Hallituksen esitys Eduskunnalle laiksi rikoslain muuttamisesta

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ

Esityksessä ehdotetaan niin kutsutun tietokoneviruksen valmistaminen ja levittäminen kriminalisoitavaksi rikoslakiin otettavalla uudella säännöksellä. Tietokoneviruksella tarkoitetaan tietojenkäsittelylle tai tieto- tai telejärjestelmän toiminnalle haittaa aiheuttamaan tai sellaisen järjestelmän sisältämiä tietoja tai ohjelmistoja vahingoittamaan suunniteltua tietokoneohjelmaa tai ohjelmakäskyjen sarjaa. Ehdotettu rikosnimike on vaaran aiheuttaminen tietojenkäsittelylle. Rangaistusasteikoksi ehdotetaan sakkoa tai vankeutta enintään kaksi vuotta.

Lisäksi esityksessä ehdotetaan rikoslain säännöstä laittomasta tuontitavaraan ryhtymisestä muutettavaksi siten, että rikoksesta säädetty enimmäisrangaistus korotetaan kuudesta kuukaudesta vankeutta yhteen vuoteen kuuteen kuukauteen vankeutta. Lievempien tapausten varalta ehdotetaan lakiin lisättäväksi uusi pykälä, jossa säädettäisiin lievästä laittomasta tuontitavaraan ryhtymisestä. Seuraamus tästä rikoksesta olisi sakkoa.

Laki on tarkoitettu tulemaan voimaan mahdollisimman pian sen jälkeen, kun se on hyväksytty ja vahvistettu.

SISÄLLYSLUETTELO

PERUSTELUT

1. Rikoslain 34 luku

1.1. Johdanto

Yleistä

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.

Yleisesti puhutaan tietokoneviruksesta tai atk-viruksesta, kun tarkoitetaan sellaista tietokoneohjelmaa tai ohjelmakäskyjen sarjaa, joka on tarkoitettu haittaamaan tietojenkäsittelyä tai tieto- tai telejärjestelmän toimintaa taikka vahingoittamaan järjestelmän sisältämiä tietoja tai ohjelmistoja. Näitä ohjelmia koskeva terminologia on vakiintumatonta ja sikäli harhaan johtavaa, että virukset ovat vain yksi – joskin yleisin – tällaisten ohjelmien alalaji. Viruksille on ominaista se, että ne eivät kykene toimimaan itsenäisesti vaan tarvitsevat aina toisen ohjelman isännäkseen. Virukset voivat levitä itsestään tietokoneessa ohjelmasta toiseen ja tietoverkon välityksellä edelleen koneesta toiseen. Niin sanotut Troijan hevoset poikkeavat viruksista siinä, 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 ovat ohjelmia, jotka toimivat itsenäisesti ja osaavat kopioida itsensä toisiin koneisiin verkon avulla.

Englanninkielisinä yhteisnimityksinä kaikille edellä mainituille ja muille vastaaville ohjelmatyypeille käytetään muun muassa termejä "malware" ja "malicious code". Suomen kieleen ei vastaavanlaista yhteisnimitystä ole vakiintunut, vaikkakin "tuho-ohjelmaa" ja "tuholaisohjelmaa" on joissakin yhteyksissä käytetty. Perusteluissa käytetään esityksen yksinkertaistamiseksi jäljempänä sanaa "virus" tarkoittamaan kaikkia puheena olevia ohjelmia.

Virukset leviävät yleisimmin joko levykkeiden tai tietoverkkojen välityksellä. Tartunnan saaneessa koneessa ollut levyke tartuttaa kaikki muutkin koneet, joissa levykettä käytetään. Tietoverkkojen julkisista postilaatikoista tai ilmoitustauluilta kopioitavat ilmaisohjelmat voivat toimia maailmanlaajuisina virusten levittämiskeinoina.

Valtaosa tällä hetkellä tunnetuista yli 40 000 viruksesta on tehty toimimaan DOS-ympäristössä. Käynnistyslohkovirukset olivat pitkään yleisin virustyyppi, mutta nykyään eniten havaintoja tulee makroviruksista. Käynnistyslohkovirukset tarttuvat levykkeiden tai kiintolevyjen käynnistyslohkoihin, josta ne voivat kopioida itsensä mille tahansa koneessa käytetylle kirjoitussuojaamattomalle levykkeelle. Jos taas saastunut levyke on levykeasemassa konetta käynnistettäessä, virus kopioi itsensä koneen kiintolevylle.

Tiedostovirukset ovat lukumääräisesti yleisin viruslaji, joka leviää tavallisten ohjelmatiedostojen mukana. Aivan viime vuosina ovat alkaneet yleistyä makrovirukset, jotka leviävät ensi sijassa tekstitiedostojen välityksellä ja joita tällä hetkellä tunnetaan jo yli 3 500. Makrovirukset ovat perinteisiä viruksia helpommin kirjoitettavissa ja onkin pelättävissä, että virusten kirjoittaminen muuttuu ainakin jossain määrin tietotekniikan asiantuntijoiden harrastuksesta enemmän tavallisten tietotekniikan käyttäjien toiminnan suuntaan.

Suomesta on löydetty useita satoja erilaisia viruksia, joista Suomessa kirjoitettuja on useita kymmeniä.

Suurimmat viimeaikaiset muutokset liittyvät Internetiin. Liikkeellä on runsaasti sellaisia vahingollisia ohjelmia, jotka esimerkiksi lähettävät käyttäjän salasanoja tai muita luottamuksellisia tietoja pois koneesta Internetin kautta tai päästävät jonkun ulkopuolisen etäkäyttämään hyökkäyksen kohteena olevaa konetta tai järjestelmää.

Eri virustyyppien lukumäärä ei sisällä tietoa esiintymismääristä, jotka ovat moninkertaiset verrattuna pelkkiin tyypityslukuihin. Yhdessä yksittäisessä tapauksessa voi olla kysymyksessä parikymmentä erillistä konetta, niin kuin jäljempänä selostettavassa Suomen Eduskunnan tapauksessa, tai sitten yli 6000 "solmua", kuten ARPANET-verkon tapauksessa.

Kaikki virukset aiheuttavat jossain muodossa vahinkoa. Suuri osa viruksista on sellaisia, että ne ainoastaan leviävät, mutta tuolloinkin ne joka tapauksessa kuluttavat levytilaa, aiheuttavat yhteensopivuusongelmia ja hidastavat koneiden toimintaa sekä aiheuttavat puhdistus- ynnä muista vastaavista tehtävistä johtuvia huomattaviakin kustannuksia. Suoranaista taloudellista vahinkoa voi aiheutua silloin, kun aktivoitunut virus esimerkiksi tuhoaa tai muuttaa tiedostoja. Tällaisissa tilanteissa varsinkin seurannaisvaikutukset saattavat olla arvaamattomia ja hyvinkin huomattavia. Esimerkiksi viruksen muuttamien tietojen perusteella tehdyt väärät päätökset hallinnossa tai yrityksissä voivat johtaa merkittäviin vahinkoihin puhumattakaan tietokoneohjatussa toiminnassa syntyvistä seurauksista – esimerkkeinä voidaan mainita virusten mahdollinen vaikutus rautatie- tai ilmaliikenteen valvontajärjestelmiin. Täysin mahdollista on myös virusten käyttäminen yhtenä elektronisen sodankäynnin muotona.

Myös ennalta ehkäisevä virusten torjunta aiheuttaa viranomaisille ja yrityksille huomattavia kustannuksia. Virustapausten aiheuttamat välilliset ja välittömät kustannukset sellaisenaan ovat nousseet viimeisten kymmenen vuoden aikana huomattaviin summiin. Kaiken kaikkiaan tämän kielteisen ilmiön kerrannaisvaikutukset ja virustorjunnan kustannukset ovat teollisuusmaissa sellaista suuruusluokkaa, että asiantuntijat pitivät niitä jopa jo eri maiden kansantalouksiin vaikuttavina. Lukuisat virustorjuntayhtiöt ovatkin jo listautuneet Wall Streetin pörssiin. Lainsäätäjän selvä kannanotto ja virusten valmistajien motivaatioon vaikuttava riittävä rangaistuspelote on siis tarpeen taloudellisistakin syistä.

Tietotekniikkarikosten suojeluobjektista

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. Virusohjelmat loukkaavat siis aina tietojenkäsittely- ja tietoliikennerauhan perusteita.

Tiedonsiirto, langallinen tai langaton, on nykyään yhä tärkeämpi osa tietojenkäsittelyä ja sen häiriöttömyys on sekä kansallisesti että kansainvälisesti ensiarvoisen tärkeää. Tietoteknisten tallenteiden, olkoonpa kysymyksessä magneettinen (kuten kiintolevy tai levyke), optinen (CD-levy), elektroninen (ROM-muistipiiri) tai mekaaninen (esimerkiksi aiemmin yleinen reikäkortti), tallennusmuoto nojaa binääriseen esitykseen, jossa eheydellä on yhtä tärkeä käytännöllinen ja oikeudellinen merkitys kuin tiedonsiirrossakin. Yhdenkin kaksi-järjestelmän numeron, joko 0:n tai 1:n (bitti, lyhennys sanoista Binary Digit) muutos, joka empiirisesti on aina ja välttämättä myös fyysinen muutos, aiheuttaa väistämättä yksinkertaisen tarkistussumman tai kehittyneemmän turvallisuusmenettelyn eli niin sanotun tunnistetiivisteen muutoksen.

Perinteisten (paperi)asiakirjojen aitoustekijöinä ovat kautta aikojen olleet sinetit ja allekirjoitukset. Ennen kuin esimerkiksi testamentin sisällölle on voitu tai vastaisuudessakaan voidaan tuomioistuimessa antaa aineellista merkitystä, on sen aitous ja alkuperä selvitettävä. Sähköisten asiakirjojen, yhden rikoslaissa nimenomaan tarkoitettujen todistuskappaleiden lajin, aitouden todistaminen eli niiden oikeudellinen relevanssi ylimalkaan tulevassa oikeuselämässä perustuu ja tulee perustumaan vertailtavien tiedostojen ristiriidattomiin tuntomerkkeihin eli esimerkiksi tiedostoista laskettuihin niin sanottuihin tunnistetiivisteisiin. Tiivisteet ovat myös osa sähköisen allekirjoituksen menettelyä. Jolleivat nämä tiivisteet, esimerkiksi todistajan hallussa oleva merkkisarja (vaikkapa B1 4E 2A BD 96 08 8B A4 67 83 D1 09 FE 52 56 6C) täsmää tuomarin tietokoneellaan laskeman merkkisarjan kanssa, eivät asiakirjat ole sisällöllisesti samoja.

Virusohjelmat voivat siis vastaisuudessa aiheuttaa laajaa oikeudellista epävarmuutta ja estää sähköisen asioinnin ja kaupankäynnin tuhoamalla sähköisten asiakirjojen luotettavuusperustan. Kysymys ei siten ole pelkästään tietojen tuhoutumisesta, jolloin esimerkiksi terveydenhuollon tiedostojen tuhoutumisella voi olla yksilön kannalta tai laajemminkin jokaisen helposti käsittämiä kohtalokkaita vaikutuksia, vaan paljolti edellä tietoturvallisuuden käsitteen ja tietotekniikkarikosten suojeluobjektin kohdalla mainitusta "eheydestä" (Integrity), joka tarkoittaa datan ja informaation oikeellisuutta ja aitoutta sekä näiden ominaisuuksien säilyttämistä.

Esimerkkejä käytännön virustapauksista

Eduskunnan mikroista löytyi joulukuussa 1993 tietokonevirus Telefonica. Virus oli uudempi kuin käytössä ollut virustentorjuntaohjelmisto, joten tartunta paljastui vasta, kun virus tuhosi erään mikrotietokoneen kiintolevyn. Kaikkiaan virus ehti saastuttaa kaksikymmentä työasemaa. Kansanedustajia neuvottiin tekemään varmuuskopiot riittävän usein sekä varomaan laittomia ohjelmistokopioita ja pelejä. Myös heidän kotikoneistaan huolehdittiin hankkimalla niihin ajanmukaiset viruksentorjuntaohjelmistot.

Huhtikuussa 1995 Kanadasta lähetettiin Internet-keskusteluryhmään 2 806 virusta sisältänyt paketti. Paketti laitettiin myöhemmin suomalaiselle www-sivulle kenen hyvänsä saataville. Viruspaketti oli saatavilla Suomessa xgw-palvelimesta, joka oli Internetin niin sanottuja "pieniä purkkitarjoajia". Eräät vihaiset asiakkaat pyrkivät kuitenkin tekemään asiasta rikosilmoituksia. Ilmoitusten kohteena ollut henkilö oli vakaasti sitä mieltä, että kysymys oli hänen sananvapaudestaan.

Keskusrikospoliisi joutui ilmoituksen saatuaan toteamaan, ettei suurenkaan virusmäärän pelkkä saataville asettaminen ollut rangaistavaa Suomen voimassa olevan oikeuden mukaan. Kyse ei keskusrikospoliisin mielestä ollut sananvapaudesta, sillä yleisvaarallisten tietokoneohjelmien saataville asettamisessa ei ollut perusoikeutena suojeltavan oikeushyvän vaatimaa sisältöä eli viestitettävää sanomaa. Keskusrikospoliisi katsoi, että yleisten vaaran lähteen avaamista koskevien oikeusperiaatteiden mukaan tällainen teon jatkaminen oli laillisesti estettävissä sulkemalla asianomainen liittymä.

Telecom Finland Oy pyysi liikenneministeriön kannanottoa siihen, voiko yhtiö purkaa Internet-verkossa virusohjelmia levittävän palveluntuottajan yhteyden tai muutoin estää yhteydet virusohjelmia sisältävään palveluun. Liikenneministeriö teki 16 päivänä kesäkuuta 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. Liikenneministeriö 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.

Minkälaisesta häiriöstä ja vahingoista voi olla kyse, oli julkisuudessa laajalti tullut selväksi jo niin sanotun "Internet Worm"-tapauksen yhteydessä Amerikan Yhdysvalloissa syksyllä 1988. Tuho-ohjelma halvaannutti lopulta yli 6 000 tietokonetta U.S. Army Research Computer Network (ARPANET)-verkossa. Tekijä tuomittiin keväällä 1991 muutoksenhakutuomioistuimessa kolmeksi vuodeksi ehdolliseen vankeuteen, 400 tunnin yhdyskuntapalveluun sekä 10 000 dollarin sakkoihin.

Saksan tietoturvallisuusasiantuntijoiden (Bundesamt für Sicherheit der Informationstechnik, BSI, Bonn) mukaan tosiasia on, että Internet Wormin kaltaisia ohjelmia on varsin helppo kehitellä, että ne ovat oleellisesti vaikeampia havaita ja että ne mahdollisesti kykenevät tunkeutumaan entistä useampaan tietokoneeseen ja käyttöjärjestelmään (Internet Worm oli siten muotoiltu, että se tunkeutui kerrallaan vain kahteen eri käyttöjärjestelmäversiolla varustettuun konetyyppiin). Niissä suhteellisen yksinkertaiset jälkienpeit-

tämistekniikat tekevät rikoksentekijän henkilöllisyyden selville saamisen käytännöllisesti katsoen mahdottomaksi.

BSI järjesti helmikuussa 1997 Bonnissa kansainvälisen tietotekniikkavirusten lainsäädäntöproblematiikkaa koskevan kokouksen, jossa todettiin, että rikostilastot ja virustapaustilastot eivät kuvaa ongelman todellista suuruutta. Rikosilmoituksia ja oikeuteen saakka saatuja selvitettyjä tapauksia on ollut lähinnä vain Yhdistyneessä Kuningaskunnassa. Esimerkiksi Exeterissä tuomittiin virusten levittäjä joulukuussa 1995 vuoden ja kuuden kuukauden ehdottomaan vankeusrangaistukseen, jolla lehdistössä ja Internetissä laajasti julkistetulla tuomiolla oli selvästi havaittu alentava vaikutus vuonna Englannissa 1996 tilastoitujen virusten määrään.

Tulevaisuuden näkymiä synkistää ja kriminalisointia puoltaa paitsi se, että nykyään on verkoissa tarjolla edellä mainitun 2 806 viruksen kaltaisia paketteja, myös se, että nämä virukset usein ovat luonteeltaan pahemman laatuisia kuin aiemmin, ja nimenomaan se, että neuvoja ja automatisoituja työkaluja virusten kirjoittamiseen löytyy entistä enemmän.

1.2. Nykytila

Voimassa olevan rikoslain mukaan viruksen valmistaminen tai levittäminen ei sellaisenaan ole rangaistavaa. Vasta sitten, kun aktivoitunut virus on aiheuttanut vahinkoa, voidaan joissakin tapauksissa rangaista sitä, jonka toimenpiteistä johtuu, että virus on saastuttanut tietojärjestelmän.

Rikoslain (39/1889) 35 luvun 1 §:n 2 momentin mukaan vahingonteosta tuomitaan myös se, joka toista vahingoittaakseen oikeudettomasti hävittää, turmelee, kätkee tai salaa tietovälineelle tallennetun tiedon tai muun tallennuksen. Törkeästä vahingonteosta on 2 §:n mukaan kysymys muun muassa silloin, kun vahingonteolla aiheutetaan erittäin suurta taloudellista vahinkoa tai rikoksen uhrille tämän olot huomioon ottaen erityisen tuntuvaa vahinkoa, ja vahingonteko on myös kokonaisuutena arvostellen törkeä. Vahingonteosta tuomitaan sakkoa tai vankeutta enintään yksi vuosi ja törkeästä vahingonteosta vankeutta vähintään neljä kuukautta ja enintään neljä vuotta. Jos vahingonteko on kokonaisuutena arvostellen vähäinen, on kysymyksessä 3 §:ssä tarkoitettu lievä vahingonteko, josta tuomitaan rangaistukseksi sakkoa. Vahingonteko on rangaistavaa ainoastaan tahallisesti tehtynä. Vahingonteko ja lievä vahingonteko ovat asianomistajarikoksia kohdistuessaan yksityiseen omaisuuteen.

Virus saattaa aiheuttaa tallennetun tiedon häviämisen tai turmeltumisen. Kun näin tapahtuu, vahingontekorikoksen objektiivinen tunnusmerkistö täyttyy. Jotta virustartunnan aiheuttajaa voitaisiin rangaista teostaan, on kuitenkin edellytyksenä, että hän on menetellyt tahallisesti tarkoituksenaan toisen vahingoittaminen. Viruksen leviäminen saattaa olla hyvin sattumanvaraista ja lähtökohtaisesti tilanne lienee sellainen, että viruksen kirjoittajalla tai levittäjällä ei ole mielessään jonkin määrätyn, tietyssä tietokoneessa tai tietyllä tietovälineellä olevan informaation vahingoittaminen. Viruksen valmistaja on saattanut – esimerkiksi taitojaan testatakseen – ainoastaan pyrkiä kirjoittamaan viruksen aikomattakaan saada sitä leviämään ja leviäminen puolestaan on saattanut aiheutua jonkun toisen huolimattomuudesta. Tällaisissa ja muissa vastaavissa tilanteissa on vähintäänkin kysymyksenalaista, voidaanko lopulta mahdollisesti tapahtuvaa vahingon aiheutumista lukea kenenkään syyksi tahallisena vahingontekorikoksena. Kysymyksenalaista on myös se, soveltuvatko vahingontekoa koskevat säännökset sanamuotonsa puolesta sellaisen viruksen levittämiseen, jonka aiheuttama vahinko on ainoastaan välillistä eikä johdu tallennetun tiedon häviämisestä tai turmeltumisesta, vaikka tuolloinkin on kysymyksessä tietojenkäsittelyn eheyden loukkaaminen, sillä yhdenkin bitin muuttaminen antaa esimerkiksi tunnistearvoa laskettaessa poikkeavan lopputuloksen ja saa sähköisen asiakirjan todistusarvon häviämään.

Rikoslain 34 luvun 1 §:n 2 momentin mukaan tuhotyöstä tuomitaan myös se, joka muun muassa tietojärjestelmän toimintaan oikeudettomasti puuttumalla aiheuttaa vakavan vaaran energiahuollolle, yleiselle terveydenhuollolle, maanpuolustukselle, oikeudenhoidolle tai muulle näihin rinnastettavalle yhteiskunnan tärkeälle toiminnolle. Jos tuhotyö tehdään aiheuttaen suurelle ihmismäärälle vakavaa hengen tai terveyden vaaraa, aiheuttaen jollekin yhteiskunnan tärkeälle toiminnolle uhkaavan vahingon pitkäaikaisuuden tai laaja-alaisuuden vuoksi taikka muusta syystä erityisen vakavaa vaaraa taikka sodan tai muiden poikkeusolojen aikana ja

rikos on myös kokonaisuutena arvostellen törkeä, on kysymyksessä 3 §:ssä tarkoitettu törkeä tuhotyö. Rangaistus tuhotyöstä on vankeutta vähintään neljä kuukautta ja enintään neljä vuotta ja törkeästä tuhotyöstä vankeutta vähintään kaksi ja enintään kymmenen vuotta. Molempien rikosten yritys on rangaistava.

Joissakin tapauksissa virustartunnan aiheuttaminen saattaa merkitä sellaista puuttumista tietojärjestelmän toimintaan, että tuhotyörikosta koskevia rangaistussäännöksiä voidaan soveltaa. Toisin kuin vahingontekorikoksissa ei tuhotyössä edellytetä vahingon syntymistä vaan pelkkä vaaran aiheutuminen riittää, joten tässä suhteessa rangaistavuuden kynnys ylittyy jo ennen viruksen aktivoitumista. Toisaalta tuhotyötä koskevat säännökset ovat sisällöltään sellaisia, että ne voivat tulla sovellettaviksi vain jokseenkin harvoin.

1.3. Viruksia koskeva sääntely eräissä valtioissa

Euroopan valtioista on tällä hetkellä voimassa virusten valmistamiseen tai levittämiseen liittyviä kriminalisointeja Alankomaissa, Italiassa, Sveitsissä, Venäjällä ja Yhdistyneessä Kuningaskunnassa. Kriminalisointeja valmistellaan lisäksi Ruotsissa ja Saksassa.

Alankomaat

Alankomaiden rikoslain vuodelta 1992 olevan säännöksen mukaan tuomitaan rangaistukseen se, joka tahallisesti tai oikeudettomasti asettaa saataville tai levittää sellaista dataa, joka on tarkoitettu aiheuttamaan vahinkoa kopioimalla itseään tietojärjestelmässä. Seuraamukseksi rikoksesta säädetään vankeutta enintään neljä vuotta tai sakkoa enintään 100 000 guldenia.

Italia

Italian rikoslakiin lisättiin vuonna 1993 säännös, jonka 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. Rikokseen syyllistynyttä rangaistaan enintään kahden vuoden vankeudella ja enintään 20 000 000 liiran sakolla.

Sveitsi

Sveitsin rikoslain vuoden 1995 alusta voimaan tulleen säännöksen 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 tekijän tarkoituksena on ollut hyödyn hankkiminen, rangaistus on vankeutta enintään viisi vuotta.

Venäjä

Venäjän rikoslaissa on säännös, joka koskee vahingollisen tietokoneohjelman luomista, käyttämistä ja levittämistä. Säännöksen mukaan rangaistaan enintään kolmen vuoden vankeudella ja sakolla sitä, joka valmistaa sellaisen ohjelman tai muuttaa olemassa olevan ohjelman sellaiseksi, että se informaatiota hävittämällä, sulkemalla, muuttamalla tai kopioimalla aiheuttaa tietojenkäsittelyn, tietojärjestelmän tai tietoverkon vahingoittumisen. Rangaistavaa on myös tällaisen ohjelman tai sen sisältävän laitteen käyttäminen ja levittäminen. Jos teolla on aiheutettu vakavia seurauksia, on seuraamus vankeutta vähintään kolme ja enintään seitsemän vuotta.

Yhdistynyt Kuningaskunta

Yhdistyneen Kuningaskunnan vuoden 1990 Computer Misuse Act (CMA) on tietotekniikkarikoksia koskeva laki, jossa on jokseenkin yleisiä rangaistussäännöksiä. Toisin kuin edellä käsitellyissä maissa ei Yhdistyneessä Kuningaskunnassa ole nimenomaista virusten valmistamista tai levittämistä koskevaa säännöstä, mutta CMA:n hyvin yleiseen

ja kattavaan muotoon laadittu pykälä kriminalisoi myös sellaisen toiminnan, jota virusten levittäminen tarkoittaa. Säännöksen mukaan on rangaistavaa mikä tahansa sellainen toiminta, joka aiheuttaa minkä tahansa tietokoneen sisällön oikeudettoman muuttamisen. Rangaistukseksi rikoksesta säädetään vankeutta enintään viisi vuotta, sakkoa tai sekä sakkoa että vankeutta.

Ruotsi

Ruotsissa on olemassa vuodelta 1992 ehdotus (SOU 1992:110) rikoslain yleisvaarallisia rikoksia koskevaksi uudeksi pykäläksi. Pykälän mukaan rangaistaisiin sitä, joka valmistaa sellaisen tietokoneohjelman tai ohjelmakäskyjen sarjan (datavirus), joka on konstruoitu niin, että se oikeudettomasti voi vaikuttaa automaattisesti käsiteltäviin tietoihin tai sellaisen käsittelyn teknisiin apuvälineisiin. Rangaistavaa olisi myös mainitunlaisen ohjelman tai ohjelmakäskyjen sarjan sellainen levittäminen, josta aiheutuu yleinen vaara, että edellä mainitut tiedot häviävät tai muuttuvat tai että tietojenkäsittelyn tekniset apuvälineet vahingoittuvat tai niiden toiminta häiriintyy. Seuraamus rikoksesta olisi sakkoa tai vankeutta enintään kaksi vuotta tai, jos rikos on törkeä, vankeutta vähintään kuusi kuukautta ja enintään kuusi vuotta. Lisäksi ehdotetaan rikoslakiin otettavaksi säännös, jossa säädettäisiin samanlainen rangaistusuhka viruksen törkeästä huolimattomuudesta tapahtuneelle levittämiselle.

Ruotsin ehdotus kuuluu osana hyvin laajaan tietotekniikkarikoksia koskevaan lainuudistushankkeeseen, joka ei ole edennyt kovinkaan nopeasti. Viruspykälästä annetuissa lausunnoissa on suhtauduttu enimmäkseen myönteisesti ajatukseen viruksen levittämisen kriminalisoimisesta. Sen sijaan valmistamisen kriminalisoimista ei ole nähty erityisen tarpeelliseksi, mikä johtuu siitä, että ehdotuksen mukaan säännöksessä tarkoitetun rikoksen valmistelu tulisi olemaan rangaistavaa.

Saksa

Saksassa on edellä mainitussa BSI:n kokouksessa esitetty luonnosehdotus viruspykäläksi. Luonnoksen mukaan rangaistaisiin vankeudella enintään viideksi vuodeksi tai sakolla sitä, joka oikeudettomasti tuottaa, levittää, tarjoaa tai asettaa saataville sellaisia ohjelmia tai dataa, jotka on tarkoitettu hävittämään, muuttamaan tai tekemään käyttökelvottomaksi tietoja tai ohjelmistoja, neuvoo valmistamaan sellaisia ohjelmia tai tuottaa niiden valmistamiseen soveltuvia välineitä. Yksityiskohtaisempi keskustelu pykälästä on Saksassa vasta alkamassa.

1.4. Ehdotettu muutos

Esityksessä ehdotetaan rikoslain yleisvaarallisia rikoksia koskevaan 34 lukuun lisättäväksi uusi 9 a §, jossa kriminalisoidaan vaaran aiheuttaminen tietojenkäsittelylle. Niin kuin edellä nykytilan kuvauksessa on todettu, viruksen levittämisellä ei niinkään tähdätä jonkin määrätyn, tietyssä paikassa sijaitsevan informaation vahingoittamiseen. Viruksen valmistaminen ja levittäminen onkin tyypillinen yleistä vaaraa aiheuttava rikos, minkä vuoksi säännös ehdotetaan sijoitettavaksi rikoslain 34 lukuun.

Ehdotetun pykälän *1 kohdan* mukaan rangaistaisiin sitä, joka, aiheuttaakseen 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.

Tekijältä edellytettäisiin tahallisuutta, joka tässä yhteydessä käsittää tarkoituksen aiheuttaa haittaa tietojenkäsittelylle tai tieto- tai telejärjestelmän toiminnalle. Käsite "tietojenkäsittely" on tässä tarkoitettu käsitettäväksi laajasti siten, että sillä tarkoitetaan kaikkea tietotekniikkaa hyväksi käyttäen tapahtuvaa tietojen käsittelemistä ja siirtoa.

Tietojärjestelmällä tarkoitetaan samaa kuin rikoslain 38 luvun 8 §:n tietomurtoa koskevassa säännöksessä eli sellaista tietojärjestelmää, jossa tietoja käsitellään, varastoidaan tai siirretään sähköisesti tai muulla vastaavalla teknisellä keinolla (HE 94/1993 vp s. 155). Tietojärjestelmä on ymmärrettävä siinä mielessä laajasti, että sillä ei tarkoiteta yksinomaan useiden tietojenkäsittely- ja siirtolaitteiden muodostamaa verkostoa, vaan yksittäinen tietokonekin voi olla pykälässä tarkoitettu tietojärjestelmä.

Telejärjestelmällä puolestaan tarkoitetaan samaa kuin televerkolla rikoslain 38 luvun 3 §:ssä siltä osin, kuin kysymys on tietojärjestelmässä käsitellyn datan siirtämiseen soveltuvasta verkosta. Viimeksi mainitun säännöksen perustelujen (HE 94/1993 vp s. 150) mukaan televerkko on siirtojohtojen sekä muiden telelaitteiden ja -rakenteiden muodostama kokonaisuus, jossa voidaan sähkömagneettisten aaltojen avulla välittää viestejä. Televerkko voi muodostua esimerkiksi organisaation sisäisestä puhelin- tai tietoliikenneverkosta. Tieto- ja telejärjestelmällä tarkoitetaan siis kaikkia automaattiseen tietojenkäsittelyyn soveltuvia järjestelmiä alkaen yksittäisestä tietokoneesta ja päätyen maailmanlaajuisiin tietoverkkoihin.

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.

Tällainen tahallisuuden vaatimus sulkee rangaistavuuden alan ulkopuolelle sellaiset tilanteet, joissa esimerkiksi tietojenkäsittelyyn perehtynyt henkilö haluaa kokeilla ohjelmointitaitojaan luomalla virusohjelman aikomatta kuitenkaan missään vaiheessa päästää aikaansaannostaan leviämään omaa konettaan kauemmaksi. Rangaistavia olisivat vain sellaiset teot, joissa tekijä alun perin on tarkoittanut viruksen leviämään ja aiheuttamaan haittaa tietojenkäsittelylle.

Tekotapoina mainitaan ohjelman tai ohjelmakäskyjen sarjan valmistaminen, saataville asettaminen ja levittäminen. Valmistamisella tarkoitetaan uuden ohjelman kirjoittamista tai olemassa olevan ohjelman muuttamista pykälässä tarkoitetun kaltaiseksi. Saataville asettaminen tarkoittaa lähinnä virusohjelman asettamista tietoverkosta yleisesti kopioitavaksi. Tyypillinen levittämistoimi puolestaan olisi esimerkiksi saastuneen tietokonelevykkeen käyttäminen tietokoneessa. Tahallisuus ei välttämättä edellytä nimenomaista levittämistarkoitusta, mutta tekijän on tiedettävä viruksen olemassaolosta ja miellettävä sen leviäminen tekonsa varsin todennäköiseksi seuraukseksi.

Ilmaisulla "tietokoneohjelma tai ohjelmakäskyjen sarja" tarkoitetaan kaikkia edellä jaksossa 1.1. kuvattuja varsinaisia viruksia ja niitä muistuttavia ohjelmia. Ohjelman tai ohjelmakäskyjen sarjan on oltava nimenomaan suunniteltu sellaiseksi, että se ominaisuuksiltaan soveltuu ensisijaisesti tietojenkäsittelyn tai tieto- tai telejärjestelmän toiminnan vaarantamiseen taikka sellaisen järjestelmän sisältämien tietojen tai ohjelmistojen vahingoittamiseen. Ohjelman on siis oltava laadittu juuri tätä tarkoitusta varten ja tekijän on oltava tästä tietoinen. Jos ohjelmaan on sen laatijan sitä tarkoittamatta tullut jokin sellainen ominaisuus, jolla on edellä mainittuja vaikutuksia, ei kysymyksessä ole pykälässä tarkoitettu ohjelma.

Rangaistavuus ei edellyttäisi, että teosta tosiasiallisesti aiheutuisi konkreettista haittaa tietojenkäsittelylle tai tieto- tai telejärjestelmän toiminnalle tai että järjestelmän sisältämät tiedot tai ohjelmistot todella vahingoittuisivat. Riittävää olisi, että ohjelma tai ohjelmakäskyjen sarja on suunniteltu aiheuttamaan vaaraa tai vahinkoa. Käytännössä tämä tarkoittaisi esimerkiksi sitä, että jos tietojärjestelmään tarttunut virus havaitaan ennen kuin se on ehtinyt aktivoitua ja aiheuttaa vahinkoa, voidaan viruksen valmistaja muiden edellytysten täyttyessä saattaa rangaistusvastuuseen teostaan. Samoin jos henkilön tietokoneelta löydetään tämän valmiiksi kirjoittama virus, joka ei vielä ole levinnyt, voidaan kirjoittajaa rangaista, jos käy selville, että hän on valmistanut viruksen nimenomaisena tarkoituksenaan aiheuttaa haittaa tietojenkäsittelylle tai tieto- tai telejärjestelmän toiminnalle eli saattaa virus leviämään.

Pykälässä tarkoitettu vaara tai vahinko voisi syntyä ensisijaisesti sen seurauksena, että virus aktivoiduttuaan keskeyttäisi tieto- tai telejärjestelmän toiminnan kokonaan tai osaksi tai muuttaisi järjestelmän toimintaa tai järjestelmän sisältämiä tietoja.

Järjestelmään tarttunut virus saattaa pysäyttää järjestelmän toiminnan kokonaan tai osaksi. Se voi myös muuttaa järjestelmän toimintaa siten, että järjestelmä esimerkiksi tuottaa muunlaista informaatiota kuin alun perin on ollut tarkoituksena. Yksittäisen tietojärjestelmän osalta tällöin on kysymyksessä vaikutuksiltaan rikoslain 36 luvun 1 §:n 2 momentissa tarkoitettua tietojenkäsittelypetosta muistuttava tilanne. Toisaalta järjestel-

män toimintaa muuttaa jo se, että esimerkiksi tietokoneen kiintolevylle tarttunut virus kuluttaa levytilaa ja hidastuttaa koneen toimintaa. Lisäksi yhdenkin bitin muuttuminen toiseksi vaikuttaa tietojenkäsittelyn eheyteen, jolloin tallennetun tiedon todistusarvo saattaa kärsiä.

Virus voi myös muuttaa järjestelmän sisältämiä tietoja joko hävittämällä niitä tai muulla vastaavalla tavalla. Tällaisessa tapauksessa kysymyksessä on vaikutuksiltaan rikoslain 35 luvun 1 §:n 2 momentissa tarkoitettuun vahingontekoon verrattava tilanne.

Pykälän *2 kohdan* mukaan rangaistaisiin myös sitä, joka asettaa saataville ohjeen 1 kohdassa tarkoitetun tietokoneohjelman tai ohjelmakäskyjen sarjan valmistamiseen tai levittää sellaista ohjetta. Ohjeella tarkoitetaan tässä niin yksityiskohtaista ohjetta, että vähänkin tietojenkäsittelyyn perehtynyt henkilö sen perusteella pystyy valmistamaan viruksen. Tällaisen ohjeen saataville asettaminen tai levittäminen on vaarallisuudeltaan lähes täysin rinnastettavissa valmiin viruksen saataville asettamiseen tai levittämiseen, joten teko on syytä saattaa samanlaisen rangaistusuhan alaiseksi. Koska ohje ei kuitenkaan voi levitä itsestään samalla tavoin kuin valmis ohjelma, ei pelkkä ohjeen valmistaminen vielä aiheuta sellaista vaaraa, että myös valmistaminen olisi syytä säätää rangaistavaksi.

Kun viruksen saataville asettaminen tai levittäminen on mahdollista vain tietotekniikkaa hyväksi käyttäen, voidaan ohje asettaa saataville tai sitä levittää tietotekniikan keinojen lisäksi esimerkiksi painokirjoituksessa.

Myös ohjeen saataville asettamisen ja levittämisen rangaistavuuden edellytyksenä on, että tekijä on toiminut tarkoituksin aiheuttaa haittaa tietojenkäsittelylle tai tieto- tai telejärjestelmän toiminnalle.

Ehdotettu rikosnimike on *vaaran aiheuttaminen tietojenkäsittelylle*. Nimikkeestä on tarkoituksellisesti jätetty pois sana "automaattiselle", sillä yleisessä kielenkäytössä ollaan vähitellen luopumassa käsitteestä "automaattinen tietojenkäsittely". Säännöksen sisällöstä käy selville, että säännös tarkoittaa nimen omaan tietotekniikkaan perustuvaa tietojenkäsittelyä.

Rangaistusasteikoksi ehdotetaan sakkoa tai vankeutta enintään kaksi vuotta. Asteikko on sama kuin yleisvaarallisen rikoksen valmistelua koskevassa rikoslain 34 luvun 9 §:ssä, jota ehdotettu säännös luonteeltaan osaksi muistuttaa. Asteikko antaa lain soveltajille riittävästi liikkumavaraa, sillä pykälässä tarkoitetut teot voivat vaaralisuudeltaan olla hyvin erilaisia. Pahimmillaan teko saattaa tosiasiallisesti merkitä rikoslain 21 luvun 13 §:ssä tarkoitettuun vaaraan toisen hengelle tai terveydelle rinnastettavan vaaran aiheuttamista. Kaikkein vakavimmissa tapauksissa tekoon voidaan soveltaa rikoslain 34 luvun tuhotyötä koskevan 1 §:n 2 momenttia.

Puheena olevien rikosten tutkinnan kannalta on lisäksi olennaista, että rangaistusasteikko on riittävä antamaan esitutkintaviranomaisille mahdollisuudet tarpeellisten pakkokeinojen käyttöön.

Pykälää ei sovellettaisi, jos teosta muualla laissa säädetään ankarampi tai yhtä ankara rangaistus.

Jos virus on aktivoitunut ja päässyt aiheuttamaan haittaa tai vahinkoa tai niiden konkreettista vaaraa, saattavat viruksen valmistajan tai levittäjän tahallisuudesta riippuen tekoon tulla sovellettaviksi esimerkiksi rikoslain 35 luvun 2 §:n säännös törkeästä vahingonteosta, 36 luvun 1 §:n 2 momentin säännös petoksesta ja 2 §:n säännös törkeästä petoksesta sekä 38 luvun 5 §:n säännös tietoliikenteen häirinnästä ja 6 §:n säännös törkeästä tietoliikenteen häirinnästä, joista kaikista on säädetty yhtä ankarat tai ankarammat rangaistusuhat kuin ehdotuksen mukaisesta vaaran aiheuttamisesta tietojenkäsittelylle. Silloin, kun tekoon soveltuisi 35 luvun 1 §:n 2 momentin säännös vahingonteosta, sovellettaisiin sekä vahingontekoa koskevaa että ehdotettua säännöstä. Tämä olisi perusteltua siitä syystä, että viruksen valmistaminen ja levittäminen joka tapauksessa on 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.

2. Rikoslain 46 luku

2.1. Nykytila

Rikoslain 46 luku uudistettiin rikoslain kokonaisuudistuksen ensimmäisen vaiheen yhteydessä tammikuun 1 päivänä 1991 voimaan tulleella lailla. Lukuun sisällytettiin laitonta tuontitavaraan ryhtymistä koskeva

6 §, jolla korvattiin aikaisempi tullimaksua kavaltaen tai salakuljettaen maahan tuotuun tavaraan ryhtymistä koskenut sakkouhkainen rikoslain 38 luvun 13 §:n säännös. Laittomasta tuontitavaraan ryhtymisestä säädetään rangaistukseksi sakkoa tai enintään kuusi kuukautta vankeutta. Lievästä tai törkeästä tekomuodosta ei ole erillistä säännöstä.

Laitonta tuontitavaraan ryhtymistä koskeva säännös vastaa siinä luetelluilta tekotavoiltaan ("kätkee, hankkii, ottaa huostaansa tai välittää") rikoslain 32 luvun 1 §:n kätkemisrikosta koskevaa säännöstä. Laittoman tuontitavaraan ryhtymisen esirikoksina tulevat kysymykseen säännöstelyrikos, törkeä säännöstelyrikos, lievä säännöstelyrikos, salakuljetus, lievä salakuljetus, veropetos, törkeä veropetos ja lievä veropetos. Kätkemisrikoksen esirikoksina mainitaan varkaus-, kavallus-, ryöstö-, kiristys-, petos-, kiskonta- ja maksuvälinepetosrikos sekä velallisen petos, törkeä velallisen petos ja tahallinen velallisen vilpillisyys. Kätkemisrikoksen rangaistusasteikko on sakkoa tai vankeutta enintään vuosi ja kuusi kuukautta, törkeästä kätkemisrikoksesta voidaan tuomita vankeutta neljästä kuukaudesta enintään neljään vuoteen ja ammattimaisesta kätkemisrikoksesta vankeutta neljästä kuukaudesta enintään kuuteen vuoteen. Kätkemisrikkomuksesta seuraamus on sakkoa.

Rikoslain 46 luvun 6 §:ää koskevissa hallituksen esityksen perusteluissa (HE 66/1988 vp ss. 176 ja 181) ei tarkemmin käsitellä rangaistusasteikkoa koskevaa kysymystä eikä myöskään pohdita törkeysluokituksen tarpeellisuutta. Käytäntö on varsinkin viime vuosina osoittanut, että laittoman tuontitavaraan ryhtymisen tunnusmerkistö voi toteutua myös sellaisella menettelyllä, jonka kohteena on huomattavan arvokas omaisuus. Huhtikuussa 1997 tuomittiin laittomasta tuontitavaraan ryhtymisestä henkilö, joka oli ottanut huostaansa neljä miljoonaa Suomeen salakuljetettua savuketta. Jos esirikoksena olisi salakuljetuksen asemesta ollut esimerkiksi varkaus, olisi tekijän menettelyä epäilemättä lähtökohtaisesti arvioitu törkeää kätkemisrikosta koskevan säännöksen pohjalta.

Rajojen ylittymisen helpottuminen helpottaa myös sellaisten laittoman tuontitavaran ryhtymisen esirikoksina kysymykseen tulevien rikosten tekemistä, joiden kohteena voi olla erittäin arvokasta omaisuutta. Näin ollen on tarpeellista saattaa laittoman tuontitavaraan ryhtymisen rangaistusasteikot paremmin vastaamaan kätkemisrikosten rangaistusasteikkoja.

2.2. Ehdotetut muutokset

Laiton tuontitavaraan ryhtyminen

Rikoslain 46 luvun 6 §:n rangaistusasteikkoa ehdotetaan muutettavaksi niin, että enimmäisrangaistus nykyisen kuuden kuukauden asemesta olisi vuosi ja kuusi kuukautta vankeutta. Näin rangaistusasteikko vastaisi kätkemisrikoksen perusmuodon rangaistusasteikkoa. Ehdotettu rangaistusasteikko mahdollistaisi asian käsittelemisen yhden tuomarin kokoonpanossa silloin, kun tällaista käsittelyä olisi pidettävä tarkoituksenmukaisena. Lisäksi ehdotettu rangaistusasteikko antaisi esitutkintaviranomaisille mahdollisuuden riittävien pakkokeinojen käyttöön, mikä ei nykyisin tule kysymykseen.

Lievä laiton tuontitavaraan ryhtyminen

Valtaosa laittoman tuontitavaraan ryhtymisen tunnusmerkistön toteuttavista rikoksista on tosiasiallisesti varsin vähäisiä. Tyypillinen tällainen teko on esimerkiksi muutaman laittomasti maahantuodun alkoholipullon tai savukekartongin ostaminen. Tällaisten tekojen osalta on tarpeen erikseen säätää lievemmästä tekomuodosta, josta rangaistuksen määrääminen voi edelleen tapahtua rangaistusmääräysmenettelyssä. Tämän vuoksi lakiin ehdotetaan otettavaksi uusi lievää laitonta tuontitavaraan ryhtymistä koskeva säännös (46 luvun 6 a §), jossa seuraamukseksi säädettäisiin sakkoa.

Rajoitussäännös, omaisuuden menettäminen ja menettelysäännös

Uuden 6 a §:n lisääminen lukuun ehdotetuin tavoin edellyttää, että 7 §:n rajoitussäännökseen, 8 §:n omaisuuden menettämistä koskevaan säännökseen ja 12 §:n menettelysäännökseen tehdään lisäystä vastaavat teknisluonteiset muutokset.

3. Esityksen vaikutukset

Esitys laajentaa 34 lukua koskevilta osiltaan jossain määrin rangaistavan menettelyn

alaa, mutta siitä ei ole odotettavissa merkittävää työmäärän lisäystä poliisi- tai syyttäjäviranomaisille taikka tuomioistuimille. Ehdotettu lisäys 34 lukuun saattaa mahdollistamalla pakkokeinojen käytön esitutkinnassa toisaalta ehkäistä pykälässä tarkoitetusta menettelystä ehkä aiheutuvien mahdollisesti huomattavienkin vahinkojen syntymistä. Esityksellä ei ole organisatorisia vaikutuksia eikä siitä aiheudu valtiolle kustannuksia.

4. Esityksen valmistelu

Esitys, jonka sisältö vastaa rauennutta hallituksen esitystä no 233/1997 vp., on valmisteltu oikeusministeriössä virkatyönä. Rikoslain 34 luvun muutosta koskevan valmistelun yhteydessä on kuultu eri viranomaisia ja yrityksiä edustaneita asiantuntijoita.

5. Voimaantulo

Laki ehdotetaan tulevaksi voimaan mahdollisimman pian sen jälkeen, kun se on hyväksytty ja vahvistettu.

Edellä esitetyn perusteella annetaan Eduskunnan hyväksyttäväksi seuraava lakiehdotus:

Laki

rikoslain muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan 19 päivänä joulukuuta 1889 annetun rikoslain (39/1889) 46 luvun 6 §, 7 §:n 2 ja 3 momentti, 8 §:n 3 momentti ja 12 §, sellaisina kuin ne ovat laissa 769/1990, sekä

lisätään 34 lukuun uusi 9 a § sekä 46 lukuun uusi 6 a § seuraavasti:

34 luku

Yleisvaarallisista rikoksista

9 a §

Vaaran aiheuttaminen tietojenkäsittelylle

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 muualla laissa säädetä ankarampaa tai yhtä ankaraa rangaistusta, *vaaran aiheuttamisesta tietojenkäsittelylle* sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

46 luku

Säännöstelyrikoksista ja salakuljetuksesta

6 §

Laiton tuontitavaraan ryhtyminen

Joka kätkee, hankkii, ottaa huostaansa tai välittää sellaista omaisuutta, johon nähden sitä maahan tuotaessa on tehty 1—5 §:ssä tai 29 luvun 1—3 §:ssä tarkoitettu rikos, taikka muulla tavoin ryhtyy sellaiseen omaisuuteen, vaikka hän tietää, että omaisuus on tällä tavalla maahan tuotu, on tuomittava *laittomasta tuontitavaraan ryhtymisestä* sakkoon tai vankeuteen enintään yhdeksi vuodeksi kuudeksi kuukaudeksi.

6 a §

Lievä laiton tuontitavaraan ryhtyminen

Jos laiton tuontitavaraan ryhtyminen, huomioon ottaen omaisuuden arvo tai muut rikokseen liittyvät seikat, on kokonaisuutena arvostellen vähäinen, rikoksentekijä on tuomittava *lievästä laittomasta tuontitavaraan ryhtymisestä* sakkoon.

7 §

Rajoitussäännös

— — — — — — — — — — — — — — —

Tämän luvun 6 ja 6 a §:ssä tarkoitetusta rikoksesta ei tuomita henkilöä, joka on osallinen tavaraa maahan tuotaessa tehtyyn rikokseen.

Tämän luvun 6 ja 6 a §:ää ei sovelleta rikoksentekijän kanssa yhteistaloudessa asuvaan henkilöön, joka ainoastaan käyttää tai kuluttaa rikoksentekijän yhteistalouden tavanomaisiin tarpeisiin hankkimaa omaisuutta.

8 §

Omaisuuden menettäminen

— — — — — — — — — — — — — — —

Kuljetusväline, jota on käytetty 1—6 a §:ssä tarkoitetun rikoksen tai 6 ja 6 a §:ssä tarkoitetun veropetoksen tekemiseen ja johon on tehty rikosesineen kätkemistä helpottavia tai muulla tavoin rikoksen tekemistä edistäviä rakennemuutoksia, voidaan tuomita valtiolle menetetyksi. Muukin kuljetusväline voidaan tuomita menetetyksi, jos sitä on pääasiallisesti käytetty sellaisen rikoksen tekemiseen.

12 §

Menettelysäännös

Se, jonka puolesta tai suostumuksin 1—6 a §:ssä tarkoitettu rikos on tehty, samoin kuin se, joka on tiennyt sellaisesta rikoksesta ja jolle omaisuus on rikoksen tekemisen jälkeen siirretty, voidaan tuomita tässä luvussa tarkoitettuun menettämisseuraamukseen, vaikka syytettä ei ole häntä tai rikoksentekijää vastaan nostettu tai rikoksentekijää tuomittu rangaistukseen.

Tämä laki tulee voimaan päivänä kuuta .

Helsingissä 7 päivänä toukokuuta 1999

Tasavallan Presidentti

MARTTI AHTISAARI

Oikeusministeri *Johannes Koskinen*

Liite

Laki

rikoslain muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan 19 päivänä joulukuuta 1889 annetun rikoslain (39/1889) 46 luvun 6 §, 7 §:n 2 ja 3 momentti, 8 §:n 3 momentti ja 12 §, sellaisina kuin ne ovat laissa 769/1990, sekä *lisätään* 34 lukuun uusi 9 a § sekä 46 lukuun uusi 6 a § seuraavasti:

Voimassa oleva laki	*Ehdotus*
46 luku	
Säännöstelyrikoksista ja salakuljetuksesta	
6 §	
Laiton tuontitavaraan ryhtyminen	
Joka kätkee, hankkii, ottaa huostaansa tai välittää sellaista omaisuutta, johon nähden sitä maahan tuotaessa on tehty 1—5 §:ssä tai 29 luvun 1—3 §:ssä tarkoitettu rikos, taikka muulla tavoin ryhtyy sellaiseen omaisuuteen, vaikka hän tietää, että omaisuus on tällä tavalla maahan tuotu, on tuomittava *laittomasta tuontitavaraan ryhtymisestä* sakkoon tai vankeuteen enintään kuudeksi kuukaudeksi.	Joka kätkee, hankkii, ottaa huostaansa tai välittää sellaista omaisuutta, johon nähden sitä maahan tuotaessa on tehty 1—5 §:ssä tai 29 luvun 1—3 §:ssä tarkoitettu rikos, taikka muulla tavoin ryhtyy sellaiseen omaisuuteen, vaikka hän tietää, että omaisuus on tällä tavalla maahan tuotu, on tuomittava *laittomasta tuontitavaraan ryhtymisestä* sakkoon tai vankeuteen enintään *yhdeksi vuodeksi* kuudeksi kuukaudeksi.
	6 a §
	Lievä laiton tuontitavaraan ryhtyminen
(uusi)	*Jos laiton tuontitavaraan ryhtyminen, huomioon ottaen omaisuuden arvo tai muut rikokseen liittyvät seikat, on kokonaisuutena arvostellen vähäinen, rikoksentekijä on tuomittava lievästä laittomasta tuontitavaraan ryhtymisestä sakkoon.*
7 §	
Rajoitussäännös	
Laittomasta tuontitavaraan ryhtymisestä ei tuomita henkilöä, joka on osallinen tavaraa maahan tuotaessa tehtyyn rikokseen.	*Tämän luvun 6 ja 6 a §:ssä tarkoitetusta rikoksesta* ei tuomita henkilöä, joka on osallinen tavaraa maahan tuotaessa tehtyyn rikokseen.
Tämän luvun 6 §:ää ei sovelleta rikoksentekijän kanssa yhteistaloudessa asuvaan hen-	Tämän luvun 6 *ja 6 a* §:ää ei sovelleta rikoksentekijän kanssa yhteistaloudessa asu-

Voimassa oleva laki	*Ehdotus*
kilöön, joka ainoastaan käyttää tai kuluttaa rikoksentekijän yhteistalouden tavanomaisiin tarpeisiin hankkimaa omaisuutta.	vaan henkilöön, joka ainoastaan käyttää tai kuluttaa rikoksentekijän yhteistalouden tavanomaisiin tarpeisiin hankkimaa omaisuutta.
8 §	
Omaisuuden menettäminen	
Kuljetusväline, jota on käytetty 1—6 §:ssä tarkoitetun rikoksen tai 6 §:ssä tarkoitetun veropetoksen tekemiseen ja johon on tehty rikosesineen kätkemistä helpottavia tai muulla tavoin rikoksen tekemistä edistäviä rakennemuutoksia, voidaan tuomita valtiolle menetetyksi. Muukin kuljetusväline voidaan tuomita menetetyksi, jos sitä on pääasiallisesti käytetty sellaisen rikoksen tekemiseen.	Kuljetusväline, jota on käytetty 1—6 *a* §:ssä tarkoitetun rikoksen tai 6 *ja 6 a* §:ssä tarkoitetun veropetoksen tekemiseen ja johon on tehty rikosesineen kätkemistä helpottavia tai muulla tavoin rikoksen tekemistä edistäviä rakennemuutoksia, voidaan tuomita valtiolle menetetyksi. Muukin kuljetusväline voidaan tuomita menetetyksi, jos sitä on pääasiallisesti käytetty sellaisen rikoksen tekemiseen.
12 §	
Menettelysäännös	
Se, jonka puolesta tai suostumuksin 1—6 §:ssä tarkoitettu rikos on tehty, samoin kuin se, joka on tiennyt sellaisesta rikoksesta ja jolle omaisuus on rikoksen tekemisen jälkeen siirretty, voidaan tuomita tässä luvussa tarkoitettuun menettämisseuraamukseen, vaikka syytettä ei ole häntä tai rikoksentekijää vastaan nostettu tai rikoksentekijää tuomittu rangaistukseen.	Se, jonka puolesta tai suostumuksin 1—6 *a* §:ssä tarkoitettu rikos on tehty, samoin kuin se, joka on tiennyt sellaisesta rikoksesta ja jolle omaisuus on rikoksen tekemisen jälkeen siirretty, voidaan tuomita tässä luvussa tarkoitettuun menettämisseuraamukseen, vaikka syytettä ei ole häntä tai rikoksentekijää vastaan nostettu tai rikoksentekijää tuomittu rangaistukseen.
	Tämä laki tulee voimaan päivänä kuuta .