaa se, missä määrin tallenteen ja siten myös siitä tehdyn tulosteen voi katsoa syntyneen siten kuin asianmukainen tietojenkäsittely edellyttää eli ilman ulkopuolista manipulointia.[112]

---

[109] Lehtimaja, Taloudellinen rikollisuus, s. 131.

[110] Tässäkin yhteydessä näkyy selvästi, miten aikaisemmin eli vielä 1980-luvun loppupuolella terminologia liittyi hyvin läheisesti tietokoneeseen: puhuttiin tietokonerikoksista. Viime aikoina tietojenkäsittelyn monimuotoistuessa pääpaino terminologiassa on siirtynyt informaatiotekniikkaan ja tietojärjestelmiin ja nykyaikana jo kyberavaruuteen, cyber-spaceen. Tietojärjestelmän käsite puolestaan on nykyään hyvin laaja ja käsittää toisaalta yksittäiset tietokoneet, toisaalta koko Internetin.

[111] Lahti, LM 91, s. 1172.

[112] Rautio, s. 5 s.

Ulkomaisia näkemyksiä

Jareborg toteaa Ruotsin väärennysrikossäännöstä käsitellessään[113] ratkaisevan kysymyksen olevan, voidaanko tallennetta tai dataa koskaan katsoa dokumentiksi, koska ei ole olemassa mitään sellaista aineellista, joka muodostaisi itsenäiseksi ymmärrettävän yksikön ja joka olisi luonnehdittavissa originaaliksi. Vaikka tallenteen alkuperäinen tekijä ja alkuperäinen sisältö pystyttäisiin identifioimaan, ei tallenteen fyysistä kuvausta voida yksilöidä niin, että voitaisiin puhua alkuperäisestä ja kopioista. Ei voi olla olemassa yhtä uniikkia kuvausta, ainoastaan lukematon määrä saman sisällön kuvauksia.

Jareborgin näkemys on kiinteästi sidoksissa ruotsalaiseen, jo aikaisemmin kuvailtuun datan kvasimateriaalista luonnetta koskevaan käsitykseen, joka merkitsee sen tosiasian jättämistä vaille huomiota, että jokaista tallennettua informaatiota edustaa selkeästi materiaalinen data.

Silvander tuntuu olevan hieman Jareborgin näkemyksestä poikkeavalla kannalla. Hän kirjoittaa seuraavasti:[114]

> Den lagrade informationen finns ju tillgänglig oberoende av hur denna för tillfälligt är lagrad. Även om data lagrats på ett systematiskt sätt, kan en fysisk person i regel ändå inte uppfatta den lagrade informationen. Då konvertering sker till visuellt läsbar text, kommer den lagrade informationen att presenteras på ett systematiskt sätt.
>
> I samband med att upptagningen konverteras till en traditionell urkund, finns det två upplagor av urkunden, den upplaga som finns lagrad i datorn och den som konverterats. En fråga som kan ställas är: Vilken av dessa är original och vilken är kopia? Enligt min åsikt är det den urkund som upprättas direkt via datorn som är att betrakta som original. Man kan i sådant fall betrakta datorn som en avancerad skrivmaskin.

Silvander päätyy lopulta toteamaan, että ”man inte utan vidare kan utmönstra en upptagning som urkund”.

Möhrenschlager näkee välittömän tunnistettavuuden dokumentti-käsitteen olennaiseksi elementiksi.[115] Hänen mukaansa se tosiasia, että sisältö on luettavissa tietokoneen näytöltä, ei merkitse muuta kuin uusia teknisiä mahdollisuuksia sisällön selvittämiseen. ”That the processing operation produces computer print-outs regardable as (forged) documents, is of no further assistance where data relevant in evidence are used direct from the computer or on data carrier for further automatic processing”, kirjoittaa Möhrenschlager eikä siis ilmeisesti näe kysymystä tallenteen vääryysominaisuuden arvioimisesta erityisen keskeisenä.

---

[113] Jareborg, RIDP 1–2/93, s. 589.
[114] Silvander, s. 362 s.
[115] Möhrenschlager, s. 343.

Ruotsissa *Datastraffrättsutredningen* on mietinnössään varsin perusteellisesti käsitellyt väärennykseen liittyviä ongelmia mukaan lukien kysymys asiakirjan (urkund t. dokument) vääryysominaisuudesta.[116]

Aito vai väärä, oikea vai väärennetty

Mietinnössä tehdään – samaan tapaan kuin meilläkin – ero aitojen (äkta) ja oikeiden (sanna) asiakirjojen välillä. Aidon vastakohtana on väärä (falsk) ja oikean vastakohtana väärennetty (osann).

Asiakirjan aitous tarkoittaa sitä, että asiakirja on peräisin siltä, joka on sen antajaksi ilmoitettu, kun taas se, että asiakirja on oikea, tarkoittaa asiakirjan sisällön oikeellisuutta suhteessa todellisuuteen. Tästä seuraa, että asiakirja voi olla aito ja oikea, aito ja väärennetty, väärä ja oikea tai väärä ja väärennetty. Tavallisin väärinkäsitys mainittujen termien suhteen on, että käsitteet väärä ja väärennetty sekoitetaan keskenään.

Tietoteknisessä ympäristössä todetaan perinteisen asiakirja-käsitteen saavan uusia ulottuvuuksia. Tällöin muun ohessa aitouden tutkiminen vaikeutuu. Tietoteknisestä tallenteesta useimmiten puuttuvat sellaiset allekirjoitukseen rinnastettavat ulkoiset tunnusmerkit, jotka osoittaisivat tallenteen aitoutta. Dataan tehdyt muutokset eivät ole lukijan nähtävissä paperitulosteessa tai näyttöpäätteellä. Datan aitouden kontrolloimisessa on pääpiirteissään olemassa kaksi eri tapaa: yleiset turvallisuustoimenpiteet ja tietotekniset menetelmät.

Käsitykseni mukaan kysymys tallenteen oikeaperäisyyden – aitouden – loukkaamisesta ei voi ratketa mitenkään kategorisesti tyytymällä ylimalkaiseen vaatimukseen ulkopuolisesta manipuloinnista. Tallenteen oikeaperäisyydellä ei voida tarkoittaa samaa kuin tulosteen oikeaperäisyydellä: tulosteen antaja on useimmiten – niin kuin määritelmäsäännöksen perusteluissa edellä kuvatuin tavoin on todettu – tietty tietojenkäsittelytapahtuma (joka tosin sekin tapahtuu ihmisen tahdosta ja toimenpitein), mutta itse tallenne – todistuskappale – on välittömästi peräisin joltakulta ihmiseltä ja sisältää tämän ihmisen luoman ajatuksen.

Jotta tällainen tallenne olisi lainkohdan tarkoittamassa mielessä '*väärä,*' tulisi sen olla omiaan antamaan erehdyttävä kuva alkuperästään tai antajansa henkilöllisyydestä, ja tämä vääryysominaisuus olisi kyettävä selvittämään itse tallenteesta. Tällainen selvittäminen, sikäli kuin se ylipäänsä on mahdollista, edellyttää tietoteknistä erityistietämystä. Huomattakoon kuitenkin, että esimerkiksi poliisin käytössä olevilla menetelmillä on niin tietojärjestelmistä kuin tietokoneistakin mahdollista saada selville hämmästyttävän paljon sellaista tietoa, jonka olemassaolo tai löytyminen on maallikolle täysin epäuskottavaa.

---

[116] SOU 1992:110, s. 229 ss.

Tallenteen laatijaa tai laatimis- tai muuttamisajankohtaa selvitettäessä rikostutkinnan keinot ovat melkoisen edistyneitä.

Euroopan neuvoston tietoteknistä väärennystä koskevan minimilistan suosituksen[117] sanamuodosta ei saada apua vääryysominaisuuden arviointiin, sillä suosituksessa ei puututa itse väärennysrikoksen tunnusmerkkeihin.[118] Perusteluissa kylläkin todetaan muun muassa, että ”as far as visible computer print-outs are concerned there are additional problems as to whether they can be considered as forged documents if their content is essentially determined by the manipulated data processing computer. Furthermore, the question may arise whether the print-out is a false document or just a genuine one containing incorrect statements of facts, a distinction which may play role in several countries.”[119]

Tallenne ja tuloste

Lainauksessa korostuu jälleen se edellä käsitelty ero, joka käsitykseni mukaan on tehtävä tallenteen ja siitä tehdyn tulosteen välille. Jos tallennetta on manipuloitu niin, että menettely konstituoi tallenteeseen kohdistuneen väärennysrikoksen, miten on suhtauduttava manipuloidusta tallenteesta tehtyyn tulosteeseen, jota käytetään tai voidaan käyttää oikeudellisesti merkityksellisenä todisteena?

On mahdollista ajatella, että tulostamisprosessin seurauksena syntyvä asiakirja *ei välttämättä olekaan väärä todistuskappale* vaan ”just a genuine one containing incorrect statements of facts”, vaikka sen kantama informaatio ei sisällöltään vastaisikaan tallenteen tuottajan alkuperäistä ajatusta tai vaikka se antaisi tallenteen alkuperästä erheellisen kuvan.

Kirjaimellisesti rikoslakia lukien voisikin päätyä sellaiseen johtopäätökseen, että jos tällaista *tulostetta* käyttää joku muu kuin *tallenteen* väärentäjä, hän ei voisikaan syyllistyä rikoslain 33 luvussa kriminalisoituun menettelyyn, vaan

---

[117] Datan tai ohjelmiston syöttäminen, muuttaminen, hävittäminen tai käytön estäminen taikka muu tietojenkäsittelyyn puuttuminen sellaisella tavalla ja sellaisissa olosuhteissa, että tekoa kansallisen lainsäädännön nojalla olisi pidettävä väärennysrikoksena, jos sen kohteena olisi ollut väärennysrikoksen perinteinen teko-objekti (”asiakirja” tms.).

[118] Ehdotuksen tarkoituksesta todetaan sen perusteluissa (EN:n raportti 89, s. 29 ss.) mm. seuraavaa: ”The proposal’s aim is to put the falsification of data having probative force on the same footing as the forgery of documents or other instruments in crminal law terms. Extension of protection is only necessary in those states that demand direct perceptibility of the content of the data and of the maker in regard to forgery of documents.” Ks. myös s. 30: ”... the question may be left open as to whether a forgery of a document and a falsification of evidentiary data only take place where there is a deception as to authenticity, i.e. as to the maker – in other words whether it is a matter of a document’s telling a lie about itself as a document or whether falsifications of the content of the statements made therein, their correctness and verasity are also covered. The text merely requires the new possibilities of manipulation to be criminalised under national law in the same way as traditional forgery of documents.”

[119] EN:n raportti 89, s. 29.

hänen toimintansa tulisi arvioida esimerkiksi pelkän petossäännösten perusteella. Tällaisesta tulkinnasta seuraisi myös, että jos käyttäjänä on tallenteen väärentäjä, olisi hän mahdollisen *tulostetta* käyttämällä suorittamansa petosrikoksen ohella syyllistynyt nimenomaan *tallenteeseen* kohdistuneeseen väärennysrikokseen.

Tällainen tulkinta ei kuitenkaan välttämättä olisi käytännön kannalta järkevää eikä ilmeisesti vastaisi yleistä oikeustajuakaan. Tietokonetta käytetään nykyään tekstin luomiseen aivan kirjoituskoneeseen rinnastettavalla tavalla eikä se, että teksti saattaa välillä olla pitkiäkin aikoja tallennettuna jollakin tietovälineellä, muuta tätä tekstin tuottamisen tosiasiallista luonnetta.

Rikoslain 33 luvun 6 §:n mukaan väärentäminen tarkoittaa todistuskappaleen sisällön oikeudetonta muuttamista. Tietoteknisen tallenteen väärentäminen tarkoittaa niin muodoin sellaista tietovälineelle kiinnitettyyn dataan kohdistuvaa menettelyä, että datan kantama informaatio ei manipuloinnin jälkeen enää vastaa antajansa ajatusta. Jotta kysymyksessä olisi nimenomaan väärennysrikos, on tekijältä edellytettävä informaation muuttamista tarkoittavaa tahallisuutta; tällaisen tahallisuuden puuttuessa voi tosiasiallisesti informaation muuttumisen aiheuttanut toimenpide tulla arvioitavaksi esimerkiksi luvatonta käyttöä tai vahingontekoa koskevien säännösten perusteella.[120]

Tekotavat

Väärennyksen – sen paremmin perinteisen kuin tietoteknisenkään väärennyksen – mahdollisia tekotapoja ei asianomaisissa rikoslain säännöksissä mainita. Tietoteknisen väärennyksen tekotapoina tulevat kysymykseen ainakin Euroopan neuvoston suosituksessa mainitut datan tai ohjelmiston syöttäminen, muuttaminen, hävittäminen tai käytön estäminen, kun tekijän tarkoituksena on informaation muuttaminen; myös muu tietojenkäsittelyyn puuttuminen mainitaan mahdollisena *modus operandina,* joten suosituksen tunnusmerkistö on tässä suhteessa avoin. Myös kaikki suosituksessa mainitut tekotavat voivat toteuttaa

---

[120] Esimerkkinä tyylipuhtaasta tietoteknisestä väärennysrikoksesta on erään yrityksen menettely Houstonissa, Texasissa vuonna 1985. Yritys otti hyvästä hinnasta hankkiakseen edullisia lainoja henkilöille, jotka eivät olleet erityisen luottokelpoisia. Yrityksellä oli oikeudeton pääsy erään suurehkon pankin salaisiin tiedostoihin ja tätä pääsymahdollisuutta yritys hyödynsi kahdella eri tavalla. Ensimmäinen metodi oli poistaa pankin rekisteristä lainanhakijaa koskevat epäedulliset tiedot. Toisen metodin mukaan rekisteristä etsittiin nuhteeton henkilö, jonka henkilöllisyys oli sopiva lainanhakijalle. Tämä sai sitten ottaa toisen henkilön henkilöllisyyden nimeä, osoitetta ja perhesuhteita myöten ja saattoi tässä uudessa identiteetissään saada lainaa tai luottokortin. Ks. Wranghult, s. 15 s. – Menettelytapoja rikosoikeudellisesti arvioitaessa erityisesti ensimmäinen metodi olisi suomalaisenkin lain mukaan selkeä väärennysrikos: tietojenkäsittelyyn soveltuvaa tallennetta (pankin rekisteriä) on väärennetty (dataa muutettu) tarkoituksena käyttää sitä harhauttavana todisteena. Molemmat metodit toteuttavat myös tietomurron ja luvattoman käytön tunnusmerkistön, minkä lisäksi teot ovat arvioitavissa myös tietojenkäsittelypetosta koskevan tunnusmerkistön valossa.

jonkin muun tietotekniikkarikoksen tunnusmerkistön, eikä rajanveto näiden ja väärennyksen välillä suinkaan ole ongelmatonta. Kysymykseen palataan jäljempänä.

Euroopan neuvoston säännössuosituksella ei ole tarkoitettu laajentaa väärennyssäännöksillä aikaisemmin suojattujen oikeudellisten intressien piiriä, vaan ne pysyvät ennallaan: sellaisten todistuskappaleiden (documents and other instruments) varmuus ja luotettavuus, joilla on merkitystä oikeudellisissa suhteissa, joskin teon luonteesta johtuen yhtenä uutena intressinä – tietotekniikkarikoksille yhteisenä – nousee esiin tietojenkäsittelyrauha, *pax computationis*.[121] Suomalaisessa lainuudistuksessa tarkoitus näyttää olleen periaatteessa sama: uusimuotoisille todistuskappaleille on annettava sama suoja kuin perinteisille asiakirjoille.[122]

Suomalaisessa lainuudistuksessa tietotekniikkarikosten kohdalla valittu menettelytapa eli perinteisiä rikoksia koskevien säännösten täydentäminen tietotekniset erityisvaatimukset huomioon ottavilla elementeillä saattaa joissakin tapauksissa johtaa keinotekoisiin konstruktioihin. Väärennyksen kohdalla näin ei – ainakaan useimmissa tilanteissa – ole. Suojeltavat intressit ovat samat, oli todistuskappale sitten tietotekninen tallenne, asiakirja tai muu määritelmäsäännöksessä mainittu, joskin lisäksi suojeluobjektina tulee kysymykseen paitsi tietojen luottamuksellisuus ja käytettävyys erityisesti tietojen eheys. Itse asiassa tietojen eheys ei käsitteenä ole kovinkaan etäällä asiakirjaväärennyksen yleisestä suojeluobjektista eli todistelun luotettavuudesta.

Vääryysominaisuuden arviointi tuottanee ongelmia varsinkin tallenteen oikeaperäisyyden joutuessa kiistanalaiseksi ja tässä suhteessa on erityisesti syytä muistaa, että tallenne ja siitä tehty tuloste ovat teknisesti täysin eri asioita ja siksi myös oikeudellisesti eri asemassa.

Oikeuskäytännössä ongelmat ovat keskittyneet lähinnä jo edellä mainituin tavoin todistuskappaleen käsitteen kattavuuteen. Tuomioistuimissa on väärennyksinä käsitelty paitsi puhelukorttien rakentamisia mm. tapauksia, joissa on ollut kysymys maksullisten satelliittitelevisiolähetysten maksuttoman katselemisen mahdollistavista piraattikorteista.

---

[121] EN:n raportti 89, s. 44 s., jossa mm. todetaan suojeltavien intressien osalta: ”The legal interest involved is the protection against unauthorised interference with the usability of computer data or programmes, thereby violating the interest of the person concerned in their continuing integrity.” Muilta osin viitataan vahingonteon kohdalla lausuttuun. – Huomattakoon, että väärennysrikoksen tunnusmerkistön voi sellaisenaan toteuttaa myös valinnaislistan datan tai ohjelmiston muuttamista koskevassa suosituksessa tarkoitettu menettely: ”Oikeudettomasti tapahtuva datan tai ohjelmiston muuttaminen.”

[122] Ks. HE 66/1988, s. 119: ”Tietotekniikan kehittämät uudet tiedontallennustavat täydentävät perinteistä asiakirjaviestintää ja yhä useammin jopa korvaavat sen. Niiden oikeudellinen sääntely on kuitenkin vielä puutteellista. Nauttimastaan todistusarvosta huolimatta uudentyyppiset tallenteet eivät saa rikosoikeudellista väärennyssuojaa. Tämän epäkohdan poistamiseksi nyt käsiteltävänä oleva määritelmäsäännös on laadittu koskemaan myös tällaisia tallenteita.”

Piraattikortit väärennyksen kohteina

Korkein oikeus antoi 27.6.2003 ennakkopäätöksen luonteisen ratkaisun piraattikorttien asemasta väärennyksen kohteena.[123] Otsikkoteksti on seuraavanlainen:

> A oli valmistanut älykortteja tallentamalla piirilevylle kiinnitettyyn mikropiiriin X Oy:n satelliittiteitse välittämien suojattujen televisiolähetysten katselemiseen tarvittavat tiedot. Älykorttia, jonka tarkoitus oli purkaa salaus vastaanottolaitteen vastaanottamasta lähetyksestä, ei voitu pitää sellaisena rikoslain 33 luvun 6 §:ssä tarkoitettuna todistuskappaleena, jota käytetään tai voidaan käyttää oikeudellisesti merkityksellisenä todisteena, joten syyte väärennyksestä hylättiin.

Ratkaisu ansaitsee tulla lähemmin tarkastelluksi, sillä mielestäni sitä kohtaan voidaan esittää perusteltua kritiikkiä.[124] Ratkaisu on tehty Rovaniemen hovioikeuden 12.6.2001 antamasta tuomiosta[125] tehdyn valituksen johdosta.

Hovioikeus oli katsonut, että lain sanamuoto ja lain valmisteluasiakirjat eivät selvästi osoita rikoslain 33 luvun 1 §:ssä säädetyllä todistuskappaleella tarkoitettavan syytteissä kuvattua automaattista tietojenkäsittelyä hyväksi käyttäen valmistettua älykorttia. Hovioikeuden mukaan rikosoikeudellinen laillisuusperiaate estää rikossäännöksen tulkitsemisen laajentavasti syytetyn vahingoksi. Hovioikeus viittasi lisäksi tuolloin eduskunnassa käsiteltävänä olleeseen hallituksen esitykseen 146/2000 laeiksi tietoyhteiskunnan palvelujen suojasta sekä rikoslain 38 luvun ja eräiden viestintälakien muuttamisesta ja sillä täytäntöön pantavaksi aiottuun 20.11.1998 annettuun direktiiviin ehdolliseen pääsyyn perustuvien tai ehdollisen pääsyn sisältävien palvelujen oikeussuojasta. Esityksessä ehdotettiin jäljempänä selostettavin tavoin säädettäväksi mm. suojauksen purkujärjestelmärikoksesta. Tekijät tuomittiin hovioikeudessa rangaistukseen vain radiolain rikkomisesta ja syytteet väärennysrikoksista hylättiin.

Korkeimman oikeuden ratkaisun perusteluissa viitataan lain esitöihin (HE 66/1988) ja todetaan niissä ensinnäkin lausutun (s. 109), että väärennysrikokset ovat luonteeltaan todistelurikoksia, jotka loukkaavat tai vaarantavat todistelutarkoituksessa tapahtuvan tiedonvälityksen luotettavuutta oikeuselämässä. Todistelulla tarkoitetaan tilanteita, joissa on kysymys tietyn tosiasian vahvistamisesta jonkin todistuskappaleen avulla. Puheena olevan hallituksen esityksen mukaan (s. 118 ja 119) todistuskappaleella tarkoitetaan esinettä, jota sille tallennetun tai siitä muutoin ilmenevän tiedon takia käytetään tai voidaan käyttää oikeudellisesti merkityksellisenä todisteena oikeuksista, velvollisuuksista ja tosiasioista.

---

123 KKO:2003:58.

124 Ks. tästä myös Pihlajamäki, Kommentti, jossa olen esittänyt saman kritiikin.

125 Tuomio nro 335. Asia oli ensiasteessa käsitelty Oulun käräjäoikeudessa, joka oli katsonut kysymyksessä olleen väärennysrikoksen.

Korkein oikeus tarkastelee syytteessä tarkoitetun älykortin toimintaa ja sen käyttötarkoitusta ja toteaa vastaanottolaitteiston tietokoneohjelmineen olevan tekninen kokonaisuus, jonka tehtävänä on vastaanottaa radiosignaaleja ja purkaa lähetyksen salaus ja joka ei ole yhteydessä lähetystoiminnan harjoittajaan. Vaikka vastaanottaja on voinut saada katseltavakseen ja kuunneltavakseen ohjelmia ilman lähetystoiminnan harjoittajan antamaa lupaa, ei hän kuitenkaan ole älykortin avulla erehdyttänyt lähetystoiminnan harjoittajaa. Älykortti ei vaikuta ohjelma lähettämiseen tai teknisen salausjärjestelmän toimintaan. Kysymys on vastaanottolaitteiston eri osien välisestä sähköisestä toiminnasta eikä siitä, että älykorttia käytettäisiin oikeudellisesti merkityksellisenä todisteena. Syytteessä tarkoitettuja älykortteja ei voida pitää rikoslain 33 luvun 6 §:ssä tarkoitettuina todistuskappaleina eikä A siis ole menettelyllään syyllistynyt väärennykseen. Ratkaisu oli yksimielinen.

Korkeimman oikeuden ratkaisun kiinnostavuutta lisää se, että runsas viikko Rovaniemen hovioikeuden tuomion antamisen jälkeen eli 21.6.2001 Turun hovioikeus antoi neljä tuomiota,[126] joissa se katsoi kysymyksessä olevan kaltaiset älykortit rikoslain 33 luvussa tarkoitetuiksi todistuskappaleiksi ja tuomitsi syytetyt väärennysrikoksista. Turun hovioikeuden perustelut eri tuomioissa ovat keskenään samankaltaiset ja niissä on katsottu älykorttien olleen automaattiseen tietojenkäsittelyyn soveltuvan tallenteen sisältäneitä kortteja, jotka ovat mahdollistaneet X Oy:n välittämien maksullisten televisiolähetysten katselemisen maksutta ja joita siten on voitu käyttää oikeudellisesti merkityksellisinä todisteina oikeudesta katsella kyseisiä lähetyksiä.

Omaa näkemystäni vastaavat Turun hovioikeuden ratkaisut saivat aikaan sen, että otin yhteyttä Eduskunnan liikenne- ja lakivaliokuntiin, minkä seurauksena hovioikeuden ratkaisujen antamishetkellä eduskuntakäsittelyn loppuvaiheessa ollut edellä mainittu hallituksen esitys 146/2000 otettiin vielä kertaalleen liikennevaliokunnan käsiteltäväksi ja ehdotettuun rikoslain 38 luvun 8 a §:n suojauksen purkujärjestelmärikosta koskevaan, sakko- tai enintään vuoden vankeusuhan sisältävään säännökseen lisättiin toissijaisuuslauseke ”jollei teosta muualla laissa säädetä ankarampaa tai yhtä ankaraa rangaistusta”.[127] Tätä perusteltiin[128] nimenomaan Turun hovioikeuden tuomioista ilmenevällä kannalla,

---

[126] Tuomiot nro 1578, 1581, 1582 ja 1583. Jutut ensiasteena käsitelleet Tampereen ja Porin käräjäoikeudet olivat päätyneet ratkaisuissaan väärennysrikoksiin.

[127] RL 38:8a (1118/2001). *Suojauksen purkujärjestelmärikos.* 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.

[128] LiVM 8/2001, s. 3.

jonka mukaan ”tietyissä tapauksissa suojauksen purkujärjestelmän, esimerkiksi ns. älykortin valmistaminen täyttää myös väärennysrikoksen tunnusmerkistön”.[129]

Korkeimman oikeuden ratkaisusta eivät käy täysin yksiselitteisesti selville ne perusteet, joilla korkeimman oikeuden mielestä älykorttia ei voida pitää väärennysrikoksen kohteeksi kelpaavana todistuskappaleena. Merkitystä on annettu sille, että älykortin avulla ei suoranaisesti erehdytetä lähetystoiminnan harjoittajaa, ja sille, että kysymys on vastaanottolaitteiston eri osien välisestä sähköisestä toiminnasta.

Tulkittavana olevan lain yli 15 vuotta sitten kirjoitetuista esitöistä on vaikea löytää kovin hyvin sovellettavissa olevia perusteluja nykyaikaisessa tietoteknisessä ympäristössä tapahtuneita tekoja ajatellen. Älykorttien tapaisia välineitä ei väärennysrikoksista säädettäessä tunnettu eikä niitä osattu ennakoida. Korkein oikeus ei ole ratkaisussaan ottanut nimenomaista kantaa siihen, voiko älykortilla oleva mikropiiri ylipäänsä olla rikoslain 33 luvun 6 §:ssä tarkoitettu automaattiseen tietojenkäsittelyyn soveltuva tallenne, mutta ratkaisu lienee luettavissa niin, että korkein oikeus sinänsä hyväksyy älykortin kelvolliseksi väärennysrikoksen kohteeksi. Korkein oikeus ei ole ottanut – eikä ole voinutkaan ottaa – kantaa myöskään siihen, olisiko A:n menettely toteuttanut suojauksen purkujärjestelmärikoksen tunnusmerkistön.

Tosiasiallisesti televisiolähetysten vastaanottamisen mahdollistava älykortti on – siltä osin kuin sen hallussapito osoittaa oikeutta televisiolähetysten katsomiseen – käsitykseni mukaan rinnastettavissa vanhaan televisiolupaan. Vaikka älykorttia ei televisioluvan tavoin esitetä lupatarkastajalle, on kummankin onnistuneella väärentämisellä sama seuraus: väärennöksen käyttäjä voi maksutta katsella televisiolähetyksiä.

Korkein oikeuskin lausuu ratkaisunsa perusteluissa älykortin toimintaa ja tarkoitusta kuvatessaan, että lähetystoimintaa harjoittavat yhtiöt ”luovuttavat suojauksen purkamiseen tarvittavan älykortin katsojille, jotka ryhtyvät sopimussuhteeseen niiden kanssa”. Sopimussuhteen syntyminen on siis edellytys älykortin saamiselle ja toisaalta älykortin oikeutettu hallussapito on osoitus sopimussuhteen olemassaolosta. Tämä ajattelutapa tuntuu selvästi ohjanneen Turun hovioikeutta.

Televisiolähetysten maksuttoman katselemisen mahdollistavien älykorttien valmistamisen suhteen korkeimman oikeuden ratkaisulla ei ole kovin kauaskantoisia seurauksia: menettely on nyttemmin joka tapauksessa rangaistavaa suojauksen purkujärjestelmärikoksena. Tietysti tuomittavan seurauksen suh-

---

[129] Samainen yhteydenottoni sai aikaan sen, että viimeisessä kokouksessaan liikennevaliokunta hyväksyi ehdotukseni muuttaa valmisteilla olleen lain nimi ”laiksi eräiden suojauksen purkujärjestelmien kieltämisestä”. Liikenne- ja viestintäministeriössä valmistellussa hallituksen esityksessä ehdotettiin maailmoja syleilevää nimeä ”laki tietoyhteiskunnan palvelujen suojasta”.

teen on suurikin ero siinä, onko käytettävissä suojauksen purkujärjestelmärikoksen yhden vuoden vankeusrangaistusmaksimi vai törkeän petoksen aina neljään vuoteen ulottuva rangaistusasteikko.

Ajateltaessa ratkaisusta ilmenevien periaatteiden vaikutusta rikoslain säännösten soveltamiseen tietoteknisessä ympäristössä tehtyihin tekoihin yleensä tuntuu korkein oikeus jättäneen vaille riittävää huomiota sen, että mahdollisesti hyvinkin pitkälle automatisoidut elektroniset toiminnot kuitenkin itse asiassa johtuvat yksinomaan ihmisten tahdonilmaisuista ja että nykyaikainen tekniikka usein tarjoaa vain uuden välineen sellaiselle lainvastaisen seurauksen saavuttamiselle, joka niin sanotuin perinteisin keinoin tehtynä on ollut ongelmatonta sovittaa rikoslain tunnusmerkistöihin.

EN:n yleissopimus ja väärennys

Euroopan neuvoston yleissopimuksen 7 artikla koskee väärennystä:

> *Tietokoneavusteinen väärennys.* Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin säätääkseen lainsäädäntönsä mukaisesti rangaistavaksi sellaisen tahallisen ja oikeudettoman datan syöttämisen, muuttamisen, tuhoamisen tai poistamisen, jonka tuloksena syntyvä väärä data on tarkoitettu käytettäväksi oikeudellisissa tarkoituksissa harhauttavana todisteena, riippumatta siitä, onko data sellaisenaan luettavissa tai ymmärrettävissä. Sopimuspuoli voi asettaa rikosvastuun syntymisen edellytykseksi sen, että teko on toteutettu petostarkoituksin tai muuta epärehellistä tarkoitusta varten.[130]

Artiklassa on kysymys vain datan aitoudesta *(authentic data),* ei sen sisällön oikeellisuudesta. Viimeksi mainitun sisällyttämisestä artiklaan toki keskusteltiin paljonkin sopimusneuvottelujen yhteydessä, mutta asiasta ei päästy yksimielisyyteen. Eräiden valtioiden toivomuksesta ja konsensuksen saavuttamiseksi artiklan loppuun lisättiin mahdollisuus asettaa rangaistavuuden edellytykseksi myös pelkkää väärentämistarkoitusta pitemmälle menevän rikollisen tarkoituksen vaatimus. Suomen lainsäädännön kannalta artikla ei edellytä toimenpiteitä.

---

[130] *Computer-related Forgery*. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law when committed intentionally and without right the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

3.2 TIETOJENKÄSITTELYPETOKSET

3.2.1 Petos (RL 36:1)

Rikoslain 36 luvun 1 §:ssä säädetään petoksesta seuraavasti:

> Joka, hankkiakseen itselleen tai toiselle oikeudetonta taloudellista hyötyä taikka toista vahingoittaakseen, erehdyttämällä tai erehdystä hyväksi käyttämällä saa toisen tekemään tai tekemättä jättämään jotakin ja siten aiheuttaa taloudellista vahinkoa erehtyneelle tai sille, jonka eduista tällä on ollut mahdollisuus määrätä, on tuomittava *petoksesta* sakkoon tai vankeuteen enintään kahdeksi vuodeksi.
>
> Petoksesta tuomitaan myös se, joka 1 momentissa mainitussa tarkoituksessa dataa syöttämällä, muuttamalla, tuhoamalla tai poistamalla taikka tietojärjestelmän toimintaan muuten puuttumalla saa aikaan tietojenkäsittelyn lopputuloksen vääristymisen ja siten aiheuttaa toiselle taloudellista vahinkoa.
>
> Yritys on rangaistava.

Petosta koskeva rikoslain 36 luku tuli uudistettuna voimaan vuoden 1991 alusta mutta tietojenkäsittelypetosta koskeva luvun 1 §:n toinen momentti muutettiin 1.7.2003 voimaan tulleella lailla 514/2003[131] edellä olevan mukaiseksi. Aikaisempi momentti oli näin kuuluva:

> Petoksesta tuomitaan myös se, joka 1 momentissa mainitussa tarkoituksessa tietojenkäsittelylaitteeseen vääriä tietoja syöttämällä tai koneelliseen tietojenkäsittelyyn muuten puuttumalla vääristää tietojenkäsittelyn lopputuloksen ja siten aiheuttaa toiselle taloudellista vahinkoa.

Petoksen lievästä ja törkeästä tekomuodosta säädetään 2 ja 3 §:ssä.[132] Kahdeksannen pykälän mukaan lievä petos on asianomistajarikos. Vuoden 1991 alussa voimaan tulleet säännökset korvasivat vanhat, osaksi alkuperäiset 36 luvussa olleet petossäännökset.[133]

---

[131] HE 2/2003, jossa ehdotetulla lainsäädännöllä saatettiin meillä voimaan EU:n puitepäätös muihin maksuvälineisiin kuin käteisrahaan liittyvien petosten ja väärennysten torjunnasta.

[132] RL 36:2: Jos petoksessa (1) tavoitellaan huomattavaa hyötyä, (2) aiheutetaan huomattavaa tai erityisen tuntuvaa vahinkoa, (3) rikos tehdään käyttämällä hyväksi vastuulliseen asemaan perustuvaa erityistä luottamusta tai (4) rikos tehdään käyttämällä hyväksi toisen erityistä heikkoutta tai muuta turvatonta tilaa ja petos on kokonaisuutena arvostellen törkeä, rikoksentekijä on tuomittava törkeästä petoksesta vankeuteen vähintään neljäksi kuukaudeksi ja enintään neljäksi vuodeksi. (1 mom.) Yritys on rangaistava. (2 mom.)

RL 36:3: Jos petos, huomioon ottaen tavoitellun hyödyn tai aiheutetun vahingon määrä taikka muut rikokseen liittyvät seikat, on kokonaisuutena arvostellen vähäinen, rikoksentekijä on tuomittava lievästä petoksesta sakkoon.

[133] RL 36:1: Joka, hankkiakseen itselleen tai toiselle laitonta aineellista etua, aiheuttaa toiselle tavaran tai rahan tappion siten, että hän esittämällä valheellisen asianlaidan tai vääristämällä tai

Perinteisesti petoksella on niin Suomessa kuin muuallakin ymmärretty ns. erehdyttämispetosta: vastapuolena oleva henkilö erehdytetään tekemään tai tekemättä jättämään jotakin. Tällaisella petosrikoksella on kolme tunnusmerkkiä: (1) erehdyttämistoimi, jollaisena voi tulla kysymykseen myös laiminlyönti, (2) erehdytetyn itsensä erehdyksen vallassa suorittama määräämistoimi (omaisuusdisponointi) sekä (3) omaisuusvahinko. Toisaalta edellytetään erehdyksen ja määräämistoimen sekä toisaalta määräämistoimen ja omaisuusvahingon välistä kausaaliyhteyttä.[134]

Nykyinen rikoslain 36 luvun 1 §:n 1 momentti tarkoittaa juuri tällaista erehdyttämispetosta eikä soveltamisalaltaan juurikaan poikkea vanhasta säännöksestä; aikaisemman tunnusmerkistön kasuistiikka on korvattu yleisemmällä teonkuvauksella. Pykälän toisen momentin tarkoittama niin sanottu tietojenkäsittelypetos on rakenteeltaan olennaisesti toisenlainen – ainoa yhtäläisyys erehdyttämispetoksen tunnusmerkistöön on vaatimus vahingon aiheuttamisesta.

Tietojenkäsittelypetokseen ei kuulu erehdyttämistä eikä erehdyksen vallassa suoritettua määräämistointa: onko kysymyksessä itse asiassa mikään petostyyppinen rikos?

Tietojenkäsittelypetoksen luonne

Nykyistä edeltäneen (sen paremmin kuin nytkään voimassa olevan) säännöksen perusteluissa ei ole pohdittu kovinkaan syvällisesti tietojenkäsittelypetoksen luonnetta. Rikoslain 36 luvun perusteluissa todetaan mm. seuraavaa:[135]

> Petoksen yleissäännöksessä erehdyttämispetosta koskeva 1 momentti muistuttaisi perusrakenteeltaan nykyistä petossäännöstä, joskin kieliasu olisi uusi. Tietojenkäsittelypetosta koskeva 2 momentti olisi sitä vastoin uuden tyyppinen kriminalisointi. Muiden maiden esimerkkiä seuraten uuden tietotekniikan vaikutukset on pyritty ottamaan huomioon siten, että ensisijaisesti tarkistetaan ja täydennetään perinteisiä käsitemääritelmiä ja rikostunnusmerkistöjä. *Sen vuoksi* (kursivointi tässä) rinnastettaisiin ihmisen erehdyttämiseen myös koneellisen tietojenkäsittelyn lopputuloksen vääristäminen.

---

salaamalla todellisen saa aikaan tai vireillä pitää erehdyksen, niin kuin jos hän myy väärennetyn tavaran oikeasta, sekoitetun puhtaasta tai virheellisen virheettömästä, taikka myy tai vuokraa saman omaisuuden kahdelle tai useammalle, taikka myymisen, lahjan tai muun välipuheen varjolla kavaltaa omaisuutta velkojalta kun ulosotto on tulossa, taikka kaupassa tai muuten väärin mittaa, punnitsee tai laskee, taikka muulla tavalla peijaa toisen, on tuomittava petoksesta sakkoon tai vankeuteen enintään kahdeksi vuodeksi taikka, jos asianhaarat ovat erittäin raskauttavat, (kuritushuoneeseen) enintään neljäksi vuodeksi. (1 mom., 30.6.1972/498) Jos joku tämän tekee ainoastaan saattaaksensa toiselle tavaran tai rahan tappion; olkoon sama laki. (2 mom.) Yritys on rangaistava. (3 mom.)

RL 36:1 a (30.6.1972/498): Jos pettäminen, aiheutetun vahingon määrä ja muut rikoksen teossa ilmenneet tai siihen johtaneet seikat huomioon ottaen, on katsottava vähäiseksi, on rikoksentekijä tuomittava lievästä petoksesta sakkoon.

134 Ks. Honkasalo, Erityinen osa I 2, s. 162 ss.

135 HE 66/1988, s. 130.

Ihmisen erehdyttämisen ja koneellisen tietojenkäsittelyn lopputuloksen vääristämisen rinnastamisen motiivina on siis perustelujen mukaan se, että ensisijaisesti uuden tietotekniikan vaikutukset rikoslainsäädäntöön on pyritty ottamaan huomioon tarkistamalla ja täydentämällä perinteisiä käsitemääritelmiä ja rikostunnusmerkistöjä. Ratkaisu on ilmeisen tekninen, sillä sisällöllisesti mainitut erehdyttäminen ja vääristäminen ovat kaukana toisistaan.

Tosin voidaan ajatella, että erehdyttämisen – tietojärjestelmän toimintaan puuttumisen – seurauksena ihmisen ajatusprosessin lopputulos jotenkin tietojenkäsittelyprosessiin rinnastettavalla tavalla vääristyisi, mutta ratkaisevaksi eroksi tietojenkäsittelyprosessissa joka tapauksessa jää disponoinnin puuttuminen: mahdollinen vahinko aiheutuu vääristyneestä lopputuloksesta sinänsä, siitä, että järjestelmän tuottama informaatio on erilaista kuin se olisi ollut ilman puuttumista järjestelmän toimintaan.

Hyvin mahdollinen on tilanne, jossa ihminen käyttää vääristynyttä lopputulosta esimerkiksi tallenteesta tehtynä tulosteena avukseen erehdyttääkseen jotakuta toista; tällöin kysymyksessä voi olla erehdyttämispetoksen tunnusmerkistön täyttävä teko, mutta tietojenkäsittelypetoksen tunnusmerkistö jää täyttymättä, koska vahinko ei aiheudu suoranaisesti vääristyneestä tietojenkäsittelyn lopputuloksesta.

On totta, että Suomen ulkopuolellakin vieraissa kielissä sanaa ”petos” tarkoittava sana on yleisesti liitetty rikoslain 36 luvun 1 §:n 2 momentissa kuvattuun menettelyyn; itse asiassa ”computer fraud” on yksi keskeisimmistä tietotekniikkarikoksista – tavallaan perusrikos hakkeroinnin ohessa – ja sitä koskeva suositus on Euroopan neuvoston minimilistan ensimmäisenä tekona.[136] Myös suosituksen perusteluissa hyväksytään rinnastus erehdyttämispetokseen jokseenkin kritiikittömästi:[137]

> Petosta tai vastaavia tekoja koskevat säännökset usein edellyttävät ihmisen erehdyttämistä (poikkeuksena esim. Kanada, Ranska, Alankomaat ja Skotlanti; kysymys on riidanalainen Englannissa ja Walesissa). Sellaisten rikosten kuin varkaus, kavallus, maksuvälinepetos ja luottamusaseman väärinkäyttö soveltamisala on yleensä rajoitettu. Monissa maissa varkautta ja kavallusta koskevat säännökset edellyttävät aineellisen objektin olemassaoloa. Silloinkin kun rikoksentekijä vääriä tietoja syöttämällä saa rahaa pankkiautomaatista, on joskus kysytty – kortinhaltijan legitimaation osoittamisen teknisesti rajoitetuista mahdollisuuksista joh-

---

[136] Sellainen datan tai ohjelmiston syöttäminen, muuttaminen, hävittäminen tai käytön estäminen taikka muu tietojenkäsittelyn lopputulokseen vaikuttava tietojenkäsittelytapahtumiin puuttuminen, joka aiheuttaa toiselle omaisuuden menetyksen tai taloudellista vahinkoa, kun teon tarkoituksena on hankkia itselle tai toiselle laitonta taloudellista hyötyä (tai vaihtoehtoisesti: kun teon tarkoituksena on laittomasti riistää toiselta tämän omaisuutta).

[137] EN:n raportti 89, s. 27.

> tuen – onko rahat ”anastettu” tai ”kavallettu” vastoin omistajan tahtoa (esim. jotkin tuomioistuimet Saksan Liittotasavallassa). Luotto- ja maksukorttirikoksia koskevat säännökset eivät sovellu kaikkiin moderneihin maksuvälinerikoksiin. Siksi useat jäsenvaltiot ovat nähneet välttämättömäksi lisätä rikoslakeihinsa joko petostunnusmerkistön laajennuksen tai uuden tietotekniikkapetosta koskevan säännöksen (Itävalta, Tanska, Saksan Liittotasavalta, Kreikka, Norja, Ruotsi; vrt. myös vastaaviin ehdotuksiin Suomessa, Portugalissa ja Sveitsissä). Tämä heijastelee yleistä mielipidettä, jonka mukaan tietyt tietokonemanipulaatiot ovat rankaisemisen arvoisia.

Euroopan neuvoston suosituksen vaikutusta lienee hyvin pitkälti se, että rikosnimike ”tietojenkäsittelypetos” (computer fraud, databedrägeri,[138] Datenbetrug) on otettu yleisesti käyttöön. Luontevampaa olisi kuitenkin ollut muodostaa tästä teosta täysin erehdyttämispetoksesta erillinen kriminalisointi, jolloin rinnastus erehdyttämispetokseen olisi rajoittunut mahdollisiin rikosnimikkeessä oleviin yhtäläisyyksiin. Uudemmasta ulkomaisesta lainsäädännöstä käy tässä suhteessa rikosnimikettä *(frode informatica)* lukuun ottamatta hyvänä esimerkkinä lisäys Italian *Codice Penaleen* joulukuun 23. päivältä 1993 (Art. 640 *ter*):

> Joka, hankkiakseen itselleen tai toiselle oikeudetonta hyötyä, jollain tavalla vääristää tieto- tai telejärjestelmän toimintaa tai muuten oikeudettomasti puuttuu siihen muuttamalla tieto- tai telejärjestelmän sisältämää tai siihen kuuluvaa dataa, informaatiota tai ohjelmistoa, tuomittakoon vankeuteen vähintään kuudeksi kuukaudeksi ja enintään kolmeksi vuodeksi sekä vähintään sadan tuhannen ja enintään kahden miljoonan liiran sakkoihin.
>
> Rangaistus olkoon vankeutta vähintään yksi ja enintään viisi vuotta sekä sakkoa vähintään kuusisataa tuhatta ja enintään kolme miljoonaa liiraa, jos teko on tehty 640 artiklan 2 momentin 1 kohdassa (törkeä petos) tarkoitetuissa olosuhteissa tai jos tekijä on käyttänyt hyväkseen asemaansa järjestelmän operaattorina.
>
> Rikos on asianomistajarikos, elleivät olosuhteet ole olleet 2 momentissa tarkoitetut tai asianhaarat muutoin raskauttavat.[139]

---

[138] Ks. Silvander, s. 340, jossa hän tietojenkäsittelypetosta (datarelaterat bedrägeri) käsitellessään toteaa, että ”det som skiljer ett sådant bedrägeri från ett traditionellt, är att den drabbade inte vilseleds även om förfarandet innebär förmögenhetsöverföring”.

[139] (1) Chiunque, alterando in qualsiasi modo il funzianomento di un sistema informatico o telematico o intervenendo senza diritto, con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da lire centomila a due milioni. (2) La pena è la reclusione da uno a cinque anni e della multa da lire seicentomila a tre milioni se ricorre una della circostanze previste dal numero 1) del secondo comma dell’articolo 640 (truffa aggravata), ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, (3) il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di qui al secondo comma o un’altra circostanze aggravante.

Säännös on selvästi itsenäinen, vaikkakin se on sijoitettu petossäännöksen yhteyteen. Ongelmaksi – mielestäni – jääkin rikosnimike: miksi puhua petoksesta, kun ei petetä? Viittaan brittiläisen *Computer Misuse Actin* kolmannen pykälän tietoteknisen aineiston oikeudetonta muuttamista koskevaan säännökseen, jossa on onnistuneesti vältetty viittaukset ns. perinteisiin rikoksiin. Tämä tietysti johtuu valitusta ja toteutetusta lainsäätämistavasta, joka poikkeaa oleellisesti yhtä hyvin suomalaisesta kuin italialaisestakin metodista.

Lieneekin perusteltua – nimityksestä huolimatta – nähdä tietojenkäsittelypetokseksi kutsuttu teko tosiasiallisesti kokonaan omaksi rikostyypikseen ja jättää vaille huomiota sitä koskevan säännöksen sijainti rikoslain 36 luvussa, sillä asiallinen yhteys erehdyttämispetoksen kanssa jää kutakuinkin olemattomaksi. Erityisiä rajanveto-ongelmia erehdyttämispetoksen ja tietojenkäsittelypetoksen välille ei helposti synny; sitä vastoin niitä voi syntyä tietojenkäsittelypetoksen ja muiden tietotekniikkarikosten välille jäljempänä havaittavin tavoin.

Teon elementit

Suomalaisen tietojenkäsittelypetosta koskevan alkuperäisen säännöksen perustelujen[140] mukaan koneellisella tietojenkäsittelyllä useimmiten tarkoitetaan automaattista tietojenkäsittelyä mutta atk-järjestelmien ohella säännös koskee myös muita tietojenkäsittelylaitteita, esimerkiksi mittareita, laskimia ja piirtureita. Säännöksen sanotaan olevan tarpeen kaikkia sellaisia tilanteita varten, joissa säännöksessä kuvatuin tavoin aiheutetaan toiselle taloudellinen vahinko ilman, että kenenkään ihmisen erehdys on ollut syy-yhteydessä aiheutuneeseen vahinkoon. Tältä osin perusteluissa lausuttu soveltuu myös nykyään voimassa olevaan säännökseen; tosin termi ”koneellinen tietojenkäsittely” on vanhentuneena nyt hylätty.

Alkuperäisen säännöksen mukaan tietojenkäsittelypetos saattoi ensinnäkin tapahtua syöttämällä tietojenkäsittelylaitteeseen vääriä tietoja; tässä yhteydessä väärällä tiedolla tarkoitettiin sellaista totuudenvastaista tai ilmeisen harhaanjohtavaa tietoa, joka ihmiselle esitettynä olisi omiaan häntä erehdyttämään.[141]

Tieto-sanan monimerkityksisyys aiheutti tässä ongelmia: puhuttiinko datasta vai informaatiosta? Ilmaisu ”syöttää väärä tieto laitteeseen” ei sanonut vielä kovinkaan paljon. Tietojärjestelmään syötetään dataa, joka edustaa jotakin informaatiota. Informaatio voi olla sellaista, että sillä on merkitystä sinänsä, tai sitten se voi olla relevanttia tietojärjestelmän toiminnan kannalta.

Vääränä tietona eivät perustelujen mukaan tulleet kysymykseen tietokoneelle annetut suorituskäskyt sinänsä, vaikka niiden antaja olisikin ylittänyt toimivaltansa ja aiheuttanut menettelyllään vahinkoa. Näin ollen vääränä tietona kaiketi

---

140 HE 66/1988, s. 133 s.

141 Ks. Nuutila, Rikosoikeus, s. 1167.

tulivat kysymykseen sellaiset tiedot, jotka itsessään ovat merkityksellisiä. Miten tällaiset tiedot voivat vaikuttaa tietojenkäsittelyn lopputulokseen? Perustelujen mukaan tiedon oli oltava sellaista, että se ihmiselle esitettynä olisi omiaan häntä erehdyttämään.

Uudessa säännöksessä on luovuttu edellytyksestä, että syötettävien tietojen tulisi olla vääriä. Perustelujen mukaan[142] myös sinänsä oikeiden tietojen syöttäminen on perusteltua säätää rangaistavaksi, jos ne syötetään petostarkoituksessa ja tarkoituksessa vääristää tietojenkäsittelyn lopputulos edellyttäen, että siten aiheutetaan toiselle taloudellista vahinkoa. Tätä on pidettävä ilman muuta tervetulleena uudistuksena: tiedon vääryysominaisuus on kovin suhteellinen käsite ja riippuu tiedon kulloisestakin käyttöyhteydestä.

Nyt myös säännöksen tekotapaluettelo on laajennettu vastaamaan kansainvälisten instrumenttien[143] petossäännöksiä: tietojen syöttämisen lisäksi myös tietojen muuttaminen, tuhoaminen ja poistaminen mainitaan nimenomaisesti ja näiden ohella myös muu puuttuminen tietojärjestelmän toimintaan voi toteuttaa rikoksen tunnusmerkistön. Aikaisemman säännöksen perusteluissakin[144] on mahdollisina tekotapoina mainittu tietokoneessa valmiina olevien tallennettujen tietojen muunteleminen, pimittäminen tai poistaminen samoin kuin tietokoneen väärin ohjelmoiminen tai oikean ohjelmoinnin luvaton muuttaminen taikka ohjelman vaihtaminen, joten asiallisesti säännöksen soveltamisalassa ei ole muutosta tapahtunut.

Sanan tieto asemesta on otettu käyttöön sana data, jolla tässä yhteydessä[145] tarkoitetaan samaa kuin Euroopan neuvoston tietoverkkorikosyleissopimuksessa eli sellaisessa muodossa olevaa tosiseikkojen, tietojen tai käsitteiden esitystä, että se soveltuu käsiteltäväksi tietojärjestelmässä, mukaan lukien ohjelmat, joiden avulla tietokone pystyy suorittamaan jonkin toiminnon. Keskeistä tässä datan määritelmässä on se, että ollakseen dataa tiedon pitää olla sähköisessä tai muussa sellaisessa muodossa, että se sellaisenaan soveltuu käsiteltäväksi tietojärjestelmässä.

Monimerkityksisen tieto-sanan korvaaminen datalla on käsitykseni mukaan erittäin oikeaan osunut ratkaisu. Euroopan neuvoston tietoverkkorikosyleissopimusta aikanaan voimaan saatettaessa datan käsite tullee yleisemminkin käytettäväksi niin rikos- kuin pakkokeinolainsäädännössäkin, mikä yhdessä nyt puheena olevan uudistuksen kanssa tekee tietotekniikkarikoksia koskevat säännöksemme entistä täsmällisemmiksi ja helpommin tulkittaviksi.

Tietojenkäsittelypetosta koskeva säännös on pyritty muutenkin saattamaan nykyistä tietoteknistä käsitteistöä vastaavaksi korvaamalla tietojenkäsittelylaite

---

142 HE 2/2003, s. 16.
143 EN:n tietoverkkorikosyleissopimus, EU:n maksuvälinepetospuitepäätös.
144 HE 66/1988, s. 133.
145 HE 2/2003, s. 17.

tietojärjestelmällä. Käsitettä käytetään myös Euroopan neuvoston yleissopimuksessa kattamaan sekä tietoverkot että yksittäiset tietokoneet.[146]

Tältäkin osin muutos on varsin perusteltu. Kun ajatellaan jotakin laitoksen, yrityksen tai viraston vaikkapa muutamasta kymmenestä työasemasta muodostuvaa lähiverkkoa, joka tukeutuu yhteen palvelinkoneeseen ja on sen ja edelleen mahdollisesti lukuisten muiden palvelinten välityksellä yhteydessä Internetiin, niin tuon lähiverkon yksittäisestä työasemasta on periaatteessa mahdollista saada yhteys satoihin miljooniin muihin työasemiin ympäri maailmaa. Mikä olisi silloin se *laite,* johon data on petollisessa tarkoituksessa syötetty, kun itse syöttäminen on tapahtunut suomalaisessa virastossa ja seuraus on ilmennyt australialaisessa yrityksessä? Olisiko laite suomalainen työasema, sen lähiverkon palvelin, johon työasema kuuluu, jonkin Internet-palveluntarjoajan vaikkapa Yhdysvalloissa sijaitseva palvelin vai australialaisen työaseman PC-laite (vai jokin muu)? Missä olisi mahtanut tapahtua se tietojenkäsittely, jonka lopputulos on vääristynyt? Kysymykset ovat ehkä paljolti teoreettisia mutta olisivat saattaneet aiheuttaa suuriakin vaikeuksia pohdittaessa esimerkiksi tekijän tahallisuuden astetta ja erityisesti asiaa tutkivien viranomaisten toimivaltuuksia.

Tietotekniikkarikoksia koskevien kriminalisointien liiallinen välinesidonnaisuus saattaa yleensäkin aiheuttaa ongelmia. Aika on tehnyt tehtävänsä: kun kymmenen vuotta sitten ajateltiin tietotekniikkarikoksia, olivat mielessä *tietokonerikokset.* Nyt tietotekniikkarikokset ovat *tietoverkkorikoksia.* Koko käsite on kokenut valtavan muutoksen, erityisesti Internetin laajenemisen myötä.

Tunnistetieto vääränä tietona

Aikaisemman tietojenkäsittelypetossäännöksen perustelujen mukaan väärän tiedon antamista olisi ollut atk-järjestelmän käyttäjäkontrollin petollinen läpäiseminen toiselle kuuluvaa tunnistetietoa käyttämällä. Kun ei uudessa esityksessä muuta lausuta, voitaneen tulkita tämän näkemyksen yhä edelleen vastaavan lainsäätäjän käsityksiä – siis siinä mielessä, että tietojenkäsittelypetokseen voisi yhä edelleen syyllistyä toiselle kuuluvaa tunnistetietoa käyttämällä, sen vääryysominaisuudesta riippumatta.

Näkemys kaipaa lähempää tarkastelua. Rikoslain 38 luvun 8 §:n tietomurtoa koskevassa yleissäännöksessä tekotapana on oikeudeton tunkeutuminen tietojärjestelmään käyttämällä tekijälle kuulumatonta käyttäjätunnusta tai turvajärjestely muuten murtamalla. Tietojenkäsittelypetosta koskevan säännöksen perustelujen mukaan tällainen tunkeutuminen siis osaltaan toteuttaisi tämän rikoksen tunnusmerkistöä.

Tietomurrossa rikos on täyttynyt heti tunkeutumisen onnistuttua. Tietomurron erityistapauksena kysymykseen tulevassa yritysvakoilussa rangaistavuuden

---

146 HE 2/2003, s. 17.

edellytyksenä on lisäksi tiedon hankkiminen toiselle kuuluvasta yrityssalaisuudesta. Tietomurtosäännöksen on nimenomaan todettu olevan toissijainen.

Tietojenkäsittelypetoksen tekijällä on aina oltava hyötymis- tai vahingoittamistarkoitus eikä liene kovinkaan helposti kuviteltavissa sellainen tilanne, että pelkkä ”petollinen” tunkeutuminen tietojärjestelmään sinänsä voisi aiheuttaa ainakaan *tietojenkäsittelyn lopputuloksen vääristymisen* kautta syntyvää vahinkoa – miten ylipäänsä väärien tunnistetietojen syöttäminen yksin voisi vaikuttaa tietojenkäsittelyn lopputulokseen?

Ainoa mahdollisuus nähdäkseni on, että sisäänpääsyä kontrolloiva tapahtuma katsottaisiin itsenäiseksi ”tietojenkäsittelyksi”, jonka lopputulos (= kontrollin läpäisy) vääristyisi läpäisyn johdosta (= väärä henkilö pääsi läpi). Tämä ajattelu ei tosin tunnu vastaavan lainsäätäjän tahtoa sikäli, että edellä selostetuin tavoin luvattoman käytön yhteydessä oli katsottu vasta tunnistuskontrollin läpäisyn jälkeinen järjestelmän käyttö sellaiseksi käytöksi, joka on tietojärjestelmälle luonteenomaista eli siis varsinaista tietojenkäsittelyä. Joka tapauksessa tämä konstruktio jättäisi kysymyksen vahingon aiheutumisesta yhä avoimeksi.

Entäpä jos tekijä kuvatuin tavoin tietojärjestelmään tunkeuduttuaan (ja tältä osin ehkä syyllistyttyään tietojenkäsittelypetoksen tunnusmerkistöä toteuttavaan menettelyyn) aiheuttaa tietojenkäsittelyn lopputuloksen *muuttumisen* ilman, että hän on syöttänyt järjestelmään dataa tai muuten puuttunut järjestelmän toimintaan?

Tietojenkäsittelypetokseen kuuluu aina tietojenkäsittelyn lopputuloksen vääristyminen eli se, että tietojenkäsittelyjärjestelmä saadaan puuttumistoimien jälkeen tuottamaan virheellistä eli sisällöltään toisenlaista informaatiota kuin järjestelmä olisi tuottanut ilman puuttumistoimia. Väärennys- ja vahingontekorikosten kohdalla voidaan havaita samantapaisia tunnusmerkistötekijöitä.

Muu puuttuminen tietojärjestelmän toimintaan

Tietojenkäsittelypetos voi edellä selostetuin tavoin tapahtua paitsi dataa tietojärjestelmään syöttämällä myös sitä muuttamalla, tuhoamalla tai poistamalla taikka tietojärjestelmän toimintaan muuten puuttumalla.

Näissä tilanteissa saattaa syntyä rajanveto-ongelmia suhteessa jäljempänä käsiteltävään vahingontekorikokseen, josta on kysymys, kun joku toista vahingoittaakseen oikeudettomasti *hävittää, turmelee, kätkee tai salaa* tietovälineelle tallennetun tiedon. Tällaisessa tilanteessa lienee määräävänä kriteerinä pidettävä sitä, aiheutuuko niin tietojenkäsittelypetoksessa kuin vahingonteossakin tunnusmerkistön täyttymisen edellytyksenä oleva vahinko jo esimerkiksi pelkästä tiedon poistamisesta vai vasta tiedon poistamisen seurauksena syntyneestä tietojenkäsittelyn lopputuloksen vääristymisestä – saattaahan olla, että hävinneellä informaatiolla sinänsä on oikealle haltijalleen taloudellista arvoa, vaikka informaation olemassaololla ei olisikaan merkitystä jollekin nimenomaiselle tietojenkäsittely*prosessille.*

Vahingon aiheutuminen, petoksen suhde vahingontekoon

Tietojenkäsittelypetossäännöksen sanamuotoa muutettiin myös sikäli, että kun aikaisemmin tekijän edellytettiin *vääristävän tietojenkäsittelynlopputuloksen,* hänen on nyt *saatava aikaan tietojenkäsittelyn lopputuloksen vääristyminen.* Uuden säännöksen perustelujen mukaan[147] esimerkiksi datan syöttäminen tietojärjestelmään käynnistää monivaiheisen prosessin, joka voi johtaa vääristyneeseen lopputulokseen. Tämän vuoksi on katsottu aiheelliseksi, että datan syöttäjän tai tietojärjestelmän toimintaan puuttujan on saatava aikaan tietojenkäsittelyn lopputuloksen vääristyminen sen sijasta, että hänen edellytettäisiin suoraan vääristävän tietojenkäsittelyn lopputulos. Tämäkin muutos on perusteltu.

Vanhan säännöksen perusteluissa todetaan petostunnusmerkistön kokonaisuuden kannalta olevan yhdentekevää, millä tavoin tietojenkäsittelyssä aikaansaatu virheellinen tieto aiheuttaa taloudellisen vahingon: tämä voi tapahtua joko ihmisen tai koneen välityksellä. Automaattisessa tietojenkäsittelyssä tuotettu virheellinen tieto voi selväkieliseen, ihmiselle ymmärrettävään muotoon tulostettuna tulla sellaisenaan inhimillisen päätöksenteon pohjaksi ja siten aiheuttaa taloudelliseen vahinkoon johtavan määräämistoimen. Tällainen teko on – niin kuin edellä jo on todettu – rangaistavissa erehdyttämispetoksena.

Usein kuitenkin tietojenkäsittelyn aikana tuotettu tieto johtaa välittömästi sellaisiin sähköisiin määräämistoimiin, joiden seurauksena esimerkiksi varoja siirtyy pankkitililtä toiselle. Tällainen automaattinen tilisiirto ei perustu kenenkään ihmisen suorittamaan kirjaustoimeen ja vasta tällaisessa tapauksessa perustelujen mukaan on kysymys tietojenkäsittelypetoksesta. Edellä väärennystä käsiteltäessä olen korostanut sitä eroa, joka on muistettava tehdä tietoteknisen tallenteen ja tallenteesta tehdyn tulosteen välillä; sama pätee soveltuvin osin myös petokseen tutkittaessa erehdyttämispetoksen ja tietojenkäsittelypetoksen keskinäistä suhdetta. Tietojenkäsittelyn lopputulos säännöksen tarkoittamassa mielessä *ei* ole esimerkiksi paperituloste, vaan se tietovälineelle kiinnitetyn datan ja sen kantaman informaation kokonaisuus, josta tuloste on eräänlainen visuaalinen kuvaus.

Äsken sanottukaan ei välttämättä selvennä tietojenkäsittelypetoksen ja vahingonteon välistä suhdetta, johon palaan tarkemmin jäljempänä vahingontekoa käsitellessäni.

Petos ja väärennys

Täysin ongelmatonta ei ole myöskään rajan vetäminen tietojenkäsittelypetoksen ja tietoteknisen väärennyksen välille. Tallennetun tiedon muuttaminen saattaa synnyttää väärän tai väärennetyn todistuskappaleen, jota sitten käytetään

---

147 HE 2/2003, s. 17.

hyödyn hankkimiseen tai vahingon aiheuttamiseen. Tällaisessa tilanteessa, kun sekä väärennyksen että petoksen tunnusmerkistöt täyttyvät, ei tietotekninen ympäristö aiheuta ongelmia: molempia säännöksiä sovelletaan yhtä aikaa.[148] Petos ja väärennys yleensäkin ovat helpommin toisistaan erotettavissa kuin tietotekniikkapetos ja tietovahingon aiheuttaminen, sillä väärennys on petoksesta poiketen luonteeltaan todistelurikos.

Väärennyksestä edellä puhuttaessa on käsitelty korkeimman oikeuden ratkaisua 1985 II 60 ja todettu, että vaikka tapauksessa yhtenä ongelmana ollut asiakirjan käsitteen ulottuvuus onkin ratkaistu rikoslain 33 luvun 6 §:n määritelmäsäännöksessä, ei säännöksen sisältämä vääryysominaisuuden määrittely ole ongelmaton. Tapauksessa kerrotusta menettelystä löytyvät kaikki *tietojenkäsittelypetoksen* tunnusmerkit: (1) hyödyn hankkimistarkoitus, (2) vääriä tietoja syöttämällä aikaansaatu tietojenkäsittelyn lopputuloksen vääristyminen ja (3) vahingon aiheutuminen. Toisaalta menettely voisi toteuttaa myös *erehdyttämispetoksen* tunnusmerkistön: vääristetty tietojenkäsittelyn lopputulos on tulostettu ja tulostetta on käytetty erehdyttämisen välikappaleena.

Erehdyttämispetos ja tietojenkäsittelypetos

Tässä tapauksessa näyttääkin ensisijaiseksi rajanveto-ongelmaksi muodostuvan erehdyttämispetoksen ja tietojenkäsittelypetoksen keskinäinen suhde. Jos edellä esitetyin tavoin katsotaan, että sen paremmin tulosteen kuin sitä vastaavan tallenteenkaan alkuperän oikeellisuuden loukkaamiseen ei riitä syötettyjen tietojen virheellisyys, ei tapauksessa olisi lainkaan kysymys väärennysrikoksesta, ellei sitten kysymyksessä ole ollut sellainen tietotekninen tallenne, että se teon seurauksena voidaan katsoa määritelmäsäännöksessä tarkoitetuin tavoin väärennetyksi. Olisin joka tapauksessa taipuvainen katsomaan, että voimassa olevankin lain mukaan tapauksessa olisi päädyttävä samaan *lopputulokseen,* johon korkein oikeus aikanaan on päätynyt, ja – edellyttäen, että erehdyttämistoimi on osoitettavissa tapahtuneeksi – että tapausta olisi arvioitava nimenomaan rikoslain 36 luvun 1 §:n 1 momentissa tarkoitettuna erehdyttämispetoksena.[149]

Esimerkkejä

Suomalaisessa oikeuskäytännössä ei varsinaisia tietojenkäsittelypetostapauksia ole esiintynyt. Ulkomailta esimerkkejä toki löytyy; seuraavassa kaksi vanhempaa mutta hyvin tyypillistä tapausta Englannista. Molemmat ovat *Stanford Research Instituten* aineistosta eikä niihin liity mitään sellaisia kansal-

---

148 Ks. Lahti, LM 91 s. 1177.
149 Ks. Lahti, LM 91 s. 1176.

lisia erikoispiirteitä, etteivätkö ne aivan hyvin olisi voineet tapahtua Suomessakin.[150]

> Ensimmäisessä tapauksessa oli kysymys yrityksen työntekijästä, jonka tehtävänä oli hoitaa yrityksen maksuliikennettä. Normaalin käytännön mukaan hänen tuli vahvistaa maksuasiakirjat ennen automaattista tietojenkäsittelyä. Kaikki maksut rekisteröitiin erityiseen tietokonerekisteriin, minkä jälkeen tietojärjestelmä suoritti maksun mm. suorilla siirroilla maksunsaajien tileille. Työntekijä valmisteli perusteettomia maksusuorituksia avaamalla pankkitilit muutamalle olemattomalle henkilölle. Sitten hän suoritti näille tileille neljä perusteetonta maksua määriltään yhteensä £ 15 000. Hän käytti hyväkseen mahdollisuutta maksaa ennen eräpäivää ja poisti maksutapahtuman tietokonerekisteristä heti kun rahat olivat siirtyneet asianomaiselle pankkitilille. Näin hän onnistui välttämään kiinnijäämisen neljän kuukauden ajan. Rikos paljastui, kun tekijän ollessa päivänä muutamana poissa töistä eräs tietotekniikkaosaston työntekijä tuli epäluuloiseksi löydettyään omituisia syöttötietoja. (SRI 85315)
>
> Toisessa tapauksessa myyntipäällikkö, jolla oli laajat valtuudet käsitellä liiketoimia yrityksen tietojärjestelmässä, loi lukuisia fiktiivisiä tavarantoimittajia ja syötti nämä järjestelmään. Väärien ostosopimusten rekisteröimisestä seurasi, että tietokone maksoi ”ostot” automaattisesti kuvitteellisten tavarantoimittajien tileille. Ristiriitaiset lausumat myyntipäällikön budjetissa saivat epäilykset heräämään. Rikollinen toiminta oli tuolloin kestänyt kahdeksantoista kuukautta ja väärien maksujen määrä oli yhteensä £ 80 000. (SRI 85317)

Molemmat edellä olevista tapauksista muistuttavat jossain määrin korkeimman oikeuden ratkaisussa 1985 II 60 tarkoitettua menettelyä. Yhteistä kaikille kolmelle tapaukselle on se, että henkilö on hänelle sinänsä kuuluneiden valtuuksien puitteissa päässyt käsittelemään yrityksen tietojärjestelmää, johon on syöttänyt vääriä tietoja seurauksin, että yritykselle on syntynyt tappiota ja tekijälle tai jollekulle muulle oikeudetonta hyötyä.

Se, mikä erottaa englantilaiset tapaukset suomalaisesta ja tekee niistä nimenomaan tietojenkäsittelypetoksia, on tietojärjestelmän yksinomainen rooli ”erehdytettynä” objektina: tietojärjestelmään syötetty virheellistä informaatiota kantanut data on suoranaisesti saanut järjestelmän suorittamaan toimia, jotka eivät ole olleet asianmukaisia; tietojenkäsittelyn lopputulos on vääristynyt.

Eräitä näkemyksiä tietojenkäsittelypetoksen suhteesta muihin tekoihin

Durham on AIDP:n syksyn 1992 kollokvion yleisraportissaan käsitellyt erehdyttämispetoksen ja tietojenkäsittelypetoksen keskinäistä suhdetta.[151] Hän to-

---

[150] Wranghult, s. 13 s.
[151] Durham, s. 107 s.

teaa kollokvion kansallisista raporteista keräämänsä informaation perusteella, että tietojenkäsittelypetos on tyypillisesti konstruoitu tietojärjestelmään tunkeutumisen tai järjestelmän käytön taikka manipuloinnin käsittävän rikoksen törkeämmäksi tekomuodoksi. *Durhamin* mukaan yhtenä ongelmana on se, että joskus on jokseenkin mielivaltaisesti todettavissa, onko tietokone osallisena varsinaisessa petollisessa transaktiossa. Riittäisikö tietokoneen pelkkä mukana oleminen poistamaan tapauksen normaalista petoskategoriasta ja vaatimaan sen erillistä analysoimista? Erityisesti petoksen ollessa kysymyksessä on huolellisesti paneuduttava selvittämään uusien tietotekniikkarikosten ja perinteisten rikosten välistä suhdetta.

Durham käsittelee myös kysymystä koneen erehdyttämisestä ja toteaa muun muassa, että ”erehdytetty” tietokone on tosiasiassa vain väline, jota on käytetty pettämään tai vahingoittamaan sen omistajaa tai jotakuta muuta henkilöä. – Tämän näkemyksen olen valmis hyväksymään sillä rajauksella, että pettämisestä ei tulisi tietojenkäsittelypetoksen yhteydessä puhua lainkaan.

Sieber näkee petoksen perinteisen tekotavan ja tietojenkäsittelypetoksen välillä teko-objektin kannalta sekä kvalitatiivisia että kvantitatiivisia eroja.[152] Edelliset ovat seurausta siirtymisestä ns. sähköisten varojen käyttämiseen, jälkimmäiset taas tietojenkäsittelyjärjestelmissä liikuteltavien varojen suurista määristä.

Tietojenkäsittelypetossäännöksen perusteluissa käsitellään petoksen ja kavalluksen keskinäistä suhdetta: kavalluksesta olisi kysymys silloin, kun pankkivirkailija oikeudettomasti siirtää varoja tietojenkäsittelylaitteiden avulla omalle tililleen, mikäli varojen on katsottava olleen hänen hallussaan siten kuin rikoslain 28 luvun 13 §:n 3 momentissa on tarkoitettu. *Nuutila* toistaa tämän käsityksen ja toteaa lisäksi, että jos konekielisen tiedoston luvaton muunteleminen on tapahtunut siinä tarkoituksessa, että tiedostoa muuntelun jälkeen voitaisiin käyttää harhauttavana todisteena, tapaukseen sovelletaan väärennysrikoksia koskevia säännöksiä.[153]

Myös *Lahden* mukaan tietojenkäsittelypetos ja kuvatunlainen kavallus ovat toisensa syrjäyttävässä suhteessa, vaikkakin kavalluksen rangaistusasteikko on lievempi kuin petoksen.[154]

Näkemykset ovat – vaikkakaan eivät vaikeuksitta – hyväksyttävissä, ainakin vanhemman tietojenkäsittelypetossäännöksen sanamuodon valossa. Kuvatunlaisessa menettelyssä pankkivirkailija tosin puuttuu automaattiseen tietojenkäsittelyyn tavalla, joka saa aikaan epäasianmukaisen lopputuloksen ja aiheuttaa toiselle taloudellista vahinkoa. Kavallussäännöksen soveltuvuuden ensi-

---

[152] Sieber, Handbook, s. 5 s.
[153] Nuutila, Rikosoikeus, s. 1167 s.
[154] Lahti, LM 91, s. 1177, HE 66/1988, s. 134.

sijaisuuden puolesta on kuitenkin puhunut se, että informaatio, jota pankkivirkailija järjestelmään syöttää, on *sinänsä* oikeata; syöttäminen vain on *oikeudetonta* ja johtaa rahojen *tosiasialliseen* anastamiseen. Tuolloisen sääntelyn taustalla olleen Euroopan neuvoston suosituksen perustelujen mukaan toisaalta jo virheettömän datan oikeudeton syöttäminen olisi riittänyt konstituoimaan tietojenkäsittelypetoksen – tilanne ei siis ole ollut ongelmaton ja ongelman suuruus riippuu muun ohessa siitä, mikä merkitys Euroopan neuvoston suositukselle perusteluineen annetaan oikeuslähteenä silloin, kun joudutaan tulkintatilanteisiin.[155]

Nykyistä säännöstä ajatellen keskeisin ongelma lienee siinä, onko kysymyksessä tietojenkäsittelyn lopputuloksen vääristyminen. Lopputulos on juuri se, johon pankkivirkailija on pyrkinyt ja järjestelmä on oikein toimimalla tuottanut lopputuloksen pankkivirkailijan antamien käskyjen seurauksena. Tämä puoltaisi kavallusta koskevan säännöksen soveltuvuuden ensisijaisuutta.

Toisaalta kavalluksen ensisijaisuuden hyväksyminen voisi johtaa siihen, että pankki- tai vastaavaa korttia käyttämällä tapahtunut oikeudeton rahojen nosto automaatista tulisikin arvioida anastusta eikä maksuvälinepetosta koskevien säännösten nojalla. Tietokoneohjattujen pankki- ja muiden automaattien väärinkäyttötapauksiin ei tietojenkäsittelypetosta koskeva säännös yleensä muutoinkaan sovellu.[156]

Lahti viittaa niihin rajanvetovaikeuksiin, joita voi aiheutua rikoslain 36 luvun 1 §:n 2 momentin soveltamisen suhteesta varkautena arvosteltavaksi tarkoitettuun tavara- tai raha-automaatin luvattomaan hyödyntämiseen, jonka osalta hän korostaa tietojenkäsittelypetoksen yhtenä tunnusmerkkinä olevaa vaatimusta tietojenkäsittelyyn puuttumisesta.[157]

Euroopan neuvoston raportissa ei käsitellä edellä esille tulleita tai niitä vastaavia rajanveto-ongelmia. Kaiken kaikkiaan suomalainen tietojenkäsittelypetossäännös vastaa sisällöltään Euroopan neuvoston suositusta.[158] Suosituksen perusteluissa todetaan suosituksessa pyrityn tyhjentävään tekotapaluetteloon:

---

[155] Suosituksessa ja sen perusteluissa korostetaan monin kohdin kansallisen lainsäätäjän tahdon ja kansallisen lainsäädäntötradition merkitystä, mikä oikeuttaa päättelemään, että suosituksen merkitys oikeuslähteenä ei voi olla meillä kovinkaan suuri – ainakaan silloin, kun omasta lainvalmisteluaineistostamme löytyy nimenomaisesti ilmaistuina suosituksessa esitetyistä poikkeavia kannanottoja.

[156] Ks. Nuutila, Rikosoikeus, s. 1167. Nuutila esittää saman näkemyksen ja toteaa, että kysymyksessä on maksuvälinepetos, jos pankki- tai muun vastaavan automaatin väärinkäyttö tapahtuu RL 37 luvussa tarkoitetun muovirahan avulla. Puhelin-, levy-, peli- tai muun vastaavan automaatin käyttäminen menetelmällä, jota ei ole sitä varten tarkoitettu, rangaistaan lievänä luvattomana käyttönä. Jos kysymyksessä on tavara-, polttoaine tai raha-automaatin väärinkäyttö keinottelemalla sen koneisto käyntiin muulla kuin rahalla, maksukortilla tai muulla maksuvälineellä, teko rangaistaan anastusrikoksena.

[157] Lahti, LM 91, s. 894 ja 1177, ks. myös HE 66/1988, s. 44.

[158] Ks. EN:n raportti 89, s. 28 s.

datan tai ohjelmiston syöttäminen (input), muuttaminen (alteration), hävittäminen (erasure) tai käytön estäminen (suppression) taikka muu tietojenkäsittelyn lopputulokseen vaikuttava tietojenkäsittelyyn puuttuminen (interference).

Syöttämisellä tässä yhteydessä tarkoitetaan toisaalta virheellisen datan syöttämistä ja toisaalta virheettömän datan oikeudetonta syöttämistä (vrt. edellä petoksen ja kavalluksen suhdetta käsiteltäessä sanottu). Esimerkkinä tällaisesta menettelystä perusteluissa mainitaan toisaalta anastetun pankkikortin väärinkäyttö pankkiautomaatissa ja toisaalta oman kortin käyttäminen luottoraja ylittäen. Niin kuin edellä on mainittu, Suomessa menettelyt on kriminalisoitu erikseen maksuvälinepetoksena, jota käsitellään seuraavaksi.

EN:n yleissopimus ja petos

Euroopan neuvoston tietoverkkorikosyleissopimuksen kahdeksannessa artiklassa on seuraava petosta koskeva säännös:

> *Tietokoneavusteinen petos.* Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin säätääkseen lainsäädäntönsä mukaisesti rangaistavaksi tahallisen ja oikeudettoman taloudellisen vahingon aiheuttamisen toiselle, kun teko on tehty:
> a) dataa syöttämällä, muuttamalla, tuhoamalla tai poistamalla;
> b) tietojärjestelmän toimintaa häiritsemällä, tarkoituksin saada itselle tai toiselle taloudellista hyötyä petoksella tai muulla epärehellisellä keinolla.[159]

Määräys vastaa hyvin pitkälti Euroopan neuvoston suosituksen vastaavaa kohtaa. Säännös ei edellytä meillä sen paremmin asiallista kuin muodollistakaan lainsäädännön tarkistamista, kun tietojenkäsittelypetosta koskeva säännös on uudistettu ottamalla huomioon mm. yleissopimuksen vaatimukset.

3.2.2 Maksuvälinepetos (RL 37:8)

Maksuvälinepetoksen kohdalla on kysymys erityisrikoksesta, joka eräissä tapauksissa muodostaa yhden tietojenkäsittelypetoksen alalajin. Maksuvälinerikoksia koskevan rikoslain 37 luvun 8 §:ssä oleva maksuvälinepetosta koskeva

---

[159] *Computer-related Fraud*. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another by:

a. any input, alteration, deletion or suppression of computer data,

b. any interference with the functioning of a computer or system, with the intent of procuring, without right, an economic benefit for oneself or for another. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

säännös, joka tuli rikoslakiin kokonaisuudistuksen ensimmäisen vaiheen yhteydessä ja jota on muutettu lailla 602/1997,[160] on seuraavanlainen:

> Joka, hankkiakseen itselleen tai toiselle oikeudetonta taloudellista hyötyä,
> 1) käyttää maksuvälinettä ilman maksuvälineen laillisen haltijan lupaa, lupaan perustuvan oikeutensa ylittäen tai muuten ilman laillista oikeutta tai
> 2) luovuttaa maksuvälineen tai maksuvälinelomakkeen toiselle saattaakseen sen ilman laillista oikeutta käytettäväksi,
>
> on tuomittava *maksuvälinepetoksesta* sakkoon tai vankeuteen enintään kahdeksi vuodeksi. (19.6.1997/602)
>
> Maksuvälinepetoksesta tuomitaan myös se, joka tilin katteen tai sovitun enimmäisluottorajan ylittäen väärinkäyttää 1 momentissa tarkoitettua maksuvälinettä ja siten aiheuttaa toiselle taloudellista vahinkoa, jollei hänellä maksuvälinettä käyttäessään ollut aikomus viipymättä korvata vahinko.

Myös maksuvälinepetoksen törkeä ja lievä tekomuoto on kriminalisoitu.[161] Maksuvälinepetos on kaikissa muodoissaan virallisen syytteen alainen rikos. Vastaavia säännöksiä ei rikoslaissa ollut ennen rikoslain kokonaisuudistuksen ensimmäisen vaiheen toteutumista.

Huolimatta siitä, että kriminalisointi sinänsä on uusi, ei säännöksellä laajennettu rangaistavuuden alaa; aikaisemmin nykyään maksuvälinepetoksiksi katsottavat teot käsiteltiin useimmiten petoksina mutta joskus myös varkauksina, kavalluksina, väärennyksinä tai varastetun tavaran kätkemisinä.

Luvun 11 §:ssä (sellaisena kuin se on laissa 514/2003) kriminalisoidaan maksuvälinepetoksen valmistelu seuraavasti:

> Joka maksuvälinepetoksen tekemistä varten
>
> 1) valmistaa, tuo maahan, hankkii, vastaanottaa tai pitää hallussaan maksuvälinelomakkeen tai
> 2) valmistaa, tuo maahan, hankkii, vastaanottaa, pitää hallussaan, myy tai luovuttaa erityisesti maksuvälinelomakkeen valmistamiseen soveltuvan välineen tai tarvikkeen taikka erityisesti tietoverkoissa tapahtuvaan maksuliikenteeseen soveltuvan tallenteen, ohjelmiston, välineen tai tarvikkeen,

---

[160] HE 38/1997.

[161] RL 37:9: Jos maksuvälinepetoksessa (1) aiheutetaan huomattavaa tai erityisen tuntuvaa vahinkoa tai (2) rikoksentekijä on rikoksen tekemistä varten tehnyt tai teettänyt maksuvälinelomakkeita, joista rikoksessa käytetty maksuväline on valmistettu, taikka rikos muuten tehdään erityisen suunnitelmallisesti ja maksuvälinepetos on myös kokonaisuutena arvostellen törkeä, rikoksentekijä on tuomittava törkeästä maksuvälinepetoksesta vankeuteen vähintään neljäksi kuukaudeksi ja enintään neljäksi vuodeksi.

RL 37:10: Jos maksuvälinepetos, huomioon ottaen tavoitellun hyödyn tai aiheutetun vahingon määrä taikka muut rikokseen liittyvät seikat, on kokonaisuutena arvostellen vähäinen, rikoksentekijä on tuomittava lievästä maksuvälinepetoksesta sakkoon.

on tuomittava *maksuvälinepetoksen valmistelusta* sakkoon tai vankeuteen enintään yhdeksi vuodeksi.

Valmistelua koskevaa säännöstä luettaessa kiinnittyy huomio säännöksen nykyaikaisuuteen: tietoverkoissa tapahtuva kaupankäynti on erityisesti otettu huomioon. Säännöksen asiallinen sisältö on edelleen suunnilleen sama kuin vuoden 1997 muutoksen jälkeen; vuoden 2003 muutokset johtuvat Euroopan unionin neuvoston 28.5.2001 hyväksymästä puitepäätöksestä muihin maksuvälineisiin kuin käteisrahaan liittyvien petosten ja väärennysten torjunnasta. Puitepäätöksen vaatimusten täyttämiseksi 11 §:n 2 kohtaan lisättiin tekotavoiksi myyminen ja luovuttaminen sekä tietoverkoissa tapahtuvaan maksuliikenteeseen soveltuvat välineet ja tarvikkeet.[162]

Maksuvälinepetossäännöstön ajanmukaisuus[163] korostuu, kun tarkastellaan vuoden 1997 uudistuksessa sisältönsä saanutta 12 §:n määritelmäsäännöstä:

> Tässä luvussa tarkoitetaan
> *1) rahalla* seteleitä ja metallirahoja, jotka Suomessa tai muussa maassa ovat virallisesti käypiä maksuvälineitä;
> *2) maksuvälineellä* pankki-, maksu- tai luottokorttia, shekkiä tai muuta välinettä taikka tallennetta, jolla voidaan suorittaa maksuja, tilinostoja tai tilisiirtoja tai jonka käyttäminen on välttämätön edellytys mainittujen suoritusten tekemiseksi; sekä
> *3) maksuvälinelomakkeella* painettua maksuvälineeksi täydennettävää lomaketta, jota ei pidetä yleisön vapaasti saatavissa, taikka sellaista korttia tai korttiaihiota, josta voidaan valmistaa maksuväline.
> Mitä tässä luvussa säädetään maksuvälineestä, sovelletaan myös julkisen valvonnan alaisen luottolaitoksen talletuksesta antamaan vastakirjaan tai muuhun saamistodisteeseen.
> Mitä tässä luvussa säädetään rahasta, sovelletaan seteleihin ja metallirahoihin myös ennen niiden liikkeelle laskua. (17.3.2000/298)[164]

Maksuvälineen käsite on aikaisempaan lakiin verrattuna laajennettu nimenomaisesti käsittämään myös erilaisten suoritusten tekemiseen soveltuva tallenne. Kun vuoden 1991 laki puhui muusta pankki-, maksu- tai luottokorttiin tai shekkiin rinnastettavasta välineestä, on epiteetti ”rinnastettava” jätetty uudesta säännöksestä pois. Näin on pyritty ratkaisuun, joka kattaisi kaikki kuviteltavis-

---

[162] HE 2/2003, s. 17 s.

[163] Jos tekstistä on havaittavissa sellaista suhtautumista nyt käsiteltävään säännöstöön, joka ei vaikuta objektiiviselta, saattaa se osaksi johtua siitä, että valmistelin oikeusministeriössä työskennellessäni muutoksia koskevan hallituksen esityksen 38/1997 vp. Valmistelu tapahtui työryhmässä, johon ohellani kuuluivat rikosylikonstaapeli Timo Laine keskusrikospoliisista, turvallisuuspäällikkö Antti Mustonen Luottokunnasta ja yksikön päällikkö Lauri Pesonen Setec Oy:stä.

[164] Kolmas momentti säädettiin tarkoituksin mahdollistaa puuttuminen euron väärentämiseen jo ennen kuin siitä tuli käypä maksuväline.

sa olevat maksuvälineet säätämishetkellä ja myös ainakin jonkin aikaa tulevaisuudessa.

Säännöstön uudistaminen sai alkunsa käytännön tarpeista ja konkreettisena uudistuksen käynnistäjänä oli edellä väärennyksen yhteydessä kuvattu puhelukorttitapaus. Keskusrikospoliisi teki oikeusministeriölle esityksen selventäviin lainsäädäntötoimiin ryhtymisestä ja asia otettiin lainvalmisteluosastolle pikaisen valmistelun kohteeksi.

Aikaisemman lain mukaan maksuvälinelomakkeella tarkoitettiin mm. maksuvälineeksi täydennettävää korttia, josta ilmeni maksavan raha- tai rahoituslaitoksen nimi tai muu tunnus ja jota ei pidetty vapaasti yleisön saatavissa. Nämä vaatimukset rajoittivat aivan liikaa maksuvälinepetoksen valmistelua koskevan säännöksen soveltamista, sillä rikolliset valmistivat erilaisia maksukortteja – joko magneettijuovakortteja tai prosessorilla varustettuja niin sanottuja sirukortteja – sellaisille blankokorteille, joihin ei ollut merkitty mitään tunnuksia. Tällaisten korttiaihioiden hallussapito tai hankkiminen ei siis voinut tulla maksuvälinepetoksen valmisteluna kysymykseen.

Maksuväline

Määritelmäsäännöksen 1 momentin 2 kohdan mukaan maksuvälineellä tarkoitetaan mitä tahansa välinettä tai tallennetta, jolla voidaan suorittaa maksuja, tilinostoja tai tilisiirtoja.[165] Tallenteella tässä yhteydessä ymmärretään mitä tahansa tallennetta eli tietovälineelle kiinnitetyn datan ja datan edustaman informaation muodostamaa kokonaisuutta, jolloin datalla tarkoitetaan niitä materiaalisia merkkejä (kirjainmerkkejä, rautahiukkasia, painaumia), jotka kulloisenkin tietovälineen (paperiarkki, tietokonelevyke, CD-levy) laadun mukaan järjestettyinä edustavat tietyn sanoman sisältöä.[166]

Väline tai tallenne voi myös olla maksun, tilinoston tai tilisiirron tekemisen välttämätön edellytys niin, että se edustaa suorituksen onnistumisen edellyttämää lisäinformaatiota. Tällaista informaatiota ovat perustelujen mukaan[167] esimerkiksi erilaiset identifioimiskeinot, joilla maksuvälineen käyttäjä kytketään maksu- tai muuhun tapahtumaan. Erilaisten korttien käyttämiseen liittyvät ns. PIN (Personal Identification Number) -koodit, tietoverkoissa tapahtuvaan kaupankäyntiin tarkoitetut sähköiset tunnisteet ja tietokoneen avulla tapahtuvaan pankkipalvelujen käyttämiseen kuuluvat asiakasnumerot ja salasanat ovat tyypillisiä tällaisia identifioimiskeinoja, joiden rinnastaminen niihin välineisiin ja tallenteisiin, joilla varsinaiset suoritukset tehdään, on nähty perustelluksi.

---

[165] Ks. Nuotio, Rikosoikeus, s. 1195 s. Nuotio tyytyy lähinnä lainaamaan hallituksen esitystä.
[166] HE 38/1997, s. 4. Vrt. myös, mitä olen edellä lausunut tallenteesta erityisesti RL 33:6:n tarkoittamassa mielessä.
[167] HE 38/1997, s. 5.

Aikaisemman säännöksen perustelujen mukaan[168] maksuvälineen käsite kattoi myös ”kaikki joko ihmisen tai koneen luettavissa olevat kortit tai muut tunnisteet, joita käyttämällä voidaan määrätä tilillä olevista varoista taikka sovituin luottoehdoin tapahtuvaa tiliveloitusta vastaan ostaa erilaisia hyödykkeitä tai palveluksia”. Toisin sanoen maksuvälineellä tarkoitettiin ”kaikkia todistuskappaleita, joita tavaroiden vaihdannassa ja palvelusten tarjonnassa yleisesti käytetään maksuna jostakin suorituksesta tai suorituksista yleensä”. Tätä perusteluissa olevaa määritelmää hyvin laajentavasti tulkiten olisi ehkä voitu voittaa suurikin osa niistä vaikeuksista, joita tietotekninen kehitys oli tuonut mukanaan, mutta lain sanamuodosta olisi silloin ajauduttu vaarallisen etäälle.

Maksuvälinelomake

Maksuvälinelomakkeella tarkoitetaan määritelmäsäännöksen 1 momentin 3 kohdan mukaan muun muassa korttia tai korttiaihiota, josta voidaan valmistaa maksuväline. Niin kuin edellä on jo mainittu, erona aikaisempaan lakiin on se, että enää ei edellytetä korttien olevan painettuja tai niiden saatavuuden olevan rajoitettua. Perusteluissa nimenomaan todetuin tavoin[169] toimintakelpoisia maksukortteja on täysin mahdollista valmistaa vapaasti kaupan olevista aineksista. Täysin tunnuksettomille korteille informaatiota kiinnittämällä voidaan saada aikaan maksuvälineitä, jotka automaattikäytössä eivät millään tavoin poikkea sellaisista korteista, joihin on painettu vaikkapa rahoituslaitoksen tunnus.[170]

Tallenne tai ohjelmisto

Maksuvälinepetoksen valmistelua koskevassa säännöksessä mainitaan paitsi maksuvälinelomake ja sellaisen valmistamiseen soveltuva väline tai tarvike myös tietoverkoissa tapahtuvaan maksuliikenteeseen soveltuva tallenne tai ohjelmisto. Perustelujen mukaan[171] tyypillinen tallenne voisi olla sellainen sähköinen tunniste (digital certificate) eli elektroninen, henkilökohtainen identifioimiskeino, joka on luotto- tai rahoituslaitoksen digitaalisesti allekirjoittama ja jolla tunnisteen haltija liitetään maksutapahtumaan. Toisaalta – edelleen perustelujen mukaan – tunnisteen ei tarvitse välttämättä olla olemassa valmiina tallenteena vaan se voidaan luoda yksittäistä maksutapahtumaa varten käyttämällä siihen tarkoitettua ohjelmistoa. Tällaisen tunnisteen tai sen luomiseen soveltuvan ohjelmiston valmistaminen tai hankkiminen on täysin verrattavissa esimerkiksi maksukorttipohjan hankkimiseen tai valmistamiseen.

---

168 HE 66/1988, s. 148 s.
169 HE 38/1997, s. 5.
170 Ks. myös Nuotio, Rikosoikeus, s. 1201.
171 HE 38/1997, s. 3.

Maksuvälinepetos tietotekniikkarikoksena

Useissa tilanteissa maksuvälinepetoksena tai sen valmisteluna rangaistava menettely ei ole luokiteltavissa tietotekniikkarikokseksi. Kuitenkin niissä tapauksissa, joissa maksuväline esitetään tietokoneohjatulle automaatille tai rikoksen tekemisessä muutoin käytetään tietojärjestelmää, menettely yleensä täyttää tietotekniikkarikoksen määritelmän tunnusmerkit. Tällaisissa tapauksissa lähes poikkeuksetta toteutuu myös tietojenkäsittelypetoksen tunnusmerkistö, mutta tällöin on sovellettava *lex specialis derogat legi generali* -sääntöä ja käsiteltävä tekoa maksuvälinepetoksena.

Edellä on tietojenkäsittelypetoksesta puhuttaessa mainittu Euroopan neuvoston raportista esimerkkinä datan tai ohjelmiston syöttämisestä toisaalta virheellisen datan syöttäminen ja toisaalta virheettömän datan oikeudeton syöttäminen, joista ensin mainitun voi toteuttaa anastetun maksuvälineen käyttäminen ja jälkimmäisen oman pankkikortin käyttäminen luottoraja tai saldo ylittäen. Nämä ovatkin yleistäen ne tilanteet, joissa maksuvälinepetosta voidaan pitää tietotekniikkarikoksena: teolta on edellytettävä sellaista sähköiseen tietojenkäsittelyyn puuttumista, jonka seurauksena tietojenkäsittelyn lopputulos vääristyy.

Kun rikoksentekijä esitettyään oikeudettomasti toiselle kuuluvan maksuvälineen suorituksia tuottavalle automaatille syöttää siihen välineen (kortin) oikean haltijan tunnistetiedot (PIN-koodin), on tästä väärien tietojen syöttämisestä seurauksena, että hän tietojenkäsittelyn lopputuloksen vääristymisen johdosta saa oikeudettomasti rahaa tai palveluja ja näin aiheuttaa toiselle vahinkoa.

Maksuvälinepetoksen täyttyminen

Niin kuin edellä tietojenkäsittelypetosta käsiteltäessä on havaittu, on lainsäätäjän tarkoituksena ollut, että jo järjestelmän käyttäjäkontrollin läpäiseminen toiselle kuuluvaa tunnistetietoa käyttämällä on tietojenkäsittelypetossäännöksessä tarkoitettua väärän tiedon syöttämistä. Maksuvälinepetos täyttyy tietojenkäsittelypetosta aikaisemmassa vaiheessa: lainkohdan alkuperäisten perustelujen mukaan[172] rikos täyttyy heti maksuvälinettä käytettäessä, esimerkiksi esitettäessä se tietoja käsittelevälle automaatille. Kenenkään erehdyttäminen tai erehtyminen ei ole välttämätöntä eikä rikoksen täyttyminen edellytä vaihdantatoimen onnistumista. Ei ole välttämätöntä, että automaatti antaa kortin esittäjälle rahaa, polttoainetta, puhelinpalveluja tai muun vastaavan suorituksen. Vahingon aiheutumista ei vaadita vaan pelkkä mahdollisuus vaihdantatoimen aikaansaamiseen riittää.

---

[172] HE 66/1988, s. 150.

Perusteluissa ei täsmennetä, mitä maksuvälineen esittämisellä tarkoitetaan. Onko esittämistä jo maksukortin syöttäminen automaattiin ilman, että edes annetaan koneen kysymää tunnuslukua, vai onko esittämisestä kysymys vasta, kun tunnusluku on annettu (tai yritetty antaa)?

Jos tekijällä ei ole tiedossaan korttiin kuuluvaa tunnuslukua vaan hän lähtee sattumanvaraisesti kokeilemaan erilaisia neljän numeron yhdistelmiä siihen saakka, kunnes automaatti joko hyväksyy tunnusluvun tai (erittäin paljon todennäköisemmin) nielaisee kortin, hän lienee esittänyt maksuvälineen automaatille ja näin muodoin käyttänyt sitä syyllistyen siis maksuvälinepetokseen.[173] Käsitykseni mukaan rikoksen ei voida vielä katsoa täyttyneen ennen tunnusluvun antamista, sillä vasta tunnusluvun – oikean tai arvatun – syöttämisellä syntyy mahdollisuus vaihdantatoimen aikaansaamiseen. Tosin mahdollisuus arvaamistilanteissa on kovin pieni, mutta se on kuitenkin olemassa.

Korkein oikeus on asettunut samalle kannalle jo edellä tietomurron yhteydessä tarkastelemassani äänestysratkaisussaan 1999:110, jonka perusteluissa todetaan muun muassa seuraavaa:

> Rangaistavuuden edellytykseksi ei nyt kysymyksessä olevassa lainkohdassa ole siten asetettu sitä, että varojen nostolle olisi yksittäistapauksessa huomioon otettavaa vaaraa. Rikos täyttyy jo siinä vaiheessa, kun pankkikortti syötetään automaattiin ja automaatille annetaan tunnusluvuksi tarkoitettu lukusarja aikomuksin nostaa kortinhaltijan tililtä varoja.[174]

Käräjäoikeus ja hovioikeus olivat hylänneet syytteen katsoen, että todennäköisyys teon onnistumiseen oli ollut hyvin pieni.[175]

Maksuvälinepetos ja muut rikokset

Toiselle kuuluvan maksuvälineen oikeudeton käyttäminen toteuttaa myös luvattoman käytön tunnusmerkistön. Täyttyneen rikoksen ollessa kysymyksessä maksuvälinepetos syrjäyttää luvattoman käytön, mutta kun kysymyksessä on

---

[173] Aikaisemman lain mukainen oikeuskäytäntö tulkitsi usein oikeudettomat pankkiautomaattinostot anastusrikoksiksi. Usein katsottiin kuitenkin, että mahdollisuudet sattumanvaraisesti tunnuslukua kokeilemalla onnistua anastuksen suorittamisessa olivat niin olemattomat, ettei teko ollut edennyt edes kelvollisen yrityksen asteelle.

[174] Vähemmistöön jäänyt jäsen lausui seuraavaa: ”Rikoslain 37 luvun maksuvälinerikoksia koskevissa lainvalmistelutöissä todetaan näiden rikosten kriminalisoinnilla pyrittävän ensisijaisesti turvaamaan maksuliikenteen varmuutta ja turvallisuutta. Tämän tavoitteen toteuttaminen ei edellytä rangaistuksen tuomitsemista sellaisesta menettelystä, jolla tavoitellun hyödyn saaminen ei ole käytännöllisesti katsoen mahdollista. A ei ole tuntenut kysymyksessä olevan pankkikortin tunnuslukua. Näissä olosuhteissa rahojen nostamisen onnistumismahdollisuus on ollut erittäin epätodennäköistä. Tämän vuoksi katson, ettei A ole syyllistynyt maksuvälinepetokseen.”

[175] Ks. Tapani, Kommentti, jossa arvioidaan KKO:n kantaa hieman kriittiseen sävyyn.

edellä kuvattu menettely – pelkkä kortin syöttäminen automaattiin – voitaneen tekoa arvioida luvattoman käytön yrityksenä. Tällöin luvattoman käytön kohteena olisivat itse asiassa sekä maksuväline että asianomainen tietojärjestelmä; tietojärjestelmä ryhtyy tunnistamaan tekijää heti maksuvälineen tultua syötetyksi ja ennen tunnusluvun antamista kysymällä tunnuslukua.

Nähdäkseni tekijän syyksi olisikin luettava nimenomaan tietojärjestelmään kohdistuneen luvattoman käytön yritys, sillä maksuvälinepetoksen yrityksen kriminalisoimatta jättämisestä voitaneen päätellä, että *maksuvälineeseen* kohdistunutta käyttöyritystä ei ole tarkoitettu saattaa rangaistusuhan alaiseksi; maksuvälinepetoksessahan on 37 luvun 8 §:n 1 momentin 1 kohdan tapauksissa aina kysymys ilman laillista oikeutta tapahtuvasta käyttämisestä. Asianomistaja, jonka etuja näin suojattaisiin, olisi toinen: maksuvälineen oikean haltijan asemesta tietojärjestelmän omistaja.

Lainkohdan alkuperäisten perustelujen mukaan[176] maksuvälinepetos ensimmäisessä momentissa tarkoitettuna oikeudettomana käyttönä ilmenee usein joko varkaus-, kavallus-, kätkemis- tai väärennysrikoksen yhteydessä. Tällöin olisi sovellettava rikosten yhtymistä koskevia sääntöjä; näin mm. silloin, kun anastetun tai kätketyn pankki- tai maksukortin käyttö edellyttää tunnuskoodin esittämistä. Väärennyksen ja maksuvälinepetoksen keskinäinen suhde määräytyisi samoin kuin väärennyksen ja petoksen suhde eli kummankin tunnusmerkistön toteutuessa tekijä tulisi tuomita sekä maksuvälinepetoksesta että väärennysrikoksesta.

Jos tekijä muuttaa pankki- tai maksukortin magneettijuovalla tai niin sanotun älykortin mikroprosessorissa olevia tietoja ja käyttää näin väärentämäänsä korttia petollisessa tarkoituksessa, on hän maksuvälinepetoksen ohessa syyllistynyt tietotekniseen väärennykseen, sillä niin magneettijuova kuin mikroprosessorikin niihin kiinnitettyine informaatioineen ovat sellaisia tietoteknisiä tallenteita, jotka tulevat kysymykseen väärennysrikoksen kohteiksi kelpaavina todistuskappaleina. Tällaisessakin tilanteessa tekijä siis tulee tuomita sekä maksuvälinepetoksesta että väärennysrikoksesta.

Maksuvälinepetossäännöksen toisen momentin tarkoittama menettely voi tulla arvioitavaksi tietotekniikkarikoksena silloin, kun rikoksentekijä omaa automaattikorttiaan käyttäessään jollain tavoin petollisesti hyödyntää automaatin toimintaa ohjaavan järjestelmän ominaisuuksia, esimerkiksi niin sanottua *off line* -tilaa, jolloin järjestelmä ei kykene tarkistamaan, onko pankkitilillä nostoa vastaavaa katetta. Menettely on tietysti mahdollista myös toisen maksuvälinettä oikeudettomasti käytettäessä.

Off line -tilan hyväksikäyttäminen on sellaista tietojenkäsittelyyn puuttumista, että se vääristää tietojenkäsittelyn lopputuloksen, ja näin ollen täyttäisi myös

---

[176] HE 66/1988, s. 152.

tietojenkäsittelypetoksen objektiivisen tunnusmerkistön. Huomattakoon, että ensimmäisestä momentista poiketen toisen momentin tunnusmerkistöön kuuluu myös vahingon aiheutuminen, joten täyttymisaste tässä suhteessa on sama kuin tietojenkäsittelypetoksen kohdalla. Säännöksen perustelujen mukaan[177] vahinko on katsottava syntyneeksi heti katteen tai luottorajan ylityksen tapahduttua.

Maksuvälinepetos ja petos

Lain perusteluista ei löydy vastausta siihen kysymykseen, miksi 37 luvun 8 §:n 1 momentin 1 kohdassa tarkoitetun maksuvälinepetoksen täyttymispiste on varhaisempi kuin petoksessa. Menettely, joka petoksena arvioitaessa tulisi rangaistavaksi yrityksenä, katsotaan maksuvälinepetoksena täytetyksi teoksi. Toisaalta yritysasteelle jäänyt maksuvälinepetos jää ainakin *tämän* rikoksen yrityksenä rankaisematta – esimerkiksi edellä kuvattu tilanne, jossa pankkikortti syötetään automaattiin ryhtymättä vielä muihin toimenpiteisiin.

Petos- ja maksuvälinepetossäännöksillä suojellut intressit eivät liene niin erilaisia, että ne kaipaisivat erilaista suojaa. Rikoslain kokonaisuudistuksen ensimmäistä vaihetta koskevassa hallituksen esityksessä todetaan 37 luvun perusteluissa[178] maksuvälinepetosta koskevan ehdotuksen toteuttamisen merkitsevän rangaistussääntelyn tiukentamista nimenomaan laittoman maksuvälinekaupan ja anastettuihin maksuvälinelomakkeisiin ryhtymisen osalta sekä samalla edistävän oikeuskäytännön yhtenäistämistä ja aikaisempaa oikeuskäytäntöä rasittavien rajanvetovaikeuksien poistamista.

Jäljempänä perusteluissa syyteoikeuden järjestelyistä puhuttaessa – maksuvälinepetos on kaikissa muodoissaan virallisen syytteen alainen – viitataan maksuliikenteen turvallisuuden yhteiskunnalliseen merkitykseen. Ehkäpä juuri yleinen etu on katsottava siksi argumentiksi, jolla ankarampaa suhtautumista maksuvälinepetoksena arvioitavaan menettelyyn voidaan perustella.

Kriminalisoinnin tarpeellisuus

Pelkästään tietotekniikkarikoksia ajatellen tuntuu maksuvälinepetosta koskeva erityiskriminalisointi jokseenkin tarpeettomalta; siksi hyvin 36 luvun 1 §:n 2 momentti kattaisi tietotekniikkarikoksiksi katsottavat maksuvälinepetokset. Kritiikin voisi ulottaa vielä pitemmällekin samalla tavoin kuin olen tehnyt petosrikosta käsitellessäni: onko ylipäänsä ollut tarkoituksenmukaisinta säätää automaattiseen tietojenkäsittelyyn kohdistuvista rikoksista yhdistämällä niitä koskevia tunnusmerkistöjä joskus väkinäiseltäkin tuntuvalla tavalla ns. perinteisiin rikostunnusmerkistöihin.

---

[177] HE 66/1988, s. 151.
[178] HE 66/1988, s. 144.

Kun tällainen linja kuitenkin on valittu ja kun lisäksi sinänsä ehdottoman käyttökelpoinen maksuvälinepetossäännös on säädetty, ei ole ainakaan helposti kuviteltavissa, että tietotekniikkarikoksiksi luettavat maksuvälinepetoksen tunnusmerkistön toteuttavat menettelyt arvioitaisiinkin jonkin muun, lähinnä tietojenkäsittelypetosta koskevan säännöksen valossa. Sitä paitsi tämänhetkinen sääntely on hyvin nykyaikaista ja kattavaa ja sellaisena kansainvälisestikin tarkasteltuna varsin edistyksellistä.

Tosin kansainvälisesti tarkasteltuna on maksuvälinepetoksen erillinen kriminalisoiminen poikkeuksellista mutta ei sentään ainutlaatuista; tällaisia kriminalisointeja sisältyy esimerkiksi Italian, Japanin ja Espanjan lainsäädäntöön.[179] Näiden säännösten joukossa omana vähemmistönään ovat vielä suomalaista säännöstä vastaavat kriminalisoinnit, joissa rangaistavuus on nimenomaisesti ulotettu kattamaan myös tekijälle itselleen kuuluvan maksuvälineen väärinkäyttämiset.[180]

Euroopan neuvoston raportissa maksuvälinepetoksiksi luokiteltavia menettelyjä käsitellään tietojenkäsittelypetosta koskevan suosituksen perusteluissa pyrkimättäkään muodostamaan niistä erillistä kategoriaa.[181] Myös *Sieber* tarkastelee pankkiautomaattien väärinkäyttötilanteita nimenomaan petoksina.[182]

3.3 VAHINGONTEKO (RL 35:1)

Vahingontekoa koskeva rikoslain 35 luvun 1 §:n säännös tuli sekin nykymuotoisena voimaan vuoden 1991 alusta lukien:

> Joka oikeudettomasti hävittää tai vahingoittaa toisen omaisuutta, on tuomittava *vahingonteosta sakkoon* tai vankeuteen enintään yhdeksi vuodeksi.
>
> Vahingonteosta tuomitaan myös se, joka toista vahingoittaakseen oikeudettomasti hävittää, turmelee, kätkee tai salaa tietovälineelle tallennetun tiedon tai muun tallennuksen.

Luvun 2 ja 3 §:ssä säädetään törkeästä ja lievästä vahingonteosta.[183] Viidennen pykälän rajoitussäännöksen mukaan luvun säännökset väistyvät, jos teosta on

---

[179] Italian osalta ks. Lanzi, s. 428; Japanin osalta Yamaguchi, s. 435 ja Espanjan osalta Gutiérrez Francés, s. 569.

[180] Ks. Durham, s. 108.

[181] Ks. EN:n raportti 89, s. 28.

[182] Sieber, Handbook, s. 5 ss.

[183] RL 35:2: Jos vahingonteolla aiheutetaan (1) erittäin suurta taloudellista vahinkoa, (2) rikoksen uhrille tämän olot huomioon ottaen erityisen tuntuvaa vahinkoa taikka (3) historiallisesti tai sivistyksellisesti erityisen arvokkaalle omaisuudelle huomattavaa vahinkoa ja vahingonteko on myös kokonaisuutena arvostellen törkeä, rikoksen tekijä on tuomittava törkeästä vahingonteosta vankeuteen vähintään neljäksi kuukaudeksi ja enintään neljäksi vuodeksi.

muualla laissa säädetty yhtä ankara tai ankarampi rangaistus. Tavallinen ja lievä vahingonteko ovat kuudennen pykälän mukaan asianomistajarikoksia kohdistuessaan yksityiseen omaisuuteen.

Aikaisempi vahingontekorikoksia koskenut sääntely rakentui ajatukselle omaisuuden fyysisestä vahingoittamisesta.[184] Näin ollen oli vähintäänkin tulkinnanvaraista, voitiinko vanhan lain vahingontekoa koskevia säännöksiä soveltaa esimerkiksi silloin, kun vahinko aiheutettiin turmelemalla tai muuntamalla tietojärjestelmään magneettisesti tai muulla sellaisella tavalla tallennettua tietoainesta ilman, että itse tietovälinettä fyysisesti vahingoitettiin.[185]

Voidaan perustellusti esittää erilaisia mielipiteitä siitä, onko tällainen tietovahingon aiheuttaminen siinä määrin rinnastettavissa perinteiseen vahingontekoon, että sen kriminalisointi on luontevasti tehtävissä samassa säännöksessä esinevahingon aiheuttamisen kanssa. Tallennettuun informaatioon kohdistuva, 35 luvun 1 §:n 2 momentissa tarkoitettu hävittämis-, turmelemis-, kätkemis- tai salaamistoimi ei vielä sellaisenaan välttämättä aiheuta sellaista havaittavissa ja arvioitavissa olevaa konkreettista vahinkoa, jollainen on seurauksena vaikkapa tietokoneen näyttöruudun rikkomisesta.

Vahingonteon kohde

Lainkohdan teko-objekteja ovat ”tietovälineelle tallennettu tieto tai muu tallennus”.[186] Tiedolla tässä lienee ymmärrettävä informaatiota – lainkohdan perusteluissa sanotaan teon kohteena voivan olla pelkkä tallennettu tieto, esitys tai muu tallennettu sisältö. Tallennuksella puolestaan perustelujen mukaan tarkoitetaan periaatteessa kaikenlaista tiedon tai esityksen taikka muun kohteen tallennettua sisältöä. Myöhemmin tosin täsmennetään tallennetulla tiedolla tarkoitettavan niin tiedon asiasisältöä kuin asiasisältöä viestittäviä merkkejäkin eli niin sanottua dataa.[187]

RL 35:3: Jos vahingonteko, huomioon ottaen vahingon vähäisyys tai muut rikokseen liittyvät seikat, on kokonaisuutena arvostellen vähäinen, rikoksentekijä on tuomittava lievästä vahingonteosta sakkoon.

184 Vahingontekoa koskeva yleissäännös oli rikoslain 35 luvun 3 §:ssä: ”Sellaisesta tahallisesta ja ilman laillista oikeutta tehdystä toisen irtaimen tahi kiinteän omaisuuden hävittämisestä tahi vahingoittamisesta, josta muualla laissa ei ole säädetty, tuomittakoon syyllinen (enintään viidensadan markan) sakkoon taikka vankeuteen korkeintaan kuudeksi kuukaudeksi. (1 mom.) Jos vahinko on vähäinen; harkitkoon tuomari, onko muuta kuin vahingonkorvaus tuomittava. (2 mom.)”

185 Ks. HE 66/88, s. 122.

186 Ks. Majanen, Rikosoikeus, s. 1148, jossa ei kuitenkaan säännöksen perustelujen lainaamista laajemmalti pohdita teko-objektin luonnetta ja olemusta.

187 Ks. HE 66/1988, s. 125.

Data teko-objektina

Olkoon itse tieto tai tiedon sisältö – informaatio – sitten tallennettua tai tallentamatonta, se sinänsä on joka tapauksessa immateriaalista ja sen rinnastaminen teko-objektina materiaaliseen ei ole ongelmatonta. Materiaalista on informaatiota kantava data ja se tietoväline, jolle data on kiinnitetty. Informaation muuttaminen ei voi tapahtua dataa muuttamatta, joten tosiasiallinen teko-objekti on siis joka tapauksessa data, informaatiota edustavat merkit. Näin ajatellen voidaan ”tietovahinko” ymmärtää konkreettisemmin, mutta silloin etäännytään lain sanamuodosta, joka asettaa nimenomaan tiedon – tarkemmin siis informaation – teon kohteeksi.

Rinnastus perinteiseen informaation kantajaan eli asiakirjaan ja sen kantamaan informaatioon kohdistuvaan tekoon selventänee esillä olevaa ongelmaa. Asiakirjan kantaman ja sähköiselle tietovälineelle kiinnitetyn informaation välillä ei periaatteessa ole mitään eroa. Kuitenkaan, jos asiakirja esimerkiksi revitään sellaiseksi silpuksi, että siinä olleen tekstin sisällöstä on täysin mahdotonta saada selkoa, ei yleensä ensimmäiseksi tule mieleen, että teon kohteena ei olisikaan ollut asiakirja vaan siinä olleitten kirjainmerkkien edustama informaatio. Jos mustekynällä kirjoitettu teksti kastelun seurauksena käy mahdottomaksi lukea, ei tilanne itse asiassa oleellisesti poikkea siitä, jos tietokonelevykettä magneettisesti käsittelemällä siihen kiinnitetty data on saatu sotketuksi niin, ettei se enää kanna alkuperäistä tai mitään muutakaan järjellistä informaatiota. Levykkeen käyttökelpoisuus uuden informaation tallentamiseen ei ehkä menettelystä kärsi mutta yhtä lailla on kastellulle paperille mahdollista sen jälleen kuivuttua kirjoittaa uutta tekstiä (tosin paperi ei yleensä tällaisessa tapauksessa enää ole läheskään uuden veroista).

Ongelman käytännöllinen merkitys ei ole suuri: vahingonteko on joka tapauksessa rangaistavaa ja kysymys on vain siitä, sovelletaanko pykälän 1 vai 2 momenttia. Kuitenkaan ei voida pitää tyydyttävänä sitä, että rikoslain säännös on sanamuodoltaan epätäsmällinen.

Tallennus ja tallenne

Se, että 35 luvussa ei käytetä 33 luvun määritelmäsäännöksen sisältämää sanaa ”tallenne”, osoittanee, että tarkoituksena on ollut tehdä ero väärennys- ja vahingontekorikosten teko-objektien välille. Käytännössä kysymyksenasettelut ovat tietoteknisen tallenteen kohdalla hyvin pitkälti yhteneväiset: missä määrin tietoteknisesti ”näkymättömään” muotoon tallennetun informaation hävittäminen tai vahingoittaminen on rinnastettavissa asiakirjan ja siihen kiinnitetyn informaation fyysiseen hävittämiseen tai vahingoittamiseen silloin, kun itse tietovälinettä ei vahingoiteta. Väärennykseen nähden ero on kuitenkin siinä, että – yleensä – todistuskappaleen arvo on juuri sen kantamassa informaatiossa ja informaation oikeudellisessa merkityksessä, kun taas vahingonteon kohdalla teon vaikutukset eivät välttämättä ole yhtä välittömiä.

Ruotsalaisessa lainvalmistelussa on pohdittu kysymystä vahingontekorikoksen objektin luonteesta muun muassa seuraavasti:[188]

> En skadegörande handling kan med hänsyn till sin fysiska karaktär enligt vår (= Datastraffrättsutredningens) uppfattning inte ha ett enbart immateriellt angreppsobjekt. Data kan knappast heller ses som en del av en sak. Data har ingen bestämd rumslig placering utan flyttas vid bearbetningen i en dator mellan olika adresser inom en databärare eller mellan olika databärare. Mest påtaglig är denna fysiska hemlöshet när data överförs i ett datanät och i synnerhet då kommunikationen sker trådlöst. – – Problemet är närmast den rättsliga komplikation som ligger i att man som nu sker subsumerar data under begreppet egendom. – – Enligt vår mening skulle ett betraktande av data som egendom kunna få inte avsedda konsekvenser utanför skadegörelsekapitlet.

Olen jo edellä määritelmäjaksossa kritisoinut ruotsalaista näkemystä datasta jonain kvasimateriaalisena. Selkeän eron tekeminen materiaalisen datan ja immateriaalisen informaation välille helpottaa joka tapauksessa tietovahingon aiheuttamisen käsittävän rikostyypin hahmottamista, oltakoon sitä koskevan säännöksen sijoittelusta sitten mitä mieltä tahansa.

Vahingontekorikoksen luokittelu

Suomalaisen vahingontekosäännöksen perusteluissa ei ole pohdittu kysymystä säännöksen sijoittelusta, vaan lähtökohdaksi on otettu tietovahingon rinnastaminen fyysiseen vahinkoon. Perusteluissa lausutaan seuraavasti:[189]

> Sähköisesti, magneettisesti tai optisesti tallennettu tieto, esitys tai muu sisältö voidaan sitä vastoin hävittää, turmella, salata tai saattaa muuten tulkintakelvottomaksi ilman, että itse tietovälinettä fyysisesti vahingoitetaan. Tästä syystä ehdotetaan, että vahingonteon kohteena voisi olla myös pelkkä tallennettu tieto, esitys tai muu tallennettu sisältö.

Niin kuin edellä jo todettiin, perustelujen mukaan niin tiedon asiasisältö kuin asiasisältöä viestittävät merkitkin voivat olla vahingonteon kohteena – huolimatta siitä, että itse säännöksessä rinnastetaan tietovälineelle tallennettu tieto *muuhun tallennukseen*, mikä *saattaisi* johtaa tarkastelemaan tallennusta informaatioon rinnastettavana immateriaalisena objektina.

Tallennuksella on kuitenkin katsottava tarkoitettavan tallenteen sisällön ohella myös niitä merkkejä, joista tallenne koostuu. Perusteluista ei käy selville, onko näin sanomalla haluttu antaa käsitteelle ”tallennus” jotenkin laajempi merkityssisältö kuin käsitteelle ”tallenne”. Edellä olen määritellyt tallenteen tietovälineelle kiinnitetyn datan ja datan edustaman informaation muodosta-

---

188 SOU 1992:110, s. 209.
189 HE 66/1988, s. 125.

maksi kokonaisuudeksi, jolloin tallenne tarkoittaisi samaa kuin tallennus. Lakiin on jäänyt terminologinen epätäsmällisyys, joka ei välttämättä jää vaille merkitystä ainakaan tilanteissa, joissa joudutaan vetämään rajaa väärennyksen ja vahingonteon tunnusmerkistöjen välille.

Edelleen perusteluissa todetaan vahingontekona voitavan pitää jo sellaista tallennuksen vahingoittamista, joka ei tosin estä ymmärtämästä tallennettua sisältöä mutta aiheuttaa esimerkiksi sellaisia kirjoitus- tai muita virheitä, joiden vuoksi tallennusta ei voida käyttää alkuperäiseen tarkoitukseensa korjauksia tekemättä. Tällaisessa tilanteessa lienee lainkohdassa tarkoitetuista tekotavoista kysymyksessä lähinnä turmeleminen, joka terminä on jossain määrin tulkinnanvarainen. Ilmeisesti ei ole edellytettävä sellaisen vahingon syntymistä, joka ei ole enää korjattavissa – näin ainakin perusteluista on pääteltävissä. Verbi ”vahingoittaa” olisi ehkä ollut yksiselitteisempi.

Antamalla tallennuksen käsitteelle edellä kerrottu niin informaation kuin datankin kattava merkitys päädytään siihen, että vahingonteko voidaan luokitella sekä data- että informaatiorikokseksi. Luokittelun käytännöllinen merkitys jää vähäiseksi, mutta herättää joka tapauksessa kysymyksen, olisiko säännöksen luonteva sijoituspaikka voinut yhtä hyvin olla rikoslain kokonaisuudistuksen toisessa vaiheessa säädetty uusi tieto- ja viestintärikoksia koskeva 38 luku.

Kun toisaalta informaation vahingoittaminen aina edellyttää myös datan manipuloimista, voidaan säännöksen nykyistä sijoittelua pitää perusteltuna. Eri asia on – niin kuin on jo voitu havaita – että säännös on tunnusmerkistöltään varsin tulkinnanvarainen suhteessa eräisiin muihin tietotekniikkarikoksiin.

Rangaistavuuden edellytykset

Säännöksessä ei edellytetä teon kohteena olevan tallennuksen kuulumista toiselle.[190] Perustelujen mukaan itse tallennuksen omistussuhteen määritteleminen on usein ongelmallista eikä myöskään tallentamiseen käytetyn tietovälineen omistussuhteilla ole ehdotonta vaikutusta siihen, millaista tallennuksen vahingoittamista on pidettävä oikeudettomana. Tästä syystä on pidetty riittävänä sitä, että rangaistavuuden edellytyksenä on toisaalta vahingoittamistarkoitus ja toisaalta se, että teko tapahtuu oikeudettomasti.

Majasen[191] mukaan oikeudettomuus tässä yhteydessä tarkoittaa sitä, että tekijällä ei ollut laillista oikeutta ryhtyä tekoonsa. Teon voi tehdä oikeudenmukaiseksi esimerkiksi loukatun suostumus, hätävarjelu tai pakkotila. Myös viranomaisilla on esimerkiksi poliisilain ja pakkokeinolain nojalla oikeus

---

190 Ks. myös Majanen, Rikosoikeus, s. 1148.
191 Majanen, Rikosoikeus, s. 1149.

voimakeinoja käyttämällä vahingoittaa toisen omaisuutta tietyissä etsintätilanteissa.[192]

Vahingoittamistarkoituksesta puhuessaan *Majanen*[193] toteaa, että jos tekijällä on vain hyvää tarkoittava aikomus parannella tai korjata jotakin tallennusta, ei kysymyksessä ole vahingonteko, vaikka tallennuksen valmistaja kokisikin toiminnan työnsä turmelemiseksi.

Greve katsoo Tanskan vahingontekosääntelyä tietovahingon aiheuttamisen kannalta tarkastellessaan, että esinevahingon aiheuttamista koskeva kriminalisointi subsumoi myös ohjelmistoon (programmellet) kohdistetun vahingonteon, kunhan kohde kuuluu toiselle ja on kiinnitetty fyysiseen esineeseen.[194] Teko-objektina ”programmellet” on kuitenkin hyvin suppeaalainen, joten ainoaksi Greven kannanotosta tehtäväksi johtopäätökseksi jää, että hän näkee tietovahingon syntyvän ensisijaisesti esinevahingon aiheuttamisen kautta.

Vahingoittamisen oikeudettomuutta edellyttää myös Euroopan neuvoston minimilistalla oleva datan tai ohjelmiston vahingoittamista koskeva suositus.[195] Suositellulla säännöksellä suojattavia oikeudellisia intressejä ovat datan ja ohjelmistojen koskemattomuus sekä häiriötön toiminta tai käyttö.[196] Suosituksessa rinnastetaan data ja ohjelmistot aineelliseen omaisuuteen tarkoittamalla saada niille samanlainen suoja tahallisia vahingoittamistoimia vastaan.

Datan hävittäminen (erasure) tarkoittaa datan tuhoamista ja saattamista täydellisen tunnistamattomaksi; vahingoittamisella (damaging) ja huonontamisella (deterioration) ymmärretään datan ja ohjelmistojen informaatiosisältöjen negatiivista muuttamista. Käytön estäminen (suppression of data) tarkoittaa tilannetta, jossa tekijä ohjelmakäskyillä estää käyttöön oikeutettua pääsemästä käsiksi dataan ja sitä käyttämästä.

Myöskään säännössuosituksessa ei nimenomaisesti edellytetä teon kohteen kuulumista toiselle ja termin ”oikeudettomasti” (without right) katsotaankin sisältävän myös tämän elementin, jonka todetaan yleensä esiintyvän aineellisesta omaisuudesta puhuttaessa.

Rikoslain 35 luvun 1 §:n 2 momentin säännös vastaa Euroopan neuvoston säännössuositusta. Turmeleminen tarkoittanee samaa kuin suosituksen ”damaging” ja ”deterioration” ja kätkeminen ja salaaminen merkitsevät samaa kuin ”suppression”.[197]

---

[192] Näin sanoessaan Majanen tarkoittaa vahingonteon oikeudettomuutta yleensä rajautumatta pelkkään tietovahingon aiheuttamiseen. Samat periaatteet soveltuvat epäilemättä myös viimeksi mainittuun, joskin käytännössä tilanteet voivat helposti kovin erityyppisiä.

[193] Majanen, Rikosoikeus, s. 1149.

[194] Greve, s. 34 ss.

[195] Datan tai ohjelmiston oikeudeton hävittäminen, vahingoittaminen, huonontaminen tai käytön estäminen.

[196] EN:n raportti 89, s. 31 ss.

[197] Ks. Majanen, Rikosoikeus, s. 1148 s. Majasen mukaan hävittämistä voi olla tallennetun tiedon saattaminen lopullisesti käyttökelvottomaan muotoon ja turmelemista tallennetun tiedon

EN:n yleissopimus ja vahingonteko

Vahingontekotyyppistä menettelyä tarkoittaa Euroopan neuvoston yleissopimuksen neljäs artikla, jonka sisältö pitkälti muistuttaa Euroopan neuvoston suosituksen vahingontekokohtaa:

> *Datan vahingoittaminen.* Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin säätääkseen kansallisen lainsäädäntönsä mukaisesti rangaistavaksi tahallisen ja oikeudettoman datan vahingoittamisen, tuhoamisen, turmelemisen, muuttamisen ja poistamisen.
>
> Sopimuspuoli voi tehdä varauman, jonka mukaan rangaistavuuden edellytyksenä on, että 1 kappaleessa tarkoitettu teko aiheuttaa huomattavaa vahinkoa.[198]

Artikla tuskin edellyttää meillä lainmuutoksia. Artiklan tämänhetkisessä, vielä epävirallisessa suomennoksessa[199] käytetään sanaa ”data”. Olkoonkin, että sana ”data” ei ole suomea ja että sitä käytettäessä itse asiassa tulisi ottaa huomioon sen monikollisuus, olisi sen nykyistä laajempi käyttö myös lakikielessä järkevää ja parantaisi joidenkin säännösten täsmällisyyttä; nykyisellääänhän ainoat rikoslain säännökset, jossa sana esiintyy, lienevät uusi tietojenkäsittelypetossäännös 36 luvun 1 §:n 2 momentissa sekä datasiirron mainitseva 38 luvun 3 §.[200]

---

asiasisällön muuttaminen toisen sisältöiseksi tai ymmärtämättömäksi taikka sellainen tiedon tai tallenteen vahingoittaminen, joka sinänsä ei estä ymmärtämästä tallennettua sisältöä mutta jonka seurauksena tallennusta ei voida käyttää alkuperäiseen tarkoitukseensa korjauksia tekemättä. *Kätkemisessä* on kysymys tiedon tai tallennuksen saattamisesta käyttäjänsä ulottumattomiin, vaikka se ei merkitsisikään tiedon tai tallennuksen lopullista tuhoamista tai hävittämistä. *Salaamisesta* itsenäisenä tekomuotona on Majasen mukaan kysymys, jos tiedon tai tallenteen sisältöön puuttumatta ei ilmaista, mistä tieto tai tallenne on löydettävissä. Pelkän salaamisen rangaistavuus edellyttää, että salaajalla on oikeudellinen velvollisuus ilmaista salassa oleva tieto tai tallennus. – Huomattakoon, että Majanen edellä selostetuissa määritelmissä käyttää sanoja ”tallennus” ja ”tallenne” ilmeisesti samaa tarkoittavina. Tämä voisi puhua sen käsityksen puolesta, että sanoille on haluttu lakitekstissäkin antaa sama merkityssisältö. – Ruotsalaisessa säännösehdotuksessa (BrB 12:1.2) käytetään sanoja ”den som olovligen utplånar, ändrar eller undertrycker data för automatisk informations-behandling”. Ilmaisun ”ändrar” selitetään kattavan EN:n suosituksen termit ”damaging” ja ”deterioration”. SOU 1992:110, s. 211.

[198] *Article 4. Data interference*.

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, alteration or suppression of computer data without right.

2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

[199] Yleissopimuksen englannin- ja suomenkieliset tekstit ovat tietoverkkorikostyöryhmän mietinnön liitteenä.

[200] Ks. tietoverkkorikostyöryhmän mietintö, jossa ehdotetaan pakkokeinolain 4 luvun 1 §:ään sisällytettäväksi datan määritelmä: ”– – tietoa, joka on tietokoneessa tai muussa vastaavassa tietojärjestelmässä taikka sen tallennusalustalla (data)”.

TCB ja vahingonteko

Lähdin TCB-jutussa hakemaan ennakkoratkaisua vahingontekosäännöksen soveltuvuuden osalta; edellä selostamani syytteen mukaanhan vahingonteko olisi ollut asianomistajien tietojärjestelmiin tallennettujen tietojen oikeudetonta turmelemista ja salaamista, joka oli tapahtunut asentamalla järjestelmiin niin sanottuja takaporttiohjelmia ja muuttamalla olemassa olleita ohjelmia tällaisiksi samoin kuin poistamalla järjestelmien keräämiä lokitietoja.

Käräjäoikeus kuitenkin hylkäsi syytteen ja perusteli hylkäämistä seuraavasti:

> RL 35 luvun 1 §:n 2 momentin mukaan vahingonteosta tuomitaan muun muassa se, joka toista vahingoittaakseen oikeudettomasti hävittää tai turmelee tietovälineelle tallennetun tiedon tai muun tallennuksen. Kuitenkin 5 §:n mukaan tämän luvun säännöksiä ei sovelleta, milloin teosta on muualla laissa säädetty yhtä ankara tai ankarampi rangaistus.
>
> Syytteen 3-kohdasta ilmenevä P:n menettely on luettu hänen syykseen 1-kohdassa luvattomana käyttönä. Kun luvattomasta käytöstä ja vahingonteosta on säädetty yhtä ankarat rangaistukset, tuohon P:n menettelyyn ei ole sovellettava toissijaista vahingontekoa koskevaa säännöstä.

Voi toki olla niin, että syyte oli huonosti laadittu, sillä en tarkoittanut tämän vahingonteoksi kuvaamani menettelyn itsessään toteuttavan luvattoman käytön tunnusmerkistöä. Ajatus oli, että (1) järjestelmiä oli *ylipäänsä* käytetty luvatta ja (2) tuon käyttämisen yhteydessä *erikseen* syyllistytty vahingoittamistahallisuutta – tässä lähinnä *dolus eventualis* -tyyppistä – osoittaneeseen, vahingonteon tunnusmerkistön toteuttavaan menettelyyn.

Valituksessani vaadin myös, että P tuomitaan rangaistukseen vahingonteosta, koska luvattoman käytön ja tietojärjestelmään kohdistuvan vahingonteon kriminalisoinneilla on tarkoitus suojata erilaisia oikeushyviä. Tietojärjestelmään kohdistuvan vahingonteon kriminalisoinnilla suojataan järjestelmän eheyttä ja luottamuksellisuutta, jota loukkaa se, että huomaamattoman järjestelmään pääsyn mahdollistamiseksi asennetaan takaportteja ja poistetaan lokitietoja. Tämän seurauksena järjestelmän haltijalle aiheutuu suoranaista taloudellista vahinkoa.

Vaasan hovioikeus toteaa ensiksi, että käräjäoikeuden päätöksestä ei nimenomaisesti ilmene, onko käräjäoikeus katsonut P:n menettelyn sinänsä täyttävän vahingonteon tunnusmerkistön. Tämän vuoksi hovioikeus ryhtyikin ensin tutkimaan, onko P syytteessä kuvatulla menettelyllään turmellut ja salannut tietojärjestelmiin tallennettuja tietoja. Hovioikeus lausuu perusteluissaan seuraavaa:

> Takaporttien asentaminen ja olemassa olevien ohjelmien muuttaminen sellaisiksi loukkaa sinänsä selkeästi tietojärjestelmän luottamuksellisuutta, koska tietojärjestelmä ja sen sisältämä informaatio ei ole enää vain siihen oikeutettujen käytettävissä. Sama menettely ja lokitietojen poistaminen loukkaa myöskin tietojärjestelmien eheyttä, koska tietojärjestelmän sisältämän informaation ja datan oikeellisuus ja aitous, tai ainakin

korkeamman asteinen varmuus siitä, on menetetty. Tämä pätee varsinkin tilanteessa, jossa pääkäyttäjän oikeudet on oikeudettomasti tietojärjestelmään tunkeutuneen henkilön hallussa. Eheyteen liittyy olennaisesti se, että tietojärjestelmien tietoa ei ole valtuudettomasti muutettu ja että mahdolliset muutokset voidaan todeta kirjausketjussa (loki). Kysymyksessä olevassa lainkohdassa tarkoitettu turmeleminen käsittääkin juuri tiedon muuttamisen kriminalisoinnin. Tämän vuoksi hovioikeus katsoo, että olemassa olevien ohjelmien muuttaminen ja lokitietojen poistaminen täyttää lainkohdan tunnusmerkistön.

Kysymyksenalaiseksi voidaan asettaa se, soveltuuko vahingontekoa koskeva säännös sanamuotonsa puolesta menettelyyn, jossa tietojärjestelmään on muuttamatta olemassa olevaa tallennettua tietoa asennettu takaporttiohjelma ja josta on aiheutunut vain välillistä vahinkoa, kuten tässä tapauksessa. Tiedon käsite on kuitenkin tarkoitettu ymmärrettäväksi laajasti ja tietovahinkoa koskevan säännöksen tarkoituksena on suojata periaatteessa kaikenlaisia tallenteita sellaiselta vahingoittamiselta, joka ei kohdistu itse tietovälineeseen (HE 66/1988 vp. s. 131). Näin ollen rikosoikeudellisen suojan on katsottava koskevan myös tietojärjestelmien ylläpitoon liittyviä ohjelmia ja tietoteknistä dataa aina sen binääriseen esitysmuotoon saakka. Hovioikeus katsoo, että viimeksi mainitun tiedon lähtökohtaiselle poissulkemiselle rikosoikeudellisen suojan ulkopuolelle ei ole olemassa kestäviä perusteita. Tässä mielessä P:n voidaan katsoa muuttaneen tietojärjestelmässä ollutta tietoa. Näin ollen myös takaportin asentamista on etenkin sen käyttötarkoitus ja edellä eheydestä ja luottamuksellisuudesta lausuttu huomioon ottaen pidettävä tietojärjestelmän tiedon turmelemisena.

Lainkohdan esitöissä ei ole tarkemmin määritelty, mitä tekotapana mainitulla salaamisella tarkoitetaan. Oikeuskirjallisuudessa on esitetty, että salaamisessa olisi kysymys tilanteesta, jossa tiedon tai tallenteen sisältöön sinänsä puuttumatta ei ilmaista, mistä tieto tai tallenne on löydettävissä. Pelkän salaamisen rangaistavuus edellyttäisi, että salaajalla on oikeudellinen velvollisuus ilmaista salassa oleva tieto tai tallennus (Heinonen ym. Rikosoikeus 1999 s. 777). Tämä ja jo edellä todettu huomioon ottaen hovioikeus katsoo, että lokitietojen poistamista on pidettävä turmelemisena eikä salaamisena.

Edellä selostetun perusteella hovioikeus katsoo P:n turmelleen tietojärjestelmän tietoja, kun hän on asentanut sinne takaportteja, muuttanut ohjelmia sellaisiksi ja poistanut omaa käyntiään osoittavia lokitietoja. Turmellulla tiedolla on sinällään katsottava olevan tietojärjestelmän omistajalle taloudellista arvoa, koska luottamuksellisuudella ja eheydellä on olennainen merkitys tietojärjestelmien asianmukaisen toimivuuden ja käyttämisen kannalta. Näin ollen P:n menettely täyttää vahingonteon objektiivisen tunnusmerkistön. Vahingontekorikoksia koskevan luvun rajoitussäännöksen esitöistä (HE 66/1988 vp. s. 127) ilmenee, että vahingontekosäännösten on tarkoitettu olevan toissijaisia muihin vahingonteon luontoisia tekoja koskeviin säännöksiin nähden, jos teosta on niissä säädetty yhtä ankara tai ankarampi rangaistus. Luvaton käyttö ei ole vahingonteon luonteinen rikos, joten pelkästään se, että törkeästä luvattomasta käytöstä, johon hovioikeus katsoo P:n syyllistyneen, on säädetty

> ankarampi rangaistus kuin vahingonteosta, ei ole esteenä myös vahingontekosäännöksen soveltamiselle. Hovioikeus katsoo vahingontekosäännöksen tässä tapauksessa syrjäytyvän kuitenkin siitä syystä, että P:n ei ole näytetty vahingoittaneen syytekohdassa 3 mainittujen asianomistajien tietojärjestelmiin tallennettuja tietoja enemmän kuin luvattoman käytön toteuttaminen on edellyttänyt.

Lisäksi hovioikeus katsoo jääneen näyttämättä, että P:n tarkoituksena olisi ollut vahingoittaa toista ja siis lopputuloksenaan päätyy vahingontekoa koskevan syytteen hylkäämiseen.

Hovioikeus kuitenkin asettuu selkeästi sille kannalle, että *objektiivisessa* suhteessa P:n menettely on täyttänyt vahingonteon tunnusmerkistön. Kysymyksessä lienee ensimmäinen ylemmänasteisen tuomioistuimen ratkaisu, jossa otetaan kantaa rikoslain 35 luvun 1 §:n 2 momentin asialliseen soveltamisalaan, ja käsitykseni mukaan hovioikeuden perustelut ovat tässä suhteessa oikeaan osuneet ja vakuuttavat. Turmelemisen käsite on nyt tullut määritellyksi tavalla, joka huomattavasti helpottaa tietovahingon aiheuttamista koskevan säännöksen tulkintaa vastaisuudessa.

Selkeästi oikeana pidän myös hovioikeuden näkemystä rikoslain 35 luvun 5 §:n rajoitussäännöksen tulkinnasta. Kannanotto tähänkin kysymykseen on tärkeä, sillä ei ole mitään syytä olettaa, etteikö samankaltaisia soveltamistilanteita esiintyisi tulevaisuudessakin.[201]

---

[201] Ks. Majanen, Rikosoikeus, s. 1151, jossa Majanen käsittääkseni varsin selkeästi kuvaa, mitä RL 35:5 tarkoittaa, kun hän lausuu vahingonteon voivan sisältyä toiseen rikokseen esimerkiksi murtauduttaessa anastustarkoituksessa johonkin sisälle. Tällöin ei varkauden tai sen yrityksen ohella tuomita erikseen vahingonteosta, ellei omaisuutta ole vahingoitettu enempää kuin varkauden toteuttaminen oli edellyttänyt. Ks. myös Nuotio, Rikosoikeus, s. 1140, jossa lyhyesti käsitellään vahingonteon ja vaaran aiheuttamisen tietojenkäsittelylle välistä konkurrenssitilannetta.

4 Vaaran aiheuttaminen tietojenkäsittelylle (RL 34:9a)

Vaaran aiheuttaminen tietojenkäsittelylle on uusin tietotekniikkarikoksia koskeva kriminalisointi rikoslaissamme. Se poikkeaa oleellisesti edellä käsitellyistä teoista siinä suhteessa, että kysymyksessä on vaarantamisrikos. Rikoslain 34 lukuun 1.12.1999 lukien lisätty uusi 9 a § (951/1999)[202] kuuluu seuraavasti:

> Joka, aiheuttaakseen haittaa tietojenkäsittelylle tai tieto- tai telejärjestelmän toiminnalle,
>
> 1) valmistaa tai asettaa saataville sellaisen tietokoneohjelman tai ohjelmakäskyjen sarjan, joka on suunniteltu vaarantamaan tietojenkäsittelyä tai tieto- tai telejärjestelmän toimintaa taikka vahingoittamaan sellaisen järjestelmän sisältämiä tietoja tai ohjelmistoja, tai levittää sellaista tietokoneohjelmaa tai ohjelmakäskyjen sarjaa taikka
>
> 2) asettaa saataville ohjeen 1 kohdassa tarkoitetun tietokoneohjelman tai ohjelmakäskyjen sarjan valmistamiseen tai levittää sellaista ohjetta,
>
> on tuomittava, jollei teosta ole muualla laissa säädetty ankarampaa tai yhtä ankaraa rangaistusta, *vaaran aiheuttamisesta tietojenkäsittelylle sakkoon* tai vankeuteen enintään kahdeksi vuodeksi.

Säännös kriminalisoi niin sanotun tietokoneviruksen valmistamisen ja levittämisen.[203] Itse asiassa viruksesta puhuttaessa tarkoitetaan vain yhtä säännöksessä tarkoitettujen ohjelmien alalajia, joka kylläkin on yleisin tällainen ohjelmatyyppi.

---

[202] HE 4/1999.

[203] Ks. Lehtonen, Datavirus, jossa Lehtonen lähinnä toistaa hallituksen esityksen tekstiä mutta kertoo myös säännöksen syntyvaiheista. Lehtonen toteaa mm. (s. 45), että lakivaliokunnan mietinnössä ”framkom hård kritik mot propositionen och dess motiveringar” ja kertoo (alav. 9), että lakivaliokunta ”ansåg att man i propositionen inte sakenligt tagit i beaktande de ställningstaganden som framfördes i samband med totalreformen av strafflagen och att man inte motiverat varför man hade frångått dem. Mål för kritiken var också obestämdheten i de begrepp som användes i rekvisiten, framförallt vad gäller de informationstekniska termerna. Frågan gällde om dessa begrepp uppfyllde det krav på bestämdhet som ingår i den straffrättsliga legalitetsprincipen i regeringsformens 6a §. Experterna kritiserade även de föreslagna stadgandena ur yttrandefrihetens synvinkel som hör till grundrättigheterna.” Kirjoituksensa lopussa (s. 52) Lehtonen toteaa, että kysymyksessä oleva osittaisuudistus ”förverkligades beklagtligtvis brådskande och med ett sådant lagförberedande arbete som inte nödvändigtvis var helt slutfört som grund. I motiveringen till propositionen ingick också tendensaktiga drag”. – Lehtosen viimeksi mainittu kritiikki jää perustelemattomaksi. Mitä tulee lakivaliokunnan esittämään ”kovaan kritiikkiin”, on tietysti itse kunkin vapaasti harkittavissa, miten lakivaliokunnan mietinnön tekstiä tulkitsee, mutta itse en valiokunnan mielipidettä, jonka mukaan ”nyt käsiteltävänä olevassa hallituksen esityksessä olisi

Virukset ja muut vahingolliset ohjelmat

Atk-sanakirjan[204] määritelmän mukaan virus on ohjelmaan tai dataan kätketty tuholaisohjelma, joka leviää muihin ohjelmiin ja tietokoneisiin monistamalla itseään siten, että monistetut virukset edelleen monistuvat. Viruksia todetaan olevan useita lajeja, joista eräät paljastumisen vaikeuttamiseksi muuttavat jatkuvasti muotoaan.

Ulkomaisessa kielenkäytössä käytetään usein yleistäen termiä ”virus” tarkoittaen kuitenkin kaikkia vahingollisia ja haitallisia ohjelmia. Virusten ohella muita tyypillisiä puheena olevia ohjelmia ovat esimerkiksi niin sanotut Troijan hevoset, loogiset pommit ja madot. Muun muassa Yhdistyneiden Kansakuntien tietotekniikkarikosmanuaalissa on käsitelty ja myös määritelty näitä käsitteitä.[205]

Suomessa on tällaisista ohjelmista joskus käytetty nimitystä ”tuho-ohjelma” tai ”tuholaisohjelma”, mutta kumpikaan näistä ei ole vakiintunut yleiseen kie-

---

ollut asianmukaista ottaa huomioon mainitut rikoslain kokonaisuudistuksen yhteydessä esitetyt arviot ja kannanotot sekä perustella, miksi niistä on nyt luovuttu” (LaVM 2/1999, s. 2), osaa tulkita erityisen ankaraksi arvosteluksi. Lakivaliokunta toteaa mm., että ehdotettu rangaistussäännös ”täyttää sananvapauden rajoittamiselta edellytetyn lailla säätämisen vaatimuksen sekä täsmällisyys- ja tarkkarajaisuusvaatimuksen. – – Rangaistussäännöksen suojeluobjektina on siten tärkeä yksityinen ja yleinen intressi, jolloin mahdollinen sananvapauden rajoitus on hyväksyttävä perusoikeusjärjestelmän kannalta. – – Valiokunta katsoo ehdotetun säännöksen olevan tarpeellinen, koska voimassa olevat säännökset eivät kata kaikkia ehdotetun tunnusmerkistön mukaisia tekoja. Suhteellisuusvaatimuksen kannalta on myös olennaista, että teon rangaistavuuden edellytyksenä on tekijän tarkoitus aiheuttaa haittaa tietojenkäsittelylle tai tieto- ja telejärjestelmän toiminnalle.” (ss. 2–3)

Lehtosen mukaan lakivaliokunta olisi kritisoinut myös ehdotuksessa käytettyä käsitteistöä. Tältä osin valiokunta toteaa seuraavaa (s. 3): ”Valiokunnan kuulemat asiantuntijat ovat arvostelleet tietokoneviruksen valmistamista ja levittämistä koskevan tunnusmerkistön sanamuotoa ja perusteluiden yksityiskohtia. Ilmeisesti tietotekniikan käsitteistö on jossain määrin täsmentymätöntä ja vakiintumatonta. Myös rikoslainsäädännön kirjoittaminen yleiskielellä vaikeuttaa yhteisymmärryksen löytymistä eri asiantuntijatahojen välillä. Tunnusmerkistöä on vaikea kirjoittaa ehdotettua selkeämmin ja yksinkertaisemmin, koska säännöksessä yhdistyy yleisvaarallisen rikoksen, tekijän tahallisuuden ja tietokoneviruksen määrittelemisen ongelmat.” Itse luen tämän lainauksen niin, että siinä annetaan tunnustusta säännöksen onnistuneesta muotoilusta.

[204] Atk-sanakirja, s. 242.

[205] UN Manual, kohta 69: ”A virus is a series of program codes that has the ability to attach itself to legitimate programs and propagate itself to other computer programs. A virus can be introduced to a system by a legitimate piece of software that has been infected, as well as by the trojan horse method discussed above.”

Kohta 71: ”A worm is similarly constructed to infiltrate legitimate data-processing programs and to alter or destroy the data, but it differs from a virus in that it does not have the ability to replicate itself. In a medical analogy, the worm can be compared to a benign tumour, the virus to a malignant one. – – ”

Kohta 72: ”A logic bomb, also known as a ’time bomb’, is another technique by which computer sabotage can be perpetrated. The creation of logic bombs requires some specialized knowledge, as it involves programming the destruction or modification of data at a specific time in the future. – – ”

lenkäyttöön.[206] Viime vuosina on enenevässä määrin ryhdytty käyttämään termiä ”haittaohjelma”, joka tuntuukin melko onnistuneelta.

Englannin kielessä käytetään jokseenkin yleisesti termejä ”malware” tai ”malicious code” kuvaamaan haitallisia ja vahingollisia ohjelmia. Jäljempänä käyttäessäni termiä ”virus” tarkoitan sillä puhekieltä myötäillen kaikkia säännöksessä tarkoitettuja haitallisia ja vahingollisia ohjelmia.

Varsinaisille virusohjelmille on ominaista se, että ne eivät kykene toimimaan itsenäisesti vaan tarvitsevat aina toisen ohjelman isännäkseen. Ne voivat levitä itsestään tietokoneessa ohjelmasta toiseen ja tietoverkon välityksellä edelleen koneesta toiseen.[207]

---

[206] Suomen Kaupunginviskaaliyhdistys r.y. ehdotti eduskunnan lakivaliokunnalle HE:n 94/1993 antamassaan lausunnossa 19.4.1994 seuraavanlaista säännöstä: ”Joka (1) tahallaan valmistaa tietokoneohjelman tai ohjelmakäskyjen sarjan, joka on tarkoitettu oikeudettomasti vaikuttamaan automaattiseen tietojenkäsittelyyn (*tuholaisohjelman*) tai (2) tahallaan tai törkeästä huolimattomuudesta levittää 1 kohdassa tarkoitettua ohjelmaa tai ohjelmakäskyjen sarjaa siten, että teko on omiaan aiheuttamaan automaattisesti käsiteltävien tietojen häviämistä, muuttumista tai turmeltumista taikka tietojenkäsittelyn teknisten apuvälineiden vahingoittumista, on tuomittava, ellei teosta muualla laissa ole säädetty ankarampaa rangaistusta, *tuholaisohjelman valmistamisesta tai levittämisestä* sakkoon tai vankeuteen enintään kahdeksi vuodeksi.” Myös keskusrikospoliisi ehdotti omassa lausunnossaan 13.4.1994 vastaavanlaista kriminalisointia: ”*Tuho-ohjelman valmistaminen*. Joka tahallaan valmistaa tietokoneohjelman tai sellaisen ohjelmakäskyjen sarjan, joka on tarkoitettu vahingoittamaan automaattista tietojenkäsittelyä, on tuomittava *tuho-ohjelman valmistamisesta* sakkoon tai vankeuteen enintään kahdeksi vuodeksi. (1 mom.) Tuho-ohjelman tai automaattista tietojenkäsittelyä vahingoittamaan tarkoitetun ohjelmakäskyjen sarjan levittämisestä on rangaistus tuomittava kuten tässä luvussa on tuhotyöstä tai 35 luvussa vahingonteosta säädetty. (2 mom.)”

[207] Virusten määritelmiä on tehty ja yritetty tehdä eri puolilla maailmaa. Ks. esimerkiksi SOU 1992:110, s. 215 ja s. 223 alav. 79; muun muassa yhdysvaltalaisesta osavaltiolainsäädännöstä löytyy kattavia määritelmiä, esim. Texasin rikoslaissa seuraavasti: ” ’Computer virus’ means an unwanted computer program or other set of instructions inserted into a computer’s memory, operating system, or program that is specifically constructed with the ability to replicate itself and to affect the other programs or files in the computer by attaching a copy of unwanted program or other set of instructions to one or more computer programs or files.” Toinen esimerkki Kalifornian rikoslaista: ” ’computer contaminant’ means any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms, which are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record, or transmit data or in some other fashion usurp the normal operation of the computer, computer system or computer network.” Ks. myös Fites ym., s. 6: ”A computer virus can be defined as malicious software which replicates itself. This definition is a little biased for our purposes: A virus need not be malicious. The key things about a computer virus are that it reproduces itself in systems other than the one in which it was created; and that it can somehow attach itself to other programs. The command file example mentioned earlier is almost a virus: It reproduced and denied access to that system (malicious, although not intended that way), and it would have done the same on any of the other computer systems maintained by that company if it had been copied; it didn’t infect any other programs, however. – A virus is just a name for a class of programs. They reproduce and infect other programs. Beyond that they could do anything any other program can. – You may

Troijan hevosiksi kutsutut ohjelmat poikkeavat varsinaisista viruksista sikäli, että ne eivät levitä itse kopioita itsestään vaan kykenevät leviämään ainoastaan käyttäjän avustuksella eli siten, että käyttäjän on kopioitava ohjelma, johon Troijan hevonen on tarttunut. Loogiset pommit ovat sellaisia Troijan hevosia, jotka on jätetty odottamaan suoritusta vasta sitten, kun jokin looginen ehto toteutuu. Madot puolestaan ovat ohjelmia, jotka toimivat itsenäisesti ja osaavat kopioida itsensä toisiin koneisiin verkon avulla.[208]

Virukset leviävät yleisimmin levykkeiden tai tietoverkkojen välityksellä. Tartunnan saaneessa koneessa ollut levyke saastuttaa kaikki muutkin koneet, joissa levykettä käytetään. Tietoverkkojen julkisista postilaatikoista tai ilmoitustauluilta kopioitavat ilmaisohjelmat saattavat toimia maailmanlaajuisina virusohjelmien levittämiskeinoina. Sähköpostin liitetiedostot ovat viime aikoina yleistyneet virusten levittämisvälineinä.

Valtaosa nykyään tunnetuista liki 100 000 haittaohjelmasta on suunniteltu toimimaan DOS (Disk Operating System) -ympäristössä.[209] Käynnistyslohkovirukset olivat pitkään yleisin virustyyppi, mutta nykyään niin sanotut makrovirukset[210] ovat voimakkaasti yleistyneet. Käynnistyslohkovirukset tarttuvat levykkeiden tai kiintolevyjen käynnistyslohkoihin, joilta ne voivat kopioida itsensä mille tahansa koneessa käytetylle kirjoitussuojaamattomalle levykkeelle. Jos taas kone käynnistetään niin, että saastunut levyke on levykeasemassa, kopioituu virus koneen kiintolevylle.

Makrovirukset leviävät ensi sijassa tekstitiedostojen välityksellä. Esimerkiksi sähköpostin liitteenä lähetettäviin tiedostoihin on helppoa piilottaa makrovirus, joka liitetiedostoa avattaessa saastuttaa asianomaisen tietokoneen. Makrovirukset ovat perinteisiä viruksia helpompia laatia, mikä saattaa aiheuttaa sen, että virusten kirjoittaminen ainakin jossain määrin muuttuu tietotekniikan asiantuntijoiden harrastuksesta tavallisten tietokoneen käyttäjien toiminnaksi.[211]

Sähköposti tarjoaa lähes rajattomat mahdollisuudet liitetiedostoihin kätkettyjen virusten levittämiseen. Osoitelistoja on kaupan, ja jos liitetiedostolle

---

run into another sort of computer vermin, the *worm*. It is a program that 'worms' its way through a system, altering small bits of data or code whenever it can get access. – A virus might also be a worm; if a worm *reproduces* itself in other systems and *infects* other programs, it would also be a virus. – Note that a computer virus is a program and it has to be *run* in order to reproduce or to do any damage. This fact is the key to several of the protection strategies discussed later."

208 Ks. HE 4/1999, s. 3.

209 Atk-sanakirja, s. 28: DOS = 1960-luvulla käyttöön tullut nimitys eräiden laitevalmistajien pienten tietokoneiden käyttöjärjestelmälle, joka sijaitsi magneettilevyllä. 1980-luvulla DOS-nimitys yleistyi tarkoittamaan mikrotietokoneen käyttöjärjestelmää.

210 Atk-sanakirja, s. 107: makrovirus = sovellusohjelman käsittelemään dataan, esimerkiksi tekstidokumenttiin kätketty sovellusohjelman toimintaa ohjaavia makroja käyttäen kirjoitettu virus.

211 Viruksista ks. myös Nuotio, Rikosoikeus, s. 1137.

keksii riittävän kiinnostavan aiheen, voi hyvinkin olettaa, että osa vastaanottajista varomattomasti avaa liitteen. Sain esimerkiksi itse jo helmikuussa 2001 osoitteesta howard.hughes@verizon.net tarjouksen ostaa 142 miljoonaa (142 000 000) sähköpostiosoitetta 149 US$:n hintaan. Myyjä ei houkutellut kauppaan virusten levittämismahdollisuudella vaan sillä, että yhden sentin hyötyminen jokaisesta nimestä merkitsisi 1,4 miljoonan dollarin tuloa, mutta ilkeämieliselle viruksen levittäjälle tällainen valmis osoitelista on tietysti varsin käyttökelpoinen.

Nyttemmin tällainen osoitteistojen kauppaaminen on saanut aivan toisenlaiset mittasuhteet ja sen seurauksena sähköpostin käyttäminen ylipäänsä on muodostunut hyvin ongelmalliseksi päivittäin tulvivan roskapostin vuoksi. Ja sitä mukaa kuin roskapostin määrä lisääntyy, ovat lisääntyneet myös sähköpostin mukana leviävät haittaohjelmat.

Virusongelma käytännössä

Virusongelma ei sinänsä Suomessa ole ollut kansainvälisesti vertailtuna mitenkään poikkeuksellisen merkittävä. Tunnetuin Suomessa kirjoitetuista haittaohjelmista lienee edelleen 25.3.1994 aktivoitunut *Finnish Sprayer* -virus, joka laukesi parissasadassa tietokoneessa viidessä valtiossa ja aiheutti yksin Suomessa miljooniin markkoihin nousseet vahingot. Viruksesta oli osattu etukäteen varoittaa ja se löydettiin ja poistettiin ennen aktivoitumispäivää yli neljästäsadasta tietokoneesta.

Saastuneiden tietokoneiden lukumäärä on tietysti aina aivan toista luokkaa kuin löydettyjen virusten lukumäärä, pahimmillaan monisatatuhatkertainen. Yksin saastuneiden koneiden puhdistaminen aiheuttaa huomattavia kustannuksia puhumattakaan niistä kustannuksista, joita yritykset, laitokset ja virastot joutuvat uhraamaan ennalta ehkäisevään virustorjuntaan. Teollisuusmaissa on virustorjunnan kustannuksilla arvioitu olevan suorastaan kansantaloudellista merkitystä.

Viime vuosina ovat tietoverkkojen kehittymisen ja laajenemisen myötä erilaiset ympäri maailmaa levinneet virukset selvästi yleistyneet. *Melissa, Loveletter*, *Anna Kournikova* ja *Code Red* lienevät tunnetuimpia viime vuosina esiintyneistä ensimmäisistä tämän tyypin haittaohjelmista ja tuoreessa muistissa ovat *Fizzer, Bugbear, Sobig, Lovsan* ja erityisesti *Swen*-mato, jonka vaikutukset sähköpostiliikenteelle olivat syksyllä 2003 varsin haitalliset.

Loveletterin kohdalla on syytä huomata, että sen tekijä onnistuttiin paikallistamaan Filippiineille, jossa häntä vastaan ei kuitenkaan oikeustoimiin tiettävästi voitu ryhtyä, koska virusohjelman laatiminen ei sikäläisen lainsäädännön mukaan ollut tuolloin rangaistavaa. Nyt tosin jo on, sillä menettely kriminalisoitiin hyvin nopeasti tapauksen paljastuttua. Tiedossani ei ole, sisältääkö sikäläinen oikeusjärjestys taannehtivan rikoslain kiellon.

Loveletterin aiheuttamat elokuuhun 2001 mennessä paljastuneet vahingot nousivat maailmanlaajuisesti peräti 8,7 miljardiin dollariin. Loveletteriä myöhemmin aktivoituneen Code Red -madon aiheuttamat vahingot puolestaan olivat samaan ajankohtaan mennessä nousseet jo noin kahteen miljardiin dollariin. Code Redin oli arvioitu elokuuhun 2001 mennessä tartuttaneen kaikkiaan 760 000 tietokonetta mutta jatkavan yhä leviämistään.[212]

Erityisesti Yhdysvalloissa vuonna 2003 riehuneen *Slammer*-viruksen saastuttamien tietokoneiden määrä kaksinkertaistui pahimmillaan 8,5 sekunnin välein. Lovsanin arvellaan jatkavan leviämistään ainakin vuoteen 2005 saakka. Swenin aiheuttamista taloudellisista haitoista ei vielä ole arvioita mutta kuvitella saattaa, että ne nousevat yksin Suomessa valtaviksi, kun satojentuhansien suomalaisen sähköpostiyhteydet katkesivat Swenin vuoksi useiksi päiviksi.

Vuoden 2004 alussa alkoi Internetissä levitä *Mydoom*-virus, joka on arvioitu tähän mennessä nopeimmin leviäväksi sähköpostivirukseksi, joka maailmanlaajuisesti tarkastellen sisältyi vuoden neljännellä viikolla arviolta joka 12. sähköpostiviestiin.[213] Mydoomin tekee vaaralliseksi se, että tietokoneen saastuttaessaan se avaa siihen takaoven, jonka avulla ulkopuolinen voi käyttää tietokonetta apuna uusissa verkkohyökkäyksissä.

Voidaan siis täysin perustellusti sanoa, että haittaohjelmat ovat erittäin suuri ongelma, joka nykyisellään näyttää muun muassa vakavasti vaarantavan sinänsä niin käyttökelpoisen ja kätevän sähköpostin käyttämisen.

Yleisvaarallinen rikos

Virussäännös on sijoitettu rikoslain yleisvaarallisia rikoksia koskevaan 34 lukuun. Perustelujen mukaan[214] viruksen levittämisellä ei niinkään tähdätä jonkin määrätyn, tietyssä tietokoneessa tai tietyllä tietovälineellä olevan informaation vahingoittamiseen. Viruksen leviäminen saattaa olla hyvin sattumanvaraista ja lähtökohtainen tilanne lienee yleensä sellainen, että viruksen kirjoittajalla tai levittäjällä ei ole tietoa siitä, minne virus lopulta päätyy. Viruksen valmistaja on esimerkiksi taitojaan testatakseen pyrkinyt kirjoittamaan viruksen aikomattakaan päästää sitä leviämään ja leviäminen puolestaan voi olla seurausta jonkun toisen huolimattomuudesta. Virusohjelman valmistaminen ja levittäminen on siis tyypillisesti yleistä vaaraa aiheuttava rikos.[215]

---

[212] Torikka – Virta. Artikkelissa siteeratun isobritannialaisen Data and Security Network -komitean jäsenen Jonathan Wignallin mukaan on pelättävissä, että madot pystyvät pian leviämään myös web-sivujen kautta, jolloin jopa pelkkä käynti www-osoitteessa voisi infektoida koneen. Tähän asti madot ovat levinneet lähinnä sähköpostin liitetiedostona tai palvelintasolla.

[213] Rinnemaa.

[214] HE 4/1999, s. 6 ja 8.

[215] Ks. Nuotio, Rikosoikeus, s. 1137 s.

Virusohjelman määritelmä

Säännöksen 1 kohdan mukaan rangaistaan sitä, joka tarkoituksin aiheuttaa haittaa tietojenkäsittelylle tai tieto- tai telejärjestelmän toiminnalle valmistaa tai asettaa saataville *sellaisen tietokoneohjelman tai ohjelmakäskyjen sarjan, joka on suunniteltu vaarantamaan tietojenkäsittelyä tai tieto- tai telejärjestelmän toimintaa taikka vahingoittamaan sellaisen järjestelmän sisältämiä tietoja tai ohjelmistoja, tai* levittää sellaista tietokoneohjelmaa tai ohjelmakäskyjen sarjaa.

Edellä on itse asiassa kursivoituna rikoslaissa oleva virusohjelman määritelmä. Itse lakitekstiin ei käsitettä ”tietokonevirus” tai ”virusohjelma” ole haluttu sisällyttää, koska termien yleiskielinenkään merkitys ei vastaa sitä, mitä säännöksellä on haluttu kriminalisoinnin piiriin sulkea. Perusteluissa tosin yksinkertaisuuden vuoksi käytetään virus-sanaa kuvaamaan kaikkia niitä ohjelmia ja ohjelmakäskyjen sarjoja, joihin kohdistuvaa menettelyä säännös koskee.[216] Ilmaisulla ”tietokoneohjelma tai ohjelmakäskyjen sarja”[217] tarkoitetaan[218] kaikkia edellä selostettuja varsinaisia viruksia ja niitä muistuttavia ohjelmia. Ohjelman tai ohjelmakäskyjen sarjan tulee nimenomaan olla suunniteltu sellaiseksi, että ominaisuuksiltaan soveltuu ensisijaisesti tietojenkäsittelyn tai tieto- tai telejärjestelmän toiminnan vaarantamiseen tai taikka sellaisen järjestelmän sisältämien tietojen tai ohjelmistojen vahingoittamiseen.

Tietojenkäsittely ja tietojärjestelmä

Perustelujen mukaan[219] *tietojenkäsittely* on tarkoitettu käsitettävän laajasti siten, että sillä ymmärretään kaikkea tietotekniikkaa hyväksi käyttäen tapahtuvaa tietojen käsittelemistä ja siirtoa. *Tietojärjestelmällä* tarkoitetaan samaa kuin tietomurtoa koskevassa säännöksessä eli sellaista tietojärjestelmää, jossa tietoja käsitellään, varastoidaan tai siirretään sähköisesti tai muulla vastaavalla teknisellä keinolla. Tietojärjestelmällä ei tarkoiteta yksinomaan useiden tietojenkäsittely- ja siirtolaitteiden muodostamaa verkostoa vaan yksittäinenkin tietokone, vaikkapa mihinkään kytkemätön sylimikro, voi olla säännöksessä tarkoitettu tietojärjestelmä.

---

[216] HE 4/1999, s. 3. Ks. Lehtonen, Datavirus, s. 46, jossa Lehtonen turhankin yksioikoisesti toteaa perusteluista löytyvän ”dataviruksen” määritelmän.

[217] Ks. HE 4/1999, s. 3: ”Tietokoneohjelma on tietojenkäsittelytehtävän esitys sarjana suorittimen toteutettavaksi tarkoitettuja toimia. Suoritin on numeerista tietoa automaattisesti käsittelevä laite, jota ohjaa muistiin tallennettu ohjelma. Kun suoritin tulkitsee ohjelmakäskyjä, se ei osaa arvioida niiden sisältöä, vaan kopioi ja levittää myös vahingollisia käskyjoukkoja.”

[218] HE 4/1999, s. 9.

[219] HE 4/1999, s. 8.

Telejärjestelmä

Telejärjestelmällä tarkoitetaan samaa kuin televerkolla rikoslain 38 luvun 3 §:ssä siltä osin kuin kysymys on tietojärjestelmässä käsitellyn datan siirtämiseen soveltuvasta verkosta. Mainitun säännöksen perustelujen mukaan[220] televerkon määritelmä sai sisältönsä teletoimintalaista (183/1987), joka sittemmin on kumottu 1.6.1997 voimaan tulleella telemarkkinalailla (396/1997). Näin ollen myös viestintäsalaisuuden loukkauksen kannalta televerkon voimassa olevana määritelmänä on pidettävä telemarkkinalain 4 §:n 3 kohdan määritelmää:

> Televerkolla tarkoitetaan siirtojärjestelmiä, jotka tekevät mahdolliseksi viestien siirron määrättyjen liityntäpisteiden välillä johtimella, radioteitse, optisesti tai muulla sähkömagneettisella tavalla.

Televerkon määritelmä on varsin kattava. Näin ollen rikoslain 34 luvun 9a §:ssä tarkoitetaan tieto- ja telejärjestelmällä kaikkia automaattiseen tietojenkäsittelyyn soveltuvia järjestelmiä alkaen yksittäisestä tietokoneesta ja päätyen maailmanlaajuisiin tietoverkkoihin.

Haitan aiheuttaminen

Tekijän on täytynyt toimia tarkoituksin aiheuttaa haittaa tietojenkäsittelylle tai tieto- tai telejärjestelmän toiminnalle. *Haitalla* tässä yhteydessä tarkoitetaan[221] paitsi suoranaista esimerkiksi tiedostojen häviämisenä tai muuttumisena ilmenevää vahinkoa myös mitä tahansa muuta sellaista vaikutusta tieto- tai telejärjestelmän toimintaan, joka jollain tavalla loukkaa järjestelmän haltijan tai muun sen käyttöön oikeutetun oikeutta järjestelmän käyttöön. Esimerkkinä tällaisesta haitasta perusteluissa mainitaan viruksen saastuttaman järjestelmän toiminnan hidastuminen tai se tosiasiallinen tilanne, että viruksen valtaama levytila ei enää ole järjestelmän käyttöön oikeutetun käytettävissä.

Perustelujen mukaan tällainen tahallisuuden vaatimus sulkee rangaistavuuden alan ulkopuolelle sellaiset tilanteet, joissa tietojenkäsittelyyn perehtynyt henkilö esimerkiksi haluaa kokeilla ohjelmointitaitojaan luomalla virusohjelman aikomattakaan kuitenkaan missään vaiheessa päästää aikaansaannostaan leviämään omaa konettaan kauemmaksi. Rangaistavia ovat vain sellaiset teot, joissa tekijä alun perin on tarkoittanut viruksen leviämään ja aiheuttamaan haittaa tietojenkäsittelylle.

Tekotavat

Säännöksessä mainitaan tekotapoina ohjelman tai ohjelmakäskyjen sarjan valmistaminen, saataville asettaminen ja levittäminen. *Valmistamisella* tarkoite-

---

220 HE 94/1993, s. 150.
221 HE 4/1999, s. 9.

taan perustelujen mukaan[222] uuden ohjelman kirjoittamista tai olemassa olevan ohjelman muuttamista säännöksessä tarkoitetun kaltaiseksi. *Saataville asettaminen* tarkoittaa lähinnä virusohjelman asettamista tietoverkosta yleisesti kopioitavaksi.[223] Tyypillisenä ”*levittämistoimena*” mainitaan saastuneen tietokonelevykkeen käyttäminen tietokoneessa. Tahallisuus ei tällöin välttämättä edellytä nimenomaista levittämistarkoitusta, mutta tekijän on tiedettävä viruksen olemassaolosta ja miellettävä sen leviäminen tekonsa varsin todennäköiseksi seuraukseksi.

Vahingon vaara

Rangaistavuus ei edellytä, että teosta tosiasiallisesti aiheutuu konkreettista haittaa tietojenkäsittelylle tai tieto- tai telejärjestelmän toiminnalle tai että järjestelmän sisältämät tiedot todella vahingoittuvat; riittää, että ohjelma tai ohjelmakäskyjen sarja on suunniteltu aiheuttamaan vaaraa tai vahinkoa. Soveltamisesimerkkinä mainitaan perusteluissa[224] ensinnäkin tilanne, jossa tietojärjestelmään tarttunut virus havaitaan ennen kuin se on ehtinyt aktivoitua ja aiheuttaa vahinkoa. Tällöin viruksen valmistaja ja/tai levittäjä voidaan muiden edellytysten täyttyessä tuomita teostaan rangaistukseen.

Toisena esimerkkinä mainitaan tilanne, jossa henkilön tietokoneelta löydetään tämän valmiiksi kirjoittama virus, joka ei vielä ole levinnyt minnekään. Kirjoittajaa voidaan rangaista, jos käy selville, että hän on valmistanut viruksen nimenomaisena tarkoituksenaan aiheuttaa haittaa tietojenkäsittelylle tai tieto- tai telejärjestelmän toiminnalle eli saattaa virus leviämään.

---

222 HE 4/1999, s. 9.

223 Huhtikuussa 1995 lähetettiin Kanadasta erääseen Internet-keskusteluryhmään 2 806 virusta sisältänyt paketti, joka myöhemmin päätyi suomalaiselle www-sivulle kenen hyvänsä saatavaksi pienestä suomalaisesta palvelimesta. Keskusrikospoliisi joutui tuolloin toteamaan, että suurenkaan virusmäärän asettaminen saataville ei ollut rangaistavaa tuolloin voimassa olleen lain mukaan, mutta katsoi, että yleisten vaaran lähteen avaamista koskevien oikeusperiaatteiden mukaan tällaisen teon jatkaminen oli laillisesti estettävissä sulkemalla asianomainen liittymä. Telecom Finland Oy:n aloitteesta liikenneministeriö teki 16.6.1995 päätöksen, jolla ohjeistettiin yleisemminkin teleliittymän sulkeminen eräissä tapauksissa. Päätöksessä katsottiin, että liikenneministeriön asiana ei ollut ottaa kantaa televerkoissa välitettyjen tai tarjolla olevien viestien sisältöön sinänsä. Ministeriö totesi kuitenkin, että Internet-verkon jossakin palvelimessa yleisesti tarjolla olevilla, suojaamattomilla virusohjelmilla voitiin tarkoituksellisesti tai tahattomasti aiheuttaa vahinkoa televerkon osana toimivalle tietokoneelle. Tarjolla olevilla virusohjelmilla voitiin aiheuttaa häiriötä myös televerkon toisen käyttäjän tietokoneelle, joka oli liitetty verkkoon modeemin kautta, vaikka tällainen tietokone ei ollutkaan televerkon osa eikä televerkkoon suoraan liitettävä päätelaite. Liikenneministeriö päätti teletoimintalain (183/1987) 10 §:n 2 momentin nojalla, että telelaitoksella on oikeus sulkea liittymä myös silloin, kun teleliittymässä osoitetaan pidettävän yleisesti tarjolla virusohjelmia, joilla voidaan aiheuttaa häiriötä joko televerkolle tai muiden käyttäjien televiestinnälle.

224 HE 4/1999, s. 9.

Säännöksessä tarkoitettu vaara tai vahinko voisi syntyä ensisijaisesti sen seurauksena, että aktivoitunut virus keskeyttää tieto- tai telejärjestelmän toiminnan kokonaan tai muuttaa järjestelmän sisältämiä tietoja.

Ohjeen saataville asettaminen ja levittäminen

Säännöksen 2 kohdan mukaan rangaistaan myös sitä, joka asettaa saataville ohjeen 1 kohdassa tarkoitetun tietokoneohjelman tai ohjelmakäskyjen sarjan valmistamiseen tai levittää sellaista ohjetta. Perustelujen mukaan[225] ohjeella tässä tarkoitetaan niin yksityiskohtaista ohjetta, että vähänkin tietojenkäsittelyyn perehtynyt henkilö sen perusteella pystyy valmistamaan virusohjelman. Ohjeen saataville asettamisen ja levittämisen kriminalisoimista perustellaan sillä, että tällainen toimi on vaarallisuudeltaan lähes täysin rinnastettavissa valmiin viruksen saataville asettamiseen tai levittämiseen. Koska ohje ei kuitenkaan voi valmiin ohjelman tavoin levitä itsestään, ei pelkän ohjeen valmistamisen ole vielä katsottu aiheuttavan sellaista vaaraa, että se olisi pitänyt säätää rangaistavaksi.

Ohjeen levittäminen voi – virusohjelman levittämisestä poiketen – tapahtua paitsi tietotekniikan keinoin myös esimerkiksi julkaisemalla se painokirjoituksessa tai muulla tavoin kirjallisesti. Myös ohjeen saataville asettamisen ja levittämisen rangaistavuus edellyttää, että tekijä on toiminut tarkoituksin aiheuttaa haittaa tietojenkäsittelylle tai tieto- tai telejärjestelmän toiminnalle.

Säännöksen toissijaisuus

Virussäännös on toissijainen: sitä ei sovelleta, jos teosta muualla laissa säädetään ankarampi tai yhtä ankara rangaistus. Virussäännöksen syrjäyttävinä säännöksinä voisivat tapauksesta ja tekijän tahallisuudesta riippuen tulla kysymykseen rikoslain 35 luvun 2 §:n säännös törkeästä vahingonteosta, 36 luvun 1 §:n 2 momentin säännös tietojenkäsittelypetoksesta ja 2 §:n säännös törkeästä petoksesta sekä 38 luvun 5 §:n säännös tietoliikenteen häirinnästä ja 6 §:n säännös törkeästä tietoliikenteen häirinnästä. Näistä kaikista on säädetty yhtä ankarat tai ankarammat rangaistusuhat kuin vaaran aiheuttamisesta tietojenkäsittelylle.

Rikoslain 35 luvun 1 §:n vahingontekoa koskevan säännöksen suhde nyt puheena olevaan säännökseen saattaa joissakin tapauksissa olla ongelmallinen, koska 35 luvun 5 §:n mukaan myös vahingontekoa koskeva säännös on toissijainen ja koska vahingonteon perustekomuodon rangaistusasteikko on lievempi. Silloin, kun vahinkoa on aiheutunut, voidaan mielestäni kuitenkin tuomita sekä vaaran aiheuttamisesta tietojenkäsittelylle (esim. viruksen levittäminen)

---

[225] HE 4/1999, s. 10.

että vahingonteosta (vahingon aiheutuminen), mikäli vahingonteon osalta on osoitettava riittävä tahallisuus. Vahingon syntyminen kuuluu vain vahingonteon tunnusmerkistöön ja (konkreettinen) vaara voi joka tapauksessa kohdistua huomattavasti yksittäisen vahingontekorikoksen asianomistajatahoa laajemmalle.

Perustelujen mukaan[226] viruksen valmistaminen ja levittäminen on joka tapauksessa siinä määrin sattumanvaraisesti konkreettisia seurauksia aiheuttava teko, että siitä tuomittavaa rangaistusta ei voida jättää riippumaan yksinomaan teon seurauksista, jotka saattavat tosiasiallisesti jäädä hyvinkin vähäisiksi huolimatta teon ehkä suurestakin vaarallisuudesta.

Kansainväliset instrumentit

Euroopan neuvoston vuoden 1989 kriminalisointisuosituksessa ei nimenomaisesti mainita viruksia ja vastaavia ohjelmia. Ongelma ei kymmenen vuotta sitten ollut lainkaan yhtä mittava kuin se on tällä hetkellä. Tosin tietokonesabotaasia koskeva minimilistan suositus[227] itse asiassa tarkoittaa hyvin pitkälti samaa kuin vaaran aiheuttamista tietojenkäsittelylle koskeva rangaistussäännös, sillä suosituksessa tarkoitettu ”sellainen datan tai ohjelmiston syöttäminen, muuttaminen, hävittäminen tai käytön estäminen taikka tietokonejärjestelmiin puuttuminen, jonka tarkoituksena on estää tietokone- tai televiestintäjärjestelmän toiminta” kyllä kattaa ainakin osan aktiivisista viruksen levittämistä tarkoittavista toimista. Suosituksen perusteluista toisaalta ilmenee, että suosituksella on tarkoitettu vahingonteon tyyppistä toimintaa, eikä perusteluissa mainita viruksia.

Kansainvälisen rikosoikeusyhdistyksen AIDP:n Rio de Janeiron kongressin päätöslauselmassa suositellaan muun muassa harkittavaksi virusten ja vastaavien ohjelmien levittämisen kriminalisoimista.

Ulkomaiset säännökset

Euroopan valtioista on Suomen lisäksi voimassa virusten valmistamiseen ja/tai levittämiseen liittyviä kriminalisointeja Alankomaissa, Italiassa, Sveitsissä, Venäjällä ja Yhdistyneessä kuningaskunnassa.[228] Kriminalisointeja valmistellaan lisäksi ainakin Ruotsissa, Saksassa ja Latviassa.

Alankomaiden rikoslain vuodelta 1992 olevan 350 a artiklan 3 momentin mukaan tuomitaan rangaistukseen se, joka tahallisesti tai oikeudettomasti asettaa saataville tai levittää sellaista dataa, joka on tarkoitettu aiheuttamaan vahinkoa kopioimalla itseään tietojärjestelmässä. Seuraamuksena on vankeutta enintään neljä vuotta tai sakkoa enintään 100 000 guldenia.

---

226 HE 4/1999, s. 10.
227 EN:n raportti, s. 35.
228 Ks. Tenhunen, Malicious Code.

Italian rikoslain vuodelta 1993 olevan artiklan 615 *quinquies* mukaan rikokseen syyllistyy se, joka levittää, välittää tai tallettaa joko itsensä tai jonkun muun valmistaman tietokoneohjelman, joka on tarkoitettu vahingoittamaan tieto- tai telejärjestelmää tai sen sisältämää taikka siihen kuuluvaa dataa tai ohjelmistoa keskeyttämällä järjestelmän toiminnan joko kokonaan tai osaksi taikka muuttamalla sen toimintaa. Rangaistuksena on vankeutta enintään kaksi vuotta ja sakkoa enintään 20 000 000 liiraa.

Sveitsin rikoslakiin lisättiin vuonna 1994 uusi 144 bis §,[229] jonka toisen momentin mukaan rangaistavaa on sellaisen ohjelman luominen, maahan tuominen, levittäminen, saataville asettaminen ja tarjoaminen, joka on tarkoitettu hävittämään, muuttamaan tai tekemään käyttökelvottomaksi elektronisesti tai vastaavalla tavalla tallennettua tai siirrettyä dataa. Rangaistavaa on lisäksi ohjeiden antaminen tällaisen ohjelman valmistamiseksi. Rangaistus rikoksesta on vankeutta enintään kolme vuotta tai sakkoa enintään 40 000 Sveitsin frangia. Jos tekijä on toiminut tarkoituksin hankkia hyötyä, rangaistuksena on vankeutta enintään viisi vuotta.

Nämä kolme peräkkäisinä vuosina säädettyä kriminalisointia ovat hyvin samantyyppisiä, mutta niissä on nähtävissä selvä kehitystrendi: Alankomaiden säännös on vielä jokseenkin yksinkertainen eikä kata kaikkia viruksiin liittyviä tilanteita, kun taas sveitsiläinen säännös on jo hyvin perusteellinen – Italian pykälä jää välimaastoon. Sveitsin säännös havaittiin kohta käytännössä liiankin tiukaksi, sillä virustorjuntaa harjoittavat yritykset havaitsivat menettelevänsä lainvastaisesti tuodessaan maahan uusia viruksia testaamista ja omien tuotteidensa kehittelyä varten. Asia hoidettiin tiettävästi tulkintateitse lakia muuttamatta.

Säännöksen arviointia

Ei liene mikään yllätys, että Suomen virussäännös muistuttaa edellä selostettuja. Kansainvälinen yhteistyö viruksia koskevissa kysymyksissä on melko tiivistä eikä se rajoitu pelkästään järjestötasolla tapahtuviin kontakteihin. Järjestöistä on tässä syytä mainita EICAR eli *European Institute for Computer Anti-virus Research,* joka pitää päämajaansa Saksassa ja toimii läheisessä yhteistyössä Pohjois-Atlantin puolustusliiton NATO:n kanssa. Järjestössä on mukana eri Euroopan ja Pohjois-Amerikan maista olevia viranomaisia, järjestöjä ja yrityksiä sekä henkilöjäseniä, tämän kirjoittaja mukaan lukien. EICAR harjoittaa aktiivista tutkimustoimintaa muun muassa viruksiin liittyvistä oikeudellisista kysymyksistä.

Suomalaisessa säännöksessä on pyritty yhdistelemään lähinnä juuri Italian ja Sveitsin säännösten hyvät puolet ja karsimaan niiden heikkoudet. Säännöksen

---

[229] Säännöksestä tarkemmin ks. Frigerio.

valmistelun yhteydessä on toimittu läheisessä yhteistyössä niin esitutkinta-viranomaisten kuin virustorjunta-alan edustajienkin kanssa. Kukaan ei oleta, että virusongelma ratkaistaisiin tällaisella kriminalisoinnilla, mutta ainakin se osoittaa lainsäätäjältä vastuuntuntoista suhtautumista ja toivottavasti jossain määrin vähentää haluja virusten valmistamiseen ja levittämiseen. Muistettava on, että tietotekniikan kehittyessä myös viranomaisten valmiudet kehittyvät ja niiden myötä lisääntyvät mahdollisuudet rikoksentekijöiden jäljittämiseen ja kiinni saamiseen.

Käytännön tapaus

Ensimmäinen tuntemani tapaus, jossa säännöstä on tuomioistuimessa sovellettu, on edellä tietomurron yhteydessä mainittu ns. Vantaan hakkerijuttu. Vaadin siinä toiselle vastaajista rangaistusta vaaran aiheuttamisesta tietojenkäsittelylle seuraavasti:

> N on 1.3.2001–19.2.2002 Helsingissä, aiheuttaakseen haittaa tietojenkäsittelylle sekä tietojärjestelmien toiminnalle, valmistanut edellä tässä syytteessä mainitusta t0rn-rootkit -ohjelmasta pikakit.tgz:ksi nimeämänsä ohjelman, levittänyt valmistamaansa ohjelmaa sekä asettanut sen muiden saataville. Pikakit.tgz-ohjelma on luonut tunkeutumisen kohteena olleeseen järjestelmään luvattoman tunkeutumisen myöhemmin mahdollistavan takaportin ja lähettänyt tiedon takaportista N:n sähköpostiosoitteeseen. Lisäksi ohjelma on tuhonnut lokitiedostoja ja luonut piilotettuja tiedostoja. Tietomurtojen suorittamisen helpottamiseksi valmistettuna ohjelma on suunniteltu vaarantamaan tietojenkäsittelyä ja tietojärjestelmän toimintaa sekä vahingoittamaan tietojärjestelmän sisältämiä tietoja.

Kysymyksessä ei siis ollut viruksen tyyppinen haittaohjelma vaan eräänlainen murtotyökalu. Rootkit-ohjelmia sinänsä voidaan käyttää myös luvallisiin tarkoituksiin mutta tässä tapauksessa katsoin mainitusta t0rn-rootkit -nimisestä ohjelmasta muunnetun version olleen sellainen, ettei sillä ollut mitään hyväksyttävää käyttötarkoitusta. Tälle kannalle päätyi myös Helsingin käräjäoikeus lainvoimaiseksi jääneessä tuomiossaan.

EN:n yleissopimus ja vahingolliset ohjelmat

Euroopan neuvoston yleissopimuksessa ei ole nimenomaisesti vahingollisia ohjelmia koskevaa artiklaa. Joiltain osin edellä jo selostetut artiklat 4 (datan vahingoittaminen) ja 6 (välineiden väärinkäyttö) kattavat myös virus- ym. vastaavia ohjelmia käyttämällä tehtyjä tekoja; sisällytetäänhän artiklassa 6 tietokoneohjelma siinä tarkoitettuihin välineisiin. Virusohjelman levittämisellä voi toteutua myös artiklassa 5 kuvattu menettely:

> *Tietojärjestelmän häirintä.* Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin säätääkseen lainsäädäntönsä mukaisesti rangaistavaksi tahallisen ja oikeudettoman tietojärjestelmän toiminnan vakavan estämisen dataa syöttämällä, siirtämällä, vahingoittamalla, tuhoamalla, turmelemalla, muuttamalla tai poistamalla.[230]

Kysymyksessä on siis tietojärjestelmän toiminnan estäminen, jonka myös virusohjelman aktivoituminen voi saada aikaan. Voimassa olevan lakimme säännös tietoliikenteen häirinnästä (RL 38:5) kattaa artiklassa kuvatun menettelyn joiltain osin, mutta artiklan täydellinen implementoiminen edellyttää joitakin lainmuutoksia.

Artikla 6 tarkoittaa myös joiltakin osin haittaohjelmiin liittyviä menettelyjä, joskin menee selvästi pitemmälle kuin rikoslain 34 luvun 9a §:n säännös. Palaan artiklan merkitykseen tarkemmin *de lege ferenda* -jaksossa.

> *Laitteiden väärinkäyttö*
>
> 1. Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin säätääkseen kansallisen lainsäädäntönsä mukaisesti rangaistaviksi seuraavat tahalliset ja oikeudettomat teot:
> a) seuraavien tuottaminen, myynti, hankkiminen, tuonti, levittäminen tai muu saataville asettaminen:
> i) väline, mukaan luettuna tietokoneohjelma, joka on suunniteltu tai muutettu ensisijaisesti tämän yleissopimuksen 2–5 artiklan mukaisesti rangaistaviksi säädettyjen rikosten tekemistä varten;
> ii) tietojärjestelmän salasana tai käyttäjätunnus tai muu vastaava tieto, joka mahdollistaa pääsyn tietojärjestelmään tai sen osaan,
> tarkoituksin, että sitä käytetään tämän yleissopimuksen 2–5 artiklan mukaisesti rangaistaviksi säädettyjen rikosten tekemiseen,
> b) tämän kappaleen a kohdan i tai ii alakohdassa tarkoitetun tuotteen hallussapito, tarkoituksin käyttää sitä 2–5 artiklan mukaisesti rangaistaviksi säädettyjen rikosten tekemiseen. Sopimuspuoli voi asettaa rikosvastuun syntymisen edellytykseksi sen, että tekijän hallussa on useita tällaisia tuotteita.
> 2. Tämän artiklan määräysten ei katsota perustavan rikosvastuuta muun muassa silloin kun tämän artiklan 1 kappaleessa tarkoitetun tuotannon, myynnin, hankkimisen, tuonnin, levittämisen tai muun saataville asettamisen tarkoituksena ei ole tehdä tämän yleissopimuksen 2–5 artiklan mukaisesti rangaistavaksi säädettyä rikosta, vaan tietojärjestelmän luvallinen testaus tai suojelu.

---

[230] *System interference.* Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

3. Kukin sopimuspuoli voi tehdä varauman, jonka mukaan se ei sovella tämän artiklan 1 kappaletta, edellyttäen kuitenkin, että varauma ei koske tämän artiklan 1 kappaleen a kohdan ii alakohdassa tarkoitettujen tuotteiden myyntiä, levittämistä tai muuta saataville asettamista.[231]

---

[231] *Misuse of devices.*

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a) the production, sale, procurement for use, import, distribution or otherwise making available of:

i) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;

ii) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b) the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3. Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

5 Tunnusmerkistöjen välistä rajankäyntiä

Edellä erinäisiä tietotekniikkarikoksia käsiteltäessä on jo useaan kertaan tullut selväksi, että tunnusmerkistöjen väliset rajat eivät ole aina yksiselitteisiä ja että tästä saattaa aiheutua vaikeuksia sovellettavan säännöksen valinnassa. Käsittelen vielä tässä jaksossa yhteenvedonomaisesti näitä rajankäyntikysymyksiä, kuitenkin niin, että jätän vaaran aiheuttamisen tietojenkäsittelylle erityyppisenä tekona tämän tarkastelun ulkopuolelle.

Lainkonkurrenssista

Lahden mukaan lainkonkurrenssista on kysymys, kun useat rangaistussäännökset ensi silmäyksellä näyttävät soveltuvan johonkin tekoon / joihinkin tekoihin, mutta yksityiskohtaisemmassa tarkastelussa yhden rangaistussäännöksen soveltamisen todetaan tekevän muun / muiden soveltamisen tarpeettomaksi (mahdottomaksi).[232] Toisin sanoen lainkonkurrenssissa yhdellä tai useammalla teolla toteutetaan usea rikostunnusmerkistö, mutta siitä huolimatta tuomitaan vain yhden rangaistussäännöksen mukaan; kysymyksessä on vain yksi rikos.[233]

Perinteisesti lainkonkurrenssin piirissä on erotettu toisistaan spesiaalisuuden, subsidiaarisuuden ja konsumptatiivisuuden tapausryhmät. Näistä ensimmäisessä tekoon yksityiskohtaisesti soveltuva säännös syrjäyttää yleisluonteisemman: *lex specialis derogat legi generali.* Kun rangaistussäännöstä sovelletaan vain siinä tapauksessa, että rikoksesta ei muualla laissa ole säädetty (yleensä ankarampaa) rangaistusta, säännös on subsidiaarinen: *lex primaria derogat legi subsidiariae.*

Konsumptatiivisuustapauksissa saa *Lahden* mukaan lainkohtien arvoastesuhde aikaan tois(t)en syrjäytymisen: konsumoivan rangaistussäännöksen soveltaminen tekee tarpeettomaksi konsumoidun rangaistussäännöksen soveltamisen edellisessä ilmaistun tunnusmerkistön ollessa deliktisen vääryyden arvioinnissa riittävän tyhjentävä; tällöin *lex consumens derogat legi consumptae.*

Lahti tekee saksalaisen *Ulrich Klugin* analyysin perusteella sen johtopäätöksen,[234] että loogisesti voidaan erottaa vain kaksi lainkonkurrenssitapausten alaryhmää eli sisältyvyyden ja ristikkyyden tapausryhmät, joista ensimmäistä hän kutsuu erityisyyden ja jälkimmäistä toissijaisuuden tapausryhmäksi.

---

232 Ks. Lahti, LM 68, s. 709 ss., ja Honkasalo, Yleiset opit II, s. 259 ss.
233 Konkurrensseista ks. myös Nuutila, Rikoslaki, s. 370 ss.
234 Lahti, LM 68, s. 716 ss.

Erityisyyden tapausryhmän osalta sääntönä on, että syrjäytyvän tunnusmerkistön on sisällyttävä välttämättömänä osana syrjäyttävään tunnusmerkistöön, jolloin välttämätön sisältyvyys merkitsee sitä, että ensiksi mainitussa abstraktisessa rikostunnusmerkistössä on katsottava ilmaistun myös viimeksi mainittu tunnusmerkistö.

Suojeltavat oikeushyvät

Toissijaisuuden tapausryhmän kohdalla on puolestaan edellytettävä, että syrjäytyvällä ja syrjäyttävällä tunnusmerkistöllä on oltava jotakin yhteistä; tunnusmerkistöjen on leikattava toisensa. *Lahden* näkemyksen mukaan teleologisella tulkinnalla on erityisen suuri merkitys arvioitaessa tunnusmerkistöjen osittaista yhteisyyttä. Huomiota on siis kiinnitettävä siihen, minkä oikeushyvien suojaamiseksi tarkasteltavat rangaistussäännökset ovat syntyneet. Myös *Nuutila* toteaa, että ratkaisun perustaksi on otettava se, millä tavalla säännökset kattavat toisen oikeudellisesti suojattujen etujen loukkauksia ja vaarantamisia.[235]

Aikaisemmin olen todennut, että tietotekniikkarikoksiksi luokiteltavat teot kohdistuvat kaikki enemmän tai vähemmän yhteen yhteiseen oikeushyvään eli tietojenkäsittelyn loukkaamattomuuteen, tietojenkäsittelyrauhaan. Korostetusti juuri tätä oikeushyvää suojaavat tietomurron ja tietojenkäsittelyn vaarantamisen kriminalisoinnit, sen sijaan muilla tietotekniikkarikoskriminalisoinneilla suojataan myös (ja erityisesti) muita oikeushyviä. Luvattoman käytön kriminalisointi on tosin lähellä tietomurtoa siinä suhteessa, että sillä ensisijaisesti pyritään turvaamaan omistajan tai muun tietojärjestelmän käyttöön oikeutetun oikeus järjestelmän yksinomaiseen käyttämiseen; edes vahingon syntyminen ei ole tunnusmerkistön täyttymisen edellytyksenä.

Tietojenkäsittelypetosta koskevan säännöksen suojeluobjekti on jo toisentyyppinen: suojaa saavat ensisijaisesti uhrin taloudelliset intressit, joskin tietojenkäsittelyyn puuttuminen ja tätä kautta tietojenkäsittelyrauhan loukkaaminen on olennainen osa teon tunnusmerkistöä. Tietovahingon aiheuttamista koskeva säännös sijoittuu tässä suhteessa samaan kategoriaan petossäännöksen kanssa.

Väärennys eroaa edellä mainituista sikäli, että oikeudeton tietojenkäsittelyyn puuttuminen ei ole mikään välttämätön tunnusmerkistötekijä. Myös yritysvakoilussa – silloinkin kun se voidaan lukea tietotekniikkarikoksiin kuuluvaksi – tietojenkäsittelyyn puuttumisen asema tunnusmerkistössä on jokseenkin vähämerkityksinen. Maksuvälinepetoksen suhteen tilanne on samankaltainen.

Äsken lausutun perusteella voidaan edellä käsitellyt teot jakaa kolmeen ryhmään sen mukaan, miten olennainen on tietojenkäsittelyn loukkaamattomuuden asema tunnusmerkistön täyttymisessä. Lähes puhtaasti tietojenkäsitte-

---

[235] Nuutila, Rikoslaki, s. 371.

lyrauhaa suojaavia säännöksiä ovat tietomurron ja luvattoman käytön kriminalisoinnit, kun taas väärennyksen, yritysvakoilun ja maksuvälinepetoksen kohdalla tietojenkäsittelyrauhalle suojaa antava elementti on vähäinen. Näiden kahden ryhmän väliin jäävät tietojenkäsittelypetos ja tietovahingon aiheuttaminen, joita koskevien säännösten ensisijaisena suojeluobjektina on jokin muu kuin tietojenkäsittelyrauha, mutta jotka myös olennaisesti suojaavat tätä rauhaa.

Varsinkin luvaton käyttö mutta myös tietojenkäsittelypetos ja tietovahingon aiheuttaminen ovat usein sellaisia tekoja, että niitä edeltää tietomurron tunnusmerkistön täyttävä menettely. Tietomurtosäännös on nimenomaisesti säädetty toissijaiseksi, joten jos tietojärjestelmään tunkeutuja sisälle päästyään jatkaa järjestelmän käyttämistä millä tavalla hyvänsä, ei häntä voida rangaista erikseen tietomurrosta.

Luvaton käyttö, petos ja vahingonteko

Tietojenkäsittelypetoksen ja tietovahingon aiheuttamisen tekeminen ei välttämättä edellytä, että tekijä luvattomasti käyttää kysymyksessä olevaa tietojärjestelmää. Jos näin kuitenkin tapahtuu – niin kuin useimmiten asianlaita lienee – on tekijä toisaalta loukannut asianomistajan oikeutta tietojärjestelmän yksinomaiseen käyttöön ja toisaalta tämän taloudellisia intressejä. Tunnusmerkistöt eivät leikkaa toisiaan; kun vahingon syntymekanismin ja tekijän tarkoituksen perusteella on ratkaistu kysymys siitä, onko vahinkoa aiheuttanut teko vahingonteko vai petos, jää tekijän syyksi joka tapauksessa myös luvaton käyttö. Luvatonta käyttöä koskeva rangaistussäännös toisin sanoen ei voi olla lainkonkurrenssissa sen paremmin petos- kuin vahingontekosäännöksenkään kanssa, vaan kysymyksessä on useampia rikoksia, joita ei välttämättä edes ole tehty samalla konkreettisella teolla.

Kokonaan toinen asia on se, että luvattomasta käytöstä voi tosiasiallisesti aiheutua asianomistajalle tuntuvaakin vahinkoa esimerkiksi siitä syystä, että asianomistaja havaitsee järjestelmässä vieraillun mutta ei saa selville, mitä siellä on tehty. Käytöstä *mahdollisesti* aiheutuneiden vahinkojen korjaaminen ja niiden vaikutusten estäminen voi aiheuttaa hyvinkin suuria kustannuksia.

Väärennys, petos ja vahingonteko

Huolimatta siitä, että tietovahingon aiheuttamisen ja tietojenkäsittelypetoksen objektiiviset tunnusmerkistötekijät osaksi ovat samanlaisia – väärien tietojen syöttäminen tai muu puuttuminen koneelliseen tietojenkäsittelyyn voi tosiasiallisesti merkitä tietovälineelle tallennetun tiedon tai muun tallennuksen hävittämistä tai turmelemista – eivät tunnusmerkistöt ainakaan periaatteessa ole siinä mielessä päällekkäisiä, että kysymyksessä yleensä voitaisiin katsoa olevan lainkonkurrenssitilanne.

Mahdolliset soveltamisongelmat ratkennevat ensisijaisesti tekijän tarkoituksen selvittämisellä ja ellei tämä riitä, ratkaisu löytynee vahingon syntymekanismista: petossäännös edellyttää nimenomaan vahingon syntymistä *tietojenkäsittelyn lopputuloksen vääristymisen* seurauksena. Sen sijaan ongelma saattaa syntyä yritysasteelle jääneen petoksen ja täytetyn vahingonteon välillä: jos tietojenkäsittelyn lopputuloksen vääristymistä ei syystä tai toisesta ehdi tapahtua ja vahinkoa kuitenkin tosiasiallisesti aiheutuu, voivat objektiivisessa suhteessa täyttyä *sekä* vahingonteon *että* petoksen yrityksen tunnusmerkistöt.

> Ns. perinteisen rikollisuuden puolelta puheena olevaan ongelmaan rinnastettava tilanne voisi olla vaikkapa seuraavanlainen:
>
> Vahvasti humaltunut A kohottaa nyrkkinsä ja ilmoittaa B:lle: ”Nyt minä hakkaan sinut!” A suuntaa kohti B:tä voimakkaan nyrkiniskun, joka kuitenkin A:n humalatilan seurauksena jää osumatta. Tilanne päättyy siihen.
>
> A:n tarkoituksena on ollut tehdä B:lle ruumiillista väkivaltaa ja hän on ryhtynyt toteuttamaan aikomaansa rikosta. Rikoslain 21 luvun 5 §:n mukaisen pahoinpitelyn *yrityksen* tunnusmerkistö on siis toteutunut kaikilta osin. Toisaalta A on uhannut B:tä rikoksella sellaisissa olosuhteissa, että B:llä on ollut perusteltu syy vakavasti pelätä henkilökohtaisen turvallisuutensa olleen vaarassa, ja rikoslain 25 luvun 7 §:ssä tarkoitetun laittoman uhkauksen tunnusmerkistö on *myös* täyttynyt. Täytetyn laittoman uhkauksen rangaistusasteikko on ankarampi kuin pahoinpitelyn yrityksen.
>
> B:n kannalta tilanne on sama, sovelletaan kumpaa lainkohtaa tahansa. Hänelle on aiheutunut vahinkoa enintään henkisen järkytyksen muodossa. – Jos asiaa tutkittaessa käy riidattomasti selville, että A:lla on ollut nimenomainen pahoinpitelemisen tarkoitus, on tämä määräävä kriteeri sovellettavaa lainkohtaa valittaessa: A tuomittaneen rangaistukseen pahoinpitelyn yrityksestä. Ratkaisu saattaa tuntua oudolta ja asettaneekin pahoinpitelyn yrityksen kriminalisoimisen mielekkyyden ainakin jossain määrin kysymyksenalaiseksi

Tietojenkäsittelypetoksen yrityksen ja tietovahingon aiheuttamisen välinen rajanveto-ongelma ratkeaa saman periaatteen mukaisesti: syytettyä ei voida tuomita ankaramman *tahallisuutta* edellyttävän tunnusmerkistön mukaan, kuin mihin hänen tahallisuutensa ulottuu. Ratkaisu ilmentää ensisijaisesti syytetyn suosimisperiaatetta, olkoonkin, että toisenkin tunnusmerkistön osalta *dolus eventualis* -tyyppinen tahallisuus *saattaisi* olla olemassa. Konkurrenssiopillisesti taas – *Lahden* edellä esitettyä jaottelua noudattaen – kysymys on toissijaisuuden tapausryhmästä.[236]

---

[236] Ks. Lahti, LM 68, s. 719 ss. sekä s. 716, alav. 24, jossa Lahti käsittelee lainkonkurrenssin vaikutusta rangaistuksen mittaamiseen ja puoltaa Suomen oikeuden kannalta käsitystä, ettei syrjäytyvä rangaistussäännös saa vaikuttaa rangaistuksen määräämiseen (esim. olemalla joka tapauksessa rangaistuksen vähimmäismäärä), koska meillä on korostettu rangaistusasteikkojen vertailun merkitystä jo siinä vaiheessa, kun ao. säännöksen toissijaisuutta pohditaan.

Edellä on jo korostettu, miten tietojenkäsittelypetokseen aina kuuluu tietojenkäsittelyn lopputuloksen vääristyminen, millä tarkoitetaan sitä, että tietojenkäsittelyjärjestelmä saadaan puuttumistoimien jälkeen tuottamaan virheellistä tietoa. *Tosiasiallisesti* näin voi tapahtua myös vahingonteko- tai väärennysrikoksen ollessa kysymyksessä. Petoksen ja vahingonteon osalta edellytetään osaksi samanlaista tarkoitusta, jollaista taas väärennyksen suhteen ei vaadita.

Jokainen näistä rikoksista on mahdollista toteuttaa samankaltaisilla toimilla, mutta petosrikoksen osalta on lisäedellytyksenä *tietojenkäsittelyn lopputuloksen* vääristyminen, josta itse asiassa on kysymys myös väärennysrikoksen kohdalla mutta jota ei vaadita vahingontekorikoksen tunnusmerkistön täyttymiseen. Vielä petosrikokselta edellytetään vahingon aiheutumista, jota rikoksen luonteesta johtuen on pidettävä myös vahingontekorikoksen välttämättömänä tunnusmerkkinä; väärennyksen suhteen tällaista vaatimusta ei ole asetettu.

Tunnusmerkistöjen osaksi päällekkäiset rakenteet selviävät hyvin, kun niitä vertaillaan toisiinsa taulukon muodossa:

Väärennys	**Vahingonteko**	**Petos**
Joka	Joka toista vahingoittaakseen	Joka hankkiakseen itselleen tai toiselle oikeudetonta taloudellista hyötyä tai toista vahingoittaakseen
valmistaa väärän automaattiseen tietojenkäsittelyyn soveltuvan tallenteen tai väärentää sellaisen käytettäväksi harhauttavana todisteena taikka käyttää väärää tai väärennettyä tallennetta tällaisena todisteena	oikeudettomasti hävittää, turmelee, kätkee tai salaa tietovälineelle tallennetun tiedon tai muun tallennuksen	dataa syöttämällä, muuttamalla, tuhoamalla tai poistamalla taikka tietojärjestelmän toimintaan muuten puuttumalla saa aikaan tietojenkäsittelyn lopputuloksen vääristymisen ja siten aiheuttaa toiselle taloudellista vahinkoa
on tuomittava sakkoon tai vankeuteen enintään kahdeksi vuodeksi	on tuomittava sakkoon tai vankeuteen enintään yhdeksi vuodeksi	on tuomittava sakkoon tai vankeuteen enintään kahdeksi vuodeksi

Tietomurto, luvaton käyttö ja vahingonteko

Erityisesti TCB-jutun yhteydessä tuli lisäksi selvästi ilmi tietomurron ja luvattoman käytön välisen suhteen ongelmallisuus. Samoin käräjäoikeuden kannan-

otto vahingontekosäännöksen sovellettavuuden suhteen ehti jo herättää epäilyn siitä, olisiko rikoslain 35 luvun 1 §:n 2 momenttia itse asiassa kovinkaan usein mahdollista soveltaa – oikeudeton tietojen muuttaminen tai turmeleminen ei voine yleensä tapahtua ilman, että samalla toteutuisi myös luvattoman käytön tunnusmerkistö. Vaasan hovioikeuden kannanotto kuitenkin poisti epäilyn.

Ongelmallinen voisi olla myös – luvattoman käytön täyttymisasteelle asetettavasta rajasta riippuen – sellainen tilanne, jossa tietojärjestelmään on tosin tunkeuduttu mutta jossa tietojärjestelmää ei ole varsinaisesti käytetty,[237] onpahan vain tyydytty esimerkiksi turmelemaan jokin järjestelmässä ollut tallennus. Tietomurto ja vahingonteko ovat kumpikin toisiinsa nähden syrjäytyviä säännöksiä, joten näyttäisi jopa siltä, että sovellettavaa säännöstä ei ole!

Näiden viimeksi mainittujen rajanvetokysymysten käytännön merkitys ei ole mitenkään erityisen suuri, sillä rikoksentekijä ei kuitenkaan jää rangaistuksetta (ellei sitten kysymyksessä satu olemaan juuri äsken mainittu tietomurto–vahingonteko-tilanne) eikä lainkohdan valinnalla ole rangaistuksen määrään olennaista vaikutusta, kun kaikista teoista on säädetty samat seuraamusuhat.

Yhteenvetoa

Edellä olevan perusteella näyttääkin nyt ilmeiseltä, että huolimatta tietotekniikkarikoksia koskevien tunnusmerkistöjen aikaisemmin todetusta (näennäisestä) päällekkäisyydestä – leikkaavuudesta – liittyy sovellettavan tunnusmerkistön valintaan vain harvoin kysymys todellisesta lainkonkurrenssitilanteesta. Yleensä soveltamisongelma ratkeaa tekijän tarkoituksen ja tosiasiallisen tapahtumainkulun selvittämisellä samoin kuin säännöksen ensisijaisen suojeluobjektin tarkastelemisella.

Kun ajatellaan rikollista menettelyä, joka toteutetaan tietojärjestelmän oikeudettomalla käyttämisellä tai sitä muistuttavalla teolla, on varhaisimmassa vaiheessa täyttyvä teko tietomurto. Laissa nimenomaisesti sanotuin tavoin tietomurtoa koskeva rangaistussäännös on toissijainen.

Täyttymisastejärjestyksessä tietojärjestelmään tunkeutumista seuraa tietomurron tavoin tietojenkäsittelyrauhaa loukkaava luvaton käyttö, josta puolestaan *saattaa* johtua vahingonteon, petoksen, väärennyksen, yritysvakoilun tai maksuvälinepetoksen tunnusmerkistön täyttyminen. Kaikkiin näihin – ensisijaisesti asianomistajan taloudellisiin intresseihin kohdistuviin tekoihin – näh-

---

[237] Esimerkiksi TCB-jutun päätöksen perusteluissa käräjäoikeus katsoi, että tietyt järjestelmässä tehdyt teot eivät olleet järjestelmän sellaista käyttämistä, joka olisi voinut tulla kysymykseen luvattomana käyttönä, kun ne eivät olleet järjestelmien käyttämistä niille ominaisella tavalla. Vaikka Vaasan hovioikeus totesikin, ettei luvattomassa käytössä voida edellyttää järjestelmää käytettävän sille ominaisella tavalla, ei kuitenkaan liene täysin yksiselitteistä, että järjestelmässä luvattoman käytön yhteydessä tehty teko sinänsä aina olisi luvatonta käyttämistä.

den luvaton käyttö on *itsenäinen* teko, joka tulee lukea tekijän syyksi kulloisenkin *muun* rikoksen ohessa.

Kun tarkastellaan väärennysrikoksen tunnusmerkistöä, voidaan havaita näennäistä leikkaavuutta suhteessa niin vahingonteon kuin petoksenkin tunnusmerkistöön. Automaattiseen tietojenkäsittelyyn soveltuvan tallenteen väärentäminen *voi* tosiasiallisesti merkitä tietovälineelle tallennetun tiedon turmelemista tai koneelliseen tietojenkäsittelyyn puuttumista.

Väärennysrikoksen tunnusmerkistöön ei kuitenkaan kuulu taloudellisten etujen loukkaaminen vaan kriminalisoinnin suojeluobjektina on todistelutarkoituksessa tapahtuvan tiedonvälityksen luotettavuus oikeuselämässä.[238] Tekijältä edellytettävä tahallisuus kohdistuu väärennyksessä harhauttavan todisteen luomiseen tai käyttämiseen, mikä tietysti *välillisesti* saattaa johtaa vahingon aiheutumiseen. Jos tallenteen väärentämisestä *sellaisenaan* aiheutuu vahinkoa, kysymyksessä ei ole vahingontekona erikseen syyksi luettava teko; tässäkin tapauksessa tekijän tarkoitus ratkaisee lopullisesti kysymyksen sovellettavan tunnusmerkistön valinnasta.

Mahdollinen on sellainen tilanne, että tallenteen väärentäjä tai joku muu syöttää tällaisen väärennetyn todistuskappaleen johonkin tietojärjestelmään seurauksin, että tietojenkäsittelyn lopputulos lopulta vääristyy. Tällainen tilanne ei juridisen arviointinsa lopputuloksen puolesta millään tavoin poikkea siitä, että joku väärennettyä asiakirjaa käyttämällä tekee perinteisen erehdyttämispetoksen: tekijän syyksi luetaan sekä väärennys että petos.

Kaiken kaikkiaan voidaan tässäkin yhteydessä korostaa sitä, että tietotekniikkarikosten tarpeetonta mystifiointia on vältettävä. Jatkuvasti muuttuvassa ja ainakin toistaiseksi vielä varsin uudessa ja oudossa tietoteknisessä ympäristössä tapahtuvat teot ovat useimmiten täysin rinnastettavissa niin sanottuihin perinteisiin rikoksiin.

Tietojenkäsittelyrauhan rikkominen?

Edellä on jo esitetty englantilaisen *Computer Misuse Actin* kolmas pykälä, josta *Wasik* kirjoittaa mm. seuraavasti:[239]

> The offence is appropriate to cover all presently conceivable cases involving deliberate alteration or erasure of any program or data held in a computer, where the defendant intended thereby to impair a computer's operation, hinder access to computer material by a legitimate user or impair the operation or reliability of computer held material, and where he knew that the intended modification was unauthorised. It does not have to be proved that the defendant had any specific target computer, program or data in mind.

---

238 Ks. HE 66/1988 s. 109.

239 Wasik, Crim.L.R. 90, s. 770.

Englantilainen säännös ei varmastikaan sellaisenaan suomeksi käännettynä soveltuisi suomalaiseen rikoslainsäädännölliseen systematiikkaan, mutta se on esimerkki siitä, miten yhdellä yleisellä muttei kuitenkaan liian avoimella säännöksellä voidaan välttää useiden samankaltaisten tunnusmerkistöjen soveltamisesta aiheutuvat ongelmat. Säännös – ja koko *Act* – saa myös heräämään epäilyn siitä, onko Suomessa valittu tapa säätää tietotekniikkarikoksista sittenkään ollut paras mahdollinen; niin spesifisiä ongelmia tähän rikosten lajiin kuitenkin liittyy.

Itse asiassa meilläkin olisi saattanut olla mahdollista jopa yhdellä ainoalla tietojenkäsittelyrauhan rikkomista koskevalla kriminalisoinnilla kattaa ne menettelyt, joita nyt tarkoitetaan väärennys-, vahingonteko- ja petossäännöksissä ja mahdollisesti myös tietomurtoa ja luvatonta käyttöä koskevissa säännöksissä, ellei – niin kuin jo aikaisemmin olen useasti joutunut toteamaan – tällainen kriminalisointi olisi ollut vaikeasti sovitettavissa suomalaiseen rikoslakijärjestelmään. Käsittelen kysymystä vielä *de lege ferenda* -jaksossa.

6 Tietotekniikkarikokset ja tahallisuus

Tässä jaksossa tarkoitukseni ei ole syvällisesti ryhtyä käsittelemään yleisiä subjektiiviseen syyksiluettavuuteen liittyviä ongelmia, vaan ainoastaan tutkia, mitä erityispiirteitä tietotekniikkarikosten osalta tahallisuusvaatimukseen saattaa liittyä. Sinänsä tietotekniikkarikokset eivät tahallisuusopillisessa suhteessa ole missään erityisasemassa verrattuna sen paremmin perinteisiin kuin muihin uusimuotoisiinkaan rikoksiin, mutta tekoympäristön monimuotoisuus ja monimutkaisuus sekä useissa tapauksissa ehkä myös tekijän vähäinen tietoisuus aikaan saatujen tai tavoiteltujen tapahtumien todellisesta luonteesta ja merkityksestä saattaa aiheuttaa ongelmia sen suhteen, mitä tekijältä itse asiassa on perustellusti voitu odottaa.

Esimerkki

Voidaan siis ennakoida tilanteita, joissa tietotekniikkarikosten erityislaadusta aiheutuu myös tunnusmerkistöjen subjektiiviseen puoleen liittyviä ongelmia.

> A on jo vuosia valmistellut väitöskirjatutkimusta, jota hän pääasiassa iltaisin on kirjoittanut työpaikkansa tietokoneella. A:n työtoveri B kantaa erinäisistä syistä kaunaa A:lle ja päättää kerran havaittuaan A:n olevan poissa huoneestaan ja A:n tietokoneen olevan auki tehdä A:lle kiusaa hyvin ilkeällä tavalla. Hän menee A:n tietokoneelle, etsii väitöskirjaluonnoksen ja käyttämällä ”delete” -komentoa kuvittelee lopullisesti hävittäneensä A:n vuosien uurastuksen tulokset.
>
> Illalla A yrittää avata väitöskirjatiedoston mutta huomaa yllätykseksi, ettei sitä löydy. A:lla on B:n aikaisempien puheiden perusteella omat epäilyksensä siitä, mitä on tapahtunut, ja niinpä hän joko
>
> 1) kokeileekin ”undelete” -komentoa jolloin väitöskirjatiedosto löytyy ja A pääsee jatkamaan työskentelyään; tai
>
> 2) uskoo tiedoston kadonneen, raivostuu, järkyttyy ja tekee rikosilmoituksen.

Mikäli B olisi ollut paremmin tietojenkäsittelyyn perehtynyt, hän olisi tiennyt, ettei ”delete”-komento suinkaan hävitä tiedostoa minnekään, se vain katkaisee siihen johtavan polun. Tiedosto on olemassa koneen kiintolevyllä ja sieltä edelleen luettavissa niin kauan kuin sen päälle ei ole tallennettu uutta dataa. Vielä tällaisen tallentamisen jälkeenkin suuri osa tiedostosta saattaa säilyä luettavana; suuri tiedosto ei ole kiintolevyllä suinkaan yhtenä kokonaisuutena vaan se on tallentuneena useisiin eri varausyksikköihin, ns. klustereihin. Varausyksikön kokoa (esimerkiksi 16 kilotavua) pienempi tiedosto (esimerkik-

si 1 kilotavu) varaa tallennettaessa koko varausyksikön, ja mikäli kysymyksessä on varausyksikkö, joka on ollut jonkin poistetun tiedoston tai sen osan täyttämä, on jäljelle jäävä 15 kilotavun osa tiedostosta edelleen luettavissa – ei aivan helposti mutta kuitenkin.[240]

B on siis ollut siinä vakaassa käsityksessä, että hän on onnistunut aikomassaan eli tuhonnut A:n työn. Tosiasiallisesti hän on kuitenkin vain piilottanut työn ja piilottanut sen vieläpä melko huonosti, mikäli etsijäksi sattuu asiansa osaava henkilö. Toisaalta on niin, että ajan mittaan väitöskirja tai osia siitä olisi *saattanut* hävitä: mikäli A ei olisi pitkään aikaan työskennellyt tutkimuksensa parissa mutta olisi sen sijaan tallentanut uusia tiedostoja, olisivat nämä saattaneet tallentua B:n poistaman väitöskirjatyön päälle ja tehneet sen mahdottomaksi lukea.

Näyttäisi siis siltä, että B:n aikoman vahingontekorikoksen toteutuminen jäisi kuitenkin ainakin ensisijaisesti riippumaan siitä, millaisiksi A *mieltää* teon seuraukset, eikä siitä, mitkä teon seuraukset tosiasiallisesti ovat. Tässä ei sinänsä ole mitään poikkeuksellista rikoslakia ajatellen, esimerkiksi laittoman uhkauksen tapauksissa asianomistajan omille tuntemuksille on annettava suuri merkitys. Sen sijaan omaisuuteen kohdistuvissa rikoksissa yleensä pystytään objektiivisesti toteamaan vahingon syntyminen tai syntymättä jääminen.

Rikoslain uuden 3 luvun (515/2003) 6 §:n mukaan tekijä on aiheuttanut seurauksen tahallaan, jos hän on tarkoittanut aiheuttaa seurauksen taikka pitänyt seurauksen aiheutumista varmana tai varsin todennäköisenä.

B:llä epäilemättä on ollut vahingonteon edellyttämä tahallisuus, kun hän on tarkoittanut hävittää A:n tekstin. Hän on myös ollut varma siitä, että on teossaan onnistunut. Jos A menettelee ensimmäisessä vaihtoehdossa kuvatuin tavoin ja palauttaa tekstin, on vaikea kuvitella ainakaan vahingonteon tunnusmerkistön täyttyvän; lievästä luvattomasta käytöstä voi olla kysymys. A voi oikeutetusti olla B:lle vihainen.

Mikäli A B:n tavoin uskoo tiedoston lopullisesti hävinneen, hän voi tehdä asiasta rikosilmoituksen. Esitutkinnassa B myöntää hävittäneensä tiedoston ja kertoo tarkkaan, miten hän on hävittämisen tehnyt. Elleivät asiaa käsittelevät viranomaisetkaan ala epäillä tiedoston häviämisen lopullisuutta, B tuomitaan lopulta vahingonteosta rangaistukseen.

Tietoteknisessä ympäristössä yksiselitteisten ja objektiivisten havaintojen tekeminen teoista ja niiden seurauksista on toki mahdollista, mutta se on usein paljon hankalampaa kuin niin sanotussa normaalimaailmassa. *Ikkuna* joko on

---

[240] Ks. esim. Järvinen, Windows 98, s. 363: ”Avain levyn kirjanpitoon on FAT-taulukko (File Allocation Table). Levyn pinta on jaettu varausyksiköihin (cluster), joista jokaista vastaa yksi FAT-taulukon alkio. Jos varausyksikkö on käytössä, FAT-taulukon alkiossa lukee sen varausyksikön numero, josta löytyy tiedoston seuraava palanen. Kun tiedosto halutaan lukea alusta loppuun, FAT-taulukon alkioista muodostuu ketju, joka kertoo mistä kohtaa levyä tiedoston osia pitää kulloinkin hakea.”

tai ei ole rikki ja jos se on rikki, se on rikottu joko tarkoituksellisesti tai vahingossa (joissakin poikkeuksellisissa tilanteissa se on toki saattanut rikkoutua itsestäänkin esimerkiksi valmistusvirheen tai äkillisen lämpötilan vaihtelun johdosta). Jos joku on nähnyt, miten ikkuna on särkynyt, voidaan hänen todistajanlausuntonsa perusteella päätellä, onko ikkunan rikkoja toiminut tahallisesti.

Tallennettua *tiedostoa* on ehkä turmeltu muuttamalla sitä mutta varmuutta muuttamisesta ei välttämättä ole helppo saada. Jos tiedosto havaitaan muutetuksi, saattaa olla hyvin vaikeaa selvittää, kuka teon on tehnyt ja milloin teko on tehty. Muuttamista ei todennäköisesti kukaan ole ollut näkemässä, joten objektiivisia havaintoja tekijän suhtautumisesta ja menettelystä ei ole käytettävissä.

Jos tahallisuudesta jää epäselvyyttä, on syyte tahallisesta rikoksesta hylättävä.[241] Kaikki edellä tietotekniikkarikoksina käsitellyt teot ovat rangaistavia vain tahallisesti tehtyinä. Mitkä ovat ne kriteerit, joiden avulla poliisi ja syyttäjä kykenevät selvittämään yksinäisestä kammiostaan tietoverkoissa ympäri maailmaa operoineen nörttirikollisen subjektiivisen syyksiluettavuuden asteen?[242]

Tahallisuus rikoslaissa

Oikeusministeriön asettaman vuonna 1999 toimintansa lopettaneen rikoslakiprojektin johtoryhmässä käsiteltiin keväällä 1999 ehdotus rikosoikeuden yleisiä oppeja koskeviksi säännöksiksi. Ehdotus johti hallituksen esitykseen 44/2002, jonka pohjalta säädettiin 1.1.2004 voimaan tullut laki rikoslain muuttamisesta.

Rikoslain uuden 3 luvun 6 §:n otsikko on ”Tahallisuus” ja sisältö seuraavanlainen:

> Tekijä on aiheuttanut tunnusmerkistön mukaisen seurauksen tahallaan, jos hän on tarkoittanut aiheuttaa seurauksen taikka pitänyt seurauksen aiheutumista varmana tai varsin todennäköisenä. Seuraus on aiheutettu tahallaan myös, jos tekijä on pitänyt sitä tarkoittamaansa seuraukseen varmasti liittyvänä.

Säännös sai lopullisen muotonsa vasta eduskuntakäsittelyssä.[243] Lakivaliokunta lausuu mietinnössään[244] seuraavasti:

---

241 Nuutila, Rikoslaki, s. 217.

242 Atk-sanakirja, nörtti (engl. nerd) = innokas tietokoneharrastaja.

243 Ks. OLJ 5/2000, erit. s. 82 ss. Ehdotuksessa kysymyksessä oleva lainkohta oli näin kuuluva:
”Tahallisuusvaatimus täyttyy, milloin rikoksen tunnusmerkistön toteutuminen vastaa sitä, mitä tekijä teon hetkellä on
1) tarkoittanut,
2) pitänyt varmana tai varsin todennäköisenä taikka
3) pitänyt varteenotettavana mahdollisuutena, milloin menettelyn on katsottava osoittavan hänen hyväksyneen tunnusmerkistön toteutumisen.”
Hallituksen esityksessä säännös oli selvästi erilainen:
”Teko on tahallinen, jos rikoksen tunnusmerkistön toteutuminen vastaa sitä, mitä tekijä on teon hetkellä tarkoittanut taikka pitänyt varmana tai varsin todennäköisenä.”

244 LaVM 28/2002.

> Ehdotettu tahallisuuden määritelmä koskee sekä seuraus- että olosuhdetahallisuutta. Seuraustahallisuuden määritteleminen ei ole niin vaikeaa tai kiistanalaista kuin rikostyypeittäin vaihtelevan olosuhdetahallisuuden. Ehdotetun säännöksen on katsottu soveltuvan erityisen huonosti talousrikosten olosuhdetahallisuuteen ja voivan nostaa niiden tahallisuuskynnystä. Sen vuoksi valiokunta ehdottaa, että pykälässä säädetään ainoastaan seuraustahallisuudesta. Olosuhdetahallisuus jää oikeuskäytännössä arvioitavaksi, jolloin huomioon on otettava tunnusmerkistöerehdystä koskeva säännös. Seuraustahallisuuden alarajan ehdotetaan määräytyvän korkeimman oikeuden vakiintuneen käytännön mukaisesti sen perusteella, kuinka todennäköisenä tekijä on seurausta pitänyt. Teko on tahallinen, kun tekijä pitää tunnusmerkistönmukaisen seurauksen syntymistä varsin todennäköisenä. Tahallisuuden alarajan määräytyminen jakaa oikeustieteilijöiden mielipiteitä. Eri tahallisuusmääritelmiä voidaan arvostella hyvin perustein ilman, että parhaasta määritelmästä päästään yhteisymmärrykseen. Valiokunta yhtyy perusteluissa esitettyyn näkemykseen, ettei ole esitetty vakuuttavia perusteita säätää korkeimman oikeuden ennakkopäätöksiin perustuvasta vakiintuneesta oikeuskäytännöstä poikkeavaa tahallisuussäännöstä, joka saattaisi johtaa ennalta vaikeasti arvattaviin seurauksiin.

Lopullinen säännös on lakivaliokunnan ehdottaman mukainen. Tietotekniikkarikoksia ajatellen säännöksen soveltaminen ei tuottane kovin suuria ongelmia, sillä ylipäänsä voitaneen katsoa, ettei vallinnutta tilannetta ole haluttu muuttaa. Lienee kuitenkin syytä hieman tarkemmin arvioida juuri tietotekniikkarikoksia erilaisten aikaisemmin esitettyjen tahallisuusopillisten teorioiden ja käsitteiden kannalta.

Tarkoitustahallisuus ja tietojenkäsittelypetos

Ainoa teko, jonka kohdalla Euroopan neuvoston vuoden 1989 raportissa nostetaan esiin kysymys syyksiluettavuuden edellyttämästä tahallisuuden *asteesta,* on tietojenkäsittelypetos; muiden tekojen osalta tyydytään yleensä toteamaan, että tekijän on täytynyt toimia tahallisesti (intentionally). Raportin mukaan[245] tietojenkäsittelypetoksen tekijältä on erityisen hyödyn hankkimistarkoituksen ohessa edellytettävä tahallisuutta, jonka on katsottava käsittävän niin *dolus directuksen* kuin *dolus eventualiksenkin.*

Rikoslain 36 luvun 1 §:n 2 momentin petostunnusmerkistön mukaiselta tahallisuudelta on edellytettävä (1) hyödyn hankkimis- tai vahingoittamistarkoitusta ja (2) tietoisuutta syötettävien tietojen vääryydestä tai siitä, että muu tietojenkäsittelyyn puuttuminen aiheuttaa tietojenkäsittelyn lopputuloksen vääristymisen.

---

[245] EN:n raportti 89, s. 29.

Tarkasteltaessa tietojenkäsittelypetoksen tahallisuusvaatimusta jo perinteiseksi katsottavan tahallisuuden asteiden kolmijaon *(dolus determinatus, d. directus ja d. eventualis)* kannalta ei raskaimman lajin – tarkoitustahallisuuden[246] – suhteen aiheudu ongelmia. *Matikkala* [247] edellyttää tarkoitustahallisuudelta toisaalta sitä, että henkilö pitää seurauksen syntymistä mahdollisena (kognitiivinen puoli) ja toisaalta sitä, että hän pyrkii aiheuttamaan seurauksen, että hän toimii aiheuttaakseen seurauksen (volitatiivinen puoli).

Nuutilan[248] mukaan tarkoitustahallisuudella tarkoitetaan sitä selväpiirteistä tapausta, jossa tekijän tarkoituksena on saada aikaan seuraus. Tekijä tahtoo, tarkoittaa tai tavoittelee jotakin. Tekijän mieltämälle seurauksen sattumisen todennäköisyydelle ei tässä tahallisuustyypissä *Nuutilan* mukaan panna juuri painoa. Täysin merkityksetön ei vahinkoseurauksen mielletty todennäköisyysaste kuitenkaan ole, sillä silloinkin, kun tekijä tahtoo aiheuttaa seurauksen, on edellytettävä, että seuraus voi sattua huomioon otettavan todennäköisyyden puitteissa.

Rikosoikeuden yleisiä oppeja koskevan ehdotuksen perusteluissa todetaan, että determinatus-tahallisuus ei edellytä arviota onnistumisen mahdollisuuksista, mutta viitataan oikeuskirjallisuuteen, jossa esitetyn mukaan vaaditaan kuitenkin, että kyse ei ole pelkästään epärealistisesta toiveajattelusta. Sellaisen tarkoitetun seurauksen syntymistä, jota tekijä asiallisesti ottaen piti poissuljettuna mahdollisuutena, ei voida lukea tekijän syyksi tahallisena.[249]

Lehtosen[250] mukaan tekijällä pitää olla tietoisuus seuraukseen johtavasta kausaalikulusta. Tekijän mielikuvan ja todellisen kausaalikulun ei tarvitse vastata täysin toisiaan. Tietoisuutta ei vaadita yksityiskohtaisesta tapahtumainkulusta.

Tietojenkäsittelypetoksen tekijällä on siis oltava tarkoitus hankkia hyötyä tai aiheuttaa vahinkoa ja tähän *mahdollisena pitämäänsä* seuraukseen hän pyrkii manipuloimalla automaattista tietojenkäsittelyä tavalla, joka mahdollistaa seurauksen toteutumisen. Edellä esitetyssä esimerkissä B:llä on ollut tarkoitus hävittää A:n tiedosto ja tähän uskomaansa seuraukseen hän on pyrkinyt käyttämällä ”delete”-komentoa, mikä menettely olisi tosiasiallisestikin ajan mittaan *saattanut* johtaa tiedoston ainakin osittaiseen häviämiseen. Koska B:n tahtoma seuraus siis voisi tapahtua muutenkin kuin vain A:n luulemana, ei B:n tuomitseminen tahallisesta vahingonteosta ole väärin.

---

[246] Honkasalon mukaan tarkoitustahallisuudella ymmärretään tilanteita, joissa seurauksen saavuttaminen on ollut tekijän tarkoituksena. Ks. Yleiset opit II, s. 81 s. Fränden määritelmä on hieman toisenlainen: gärningsmannen utför handlingen i en viss avsikt, varvid den insedda och även straffrättsligt relevanta följden får honom att handla (Frände, Straffrätt, s. 123). – Tietojenkäsittelypetoksen kannalta ei määrittelyjen eroavuuksilla ole merkitystä.

[247] Matikkala, Vastuu, s. 199

[248] Nuutila, Rikoslaki, s. 217.

[249] Ks. OLJ 5/2000, s. 83.

[250] Lehtonen, Veropetos, s. 369.

Varmuustahallisuus ja tietotekniikkarikokset

Dolus directuksen eli varmuustahallisuuden piiriin luettavat tapaukset saattavat olla tarkoitustahallisuuden tilanteita ongelmallisempia erityisesti silloin, kun joudutaan pohtimaan tietojenkäsittelypetoksen ja muiden tietotekniikkarikosten välistä rajanvetoa. *Honkasalon* mukaan puheena oleva tahallisuuden aste on kysymyksessä, kun tekijä ei ole seurausta suorastaan tarkoittanut mutta on nähnyt sen tavoittelemaansa päämäärän välttämättömästi liittyväksi.[251]

Fränden määritelmä on asiallisesti samanlainen: tekijällä on tietty – laillinen tai laiton – tarkoitus ja tekijä pitää varmana, että tarkoituksen toteutuessa syntyy myös rikosoikeudellisesti relevantti seuraus.[252] *Matikkalan* mukaan *d. directus* kognitiivisesti edellyttää seurauksen pitämistä varmana, mutta ei sisällä varsinaista voluntatiivista elementtiä; varmuustahallisuuden piiriin voidaan lukea myös ne tapaukset, joissa seuraus on tekijän päätavoitteeseen nähden sen välttämätön sivuseuraus.[253]

Nuutilan mukaan varmuustahallisuuteen ei sisälly tahtomomenttia suhteessa kiellettyihin seurauksiin. Tahallisesti menettelee se, joka ei suoranaisesti pyri kielletyn seurauksen aikaansaamiseen mutta joka ymmärtää tavoittelemansa päämäärän saavuttamiseen liittyvän käytännöllisellä varmuudella myös kielletyn seurauksen aiheutuminen.[254] Vastuu seuraa siihen katsomatta, pitikö tekijä oheisseurauksia tavoittelemisen arvoisina vai peräti epätoivottavina.[255]

Vaikka *d. directus* näyttäisikin siis olevan jokseenkin lähellä *d. determinatusta,* voidaan niiden eroa konkretisoida tietotekniikkarikosten kohdalla esimerkiksi seuraavalla tavalla:

> A haluaa aiheuttaa kilpailijalleen B:lle taloudellista vahinkoa. Tätä tarkoitustaan hän ryhtyy toteuttamaan tunkeutumalla B:n omistaman yrityksen tietojärjestelmään ja poistamalla siellä käsiteltävänä ollutta maksuliikenteeseen liittynyttä informaatiota. A:n menettelystä saattaa olla seurauksena, että
> 1) B:n yritys jättää huomattavan määrän laskuja perimättä ja kärsii taloudellista vahinkoa; tai
> 2) tapahtunut havaitaan yrityksessä ja tiedostot palautetaan ennalleen, mistä aiheutuu runsaasti kustannuksia.

A:n menettelyä tulee lähtökohtaisesti arvioida tietojenkäsittelypetoksena. A:lla on ollut selvä tarkoitus aiheuttaa B:lle vahinkoa puuttumalla yrityksen tietojenkäsittelyyn ja saamalla sen lopputulos vääristymään. Ensimmäisessä vaihtoehdossa A:n tarkoitus toteutuukin juuri hänen haluamallaan tavalla.

---

[251] Ks. Yleiset opit, s. 83 s.
[252] Ks. Frände, Straffrätt, s. 126 s.
[253] Matikkala, Vastuu, s. 199.
[254] Nuutila, Rikoslaki, s. 218 s.
[255] Näin OLJ 5/2000, s. 83.

Tietojenkäsittelypetoksen ohella A on syyllistynyt tietomurtoon (josta tosin ei erikseen rangaista) ja luvattomaan käyttöön. Näiden tunnusmerkistöjen täyttyminen on ollut A:n tavoitteleman päämäärän saavuttamisen välttämätön edellytys, mikä A:n on täytynyt ymmärtää. Tietojenkäsittelypetoksen kohdalla A:n tahallisuutta on pidettävä tarkoitustahallisuutena kun taas luvattoman käytön ja tietomurron osalta kysymys on varmuustahallisuudesta.

Vaihtoehdoista jälkimmäisen toteutuessa tilanne muuttuu mielenkiintoiseksi. B:lle aiheutuu A:n menettelystä vahinkoa mutta vahinko ei synny A:n tarkoittamalla tavalla. A on menetellyt samalla tavalla ja on täysin A:sta riippumatonta, että vahinko nyt aiheutuukin toisella tavalla. Objektiivisesti arvioiden A:n menettely täyttää sekä petoksen yrityksen että vahingonteon tunnusmerkistön; vahinko ei ole johtunut tietojenkäsittelyn lopputuloksen vääristymisestä eikä petoksen tunnusmerkistö näin ollen täyty. A:lla on ollut vahingoittamisen tarkoitus, joten sikäli myös vahingonteon subjektiivinen tunnusmerkistö voisi täyttyä. Tilanteeseen sopinee edellä esitetty *Lehtosen* lausuma: tietoisuutta ei vaadita yksityiskohtaisesta tapahtumainkulusta. Syyttäjänä lähtisin arvioimaan tapausta ensi sijassa petoksen yrityksenä.[256]

Ehdollinen tahallisuus ja tietotekniikkarikokset

Tilanne mutkistuu siirryttäessä tahallisuuden lievimmän asteen ehdollisen tahallisuuden eli *d. eventualiksen* tarkastelemiseen; jo käsite sinänsä on vaikeaselkoinen. *Honkasalo* katsoo puheena olevan tahallisuuden asteen olevan kysymyksessä, kun tekijä ei ole seurausta suorastaan tarkoittanut eikä mieltänyt sitä myöskään tarkoittamaansa seuraukseen välttämättömästi liittyväksi, vaan on mieltänyt, että hänen jotakin luvallista tai luvatonta päämäärää tavoittelevasta teostaan jonkinmoisella todennäköisyydellä voi syntyä rikosoikeudellisesti relevantti seuraus.[257]

Honkasalon mukaan paras ohje rajan vetämiseksi tahallisuuden lievimmän asteen ja tuottamuksen välille saadaan positiivisesta tahtoteoriasta, siitä, onko tekijän tahdon suhtautuminen miellettyyn seuraukseen myönteinen. *Frände* pitää parempana puhua tässä kohden välinpitämättömyystahallisuudesta (likgiltighetsuppsåt).[258]

Toinen *Honkasalon* esittelemä tahallisuuden ja tuottamuksen välistä rajanvetoa koskeva teoria on mieltämisteoria, jonka mukaan merkitsevä on se todennäköisyyden aste, jolla tekijä on mieltänyt seurauksen johtuvan teostaan. *Frände*

---

[256] Tietotekniikkarikosten erityislaatua osoittaa se, että olisi kovin vaikeaa kuvitella tilannetta, jossa jouduttaisiin pohtimaan RL 36:1.1:n mukaisen erehdyttämispetoksen yrityksen ja RL 35:1.1:ssä tarkoitetun vahingonteon tunnusmerkistöjen mahdollista päällekkäisyyttä.

[257] Yleiset opit II, s. 84 ss.

[258] Frände, Straffrätt, s. 127 ss.

käyttää tässä käsitettä todennäköisyystahallisuus (sannolikhetsuppsåt): koska tekijä on ymmärtänyt, että hänen tekonsa varsin todennäköisesti tulee aiheuttamaan tietyn seurauksen, hän on aiheuttanut seurauksen tahallisesti. *Fränden* mukaan molemmat – sekä tahto- että mieltämisteoria – ovat oikeassa, eikä hän ota kantaa niiden paremmuusjärjestykseen.

Matikkala on todennut oikeuskäytännön 1970-luvun loppupuolelta alkaen ilmentäneen mieltämisteorian omaksumista, vaikkakaan positiivista tahtoteoriaa ei käytännössä ole unohdettu.[259] Kuitenkin johtopäätös, että vallitseva sisältönormi oikeuskäytännössä olisi painottunut mieltämisteorian mukaiseksi, on Matikkalan mukaan varsin relatiivinen muun muassa siitä syystä, että pääosa ennakkopäätöksistä koskee surmaamistahallisuutta.[260]

Nuutila toteaa, että tahallisuutta ei voida perustaa sen varaan, että tekijän olisi pitänyt mieltää seuraus todennäköiseksi, koska tällaisen tekijään kohdistuvan vaatimuksen asettaminen kuuluu vain tuottamukseen. ”Vaikka olisimme sitä mieltä, että lähes kuka tahansa olisi tilanteessa mieltänyt aiheuttavansa seurauksen, tekoa ei voida pitää tahallisena, jos ei voida osoittaa *myös tekijän* tosiasiassa mieltäneen seurauksen todennäköisyyttä”, kirjoittaa *Nuutila.*[261]

Menemättä tässä tämän syvemmälle syyksiluettavuusoppien tarkasteluun voidaan todeta, että jos *dolus eventualiksen* käsite on vaikea yleensä, on se sitä myös tietotekniikkarikosten kohdalla.

> Tietojärjestelmään tunkeutuneen hakkerin nimenomaisena tarkoituksena saattaa olla vain seikkailla järjestelmässä. Järjestelmä voi kuitenkin olla sellainen, että pienikin huolimattomuus saattaa aiheuttaa muutoksia datassa, ja nämä muutokset puolestaan kenties aiheuttavat vahinkoa joko itsessään tai sitten vaikuttamalla tietojenkäsittelyn lopputulokseen. Jos hakkeri on *mieltänyt,* että hänen teostaan (joka tarkoitustahallisuuden kannalta ajateltuna olisi luvatonta käyttöä) saattaa ”jonkinmoisella todennäköisyydellä” tai ”varsin todennäköisesti” aiheutua datan sellainen muuttuminen, että järjestelmän haltijalle joko suoranaisesti (tärkeää tietoa katoaa) tai välillisesti (tietojenkäsittelyn lopputulos vääristyy) koituu vahinkoa, onkin tilannetta lähdettävä arvioimaan vahingonteko- ja petostunnusmerkistöjen valossa.
>
> Saattaa olla myös niin, että hakkerin tarkoituksena on ollut ainoastaan pyrkiä suojaukset murtamalla pääsemään sisälle järjestelmään mutta tyytyä pelkästään tähän; toisin sanoen subjektiivisessa suhteessa hänen tahallisuutensa ei ole ulottunut tietomurron tunnusmerkistön toteuttavaa menettelyä pitemmälle. Jostain hänen tietoisesti tahtomattomastaan syystä teko kuitenkin on saattanut objektiivisessa suhteessa edetä luvat-

---

[259] Matikkala, LM 92, s. 962 ss. Ks. myös OLJ 5/2000, s. 84.

[260] Ks. myös Matikkala, Vastuu, s. 207 ss., jossa Matikkala on perusteellisesti käsitellyt surmaamistahallisuutta koskevaa oikeuskäytäntöä

[261] Nuutila, Rikoslaki, s. 224.

> toman käytön asteelle. Kummankaan rikoksen tunnusmerkistötekijöihin ei kuulu vahingon aiheutuminen, mutta voitaneen lähtökohtaisesti olettaa, että osaavan hakkerin *on miellettävä* ainakin tietojärjestelmän käynnistymisen mahdollisuuden olemassaolo.

Tällöin voitaisiin katsoa, että *d. eventualis* -tyyppinen tahallisuus olisi olemassa myös luvattomaan käyttöön nähden, mistä puolestaan hieman kärjistäen voitaisiin päätellä, että tietomurron onnistuessa juuri tarkoitetulla tavalla olisi tuolloin itse asiassa kysymys luvattoman käytön yrityksestä. Lähtökohtaisesti näin ei voida väittää, mutta asetelma ei kuitenkaan liene täysin poissuljettu, sillä joissakin yksittäistapauksissa – tekijän tiedoista ja taidoista ja kysymyksessä olevasta järjestelmästä riippuen – järjestelmän käynnistymisen mahdollisuutta voitaisiin ehkä pitää tunkeutumisen varsin todennäköisenä seurauksena.

Tietotekniikkarikoksiin liittyvä syyksiluettavuusproblematiikka osaltaan osoittaa sitä edellä useaan kertaan havaittua tosiasiaa, että tietotekniikkarikosten tunnusmerkistöjen väliset rajat eivät ole selkeitä.

Tekijän taitotieto

Kovin suurta elämänkokemusta ei vaadita sen ymmärtämiseen, että ikkuna varsin todennäköisesti särkyy, jos siihen heitetään riittävän suuri kivi riittävän voimakkaasti. Jokaisen liiketoimintaa harjoittavan kirjanpitovelvollisen on ymmärrettävä, että kirjanpidon täydellinen laiminlyöminen vaikeuttaa oikean ja riittävän kuvan saamista kirjanpitovelvollisen toiminnan taloudellisesta tuloksesta tai taloudellisesta asemasta. Jokaiselta tienkäyttäjältä voidaan edellyttää sen ymmärtämistä, että kiskoilla kulkevan ajoneuvon on varsin vaikeaa – suorastaan mahdotonta – tehdä äkkinäisiä väistöliikkeitä.

Tietotekniikan käyttäjiä on Suomessa paljon, varmastikin runsaasti yli puolet kansasta joutuu nykyään työtehtävissään tai kotonaan tekemisiin erilaisten tietoteknisten sovellusten kanssa. Kuinkahan moni tekstinkäsittelyä työkseen tai harrastuksekseen suorittavista tietää, mitä tekstitiedostolle tapahtuu ”delete” -komennolla tai miten ”tallenna” -komento saa tietokoneen täyttämään kiintolevyn klustereita? Onko jokainen sähköpostin lähettäjä selvillä siitä, että vaikkapa Helsingistä Turkuun lähetetty sähköpostiviesti saattaa kulkea 10–20 reitittimen[262] kautta, jolloin reititinten lokeihin tallentuu tietoja viestistä?[263] Mahtaako kaikille Internetin käyttäjille olla selvää, että tarvittaessa heidän surffailureittinsä ovat hyvinkin tarkkaan selvitettävissä?

Tietojenkäsittelyä hyödyntävä henkilö ei siis välttämättä ollenkaan tiedä, millaisia tapahtumaketjuja hänen koneelle antamansa käskyt käynnistävät, eikä

---

[262] Atk-sanakirja, s. 161: reititin (engl. router) = verkon solmussa laite tai ohjelmisto, joka ohjaa osoitteen perusteella verkossa siirrettävää tietoa, mahdollisesti erilaiseen verkkoon.

[263] Sähköpostin kulusta ks. Kiviniemi, s. 185 ss.

välttämättä lainkaan pysty ennakoimaan jonkin menettelynsä seurauksia. Jos tällainen henkilö ryhtyy tekemään tietotekniikkarikoksia, ei hän siis välttämättä ole selvillä siitä, millä tavoin hänen aikomansa seuraus toteutuu (jos se ylipäänsä on toteutuakseen). Ja kääntäen: kun tällainen henkilö käyttää tietotekniikkaa, hän voi tahtomattaan saada aikaan sellaisen seurauksen, jonka aiheuttaminen objektiivisesti ajatellen olisi rikollista menettelyä.

Peittämisperiaate

Nuutila kuvailee peittämisperiaatetta sanomalla, että tahallisuuden on ”peitettävä” koko oikeudenvastainen teko.[264] Tekijän on oltava tietoinen kaikista niistä tosiasioista, joista teon rangaistavuus riippuu. Ennen kaikkea tahallisuuden tulee kattaa teonhetkiset olosuhteet ja teosta riippuvat seuraukset. Muut seikat, jotka tahallisuuden tulee kattaa, riippuvat kulloisestakin tunnusmerkistöstä.

Peittäminen ja tietotekniikkarikokset

Tietotekniikkarikosten kohdalla peittäminen saattaa jäädä vajaaksi sen vuoksi, että tekijällä ei ole tietoisuutta kaikista tosiasioista. Näiden rikosten ollessa kysymyksessä se tietämisen taso, joka tekijällä on *täytynyt* olla, jotta hänen menettelyään lähtökohtaisesti voitaisiin pitää tahallisena, on epäilemättä keskimääräistä korkeampi. Tekijän *täytyy* tosiasiassa mieltää tietyn tapahtuman voivan olla hänen menettelynsä todennäköinen seuraus, mutta tällaista mieltämistä tuskin voidaan edellyttää, jos tekijä ei tiedä riittävästi tietojärjestelmän toiminnasta ymmärtääkseen edes pääpiirteisesti, mitä toimintoja hänen antamansa käskyt saavat aikaan.

Jonkin tietotekniikkarikoksen tunnusmerkistöön kuuluvan seurauksen aiheuttaminen sitä tahtomatta voi siis pääsääntöisesti tulla tahallisena rikoksena rangaistavaksi vain, jos tekijällä on ollut riittävän hyvä tietotekniikan tuntemus, jotta hän on *voinut* mieltää seurauksen todennäköiseksi.

Henkilö saattaa ilkivaltaisessa tarkoituksessa lähettää jollekulle tämän pyytämättä sähköpostin liitteenä sisällöltään rikollisen, esimerkiksi lapsipornografista kuvamateriaalia sisältävän kymmenien megatavujen suuruisen tiedoston osaamatta ottaa huomioon, että vastaanottajan vanhalla hitaalla modeemilla tiedoston vastaanottaminen kestää pahimmillaan tuntikausia ja estää sähköpostin muun käyttämisen. Objektiivisesti ajatellen tällainen roskapostin lähettäminen voisi olla tietoliikenteen häirintää mutta sitä ei lähettäjän tahallisuus kata, jos hän ei ole ollut selvillä modeemin nopeuden käytännön merkityksestä, vaan menettely on arvioitavissa ainoastaan rikoslain 17 luvun säännösten valossa.

---

[264] Nuutila, Rikoslaki, s. 227 ss.

Erehdys ja selonottovelvollisuus

Nuutila jakaa erehdykset kolmeen eri tyyppiin: tunnusmerkistöerehdykseen, kieltoerehdykseen ja soveltamiserehdykseen.[265] Ensin mainittu merkitsee erehtymistä jonkin tunnusmerkistössä tarkoitetun tosiasian olemassaolosta ja asioiden tosiasiallisesta tilasta, kieltoerehdyksen ollessa kysymyksessä tekijä erehtyy menettelynsä lainmukaisuudesta, ja soveltamiserehdyksestä voidaan *Nuutilan* mukaan puhua silloin, kun tekijä tuntee kiellon pääpiirteissään ja tuntee tosiasiat mutta soveltaa lakia mielessään toisella tavoin kuin tuomioistuin. Tunnusmerkistöerehdys yleensä poistaa tahallisuuden.[266] Kieltoerehdys ei vaikuta tahallisuuteen mutta saattaa tulla kysymykseen anteeksiantoperusteena. Soveltamiserehdyksen kohdalla kysymys on siitä, sallitaanko tekijän luottaa käsitykseensä vai asetetaanko hänelle selonottovelvollisuus.[267]

Rikosoikeuden yleisten oppien uudistus toi rikoslakiin kolme nimenomaista säännöstä erehdyksestä: 4 luvun 1 § koskee tunnusmerkistöerehdystä, 2 § kieltoerehdystä ja 3 § vastuusta vapauttavaa seikkaa koskevaa erehdystä.[268]

Tietotekniikkarikosten kohdalla on helppoa kuvitella erilaisia erehtymistilanteita. Tietojärjestelmän käyttäjällä ei vastoin luuloaan olekaan oikeutta käyttää kysymyksessä olevaa järjestelmää. Henkilö saattaa erehdyksessä viedä virustarkistamattoman levykkeen kotoaan työpaikalle ja saastuttaa työpaikan tietojärjestelmän. Henkilö saattaa muuttaa sellaista dataa, joka vastoin hänen luuloaan onkin merkityksellinen todistuskappale. Edelleen henkilö saattaa syöttää tietojärjestelmään dataa, joka vastoin hänen uskoaan aiheuttaakin vahinkoa järjestelmässä oleville tiedoille.

---

[265] Nuutila, Rikoslaki, s. 233 s. Aikaisemmista käsityksistä ks. esim. Vikatmaa, s. 184 ss.

[266] Ks. myös Frände, Grundelement, s. 65 ss. Frände toteaa mm. seuraavaa: ”Den grundläggande typen av rekvisitvillfarelse innebär således att gärningsmannen inte alls har uppskattat sannolikheten för en viss följd. Ex post kan man säga att han inte alls insåg den ontologiska möjligheten för följd. Gärningsmannen saknar nödvändig kunskap.”

[267] Selonottovelvollisuudesta ks. Vikatmaa s. 120 ss. Vikatmaa esittää kysymyksen ”Voidaanko selonottovelvollisuus oikeutemme mukaan teorian tasolla asettaa?” ja vastaa siihen varovaisen myönteisesti toteamalla, ettei tässä vaiheessa ole ilmaantunut vakavaa estettä mainitun velvollisuuden asettamiselle oikeutemme kannalta.

[268] *1 §: ”Tunnusmerkistöerehdys.* Jos tekijä ei teon hetkellä ole selvillä kaikkien niiden seikkojen käsilläolosta, joita rikoksen tunnusmerkistön toteutuminen edellyttää, tai jos hän erehtyy sellaisesta seikasta, teko ei ole tahallinen. Vastuu tuottamuksellisesta rikoksesta voi kuitenkin tulla kysymykseen tuottamuksen rangaistavuutta koskevien säännösten mukaan.” *2 §: ”Kieltoerehdys.* Jos tekijä erehtyy pitämään tekoaan sallittuna, hän on rangaistusvastuusta vapaa, jos erehtymistä on pidettävä ilmeisen anteeksiannettavana seuraavien seikkojen vuoksi: (1) lain puutteellinen tai virheellinen julkistaminen; (2) lain sisällön erityinen vaikeaselkoisuus; (3) viranomaisen virheellinen neuvo; tai (4) muu näihin rinnastettava seikka.” *3 §: ”Vastuusta vapauttavaa seikkaa koskeva erehdys.* Jos tekoon ei liity 4–6 §:ssä tarkoitettua vastuuvapausperustetta, mutta tekotilanteeseen, sellaisena kuin tekijä sen perustellusti käsitti, olisi tällainen peruste liittynyt, häntä ei rangaista tahallisesta rikoksesta. Vastuu tuottamuksellisesta rikoksesta voi kuitenkin tulla kysymykseen tuottamuksen rangaistavuutta koskevien säännösten mukaan.”

Tahallisuuden kannalta nämä tilanteet eivät sinänsä ole ongelmallisia: Erehdys poistaa tahallisuuden, eivätkä teot ole tuottamuksellisina rangaistavia. Mutta kuinka pitkälle menevä velvollisuus henkilöllä on selvittää, onko hän oikeutettu käyttämään järjestelmää, onko levyke virustarkistettu, onko tallennettu data luonteeltaan todistuskappale, minkä luonteista on hänen syöttämänsä data?

Vastaus tähän kysymykseen riippuu mielestäni suuresti kysymyksessä olevan henkilön tietoteknisen tietämyksen tasosta – ainakin silloin, kun erehdys on luokiteltavissa soveltamiserehdyskategoriaan. Toisaalta on toki niin, että mitä paremmat tiedot henkilöllä on tietoteknisistä kysymyksistä, prosesseista ja järjestelmistä, sitä suuremmalla syyllä hänen voidaan lähtökohtaisesti vaatia ymmärtävän toimiensa merkityksen, mutta toisaalta syvällisempi tietämys merkitsee myös sitä, että hänellä on paremmat edellytykset ymmärtää selonotto-*mahdollisuuksien* olemassaolo.[269]

Näin ollen esimerkiksi sellaisen henkilön selonottovelvollisuus, joka työpaikallaan jonkun työtoverinsa huoneessa tämän (vastoin kaikkia tietoturvallisuusperiaatteita) avoimeksi jättämää työasemaa sinänsä hänelle kuuluviin työtehtäviin, mutta ilman nimenomaista lupaa käyttäessään joutuukin sellaiseen järjestelmän osaan, johon hän omalta koneeltaan ei pääsisi, jää nähdäkseni riippumaan hänen tietämyksestään ja kokemuksestaan: jos hän on työtehtävissään käyttänyt lähinnä tekstinkäsittelyohjelmia perehtymättä sen syvällisemmin tietojärjestelmän rakenteeseen, ei voitane kohtuudella edellyttää, että hän ryhtyisi selvittämään, onko hänen tilapäisesti käyttämältään koneelta vaara joutua luvattomille teille. Jos hän taas sattuukin olemaan vaikkapa työpaikan atk-tukihenkilö, on hänen ymmärrettävä, että toisen koneesta saattaa löytyä sellaista kvalifioitua tietoa, jota ei toisten luettavaksi ole lainkaan aiottu.

Samoin levykkeen tarkistamisen virusinfektion varalta on katsottava kuuluvan atk-tukihenkilön normaaleihin rutiineihin, kun taas esimerkiksi yleensä pelkästään asianhallintajärjestelmällä työhuoneessaan syytteitä laativan kihlakunnansyyttäjän ei välttämättä voida edellyttää ymmärtävän tartunnan vaaran olemassaoloa ja ryhtyvän toimenpiteisiin vaaran poistamiseksi.[270]

Eräänlaisena selonottovelvollisuuden vastakohtana *Nuutila* näkee luottamusperiaatteen, jonka mukaan henkilö saa luottaa niihin tietoihin, joita hänellä on tai joita hän on saanut.[271] Luottamusperiaatteen ja selonottovelvollisuuden väli-

---

[269] Ks. Nuutila, Rikoslaki, s. 244 s., jossa Nuutila käsittelee tätä sivuavaa kysymystä ja toteaa, että erehtyjän sosiaalisella asemalla on merkitystä arvioitaessa selonottovelvollisuuden laajuutta. Mitä vastuullisemmassa tehtävässä ja paremmin koulutettu henkilö on, sitä voimakkaampana voidaan selonottovelvollisuutta pitää.

[270] Tältä osin totuus on kylläkin jo toisenlainen: oikeushallinnon tietojärjestelmässä annetaan aika ajoin virusvaroituksia, eikä yhdellekään syyttäjälle tai tuomarille enää pitäisi olla epäselvää, että virukset ovat todellinen uhka.

[271] Nuutila, Rikoslaki, s. 244.

nen suhde riippuu *Nuutilan* mukaan osaltaan myös rikoksen laadusta: mitä vähäisemmästä rikoksesta on kysymys, sitä lievempi lienee selonottovelvollisuuskin ja sitä laajempi vastaavasti luottamuksensuoja.

Johtopäätöksiä

Kaiken kaikkiaan siis tahallisuusvaatimuksen arviointi tietotekniikkarikosten kohdalla saattaa jonkin verran poiketa niin sanotuista perinteisistä rikoksista yleensä – ei toki aina; silloin, kun kysymyksessä on jokin erikoisrikos, esimerkiksi vero- tai ympäristörikos, esiintyy epäilemättä tilanteita, joissa tekijältä on edellytettävä keskimääräistä korkeampaa tietoa jostakin spesifisestä kysymyksestä, jotta hänen voitaisiin katsoa voineen mieltää seuraus todennäköiseksi. Mutta pääsäännöksi voitaneen hyväksyä, että tietotekniikkarikoksen lukeminen tekijänsä viaksi tahallisena tekona edellyttää tekijältä sellaista tietoteknistä taitotietoa, joka mahdollistaa oman menettelyn arvioimisen tietojenkäsittelytapahtuman kannalta.

Seuraus- ja varmuustahallisuudet eivät ole tietotekniikkarikostenkaan kohdalla erityisen ongelmallisia. Sen sijaan tahallisuuden alimman asteen ja tuottamuksen välisen rajan määritteleminen on käytännönkin kannalta tärkeää, koska yksikään edellä käsitellyistä tietotekniikkarikoksista ei ole rangaistava tuottamuksellisena.[272]

Tietomurron osalta tätä rajanvetoa tuskin joudutaan liiemmälti pohtimaan, sillä turvajärjestelyn murtamisen tulee tapahtua jollakin tekijän nimenomaisella toimella ja tekijä yleensä tiennee, mitä on tekemässä. Luvattoman käytön osalta tilanne on jo toinen, sillä tekijän täytyisi olla tietoinen paitsi käyttämisen luvattomuudesta myös siitä, että hän ylipäänsä käyttää tietojärjestelmää. Edellä luvatonta käyttöä käsiteltäessä on tullut ilmi, että rikoslaissa tarkoitettu käyttämisen käsite itsessään ei ole ollenkaan selvä edes lainkäyttäjille. Voidaanko edellyttää käsitteen olevan sen selvempi niille henkilöille, joiden tekemisiin lakia sovelletaan?

Väärennyksen, petoksen ja vahingonteon kohdalla ongelmat ovat samansuuntaisia. Tekijän on voitava pitää todennäköisenä, että hänen toimimisensa tietojärjestelmässä saattaa johtaa tallenteen tai tietojenkäsittelyn lopputuloksen muuttumiseen tai tallennettujen tietojen turmeltumiseen. Tämä taas yleensä edellyttää, että tekijän täytyy tietää, mitä hänen antamiensa käskyjen seurauksena tietojärjestelmässä tapahtuu.

---

[272] Silloin, kun rikoslain 34 luvun 9a §:ää ryhdyttiin oikeusministeriössä valmistelemaan, oli alkuvaiheessa esillä ajatus, että vahingollisen ohjelman levittäminen olisi kriminalisoitu myös törkeästä huolimattomuudesta tehtynä. Tämä kohtasi kuitenkin sellaista vastustusta eri tahoilta, että ajatuksesta ainakin tässä vaiheessa luovuttiin.

7 Arvioita ja ehdotuksia

7.1 VOIMASSA OLEVAN TIETOJENKÄSITTELY-RAUHAA SUOJAAVAN SÄÄNNÖSTÖN ARVIOINTIA

Yleistä

Ajateltaessa edellä osan II luvuissa 2–4 käsiteltyjen säännösten kattavuutta yleensä voidaan epäilemättä sanoa, että ne eivät juuri aukkoja jätä: ne ovat sovellettavissa lähes kaikkeen sellaiseen tietojenkäsittelyrauhaa vaarantavaan menettelyyn, jonka tämänhetkisen tietämyksen perusteella voidaan katsoa vaativan rikosoikeudellista sääntelyä. Tilanne muuttui vielä oleellisesti entistä paremmaksi sen jälkeen, kun vaaran aiheuttamista tietojenkäsittelylle koskeva säännös tuli voimaan.

Myös kansainvälisesti tarkasteltuna suomalainen sääntely on korkealla tasolla. Euroopan neuvoston vuoden 1989 suosituksen asettamat vaatimukset on täytetty ja osin ylitettykin ja ilmeistä on, että Euroopan neuvoston tietoverkkorikosyleissopimuksen implementoinnissakaan ei aineellisiin rikosoikeudellisiin säännöksiin kovin paljon tarvitse kajota.

Samoin vertailussa vieraiden valtioiden lainsäädäntöihin Suomi selviytyy kunnialla. Ei voitane suoralta kädeltä osoittaa yhtään sellaista valtiota, jonka tietotekniikkarikoksia koskeva sääntely olisi ainakaan selvästi suomalaista paremmalla tasolla.

Tähän hyvään tilanteeseen vaikuttaa varmasti osaltaan se, että säännökset oli teknisesti helppo uudistaa rikoslain kokonaisuudistuksen yhteydessä, kun jouduttiin muutenkin arvioimaan esimerkiksi perinteisten petos-, väärennys- ja vahingontekorikosten tunnusmerkistöjen kattavuutta. Toisaalta on nähtävissä, että tästä menettelystä on saattanut aiheutua ongelmiakin: kun kaikkia tietotekniikkarikossäännöksiä ei ole kirjoitettu niitä yhtenä rikoskategoriana arvioiden ja kun ne osaksi vielä ajoittuvat kokonaisuudistuksen eri vaiheisiin, ei säännösten keskinäinen suhde aina ole niin selkeä kuin se voisi olla.

Olen edellä esittänyt ajoittain mahdollisesti voimakkaaltakin vaikuttavaa kritiikkiä lainvalmistelua kohtaan. On kuitenkin syytä korostaa, että yleisesti ottaen lainvalmistelun lopputulos on ollut erittäin hyvä ja että ne epäkohdat ja muutostarpeet, joita nyt on havaittavissa, johtuvat valtaosaltaan pikemminkin muutoksista tietoteknisessä ympäristössä kuin lainvalmistelun ja lainsäädännön heikkouksista. Kymmenen vuotta ei rikoslain historiassa ole pitkä aika, mutta tietotekniikan historiassa kymmenen vuoden ajanjakso merkitsee totaalista

muutosta, jonka ennakoiminen ei yksinkertaisesti ole ollut mahdollista. Kritiikin tarkoitus onkin osaltaan korostaa tätä seikkaa ja kiinnittää nykyisten ja tulevien lainvalmistelijoiden huomio esimerkiksi sen yhteistyön merkitykseen, jota lainvalmistelijoiden, lainkäyttäjien ja tietotekniikan ammattilaisten kesken tulisi tehdä pyrittäessä luomaan mahdollisimman kestäviä ja käytännössä helposti sovellettavia rikoslainsäädännöllisiä ratkaisuja harkittavina oleviin ja harkittaviksi tuleviin kysymyksiin.

Käsittelen seuraavassa yhteenvedonomaisesti yksittäisiä säännöksiä lähinnä vielä kriittisiä näkemyksiä esittäen, säännöksissä mielestäni esiintyviä puutteellisuuksia ja virheellisyyksiä esille tuoden. Kokonaisuudessaan säännökset siis kuitenkin vastaavat hyvin edellä mainittuja kansainvälisiä vaatimuksia ja ovat myös kotimaisia käytännön tarpeita ajatellen riittävän kattavia.

Tietomurto ja luvaton käyttö

Olen edellä tietomurtoa ja luvatonta käyttöä käsitellessäni useaan kertaan todennut, että niiden keskinäinen suhde on hankala: teoista on säädetty samanlaiset rangaistusuhat, vaikka niissä kriminalisoidut menettelyt eroavat toisistaan niin, että tietomurron on useassa tapauksessa katsottava sisältyvän luvattomaan käyttöön ja näin ollen syrjäytyvän sen tieltä. Kummankin teon yritys on kriminalisoitu ja näyttää siltä, että sovellettavan säännöksen valinta voisi tapahtua lähes pelkästään tekijän esitutkinnassa selvitetyn tarkoituksen eikä hänen tosiasiallisen menettelynsä perusteella. Toisaalta tällaisen valinnan lopputuloksella, olipa sitten kysymys yrityksestä tai täytetystä teosta, ei ole käytännön kannalta olennaista merkitystä.

Luvattomassa käyttämisessä itse ”käyttämisen” merkityssisältö on epämääräinen eikä käyttämisestä säännöksen perusteluissa sanottu oikein tunnu vastaavan sitä, mitä tietojärjestelmässä käytännössä tapahtuu hakkerin yrittäessä tunkeutua tai tunkeutuessa järjestelmään.

Tietomurron ja luvattoman käytön tunnusmerkistöjen huonoon keskinäiseen yhteensopivuuteen lienee yhtenä syynä juuri se, että ne on säädetty täysin toisistaan riippumatta: luvatonta käyttöä koskeva säännös rikoslain kokonaisuudistuksen ensimmäisessä vaiheessa osana varallisuusrikosuudistusta ja tietomurtosäännös tieto- ja viestintärikoksia koskevan 38 luvun osana (ja sen systematiikkaan ja ideaan sopivana) kokonaisuudistuksen toisessa vaiheessa puoli vuosikymmentä myöhemmin.

Väärennys

Itse väärennystä koskevat säännökset – niin kriminalisointi kuin määritelmäkin – lienevät sanamuotonsa perusteella käytännön kannalta melko ongelmattomia. Se kritiikki, jota olen edellä esittänyt, kohdistuu lähinnä säännösten perusteluihin ja perusteluissa tallenteesta ja tulosteesta lausuttuun.

”Automaattiseen tietojenkäsittelyyn soveltuva tallenne” on varmaankin yhtenä todistuskappaleen lajina aivan kelvollinen, joskaan ei täysin ongelmaton, joten käsitteen määrittely olisi ehkä ollut hyvä tehdä jossakin vaiheessa lainvalmistelua – ainakin perusteluissa, mahdollisesti jopa laissa. Nykyaikaiseen tietotekniseen ympäristöön paremmin soveltuva termi olisi mielestäni ”tietotekninen tallenne” osan I luvussa 1.2 määritellyin tavoin ymmärrettynä.

Harkitsemisen arvoista voisi myös olla julkisuuslain 5 §:n 1 momentin asiakirja-käsitteen implementoiminen tavalla tai toisella rikoslain 33 lukuun. Vaikuttaisi siltä, että käsitteen ”todistuskappale” voisi kokonaisuudessaan korvata julkisuuslain asiakirja-käsitteellä sillä lisäyksellä, että asiakirjaa käytetään tai voidaan käyttää oikeudellisesti merkityksellisenä todisteena oikeuksista, velvoitteista tai tosiasioista.

Petos

Petossäännöksen kohdalla ongelmallisimmalta vaikuttanut teonkuvauksen osa ”tietojenkäsittelylaitteeseen vääriä tietoja syöttämällä tai koneelliseen tietojenkäsittelyyn muuten puuttumalla” on nyt muutettu. Kaiken kaikkiaan rikoslain 36 luvun 1 §:n 2 momentti vaikuttaa varsin onnistuneelta ja asianmukaiselta säännökseltä, joka vastaa myös kansainvälisten instrumenttien asettamia vaatimuksia.

Vahingonteko ja luvaton käyttö

Vahingonteko on mielestäni ehkä yllättävästikin ongelmallisin suhteessa luvattomaan käyttöön ja tähän on syynä ”käyttämisen” käsitteen epätäsmällinen sisältö. Jos käyttämiselle annetaan laaja merkitys ja katsotaan, että luvattoman käytön yhteydessä tehdyt vahingontekotoimet itsessään ovatkin vain luvatonta käyttämistä, jää toissijaisen vahingontekosäännöksen käytännön soveltamisala kovin rajatuksi. Vaasan hovioikeuden kannanotto tosin puhuu tällaista tulkintaa vastaan ja mahdollistaisi siis vahingontekosäännöksen itsenäisen soveltamisen luvattoman käytön ohessa.

Tietomurron, luvattoman käytön ja vahingonteon rangaistusasteikot ovat samat. Näin ollen henkilö A, joka tunkeutuu tietojärjestelmään tekemättä siellä mitään, henkilö B, joka tunkeutuu samaan tietojärjestelmään ja selailee siellä olevia tiedostoja niitä vahingoittamatta, sekä henkilö C, joka tunkeutuu myös samaan tietojärjestelmään, selailee siellä olevia tiedostoja ja lopuksi hävittää nämä tietojärjestelmän haltijalle arvokkaat tiedostot, syyllistyvät kaikki menettelyyn, jonka lainsäätäjä on arvioinut saman rangaistusuhan arvoiseksi. Tällainen eriasteisten loukkausten samanlainen arvottaminen ei ole lainkaan loogista, olkoonkin, että rangaistusasteikon sisällä on tietysti rangaistuksen mittaamisessa mahdollista ottaa teon tosiasiallinen vakavuus huomioon.

Lähtökohtaisesti olisi mielestäni varsin perusteltua, suorastaan välttämätöntä, että vaarallisuusasteiltaan selvästi erilaiset ja tietojenkäsittelyrauhaan sel-

västi eriasteisesti kajoavat menettelyt tulisi myös sanktioida selvästi toisistaan poikkeavalla tavalla. Tilanne on sikälikin epätyydyttävä, että rikosten selvittäminen on vaarassa jäädä puolitiehen, kun helposti näytettävissä oleva tietomurto tuottaa saman seuraamuksen kuin mahdollisesti paljonkin vaikeammin tutkittava vahingonteko.

Vahingonteon kohdalla aiheutuu vaikeuksia myös termin ”tallennus” käytöstä. Niin tallennuksen kuin tallenteenkin kantasana on verbi tallentaa ja tästä johtamalla sana ”tallennus” vie ajatukset lähinnä tallentamis*tapahtumaan,* jonka tuloksena syntyy tallenne.[273] Lainkohdassa ei kuitenkaan selvästikään ole tallennuksella ajateltu tallentamisen synonyymiä, vaan ilmeisesti sille on tahdottu antaa suunnilleen tallennetta vastaava merkitys. Käytännön kannalta ongelma ei tosin ole suuri.

Yritysvakoilu, maksuvälinepetos ja vaaran aiheuttaminen tietojenkäsittelylle

Silloin, kun yritysvakoilusäännöstä joudutaan arvioimaan tietojenkäsittelyrauhan loukkauksen kannalta, voidaan tämä yleensä tehdä tietomurtoa ja luvatonta käyttöä koskevien säännösten pohjalta. Siltä osin kuin säännöksessä on tietotekniikkarikoselementtejä, ei niihin näyttäisi liittyvän lain kirjoittamistavasta aiheutuvia ongelmia.

Maksuvälinepetosta ja vaaran aiheuttamista tietojenkäsittelylle koskeva sääntely on rikoslaissamme varsin uutta ja sitä laadittaessa on tietotekniikan vaatimukset pyritty ottamaan huomioon mahdollisimman hyvin. Näin ollen näissä säännöksissä ei vielä ole havaittavissa puutteita, mikä ei suinkaan merkitse sitä, etteikö niidenkin tarkistaminen voisi jo lähitulevaisuudessa olla ajankohtaista, vaikka niiden valmistelussa on kestävän ratkaisun löytäminen ollut yhtenä nimenomaisena tavoitteena. Erityisesti rikoslain 34 luvun 9a §:n soveltamisalan määrittely sen nykyisen sanamuodon pohjalta saattaa ajan mittaan vaikeutua, kun sellaisten haittaohjelmien määrä, jotka eivät luonteeltaan ja toiminnoiltaan vastaa perinteisiä niin sanottuja virusohjelmia, jatkuvasti lisääntyy.

---

[273] Suomen kieli ei tässä suhteessa ole aivan johdonmukainen; esimerkiksi ”rakentaa – rakennus – rakenne” suhtautuvat toisiinsa eri tavoin kuin ”tallentaa – tallennus – tallenne”. ”Tulostaa – tulostus – tuloste” taas ovat viimeksi mainittuja muistuttavia, samoin ”suorittaa – suoritus – suorite”. Ajateltaessa sanoja ”julistaa – julistus – juliste” voitaisiin kylläkin tehdä se johtopäätös, että keskimmäinen sana viittaa nimenomaan sisältöön eikä ainakaan pelkästään julistamistapahtumaan; joulurauhan julistuksessa Turun kaupungin kansliapäällikkö lukee joulurauhanjulistuksen.

7.2 VAIHTOEHTOJA TIETOJENKÄSITTELYRAUHAA SUOJAAVIEN SÄÄNNÖSTEN UUDISTAMISEKSI

7.2.1 Yleistä

Tietotekniikka kehittyy tavattoman nopeasti ja kehityksen myötä syntyy väistämättä uusia kriminalisointitarpeita, olkoonkin, että tietojenkäsittelyrauhan loukkaamiset pitäisi pyrkiä ensisijaisesti ehkäisemään teknisin ja hallinnollisin keinoin ja että rikosoikeudellisten keinojen asema *ultima rationa* on tässä suhteessa yleisesti hyväksytty.

On täysin mahdotonta edes lähitulevaisuutta ajatellen kyetä ennakoimaan, millaisia mahdollisuuksia tietotekninen kehitys tulee luomaan rikolliselle toiminnalle. Lainsäädännön on hyvin vaikea pysyä edes jotenkuten ajan tasalla – tietotekniikkarikollisuuden erityislaatu asettaa lainsäätäjälle vaatimuksia, joihin vastaaminen edellyttää jatkuvaa seuranta- ja tutkimustyötä sekä myös yhteistyötä käytännön lainsoveltajien ja tietotekniikan ammattilaisten kanssa.

Eduskunnan lakivaliokunta on mietinnössään rikoslain kokonaisuudistuksen toista vaihetta koskevasta hallituksen esityksestä todennut muun muassa seuraavaa:[274]

> Valiokunta pitää tässä vaiheessa perusteltuna hyväksyä hallituksen esityksessä omaksutut ratkaisut ja katsoo, että voimassa olevat ja nyt ehdotetut säännökset vastaavat hyvin kansainvälisestä yhteistyöstä saatuja kokemuksia. Tietokoneisiin ja ohjelmiin kohdistuvilta väärinkäytöksiltä on vastaisuudessakin suojauduttava ensisijaisesti teknisin ratkaisuin ja muin tietoturvallisuutta parantavin keinoin. – – Valiokunta pitää tärkeänä, että tietokonerikollisuuden kehitystä ja sen eri ilmenemismuotoja seurataan tarkoin kansainvälisessä yhteistyössä ja lainsäädäntöä uudistetaan tarvittaessa.

AIDP:n Rion kongressin tietotekniikkarikoksia koskevan päätöslauselman johdannossa lausutaan seuraavasti:

> Recognizing the proliferation of information technology and the emergence of an information society which is bringing about fundamental changes in all aspects of life;
>
> Noting that a range of antisocial activities are subverting information technology to the detriment of individuals and of all sectors of society;
>
> Aware that the rapid expansion of inter-connectivity of information technology in the world transcends traditional national boundaries, and involves both developed and developing countries;

---

[274] LaVM 22/1994, s. 8.

> Concerned that abuse of information technology is occurring at the national and international level;
> Concluding, therefore, that such activity is relevant to all states; – –.

Vaikka päätöslauselman johdannosta karsitaankin asiaan kuuluva juhlallinen paatoksellisuus, voidaan helposti huomata, että 1990-luvun puolivälissä Kansainvälinen rikosoikeusyhdistys piti tietotekniikkarikollisuutta suurempana uhkana kuin Suomen eduskunta, joka oli tyytynyt Euroopan neuvoston suosituksen implementoimiseen.

AIDP:n päätöslauselmassa todetaan tietotekniikan kehityksen ja muuttuneiden rikollisuutta koskevien käsitysten edellyttävän, että kriminalisoimisen kohteina tulisi harkita myös Euroopan neuvoston suosituksessa nimenomaisesti mainitsemattomia tekoja. Esimerkkeinä tällaisista teoista mainitaan liikennöinti luvattomasti hankittuja salasanoja käyttämällä, tiedon hankkiminen muista luvattoman tietojärjestelmään tunkeutumisen mahdollistavista keinoista sekä virusten ja vastaavien ohjelmien levittäminen.[275]

Päätöslauselmassa korostetaan tulevaisuudessa tehtävän työn osalta muun muassa jatkuvan tutkimuksen ja uusien rikosten ehkäisemiseen tähtäävien keinojen hyväksymisen merkitystä informaatioteknologian luomiin uusiin haasteisiin vastaamisessa.[276]

Käsittelen tässä luvussa muutamia sellaisia ongelma-alueita, joilla mielestäni jo nyt ja ainakin lähitulevaisuudessa on olemassa selviä tarpeita aineellisen rikoslainsäädännön kehittämiseen. Nämä tarpeet johtuvat joko olemassa olevista säännöksistä itsestään, niiden iästä ja / tai kirjoittamistavasta, taikka kansainvälisistä velvoitteista eli lähinnä Euroopan neuvoston verkkorikoskonventiosta.

7.2.2 Voimassa olevien säännösten tarkistaminen

Tietomurto, luvaton käyttö ja vahingonteko; ensimmäinen vaihtoehto

Edellä selitin, miten epäjohdonmukainen tietomurtoa, luvatonta käyttöä ja vahingontekoa koskevien kriminalisointien keskinäinen suhde on. Ongelmat voisivat ratketa pitkälti ”käyttämisen” käsitteen määrittelemisellä: jos jo tietojärjestelmän tai sen osan käynnistäminen katsottaisiin ja nimenomaisesti määriteltäisiin järjestelmän käyttämiseksi, kattaisi luvaton käyttö lähes kaikki nyt täytetyiksi tietomurroiksi katsottavat teot ja luvattoman käytön yrityksinä voitaisiin käsitellä nykyisin tietomurron yrityksiksi jäävät teot. Tällöin *tietomurtosäännös voitaisiin tarpeettomana kumota.*

---

[275] Päätöslauselma, kohta 10.
[276] Päätöslauselma, kohdat 24–28.

Toinen vaihtoehto

Äsken mainittu voisi kuitenkin olla turhankin radikaali ratkaisu. Selkeämpää olisi erottaa tietojärjestelmän luvatonta käyttämistä koskeva säännös yleisestä luvattomasta käytöstä ja siinä määritellä selkeästi, mitä teolla tarkoitetaan, ja samalla poistaa rajanveto-ongelma tietomurtoon nähden. Rikosnimike voisi olla *tietojärjestelmän luvaton käyttö*, säännös voisi sijaita rikoslain 28 luvussa 7 a §:nä ja sen sanamuoto voisi olla näin kuuluva:

> Joka toiselle kuuluvaan tietojärjestelmään oikeudettomasti tunkeuduttuaan tai muuten luvattomasti käyttää sellaista järjestelmää siihen tallennettua dataa selaamalla, muuttamalla tai poistamalla, siinä olevia ohjelmistoja käyttämällä, järjestelmään uutta dataa tai uusia ohjelmistoja lisäämällä taikka muulla vastaavalla tavalla, on tuomittava, ellei teosta muualla laissa ole säädetty yhtä ankaraa tai ankarampaa rangaistusta, *tietojärjestelmän luvattomasta käytöstä* sakkoon tai vankeuteen enintään yhdeksi vuodeksi kuudeksi kuukaudeksi.
>
> Yritys on rangaistava.

Koska luvaton käyttö loukkaa tietojenkäsittelyrauhaa tietomurtoa syvemmin, täytyy rangaistusasteikkojen olla erilaiset. Euroopan neuvoston yleissopimus edellyttää, että tietomurtoon syyllistynyt rikoksentekijä on voitava luovuttaa, ja näin ollen tietomurrosta tuomittavan enimmäisrangaistuksen laskeminen nykyisestä ei käy päinsä.[277] Sen sijaan luvattoman käytön enimmäisrangaistus olisi hyvin nostettavissa yhdestä vuodesta puoleentoista vuoteen vankeutta. Näinhän on sitä paitsi jo meneteltykin moottoriajoneuvon käyttövarkauden kohdalla.

Koska luvaton käyttö ja vahingonteko kohdistuvat tietojenkäsittelyrauhan eri osa-alueisiin, tulisi niidenkin välinen raja selvästi määritellä, jotta tekijä tarvittaessa voitaisiin tuomita *myös* vahingonteosta luvattoman käytön ohella katsomatta, että vahingontekosäännös väistyy luvattoman käytön tieltä. Tämä ei kuitenkaan vielä poistaisi sitä epäsuhtaa, joka vallitsee rangaistusasteikkojen kesken: tietoteknisessä ympäristössä vahingonteko on luvatonta käyttöä pidemmälle menevä loukkaus ja siitä tulisi rangaista ankarammin. Vaikka tämä tekojen vakavuuden vertailu ei välttämättä rajoitu vain tietotekniseen ympäristöön, olisi ajateltavissa seuraavanlainen *tietovahingon aiheuttamista* koskeva säännös (RL 35:1a):

> Joka toista vahingoittaakseen oikeudettomasti hävittää, turmelee, kätkee tai salaa tietojärjestelmässä olevaa dataa, on tuomittava *tietovahingon aiheuttamisesta* sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

---

[277] Rikoksen johdosta tapahtuvasta luovuttamisesta annetun lain (456/1970) 4 §:n 1 momentin mukaan rikoksentekijää ei saa luovuttaa, ellei luovutuspyynnössä tarkoitettu teko ole sellainen rikos, josta Suomen lain mukaan säädetty ankarin rangaistus on vähintään vuosi vankeutta.

Vahingonteon perusmuodon enimmäisrangaistus on tällä hetkellä vuosi vankeutta. Huomattakoon, että törkeän vahingonteon asteikko on vankeutta neljästä kuukaudesta neljään vuoteen eli sama kuin törkeillä rikoksilla yleensä, vaikka perustekomuoto on sanktioitu ”normaalia” lievemmin. Tämänkin kanssa olisi sopusoinnussa, että tietovahingon aiheuttamisen (ja miksei myös vahingonteon yleensä) enimmäisrangaistus olisi kaksi vuotta vankeutta.

Lopputulos olisi siis se, että tietomurtoa koskeva säännös säilyisi ennallaan, tietojärjestelmän luvattoman käytön rangaistusmaksimi olisi vuosi ja kuusi kuukautta vankeutta ja tietovahingon aiheuttamisen enimmäisrangaistus kaksi vuotta vankeutta. Rikoslain 35 luvun 5 §:n rajoitussäännökselle ei tarvitsisi tehdä mitään, sillä nyt tietovahingon aiheuttamisen ei enää voitaisi väittääkään väistyvän luvattoman käytön tieltä. Rikoslain 35 luvun 1 §:n 2 momentti tulisi kumota. Tekojen lievät tekomuodot voitaisiin kriminalisoida muuttamalla 28 luvun 9 §:n ja 35 luvun 3 §:n sanamuodot sellaisiksi, että ne kattaisivat myös nyt puheena olevat rikokset; törkeiden tekomuotojen osalta voitaisiin menetellä vastaavasti 28 luvun 8 §:n ja 35 luvun 2 §:n sanamuotoja tarkistamalla.

Kolmas vaihtoehto

Mahdollista olisi myös yksinkertaisesti nostaa kaikkien luvattomien käyttöjen enimmäisrangaistus puoleentoista vuoteen vankeutta ja kaikkien vahingontekojen enimmäisrangaistus kahteen vuoteen vankeutta. Tällaiset muutokset luultavasti olisivat aivan paikallaan ajatellen myös muita kuin tietotekniikkarikoksina käsiteltäviä luvattomia käyttöjä ja vahingontekoja.

Tällöin pitäisi kuitenkin rikoslain 35 luvun 1 §:n 2 momentista häivyttää sana ”tallennus”. Tämä onnistuisi korvaamalla ilmaisu ”tietovälineelle tallennettu tieto tai muu tallennus” sanoilla ”tietojärjestelmässä oleva data”. Sana ”data” on jo otettu käyttöön uudistetussa rikoslain 36 luvun 1 §:n 2 momentissa.

Petos

Vahingonteon rangaistusasteikon korottaminen edellä sanotuin tavoin selkiyttäisi myös vahingonteon ja petoksen keskinäistä suhdetta: vahingonteon yritys ei ole rangaistavaa ja täytetyn teon ollessa kysymyksessä vahingontekoa koskeva säännös joka tapauksessa väistyisi.

7.2.3 Tietojenkäsittelyrauhan rikkominen

Osan II luvuissa 2–4 on jo käynyt selville, että tietoverkkorikosyleissopimus ei edellytä aineelliseen rikoslainsäädäntöömme tehtäväksi kovin monia muutoksia. Kuitenkin sopimuksen 6 artiklan, *välineiden väärinkäyttö,* implementoiminen edellyttää uuden säännöksen luomista.

Valmistelu

Tietoverkkorikostyöryhmä on mietinnössään esittänyt ehdotuksensa, jota käsittelen jäljempänä. Muitakin vaihtoehtoja voidaan kuvitella ja artikla voisikin olla implementoitavissa niin, että rikoslain 38 lukuun lisättäisiin uusi pykälä, jonka otsikko olisi *"Tietojenkäsittelyrauhan rikkomisen valmistelu":*

> Joka oikeudettomasti [tietojenkäsittelyrauhan rikkomista] varten
> 1) valmistaa, myy, hankkii, tuo maahan tai asettaa saataville sellaisen välineen tai tietokoneohjelman, joka on suunniteltu tai muunnettu erityisesti [tietojenkäsittelyrauhan rikkomiseen] soveltuvaksi, tai salasanan, käyttäjätunnuksen tai muuta sellaista dataa, jota käyttämällä tietojärjestelmään tai sen osaan voidaan oikeudettomasti tunkeutua, tai levittää sellaista välinettä, tietokoneohjelmaa tai dataa taikka
> 2) pitää hallussaan sellaista välinettä, tietokoneohjelmaa tai dataa tarkoituksin, että sitä käytetään [tietojenkäsittelyrauhan rikkomiseen],
>
> on tuomittava, jollei teosta ole muualla laissa säädetty ankarampaa tai yhtä ankaraa rangaistusta, *tietojenkäsittelyrauhan rikkomisen valmistelusta* sakkoon tai vankeuteen enintään [kuudeksi kuukaudeksi][yhdeksi vuodeksi].

Ehdottamassani säännöksessä, joka sinänsä kyllä vastaisi 6 artiklan kriminalisointivelvoitetta, on se heikkous, että siinä käytetään termiä "tietojenkäsittelyrauhan rikkominen", jota ei ole hallituksen esitystä 4/1999 lukuun ottamatta määritelty missään. Sen voisi tietysti määritellä asianomaisen säännöksen perusteluissa, mutta parempi olisi tietysti määritellä se suoraan laissa. Toinen vaihtoehto on luetella nimenomaisesti ne rikokset, joita halutaan tarkoittaa. Kolmas vaihtoehto on säätää jäljempänä ehdottamani tietojenkäsittelyrauhan rikkomista koskeva kriminalisointi.

Puheena olevan, valmistelua koskevan kriminalisoinnin tarpeellisuudesta ei pitäisi olla epäilyksiä. Tietomurto ensinnäkin on sellainen perusrikos, että se onnistuessaan avaa rikoksentekijälle tilaisuuden osaamisensa asettamissa rajoissa liikkua verkossa lähes rajattomasti ja tehdä mahdollisesti todella vakavia tekoja. Näin ollen kaikenlainen järjestelmiin tunkeutuminen olisi syytä tehdä mahdollisimman vaikeaksi – ja siinä suhteessa tietysti muut kuin rikosoikeuden keinot ovat ensisijaisia – sekä myös sanktioida riittävän vakavasti.

Internetistä on rikoksentekijöiden saatavilla lukuisia erilaisia ohjelmia, jotka on suunniteltu tai muunnettu nimenomaan rikoksen tekemiseen soveltuviksi. Tällaisia ovat esimerkiksi sellaiset verkonkuunteluohjelmat, joilla kerätään verkkoliikenteestä käyttäjätunnus–salasana-pareja, samoin kuin tietoturva-aukkojen laajamittaisen etsimisen mahdollistavat skannausohjelmat. Tällaisten ja vastaavien sinänsä hyvin haitallisten ja vahingollistenkin ohjelmien levittäminen ei nykyisellään ole Suomen (eikä yleensä muidenkaan maiden) lainsäädännön mukaan rangaistavaa.

Täytetty teko

Esitän lopuksi vaihtoehdon, joka käsitykseni mukaan poistaisi olemassa olevien säännösten välisiä rajanveto-ongelmia (ja myös helpottaisi edellä esitetyn valmistelukriminalisoinnin säätämistä). Rikoslain 38 lukuun voisi lisätä seuraavanlaisen 8 a §:n (jolloin pykälässä nyt oleva suojauksen purkujärjestelmärikosta koskeva säännös[278] siirtyisi 8 b §:ksi):

> *Tietojenkäsittelyrauhan rikkominen.* Joka, hankkiakseen itselleen tai toiselle oikeudetonta taloudellista hyötyä, toista vahingoittaakseen tai saadakseen aikaan harhauttavan todisteen,
> 1) oikeudettomasti hävittää, turmelee, kätkee tai salaa tietoteknisen tallenteen tai muuta tietojärjestelmään tallennettua tai siellä olevaa dataa,
> 2) edellä mainitulla tai muulla tavalla muuttaa sellaista tallennetta tai dataa niin, että se on omiaan antamaan alkuperästään tai antajansa henkilöllisyydestä erehdyttävän kuvan, tai
> 3) edellä mainituilla tai muilla tavoilla tietojenkäsittelyyn puuttumalla saa aikaan tietojenkäsittelyn lopputuloksen sellaisen vääristymisen, josta jollekulle aiheutuu taloudellista vahinkoa,
>
> on tuomittava, jollei teosta ole muualla laissa säädetty ankarampaa tai yhtä ankaraa rangaistusta, *tietojenkäsittelyrauhan rikkomisesta* sakkoon tai vankeuteen enintään kahdeksi vuodeksi.
>
> Yritys on rangaistava.

Tällaisella säännöksellä tulisi itse asiassa tietojenkäsittelyrauhankin käsite määritellyksi. Erillinen määritelmä vaikkapa 38 luvun 10 a §:ään tarvittaisiin vielä tietoteknisestä tallenteesta.

Tietojenkäsittelyrauhan rikkominen voisi olla rangaistavaa myös törkeänä ja lievänä tekomuotona, jolloin ankaroittamisperusteina voisivat tulla kysymykseen aiheutetun vahingon suuruus, tavoitellun hyödyn määrä, tallenteen erityinen merkityksellisyys, luottamuksellisen aseman väärinkäyttäminen ja teon erityinen suunnitelmallisuus. Vahingon vähäisyys ja muut tekoon liittyvät olosuhteet puolestaan voisivat oikeuttaa tarkastelemaan menettelyä rikkomustyyppisenä tekona.

Pykälä kattaisi voimassa olevasta laista tietojenkäsittelypetosta, tietovahingon aiheuttamista ja tietoteknistä väärennystä koskevat säännökset, joten rikoslain 35 luvun 1 §:n 2 momentti ja 36 luvun 1 §:n 2 momentti olisi kumottava ja 33 luvun 6 §:n määritelmäsäännöksestä poistettava sanat ”automaattiseen tietojenkäsittelyyn soveltuvaa tallennetta”.

Koko tietotekniikkarikoskonsepti (ja erityisesti datarikoskonsepti) on melko selkeä: tietojärjestelmään tunkeudutaan ja sitä käytetään oikeudettomasti ja

---

[278] HE 146/2000.

käyttämisen yhteydessä järjestelmässä olevaa dataa hävitetään, muutetaan, kopioidaan jne. tai järjestelmään syötetään uutta dataa, mistä kaikesta todennäköisesti tavalla tai toisella aiheutuu järjestelmän oikealle haltijalle välitöntä tai välillistä vahinkoa. Tämän peruskaavan pohjalta voi sitten kehittyä erilaisia modifikaatioita, joiden perusluonne pysyy silti samana, ja tältä pohjalta voitaisiin hyvinkin kuvitella säädettäväksi edellä olevan kaltainen yleinen kriminalisointi.

Tällaista kriminalisointia puoltaisi myös se, että tietojenkäsittelyrauha on jo jossain määrin hyväksytty tietotekniikkarikosten suojeluobjektiksi. Ehdottamallani tavalla menetellen erotettaisiin selkeästi muista rikoksista ne rikokset, joissa tietojenkäsittelyrauhan merkitys on keskeinen ja jotka ovat esittämäni tietotekniikkarikoksen määritelmän mukaisia tekoja.

Tietotekniikkarikossääntelystä tulisi johdonmukainen kokonaisuus*: luvattomasta käytöstä*, jonka soveltamisala jäisi suhteellisen vähäiseksi, säädettäisiin nykyiseen tapaan 28 luvussa, vaaran *aiheuttamisesta tietojenkäsittelylle* 34 luvussa sekä *tietomurrosta, tietojenkäsittelyrauhan rikkomisesta* ja *tietojenkäsittelyrauhan rikkomisen valmistelusta* 38 luvussa. Yritysvakoilua ja maksuvälinepetosta koskeville säännöksille ei tarvitsisi tehdä mitään, ne luontuvat hyvin nykyiseen ympäristöönsä myös tietoteknisten elementtiensä osalta.

Edellä selostettu yleinen tietotekniikkarikoskonsepti asettaa lainsäätäjälle sen kehyksen, jonka puitteissa rankaisemisen arvoiseksi katsottavat menettelyt olisi kuvattava rikosoikeusjärjestelmän kanssa sopusoinnussa olevissa säännöksissä ja varustettava oikeiksi arvioiduilla sanktioilla. Hankalaksi tämän lainsäädäntötyön tekee teknisen kehityksen nopeus: varmuutta ratkaisujen kestävyydestä ei voi olla. Niinpä lainlaatijoilta, sekä valmistelijoilta että säätäjiltä, on edellytettävä asenteen muutosta, valmiutta tarvittaessa nopeisiin osittaisuudistuksiin ja halua pysytellä kehityksen vauhdissa mukana.

7.2.4 Tietoverkkorikostyöryhmän ehdotukset

7.2.4.1 Aineellinen rikosoikeus

Tietoverkkorikosvälineet

Ehkäpä merkittävin tietoverkkorikostyöryhmän rikosoikeudellisista ehdotuksista on yleissopimuksen 6 artiklan *(välineiden väärinkäyttö)* implementoimiseksi ehdotettu rikoslain 34 luvun 9 a §:n muutos. Ehdotuksen mukainen säännös on seuraavanlainen:

> Joka aiheuttaakseen haittaa tai vahinkoa tietojenkäsittelylle taikka tieto- tai viestintäjärjestelmän toiminnalle tai turvallisuudelle
> 1) tuo maahan, valmistaa, myy tai muuten levittää taikka asettaa saataville
>   a) sellaisen laitteen tai tietokoneohjelman tai ohjelmakäskyjen sarjan, joka on suunniteltu tai muunnettu ensisijaisesti vaarantamaan tai vahingoittamaan tietojenkäsittelyä taikka tieto- tai viestintäjärjestelmän toimintaa taikka tietojärjestelmän suojauksen murtamiseen tai
>   b) tietojärjestelmän salasanan tai käyttäjätunnuksen tai muun vastaavan tiedon taikka
> 2) levittää tai asettaa saataville 1 kohdassa tarkoitetun tietokoneohjelman tai ohjelmakäskyjen sarjan valmistusohjeen,
>
> on tuomittava, jollei teosta muualla laissa säädetä ankarampaa tai yhtä ankaraa rangaistusta, *vaaran aiheuttamisesta tietojenkäsittelylle* sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

Lisäksi työryhmä ehdottaa rikoslain 34 lukuun täysin uutta 9 b §:ää *(tietoverkkorikosvälineen hallussapito)* seuraavasti:

> Joka ilman hyväksyttävää syytä pitää hallussaan 9 a §:n 1 kohdassa tarkoitettua laitetta, tietokoneohjelmaa, ohjelmakäskyjen sarjaa tai tietoa on tuomittava tietoverkkorikosvälineen hallussapidosta sakkoon tai vankeuteen enintään yhdeksi vuodeksi.

Ehdotetun 9 a §:n tekotapaluettelo vastaa perustelujen mukaan[279] pääosin voimassa olevan lain sisältämää ja sen tarkoituksena on kattaa valmistamisen ohella kaikki sellaiset aktiiviset toimenpiteet, joiden seurauksena tietokonevirus, tekninen laite tai tietomurto-ohjelma voi siirtyä muiden henkilöiden käytettäväksi. *Maahantuonnin* mainitseminen itsenäisenä tekotapana on perustelujen mukaan tarpeellista erityisesti laitteiden osalta. *Valmistamisella* tarkoitetaan esimerkiksi uuden ohjelman kirjoittamista tai olemassa olevan muuttamista pykälässä tarkoitetun kaltaiseksi, *myyminen* tarkoittaa välineen vastikkeellista luovutusta ja *saataville asettamisella* tarkoitetaan välineen laittamista esimerkiksi Internet-sivulle halukkaiden vapaasti kopioitavaksi. *Levittämisellä* tarkoitetaan kahta erilaista tekotapaa: ensinnäkin välineen vastikkeetonta luovuttamista esimerkiksi sähköpostin välityksellä toiselle henkilölle tai henkilöille ja toiseksi tietokonevirusten osalta viruksen käyttämistä levittämällä sitä uhrien koneisiin.

Ehdotuksessa ei määritellä tietoverkkorikosvälineen käsitettä, joka saa sisältönsä ehdotetusta säännöksen sisällöstä, 9 a §:n 1 kohdan a alakohdasta. Perusteluissa todetaan, että jos väline on sellainen, että sitä voidaan käyttää sekä säännöksessä tarkoitettuihin moitittaviin tarkoituksiin että muihin hyväksyttä-

---

[279] Tietoverkkorikostyöryhmän mietintö s. 61 ss.

viin tarkoituksiin, välineen ensisijainen käyttötarkoitus ratkaisee sen, onko välinettä pidettävä säännöksessä tarkoitettuna tietoverkkorikosvälineenä vai ei. Perusteluissa viitataan yleissopimuksen selitysmuistioon, jossa on todettu kaksikäyttöisten välineiden eli välineiden, joita voidaan käyttää niin hyväksyttäviin kuin rikollisiinkin tarkoituksiin, lähtökohtaisesti rajautuvan säännöksen soveltamisalan ulkopuolelle. Välineen ensisijainen käyttötarkoitus on perustelujen mukaan se kriteeri, jolla välineen luonne määritellään, mutta yksittäistapauksissa ratkaisu luonnollisesti jää riippumaan kunkin välineen erityispiirteistä.

Ehdotettu 9 b § ei koskisi 9 a §:n 2 kohdassa tarkoitettua valmistusohjetta. Välineen hallussapito ei olisi rangaistavaa, jos hallussapitoon on hyväksyttävä syy.[280]

Rikoslain 34 lukuun ehdotetaan myös uutta 13 §:ää, jonka mukaan oikeushenkilön rangaistusvastuu ulotettaisiin koskemaan vaaran aiheuttamista tietojenkäsittelylle sekä tietoverkkorikosvälineen hallussapitoa. Säännös perustuu suoraan tietoverkkorikosyleissopimuksen 12 artiklaan.[281]

Vahingonteko

Vahingontekorikosten osalta tietoverkkorikostyöryhmän esitykset ovat jokseenkin suppeat: yleissopimuksen edellyttämällä tavalla työryhmä ehdottaa, että rikoslain 35 luvun 1 §:ään lisättäisiin tietovahingon aiheuttamisen yrityksen kriminalisoiva 3 momentti[282] ja että lukuun lisättäisiin uusi 8 §, joka ulottaisi oikeushenkilön rangaistusvastuun luvun 1 §:n 2 momentissa tarkoitettuun tietovahingon aiheuttamiseen sekä 3 §:ssä tarkoitettuun törkeään vahingontekoon siltä osin kuin lainkohtaa sovelletaan 1 §:n 2 momentissa tarkoitettuihin tekoihin.[283]

Rikoslain 38 luku

Rikoslain 38 luvun 5 §:ssä tarkoitetun tietoliikenteen häirinnän, 6 §:ssä tarkoitetun törkeän tietoliikenteen häirinnän sekä 7 §:ssä tarkoitetun lievän tietoliikenteen häirinnän yritys ehdotetaan säädettäväksi rangaistavaksi. Ehdotus perustuu yleissopimuksen 11 artiklan 2 kohtaan.

Lukuun ehdotetaan lisättäväksi uusi *tietojärjestelmän häirintää* koskeva 7 a §:

> Joka toista vahingoittaakseen oikeudettomasti dataa syöttämällä, siirtämällä, vahingoittamalla, muuttamalla tai poistamalla taikka muulla näihin verrattavalla tavalla estää tietojärjestelmän toiminnan tai aiheuttaa

---

280 Ks. tietoverkkorikostyöryhmän mietintö s. 68 s.
281 Tietoverkkorikostyöryhmän mietintö s. 69.
282 Törkeän vahingonteon yritys on jo kriminalisoitu 1.2.2003 voimaan tulleella lailla 17/2003.
283 Ks. tietoverkkorikostyöryhmän mietintö s. 69.

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

Yritys on rangaistava.

Säännösehdotuksen tarkoituksena on saattaa lainsäädäntömme vastaamaan yleissopimuksen 5 artiklan vaatimuksia. Perusteluissa[284] viitataan yleissopimuksen selitysmuistion 65 ja 67 kohtiin, joiden mukaan artiklan tarkoituksena on suojata erityisesti viestintäjärjestelmiä virus- ja palvelunestohyökkäyksiltä. Jälkimmäisellä *(Denial of Service, DoD)* tarkoitetaan esimerkiksi hyökkäyksen kohteena olevan tietojärjestelmän tahallista ylikuormittamista tarkoituksena estää sen toiminta tai aiheuttaa sille haittaa.[285]

Rikoslain 38 lukuun ehdotettu 7 b § kriminalisoisi *törkeän tietoliikenteen häirinnän.* Kvalifiointiperusteina mainitaan rikoksella aiheutettava erityisen tuntuva haitta tai taloudellinen vahinko sekä rikoksen erityinen suunnitelmallisuus. Perustelujen[286] mukaan erityisellä taloudellisella vahingolla tarkoitettaisiin lähinnä teolla aiheutetun seurauksen rahassa mitattavia vaikutuksia tietojärjestelmän haltijalle kun taas erityisen tuntuvalla haitalla tarkoitetaan seurauksen muita kuin rahassa mitattavia vahingollisia vaikutuksia. Esimerkkinä mainitaan tietojärjestelmän käyttömahdollisuuksien menettäminen tai heikkeneminen.[287]

Erityisellä suunnitelmallisuudella tarkoitettaisiin varsinaista tekoa edeltäviä laajoja valmistelutoimenpiteitä sekä erityisiä toimia teon jälkeen jälkien peittämiseksi.

Tietoverkkorikostyöryhmä ehdottaa syyteoikeutta koskevaa 38 luvun 10 §:ää muutettavaksi niin, että tietojärjestelmän häirintä ja törkeä tietojärjestelmän häirintä olisivat asianomistajarikoksia. Tätä perustellaan sanomalla, että tietojärjestelmän häirintää koskevilla säännöksillä suojataan pääasiassa yksityistä etua. Säännöksessä nykyäänkin mainittu tärkeää yleistä etua ja teleyrityksen työntekijää koskeva poikkeus soveltuisi myös tietojärjestelmän häirintään.

Lukuun ehdotetaan lisäksi uutta 12 §:ää, joka ulottaisi oikeushenkilön rangaistusvastuun viestintäsalaisuuden loukkaukseen, törkeään viestintäsalaisuu-

---

284 Tietoverkkorikostyöryhmän mietintö, s. 70 s.

285 Edellä tietomurtoa käsiteltäessä selostetussa Helsingin käräjäoikeuden 5.12.2003 antamassa tuomiossa tekijöiden syyksi luettiin tietoliikenteen häirintänä tyypillinen palvelunestohyökkäys, tarkemmin ottaen sellaisen alalaji hajautettu palvelunestohyökkäys (*Distributed Denial of Service, DDoS*). Tekijät olivat yhden isäntäkoneen alle muodostaneet kymmenistä murtamistaan koneista verkon, jota käytettiin tiettyjen IRC-piireissä epäsuosioon joutuneiden koneiden lamaannuttamiseen.

286 Tietoverkkorikostyöryhmän mietintö, s. 72.

287 Ensimmäinen kvalifiointiperuste on asiallisesti sama kuin törkeässä vahingonteossa. Tässä se on kuitenkin kirjoitettu onnistuneemmin eikä esimerkiksi edellä TCB-juttua selostettaessa esille tullut haitan ja vahingon käsitteiden sekaantuminen olisi enää niin helppoa.

den loukkaukseen, tietoliikenteen häirintään, törkeään tietoliikenteen häirintään, tietomurtoon, tietojärjestelmän häirintään ja törkeään tietojärjestelmän häirintään. Pykälä täyttäisi tietoverkkorikosyleissopimuksen 12 artiklassa asetetut vaatimukset.

Rikoslain 49 luku

Samainen 12 artikla edellyttää myös, että oikeushenkilön rangaistusvastuu laajennetaan koskemaan tekijänoikeusrikosta. Työryhmä ehdottaa tästä säätävän uuden 4 §:n lisäämistä rikoslain 49 lukuun.

Arviointia

Ehdotetut muutokset ja lisäykset epäilemättä saattaisivat rikoslakimme vastaamaan tietoverkkorikosyleissopimuksen vaatimuksia. Työryhmä ehdottaa varauman tekemistä ainoastaan siltä osin kuin on kysymys yleissopimuksessa tarkoitettujen rikosten yrityksen kriminalisoimisesta; työryhmä katsoo,[288] että rikoslain 35 luvun 3 §:n lievän vahingonteon ja 33 luvun 3 §:n lievän väärennyksen yrityksen kriminalisoiminen ei olisi tarkoituksenmukaista, koska se johtaisi tekojen vähäisyys huomioon ottaen liian laajaan rikosoikeudelliseen vastuuseen. Lievän väärennyksen osalta työryhmä kiinnittää vielä huomiota siihen, että väärennysvälineen ja -tarvikkeen hallussapito on joka tapauksessa rikoslain 33 luvun 4 §:n nojalla rangaistavaa väärennysaineiston hallussapitona.

Työryhmän ansiokasta ehdotusta jää kuitenkin rasittamaan sama puute, josta koko tietotekniikkarikoksia koskeva sääntelymme on kärsinyt: valitulla lainsäädäntömetodilla ei päästä tarkastelemaan tietotekniikkarikoksia yhtenä kokonaisuutena. Ehdotettu uudistus ei esimerkiksi korjaa sitä mainitsemaani mielestäni tuntuvaa epäkohtaa, että tietomurron, luvattoman käytön ja vahingonteon rangaistusasteikot ovat samanlaiset. Tähän kokonaisuuteen sopivat jokseenkin huonosti myös rikoslain 34 luvun 9 a ja 9 b §:n rangaistusasteikot. Esimerkiksi salasanojen murtautumistarkoituksessa tapahtunut hallussapito on voimassa olevan lain nojalla katsottu tietomurron yritykseksi, mutta ehdotuksen mukainen lainsäädäntö rinnastaisi tällaisen hallussapidon moitittavuudeltaan täytettyyn tietomurtoon.

Lainsäätäjä ei siis missään tapauksessa saisi kuvitella, että tietoverkkorikosyleissopimuksen ehdotetulla tavalla tapahtuvalla implementoinnilla tietotekniikkarikoksia koskeva rikoslainsäädäntömme olisi saatettu kuntoon. Hienosäätöä riittää – puhumattakaan siitä, että uusia kriminalisointitarpeita tulee aivan varmasti ilmaantumaan jatkuvasti.

---

[288] Tietoverkkorikostyöryhmän mietintö, s. 29.

7.2.4.2 Pakkokeino- ja esitutkintalainsäädäntö

Kuvailen seuraavassa lyhyesti tietoverkkorikostyöryhmän pakkokeino- ja esitutkintalainsäädäntöön liittyvät ehdotukset. Tässä esitettävällä on lähinnä informatiivinen merkitys enkä ryhdy tarkemmin analysoimaan ehdotettuja säännöksiä.

Pakkokeinolain 4 luku

Työryhmä ehdottaa ensinnäkin pakkokeinolain 4 luvun 1 §:n 1 momenttia muutettavaksi niin, että siinä esineen ohella mainitaan myös *asiakirja* takavarikon kohteena.[289] Lisäksi pykälään ehdotetaan uutta toista ja kolmatta momenttia, joista ensin mainittu sisältäisi pakkokeinolain tarpeita vastaavan *datan* määritelmän:

> Mitä 1 momentissa säädetään, koskee myös tietoa, joka on tietokoneessa tai muussa vastaavassa tietojärjestelmässä taikka sen tallennusalustalla *(data).*
>
> Mitä 2 luvun 2 ja 8 §:ssä säädetään asiakirjasta, sovelletaan myös datan muodossa olevaan asiakirjaan.

Ehdotettujen lisäysten tarkoituksena ei ole muuttaa vallitsevaa tilannetta vaan ainoastaan selventää sitä. Datan määritelmä vastaa asiallisesti suunnilleen yleissopimuksen 1 artiklan b kohdan määritelmää mutta on pelkistetympi ja tarkoitettu vain pakkokeinolakia sovellettaessa käytettäväksi.

Pakkokeinolain 4 lukuun ehdotetaan lisättäväksi uusi *datan kopiointia ja takavarikointia* koskeva 4 a §:

> Data voidaan kopioida ja tallentaa se toiselle tallennusalustalle, jos on syytä olettaa, että se voi olla todisteena rikosasiassa.
>
> Data voidaan kopioinnin lisäksi poistaa alkuperäisestä tallennusalustasta tai muutoin estää sen käyttö, jos on syytä olettaa, että se on rikoksella joltakulta viety tai että tuomioistuin julistaa sen menetetyksi taikka jos se on rikoksen selvittämiseksi tarpeen.
>
> Edellä 2 momentissa tarkoitetun toimenpiteen osalta on voimassa mitä takavarikosta säädetään.

Käytännössä datan alkuperäiseltä tallennusalustalta tapahtuvan kopioinnin luonne on ollut jossain määrin epäselvää. Epäselvyyttä on ollut omiaan lisäämään rinnastaminen paperiasiakirjan takavarikkoon: sitä ei ole kyseenalaistettu, etteikö asiakirjan konkreettinen haltuunotto olisi takavarikoimista, mutta myöskään ei ole ajateltu paperiasiakirjasta otetun kopion olevan takavarikon

---

[289] Ks. tietoverkkorikostyöryhmän mietintö, s. 73 s.

kohteena, jos alkuperäinen kappale on jäänyt haltijalleen. Korkein oikeus on kuitenkin ratkaisussaan 2002:85 katsonut, että takavarikko oli kohdistunut poliisin tietokoneen kovalevystä tekemään kopioon. Korkeimman oikeuden sanamuodoltaan hieman epäjohdonmukaisessa ratkaisussa tosin todetaan, että poliisilla oli ollut oikeus kovalevyn kopioimiseen takavarikoitavan aineiston löytämiseksi.

Ehdotetun säännöksen tarkoituksena[290] on selventää tilannetta säätämällä, että kopiointi sinänsä ei vielä olisi takavarikoimista. Tämä tuntuu tarkoituksenmukaiselta ratkaisulta ajatellen sitä valtavaa tietomäärää, joka jo tavallisen kotikoneen kovalevylle saattaa sisältyä: kun data paperitulosteina täyttäisi useita täysperävaunullisia rekka-autoja, on selvää, että sen analysoiminen vaatii runsaasti aikaa. Datan haltijan etujen mukaista on yleensä, että tuo analysointi tehdään käyttämällä kopiota, jolloin alkuperäinen data voi jäädä haltijalleen, mutta tutkinnan kannalta on epätarkoituksenmukaista, jos kopion ajatellaan olevan takavarikossa jo siinä vaiheessa, kun takavarikoitavaa aineistoa vasta etsitään.

Korkeimman oikeuden edellä mainitussa ratkaisussa omaksuma kanta johtaisi siihen, että takavarikkoa koskevien säännösten tulisi ulottua myös esitutkinta-aineistoon liitettyihin tavallisten asiakirjojen jäljennöksiin. Tämä aiheuttaisi aivan tarpeetonta vaivaa esimerkiksi laajoissa talousrikosasioissa, kun syytteen nostamisen määräajalle tulisi aika ajoin hakea pidennystä vain sen vuoksi, että esitutkintapöytäkirjan liitteenä on kopioita kirjanpitoaineistosta.

Tietoverkkorikosyleissopimuksen 19 artiklan 4 kohta edellyttää, että sopimuspuolet ryhtyvät ”tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin antaakseen toimivaltaisille viranomaisilleen valtuudet määrätä henkilö, jolla on tietoa tietojärjestelmän toiminnasta tai siihen sisältyvän datan suojaamiseen sovelletuista menetelmistä, esittämään tarvittavat tiedot, siinä määrin kuin se katsotaan kohtuulliseksi” dataan kohdistuvan etsinnän suorittamiseksi. Sopimusmääräyksen implementoimiseksi työryhmä ehdottaa 4 lukuun uutta *tietojärjestelmän haltijan tietojenantovelvollisuutta* koskevaa 4 b §:ää:[291]

> Tietojärjestelmän haltija, ylläpitäjä tai muu henkilö on velvollinen antamaan esitutkintaviranomaiselle tämän pyynnöstä tiedossaan olevat 4 a §:ssä tarkoitetun toimenpiteen suorittamiseksi tarpeelliset salasanat ja muut vastaavat tiedot.
>
> Mitä 1 momentissa säädetään, ei kuitenkaan koske epäiltyä eikä henkilöä, joka esitutkintalain 27 §:n nojalla on oikeutettu tai velvollinen esitutkinnassa kieltäytymään todistamasta.
>
> Jos henkilö kieltäytyy antamasta tietoja, häntä voidaan kuulustella tuomioistuimessa siten kuin esitutkintalain 28 §:ssä säädetään.

---

290 Ks. tietoverkkorikostyöryhmän mietintö, s. 74 ss.

291 Ks. tietoverkkorikostyöryhmän mietintö, s. 79 s.

Lisäksi pakkokeinolain 4 lukuun ehdotetaan lisättäväksi *datan säilyttämismääräystä* koskeva 4 c § sekä *datan säilyttämismääräyksen kestoa ja salassapitovelvollisuutta* koskeva 4 d §:[292]

> 4 c §. Jos on syytä olettaa, että tietty data, jolla on merkitystä tutkittavana olevan rikoksen selvittämiselle, häviää tai sitä muutetaan, pidättämiseen oikeutettu virkamies voi määrätä sen, jonka hallussa tai määräysvallassa data on, säilyttämään sen muuttumattomana.
>
> Jos asia ei siedä viivytystä, 1 momentissa tarkoitetun säilyttämismääräyksen voi antaa muukin esitutkintaa suorittava virkamies. Asia on silloin välittömästi saatettava pidättämiseen oikeutetun virkamiehen päätettäväksi.
>
> Mitä 1 momentissa säädetään, koskee myös tietojärjestelmän välityksellä siirrettyä viestiä ja siihen liittyvää tietoa viestin alkuperästä, määränpäästä, reitistä ja koosta sekä viestinnän ajankohdasta, kestosta, laadusta ja muista vastaavista seikoista *(liikennetieto).*
>
> Esitutkintaviranomaisella ei ole 1 momentissa tarkoitetun säilyttämismääräyksen nojalla oikeutta saada tietoonsa viestin, liikennetiedon tai muun tallennetun tiedon sisältöä. Jos 3 momentissa tarkoitetun viestin välittämiseen on osallistunut useampi palveluntarjoaja, esitutkintaviranomaisella on kuitenkin oikeus saada tietoonsa palveluntarjoajien tunnistamiseksi tarvittavat liikennetiedot.
>
> 4 d §. Datan säilyttämismääräys annetaan määräajaksi, enintään kolmeksi kuukaudeksi. Määräaikaa voidaan pidentää enintään kolmella kuukaudella kerrallaan, jos rikoksen tutkinta sitä edellyttää.
>
> Säilyttämismääräyksen saanut on velvollinen pitämään salassa saamansa määräyksen.
>
> Rangaistus 2 momentissa säädetyn salassapitovelvollisuuden rikkomisesta tuomitaan rikoslain 38 luvun 1 tai 2 §:n mukaan, jollei teosta muualla laissa säädetä ankarampaa rangaistusta.

Datan säilyttämismääräys olisi uusi pakkokeino, jonka avulla voitaisiin turvata esitutkinnan kannalta relevantin datan säilyminen siihen saakka, kunnes siihen voidaan kohdistaa etsintä ja takavarikko. Pakkokeino olisi jokseenkin lievä, sillä se ei oikeuttaisi tiedon saantiin kysymyksessä olevan datan sisällöstä. Säännöksillä saatettaisiin lainsäädäntömme vastaamaan tietoverkkorikosyleissopimuksen 16 ja 17 artiklan vaatimuksia.

Vieraan valtion oikeusapupyynnön johdosta tapahtuvaa takavarikosta päättämistä koskevaan pakkokeinolain 4 luvun 15 a §:ään ehdotetaan lisättäväksi data esineen ja asiakirjan oheen sellaiseksi objektiksi, joka sanotunlaisen pyynnön johdosta voidaan takavarikoida.

Edellä selostettuun ehdotettuun 4 a §:ään liittyen ehdotetaan lukuun uutta 17 a §:ää, jonka mukaan data olisi palautettava sen omistajan tai haltijan käytettäväksi, jos 4 a §:n 2 momentissa tarkoitettu takavarikko kumotaan.

---

[292] Tietoverkkorikostyöryhmän mietintö, s. 80 ss.

Esitutkintalaki

Todistajan ilmaisuvelvollisuutta koskevaan esitutkintalain 27 §:ään ehdotetaan lisättäväksi uusi 2 momentti:

> Todistaja, jolla on 1 momentissa tarkoitettu ilmaisuvelvollisuus, on velvollinen myös esittämään hallussaan olevan rikostutkinnan kannalta merkityksellisen asiakirjan tai muun todistusaineiston.

Datan muodossa olevan aineiston katsottaisiin olevan todistajan hallussa, jos tietokone, tietojärjestelmä tai erillinen tallennusalusta, jolla data sijaitsee, on todistajan hallussa tai jos data sen fyysisestä sijainnista riippumatta on todistajan hallinnassa ja käytettävissä.[293] Perustelujen mukaan ehdotetun säännöksen tarkoituksena on selkiyttää voimassa olevaa sääntelyä velvoittamalla todistaja tietyissä tilanteissa itse esittämään kysymyksessä olevan kaltaisen aineiston. Esittämisvelvollisuutta rajoittaa kuitenkin suhteellisuusperiaate.

Esitutkintalain 28 §:ään työryhmä ehdottaa uutta 2 momenttia:

> Mitä 1 momentissa säädetään, sovelletaan myös todistajaan, joka kieltäytyy esittämästä asiakirjaa tai muuta todistusaineistoa.

Esitutkintalain 28 §:n 1 momentin mukaan todistamasta kieltäytyvän todistajan kuulustelu voidaan suorittaa tuomioistuimessa ja samaa menettelyä ehdotetaan sovellettavaksi myös ehdotetun 27 §:n 2 momentin mukaisesta velvollisuudesta kieltäytyvään todistajaan. Tuomioistuimella olisi kieltäytymistilanteissa käytettävissään oikeudenkäymiskaaren 17 luvun 15 §:n mukainen uhkasakko, minkä lisäksi olisi mahdollista määrätä ulosottomies noutamaan aineisto.[294]

Esitutkintalakiin ehdotetut muutokset saattaisivat voimaan tietoverkkorikosyleissopimuksen 18 artiklan esittämismääräystä koskevat määräykset.

Laki kansainvälisestä oikeusavusta rikosasioissa

Lain 15 §:ään ehdotetaan lisättäväksi uusi 2 momentti, jonka mukaan kaksoisrangaistavuuden vaatimus pakkokeinojen käyttöä koskevan oikeusavun antamisessa ei koskisi ehdotetun pakkokeinolain 4 luvun 4 c §:ssä tarkoitettua datan säilyttämismääräystä. Datan säilyttämismääräys olisi luonteeltaan valmisteleva toimenpide, joka ei sellaisenaan antaisi viranomaisille mahdollisuutta datan sisältöön kajoamiseen vaan ainoastaan varmistaisi datan tallessa pysymisen varsinaisten pakkokeinojen käyttämiseen saakka. Ehdotettu muutos saattaisi

---

[293] Tietoverkkorikostyöryhmän mietintö, s. 83 s. Perusteluissa puhutaan ”epäillystä”, vaikka ilmiselvästi tarkoitetaan todistajaa; kysymyksessä lienee pelkkä painovirhe.

[294] Tietoverkkorikostyöryhmän mietintö, s. 84.

lainsäädäntömme vastaamaan yleissopimuksen 29 artiklan 3 kappaleen määräyksiä.[295]

Lisäksi ehdotetaan lain 23 §:ään lisättäväksi *datan säilyttämismääräys* niiden pakkokeinojen luetteloon, jotka vieraan valtion oikeusapupyynnön johdosta voidaan todisteiden hankkimiseksi panna toimeen.

[295] Tietoverkkorikostyöryhmän mietintö, s. 84 s.

8 Lopuksi

Lainsäädännöstä

Olen osan I jaksossa 1.1.2 asettanut tämän tutkimuksen keskeiseksi tavoitteeksi sen selvittämisen, miten tietotekniikkarikossäännösten sijoittamista rikoslakiin koskevassa lainsäädäntötyössä on onnistuttu – miten säännökset täyttävät selkeyden ja yksiselitteisyyden vaatimukset ja miten luontevasti ja johdonmukaisesti ne asettuvat osaksi rikosoikeudellista sääntelyjärjestelmäämme.

Lainsäätäjän tehtävä ei ole ollut helppo. Kun ensimmäisiä säännöksiä ryhdyttiin 1980-luvulla valmistelemaan, ei edes tietotekniikan alkeiden tunteminen kuulunut sen paremmin juristien kuin muidenkaan sellaisten ihmisten perusvalmiuksiin, joiden ammattiin tai harrastuksiin tietotekniikka ei erityisesti liittynyt. Tietotekninen ympäristö oli lainsäätäjälle arvatenkin koko lailla vieras.

Nyt, vajaat kaksikymmentä vuotta myöhemmin, tietotekninen ympäristö on aivan toisenlainen. Tietotekniikka ja sen soveltaminen on saavuttanut sellaisen laajuuden, että vaikka juristit ja muutkin ihmiset luontevasti käyttävät tietoteknisiä sovelluksia työssään, on tietotekniikan todellinen hallitseminen ja ymmärtäminen edelleen maallikoille perin vaikeaa.

Tavat, joilla tietotekniikka voi liittyä rikosten tekemiseen, ovat myös olennaisesti muuttuneet. Parikymmentä vuotta sitten ei rikollinen yleensä ollut poliisia tai syyttäjää etevämpi tietotekniikkaekspertti ja mahdollisina tekotapoina nähtiinkin yleensä vain yksittäisiin tietojenkäsittelylaitteisiin kohdistuvat hyökkäykset, jotka useimmiten ajateltiin tehtäviksi laitteissa olevaa dataa käsittelemällä. Esimerkiksi virastojen ja laitosten tiedonsiirto tapahtui lähes yksinomaan asiakirjoja lähettämällä ja edistyneinkin tekninen apuväline, telekopiolaite, tuotti turvallisia (joskin joskus hieman huonosti luettavuutensa säilyttäviä) paperitulosteita. Nykyinen toimintaympäristö yhä lisääntyvine ja yhä enemmän tietoverkkoihin tukeutuvine tietoteknisine sovelluksineen on täysin erilainen ja paljon haavoittuvaisempi, vaikka paperin kulutus ei olekaan vähentynyt.

Tietotekniikkarikoksista on tullut vaarallisia rikoksia. Yhteiskunnan elintärkeiden toimintojen häiritseminen tai jopa keskeyttäminen voi olla teknisesti jokseenkin helposti toteutettavasti osaavan tekijän ollessa asialla.

Tätä taustaa vasten tarkasteltuna ja edellä tässä tutkimuksessa lausuttu huomioon ottaen voidaan mielestäni perustellusti sanoa lainsäätäjän onnistuneen tehtävässään vähintäänkin tyydyttävästi. Arviointia tietysti vaikeuttaa se, että säännöksiä ei ole käytännössä kovin usein päästy soveltamaan, mistä puoles-

taan seuraa, että esimerkiksi tähänastisten harvojen korkeimman oikeuden ratkaisujen perusteella ei liene syytä tehdä kovin pitkälle meneviä yksittäistapauksiin ulottuvia yleisempiä johtopäätöksiä. Joka tapauksessa säännelty alue on kansainvälisestikin vertailtuna varsin kattava eikä aukoista voida puhua.

Syynä viimeksi mainittuun tilanteeseen on epäilemättä paitsi se, että tietotekniikkarikosten kohdalla on ylipäänsä tehty poikkeuksellisen paljon edellä osan I jaksossa 2.1 perusteellisesti selostettua korkeatasoista kansainvälistä yhteistyötä, myös tietysti se, että Suomi on aktiivisesti osallistunut tähän yhteistyöhön. Ilman kansainvälisiä aloitteita ja malleja tietotekniikkarikoksia koskeva lainsäädäntömme tuskin olisi kattavuudeltaan lähelläkään sitä tasoa, millä se on nyt. Selvää on, että myös vastaisuudessa kansainvälisen yhteistyön merkitys tulee olemaan keskeinen. Rikosten tekemistä haittaavien valtioiden välisten rajojen menettäessä merkityksensä on valtioiden erilaisilla yhteenliittymillä korostunut tarve harmonisoida jäsentensä rikoslainsäädäntöä eikä harmonisoiminen onnistu ilman yhteisiä tutkimuksia, neuvotteluja ja kompromisseja. Osan I jaksossa 2.2 luotu katsaus eräiden valtioiden lainsäädäntöön osoittaa, että harmonisointitoimet ovat tuottaneet tulosta, ja lisää tuloksia on odotettavissa Euroopan neuvoston tietoverkkorikosyleissopimuksen ratifiointien ja kansainvälisen voimaantulon myötä.

Olkoonkin, että sääntelymme on kattavaa, jää toki myös kritiikille sijaa. Suomessa valittu lainsäätämistapa implementoitaessa Euroopan neuvoston vuoden 1989 suositusta eli työn kytkeminen rikoslain meneillään olleeseen kokonaisuudistukseen johti siihen, että tietotekniikkarikossäännöstöä ei arvioitu kokonaisuutena. Tästä ovat olleet seurauksena edellä erityisesti osan II jaksossa 7.1 kuvatut epäkohdat: tunnusmerkistöjen välisten rajojen tietynasteinen epämääräisyys sekä rangaistusasteikkojen epäjohdonmukaiset suhteet.

Viimeksi mainittua pidänkin ehkä voimassa olevan sääntelyn pahimpana epäkohtana: niin kauan kuin tietomurrosta, luvattomasta käytöstä ja vahingonteosta on huolimatta tekojen selvästi eriasteisesta haitallisuudesta säädetty samanlaiset rangaistusuhat, ei sääntelyä voi pitää tyydyttävänä. Valitettavasti tietoverkkorikostyöryhmän toimeksiantoon ei kuulunut voimassa olevan sääntelyn laajempi arviointi, sillä tilaisuus epäkohdan korjaamiseen olisi ollut hyvä.

Voimassa olevat säännökset kaipaavat siis yhä edelleen lainsäätäjän toimia, jotta tietotekniikkarikoksia koskevat kriminalisoinnit muodostaisivat yhtenäisen ja loogisen kokonaisuuden. Tunnusmerkistöjä ajatellen petossäännöksen hiljattain tapahtunut nykyaikaistaminen ei yksinään ole vielä riittävä parannus.

Tietojenkäsittelyrauhasta

Tutkimuksen edistymisen myötä olen ottanut käyttöön lainvalmistelussa jo aikaisemmin jossain määrin ja joissain muodoissa esiintyneen tietojenkäsittelyrauhan käsitteen ja pyrkinyt antamaan sille täsmällisen sisällön. Tällaisen

uuden – tai ainakin Suomessa tähän saakka harvoin käytetyn – käsitteen tarpeellisuus voidaan tietysti kyseenalaistaa, mutta vakaa käsitykseni on, että se helpottaa tietoteknisessä ympäristössä tehtyjä rikoksia koskevan sääntelyn systematisointia ja auttaa ymmärtämään kriminalisointien tarpeellisuuden.

Voitaisiin ehkä väittää, että koko tietotekniikkarikoksen käsite olisi viime vuosina hämärtynyt, kun tietotekniikan rooli niin sanottujen perinteisten rikosten tekemisessä ja selvittämisessä on kasvanut, ja että tässäkin mielessä tietojenkäsittelyrauhan merkityksen korostaminen olisi aiheetonta. Itse näen kuitenkin tilanteen juuri päinvastaisena: erilaisten tietojärjestelmien määrän räjähdysmäinen kasvu, järjestelmien suorituskyvyn ja tallennuskapasiteetin jatkuva lisääntyminen ja käyttäjien tuleminen yhä tiiviimmin toisistaan riippuvaisiksi on luonut uudentyyppisen maailman, jossa perinteiset lainalaisuudet eivät enää vaikuta.

Henkeen ja terveyteen kohdistuvien sen paremmin kuin varallisuusrikostenkaan perimmäiseen olemukseen tällainen kehitys ei vaikuta, vaikka niiden tekemisessä käytettäisiinkin tietotekniikkaa, mutta tietotekniikkarikosten – tekojen, joiden kohteena, välineenä tai tekoympäristönä on tietojärjestelmä siihen kuuluvine laitteineen ja joiden tekeminen tai rikosprosessuaalinen käsitteleminen edellyttää tietoteknistä osaamista – määrä ja monimuotoisuus lisääntyy. Kuitenkin niiden peruskaava eli oikeudeton tunkeutuminen tietojärjestelmään ja sitä mahdollisesti seuraava järjestelmän sisältämän datan oikeudeton käsitteleminen pysynee ennallaan.

Tietojärjestelmiin tallennetun ja järjestelmissä tai niiden välillä liikkuvan datan merkitys korostuu datan määrän lisääntymisen myötä. Entistä tärkeämmäksi muodostuu näin ollen tietojenkäsittelyrauhan tarkoittama olotila eli se, että tiedot säilyvät luottamuksellisina, eheinä ja käytettävinä. Yksi tapa turvata tietojenkäsittelyrauha on kriminalisoida sen loukkaukset. Tässä tutkimuksessa on tullut selvästi esille, että tällaiset kriminalisoinnit muodostavat luontevan kokonaisuuden ja että juuri tietojenkäsittelyrauha on se yhteinen nimittäjä, joka kytkee erilliset rangaistussäännökset toisiinsa. Myös osan II jaksossa 7.2.3 esittämäni ehdotus tietojenkäsittelyrauhan rikkomista koskevasta säännöksestä osoittaa, että itse asiassa kysymys on yhdestä ainoasta rikollisesta menettelytavasta, yhden nimenomaisen intressin turvaamisesta.

Summary

Antti Pihlajamäki

THE PROTECTION OF DATA PROCESSING UNDER CRIMINAL LAW

Provisions on Data Crimes in the Finnish Criminal Code

This study is divided into two parts. The general part contains two chapters. The first, introductory chapter deals with the importance and objects of the study as well as the concepts and methods used therein. The second chapter of the first part delineates the international co-operation concerning information technology crimes (IT-crimes) and also describes the national provisions of certain countries regarding the offences in question.

The second part contains eight chapters in which the provisions of data crimes are discussed in detail. In addition, the element of intent especially in respect of IT-crimes is dealt with. Finally, some conclusions and suggestions for the development of legislation are presented.

Introduction

The first provisions on IT-crimes were introduced into the Finnish Criminal Code in connection with the first stage in the total reform of the Criminal Code. These provisions entered into force at the beginning of 1991. In September 1995 the second stage of the total reform came into force. Also it included some provisions on IT-crimes. After these and a couple separate amendments, the Finnish provisions conformed quite well with the 1989 Recommendation of the Council of Europe. At the moment, the implementation of the 2001 Convention on Cyber-crime is in progress but it can be anticipated that in the field of substantive criminal law the amendments to the legislation shall not be very fundamental.

Two different techniques could have been used to write the provisions: either a specific law on IT-crimes could have been enacted or the provisions on IT-crimes could have been combined with the provisions on traditional crimes, such as fraud and forgery. The Finnish authorities have chosen the latter option. This choice may give rise to some incoherence because IT-crimes have never been considered as a unity.

In this study the IT-crimes are divided into data crimes and information crimes. The category of data crimes is the subject of the study and includes

offences which normally can be committed through the manipulation of stored computer data. The offences discussed in the study are unauthorised access, computer espionage, unauthorised use, computer-related forgery, computer-related fraud, means of payment fraud, damage to data, and data processing endangerment.

All of these offences have one common feature: they disturb data processing peace, *pax computationis.* Data processing peace is a new concept which has to some extent been used in the preparatory works of criminal legislation but not for example in the text of the Criminal Code itself. Data processing peace consists of three elements: the confidentiality, the integrity, and the availability of data. For example in the Anglo-American legal usage the term ”cia-offences” is commonly used to describe the category of the offences in question. Different data crimes disturb different elements of data processing peace. For example unauthorised access primarily disturbs the confidentiality of data while computer-related fraud primarily infringes upon the integrity of data. However, every data crime disturbs at least one of the elements of data processing peace.

Also the definition of IT-crime has been developed in the study. According to the definition, an information technology crime is an offence that is directed against, utilises, or is set against the data processing system with its devices, and the commission and/or procedural handling of which requires specific knowledge of information technology.

International Co-operation and Foreign Legislation

Over the past two decades international co-operation concerning IT-crimes has been very active and comprehensive. This work has been conducted within the framework of the OECD, the United Nations, the Council of Europe, the European Union, the International Association of Penal Law AIDP, the International Criminal Police Organisation Interpol, and so on. Several international instruments have been developed, the most important of which is the Council of Europe Convention on Cyber-crime. The significance of the work in the organisations mentioned cannot be stressed sufficiently: cyber-crime does not respect boundaries between states, and harmonisation of criminal and procedural legislation is of great importance.

The work on IT-crime conducted within the framework of the OECD, the Council of Europe, the United Nations, the AIDP, and the EU is discussed in detail in the study. Especially the 1986 OECD Recommendation, the 1989 Council of Europe Recommendation and 2001 Convention, and the 1994 United Nations Manual have been mentioned as basic instruments which have given guidelines for national legislators.

Different countries have chosen different legislative techniques when they have implemented international recommendations and conventions. In the

study, provisions on IT-crime in Sweden, Denmark, Germany, the United Kingdom, Switzerland, Italy, and the United States are examined. On the basis of this examination it is concluded that even though the legislation for example in common law countries seems to be very different from the Nordic legislation, there is very little difference in the scope of punishable behaviour. It can also be expected that the present differences will disappear almost completely in tandem with the implementation of the Cyber-crime Convention.

Offences Disturbing the Confidentiality of Data

Unauthorised access and unauthorised use have been regarded as offences which primarily disturb the confidentiality of data. If somebody has entered or used an information system, the owner or legitimate possessor of the system can never be absolutely sure whether something has been changed or not. The confidentiality of data has been lost. – Also computer espionage in cases where it is committed by breaking into a computer system has been included in this category.

Unauthorised access, hacking or cracking, has been a punishable offence in Finland since 1 September 1995. The provision in chapter 38, section 8 of the Criminal Code covers actions where the offender breaks into a computer system using access codes or passwords belonging to another or in other comparable way. The provision is secondary and can be applied only when the behaviour is not criminalised elsewhere in the law. Hacking is probably the most common IT-offence but only a few cases have been brought before the courts in Finland.

The provision on unauthorised use in chapter 28, section 7 of the Criminal Code entered into force at the beginning of 1991. The offence involves using, without right, property belonging to another. The concept of property also covers a computer system. Unauthorised use can be committed also after the offender has accessed the system via a network. The offender need not have the system physically in his/her possession. Mere hacking changes into unauthorised use as soon as the offender begins to use the system he/she has hacked. Some cases of unauthorised use have been handled in the Finnish courts.

The provisions on computer espionage are contained in chapter 30, section 4 of the Criminal Code and entered into force at the beginning of 1991. The offence covers, *inter alia,* situations where the offender has accessed a system including trade secrets in a way similar to that referred to in the provision on unauthorised access. Thus, computer espionage, which primarily can be defined as theft of information, can sometimes be regarded as a form of qualified unauthorised access.

Offences Disturbing the Integrity of Data

Criminalisation of computer-related forgery, computer-related fraud, and damage to data primarily protects the integrity of data. When any of these offences has been committed the content of the data has necessarily been changed and data have lost their integrity. – The Finnish Criminal Code also includes a provision on means of payment fraud, which can be seen as a specific form of fraud.

Computer-related forgery, i.e. falsification of an existing piece of evidence or preparation of a new false piece of evidence, is an IT-crime in cases where the object of the offence is in the form of computer data. A recording suitable for electronic data processing is expressly mentioned in the Criminal Code as one of the pieces of evidence which can be forged. The present provision on forgery in chapter 33, section 1 of the Criminal Code entered into force at the beginning of 1991. Prosecutors have brought charges in only a couple of computer-related forgery cases.

The modernized provision on computer-related fraud in chapter 36, section 1 of the Criminal Code entered into force in July 2003 but the idea of fraudulent manipulation of computer data was implemented in the Criminal Code already in 1991. The criminalised behaviour is described in the provision in the same manner as in most of the international instruments on the topic. Computer-related fraud has been quite unknown in practice.

Means of payment fraud has been separately criminalised only in a few countries, Finland among them. The provision in chapter 37, section 8 of the Criminal Code was enacted in 1991 but it was reformed in 1997 and covers, at the moment, actions aimed at, e.g., electronic money transfers and electronic commerce. In fact, many of the actions falling within the scope of this provision could be handled as computer-related frauds, but it seems that there is certain use also for a specific provision.

The provision on damage to data in chapter 35, section 1 of the Criminal Code criminalises unlawful damaging of stored computer data. It is not required that the data carrier somehow be harmed; if the unlawful change of the content of data causes damages to somebody the offender has made himself/herself guilty of damage to data. A few offenders have been sentenced for this offence.

Data Processing Endangerment

There are not very many countries where specific provisions concerning computer viruses and other malicious codes exist. Chapter 34, section 9a of the Finnish Criminal Code entered into force in December 1999. According to the provision, data processing endangerment means production and distribution of computer programs which are planned to cause harm or damage to data processing. Data processing endangerment can be regarded as an offence which

most seriously disturbs all of the three elements of data processing peace. Over the course of the few past years it has become obvious how seriously viruses and other malicious codes can hamper the use of world-wide information systems. Unfortunately, it has also become evident that the creators and distributors of those harmful programs can only in a very few cases be detected and brought to justice.

This is the case also in Finland. The provision on data processing endangerment has so far been applied only once. In this case the offenders had not even prepared a virus program but a specific program intended to facilitate the use of security loopholes which the offenders had found by scanning almost 200,000 data processing systems all over the world. In December 2003, the District Court of Helsinki regarded such a malicious program as a program meant in the provision in question.

Conclusions and Proposals

As an overall assessment, it can, without any doubt, be stated that Finnish legislation on data crimes is quite comprehensive and up-to-date. The comparison to foreign legislation shows that Finland has diligently fulfilled the obligations which have been imposed in existing international instruments. The implementation of the Cyber-crime Convention will in some degree extend the scope of punishable behaviour but the changes will not be fundamental. Articles 5 (system interference) and 6 (misuse of devices) of the Convention are the provisions which give reason for some adjustment of the present Finnish legislation.

However, from the domestic point of view, some criticism can be directed at the Finnish provisions. One of the main reasons for this seems to be the legislative technique which has not made it possible to consider data crimes as one unitary crime category.

With respect to the penal scales for different data crimes, clear inconsistency can be found. If somebody breaks into a data processing system without doing anything else, the offender is guilty of unauthorised access. If the offender, after having broken into a system, in a way or another uses the data stored in the system without damaging them, the offence changes into unauthorised use. And finally, if the offender who uses the data also damages them, he/she is to be sentenced for damage to data. Unauthorised access is not as serious threat to data processing peace as unauthorised use, which insults the rights of the victim more deeply. Damage to data goes further and is clearly a more serious violation than is unauthorised use.

Even so, the penal scales for unauthorised access, unauthorised use, and damage to data are the same. For every offence the offender can be sentenced to a fine or to imprisonment for at most one year.

Adjusting the penal scales would not be very simple because the provision on unauthorised use concerns the use of all forms of property and the provision on damage to data is linked to the general provision on damage to property. Thus, even though it would be more than sensible to have as maximum penalties one year of imprisonment for unauthorised access, 18 months for unauthorised use, and two years for damage to data, the realization of the idea would meet many practical difficulties and would require an overall examination of the provisions and chapters concerned.

Another disadvantage which has been identified in the study is the indefinite nature of the boundaries between the scopes of application of certain provisions. The essential elements of computer-related fraud, computer-related forgery, and damage to data seem to be rather similar. Every one of these offences can, in fact, be committed in the same way: entering, altering, deleting, or suppressing data in a data processing system. Which provision could be applied should depend on the final result of the action but, for example, a typical consequence of every offence is economic loss to the owner or the lawful possessor of data or the system.

So far, this problem has not been important in practice because the number of cases handled by the authorities has remained quite low. However, rewriting of the elements of these three offences could be recommended, at least for the future.

Some proposals which might solve most of the difficulties mentioned above have been presented in the study. Some of them concern penal scales and some of them aim at more IT-specific provisions. One proposal is to replace most of the existing provisions on IT-offences by one general provision, disturbing of data processing peace, which would cover the scope of behaviour mentioned in the present provisions on computer-related fraud, computer-related forgery, and damage to data.

As mentioned above, the implementation of the Council of Europe Cybercrime Convention is as of this writing (in June 2004) in progress. This process will not, however, mean an overall assessment of all the legislation on IT-crimes and the legislator will, even so, have some work to do. On the other hand, the development of information technique is so rapid that the criminal legislation in question can never be fully up-to-date. Therefore the authorities must constantly and actively follow the situation and be prepared for quick legislative actions, when necessary.

Finnish Lawyers' Association 2004
ISBN 951-855-233-9

Oikeustapaushakemisto

Oikeustapaushakemistoon on koottu ne korkeimpien oikeuksien ja hovioikeuksien päätökset, joita kirjassa on käsitelty tai joihin on viitattu.

Asiahakemisto

Hakemisto täydentää sisällysluetteloa.

SUOMALAISEN LAKIMIESYHDISTYKSEN JULKAISUJA
A-sarja N:o 258

Tietotekniikan huima kehittyminen parin viimeksi kuluneen vuosikymmenen aikana on ulottanut vaikutuksensa myös rikosoikeuteen. Elektronisessa muodossa olevaa todistusaineistoa voi liittyä lähes mihin tahansa rikokseen, mutta myös varsinaisten tietotekniikkarikosten määrä on jatkuvasti lisääntynyt.

Tässä teoksessa käsitellään Suomen rikoslain datarikoksia koskevaa sääntelyä. Datarikoksella ymmärretään rangaistavaa tekoa, jonka kohteena tai tekovälineenä on tietojärjestelmässä oleva data. Kaikilla datarikoksilla on yksi yhteinen suojeluobjekti, tietojen luottamuksellisuudesta, eheydestä ja käytettävyydestä koostuva tietojenkäsittelyrauha. Teoksessa tutkitaan, miten rikoslakimme säännökset onnistuvat antamaan suojaa tietojenkäsittelyrauhalle ja miten lainsäätäjä on onnistunut pannessaan täytäntöön tietotekniikkarikollisuutta koskevia kansainvälisiä suosituksia ja muita instrumentteja. Tietotekniikkarikoksia koskeva kansallinen sääntely perustuu niin Suomessa kuin ulkomaillakin paljolti kansainvälisissä järjestöissä tehtyyn harmonisointityöhön, jota teoksessa selvitetään laajasti.

Yksityiskohtaisesti arvioidaan tietomurtoa, yritysvakoilua, luvatonta käyttöä, väärennystä, petosta, maksuvälinepetosta, vahingontekoa ja vaaran aiheuttamista tietojenkäsittelylle koskevaa sääntelyä. Oikeuskäytäntöä tietotekniikkarikoksista on toistaiseksi varsin vähän, mutta harvoja olemassa olevia hovioikeuksien ja korkeimman oikeuden ratkaisuja analysoidaan teoksessa perusteellisesti. Voimassa olevan lainsäädännön ja oikeuskäytännön arvioinnin perusteella teoksessa annetaan muutamia lainsäädäntösuosituksia.

Teos on Suomen ensimmäinen tietotekniikkarikoksia koskeva laaja oikeustieteellinen tutkimus. Kirjoittaja on yli kymmenen vuoden ajan perehtynyt tietotekniikkarikoksiin paitsi tutkijana myös kouluttajana, lainvalmistelijana ja syyttäjänä. Rikosvastuun käytännön toteuttamiseen liittyvät näkökohdat ovatkin teoksessa useissa kohdin keskeisesti esillä, minkä vuoksi teos on hyödyllinen apuväline kaikille tietotekniikkarikoksiin liittyvissä lainkäyttötehtävissä toimiville.

LAKIMIESKUNNAN OMA LAATUKUSTANTAJA 1934–2004

www.lakimies.org
sly@lakimies.org

ISSN 0356-7206
ISBN 951-855-233-9