Luottamus. Tietoturva. Sähköiset palvelut.

LUOTI-julkaisuja 4/2006

Tietoturvallisuuslainsäädäntö

Kansainvälinen vertailututkimus

Luottamus ja tietoturva sähköisissä palveluissa – kehittämisohjelma

Tietoturvallisuuslainsäädäntö
Kansainvälinen vertailututkimus

ISBN 952-201-780-9
LUOTI-julkaisuja 4/2006
Helsinki 2006

Julkaisija

KUVAILULEHTI

Julkaisun päivämäärä

28.08.2006

Tekijät	Julkaisun laji
Lauri Railas, Asianajotoimisto Krogerus Oy	Raportti
	Toimeksiantaja: Liikenne- ja viestintäministeriö

Julkaisun nimi

Tietoturvallisuuslainsäädäntö. Kansainvälinen vertailututkimus.

Tiivistelmä

Selvitys on tehty liikenne- ja viestintäministeriön toimeksiannosta kuuluen osana ministeriön LUOTI-ohjelmaan, ja siinä arvioidaan ja kootaan yhteen tietoturvallisuuden kannalta merkittävimmät säännökset ja velvoittavat määräykset olennaisine sisältöineen. LUOTI-ohjelma on osa kansallista tietoturva-strategiaa. Selvitys on kohdennettu Suomeen, Ruotsiin, Norjaan, Tanskaan, Saksaan, Venäjään ja Viroon. Selvitys on tehty erityisesti yritysten tarpeita silmällä pitäen.

Selvityksen kohteena ovat erityisesti henkilötietojen ja viestintätietojen sääntely, sähköiseen allekirjoitukseen ja tunnistamiseen liittyvät säännökset, biometriikka ja kameravalvonta, sähköisten palvelujen tuottamiseen liittyvät säännökset, tietoturvallisuuden alan hallinnointiin liittyvät säännökset sekä muu olennaisesti sähköisen viestinnän ja tietoturvallisuuden alan keskeinen sääntely. Tietoturvallisuutta koskeva velvoittava lailla sääntely liittyy yleensä itse tietoa, kuten henkilötietojen suojaa tai yleisten asiakirjojen julkisuutta, koskevaan sääntelyyn. Yritysten osalta on olennaista yritysalaisuuksien suojaaminen, joka on osin lakisääteistä, mutta tapahtuu osin sopimusjärjestelyin ja käytännön toimenpitein. Yrityksen ja viranomaisten toiminnan helpottamiseksi tietoturvallisuuden edistämisessä ja toiminnan arvioimisessa on kehitetty tietoturvastandardeja, joita selvityksessä myös käsitellään.

Selvityksen ensimmäisissä jaksoissa tarkastellaan tietoturvalainsäädäntöön liittyvää kansainvälistä yhteistyötä ja EU-lainsäädäntöä. Kansainvälistä yhteistyötä käsittelevien jaksojen jälkeen luodaan katsaus selvityksen kohteena olevien maiden kansalliseen lainsäädäntöön niin, että keskitytään kunkin maan lainsäädännön erityispiirteisiin kansainvälisen sääntelyjärjestelmän suomissa puitteissa.

Yleisesti voidaan todeta, että missään tutkittavana olevassa maassa ei tietoturvaa koskevaa lainsäädäntöä ole kodifioitu. Toisaalta tietoturvan merkitys tiedostetaan kaikissa selvityksen kohteena olevissa maissa, usein osana kansallista tietoyhteiskuntastrategiaa.

Avainsanat (asiasanat)

Tietoturva, sähköiset palvelut, palvelunkehitys, tietoturvauhkat, lainsäädäntö

Muut tiedot

Selvityksessä valittujen painopisteiden valintaan on osallistunut LUOTI-hankkeen lainsäädäntöryhmä. Selvityksen valmistelun aikana on seurattu tiiviisti mm. LUOTI-ohjelman kevään 2006 pilottiprojekteissa esiin tulleita oikeudellisia kysymyksiä. Yhteyshenkilö Tuire Saaripuu.

Sarjan nimi ja numero	ISBN
LUOTI-julkaisuja 4/2006	952-201-780-9

Kokonaissivumäärä	Kieli	Hinta	Luottamuksellisuus
	suomi		julkinen

Jakaja	Kustantaja
Liikenne- ja viestintäministeriö	Liikenne- ja viestintäministeriö

Utgivare

PRESENTATIONSBLAD

Utgivningsdatum

28.08.2006

Författare	Typ av publikation
Lauri Railas, Advokatbyrå Krogerus Oy	Rapport
	Uppdragsgivare: Kommunikationsministeriet

Publikation

Informationsskyddslagstiftning. En internationell, komparativ undersökning.

Referat

Undersökningen gjordes på uppdrag av kommunikationsministeriet som en del av ministeriets LUOTI-program. I undersökningen bedöms och sammanställs de viktigaste bestämmelserna och bindande föreskrifterna ur informationsskyddsperspektiv och det väsentligaste innehållet i dem. LUOTI-programmet ingår i den nationella informationsskyddstrategin. Undersökningen har koncentrerats till Finland, Sverige, Norge, Danmark, Tyskland, Ryssland och Estland. Utredningen utfördes särskilt med tanke på företagens behov.

Undersökningen var speciellt inriktad på regleringen av personuppgifter och kommunikationsuppgifter, bestämmelser om elektronisk underskrift och identifikation, biometri och kameraövervakning, bestämmelser om produktion av elektroniska tjänster, stadganden om administration av informationsskyddsbranschen samt övrig väsentlig och central reglering av elektronisk kommunikation och informationsskyddsbranschen. Den bindande regleringen av informationsskyddet i lag anknyter ofta till specifik information, såsom reglering om skydd av personuppgifter eller publicering av allmänna dokument. För företagens del är det väsentliga att företagssekretessen bevaras, något som är lagstadgat, men som delvis sköts genom olika avtal och praktiska åtgärder. För att underlätta företagets och myndigheternas verksamhet har man utvecklat informationsskyddsstandarder för främjande och bedömning av verksamheten. Dessa behandlas också i utredningen.

De första avsnitten i utredningen granskar det internationella samarbetet och EU-lagstiftningen i anknytning till informationsskyddslagstiftning. Efter avsnitten om internationellt samarbete följer en översikt av den nationella lagstiftningen i de länder som ingår i utredningen. Där koncentrerar man sig på specialdragen i respektive lands lagstiftning inom de ramar som det internationella regelverket har ställt upp.

Allmänt taget kan man konstatera att lagstiftningen om informationsskydd inte har kodifierats i något av de undersökta länderna. Å andra sidan är man i alla de länder som undersökningen omfattade medveten om vikten av ett informationsskydd, ofta som ett led i den nationella informationssamhällsstrategin.

Nyckelord

Informationsskydd, elektroniska tjänster, tjänsteutveckling, hot mot informationsskydd, lagstiftning

Övriga uppgifter

LUOTI-projektets lagstiftningsgrupp deltog i valet av tyngdpunktsområden för utredningen. Under beredningen av undersökningen har man intensivt följt med bl.a. de juridiska frågor som dök upp under LUOTI-programmets pilotprojekt våren 2006. Kontaktperson Tuire Saaripuu.

Seriens namn och nummer	ISBN		
LUOTI publikationer 4/2006	952-201-780-9		
Sidoantal	Sråk: finska	Pris	Sekretessgrad: offentlig
Distribution: Kommunikationsministeriet		Förlag: Kommunikationsministeriet	

The publisher

LUOTI

DESCRIPTION

Date of publication

28 August, 2006

Authors	Type of publication
Lauri Railas, Krogerus Attorneys Ltd	Report
	Assigned by Ministry of Transport and Communications

Name of the publication

Information security legislation. International comparative study.

Abstract

This report was prepared on assignment from the Ministry of Transport and Communications as part of the Ministry's LUOTI programme. It is an evaluation and compilation of the essential legislation and imperative regulations regarding information security, with a summary of their content. The LUOTI programme is part of the National Information Security Strategy. The report covers Finland, Sweden, Norway, Denmark, Germany, Russia and Estonia, and has been prepared particularly with the needs of business in mind.

The report focuses specifically on provisions regarding personal data and telecommunications data; provisions, biometrics and camera surveillance related to digital signatures and identification; provisions regarding e-services; provisions regarding information security administration and other essential provisions regarding electronic communications and information security. Imperative legislation on information security usually concerns the information itself, as in the protection of personal data or the publicity of official documents. For businesses, protecting commercial secrets is an essential point; this is partly covered by legislation but partly managed through contractual arrangements and practical measures. In order to make things easier for businesses and the authorities in promoting information security and in assessing their operations, data security standards have been developed. These are also discussed in the report.

The first sections of the report focus on international cooperation regarding legislation on data protection and EU legislation. This is followed by a survey of the national legislation of the countries included in the report, focusing on the special features of each within the framework of the international regulatory system.

In general, it may be noted that data protection legislation has not been codified in any of the countries studied. On the other hand, all of these countries do acknowledge the importance of data protection; this acknowledgement is usually incorporated in a national information society strategy.

Keywords

Data protection, e-services, service development, data protection threats, legislation

Miscellaneous

The legislation working group of the LUOTI project contributed to the selection of focus areas in the report. Legal issues that have emerged in the LUOTI pilot projects during spring 2006 have been monitored closely. The contact person is Tuire Saaripuu.

Serial name and number		ISBN	
LUOTI publications 4/2006		952-201-780-9	
Pages, total	Language Finnish	Price	Confidence status Public
Distributed by Ministry of Transport and Communications		Published by Ministry of Transport and Communications	

Esipuhe

Liikenne- ja viestintäministeriö on selvittänyt Luottamus ja tietoturva sähköisissä palveluissa (LUOTI) -ohjelmaan liittyen eräiden eurooppalaisten valtioiden tietoturvaan liittyvää lainsäädäntöä. Selvitys on teetetty erityisesti yritysten tarpeita silmällä pitäen. Selvityksen tarkoituksena on ollut luoda yrityksille edellytyksiä toimia nopeasti kansainvälistyvällä toimialalla tuottamalla asiantuntemusta ja käytännön-läheistä materiaalia niiden käyttöön.

Selvityksessä arvioidaan ja kootaan yhteen tietoturvallisuuden kannalta merkittävimmät säännökset ja velvoittavat määräykset olennaisine sisältöineen. Selvitys on kohdennettu Suomeen, Ruotsiin, Norjaan, Tanskaan, Saksaan, Venäjään ja Viroon.

Tietoturvan merkitys on nostettu kaikissa selvityksen kohteena olevissa maissa usein osaksi kansallista tietoyhteiskuntastrategiaa. Missään tutkittavana olevassa maassa ei tietoturvaa koskevaa lainsäädäntöä ole kodifioitu omaksi säädöksekseen.

Kaikki selvityksessä esitetyt johtopäätökset ovat tekijän omia, eivätkä edusta liikenne- ja viestintäministeriön näkemystä tai virallista kantaa.

Tutkimuksen tekijä on asianajaja, oikeustieteen tohtori Lauri Railas Asianajotoimisto Krogerus Oy:stä. Tutkimuksen kohteen ja painopisteiden valintaan ovat vaikuttaneet LUOTI-ohjelman lainsäädäntöryhmän jäsenet. Haluan kiittää tutkimuksen tekijää, lainsäädäntöryhmän jäseniä sekä muita LUOTI-hankkeessa mukana olleita hyvin tehdystä työstä ja arvokkaista huomioista.

Helsingissä elokuussa 2006

Tuire Saaripuu
Ylitarkastaja

Tiivistelmä

Selvityksessä esitellään tietoturvallisuuden kannalta merkittävimmät säännökset ja velvoittavat määräykset olennaisine sisältöineen Suomessa, Ruotsissa, Norjassa, Tanskassa, Saksassa, Venäjällä ja Virossa. Selvitys on lähtökohtaisesti tehty yritysten tarpeita silmällä pitäen.

Selvityksen kohteena ovat erityisesti henkilötietojen ja viestintätietojen sääntely, sähköiseen allekirjoitukseen ja tunnistamiseen liittyvät säännökset, biometriikka ja kameravalvonta, sähköisten palvelujen tuottamiseen liittyvät säännökset, tietoturvallisuuden alan hallinnointiin liittyvät säännökset sekä muu olennaisesti sähköisen viestinnän ja tietoturvallisuuden alan keskeinen sääntely.

Tietoturvallisuutta koskeva sääntely on näin ymmärretty ja käsitelty laajasti. Tietoturvallisuus on tärkeä yhteiskunnallinen tavoite. Eri maissa on laadittu ohjelmia ja strategioita tietoturvallisuuden edistämiseksi. Pyrkimyksenä on lisätä yleistä luottamusta sähköisiin palveluihin, joiden käytön yleistymisen katsotaan lisäävän tehokkuutta ja taloudellista kehitystä.

Tietoturvallisuus on osa yhteiskunnan infrastruktuurin sekä jokaisen organisaation ja kotitalouden turvallisuutta, mutta se on silti tavallaan vain väline muiden tavoitteiden, kuten yksityiselämän tai yrityssalaisuuksien suojaamisen tai toisaalta avoimen julkishallinnon luotettavuuden, turvaamiseksi. Tietoturvallisuussäännösten välineellisyys näkyykin siitä, ettei tietoturvasäännöksiä ole yleensä koottu yhtenäisiksi säännöstöiksi vaan säännökset löytyvät pitkälle juuri niistä laeista, jotka määrittävät itse tiedon aseman. Säännökset painottavat niitä kysymyksiä, jotka ovat säännösten tarkoituksen kannalta olennaisia.

Esimerkiksi henkilötietojen suojaa koskevat lait asettavat henkilötietojen käsittelijälle velvoitteen huolehtia henkilötietojen tietoturvallisuudesta. Sähköiseen hallintoon liittyvät säännökset puolestaan painottavat hallinnon avoimuuden ja säilytettävän tiedon luotettavuuden turvaamiseksi tiedon eheyttä koskevia vaatimuksia.

Yritysten osalta on olennaista yritysalaisuuksien suojaaminen, jota tukevat mm. rikoslain säännökset, mutta tavoite toteutetaan paljolti sopimusjärjestelyin ja organisatorisin toimenpitein.

Varsinainen tietoturvallisuutta koskeva sääntely tapahtuu yleislausekkein, joita voivat täydentää esimerkiksi lakien esitöissä tai valvontaviranomaisten määräyksin annetut täsmennykset. Kun tietotekniikka kehittyy koko ajan, on olennaista, että sääntely on teknologianeutraalia. Osa sääntelystä on ohjeistuksen tasoista. Yrityksen ja viranomaisten toiminnan helpottamiseksi tietoturvallisuuden edistämisessä ja toiminnan arvioimisessa on kehitetty tietoturvastandardeja, joita

tässä selvityksessä myös käsitellään. Standardien velvoittavuus voi syntyä myös sopimusjärjestelyn tai itsesääntelyn kautta.

Tietoverkkoihin kohdistuvat tietoturvaongelmat ovat luonteeltaan kansainvälisiä, minkä vuoksi niitä on pyritty ratkaisemaan kansainvälisin sopimuksin. Selvityksen kohteena olevista maista kuusi kuuluu Euroopan unioniin ja kaikki kuuluvat Euroopan neuvostoon. Sen vuoksi selvityksen ensimmäisissä jaksoissa tarkastellaan lähinnä tietosuojaan ja sähköiseen liiketoimintaan liittyviä kansainvälisiä sopimuksia ja EU-lainsäädäntöä, jotka enenevässä määrin muodostavat pohjan kansallisille sääntelytoimille.

Kansainvälistä yhteistyötä käsittelevien jaksojen jälkeen luodaan katsaus selvityksen kohteena olevien maiden kansalliseen lainsäädäntöön niin, että keskitytään kunkin maan lainsäädännön erityispiirteisiin kansainvälisen sääntelyjärjestelmän suomissa puitteissa.

Aluksi tarkastellaan kunkin maan perustuslainsäännöksiä, joihin yksityisyyden suojaa koskevat säännöt ovat kirjattuina. Sen jälkeen tarkastellaan tietoturvan sääntelyyn ja kehittämiseen liittyviä toimia kussakin maassa. Missään tutkittavana olevassa maassa ei tietoturvaa koskevaa lainsäädäntöä ole koottu yksiin kansiin. Toisaalta tietoturvan merkitys tiedostetaan kaikissa näissä maissa, usein osana kansallista informaatioyhteiskuntastrategiaa.

Viimeisiä vuosia ovat leimanneet kansainvälisesti ja kansallisesti taistelu terrorismia ja järjestäytynyttä rikollisuutta vastaan. Tämä näkyy myös tietoturvallisuuden merkityksen korostumisessa entisestään. Pakkokeinoja koskevat säännökset ovat tyypillisesti kansallisessa toimivallassa olevia säännöksiä, joita on paikoin käyty läpi viranomaistoiminnan erityispiirteitä koskevissa kolmansissa jaksoissa.

Kunkin katsauksen neljäs jakso käsittelee julkisen ja yksityisen organisaation hallussa olevaa tietoa koskevaa lainsäädäntöä. Hallinnon avoimuus ei välttämättä ole itsestäänselvyys, sillä esimerkiksi Saksassa tätä koskeva lainsäädäntö on varsin tuoretta. Yrityssalaisuuksien suoja puolestaan on osa teollisoikeuksia koskevaa kansainvälistä sopimusjärjestelmää.

Kansallisten katsausten viidennet jaksot käsittelevät kansallisia tietosuoja-säännöksiä, viranomaisia ja näiden keskeisiä kannanottoja. Tietosuojaa koskevia erityissäännöksiä voi olla sadoittain eri puolilla aineellista lainsäädäntöä. Selvityksessä käydään läpi vain yleissäännökset.

Kuudennet jaksot käsittelevät sähköisiä palveluja koskevia säännöksiä, minkä jälkeen seuraavat jaksot käsittelevät sähköisiä allekirjoituksia ja tunnistamista. Sähköinen allekirjoitus on säännelty yksityiskohtaisesti direktiivillä, sen sijaan sähköinen etätunnistaminen on käytännössä sääntelemättä. Henkilön tunnistaminen asioinnin yhteydessä vähentää yksityisyyden suojaa, minkä vuoksi on kansallisessa laissa saatettu edellyttää mahdollisuutta asioida anonyymisti. Pankkisäännökset

edellyttävät kuitenkin asiakkaan tunnistamista. Kahdeksansissa jaksoissa on nostettu esille eräitä ajankohtaisia tietoturvan ja sähköisten palvelujen kysymyksiä. Painopiste on eräissä aineellisissa EU-säännöksissä. Lopuksi on käsitelty tietoturvallisuuden yleisiin palveluihin, kuten hälytyspalveluihin, standardointiin ja sertifiointiin liittyviä palveluja eri maissa.

Kansalliset jaksot on tarkoitettu kuvaamaan kunkin maan säännöksiä vain pääpiirteissään, joten tarkempi tutustuminen on tarpeen täsmällisemmän kuvan saamiseksi.

Lyhenteet ja terminologia

BITS	Basnivå för Informationssäkerheten (Ruotsi)
BS	British Standard
BSI	Bundesamt für Sicherheit in der Informationsteknik, Saksan tietoturvavirasto
B2B	Business-to-Business, yritysten välinen
B2C	Business-to-Consumer, yrityksen ja kuluttajan välinen
CC	Common Criteria
CERT	Computer Emergency Response Team
CMA	Communications Management Association
CSIRT	Computer System Information Response Team
DNS	Domain Name System
DoS	Denial of service attack
DTI	Department of Trade and Industry, Englanti
EDI	Electronic Data Interchange, organisaatioiden välinen sähköinen tiedonsiirto (OVT)
EGG	Elektronischer Geschäftsverkehr-Gesetz, Saksa 20001
EkomL	Lag (2000/389) om elektronisk kommunikation, Ruotsi
Ekomloven	Lov (83/2003) om elektronisk kommunikasjon, Norja
EMP	Elektromagneettinen pulssi
ENISA	European Network and Information Security Agency
ETA	Euroopan talousalue
ETY	Euroopan talousyhteisö
EU	Euroopan unioni
EURID	European Registry for Internet Domains
EY	Euroopan yhteisö
EYVL	Euroopan yhteisön virallinen lehti
FATF	Financial Action Task Force
FSB	Venäjän sotilaallinen turvallisuuspalvelu
FSM	Federal Service of Finance Monitoring, Venäjä
FZ	Venäjän Federaation lakikokoelma
GPS	global positioning system
HPM	mikroaaltoase
IAASB	International Auditing and Assurance Standards Board
IFAC	International Federation of Accountants
ISMS	Information Security Management Systems
ISO	International Standardisation Organisation

IT	informaatioteknologia
ICT	informaatio- ja kommunikaatioteknologia
IuKDG	Informations- und Kommunikationsdienste-Gesetz, Saksa
KBM	Krisberedskapsmyndigheten, Ruotsi
KKO	Korkein oikeus
KP-sopimus	YK:n kansalais- ja poliittisia oikeuksia koskeva yleissopimus
LUOTI	Luottamus ja tietoturva sähköisissä palveluissa, liikenne- ja viestintäministeriön ohjelma
MdStV	Mediendienste-Staatsvertrag, Saksa
OECD	Organisation of Economic Cooperation and Development
PeVL	Eduskunnan perustuslakivaliokunnan lausunto
PKI	Public Key Infrastructure, julkisen avaimen järjestelmä
PuL	Personuppgiftslagen 1998:204, Ruotsi
RFID	Radio Frequency Identifier
RL	Rikoslaki 39/1889
RT	Riigi Tietaja, Viron virallinen lehti
SEPA	Single European Payment Area
SigG	Signaturgesetz, laki sähköisistä allekirjoituksista, Saksa 2001
SigV	Signaturverordnung, asetus sähköisistä allekirjoituksista, Saksa 2001
SopMenL	Laki sopimattomasta menettelystä elinkeinotoiminnassa 1061/1978
SopS	Sopimussarja
StPO	Strafprozessordnung, Saksa
TIEKE	Tietoyhteiskunnan kehittämiskeskus ry
TMG	Telemediengesetz, Saksa
TRIPS	GATT Trade Related Intellectual Property Rights -sopimus
TSL	Työsopimuslaki 55/2001
UBL	Universal Business Language
UWB	Gesetz gegen den unlauteren Wettbewerb, Saksa (2004)
VAHTI	Valtionhallinnon tietoturvallisuuden johtoryhmä
VejL	veiledning, ohjeisto
WTO	World Trade Organisation, Maailman kauppajärjestö

Sisällysluettelo

1. Johdanto

1.1 Selvityksen tavoitteista

Tämä selvitys on tehty liikenne- ja viestintäministeriön toimeksiannosta ja kuuluu osana ministeriön LUOTI-ohjelmaan, ja siinä arvioidaan ja kootaan yhteen tietoturvallisuuden kannalta merkittävimmät säännökset ja velvoittavat määräykset olennaisine sisältöineen. Selvitys on kohdennettu Suomeen, Ruotsiin, Norjaan, Tanskaan, Saksaan, Venäjään ja Viroon.

Selvityksen kohteena ovat mm. henkilötietojen ja viestintätietojen sääntely **(data-turvallisuus)**, sähköiseen allekirjoitukseen ja tunnistamiseen liittyvät säännökset **(transaktio- ja dataturvallisuus)**, biometriikka ja kameravalvonta **(yksityisyyden suoja, yleinen turvallisuus, transaktioturvallisuus)**, sähköisten palvelujen tuottamiseen liittyvät säännökset **(dataturvallisuus)**, tietoturvallisuuden alan hallinnointiin liittyvät säännökset sekä muu olennaisesti sähköisen viestinnän ja tietoturvallisuuden alan keskeinen sääntely.

Selvitys tehdään yritysten tarpeisiin, minkä perusteella käsiteltävät aiheet on rajattu.

Julkinen ja yksityinen sektori nivoutuvat kuitenkin toisiinsa oleellisesti tietoturvan osalta. Julkinen valta on monissa tutkittavissa maissa panostanut tietoturvan kehittämiseen erillisin ohjelmin ja toimenpitein. On luotu kansallisia tietoturvaohjelmia, usein osana yleistä tietoyhteiskuntastrategiaa. Näissä korostetaan säännönmukaisesti julkisen ja yksityisen sektorin yhteistyötä tietoturva-asioissa. Euroopan tasolla on puolestaan äskettäisessä komission tiedonannossa[1] tuotu esille sama asia. Sähköisen kaupankäynnin kehittämisen nähdään lisäävän jäsenvaltioiden välistä kauppaa niin tavaroiden, palvelujen kuin pääomankin osalta. Taustalla on myös panostus talouden dynaamisuuden lisäämiseksi. Sähköisin asiointi- ja kaupankäyntimenetelmin voidaan luoda tehokkuutta ja kustannussäästöjä. Tämä edellyttää kuitenkin luottamusta sähköisten menetelmien ja asioinnin turvallisuuteen ja sähköisesti välitettyjen tietojen säilymiseen vain niihin oikeutettujen hallussa.

[1] Komission tiedonanto neuvostolle, Euroopan Parlamentille, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle, Turvallisen tietoyhteiskunnan strategia – ”Lisää vuoropuhelua, yhteistyötä ja vaikutusmahdollisuuksia”; KOM (2006) 251 lopullinen, 31.5.2006.

1.2 Mitä tietoturva on?

Tietoturvalle on annettu säännöksissä ja standardeissa määritelmiä, jotka muistuttavat pitkälle toisiaan. Tietoturvallisuus kuvataan normaalisti yleisin määritelmin. Sähköisen viestinnän tietosuojalaki sisältää määritelmän, jota ei ole lain taustalla olevassa direktiivissä. Lain määritelmän mukaan tietoturvalla tarkoitetaan hallinnollisia ja teknisiä toimia, joilla varmistetaan se, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla, ettei tietoja voida muuttaa muiden kuin siihen oikeutettujen toimesta ja että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä. Suomen julkishallinnossa tietoturva on määritelty VAHTI:n eli valtionhallinnon tietoturvallisuuden johtoryhmän ohjeistossa.[2]

Tietoturva on siis hallinnollisia ja teknisiä toimia, joilla tiedon luottamuksellisuus säilytetään tietojärjestelmissä.[3] Tämä tarkoittaa sitä, että laitteistot, ohjelmistot, tietoliikenneyhteydet ja tiedot ovat suojatut fyysisesti, teknisesti ja toiminnallisesti.

Tietoturvallisuus rakentuu tiedon kolmen ominaisuuden eli luottamuksellisuuden, eheyden ja käytettävyyden turvaamisella. Tiedon eheys sisältää aina tietolähteen todennuksen. Tietoturvaan liittyy lisäksi kiistämättömyyden ja pääsynvalvonnan tekninen toteuttaminen.

---

[2] VAHTI-ohjeisto jakaa tietoturvallisuuden seuraaviin kahdeksaan osa-alueeseen.

- Hallinnollinen turvallisuus, johon sisältyvät johdon hyväksymät periaatteet, käytettävissä olevat resurssit, vastuunjako ja riskien arviointi.
- Henkilöstöturvallisuus, johon sisältyy henkilöstöön liittyvien luotettavuusriskien minimointi esimerkiksi toimenkuvien, käyttöoikeuksien määrittelyn, koulutuksen ja valvonnan sekä turvallisuusselvitysten avulla.
- Fyysinen turvallisuus, jolla tarkoitetaan laitteisto-, käyttö- ja arkistotilojen suojaamista fyysisiltä tapaturmilta tai vahingoittamisyrityksiltä.
- Tietoliikenneturvallisuus, jolla tarkoitetaan tietoverkoissa liikkuvien tietojen luottamuksellisuuden, eheyden ja käytettävyyden varmistamiseen liittyviä toimenpiteitä.
- Laitteistoturvallisuus, jolla tarkoitetaan tietojenkäsittely- ja tietoliikennelaitteiden turvallisuus-ominaisuuksia mukaan lukien yhtenäinen laitteistopolitiikka ja huoltosopimukset.
- Ohjelmistoturvallisuus, johon sisältyvät käyttöjärjestelmien, tietoliikenneohjelmistojen ja sovellus-ohjelmistojen turvallisuusominaisuudet.
- Tietoaineistoturvallisuus, jolla tarkoitetaan tietojen ja tietojärjestelmien tunnistamista ja luokittelua sekä tietovälineiden hallintaa ja säilytystä koko niiden elinkaaren ajan.
- Käyttöturvallisuus, jolla tarkoitetaan niitä menettelytapoja, joilla päivittäisessä toiminnassa säilytetään hyvä tietoturvallisuuden taso. Käyttöturvallisuus liittyy henkilöstön työkäytäntöjä koskeviin periaatteisiin, tietojenkäsittelyn käyttöympäristöön ja turvallisuuteen liittyvien tapahtumien valvontaan.

[3] Euroopan komissio käytti ilmaisua "tietojärjestelmä" tiedonannossaan vuonna 2001 laajimmassa merkityksessään todeten, että sähköiset tiedonsiirtoverkot ja niiden yhdistämät järjestelmät lähentyvät toisiaan jatkuvasti. Tietojärjestelmiin katsotaan tällöin kuuluviksi muun muassa erillismikrot, kämmentieto-koneet, matkapuhelimet, intranet- ja extranet-verkot ja tietenkin Internet-verkot, -palvelimet ja muu infrastruktuuri.

Luottamuksellisuudella varmistetaan, että tiedot ovat vain niillä, joille tiedot on tarkoitettu. Luottamuksellisuus suojaa yksityisyyttä ja tiedon omistusoikeutta.

Tiedon eheys tarkoittaa, ettei tieto ole muuttunut siirrettäessä eikä säilytettäessä. Tiedon eheyden varmistamiseen liittyy aina lähettäjän ja tiedon alkuperän todennus. Eheys ja todennus yhdessä varmistavat, että lähetty tieto on vastaanottajan saavuttaessaan juuri siinä muodossa, missä se lähetettiin.

Todennuksella varmistetaan, että osapuolet ovat niitä, joita sanovat olevansa. Henkilöiden osalta puhutaan usein tunnistamisesta. Esimerkiksi sähköisessä kaupankäynnissä ja viranomaispalveluissa sekä henkilöiden välisessä viestinnässä on usein tärkeää tietää varmasti, kuka toinen osapuoli on ja mistä tieto on peräisin. Tarvitaan osapuolen ja tietolähteen eli tiedon alkuperän todennusta.

Tiedon luottamuksellisuuden ja eheyden taso ja tarve ovat toisistaan riippumattomia. Tieto voi olla kaikille avointa ja julkista, mutta sen on oltava varmasti oikeaa. Esimerkiksi julkisesti välitetyn viranomaistiedotteen muuttuminen voi aiheuttaa merkittävää vahinkoa. Toisaalta voi olla hyvin luottamuksellista tietoa, jonka ei kuitenkaan välttämättä tarvitse olla aivan virheetöntä.

Kiistämättömyydellä tarkoitetaan, ettei tiedon lähettäjä voi kiistää lähettäneensä tietoa ja olleensa jossakin tapahtumassa osapuolena. Kiistämättömyys edellyttää osapuolen tai tietolähteen todennusta vahvassa muodossa, ja se toteutetaan normaalisti sähköisellä allekirjoituksella. Kiistämättömyys on ehdoton edellytys monien palvelujen ja toimintojen toteuttamiselle tietoverkkojen kautta.

Pääsyn valvonnalla tarkoitetaan, että käyttäjien pääsyä koneessa olevaan tietoon rajoitetaan ja valvotaan. Pääsyn valvonnalla tarkistetaan, onko osapuolella oikeus palvelun ja tiedon käyttöön. Pääsyn valvonnan tavoitteena on osaltaan turvata tiedon luottamuksellisuus ja eheys. Pääsyn valvonta turvaa osaltaan myös saatavuutta ehkäisten järjestelmään kohdistuvia hyökkäyksiä.

Käytettävyydellä tarkoitetaan, että tiedon tulee olla niiden käytettävissä, jotka sitä tarvitsevat ja joille se on tarkoitettu. Tiedon käytettävyys on vaikeimmin toteutettava tietoturvan muoto.

1.3 Tietoturvauhkia

Euroopan komission ehdotuksessa neuvoston tietoverkkorikollisuutta koskevaksi puitepäätökseksi vuodelta 2005 käsitellään erityisesti rikollisuuden aiheuttamia tietoturvauhkia. Ehdotuksessa todetaan, että monet vakavimmista tietojärjestelmiin kohdistuvista hyökkäyksistä on suunnattu sähköisen viestinnän verkko-operaattoreita tai sähköistä kauppaa harjoittavia yrityksiä vastaan.

Myös perinteisemmille toimintamuodoille, kuten tehdasteollisuudelle, palveluille, sairaaloille, muille julkisoikeudellisille yhteisöille ja itse julkishallinnolle voidaan aiheuttaa suurta vahinkoa nykyisessä viestintäympäristössä, kun eri alojen keskinäiset kytkökset lisääntyvät jatkuvasti. Organisaatiot eivät kuitenkaan ole ainoita uhreja, vaan hyökkäyksillä voi olla suoria ja vakavaa vahinkoa aiheuttavia vaikutuksia myös yksityisiin kansalaisiin. Osa hyökkäyksistä aiheuttaa huomattavaa taloudellista vahinkoa niin julkisyhteisöille, yrityksille kuin kansalaisillekin. Tämä saattaa nostaa tietojärjestelmien hintaa, jolloin harvemmilla käyttäjillä on niihin varaa.

Hyökkäysmenetelmiä voidaan kehittää edelleen ja hyökkäysten tavoitteet voivat käydä yhä kunnianhimoisemmiksi. Kasvavaa huolta aiheuttaa pelko siitä, että järjestäytynyt rikollisuus alkaa käyttää viestintäverkkoja omiin tarkoituksiinsa hyökätäkseen tieto-järjestelmiä vastaan. Tietojärjestelmiin murtautumiseen ja sivustojen turmelemiseen erikoistuneet järjestäytyneet hakkeriryhmät toimivat yhä useammin maailman-laajuisesti. Eräät ryhmät yrittävät kiristää rahaa tarjoamalla uhreilleen apua sen jälkeen, kun ovat murtautuneet näiden tietojärjestelmiin. Suurten hakkeriryhmien pidätysten perusteella voidaan arvioida, että tietojärjestelmiin murtautuminen on yhä useammin järjestäytyneen rikollisuuden piiriin kuuluva ilmiö. Järjestäytyneet rikollisryhmät ovat tehneet useita monimutkaisia teollis- ja tekijänoikeuksiin kohdistuneita hyökkäyksiä ja erilaisten pankkipalveluiden välityksellä on yritetty varastaa huomattavia rahasummia.

Yhdysvaltalainen Communications Management Association (CMA) on julkaissut vuosikymmenen alussa tutkimuksen, jonka mukaan joka kolmas Yhdistyneen Kuningaskunnan suuryritys ja julkishallinnon elin on joutunut hakkerihyökkäyksen kohteeksi. Vahingon laatu vaihtelee yritysten pankkitileille tunkeutumisesta tietovarkauksiin.

Huolestuttavia ovat myös murrot sähköistä kaupankäyntiä harjoittavien yritysten tietokantoihin, joihin on tallennettu asiakkaiden luottokortti- ja muut tiedot. Tällaiset hyökkäykset lisäävät maksupetosten todennäköisyyttä ja pakottavat pankit peruuttamaan tuhansia kortteja ja antamaan tilalle uusia. Lisäksi ne aiheuttavat

aineetonta vahinkoa yrityksen maineelle ja horjuttavat kuluttajan luottamusta sähköiseen kaupankäyntiin ja sähköistä kaupankäyntiä harjoittaviin yrityksiin.

Ajankohtainen ongelma on ollut ns. *phishing*-ilmiö, jossa verkkopankkipalveluiden käyttäjiltä pyritään saamaan näiden pankkitunnuksia erehdyttävin viestein.

Yritysnäkökulmasta voidaan todeta, että Tampereen teknillisen yliopiston tuoreen tutkimuksen mukaan valtaosa yritysten tietoturvauhkista tulee yritysten sisältä eli ne liittyvät henkilöstöturvallisuuteen. Liiketoiminnan tietojen turvallisuudesta valtaosa luodaan henkilöstön arkipäivän rutiineja kehittämällä ja vain murto-osa teknisten suojaamiskeinojen avulla.

1.4 Tietoturvan sääntely ja yritysnäkökulma

Tietoturvan merkitys sähköiseen viestintään nojaavan yhteiskunnan perustekijänä on kiistaton. Siksi ajoittain on esitetty ajatuksia kattavan tietoturvallisuuslain säätämisestä.

Hallinnollisten ja teknisten menettelytapojen yksityiskohtainen sääntely laintasoisella säädöksellä dynaamisella tietotekniikan alalla on kuitenkin hankalaa ja epätarkoituksenmukaista. Tietoturvaan liittyvät lainsäännökset ovatkin lähinnä yleisluonteisia velvoitteita, joiden sisältöä kuvataan esitöissä, tai sitten itse tietoa ja sen teknistä ainesosaa, dataa koskevia säännöksiä, joilla määritellään tiedon julkisuus tai luottamuksellisuus. Johtamisjärjestelmien, menettelytapojen ja teknisten ratkaisujen standardointi ja sertifiointi ovat avuksi tietoturvan edistämisessä. Siksi lainsäädäntö ei siihen juuri kajoa. Tietoturvan ylläpitämiseen saatetaan paikka paikoin laissa nimenomaisesti velvoittaa painottaen käyttötarkoituksesta riippuvia seikkoja, kuten tiedon saavutettavuutta ja eheyttä. Toisaalta velvoite voi syntyä epäsuorasti siten, että yrityksellä on lain ja sopimusten perusteella velvollisuus pitää tieto luottamuksellisena. Tuottamuksellinenkin tiedon vuotaminen ulos voi johtaa vahingonkorvausseuraamuksiin.

Tietoturvan kannalta keskeistä lainsäädäntöä onkin itse tietosisältöä koskeva lainsäädäntö, jossa tiedon luottamuksellisuutta, salassapitoa, julkisuutta tai sitten luotettavuutta, eheyttä tai saavutettavuutta säännellään. Joitakin yleistyksiä voidaan tämän suhteen tehdä. Viranomaisen hallussa oleva tieto ja asiakirjat ovat yleensä julkisia. Informaation vapaa leviäminen on osa sananvapautta ja demokraattista yhteiskuntaa ja siksi oikeus vapaaseen tiedonvälitykseen on perusoikeussäännöksissä säännönmukaisesti turvattu. Avoimuus on hyvän hallinnon perusperiaatteita ja siksi viranomaisen hallussa oleva tieto ja asiakirjat ovat useimmissa länsimaisissa yhteiskunnissa julkisia, ellei intressipunnintaan liittyviä perusteita ole pitää nämä salaisina.

Informaation leviämisen vastaintressinä on yksityisyyden suoja perusoikeutena sekä muut intressit pitää tieto salaisena, kuten yleinen turvallisuus.

Tieto on yrityksissä merkittävä voimavara. Yrityssalaisuudet rinnastetaan säännönmukaisesti teollisoikeuksiin, ja esimerkiksi know-how eli taitotieto on lisensioinnin kohteena samalla tavoin kuin patentit ja tavaramerkit. Keksinnöllinen yritystieto on patentoitavissa ja valtaosa patenttijärjestelmistä antaa etuoikeuden sille, joka rekisteröi hakemuksensa ensin. Maailman kauppajärjestön WTO:n teollisoikeuksia koskeva TRIPS-sopimus sääntelee myös yrityssalaisuuksien suojaa. Tiedon esitystapa voi saada tekijänoikeudellista tietokantojen suojaa tai luettelosuojaa tai voi jopa ylittää teoskynnyksen, minkä vuoksi sen levittäminen kohtaa tekijänoikeuslainsäädännössä säädettyjä rajoituksia riippumatta itse tiedon suojasta.[4]

Vapaan tiedonkulun vastapainona on henkilön oikeus yksityisyyteen ja sen kunnioittamiseen. Voidaan sanoa, että yksityishenkilö pääsääntöisesti omaa oikeudet itseään koskevaan tietoon ja sen käyttämiseen. Yksityishenkilön on voitava elää ja kommunikoida luottaen siihen, ettei hänen mielipiteitään ja henkilöään koskeva tieto vastoin hänen tahtoaan joudu ulkopuolisen tietoon. Yksityishenkilöllä on oikeus yksityisyyteen myös työpaikalla. Tärkeä julkinen intressi, kuten rikostutkinta, voi muodostaa poikkeuksen tiedollisesta itsemääräämisoikeudesta. Viranomainen voi kohdistaa yksilöön pakkokeinoja, joiden toteuttaminen edellyttää, koska kyse on perusoikeuksiin kajoamisesta, yleensä laissa säädetyn prosessin, tuomioistuimen määräyksen tai luvan saamista toimenpiteelle. Pakkokeinoilla on liittymä tietoon, sen suojaamiseen tai tietoturvallisuuteen kahdella tavalla. Ensinnäkin laissa määrätyillä perusteilla viranomaisella on oikeus saada tieto muuten yksityisyyden piiriin kuuluvasta tiedosta. Toisaalta viranomaisilla on oikeus ja velvollisuus estää laissa määrätyissä tapauksissa tiedon levittäminen viestinnän keinoin verkossa tai muualla tiedonvälityksessä.

Perusoikeudet eivät ole absoluuttisia, vaan niitä voidaan rajoittaa hyväksyttävistä syistä kuten muiden perusoikeuksien toteutumiseksi. Perusoikeuksien rajoittaminen merkitsee aina intressipunnintaa, ja perusoikeuksiin kajoamisen laajuuden täytyy olla hyväksyttävässä suhteessa saavutettavaan etuun nähden (ns. suhteellisuusperiaate). Tietoliikenteen ja tietoturvallisuuden vaarantumista voidaan nykyaikana pitää riskinä yksilön ja yhteiskunnan laajasti ymmärretyn turvallisuuden kannalta. Eräät tietoturvatoimenpiteet merkitsevät käytännössä rajoituksia sananvapauden käyttämiselle. Näillä toimilla turvataan esimerkiksi tietoverkkojen toimivuus ja turvallisuus ja luodaan näin edellytykset sananvapauden käyttämiselle ja viestinnän luottamuksellisuudelle

[4] Tietoturva ja tekijänoikeuden suoja kohtaavat tavallaan mm. suojauksen purkua koskevissa kysymyksissä.

tietoverkoissa.[5] Perusoikeuksien käyttämiseen ja niiden toteutumisen edistämiseen liittyvät seikat ovat hyväksyttäviä perusteita tietoverkoissa tapahtuvan toiminnan rajoituksille eräissä tapauksissa.

Yritysten kannalta henkilön yksityiselämän kunnioittaminen merkitsee työntekijän yksityisyyden lisäksi myös asiakastietojen keruulle, markkinoinnille, mainonnalle ja asiakkaiden kontrolloinnille asetettuja rajoituksia. Yrityksellä on laissa säädettyjä velvollisuuksia turvata tietoa, sen luottamuksellisuutta, eheyttä tai molempia. Tyypillisinä esimerkkeinä toimivat tietosuojalainsäädäntö sekä pankkisalaisuuden turvaksi säädetty lainsäädäntö.

Tietoa koskevan lainsäädännön laaja kartoittaminen ei ole helposti toteutettavissa. Esimerkiksi tietosuojaa koskevia pykäliä löytyy Suomessa noin 600 laista tai asetuksesta. Tämä monipuolinen lainsäädäntö on lähtökohtaisesti kansallista, mutta yritysten toimintojen kansainvälisyys asettaa erityisvaatimuksia. Esimerkiksi amerikkalainen elintarvikeviranomainen velvoittaa säilyttämään elintarvikkeita koskevat tutkimustiedot koskemattomina kymmenen vuoden ajan. Markkinoille osallistuminen velvoittaa noudattamaan normeja.

Yrityksen omassa intressissä on puolestaan erityisesti sen liikesalaisuuksien säilyminen kovan kilpailun vallitessa. Joissakin maissa voi tiedon luokittelu yritys-salaisuudeksi edellyttää yrityksen omia, lähinnä organisatorisia toimia tiedon suojaamiseksi. Liikesalaisuudet voivat olla peräisin yhteistyöyritykseltä ja liikesalaisuuksien säilyminen voi olla sopimusvelvoite, mutta joissakin maissa myös lainsäädäntöön perustuva velvoite. Sähköisen viestinnän tietosuojadirektiivin johdanto-lauseissa puhutaan oikeushenkilöiden oikeutettujen etujen suojaamisesta. Joissakin maissa, kuten Ruotsissa ja Venäjällä, on säädetty erityislainsäädäntöä yritys-salaisuuksien suojaksi, muualla sääntely tapahtuu puolestaan yleislainsäädännön puitteissa. Tietoturvatoimenpiteillä varmistetaan myös liikesalaisuuksien säilyminen ja torjutaan yritysvakoilua.

Samalla tavoin kuin tietoturvaa ollaan kohottamassa perusoikeudeksi, voidaan myös yrityksissä nähdä tietoturvan ylläpitäminen omien intressien mukaisen toiminnan lisäksi myös yhteiskunnallisena velvollisuutena. Tätä näkemystä voi perustella myös sillä, että yleisen tietoturvan ylläpitäminen edellyttää toimijoiden yhteistyötä.

---

[5] Näin Suomen eduskunnan perustuslakivaliokunta sähköisen viestinnän tietosuojalain 20 §:n osalta (PeVL 9/2004 vp - HE 125/2003 vp).

Eräs tietoturvallisuuden alalaji yritysnäkökulmasta on transaktioturvallisuus, joka on muiden tietoturvan alalajien sovellus. Vaihdannan osapuolten henkilöllisyys on todennettava ja maksujärjestelmien yksityiskohtien kanssa suojattava, paitsi yksityisyyden suojan turvaamiseksi, myös väärinkäytösten, kuten petosten ehkäisemiseksi. Sähköisten maksujärjestelmien ylläpitäminen edellyttää tietoturvallisuustoimenpiteitä. Osapuolten tunnistaminen on kuitenkin tarpeen rahanpesurikollisuuden torjumiseksi. Tietoturvallisuustoimenpiteet voivat kohdistua yksittäistä transaktiota koskevien tietojen suojaamiseen, esimerkkinä julkiseen tarjouskilpailuun osallistuvien tarjousten salassa pitäminen.

Olisi luontevaa ajatella, että kaikkien intressissä olisi maksimiturvallisuus transaktioissa. Vaihdannan edut voivat kuitenkin johtaa turvallisuustason laskemiseen kustannussyistä. Jos esimerkiksi petoksia tapahtuu jollakin alalla tai alueella harvoin, voivat ongelmien aiheuttamat kustannukset alittaa turvallisuustoimenpiteiden aiheuttamat kustannukset.

Elinkeinoelämän ja tietoverkkojen kansainvälisyys sekä transaktioiden toteuttaminen etätoimenpitein kuitenkin lisäävät riskejä. Keskeinen peruste uudelle lainsäädännölle on luottamuksen lisääminen sähköiseen asiointiin.

Elinkeinoelämä on tiedostanut tietoturvallisuuden tärkeyden. Toisaalta elinkeinoelämän järjestöt ovat monesti korostaneet, ettei lainsäädäntöä tulisi tehdä pakottavaksi. Yleistä tietoturvavelvoitetta ei ole kaikille yrityksille lainsäädännössä asetettu kuin tietosuojamääräysten ylläpitämisen osalta. Tietoturvatoimenpiteiden tarpeellisuus voi vaihdella yrityksen toimialan, koon, suojeltavan tiedon laadun ja käyttötarkoituksen sekä käytetyn teknologian ja kustannusten mukaan. Sen vuoksi elinkeinoelämän järjestöt ovat korostaneet sääntelyn joustavuutta ja johdonmukaisuutta. Kun sekä riskit että tekniikat voivat muuttua, olisi tietoturvavelvoitteiden oltava teknologianeutraaleja ja ”geneerisiä”. Mitään standardeja ei sellaisenaan tulisi suosia, vaan tietoturva olisi nähtävä prosessina.

Tietoturvallisuuden ylläpitäminen on myös yhteiskunnan infrastruktuurin turvaamista sitä vastaan suunnattuja hyökkäyksiä vastaan. Terrorismia vastaan käytävä taistelu on monissa maissa näkynyt myös tietoturvallisuuden parissa tehtävässä työssä. On tiedostettu se, kuinka tietoturvallisuus on osa valtakunnan turvallisuutta ja terrorismi muodostaa yhden tietoturvauhan samalla, kun terrorismin rahoitus rinnastetaan rahanpesuun. Toisaalta terrorismin torjumisessa käytettävät keinot merkitsevät rajoituksia yksityisyydelle.

Tietosuojaa on säännelty Euroopan yhteisön toimialaan kuuluvilla alueilla direktiivein. Jäsenvaltioiden erilaisista perusoikeussäännöksistä johtuen tietosuojassa on kuitenkin

eroja. Lisäksi yleisen turvallisuuden, maanpuolustuksen tai valtion turvallisuuden suojelemiseksi tai rikosoikeuden säännösten täytäntöön panemiseksi tehtävät toimet ovat kansallisessa toimivallassa, minkä vuoksi jäsenmaiden välillä vallitsee eroja näiden suhteen.

1.5 Mitä lakia sovelletaan?

Kansainvälisessä ympäristössä nousevat esille myös lainvalintakysymykset ja lain soveltaminen oman valtion rajojen ulkopuolella. Voiko työnantaja käsitellä työntekijöidensä henkilökohtaisia sähköposteja, jos siirtää sähköpostipalvelimen valtioon, jossa työntekijöiden henkilökohtaiset sähköpostit eivät nauti yksityisyyden suojaa?

Kuten seuraavassa jaksossa käy ilmi, tietoturva- ja erityisesti tietosuojakysymyksiä on säännelty runsaasti ylivaltiollisella tasolla. Vaikka yksityisyyden suojan tarpeesta vallitseekin yhteisymmärrys teollistuneissa maissa, voivat käytännön lainsäädäntötoimet vaihdella eri maiden välillä. Esimerkiksi työnantajan oikeus käsitellä työntekijöiden sähköpostiviestien tunnistetietoja voi vaihdella maakohtaisesti. Yritykset, jotka toimivat useassa maassa, ovat siten erilaisten säännösten piirissä eri maissa toimiessaan. On myös mahdollista, että eri maiden normit ovat keskenään ristiriidassa. Myös valvontaviranomaisten toimivaltakysymykset voivat nousta esille.

Lainsäännöksissä on usein määritelty sääntöjä säännösten soveltamisalan suhteen. Valtioilla on oikeus säätää lakeja lainkäyttövaltansa piiriin kuuluvista asioista. Kansainvälisin sopimuksin on luotu sääntöjä lainvalintatilanteisiin. Oikeudenalaa, joka sääntelee yksityisoikeudellisiin kysymyksiin liittyviä lainvalintakysymyksiä, kutsutaan kansainväliseksi yksityisoikeudeksi.

Esimerkiksi työntekijän oikeutta yksityisyyteen työpaikalla koskevat lainsäännökset määräytyvät sopimusvelvoitteisiin sovellettavaa lakia koskevan Rooman yleissopimuksen perusteella. Tämä yleissopimus antaa kuitenkin pakottavalle lainsäädännölle merkitystä riippumatta siitä, mikä laki tulisi yleisesti sovellettavaksi. Sen vuoksi tuomioistuin voi antaa merkitystä ulkomaisille pakottaville oikeussäännöille esimerkiksi tietosuojasäännösten osalta. Rikosoikeudelliset lainsäännökset sisältävät puolestaan rikosoikeuden alueellista sovellettavuutta koskevia sääntöjä.

Yritysten intressissä on luonnollisesti välttää oikeudellisia ongelmia. Sen vuoksi ne voivat valita toimintaperiaatteensa ankarimman soveltuvan lainsäädännön perusteella. Tämä vie niiltä kuitenkin toimimismahdollisuuksia niissä maissa, joissa sääntely on lievempää.

2. Yksityisyyden suojan ylikansallinen sääntely

2.1 Rajanvetoa

Henkilötietolainsäädännön, henkilötietojen käsittelyn sähköisessä viestinnässä, sähköisten palvelujen tuottamisen sekä sähköisen allekirjoituksen osalta, Venäjää lukuun ottamatta, selvityksen kohteena olevien maiden lainsäädäntö perustuu EY-direktiiveihin, jotka eivät kuitenkaan ole täysharmonisoivia, joten niiden täytäntöönpano voi sisältää kansallisia eroja.

On tarkoituksenmukaista toiston välttämiseksi esittää direktiivien pohjalta luotu yhteinen sääntelyjärjestelmä ensin ja tämän jälkeen kansallisia sääntöjä selvitettäessä tuoda esille mahdolliset kansalliset erityispiirteet, joita kyseisen maan lainsäädäntöön on otettu. Osa lainsäädännöstä, mm. viranomaisasiakirjojen julkisuuslainsäädäntö, ei perustu yhteisöoikeuteen.

Koska tietosuoja ja tietoturva liittyvät olennaisesti perusoikeusjärjestelmän kanssa, ja kansallinen perusoikeusjärjestelmä niveltyy kaikissa selvityksen kohteena olevissa maissa kansainvälisiin ihmisoikeussopimuksiin, on syytä tuoda esille myös nämä määräykset.

2.2 Ihmisoikeussopimukset

Kansainvälisissä ihmisoikeussopimuksissa yksityisyyden suoja on perusteellisesti säännelty.

Kansalais- ja poliittisia oikeuksia koskevan yleissopimuksen (KP-sopimuksen) 17. artiklan mukaan kenenkään yksityiselämään, perheeseen, kotiin tai kirjeenvaihtoon ei saa mielivaltaisesti tai laittomasti puuttua eikä suorittaa hänen kunniaansa tai mainettaan loukkaavia hyökkäyksiä. Lisäksi jokaisella on oikeus lain suojaan tällaista puuttumista tai tällaisia hyökkäyksiä vastaan.

Euroopan neuvoston ihmisoikeussopimuksen 8. artiklan mukaan jokaisella on oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa ja kirjeenvaihtoonsa kohdistuvaa kunnioitusta. 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.

Myös yleissopimus lapsen oikeuksista sääntelee yksityisyyden suojaa (16. artikla).

Tietoturvatoimenpiteet ja yksityisyyden suoja voivat olla ristiriidassa sananvapauden kanssa. Sananvapaus on yleisesti tunnustettu oikeus, joka on tunnustettu myös kansainvälisissä ihmisoikeussopimuksissa.

KP-sopimuksen 19. artiklan 2. kohta antaa jokaiselle sananvapauden. Tämä oikeus sisältää vapauden hankkia, vastaanottaa tai levittää kaikenlaisia tietoja ja ajatuksia riippumatta alueellisista rajoista joko suullisesti, kirjallisesti tai painettuna taiteellisessa muodossa tai muulla henkilön valitsemalla tavalla. Saman artiklan 3. kohta kuitenkin lisää, että sananvapauden käyttö merkitsee erityisiä velvollisuuksia ja erityistä vastuuta. Se voidaan sen tähden asettaa tiettyjen rajoitusten alaiseksi, mutta näiden tulee olla laissa säädettyjä ja sellaisia, jotka ovat välttämättömiä toisten henkilöiden oikeuksien ja maineen kunnioittamiseksi tai valtion turvallisuuden tai yleisen järjestyksen, terveydenhoidon tai moraalin suojelemiseksi.

Euroopan ihmisoikeussopimuksen 10. artikla on sisällöltään pitkälti samanlainen. Jokaisella on sananvapaus, joka sisältää vapauden pitää mielipiteitä sekä vastaanottaa ja levittää tietoja ja ajatuksia alueellisista rajoista riippumatta ja viranomaisten siihen puuttumatta. Koska sananvapauden käyttöön liittyy velvollisuuksia ja vastuuta, se voidaan asettaa sellaisten muodollisuuksien, ehtojen, rajoitusten ja rangaistusten alaiseksi, joista on säädetty laissa, ja jotka ovat välttämättömiä demokraattisessa yhteiskunnassa kansallisen turvallisuuden, alueellisen koskemattomuuden tai yleisen turvallisuuden vuoksi, epäjärjestyksen tai rikollisuuden estämiseksi, terveyden tai moraalin suojaamiseksi, muiden henkilöiden maineen tai oikeuksien turvaamiseksi, luottamuksellisten tietojen paljastumisen estämiseksi tai tuomioistuimien arvovallan ja puolueettomuuden varmistamiseksi.

Voidaan myös esittää kysymys, onko tietoturvallisuutta taattu kansainvälisissä ihmisoikeussopimuksissa. Kansalaisoikeuksia ja poliittisia oikeuksia koskevan kansainvälisen yleissopimuksen[6] 9. artiklan mukaan jokaisella on oikeus vapauteen ja henkilökohtaiseen turvallisuuteen. Ketään ei saa mielivaltaisesti pidättää tai vangita. Keneltäkään ei saa riistää hänen vapauttaan, paitsi laissa säädetyillä perusteilla ja sen määräämässä järjestyksessä. Vastaavantyyppinen määräys on Euroopan neuvoston

[6] Suomen osalta ks. asetus yleissopimuksen sekä siihen liittyvän valinnaisen pöytäkirjan voimaansaattamisesta 30.1.1976/108, SopS 8.

ihmisoikeussopimuksessa[7], jossa on lisäksi yksityiskohtainen sallittujen vapaudenriisto-perusteiden luettelo.

Euroopan ihmisoikeussopimuksessa käsitteen ”henkilökohtainen turvallisuus” on katsottu antavan turvaa mielivaltaista vapauteen puuttumista vastaan ja vahvistavan ihmisen vapaudenriistoa vastaan nauttimaa suojaa. Muuten ei henkilökohtaiselle turvallisuudelle ole annettu Euroopan ihmisoikeussopimuksen valvontaelimissä erityistä itsenäistä merkitystä. YK:n ihmisoikeuskomitea on kansalais- ja poliittisia oikeuksia koskevan yleissopimuksen perusteella katsonut, että viittaus henkilökohtaiseen turvallisuuteen ei rajoitu koskemaan ainoastaan vapaudenriistotilanteita.[8]

Euroopan unionin perusoikeuskirjaan vuodelta 2000 on kirjattu ne perusoikeudet, joita Euroopan yhteisön tuomioistuin on 1960-luvun lopulta lähtien vahvistanut. Perus-oikeuskirja on otettu osaksi vastoinkäymisiä kohdannutta ehdotusta perustuslailliseksi sopimukseksi. Mikäli perusoikeuskirja saisi muodollisesti sitovan muodon, sovellettaisiin sitä EU-toimielinten tai kansallisten viranomaisten soveltaessa EU-oikeutta.

Perusoikeuskirjan 6. artiklassa taataan jokaiselle oikeus vapauteen ja henkilö-kohtaiseen turvallisuuteen. Perusoikeuskirjan 7. artiklassa todetaan, että jokaisella on oikeus siihen, että hänen yksityis- ja perhe-elämäänsä, kotiaan sekä viestejään kunnioitetaan. Nimenomainen määräys henkilötietojen suojasta on kirjattu perusoikeus-kirjan 8. artiklaan, jonka mukaan jokaisella on oikeus henkilötietojensa suojaan. Lisäksi tietojen käsittelyn on oltava asianmukaista ja sen on tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla. Jokaisella on oikeus tutustua niihin tietoihin, joita hänestä on kerätty, ja saada ne oikaistuksi. Riippumattoman viranomaisen on valvottava näiden sääntöjen noudattamista.

Perusoikeuskirjan 11. artiklan mukaan jokaisella on oikeus sananvapauteen. Tämä oikeus sisältää mielipiteenvapauden sekä vapauden vastaanottaa ja levittää tietoja tai ajatuksia viranomaisten siihen puuttumatta ja alueellisista rajoista riippumatta. Myös tiedotusvälineiden vapautta ja moniarvoisuutta kunnioitetaan.

Perustusoikeuskirja sisältää määräyksiä hallinnon avoimuusperiaatteesta. Sen 41. artiklan mukaan jokaisella on oikeus siihen, että unionin toimielimet, elimet ja laitokset

---

[7] Suomen osalta ks. asetus yleissopimuksen ja siihen liittyvien lisäpöytäkirjojen voimaansaattamisesta sekä yleissopimuksen ja lisäpöytäkirjojen eräiden määräysten hyväksymisestä annetun lain voimaantulosta (Euroopan neuvoston ihmisoikeussopimus) 18.5.1990/439, SopS 19.

[8] Matti Pellonpää, Euroopan ihmisoikeussopimus, 2005, s. 275.

käsittelevät hänen asiansa puolueettomasti, oikeudenmukaisesti ja kohtuullisessa ajassa. Tähän oikeuteen sisältyy erityisesti mm. jokaisen oikeus tutustua häntä koskeviin asiakirjoihin ottaen huomioon oikeutetun luottamuksellisuuden, salassapitovelvollisuuden ja liikesalaisuuden vaatimukset.

2.3 Tietosuojan ylikansallista sääntelyä

Tietosuojaa on säännelty runsaasti ylivaltiollisella tasolla. Euroopan neuvosto ja EU ovat olleet keskeisiä sääntelijöitä tässä suhteessa. Myös OECD on osallistunut kansainväliseen tietosuoja- ja tietoturvayhteistyöhön suosituksin.

2.3.1 Euroopan neuvoston tietosuojayleissopimus 1981

Euroopan neuvostossa on valmisteltu yleissopimus yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä (SopS no 36/1992, jäljempänä tietosuojasopimus). Sopimuksen tarkoituksena on turvata henkilötietojen automaattisessa tietojenkäsittelyssä jokaiselle hänen kansalaisuudestaan tai asuinpaikastaan riippumatta hänen oikeutensa ja perusvapautensa ja erityisesti hänen oikeutensa yksityisyyteen. Sopimusta sovelletaan automaattisesti käsiteltäviin henkilörekistereihin ja henkilötietojen automaattiseen tietojenkäsittelyyn julkisella ja yksityisellä sektorilla. Tietosuojasopimuksen on ratifioinut 20 valtiota, joiden joukossa ovat kaikki Euroopan unionin jäsenmaat.

Euroopan neuvosto on antanut tietosuojasopimuksen perusteella kymmenen alakohtaista suositusta, joilla pyritään edistämään tietosuojan harmonisointikehitystä. Suositukset koskevat muun muassa suoramarkkinointia, poliisitoimen tietosuojaa, työelämää ja viranomaisten henkilötietojen luovuttamista. Esimerkiksi Euroopan neuvoston teletoiminnan tietosuojaa koskevassa suosituksessa R(95)4 kehotetaan tarjoamaan telepalveluja, joissa otetaan huomioon käyttäjien yksityisyydensuoja ja viestinnän luottamuksellisuus. Televerkot olisi rakennettava näitä tarkoituksia silmällä pitäen. Telepalveluja tulisi olla mahdollista käyttää nimettömänä. Teleyrityksen palveluksessa olevilla henkilöillä tulisi olla vaitiolovelvollisuus työn suorittamisessa saamiensa viestien sisältöä koskevien tietojen osalta. Henkilötietoja saisi käsitellä lähinnä vain yhteyden muodostamista tai palvelun tarjoamista ja laskutusta varten sekä palvelun tai verkon moitteettoman toiminnan varmistamiseksi. Teleyrityksen tulisi varmistaa televerkon ja telepalvelujen turvallisuus sekä tiedottaa televerkon turvallisuusriskeistä ja mahdollisuuksista niiden vähentämiseen. Lisäksi suosituksessa käsitellään tietojen luovutusta, laskuerittelyä, kutsuvan yhteyden tunnistusta, kutsunsiirtoa ja tilaajaluetteloita koskevia periaatteita. Periaatteet ovat hyvin samansuuntaisia kuin sähköisen viestinnän tietosuojadirektiivissä.

Euroopan neuvosto on myös laatinut suositusluonnoksen henkilötietojen käsittelystä kameravalvonnan yhteydessä.

2.3.2 EU:n henkilötietodirektiivi (95/46/EY)

EU on säännellyt henkilötietojen suojaa direktiivillä jo yli kymmenen vuotta sitten. Direktiivi on yhteisön laki, joka on osoitettu jäsenvaltioille. Direktiivi annetaan Euroopan laajuisesti, ja kaikkien jäsenvaltioiden on varmistettava, että sitä noudatetaan niiden oikeusjärjestelmässä. Direktiivissä säädetään lopputuloksesta. Kukin jäsenvaltio voi itse päättää tavoista, miten se soveltaa direktiiviä, kunhan lopputulos on sama.

Periaatteessa direktiivi tulee voimaan kansallisten täytäntöönpanotoimenpiteiden (kansallinen laki) välityksellä. On kuitenkin mahdollista, että vaikka jäsenvaltio ei vielä olisikaan saattanut direktiiviä voimaan, joillakin sen säännöksillä voi olla välitöntä vaikutusta. Tämä tarkoittaa sitä, että jos direktiivissä annetaan välittömiä oikeuksia yksityishenkilöille, yksityishenkilö voi vedota direktiiviin oikeudessa ilman, että hänen tarvitsee odottaa kansallisella lainsäädännöllä tapahtuvaa täytäntöönpanoa. Lisäksi, jos yksityishenkilö on mielestään kärsinyt vahinkoa, koska kansalliset viranomaiset eivät ole panneet direktiiviä täytäntöön oikein, hänellä saattaa olla oikeus vaatia vahingonkorvausta. Vahingonkorvaus voidaan tuomita vain kansallisissa tuomio-istuimissa.

Tietotekniikan kehitys ja uudet televerkot helpottavat henkilötietojen siirtämistä yli rajojen. Sen seurauksena jonkin EU:n jäsenvaltion kansalaisia koskevia tietoja käsitellään joskus toisessa jäsenvaltiossa. Koska henkilötietoja kerätään ja vaihdetaan yhä useammin, tarvitaan tietojen siirtoa koskevaa sääntelyä.

Tietosuojaa koskevissa kansallisissa laeissa edellytetään tietojen käsittelijöiltä eli ”rekisterinpitäjiltä” yleensä hyviä tiedonhallintakäytäntöjä. Näitä ovat velvollisuus käyttää tietoja asianmukaisesti ja turvallisella tavalla sekä velvollisuus käyttää henkilötietoja ainoastaan nimenomaisiin ja laillisiin tarkoituksiin. Kansalliset lait myös takaavat yksityishenkilöille eräitä oikeuksia, kuten oikeuden saada tietää, milloin ja mistä syystä henkilötietoja on käsitelty, oikeuden saada rekistereissä olevia tietoja ja tarvittaessa oikeuden saada tiedot muutetuiksi tai poistetuiksi.

Vaikka tietosuojaa koskevilla kansallisilla laeilla on pyritty takaamaan samat oikeudet, lainsäädännöissä on kuitenkin ollut joitakin eroavaisuuksia. Nämä erot ovat saattaneet aiheuttaa esteitä tiedon vapaalle liikkuvuudelle ja lisätaakkoja taloudellisille toimijoille ja kansalaisille. Eräitä näistä ongelmista olivat tarve rekisteröityä tai saada lupa tietojen käsittelemiseen valvovilta viranomaisilta useassa jäsenvaltiossa, tarve noudattaa eri standardeja ja mahdollinen kielto siirtää tietoja toiseen EU:n jäsenvaltioon. Joissakin

jäsenvaltioissa ei lisäksi ollut tietosuojaa koskevia lakeja. Näistä syistä tarvittiin Euroopan tasoista toimintaa, ja tämä tapahtui EY:n direktiivien muodossa.

Tämän alan kansallisten säännösten yhdenmukaistamiseksi kehitettiin direktiivi 95/46/EY (tietosuojadirektiivi), jonka tarkoituksena oli poistaa tietojen vapaan liikkuvuuden esteet siten, että tietosuojaa ei heikennettäisi.

Direktiivin tuloksena kaikkien kansalaisten henkilötiedoilla on sama suoja kaikkialla unionissa. EU:n viidentoista jäsenvaltion oli saatettava kansallinen lainsäädäntönsä direktiivin säännösten mukaiseksi 24. lokakuuta 1998 mennessä.

2.3.2.1 Direktiivin käsitteitä

Tietosuojadirektiiviä sovelletaan toimintoihin tai toimintojen kokonaisuuksiin, joita kohdistetaan henkilötietoihin[9], mitä kutsutaan tietojen käsittelyksi[10]. Tällaisia toimintoja ovat mm. henkilötietojen kerääminen, niiden säilyttäminen ja luovuttaminen. Direktiiviä sovelletaan tietoihin, joita käsitellään automaattisesti (esimerkiksi tietokoneella oleva asiakasrekisteri) ja tietoihin, jotka ovat osa tai joiden on tarkoitus muodostaa osa ei-automaattista rekisteröintijärjestelmää[11], josta ne ovat saatavilla tiettyjen kriteerien mukaisesti. (Tällaisia ovat esimerkiksi perinteiset paperikortistot, joissa asiakastiedot ovat aakkosjärjestyksessä nimen perusteella.)

Tietosuojadirektiiviä ei sovelleta tietoihin, joita käsitellään pelkästään henkilökohtaisista syistä tai kotitalouden tarpeisiin (esimerkiksi sähköisessä muodossa oleva henkilökohtainen päiväkirja tai perheenjäsenten ja ystävien tiedot sisältävä kortisto). Sitä ei myöskään sovelleta sellaisilla aloilla kuin yleinen turvallisuus, puolustus tai rikosoikeus, jotka eivät kuulu EY:n toimivaltaan ja jotka ovat edelleen kansallisia etuoikeuksia.

---

[9] ”Henkilötiedoilla" tarkoitetaan kaikenlaisia tunnistettuja tai tunnistettavissa olevia luonnollista henkilöä ("rekisteröity") koskevia tietoja; tunnistettavissa olevana pidetään henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa, erityisesti henkilönumeron taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.

[10] "Henkilötietojen käsittelyllä" tarkoitetaan kaikenlaisia sellaisia toimintoja tai toimintojen kokonaisuuksia, joita kohdistetaan henkilötietoihin joko automaattisen tietojenkäsittelyn avulla tai manuaalisesti, kuten tietojen kerääminen, tallentaminen, järjestäminen, säilyttäminen, muokkaaminen tai muuttaminen, tiedon haku, kysely, käyttö, luovuttaminen siirtämällä, levittämällä tai asettamalla muutoin saataville, yhteensovittaminen tai yhdistäminen sekä suojaaminen, poistaminen tai tuhoaminen.

"Henkilötietojen käsittelijällä" tarkoitetaan luonnollista tai oikeushenkilöä, julkista viranomaista, virastoa tai muuta toimielintä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.

[11] "Henkilötietojen rekisteröintijärjestelmällä" tarkoitetaan kaikkia sellaisia järjestettyjä henkilötietojen kokoelmia, joista tiedot ovat saatavilla tietyin perustein, oli kokoelma sitten keskitetty, hajautettu tai toiminnallisin tai maantieteellisin perustein jaettu.

Kansallisessa lainsäädännössä on yleensä säädetty yksityishenkilön suojasta näissä asioissa.

Rekisterinpitäjä[12] on henkilö tai yhteisö, joka määrittelee henkilötietojen käsittelyn tarkoituksen ja keinot. Lääkäri on yleensä potilastietojen rekisterinpitäjä; yritys on sen asiakkaita ja työntekijöitä koskevien tietojen rekisterinpitäjä; urheiluseura pitää rekisteriä jäsenistään ja yleinen kirjasto pitää rekisteriä käyttäjistään. Rekisterinpitäjien on kunnioitettava useita periaatteita. Periaatteiden tarkoituksena ei ole vain rekisteröityjen suojelu, vaan ne ovat myös osoitus hyvistä liikekäytännöistä, jotka myötävaikuttavat luotettavaan ja tehokkaaseen tietojenkäsittelyyn.

Kaikkien rekisterinpitäjien on noudatettava sijaintijäsenvaltionsa tietojenkäsittelyä koskevia sääntöjä, vaikka käsitellyt tiedot koskisivatkin toisessa valtiossa asuvaa henkilöä. Jos rekisterinpitäjä ei ole sijoittautunut yhteisön alueelle (esimerkiksi ulkomainen yhtiö), sen on noudatettava jäsenvaltion lainsäädäntöä, jos käsittely-laitteisto (esimerkiksi tietojenkäsittelykeskus) sijaitsee Euroopan yhteisössä.

2.3.2.2 Perusvaatimukset tietojen käsittelylle

Direktiivissä asetetaan perusvaatimuksia itse tiedoille. Tietoja on käsiteltävä asian-mukaisella ja lainmukaisella tavalla ja tiedot on kerättävä nimenomaisia ja laillisia tarkoituksia varten ja käytettävä sen mukaisesti. Lisäksi tietojen on oltava olennaisia eikä liian laajoja siihen tarkoitukseen, jota varten niitä käsitellään. Tietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä.

Rekisterinpitäjien on tarjottava rekisteröidyille riittävä mahdollisuus korjata, poistaa tai jäädyttää heitä koskevat virheelliset tiedot. Tietoja, joiden perusteella henkilö voidaan tunnistaa, ei pidä säilyttää kauemmin kuin on tarpeen.

Direktiivissä säädetään, että kaikissa jäsenvaltioissa on oltava yksi tai useampi viranomainen, jonka tehtävä on valvoa direktiivin soveltamista. Yksi valvonta-viranomaisen velvollisuuksista on pitää ajan tasalla olevaa julkista rekisteriä, josta kaikki voivat saada tietoonsa kaikkien rekisterinpitäjien nimet ja heidän suorittamiensa käsittelyjen laadun.

---

[12] "Rekisterinpitäjällä" tarkoitetaan direktiivissä luonnollista tai oikeushenkilöä, julkista viranomaista, virastoa tai muuta toimielintä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoituksen ja keinot; jos käsittelyn tarkoitus ja keinot määritellään kansallisilla tai yhteisön laeilla tai asetuksilla, rekisterinpitäjä tai erityiset perusteet rekisterinpitäjän nimeämiseksi voidaan vahvistaa kansallisten tai yhteisön säännösten mukaisesti.

Periaatteessa kaikkien rekisterinpitäjien on ilmoitettava valvontaviranomaiselle tietojen käsittelystä. Jäsenvaltiot voivat sallia, että tietyt tietojen käsittelyn tyypit, joihin ei liity erityisiä riskejä, vapautetaan ilmoitusmenettelystä tai menettelyä voidaan yksinkertaistaa. Vapauttaminen ja yksinkertaistaminen voidaan sallia myös, jos rekisterinpitäjä on kansallista lakia noudattaen nimennyt riippumattoman tietosuojasta vastaavan henkilön. Jäsenvaltiot voivat vaatia, että valvontaviranomaiset tarkistavat ennakolta tietojen käsittelyt, joihin liittyy erityisiä riskejä. Jäsenvaltioiden on päätettävä, mihin tietojen käsittelyyn liittyy erityisiä riskejä.

2.3.2.3 Milloin henkilötietoja voidaan käsitellä?

Henkilötietoja voidaan direktiivin mukaan käsitellä ainoastaan seuraavissa tapauksissa:

- Rekisteröity on yksiselitteisesti antanut suostumuksensa[13] eli jos hän on riittävästi asiasta tietoja saatuaan vapaasti ja nimenomaisesti hyväksynyt tietojen käsittelyn.
- Tietojen käsittely on tarpeen rekisteröidyn toivoman sopimuksen täytäntöön panemiseksi tai sopimuksen tekemiseksi; esimerkiksi tietojen käsittely laskutuksen yhteydessä tai työpaikan tai lainan hakijaan liittyvien tietojen käsittely.
- Laki edellyttää tietojen käsittelyä.
- Tietojen käsittely on tarpeen rekisteröidyn elintärkeän edun suojelemiseksi. Tästä on esimerkki auto-onnettomuuden yhteydessä lääkintähenkilökunnan tajuttomalle henkilölle tekemä verikoe, jos sitä pidetään tarpeellisena rekisteröidyn hengen pelastamiseksi.
- Tietojen käsittely on tarpeen yleisen edun mukaisten tehtävien suorittamiseksi tai viranomaisten (kuten valtion viranomaiset, veroviranomaiset, poliisi) tehtävien täyttämiseksi.
- Tietoja voidaan myös käsitellä aina, kun rekisterinpitäjällä tai kolmannella osapuolella on oikeutettu syy siihen. Syy ei kuitenkaan voi ylittää rekisteröidyn perusoikeuksia ja erityisesti oikeutta yksityisyyden suojaan. Tällä määräyksellä vakiinnutetaan tarve päästä kohtuulliseen tasapainoon käytännössä rekisterinpitäjien liike-edun ja rekisteröityjen yksityisyyden välillä. Tasapainoa arvioi ensisijaisesti tietosuojaviranomaisten valvonnassa toimiva rekisterinpitäjä, vaikka tuomioistuimilla on tarvittaessa lopullinen päätösvalta.

---

[13] "Rekisteröidyn suostumuksella" tarkoitetaan kaikenlaista vapaaehtoista, yksilöityä ja tietoista tahdon ilmaisua, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn.

2.3.2.4 Arkaluontoiset tiedot

Arkaluontoisten tietojen käsittelyä koskevat erittäin tiukat säännöt. Tällaisia tietoja ovat rodulliseen tai etniseen alkuperään, poliittisiin mielipiteisiin, uskonnolliseen tai filosofiseen vakaumukseen, ammattiyhdistysten jäsenyyteen, terveyteen tai seksuaaliseen käyttäytymiseen liittyvät tiedot. Periaatteessa näitä tietoja ei voida käsitellä. Poikkeuksia voidaan sallia hyvin erityisin edellytyksin. Tällaisia edellytyksiä ovat: rekisteröity on antanut nimenomaisen suostumuksensa siihen, tietojen käsittely työllisyyslain puitteissa, tapaukset joissa rekisteröidyn on mahdotonta antaa suostumusta (esim. liikenneonnettomuuden uhrille tehtävä verikoe), julkisesti ilmoitettujen henkilötietojen käsittely tai ammattiyhdistysten, poliittisten puolueiden tai kirkkojen tekemä jäsentensä tietojen käsittely. Jäsenvaltiot voivat tietyissä tapauksissa määrätä lisää poikkeuksia elintärkeiden yleisten etujen suojelemiseksi.

2.3.2.5 Internet

Internetin kaltaisen merkittävän siirtovälineen jättäminen pois tietosuojadirektiivin soveltamisalasta olisi sekä epäloogista että oikeudellisesti perusteetonta. Koska Internetin välityksellä siirretään suuria määriä erilaisia henkilötietoja kaikkialla maailmassa, myös maihin, joissa tietosuojan taso ei ole riittävä, kysymykseen on kiinnitettävä erityistä huomiota. Tietosuojadirektiivi on sen vuoksi teknisesti neutraali: sitä sovelletaan aina henkilötietojen käsittelyssä käytetystä teknisestä menetelmästä riippumatta. Direktiivi koskee esimerkiksi henkilötietojen näkymätöntä keräämistä Internetissä (esim. käyttäjien surffailutapojen seurannassa käytetyt evästeet). Jos toisaalta henkilötietoja kerätään ”näkyvällä” tavalla, voidaan katsoa, että omia tietojaan siirtävä yksityishenkilö on antanut suostumuksensa sellaiseen siirtoon, jos hänelle on riittävästi tiedotettu siihen liittyvistä riskeistä.

2.3.2.6 Rekisteröidyn tiedonsaantioikeus

Rekisterinpitäjien on ilmoitettava keruusta rekisteröidylle aina rekisteröidyn henkilötietoja kerätessään, ellei rekisteröidylle ole jo ilmoitettu asiasta. Rekisteröidyllä on oikeus tietää, kuka on rekisterinpitäjä, mitä tarkoitusta varten tietoja käsitellään, esimerkiksi kuka tiedot saa ja mitä erityisiä oikeuksia rekisteröidyillä on. Rekisteröidyllä on oikeus saada nämä tiedot siitä riippumatta, onko tiedot saatu suoraan tai välillisesti kolmansilta osapuolilta. Viimeksi mainittuun tapaukseen saattaa liittyä poikkeuksia, jos tämän tiedon antaminen osoittautuu mahdottomaksi tai äärimmäisen vaikeaksi tai jos laki sitä vaatii.

Rekisteröity voi tiedustella keneltä tahansa rekisterinpitäjältä, käsitteleekö tämä rekisteröityä koskevia henkilötietoja, saada kopion tiedoista selkeäkielisessä muodossa

ja saada kaikki käytettävissä olevat tiedot niiden lähteistä. Jos henkilötiedot ovat virheellisiä tai niitä on käsitelty laittomasti, rekisteröidyllä on oikeus pyytää tietojen korjaamista, poistamista tai jäädyttämistä. Sellaisissa tapauksissa rekisteröity voi myös vaatia, että rekisterinpitäjä ilmoittaa asiasta virheelliset tiedot nähneille kolmansille osapuolille, ellei tämä osoittaudu mahdottomaksi. Tietoihin tutustumisesta voidaan joissakin tapauksissa periä kohtuullinen maksu.

Rekisteröityyn merkittävästi vaikuttavat päätökset, kuten päätökset lainan tai vakuutuksen myöntämisestä, saatetaan tehdä pelkästään automaattisen tietojen käsittelyn pohjalta. Sen vuoksi rekisterinpitäjän on noudatettava asianmukaisia suoja-toimenpiteitä, esimerkiksi annettava rekisteröidylle mahdollisuus keskustella kerättyjen tietojen taustalla olevista syistä ja kyseenalaistaa päätökset, jotka perustuvat virheellisiin tietoihin.

2.3.2.7 Poikkeukset ja rajoitukset

Oikeus yksityisyyteen saattaa joskus olla ristiriidassa ilmaisunvapauden kanssa ja erityisesti lehdistön ja muiden tiedotusvälineiden vapauden kanssa. Jäsenvaltioiden on sen vuoksi tietosuojaa koskevissa laeissaan säädettävä poikkeuksista, jotta näiden erilaisten, mutta yhtä lailla perustavanlaatuisten, oikeuksien välillä saavutettaisiin tasapaino.

Kansallisissa laeissa voidaan sallia myös muita poikkeuksia direktiiviin. Näitä ovat velvollisuus tiedottaa rekisteröidylle, tiedonkäsittelyn julkistaminen ja velvollisuus kunnioittaa hyvän tietohallinnon perusperiaatteita. Poikkeukset sallitaan, jos ne ovat muun muassa tarpeen kansallisen turvallisuuden, puolustuksen, rikosten selvittämisen tai rikoslain täytäntöönpanon vuoksi tai rekisteröityjen suojelemiseksi tai muiden oikeuksien ja vapauksien puolustamiseksi. Lisäksi voidaan myöntää poikkeus oikeudesta tutustua tietoihin, jotka on käsitelty tieteellisiä tai tilastointitarkoituksia varten.

Jos tietoja siirretään maihin, jotka eivät ole EU:n jäsenvaltioita, saattaa olla tarpeen ryhtyä erityisiin varotoimenpiteisiin, jos tietosuojan taso kyseisessä maassa ei vastaa yhteisön lainsäädännön vaatimaa tasoa. Ilman erityisiä sääntöjä direktiivin tarjoama korkealaatuinen tietosuoja murenisi nopeasti, koska tietoja voidaan nykyään siirtää helposti kansainvälisissä verkoissa.

Direktiivin periaate on, että henkilötietoja voidaan siirtää ainoastaan sellaisiin EU:n ulkopuolisiin maihin, jotka takaavat tietosuojan ”riittävän” tason. Komissiossa tutkitaan

erimaiden tietosuojasäännöstöjä ja käydään neuvotteluja EU:n tärkeimpien kauppakumppanien kanssa, jotta voitaisiin päättää, missä maissa tietosuojan taso on riittävä.[14]

Jos tietyssä kolmannessa maassa ei taata tietosuojan riittävää tasoa, tarkemmin määritellyt tietojensiirrot on direktiivin mukaan estettävä. Jäsenvaltioiden on ilmoitettava komissiolle kaikista sellaisista estämistoimenpiteistä, jonka jälkeen yhteisön toimenpiteellä varmistetaan, että jäsenvaltion päätös estää tietojen siirtäminen joko laajennetaan koskemaan kaikkia kyseisenlaisia EU:sta tehtäviä tietojen siirtoja tai perutaan.

2.3.2.8 Sopimukset tiedonsiirrosta

Henkilötietojen siirtämisen estäminen on viimeisenä käyttöön otettava keino. Tietojen riittävä suojaus voidaan varmistaa muilla tavoin häiritsemättä kansainvälisiä tiedonsiirtoja ja liiketoimia, joihin tiedot liittyvät. Jos EU:n yritykset ovat epävarmoja siitä, tarjoaako EU:n ulkopuolisen maan lainsäädäntö tai muut säännöt tietosuojan riittävän tason, niiden kannattaa hoitaa tietosuoja itse. Se voidaan tehdä tiedot lähettävän yhtiön ja tiedot vastaanottavan EU:n ulkopuolisen maan yhtiön välisellä sopimuksella.

Sopimuksen tarkoituksena on antaa riittävät takeet henkilöiden yksityisyyden suojasta ja perusoikeuksien ja -vapauksien suojasta sekä vastaavien oikeuksien soveltamisesta. Jos toteutetaan asianmukaisia suojatoimenpiteitä, EU:n jäsenvaltiolla ei pitäisi olla syytä estää sen kansalaisia koskevien tietojen siirtämistä.[15]

2.3.2.9 Direktiivin tietoturvamääräykset

Käsittelyn turvallisuuden osalta direktiivissä määrätään, että jäsenvaltioiden on säädettävä siitä, että rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi vahingossa tapahtuvalta tai laittomalta tuhoamiselta, vahingossa tapahtuvalta häviämiseltä, muuttamiselta, luvattomalta luovuttamiselta tai tietojen antamiselta, erityisesti jos käsittely muodostuu tietojen siirtämisestä verkossa, sekä kaikelta muulta laittomalta käsittelyltä.

Ottaen huomioon kehityksen taso ja toimenpiteiden kustannukset on taattava asianmukainen turvallisuuden taso suhteessa käsittelyn riskeihin ja suojattavien tietojen luonteeseen.

---

[14] Yhdysvaltain osalta ks. komission päätös 2000/520/EY, EYVL 215, 25.8.2005, s. 7.

[15] http://europa.eu.int/comm/justice_home/fsj/privacy/modelcontracts/index_en.htm

Jäsenvaltioiden on säädettävä, että jos käsittely suoritetaan rekisterinpitäjän lukuun, tämän on valittava henkilötietojen käsittelijä, joka antaa riittävät takeet käsittelyyn liittyvistä teknisistä ja organisatorisista turvatoimista, ja huolehdittava siitä, että nämä toimet toteutetaan.

Kun käsittely suoritetaan rekisterinpitäjän lukuun, käsittelyä on säänneltävä sopimuksella tai oikeudellisella asiakirjalla, joka sitoo käsittelijän rekisterinpitäjään ja jossa erityisesti säädetään siitä, että

- käsittelijä toimii ainoastaan rekisterinpitäjän ohjeiden mukaisesti,
- käsittelijä on lisäksi velvollinen noudattamaan 1. kohdassa tarkoitettuja velvoitteita sellaisina kuin ne on määritelty sen jäsenvaltion lainsäädännössä, jonne käsittelijä on sijoittautunut.

Todisteiden säilyttämiseksi tietojen suojaamiseen ja tarpeellisten teknisiä ja organisatorisia toimenpiteitä koskeviin vaatimuksiin liittyvien sopimusten tai oikeudellisten asiakirjojen osien on oltava kirjallisina tai muussa vastaavassa muodossa.

Direktiivi sisältää lainvalintasääntönsä. Kunkin jäsenvaltion on sovellettava henkilötietojen käsittelyyn kansallisia säännöksiä, jotka se antaa tämän direktiivin mukaisesti, jos

a. käsittely suoritetaan kyseisen jäsenvaltion alueella sijaitsevassa rekisterinpitäjän toimipaikassa tapahtuvan toiminnan yhteydessä; jos sama rekisterinpitäjä on sijoittautunut usean jäsenvaltion alueelle, sen on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että kussakin toimipaikassa noudatetaan sovellettavan kansallisen oikeuden mukaisia velvoitteita,
b. rekisterinpitäjä ei ole sijoittautunut kyseisen jäsenvaltion alueelle, vaan paikkaan, jossa jäsenvaltion kansallista lakia sovelletaan kansainvälisen julkisoikeuden nojalla,
c. rekisterinpitäjä ei ole sijoittautunut yhteisön alueelle, mutta käyttää henkilötietojen käsittelyssä automatisoituja tai muunlaisia välineitä, jotka sijaitsevat kyseisen jäsenvaltion alueella, paitsi jos näitä välineitä käytetään ainoastaan tiedonsiirtoon yhteisön alueen kautta. Tällöin rekisterinpitäjän on nimettävä kyseisen jäsenvaltion alueelle sijoittautunut edustaja.

2.3.3 Sähköisen viestinnän tietosuojadirektiivi (2002/58/EY)

2.3.3.1 Suhde henkilötietodirektiiviin

Direktiivi 2002/58/EY on osa telealan sääntelypakettia, joka on uusi säädös sähköisen viestinnän alan sääntelemiseksi ja viestinnän alan nykyisen sääntelyn korvaamiseksi. Telealan sääntelypakettiin kuuluu neljä muuta direktiiviä, jotka koskevat yleisiä puitteita, käyttöoikeuksia ja yhteenliittämistä, valtuuksia ja toimilupia sekä yleispalvelua.

Direktiivillä on kumottu 15. joulukuuta 1997 annettu direktiivi 97/66/EY. Direktiivissä käsitellään joitakin varsin arkaluonteisia aiheita, kuten yhteystietojen säilyttämistä jäsenvaltioiden poliisivalvontatarkoituksiin (tietojen pidättäminen), ei-toivottujen sähköpostiviestien lähettämistä, evästeiden (*cookies*) käyttöä ja henkilötietojen sisällyttämistä julkisiin luetteloihin.

Direktiivi toimii yhdessä henkilötieto- eli tietosuojadirektiivin kanssa. Direktiivin 1. artiklassa säädetään, että direktiivin säännöksillä täsmennetään ja täydennetään henkilötietodirektiiviä perusoikeuksien ja perusvapauksien suojan varmistamiseksi henkilötietojen käsittelyssä sähköisen viestinnän alalla sekä tällaisten tietojen ja sähköisten viestintälaitteiden ja viestintäpalvelujen vapaan liikkuvuuden varmistamiseksi yhteisössä. Direktiivi rakentuu henkilötietodirektiivin määritelmille, mutta sisältää joukon itsenäisiä määritelmiä, joiden tunteminen on välttämätöntä direktiivin sisällön avautumiselle.

2.3.3.2 Direktiivin tietoturvamääräykset

Yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajan on toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet varmistaakseen tarjoamiensa palvelujen turvallisuuden, verkon turvallisuuden osalta tarvittaessa yhdessä yleisen viestintäverkon tarjoajan kanssa. Näillä toimenpiteillä on voitava varmistaa riskiin suhteutettu turvallisuustaso ottaen huomioon uusin tekniikka ja toimenpiteiden käyttöönottokustannukset.

Jos verkon turvallisuuteen kohdistuu erityinen riski, on yleisesti saatavilla olevan sähköisen viestintäpalvelun tarjoajan ilmoitettava tilaajille tällaisesta riskistä, ja jos palvelujen tarjoaja ei voi vaikuttaa riskiin, mahdollisista korjauskeinoista mukaan lukien asiaan liittyvät todennäköiset kustannukset.

2.3.3.3 Viestinnän luottamuksellisuus

Direktiivissä muistutetaan perusperiaatteesta, jonka mukaan jäsenvaltioiden on kansallisella lainsäädännöllä varmistettava yleisen viestintäverkon välityksellä tapahtuvan viestinnän luottamuksellisuus. Vaikka direktiivi ei asiaa nimenomaisesti mainitsekaan, viesti ei ole luottamuksellinen, jos se on saatettu yleisesti vastaanotettavaksi. Jäsenmaiden on erityisesti kiellettävä se, että muut henkilöt kuin käyttäjät ilman kyseisten käyttäjien nimenomaista suostumusta[16] kuuntelevat, salakuuntelevat ja tallentavat viestintää.

Luottamuksellisuus ei koske laillisesti sallittua viestinnän ja siihen liittyvien liikennetietojen tallentamista, joka tapahtuu tavanomaisen liiketoiminnan yhteydessä todisteeksi liiketapahtumasta tai mistä tahansa muusta liiketoimintaan liittyvästä yhteydenpidosta.

2.3.3.4 Liikennetiedot luottamuksellisia

Itse viestinnän sisällön ohella myös liikennetiedot[17] (Suomen laissa puhutaan **tunnistetiedoista**) ovat luottamuksellisia. Vastaanottajan liikennetiedot voivat olla luottamuksellisia, vaikka viesti olisi tarkoitettu yleisesti vastaanotettavaksi. Direktiivissä on sääntöjä liikennetietojen käsittelystä, jotka seuraavat osin henkilötietodirektiivin periaatteita.

Liikennetietoja voidaan käsitellä tilaajalaskutusta ja yhteenliittämistä koskevia maksuja varten. Tällainen käsittely on sallittua ainoastaan sen ajanjakson loppuun asti, jona lasku voidaan laillisesti riitauttaa tai maksu periä.

Yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoaja voi sähköisten viestintäpalvelujen markkinoimiseksi tai lisäarvopalvelujen[18] tarjoamiseksi käsitellä liikennetietoja siinä määrin ja niin kauan kuin tällainen palvelu tai markkinointi edellyttää, jos tilaaja tai käyttäjä, jota tiedot koskevat, on antanut siihen suostumuksensa. Käyttäjille[19] tai tilaajille on annettava mahdollisuus perua liikennetietojen

---

[16] Käyttäjän tai tilaajan ”suostumuksella” tarkoitetaan sähköisen viestinnän tietosuojadirektiivissä samaa kuin rekisteröidyn suostumuksella tietosuojadirektiivissä 95/46/EY.

[17] ”Liikennetiedoilla” tarkoitetaan direktiivissä tietoja, joita käsitellään sähköisessä viestintäverkossa välitettävää viestintää tai sen laskutusta varten.

[18] ”Lisäarvopalvelulla” tarkoitetaan direktiivissä palvelua, joka edellyttää muiden kuin viestinnän välittämisessä tai laskutuksessa tarvittavien liikennetietojen tai muiden paikkatietojen kuin liikennetietojen käsittelyä.

[19] ”Käyttäjällä” tarkoitetaan luonnollisia henkilöitä, jotka käyttävät yleisesti saatavilla olevaa sähköistä viestintäpalvelua yksityis- tai liikeasioihin olematta välttämättä tämän palvelun tilaajia.

käsittelyä koskeva suostumuksensa milloin tahansa. Palvelun tarjoajan on ilmoitettava tilaajalle tai käyttäjälle, minkä tyyppisiä liikennetietoja käsitellään ja kuinka kauan niiden käsittely kestää.

Liikennetietojen käsittely on rajoitettava yleisten viestintäverkkojen ja yleisesti saatavilla olevien palvelujen tarjoajien vastuulla toimiviin henkilöihin, jotka käsittelevät laskutusta tai liikenteenhallintaa, asiakastiedusteluja, petosten paljastamista, sähköisten viestintäpalvelujen markkinoimista tai lisäarvopalvelujen tarjoamista, ja sitä voidaan suorittaa ainoastaan kyseisten toimien vaatimassa laajuudessa.

Tilaajia ja käyttäjiä koskevat liikennetiedot, jotka yleisen viestintäverkon tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoaja käsittelee ja tallentaa, on poistettava tai tehtävä nimettömiksi, kun niitä ei enää tarvita viestinnän välittämiseen.

Direktiivin 15. artiklan mukaan liikennetietojen käsittelyyn on oikeus väärinkäytöstapauksissa. Artiklan mukaan kaikki liikennetietoja koskevat artiklat voidaan sivuuttaa, jos se on välttämätöntä esimerkiksi rikosten tai sähköisen viestintäjärjestelmän luvattoman käytön torjunnan, tutkinnan, selvittämisen ja syyteharkinnan varmistamiseksi.

2.3.3.5 Paikkatiedot

Jos yleisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen käyttäjien tai tilaajien muita paikkatietoja[20] kuin liikennetietoja voidaan käsitellä, näitä tietoja saa käsitellä vain silloin, kun ne on tehty nimettömiksi tai jos käyttäjät tai tilaajat ovat antaneet siihen suostumuksensa, ja tietoja saa käsitellä ainoastaan siinä määrin ja niin kauan kuin lisäarvopalvelujen tarjoaminen edellyttää. Ennen kuin käyttäjät tai tilaajat antavat suostumuksensa, palvelun tarjoajan on ilmoitettava heille, minkä tyyppisiä muita paikkatietoja kuin liikennetietoja käsitellään, mikä on käsittelyn tarkoitus ja kuinka kauan se kestää sekä siirretäänkö tiedot kolmannelle osapuolelle lisäarvopalvelun tarjoamista varten. Käyttäjille tai tilaajille on

---

[20] ”Paikkatiedoilla” tarkoitetaan sähköisessä viestintäverkossa käsiteltäviä tietoja, jotka ilmaisevat yleisesti saatavilla olevan sähköisen viestintäpalvelun käyttäjän päätelaitteen maantieteellisen sijainnin.

Paikkatieto voi ilmaista esimerkiksi tukiasemapaikannuksen (cell-id) avulla GSM-puhelimen käyttäjän maantieteellisen sijainnin riippumatta siitä, puhuuko käyttäjä puhelimeen vai ei. Paikkatiedot voivat liittyä myös muihin välineisiin kuin viestintään käytettäviin päätelaitteisiin. Esimerkkinä voidaan mainita erilaiset paikannusrannekkeet, joilla ei voida lähettää tai vastaanottaa viestejä, mutta joiden maantieteellinen sijainti voidaan selvittää esimerkiksi tukiasema paikannuksen ja satelliittipaikannuksen (GPS) keinoin. Paikantaminen antaa myös uusia mahdollisuuksia monenlaisen paikkatietoon perustuvan kaupallisen toiminnan ja muun muassa mainonnan toteuttamiseen.

annettava mahdollisuus milloin tahansa peruuttaa suostumuksensa muiden paikkatietojen kuin liikennetietojen käsittelyyn.

Jos muiden paikkatietojen kuin liikennetietojen käsittelyyn on saatu käyttäjien tai tilaajien suostumus, käyttäjällä tai tilaajalla on edelleen oltava mahdollisuus helposti ja veloituksetta kieltää väliaikaisesti tällaisten tietojen käsittely kunkin verkkoyhteyden tai kunkin viestintätapahtuman osalta.

Muiden paikkatietojen kuin liikennetietojen käsittely edellä olevan mukaisesti on rajoitettava yleisen sähköisen viestintäverkon tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajan tai lisäarvopalvelua tarjoavan kolmannen osapuolen vastuulla toimiviin henkilöihin, ja sitä saa suorittaa ainoastaan lisäarvopalvelun tarjoamisen vaatimassa laajuudessa.

2.3.3.6 Poikkeukset tietosuojasta

Direktiivissä säädetään tietojen pidättämisestä, että jäsenvaltiot voivat poistaa tietosuojan ainoastaan rikostutkinnan mahdollistamiseksi tai kansallisen turvallisuuden, maanpuolustuksen ja yleisen turvallisuuden säilyttämiseksi. Tällaiseen toimenpiteeseen voidaan ryhtyä vain, jos toimenpide on "asianmukainen ja oikeassa suhteessa sen tarkoitukseen nähden ja välttämätön demokraattisessa yhteiskunnassa".

2.3.3.7 Roskaposti ja muu ei-toivottu viestintä

Direktiivissä on suostumukseen perustuva lähestymistapa ei-toivotuille kaupallisille sähköpostiviesteille[21] eli *spammingille*, toisin sanoen käyttäjien on annettava ennalta suostumuksensa vastaanottaa kyseisiä viestejä. Tämä suostumukseen perustuva järjestelmä kattaa myös suoramarkkinointitarkoituksessa lähetetyt tekstiviestit ja muut sähköiset, mihin tahansa kiinteään päätelaitteeseen tai matkaviestimeen lähetetyt sähköiset viestit.

Ilman ihmisen työpanosta toimivien automatisoitujen soittojärjestelmien (automaattisten soittolaitteiden), telekopiolaitteiden tai sähköpostin käyttö suoramarkkinointitarkoituksiin voidaan direktiivin mukaan sallia ainoastaan, jos se kohdistuu tilaajiin, jotka ovat antaneet siihen ennalta suostumuksensa. Tällä tarkoitetaan nimenomaan luonnollisia henkilöitä tilaajina, ei yrityksiä.

---

[21] ”Sähköpostilla” tarkoitetaan yleisessä viestintäverkossa lähetettävää teksti-, puhe-, ääni- tai kuvaviestiä, joka voidaan tallentaa verkkoon tai vastaanottajan päätteelle, kunnes vastaanottaja on vastaanottanut sen. Tämä määritelmä kattaa myös kännyköiden tekstiviestit, mikä poikkeaa suomalaisesta käsitteistöstä.

Jos luonnollinen henkilö tai oikeushenkilö saa asiakkailtaan heidän sähköpostiinsa liittyviä yhteystietoja tuotteen tai palvelujen myynnin yhteydessä, käyttää näitä yhteystietoja omien vastaavien tuotteidensa ja palvelujensa suoramarkkinoinnissa edellyttäen, että asiakkaille annetaan selkeästi ja selvästi yhteystietojen ottamisen ja jokaisen viestin yhteydessä mahdollisuus maksutta ja helposti kieltää tällainen yhteystietojensa käyttö, mikäli asiakas ei ole jo alun perin kieltänyt sitä.

Sellaisen sähköpostin lähettäminen suoramarkkinointitarkoituksessa on kiellettävä, jossa peitetään tai salataan sen lähettäjän henkilöllisyys, jonka puolesta viesti on lähetetty tai jossa ei ole voimassa olevaa osoitetta, johon vastaanottaja voi lähettää pyynnön siitä, että kyseinen viestintä lopetetaan.

2.3.3.8 Evästeet

Evästeet (*cookies*) ovat Internetin käyttäjän ja www-palvelimen välillä vaihdettua salattua tietoa ja ne tallentuvat tiedostoon käyttäjän kovalevylle. Tällä tiedolla mahdollistettiin aluksi kahden liittymän välinen tietojen jatkuvuus, mutta siitä tuli myös usein huonomaineisen Internetin käyttäjän toimien valvontaväline.

Tältä osin direktiivissä määrätään, että käyttäjillä on oltava mahdollisuus kieltää evästeen tai muun vastaavan menetelmän tallentaminen päätelaitteelleen. Tätä tarkoitusta varten käyttäjien on myös saatava selkeää ja täsmällistä tietoa evästeiden tarkoituksesta ja tehtävästä.

2.3.3.9 Puhelinpalveluja koskevat määräykset

Direktiiviin on otettu yksityiskohtaiset määräykset liittymän tunnistamisesta puhelinpalveluja käytettäessä. Jos teleyritys tarjoaa puhelujen osalta liittymän tunnistusta, on yksityisyyden suojan kannalta tärkeää, että tilaajalle annetaan mahdollisuus poistaa liittymänsä tunnistus esimerkiksi silloin, kun hän ei halua vastaanottajan näkevän, kuka on soittaja.

Jos kutsuvan tilaajan tunnistusta tarjotaan, palvelun tarjoajan on tarjottava soittavalle käyttäjälle mahdollisuus estää helposti ja veloituksetta kutsuvan tilaajan tunnistus puhelukohtaisesti. Soittavalla tilaajalla on oltava tämä mahdollisuus liittymäkohtaisesti. Jos taas kutsuvan tilaajan tunnistusta tarjotaan, palvelun tarjoajan on tarjottava vastaanottavalle tilaajalle mahdollisuus helposti ja tämän toiminnan kohtuullisen käytön osalta veloituksetta estää tulevien puhelujen tilaajan tunnistus. Jos kutsuvan tilaajan tunnistusta tarjotaan, ja jos kutsuvan tilaajan tunnistus näkyy näytössä ennen puhelun yhdistymistä, palvelun tarjoajan on tarjottava vastaanottavalle tilaajalle mahdollisuus helposti kieltäytyä vastaanottamasta tulevia puheluja, jos soittava käyttäjä tai tilaaja on

estänyt kutsuvan tilaajan tunnistuksen. Jos yhdistetyn tilaajan tunnistusta tarjotaan, palvelun tarjoajan on tarjottava vastaanottavalle tilaajalle mahdollisuus helposti ja veloituksetta estää yhdistetyn tilaajan tunnistuksen näyttösoittajalle.

Jäsenvaltioiden on varmistettava, että tilaajat voivat helposti ja veloituksetta estää kolmannen suorittaman automaattisen soitonsiirron päätelaitteeseensa.

2.3.3.10 Laskutus ja puhelinluettelot

Tilaajilla on oltava oikeus saada laskunsa teleyrityksiltä erittelemättöminä. Jäsenvaltioiden on sovellettava kansallisia säännöksiä sovittaakseen yhteen toisaalta eriteltyjä laskuja saavien tilaajien oikeudet ja toisaalta soittavien käyttäjien ja vastaanottavien tilaajien oikeus yksityisyyteen, esimerkiksi varmistamalla, että tällaisille käyttäjille ja tilaajille on olemassa riittävästi vaihtoehtoisia, yksityisyyttä parantavia viestintä- tai maksutapoja. Tämän määräyksen ymmärtämiseksi voidaan esimerkkinä mainita tilanne, jossa tilaajana on työnantaja ja käyttäjänä työntekijä.

Direktiivin mukaan yhteisön kansalaisten on annettava ennalta suostumuksensa siihen, että heidän puhelinnumeronsa (kiinteän puhelimen tai matkapuhelimen), sähköpostiosoitteensa ja fyysinen osoitteensa voivat olla julkisissa luetteloissa.

2.3.4 Uudet määräykset teletunnistetietojen tallettamisesta

Tunnistamistietojen käyttöä rikostutkintaan on säännelty EU-tasolla vuoden 2006 alussa. Uuden säännöksen perusperiaatteet on käyty läpi kappaleessa 4.5 jäljempänä.

3. Sähköisten palvelujen tuottaminen

3.1 Direktiivi sähköisestä kaupankäynnistä 2000/31/EY

Direktiivillä luodaan keveät ja joustavat oikeudelliset puitteet sähköiselle kaupankäynnille ja siinä käsitellään vain niitä tekijöitä, jotka ovat ehdottomasti tarpeen sähköisen kaupankäynnin sisämarkkinoiden moitteettoman toiminnan varmistamiseksi. Direktiivi on laadittu teknologiselta kannalta katsottuna neutraalisti, jotta vältettäisiin tarve mukauttaa lainsäädäntöä jatkuvasti uuden kehityksen mukaisesti. Se kattaa monenlaisia sähköisesti tarjottavia palveluja (nk. ”tietoyhteiskunnan palveluja”), joihin sisältyvät esimerkiksi sähköiset sanomalehdet ja erikoistuneet uutispalvelut (esim. yritys- tai rahoitustietoja tarjoavat), erilaisten tuotteiden (esim. kirjojen, tietokonelaitteiden ja -ohjelmien, lääkkeiden) verkkomyynti ja rahoituspalvelujen (pankki- ja investointipalvelut) tarjoaminen Internetin kautta. Varsinkin viimeksi mainitut ovat tärkeitä, koska ne sopivat erityisen hyvin valtioiden rajat ylittävään palvelujen tarjoamiseen. Direktiiviä sovelletaan laaja-alaisesti kaikilla lainsäädännön aloilla, jotka liittyvät tietoyhteiskunnan palvelujen tarjoamiseen riippumatta siitä, onko kyseessä julkis-, yksityis- vai rikosoikeus. Lisäksi se soveltuu yhtä hyvin yritysten väliseen (B2B) kuin yritysten ja kuluttajien väliseen (B2C) sähköiseen kauppaan.

Direktiivin kulmakivenä on sisämarkkinalauseke, joka luo oikeusvarmuutta ja selkeyttä, jota tietoyhteiskunnan palvelujen tarjoajat tarvitsevat voidakseen tarjota palveluja kaikkialla yhteisössä. Välittäjien vastuuta koskevilla säännöksillä lisätään välityspalvelujen tarjoajien oikeusvarmuutta ja edistetään näin osaltaan perusvälityspalvelujen tarjontaa Internetissä.

Samalla tiedottamista ja avoimuutta koskevilla vaatimuksilla, kaupallista viestintää koskevilla säännöillä sekä sähköisiä sopimuksia koskevilla perusperiaatteilla asetetaan tiukat vaatimukset verkkokaupalle kaikissa jäsenvaltioissa. Näin myös parannetaan kuluttajien luottamusta.

Sähköiselle kaupankäynnille ominainen valtioiden rajat ylittävä toiminta edellyttää, että sen toimintaa koskevassa lainsäädännössä on tarjottava oikeusvarmuus sekä yrityksille että kuluttajille. Oikeusvarmuus toteutuu – muiden liitännäistoimenpiteiden ohella – direktiivin perustekijän, sisämarkkinalausekkeen ansiosta.

Tähän säännökseen sisältyy kaksi täydentävää tekijää: kunkin jäsenvaltion on varmistettava, että sen alueelle sijoittautunut tietoyhteiskunnan palvelujen tarjoaja noudattaa jäsenvaltiossa sovellettavia kansallisia säännöksiä, jotka kuuluvat ”yhteen

sovitetun alan” piiriin, myös silloin, kun hän tarjoaa palveluja toisessa jäsenvaltiossa. Vastaavasti jäsenvaltio ei saa rajoittaa vapautta tarjota tietoyhteiskunnan palveluja toisesta jäsenvaltiosta syistä, jotka kuuluvat yhteen sovitetun alan piiriin.

Sähköiselle kaupankäynnille ominainen valtioiden rajat ylittävä toiminta edellyttää, että sen toimintaa koskevassa lainsäädännössä on tarjottava oikeusvarmuus sekä yrityksille että kuluttajille. Oikeusvarmuus toteutuu – muiden liitännäistoimenpiteiden ohella – direktiivin perustekijän, sisämarkkinalausekkeen ansiosta.

Tähän säännökseen sisältyy kaksi täydentävää tekijää: kunkin jäsenvaltion on varmistettava, että sen alueelle sijoittautunut tietoyhteiskunnan palvelujen tarjoaja noudattaa jäsenvaltiossa sovellettavia kansallisia säännöksiä, jotka kuuluvat yhteen sovitetun alan piiriin, myös silloin, kun hän tarjoaa palveluja toisessa jäsenvaltiossa. Vastaavasti jäsenvaltio ei saa rajoittaa vapautta tarjota tietoyhteiskunnan palveluja toisesta jäsenvaltiosta syistä, jotka kuuluvat yhteen sovitetun alan piiriin.

Sisämarkkinalausekkeeseen voidaan soveltaa joitakin rajoitettuja poikkeuksia, jotka esitetään direktiivin liitteessä. Sisämarkkinalausekkeesta voidaan myös poiketa tapauskohtaisesti, ja jäsenvaltiot voivat hyödyntää tätä toteuttaakseen toimenpiteitä, kuten seuraamuksia tai kieltoja, joilla rajoitetaan tietyn Internet-palvelun tarjontaa toisesta jäsenvaltiosta, jos on tarpeen suojella tiettyjä, esimerkiksi kuluttajien etuja. Kaikkiin jäsenvaltioiden tämän säännöksen nojalla toteuttamiin toimenpiteisiin on sovellettava tiukasti 3. artiklan 4.–6. kohdan mukaisia ehtoja.

Koska direktiivin 4. artiklan 1. kohdassa kielletään jäsenvaltioita asettamasta ennakkolupaa (tai vaikutukseltaan vastaavaa vaatimusta) tietoyhteiskunnan palvelun tarjoajan toiminnan aloittamisen tai jatkamisen edellytykseksi, lupajärjestelmää ei ole olemassa missään jäsenvaltiossa. Ne jäsenvaltiot, joissa oli harkittu tällaisten järjestelmien käyttöönottoa kaikkien tai joidenkin tietoyhteiskunnan palvelujen osalta, jättivät sen tekemättä ja joissakin tapauksissa lakkauttivat voimassa olleet lupavaatimukset. Näin on varmistettu, että sijoittautuminen tietoyhteiskunnan palvelujen tarjoajaksi jäsenvaltioon on helppoa eikä sille ole byrokraattisia esteitä.

Direktiivin 5. artiklalla sitä vastoin varmistetaan palvelun tarjoajan henkilöllisyyttä ja sijoittautumispaikkaa koskevien tietojen avoimuus ja parempi saanti. Siinä muun muassa vaaditaan, että palvelun tarjoajasta annetaan nimi, maantieteellinen osoite, yhteystiedot, jotka mahdollistavat nopean yhteydenoton, sekä tätä koskevat kaupparekisterissä tai muussa vastaavassa julkisessa rekisterissä olevat tiedot. Artikla on pantu lähes sanasanaisesti täytäntöön useimpien jäsenvaltioiden ja ETA-maiden lainsäädännössä.

Direktiivillä täydennetään nykyisiä kuluttajansuojaa koskevia direktiivejä esimerkiksi lisäämällä yhteisön lainsäädäntöön avoimuutta koskeva vaatimus, jota on noudatettava Internetissä julkaistavassa kaupallisessa viestinnässä, myös alennuksissa, tarjouksissa, kilpailuissa ja peleissä. Näillä vaatimuksilla parannetaan kuluttajansuojaa ja kuluttajien luottamusta verkkokauppaan, ja niitä täydennetään vielä ehdotetulla asetuksella myynninedistämisestä sisämarkkinoilla ja ehdotetulla direktiivillä sopimattomista elinkeinonharjoittajien ja kuluttajien välisistä kaupallisista menettelyistä sisämarkkinoilla sekä ehdotetulla asetuksella yhteistyöstä täytäntöönpanoasioissa. Lisäksi direktiivin 6. artiklan a-alakohdan vaatimus yksilöidä selkeästi kaupallinen viestintä vastaa rajatonta televisiotoimintaa koskevan direktiivin 10. artiklan 1. kohdassa televisiolähetyksiin sovellettavaa vaatimusta. Käytännössä kaikki jäsenvaltiot saattoivat 6. artiklan a-alakohdan osaksi kansallista lainsäädäntöä lähes kirjaimellisesti.

Direktiivissä jätettiin jäsenvaltioille mahdollisuus sallia tai kieltää niiden alueelle sijoittuneiden tietoyhteiskunnan palvelujen tarjoajien harjoittama ei-toivottu kaupallinen viestintä sähköpostin kautta ja direktiivissä vaadittiin vain, että tällaiset ei-toivotut viestit on pystyttävä tunnistamaan selvästi.

Ei-toivotusta kaupallisesta viestinnästä on kuitenkin tullut yhä suurempi ongelma kuluttajille ja yrityksille. Tämän vuoksi asiaa on nyt käsitelty yhteisön tasolla sähköisen viestinnän tietosuojadirektiivissä 2002/58/EY, jossa sallitaan ei-toivottujen kaupallisten viestien lähettäminen sähköpostitse vain vastaanottajan ennalta antaman suostumuksen jälkeen, kun vastaanottaja on luonnollinen henkilö tai kun kyseessä on vakiintunut kauppasuhde. Lisäksi komissio on käynnistänyt täydentäviä toimenpiteitä koskevia toimia, jotka liittyvät erityisesti ei-toivotun kaupallisen viestinnän teknisiin ja kansainvälisiin näkökohtiin. Jälkimmäisessä tapauksessa komissio keskittää pyrkimyksensä kansainväliseen yhteistyöhön torjuakseen ei-toivottuja viestejä, joista suurin osa on peräisin EU:n ulkopuolelta.

Direktiivissä velvoitetaan jäsenvaltiot varmistamaan, että säänneltyjen ammattien harjoittajat voivat käyttää sähköistä kaupallista viestintää, jos se on erityisesti ammatin riippumattomuutta, kunniaa ja arvoa koskevien ammattisääntöjen mukaista. Tämä tarkoittaa sitä, että säännellyn ammatin harjoittajat voivat tarjota tietoa asiakkaille verkkosivuilla, mikä ei ollut aiemmin mahdollista useissakaan jäsenvaltioissa. Monien jäsenvaltioiden täytäntöönpanolainsäädännössä vahvistetaan nimenomaisesti periaate, jonka mukaan säänneltyjen ammattien harjoittajat saavat mainostaa Internetissä 8. artiklan 1. kohdan edellytysten mukaisesti.

Euroopan tasolla säänneltyjä ammatteja edustavat järjestöt ovat ottaneet myönteisesti vastaan direktiivissä esitetyn kehotuksen kehittää käytännesääntöjä, jotka liittyvät kaupallisen viestinnän käyttöön. Tilintarkastajat, lakimiehet, lääkärit, farmaseutit ja

kiinteistönvälittäjät ovat laatineet Euroopan tasoisia käytännesääntöjä, joissa käsitellään nimenomaan sähköistä kaupallista viestintää. Joissakin käytännesäännöissä käsitellään pelkästään Internetissä tapahtuvaa kaupallista viestintää, toiset taas kattavat laajemman valikoiman Internet-pohjaisia palveluja. Yhteistä kaikille käytännesäännöille on se, että niissä korostetaan velvoitetta antaa tarkkoja ja todenmukaisia tietoja ja pidättäytyä mainonnasta, joka on ”ylikaupallista”, jotta säilytetään ammattikunnan arvokkuus.

Direktiivissä on kolme säännöstä, jotka koskevat sähköisesti tehtäviä sopimuksia. Tärkein näistä on jäsenvaltioiden velvoite huolehtia siitä, että niiden oikeusjärjestelmässä annetaan mahdollisuus sopimusten tekemiseen sähköisessä muodossa (ks. 9. artiklan 1. kohta). Tämä säännös itse asiassa edellyttää sitä, että jäsenvaltiot tarkastelevat kansallista lainsäädäntöään ja poistavat sieltä säännökset, jotka saattavat estää sopimusten tekemisen sähköisessä muodossa. Monet jäsenvaltiot ovat sisällyttäneet lainsäädäntöönsä yleislausekkeen, jonka mukaan sähköisessä muodossa tehdyillä sopimuksilla ja sopimusoikeudellisella kirjeenvaihdolla on sama oikeudellinen vaikutus kuin perinteisemmin keinoin tehdyillä toimilla. Suomen osalta tällainen määräys koskee niitä harvoja sopimuksia, jotka lain mukaan on tehtävä kirjallisesti.

Direktiivin säännöksiä täydentävät sähköisistä allekirjoituksista annetun direktiivin 1999/93/ETY säännökset, joilla pyritään varmistamaan, että sähköiset allekirjoitukset tunnustetaan oikeudellisesti velvoittaviksi, jolloin mahdollistetaan perinteisesti paperilla tehtävien ja sähköisesti tehtävien sopimusten toiminnallinen vastaavuus. Etenkin direktiivin 1999/93 5. artiklan 1. kohdassa annetaan "hyväksyttyyn varmenteeseen" perustuvalle sähköiselle allekirjoitukselle, joka liittyy sähköisessä muodossa olevaan tietoon, sama asema kuin paperilla olevaan tietoon käsin kirjoitetulle allekirjoitukselle. Direktiivin 1999/93 5. artiklan 2. kohdassa säädetään kuitenkin, että sähköiseltä allekirjoitukselta ei voida evätä oikeudellista vaikutusta ja hyväksyttävyyttä todisteena oikeudellisissa menettelyissä yksinomaan sen vuoksi, että allekirjoitus on sähköisessä muodossa tai se ei perustu hyväksyttyyn varmenteeseen.

Direktiivin 12.–14. artiklassa annetaan täsmällisesti määritellyt rajoitukset välittäjinä toimivien palvelun tarjoajien vastuusta, kun niiden tarjoamia palveluja ovat vain siirtotoiminta, tallentaminen ja säilytys. Direktiivissä säädettyjä vastuuta koskevia rajoituksia sovelletaan tiettyihin selvästi rajattuihin toimiin, joita Internet-välittäjät harjoittavat eikä palveluiden tarjoajien eri luokkiin tai tiedon eri lajeihin. Direktiivissä säädetyt vastuuta koskevat rajoitukset on vahvistettu horisontaalisesti eli ne kattavat sekä siviili- että rikosoikeudellisen vastuun kolmansien osapuolien toteuttamien kaikentyyppisten laittomien toimien osalta.

Direktiivi ei vaikuta sellaisen henkilön vastuuseen, joka toimii sisällön lähteenä eikä se vaikuta välittäjien vastuuseen tapauksissa, jotka eivät kuulu direktiivissä määriteltyjen rajoitusten piiriin. Direktiivi ei myöskään vaikuta kansallisen tuomioistuimen tai viranomaisen mahdollisuuteen vaatia palvelun tarjoajaa lopettamaan lainvastainen toiminta tai ehkäistä se. Nämä kysymykset on ratkaistava jäsenvaltioiden kansallisessa lainsäädännössä.

Direktiivissä säädettyjä välittäjien vastuuta koskevia rajoituksia pidettiin välttämättöminä, jotta voitaisiin taata peruspalvelujen tarjonta, joka takaa tiedon jatkuvan ilmaisen virran verkossa, ja tarjota puitteet, jotka mahdollistavat Internetin ja sähköisen kaupankäynnin kehittymisen. Jäsenvaltioiden lainsäädännön ja oikeuskäytännön eroavaisuudet ja niistä seuraava oikeudellinen epävarmuus rajat ylittävissä toimissa uhkasivat luoda esteitä palvelujen vapaalle tarjonnalle valtioiden välillä. Yhteisön tason toimet rajoitettiin kuitenkin niihin, joita pidettiin välttämättöminä estämään tällaisen riskin toteutuminen.

Direktiivin 12.–14. artiklassa säädetään yhdenmukaistamisesta niissä tapauksissa, joissa artikloissa tarkoitettuja, välittäjinä toimivia palvelujen tarjoajia ei voida pitää vastuullisina. Jäsenvaltiot eivät voi asettaa lisäedellytyksiä, jotka välittävän palvelun on täytettävä, ennen kuin siihen voidaan soveltaa vastuuta koskevia rajoituksia. Monissa jäsenvaltioissa päätettiin panna 12.–14. artikla täytäntöön lähes sanasanaisesti.

Direktiivin 12.–14. artiklassa käsiteltyjen seikkojen lisäksi jotkin jäsenvaltiot ovat päättäneet säätää hyperlinkkien ja hakukoneiden tarjoajien vastuuta koskevista rajoituksista. Perusteena on ollut luoda kannustimia investointeja ja innovaatiotoimintaa varten ja lujittaa sähköisen kaupankäynnin kehittämistä parantamalla palvelun tarjoajien oikeudellisen tilanteen selkeyttä. Direktiivissä ei pidetty tarpeellisena käsitellä hyperlinkkejä ja hakukoneita, mutta komissio on kannustanut jäsenvaltioita kehittämään Internet-välittäjien oikeusturvaa edelleen. On rohkaisevaa, että jäsenvaltioiden tuoreessa oikeuskäytännössä tunnustetaan linkkien ja hakukoneiden merkitys Internetin toiminnalle. Tämä oikeuskäytäntö näyttää pääosin noudattavan sisämarkkinatavoitetta varmistaa perusverkkopalvelujen tarjonta, jolla edistetään Internetin ja sähköisen kaupan kehitystä. Näin ollen mainittu oikeuskäytäntö ei näytä aiheuttavan sisämarkkinoihin liittyviä ongelmia.

Direktiivin 15 artiklassa kielletään, että jäsenvaltiot eivät saa asettaa palvelun tarjoajille 12.–14. artiklassa tarkoitettujen palvelujen toimittamisen osalta yleistä velvoitetta valvoa siirtämiään ja tallentamiaan tietoja tai yleistä velvoitetta pyrkiä aktiivisesti saamaan selville laitonta toimintaa osoittavia tosiasioita tai olosuhteita. Tämä on tärkeää, koska miljoonien verkkosivujen yleinen valvonta olisi käytännössä mahdotonta. Edellytykset, joilla Internet-palvelinpalvelujen tarjoaja voidaan vapauttaa

vastuusta 14. artiklan 1. kohdan b-alakohdan mukaisesti, muodostavat perustan laittoman ja haitallisen tiedon ilmoitus- ja poistamismenettelyiden kehittämiselle. Direktiivin 14. artiklaa sovelletaan horisontaalisesti kaikentyyppiseen tietoon. Kun direktiivi hyväksyttiin, sovittiin, että ilmoitus- ja poistamismenettelyjä ei pitäisi säännellä direktiivillä. Direktiivin 16. artiklassa ja johdanto-osan 40. kappaleessa nimenomaisesti kannustetaan itsesääntelytoimiin direktiivin soveltamisalalla.

Sähköisen kaupankäynnin mukanaan tuoma mahdollisuuksien lisääntyminen ja maantieteellisen kattavuuden laajentuminen voi myös aiheuttaa valtioiden rajat ylittäviä riitoja kauppakumppaneiden välille. Tällaisissa tapauksissa on ratkaisevan tärkeää, että käytettävissä on nopeita ja joustavia tuomioistuinten ulkopuolisia riitojen ratkaisumenettelyjä. Tästä syystä direktiivissä velvoitetaan jäsenvaltiot mahdollistamaan sähköisesti käytettävien tuomioistuinten ulkopuolisten riitojen ratkaisumenettelyjen kehittäminen ja kannustamaan tällaisten menettelyjen kehittämistä. Viime vuosina on ollut runsaasti aloitteita, jotka koskevat tuomioistuinten ulkopuolisia riitojen ratkaisumenettelyjä ja ne ovat usein liittyneet käytännesääntöihin.

3.2 Muita sähköistä liiketoimintaa koskevia säädöksiä

3.2.1 Etämyyntidirektiivit

Etämyynnin kuluttajaoikeudellisten kysymysten sääntelemiseksi on annettu kaksi keskeistä direktiiviä. Säännökset ovat lähinnä kuluttajaoikeudellisia ja sopimusoikeuteen liittyviä, mutta joitakin sähköisten palvelujen tuottamisen kannalta keskeisiä, tietoturvaa ja tietosuojaa sivuavia kohtia voidaan nostaa esille.

Etämyyntidirektiivi[22] sääntelee etäsopimuksia eli elinkeinonharjoittajan ja kuluttajan välisiä, tavaraa tai palvelua koskevaa sopimusta, joka tehdään elinkeinonharjoittajan järjestämän sellaisen etämyynti- tai palvelutarjontamenetelmän avulla, jossa käytetään yksinomaan yhtä tai useampaa etäviestintävälinettä sopimuksen tekemiseen asti, mukaan lukien sopimuksen tekeminen.

Direktiivin 4. artiklassa säädetään kuluttajille ennen sopimuksen tekoa annettavista ennakkotiedoista hinnan ja muiden relevanttien tekijöiden suhteen. Menemättä yksityiskohtiin kaikista tiedoista voidaan kuitenkin mainita, että nämä tiedot, joiden kaupallisesta tarkoituksesta ei saa olla epäselvyyttä, on annettava selkeinä ja

[22] Euroopan parlamentin ja neuvoston direktiivi 97/7/EY, annettu 20. toukokuuta 1997, kuluttajansuojasta etäsopimuksissa, EYVL L 144, 4.6.1999, s. 19.

ymmärrettävinä käytettyyn etäviestintävälineeseen soveltuvalla tavalla ja noudattaen erityisesti hyvää kauppatapaa sekä periaatteita, joilla suojellaan niitä henkilöitä, kuten alaikäisiä, jotka jäsenvaltioiden lainsäädännön mukaan eivät ole oikeustoimikelpoisia. Lisäksi puhelimitse tapahtuvissa yhteyksissä elinkeinonharjoittajan henkilöllisyys ja soiton kaupallinen tarkoitus on tehtävä täsmällisesti selväksi aina kuluttajan kanssa käytävän keskustelun alussa.

Direktiivin 5. artiklan mukaan kuluttajan on saatava kirjallinen vahvistus tai vahvistus muulla kuluttajan saatavissa ja käytettävissä olevalla pysyvällä tavalla em. tiedoista hyvissä ajoin sopimuksen täyttämisen kuluessa ja tavaroita toimitettaessa viimeistään tavaran luovutushetkellä paitsi, jos kyse on tavaran toimittamisesta kolmannelle. Vahvistusta ei tarvita, jos tiedot on jo ennen sopimuksen tekemistä toimitettu kuluttajalle kirjallisina tai muulla kuluttajan saatavissa ja käytettävissä olevalla pysyvällä tavalla.

Rahoituspalvelujen etämyyntidirektiivi[23], jolla säännellään kuluttajansuojaa rahoituspalvelujen myynnissä etämyyntivälineitä käytettäessä, sääntelee myös yksityiselämän suojaan kuuluvia kysymyksiä. Direktiivin 10. artikla suojaa kuluttajia niiltä yhteydenotoilta, joita he eivät halua pankki-, luotto-, vakuutus-, yksilöllisiä eläkejärjestely-, sijoitus- tai maksupalvelua tarjoavilta palvelujen tarjoajilta. Direktiivin 10. artiklassa säädetään kuluttajalta tarvittavasta, kuluttajan ennakolta antamasta suostumuksesta, kun palvelujen tarjoaja käyttää yhteydenotossaan automaattisia soittojärjestelmiä, telekopiolaitteita sekä muita etäviestintävälineitä.

3.2.2 Maksuliikenne ja rahanpesun estäminen

Yksi tietoturvan ja rikollisuuden torjunnan kannalta keskeisimmistä alueista on maksuliikennettä ja rahanpesua koskeva lainsäädäntö. Maksuliikenteeseen liittyvät transaktiot edellyttävät nimittäin normaaleista kaupallisista transaktioista poiketen maksajan henkilöllisyyden toteamista ja sitä koskevien tietojen liittämistä transaktioon.

Tilisiirtoja koskevan sääntelyjärjestelmän osalta keskeinen on Euroopan parlamentin ja neuvoston direktiivi 97/5/EY rajojen yli suoritettavista tilisiirroista, jolla helpotetaan ulkomaan tilisiirtoja säätämällä yhteisistä vaatimuksista, joilla suojellaan asiakkaita.

Maksuliikennettä koskevaan lainsäädäntöön on sittemmin lisätty asetus 2560/2001/EY rajat ylittävistä maksuista. Näitä ovat rajat ylittävät tilisiirrot, sähköiset rajat ylittävät

---

[23] Euroopan parlamentin ja neuvoston direktiivi 2002/65/EY, annettu 23. syyskuuta 2002, kuluttajille tarkoitettujen rahoituspalvelujen etämyynnistä, EYVL L 271, 9.10.2002, s. 16.

maksutapahtumat ja rajat ylittävät sekit. Asetuksella poistettiin ulkomaan ja kotimaan maksujen hintaero. Tämä asetus on tehnyt monenlaiset euromääräiset maksut sisämarkkinoilla asiakkaille helpommiksi ja halvemmiksi ja polkaissut käyntiin alan hankkeen yhtenäisen euromaksualueen (SEPA) luomiseksi.

On lisäksi olemassa suositus (97/489/EY) elektronisen maksuvälineen avulla toteutetuista maksutapahtumista ja erityisesti liikkeeseenlaskijan ja haltijan välisestä suhteesta, jolla on tarkoitus suojata elektronisia maksuvälineitä kuten maksukortteja käyttäviä asiakkaita.[24]

Sähköisestä rahasta on laadittu direktiivi 2000/46/EY, jonka soveltaminen ei ole kuitenkaan kaikilta osin vastannut direktiivin tavoitteita.

Ns. etämyyntidirektiivin 8. artikla sisältää määräyksiä korttimaksuista. Sen mukaan jäsenvaltioiden on huolehdittava siitä, että on olemassa asianmukaiset toimenpiteet, joilla kuluttaja voi pyytää maksun peruuttamista, jos hänen maksukorttiaan on käytetty väärin direktiivin alaan kuuluvissa etäsopimuksissa ja jos on tapahtunut väärinkäytös, saada hyvityksen maksamistaan maksuista tai niiden palautuksen.

Maksujärjestelmän uudistamiseksi on viime vuoden lopulla tehty kattava komission ehdotus.[25] Sen mukaan maksupalveluntarjoajan olisi voitava määrittää yksiselitteisesti tiedot, jotka se vaatii voidakseen toteuttaa maksutoimeksiannon. Jotta voitaisiin välttää epäyhtenäisyyttä eikä vaarannettaisi yhdennettyjen maksujärjestelmien perustamista yhteisöön, jäsenvaltiot eivät toisaalta saisi kuitenkaan edellyttää, että maksutapahtumissa käytetään juuri tiettyä tunnistetta. Maksupalveluntarjoajan ankara vastuu olisi rajoitettava maksutapahtuman toteuttamiseen oikein maksupalvelunkäyttäjän maksutoimeksiannon mukaisesti.

Jotta olisi mahdollista ehkäistä petoksia tehokkaasti ja torjua maksupetoksia kaikkialla yhteisössä, olisi säädettävä tehokkaasta tietojenvaihdosta maksupalveluntarjoajien välillä. Palveluntarjoajien olisi saatava kerätä, käsitellä ja vaihtaa maksupetoksiin osallisten henkilöiden henkilötietoja. Tässä toiminnassa olisi noudatettava henkilötietodirektiiviä 95/46/EY.

---

[24] Muita suosituksia ovat rahoituslaitosten, tavara- ja palvelukauppaa harjoittavien yritysten ja kuluttajien suhteet kattava annettu komission suositus 87/598/ETY sekä maksujärjestelmistä ja erityisesti kortin haltijan ja kortin myöntäjän välisestä suhteesta annettu komission suositus 88/590/ETY.

[25] Ehdotus Euroopan parlamentin ja neuvoston direktiivi maksupalveluista sisämarkkinoilla ja direktiivien 97/7/EY, 2000/12/EY ja 2002/65/EY muuttamisesta. KOM (2005) 603 lopullinen.

Tällä hetkellä vireillä on myös sääntelyehdotus[26] **maksajaa koskevien tietojen toimittamisesta varainsiirtojen mukana**. Asetusehdotuksessa vahvistetaan säännöt, joiden avulla varainsiirrot voidaan jäljittää, ja joita sovelletaan kaikkiin maksupalvelujen tarjoajiin, jotka osallistuvat maksutapahtumaan jossain vaiheessa. Asetusehdotuksen tavoitteena on saattaa rahanpesunvastaisen toimintatyöryhmän (FATF) sähköisistä maksusuorituksista antama erityissuositus VII osaksi yhteisön lainsäädäntöä. FATF on hallitustenvälinen elin, jonka tavoitteena on laatia ja edistää strategioita rahanpesun ja terrorismin rahoituksen torjumiseksi niin kansallisella kuin kansainväliselläkin tasolla.

Ehdotuksen mukaan maksajan käyttämän maksupalvelujen tarjoajan tulee valvoa sitä, että varainsiirroissa on täydelliset, tarkat ja tarpeelliset tiedot maksajasta. Maksajaa koskevilla täydellisillä tiedoilla tarkoitetaan maksajan nimeä, osoitetta ja tilinumeroa. Osoitteen sijasta voidaan ilmoittaa maksajan syntymäaika ja -paikka, asiakasnumero tai kansallinen henkilötunnus. Tapauksissa, joissa sekä maksajan käyttämä maksupalvelujen tarjoaja että maksunsaajan käyttämä maksupalvelujen tarjoaja on sijoittautunut yhteisön ulkopuolelle, varainsiirtojen mukana on toimitettava ainoastaan maksajan tilinumero tai yksilöllinen tunniste, jonka avulla siirto voidaan jäljittää takaisin maksajaan.

Jos maksunsaajan käyttämä maksupalvelujen tarjoaja kuitenkin sitä pyytää, maksajan käyttämän maksupalvelujen tarjoajan on toimitettava tälle täydelliset tiedot maksajasta kolmen työpäivän kuluessa pyynnön vastaanottamisesta. Yhteisön alueelta yhteisön ulkopuolella oleville maksunsaajille tehtävien varainsiirtojen mukana on toimitettava täydelliset tiedot maksajasta.

Maksunsaajan maksupalvelujen tarjoajien tulee ilmoittaa epäilyttävistä maksutapahtumista rahanpesun ja terrorismin rahoituksen torjunnasta vastaaville viranomaisille. Maksunsaajan käyttämän maksupalvelujen tarjoajan on säilytettävä vastaanottamansa maksajaa koskevat tiedot viisi vuotta.

Rahanpesun ehkäisemistä varten on säädetty ns. kolmas rahanpesudirektiivi[27], joka on pantava täytäntöön vuoden 2007 joulukuussa. Aikaisempi direktiivi[28] on vuodelta 1991 ja siinä säädettiin asiakkaan tunnistamisvelvollisuudesta, mutta se sisälsi suhteellisen vähän säännöksiä tätä koskevien menettelyjen yksityiskohdista.

---

[26] Ehdotus: Euroopan parlamentin ja neuvoston asetus, maksajaa koskevien tietojen toimittamisesta varainsiirtojen mukana, KOM(2005) 343 lopullinen.

[27] Euroopan parlamentin ja neuvoston direktiivi 2005/60/EY, annettu 26. päivänä lokakuuta 2005, rahoitusjärjestelmän käytön estämisestä rahanpesutarkoituksiin sekä terrorismin rahoitukseen, EYVL L 309, 25.11.2005.

[28] Neuvoston direktiivi 91/308/ETY.

Uusi, kolmas rahanpesudirektiivi on sen sijaan varsin seikkaperäinen tunnistamisvaatimusten suhteen. Asiakkaan ja todellisen omistajan ja edunsaajan henkilöllisyys todennetaan ennen liikesuhteen aloittamista tai liiketoimen suorittamista. Jäsenvaltioiden on kiellettävä luotto- ja rahoituslaitoksia ylläpitämästä anonyymejä tilejä tai anonyymejä haltijavastakirjoja. Asiakkaan tuntemisvelvollisuus jaetaan kolmeen luokkaan; tavalliseen, tehostettuun tai yksinkertaistettuun sen mukaan, mikä niissä on rahanpesun tai terrorismin rahoituksen riski. Tätä riskiä arvioitaessa tulee ottaa huomioon itse asiakas, liikesuhde, tuote sekä liiketoimi. Asiakkaan tunnistaminen ja tämän henkilöllisyyden todentaminen tapahtuu luotettavasta ja riippumattomasta lähteestä peräisin olevien asiakirjojen tai tietojen perusteella. Direktiivi mahdollistaa ns. etätunnistuksen, mutta tehostetun tunnistamisvelvollisuuden ollessa kyseessä edellytetään myös lisätoimenpiteitä.

3.2.3 Hankintadirektiivit

Euroopan parlamentti ja neuvosto hyväksyivät vuonna 2004 kaksi direktiiviä[29], jolla julkisten hankintojen sääntelyjärjestelmää saatettiin ajan tasalle. Monista direktiivien uudistuksista voidaan todeta, että direktiiveillä mahdollistetaan sähköinen hankintatoimi. Direktiivit sisältävät tähän liittyviä määräyksiä mm. ilmoitusmenettelyistä ja määräajoista. Direktiivin mukaan jäsenvaltiot voivat halutessaan ottaa käyttöön sähköiset huutokaupat sekä ns. dynaamiset hankintamenettelyt. Direktiivit eivät sisällä ehdottomia määräyksiä sähköisistä allekirjoituksista, mutta jäsenvaltiot voivat tässä suhteessa asettaa hankintayksiköille omia vaatimuksiaan.

3.3 Tietoliikennesäännökset

Euroopan Unionissa on tietoliikennepalvelut vapautettu moniosaisella lainsäädäntöpaketilla. Tähän pakettiin kuuluvat ns. käyttöoikeusdirektiivi[30], ns. valtuutusdirektiivi[31],

---

[29] Euroopan Parlamentin ja Neuvoston direktiivi 2004/18/EY, annettu 31 päivänä maaliskuuta 2004, julkisia rakennusurakoita sekä julkisia tavara- ja palveluhankintoja koskevien sopimusten tekomenettelyjen yhteensovittamisesta, EYVL L 134, 30.4.2004, s. 114; ja Euroopan parlamentin ja neuvoston direktiivi 2004/17/EY, annettu 31. päivänä maaliskuuta 2004, vesi- ja energiahuollon sekä liikenteen ja postipalvelujen alalla toimivien yksiköiden hankintamenettelyjen yhteensovittamisesta, EYVL L 134, 30.4.2004, s. 1.

Direktiivien mukaan jäsenvaltioiden oli saatettava ne osaksi lainsäädäntöään 31. tammikuuta 2006 mennessä. Monissa maissa, mm. Suomessa tämä on kuitenkin viivästynyt.

[30] Euroopan parlamentin ja neuvoston direktiivi 2002/19/EY, annettu 7. päivänä maaliskuuta 2002, sähköisten viestintäverkkojen ja niiden liitännäistoimintojen käyttöoikeuksista ja yhteen liittämisestä.

[31] Euroopan parlamentin ja neuvoston direktiivi 2002/20/EY, annettu 7. päivänä maaliskuuta 2002, sähköisiä viestintäverkkoja ja -palveluja koskevista valtuutuksista.

ns. puitedirektiivi[32] sekä ns. yleispalveludirektiivi[33]. Samassa yhteydessä on säädetty myös sähköisen viestinnän tietosuojadirektiivi, joka on monissa maissa implementoitu samalla säädöksellä em. tietoliikennettä koskevien direktiivien kanssa. Tässä yhteydessä ei ole syytä selvittää tarkemmin markkinadirektiivien sisältöä, vaikka niillä voi luonnollisesti olla vaikutuksia myös tietoturvapalvelujen tarjonnassa muiden tietoliikennepalvelujen yhteydessä.

3.4 Tekijänoikeudet ja verkkotunnukset

Tietoturvallisuuden ja tekijänoikeuksien tavoitteet poikkeavat toisistaan, sillä tietoturvallisuudella pyritään turvaamaan tiedon luottamuksellisuutta ja suojaamaan tietojärjestelmiä. Tekijänoikeuksilla ja niiden lähioikeuksilla taas turvataan kaupallisia ja moraalisia oikeuksia. Kun kyse on sähköisestä tiedosta, tekniset suojauskeinot ja pakkokeinot kuitenkin muistuttavat toisiaan. Tekijänoikeuden loukkaukset ovat osa tietoverkkorikollisuutta.

EU:n tekijänoikeusdirektiivi[34] luo järjestelmän tekijänoikeuksien suojaamiselle tietoyhteiskunnassa. Direktiivin 6. artiklan mukaan jäsenvaltioiden on säädettävä riittävästä oikeudellisesta suojasta tehokkaiden teknisten toimenpiteiden kiertämistä vastaan, jos asianomainen teon suorittaja on tiennyt tai hänellä on ollut perusteltu aihe tietää toimintansa tarkoittavan kiertämistä.

Direktiivissä tarkoitetaan teknisillä toimenpiteillä tekniikoita, laitteita tai osia, jotka on suunniteltu normaalissa käyttötarkoituksessa estämään tai rajoittamaan teoksiin tai muuhun aineistoon kohdistuvia tekoja, joihin ei ole saatu lupaa laissa säädettyjen tekijänoikeuden tai tekijänoikeuden lähioikeuksien haltijalta tai direktiivissä tarkoitetun *sui generis* -oikeuden haltijalta. Teknisiä toimenpiteitä pidetään tehokkaina, jos oikeudenhaltijat valvovat suojatun teoksen tai muun aineiston käyttöä jonkin sellaisen pääsynvalvontatoimen tai suojauskeinon avulla, jolla tavoiteltu suoja saavutetaan, ja joita ovat esimerkiksi teoksen tai muun aineiston salaus, muuntaminen tai muunlainen muuttaminen taikka kopioinnin valvontajärjestelmä.

---

[32] Euroopan parlamentin ja neuvoston direktiivi 2002/21/EY, annettu 7. päivänä maaliskuuta 2002, sähköisten viestintäverkkojen ja -palvelujen yhteisestä sääntelyjärjestelmästä.

[33] Euroopan parlamentin ja neuvoston direktiivi 2002/22/EY, annettu 7. päivänä maaliskuuta 2002, yleispalvelusta ja käyttäjien oikeuksista sähköisten viestintäverkkojen ja -palvelujen alalla.

[34] Euroopan parlamentin ja neuvoston direktiivi 2001/29/EY, annettu 22. päivänä toukokuuta 2001, tekijänoikeuden ja lähioikeuksien tiettyjen piirteiden yhdenmukaistamisesta tietoyhteiskunnassa.

Jäsenvaltioiden on säädettävä tässä direktiivissä säädettyjen oikeuksien ja velvollisuuksien loukkauksia koskevista asianmukaisista seuraamuksista ja oikeussuojakeinoista, ja niiden on toteutettava tarvittavat toimenpiteet varmistaakseen, että näitä seuraamuksia ja oikeussuojakeinoja sovelletaan. Näin säädettyjen seuraamusten on oltava tehokkaita, oikeasuhteisia ja vaikuttavia.

Kunkin jäsenvaltion on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että oikeudenhaltijat, joiden etuihin sen alueella suoritetut loukkaavat toimet vaikuttavat, voivat nostaa vahingonkorvauskanteen ja/tai hakea kieltoa tai määräystä ja tarvittaessa loukkaavan aineiston sekä 6. artiklan 2. kohdassa tarkoitettujen laitteiden, tuotteiden tai osien takavarikointia.

Jäsenvaltioiden on varmistettava, että oikeudenhaltijoilla on mahdollisuus hakea kieltoa tai määräystä sellaisia välittäjiä vastaan, joiden palveluja kolmas osapuoli käyttää tekijänoikeuden tai lähioikeuden rikkomiseen.

GATT-järjestelmän TRIPS-sopimus sisältää myös tekijänoikeudellisia säännöksiä ja mm. mahdollisuuden takavarikoida laittomia tuotteita.

EU on ottanut käyttöön oman ”.eu”-päätteisen verkkotunnuksen. Tästä on säädetty Euroopan parlamentin ja neuvoston asetuksessa[35] ja komission päätöksellä on Brysselissä toimiva *European Registry for Internet Domains* (EURID) nimetty eu-aluetunnusrekisteriksi, jonka tehtäväksi on annettu ”.eu”-aluetunnuksen organisointi, hallinto ja ylläpito.

3.5 Sähköiset allekirjoitukset ja tunnistaminen

3.5.1 Direktiivi 1999/93/EY

Sähköisiä allekirjoituksia koskeva lainsäädäntö tuntee kaksi suuntausta. Liberaalimpi kulttuuri sääntelee vain allekirjoituksen vaikutukset jättäen allekirjoituksen teknisen toteutuksen sääntelemättä. Toinen suuntaus on selvästi teknologiasuuntautunut. Eurooppalainen järjestelmä jää näiden kahden muodon väliin.

EU-direktiivin tarkoituksena on luoda yhteisön puitteet sähköisille allekirjoituksille, tarjota allekirjoitustuotteille ja -palveluille vapaa liikkuvuus sekä turvata sähköisten allekirjoitusten oikeudellinen tunnustaminen. Direktiivi ei sääntele sopimusten muoto-

[35] Euroopan parlamentin ja neuvoston asetus (EY) N:o 733/2002, annettu 22. päivänä huhtikuuta 2002, aluetunnuksen ".eu" perustamisesta.

vaatimuksia eikä pätevyyttä. Suljetun järjestelmän osallisilla on oikeus neuvotella erityisehdot sähköisten allekirjoitusten käytölle tässä järjestelmässä.

Direktiivi tuntee kolmentyyppisiä sähköisiä allekirjoituksia. Yksinkertainen **sähköinen allekirjoitus** tunnistaa tiedon ja yksilöi sen alkuperän. Tällainen allekirjoitus voi olla sähköpostin lopussa oleva henkilön nimi tai PIN-tunnus. Alkuperän yksilöinnin on liityttävä tietoon eikä vain yksikköön. Toinen sähköisen allekirjoituksen muoto on **kehittynyt sähköinen allekirjoitus**, joka täyttää direktiivin 2. artiklan 2. kohdan vaatimukset. Tällainen allekirjoitus liittyy yksiselitteisesti sen allekirjoittajaan, sillä voidaan yksilöidä allekirjoittaja, se on luotu menetelmällä, jonka allekirjoittaja voi pitää yksinomaisessa valvonnassaan, ja joka on liitetty muuhun sähköiseen tietoon siten, että tiedon mahdolliset muutokset voidaan havaita. Vaikka vaatimukset ovat teknologianeutraalit, viitataan niillä käytännössä julkisen avaimen infrastruktuuriin (*PKI = public key infrastructure*) perustuviin sähköisiin allekirjoituksiin, jotka perustuvat asymmetristen salakirjoitusmenetelmien käyttöön. Kolmas direktiivin tuntema sähköinen allekirjoitus täyttää 5. artiklan 1. kohdan vaatimukset ja vaikka direktiivi ei nimitystä käytäkään, on allekirjoitusta käytännössä alettu nimittää **”kvalifioiduksi” sähköiseksi allekirjoitukseksi**. Tällainen allekirjoitus on

- kehittynyt sähköinen allekirjoitus,
- joka perustuu laatuvarmenteeseen ja
- on luotu turvallisella allekirjoitusten luomismenetelmällä sekä
- täyttää direktiivin liitteiden vaatimukset.

Allekirjoittaja on luonnollinen henkilö, jolla on luonnollisesti hallussaan allekirjoituksen luomistiedot ja joka toimii itsensä tai edustamansa luonnollisen henkilön tai oikeushenkilön puolesta.

Allekirjoitusten hyväksyttävyyttä säädellään 5. artiklassa. Artiklan 1. kohdan mukaan ”kvalifioitu” sähköinen allekirjoitus täyttää laissa olevien muotovaatimusten ja oikeudenkäyntien näyttövaatimusten osalta samat vaatimukset kuin perinteinen käsintehty allekirjoitus. Saman artiklan 2. kohdassa todetaan, ettei sähköistä allekirjoitusta saa syrjiä pelkästään sillä perusteella, ettei se täytä kvalifioidulle sähköiselle allekirjoitukselle asetettuja vaatimuksia. Tällä tavalla direktiivi tavallaan tunnustaa kaikkien sähköisten allekirjoitusten pätevyyden, mutta vain tapauskohtaisesti. Sähköisten allekirjoitusten oikeudellisen tunnustamisen on perustuttava objektiivisiin arviointiperusteisiin eikä oltava sidoksissa siihen, onko palvelun tarjoaja saanut valtuutuksen. Varsinaisen ratkaisun tekevät kunkin maan tuomioistuimet. Äskettäin julkaistussa

komission raportissa[36] todetaan, ettei toistaiseksi ole muodostunut riittävästi oikeuskäytäntöä sen arvioimiseksi, kuinka sähköiset allekirjoitukset käytännössä tunnustetaan.

Yleisölle suunnattuja varmennepalveluja tarjoavat varmennepalvelujen tarjoajat kuuluvat kansallisten vastuusääntöjen piiriin. Lisätäkseen käyttäjien luottamusta sähköiseen viestintään ja kaupankäyntiin varmennepalvelujen tarjoajien on noudatettava tietoturvalainsäädäntöä ja kunnioitettava yksityisyyden suojaa. Salanimien käyttö varmenteissa on sallittu.

3.5.2 Sähköiset allekirjoitukset aineellisessa yhteisölainsäädännössä

Sähköisten allekirjoitusten käyttö voi perustua nimenomaisiin aineellisen oikeuden määräyksiin. Toistaiseksi yhteisölainsäätäjä on pidättäytynyt yhtenäisten vaatimusten asettamisesta sähköiselle allekirjoituksen käytölle. Ongelmana on ollut myös kansallisten varmenteiden yhteentoimivuus.

Neuvoston viides arvonlisäverodirektiivi antaa mahdollisuuden sähköisten laskujen käyttöön. Jäsenvaltioiden on hyväksyttävä verkkolasku, jos laskuttajalla on todentaa laskun alkuperä ja varmistaa sen sisällön eheys joko

- kehittyneellä sähköisellä allekirjoituksella,
- jäsenvaltion niin vaatiessa ns. kvalifioidulla sähköisellä allekirjoituksella tai
- sähköisellä tiedonsiirrolla (EDI), kun sitä koskeva tiedonsiirtosopimus edellyttää sellaisten menetelmien käyttöä, jotka takaavat tietojen alkuperän aitouden ja niiden eheyden.

Direktiivissä todetaan kuitenkin lievennyksenä, että laskut voidaan kuitenkin toimittaa sähköisesti muilla keinoin edellyttäen, että asianomainen jäsenvaltio hyväksyy tai asianomaiset jäsenvaltiot hyväksyvät ne.

Sähköisen allekirjoituksen tarkoituksena on tässä direktiivissä varmistaa tekninen turvallisuus tiedonsiirron ja säilytyksen aikana. Sähköisellä allekirjoituksella ei ole tässä tapauksessa siis juridista sisältöä. Itse asiassa direktiivi kieltää jäsenmaita vaatimasta laskujen allekirjoittamista.

---

[36] Report from the Commission to the European Parliament and the Council; Report on the operation of the Directive 1999/93/EC on a Community framework for electronic signatures, COM (2006) 120 final, 15.3.2006.

Koska eri jäsenvaltioiden vaatimat tekniset muodollisuudet poikkeavat toisistaan, muodostuu rajat ylittävissä laskutuksissa ongelmia sovellettavien muotosääntöjen valinnassa. Jotkut jäsenvaltiot asettavat muotovaatimuksia arkistointiin ja aikaleimaukseen. Eheyden, aitouden ja luettavuuden vaatimukset soveltuvat koko arkistoinnin ajan.

Verkkolaskutusta todennäköisesti merkittävämpi kehittyneempien sähköisten allekirjoitusten käytön edistäjä yhteisötasolla on sähköisten julkisten hankintojen käyttöönotto. Uudet hankintadirektiivit[37], joiden säätämisen keskeisenä pontimena oli juuri sähköisten hankintojen sääntely, ovat parhaillaan täytäntöönpanovaiheessaan. Direktiivit eivät lopulta sääntele, minkälaista sähköistä allekirjoitusta olisi käytettävä tarjousmenettelyssä, vaan jättävät täsmällisempien säännösten antamisen tässä suhteessa jäsenmaille olettaen kuitenkin, että ratkaisu vastaa tapaa, jolla kyseisessä jäsenvaltiossa on pantu täytäntöön sähköisiä allekirjoituksia koskeva direktiivi.

Kun jäsenvaltiot voivat valita eritasoiset allekirjoitussovellukset tarjousmenettelyn pohjaksi, merkitsee tämä riskiä siitä, että hankintamarkkinat voivat fragmentoitua kansallisten ratkaisujen pohjalle, mikä aiheuttaa ongelmia jäsenvaltioiden väliselle kaupalle. Sähköisen allekirjoituksen ratkaisujen yhteen toimivuutta, joka saavutettaisiin vastavuoroisen tunnustamisen kautta, korostetaan komission toimintasuunnitelmassa sähköisten hankintojen edistämiseksi vuodelta 2004. Komission tarkoituksena on sähköisen hankintatoimen vakiinnuttaminen vuoteen 2010 mennessä. Sähköisessä hankintatoimessa käytettävät sähköisten allekirjoitusten ratkaisut eivät kuitenkaan saisi poiketa ratkaisuista muuhun sähköisten allekirjoitusten käyttöön.

3.5.3 Biometriikka ja tunnistaminen

EU ei ole säännellyt sähköistä tunnistamista eikä tunnistamismenetelmien, kuten biometrian käyttöä vaihdannallisiin tarkoituksiin.[38] Tunnistamista koskevat kysymykset liittyvätkin olennaisemmin tällä hetkellä rikollisuuden, kuten rahanpesun ja terrorismin

---

[37] Euroopan Parlamentin ja Neuvoston direktiivi 2004/18/EY, annettu 31. päivänä maaliskuuta 2004, julkisia rakennusurakoita sekä julkisia tavara- ja palveluhankintoja koskevien sopimusten tekomenettelyjen yhteensovittamisesta, EYVL L 134, 30.4.2004, s. 114; ja Euroopan parlamentin ja neuvoston direktiivi 2004/17/EY, annettu 31. päivänä maaliskuuta 2004, vesi- ja energiahuollon sekä liikenteen ja postipalvelujen alalla toimivien yksiköiden hankintamenettelyjen yhteensovittamisesta, EYVL L 134, 30.4.2004, s. 1.

Direktiivien mukaan jäsenvaltioiden oli saatettava ne osaksi lainsäädäntöään 31. tammikuuta 2006 mennessä. Monissa maissa, mm. Suomessa tämä on kuitenkin viivästynyt.

[38] Sähköisestä tunnistamisesta lähemmin Myhr, Thomas, Regulating a European eID, A preliminary study on a regulatory framework for entity authentication and a pan European Electronic ID for the Porvoo e-ID Group, 31 January 2005.

torjuntaan, vaikka asia tässä yhteydessä esitetään sähköisiä palveluja koskevassa jaksossa.

Biometriikan käyttöön liittyy neuvoston asetus (EY) N:o 2252/2004, annettu 13. päivänä joulukuuta 2004, jäsenvaltioiden myöntämien passien ja matkustusasiakirjojen turvatekijöitä ja biometriikkaa koskevista vaatimuksista.

Jäsenvaltioiden myöntämien passien ja matkustusasiakirjojen on oltava asetuksen liitteessä säädettyjen turvallisuutta koskevien vähimmäisvaatimusten mukaiset.

Passeissa ja matkustusasiakirjoissa on oltava tallennusväline, johon on tallennettu kasvokuva. Jäsenvaltioiden on tallennettava niihin myös sormenjäljet yhteen toimivassa muodossa. Tiedot on suojattava ja tallennusvälineen on oltava kapasiteetiltaan riittävä ja kyettävä takaamaan tietojen eheys, aitous ja luottamuksellisuus.

Asetusta sovelletaan jäsenvaltioiden myöntämiin passeihin ja matkustusasiakirjoihin. Sitä ei sovelleta jäsenvaltioiden kansalaisilleen myöntämiin henkilökortteihin eikä väliaikaisiin passeihin ja matkustusasiakirjoihin, jotka ovat voimassa enintään 12 kuukautta.

Passeja ja matkustusasiakirjoja varten on annettava teknisiä lisäeritelmiä, jotka koskevat seuraavia seikkoja:

a) lisäturvaominaisuudet ja -vaatimukset, muun muassa tehostetut vaatimukset väärentämisen estämiseksi;

b) tekniset eritelmät biometristen tunnisteiden tallennusvälinettä ja sen suojaamista varten, luvattoman pääsyn estäminen mukaan luettuna;

c) kasvokuvaa ja sormenjälkiä koskevat laatuvaatimukset ja yhteiset säännöt.

Voidaan päättää, että edellä tarkoitetut eritelmät ovat salaisia eikä niitä saa julkaista. Tällöin ne saatetaan ainoastaan jäsenvaltioiden nimeämien, tulostuksesta vastaavien laitosten käyttöön ja jäsenvaltion tai komission asianmukaisesti valtuuttamien henkilöiden tietoon.

Kunkin jäsenvaltion on nimettävä yksi laitos, joka vastaa passien ja matkustusasiakirjojen tulostuksesta. Sen on ilmoitettava tämän laitoksen nimi komissiolle ja muille jäsenvaltioille. Kaksi tai useampi jäsenvaltio voi nimetä saman laitoksen. Kullakin jäsenvaltiolla on oikeus vaihtaa nimeämäänsä laitosta. Sen on ilmoitettava tästä komissiolle ja muille jäsenvaltioille.

Tietosuojasäännösten estämättä henkilöillä, joille passi tai matkustusasiakirja on myönnetty, on oikeus tarkistaa passin tai matkustusasiakirjan sisältämät henkilötiedot ja tarvittaessa pyytää tietojen korjaamista tai poistamista.

Passiin tai matkustusasiakirjaan ei saa sisällyttää muita koneellisesti luettavia tietoja kuin ne, joista säädetään tässä asetuksessa tai sen liitteessä tai jotka mainitaan passissa tai matkustusasiakirjassa sen myöntävän jäsenvaltion kansallisen lainsäädännön mukaisesti.

Passien ja matkustusasiakirjojen sisältämiä biometrisiä tunnisteita saa käyttää ainoastaan asiakirjan aitouden toteamiseksi; haltijan henkilöllisyyden varmistamiseksi vertaamalla biometrisiä tunnisteita suoraan saatavilla oleviin tunnisteisiin tilanteessa, jossa passi tai muu matkustusasiakirja on lain mukaan esitettävä.

3.5.4 Salaus- ja suojausjärjestelmät

Euroopan parlamentin ja neuvoston direktiivi 98/84/EY ehdolliseen pääsyyn perustuvien ja ehdollisen pääsyn sisältävien palvelujen oikeussuojasta yhdenmukaisti jäsenvaltioiden lainsäädäntöä suojattujen palvelujen ja suojattuihin palveluihin pääsyn mahdollistavien laitteiden ja tietokoneohjelmien osalta. Tämän ns. **ehdollisen pääsyn direktiivin** säännöksillä pyritään suojaamaan yhtäältä maksullisia televisio- ja radiolähetyksiä sekä toisaalta tietoyhteiskunnan etäpalveluja. Direktiivillä pyritään vaikuttamaan sellaisiin kaupallisiin toimiin, kuten purkujärjestelmien valmistaminen, maahantuonti ja myynti, joiden kohteena ovat laittomat suojauksen purkujärjestelmät. Teknisesti suojattuja palveluja tarjoavat erityisesti kaapeli- ja satelliittitelevisioyhtiöt, mutta myös muissa viestintäverkoissa maksullisia sisältöjä tarjoavat yritykset hyötyvät sääntelystä.

Direktiivillä edesautetaan sitä, että palveluntarjoaja saa maksun tarjoamastaan palvelusta. Direktiivissä ei sen sijaan ole säännöksiä suojauksen oikeudettomasta purkamisesta.

Jäsenvaltiot voivat halutessaan kieltää kansallisilla säännöillä yksityisiltä henkilöiltä suojauksen purkujärjestelmien oikeudettoman hallussapidon. Direktiivin 4. artiklan mukaan jäsenvaltioiden on kiellettävä alueellaan

- laittomien laitteiden valmistaminen, tuonti, levittäminen, myynti, vuokraus tai hallussapito kaupallisessa tarkoituksessa;
- laittoman laitteen asentaminen, huolto tai vaihtaminen kaupallisessa tarkoituksessa;
- kaupallisen viestinnän käyttö laittomien laitteiden käytön edistämiseksi.

Direktiivin 5. artiklan mukaan jäsenvaltioiden on säädettävä seuraamuksia, joiden on oltava tehokkaita, vakuuttavia ja sääntöjen vastaisen toiminnan mahdolliseen vaikutukseen suhteutettuja. Jäsenvaltioiden on lisäksi toteutettava tarvittavat toimenpiteet varmistaakseen sen, että suojattujen palvelujen tarjoajat voivat turvautua asianmukaisiin oikeuskeinoihin, muun muassa vahingonkorvauskanteen nostamiseen ja kieltotuomion tai muun ehkäisevän toimenpiteen hakemiseen sekä tarvittaessa pyytää laittomien laitteiden poistamista markkinoilta.

Ehdollisen pääsyn direktiivi ei koske niitä teknisiä suojakeinoja, joita käytetään tekijänoikeudellisen teoksen ja muun suojakohteen turvaamiseksi. Direktiivin 2001/29/EY artiklassa 6 säädetään teknisten suojaustoimenpiteiden suojasta. Jäsenvaltioiden on säädettävä riittävästä oikeudellisesta suojasta tehokkaiden teknisten toimenpiteiden kiertämistä vastaan, jos asianomainen teon suorittaja on tiennyt tai jos hänellä on ollut perusteltu aihe tietää toimintansa tarkoittavan kiertämistä. Lisäksi Jäsenvaltioiden on säädettävä riittävästä oikeudellisesta suojasta sellaisten laitteiden, tuotteiden tai osien valmistusta, maahantuontia, levitystä, myyntiä, vuokrausta, myyntiin tai vuokraukseen liittyvää mainostamista tai kaupallisessa tarkoituksessa tapahtuvaa hallussapitoa taikka sellaisten palvelujen tarjoamista vastaan a) joita markkinoidaan, mainostetaan tai pidetään kaupan keinoina kiertää tehokkaiden teknisten toimenpiteiden kiertämiseksi, tai joiden tarkoituksella tai käytöllä on tällaisen kiertämisen lisäksi vain vähäistä muuta kaupallista merkitystä, tai jotka on pääasiallisesti suunniteltu, tuotettu, mukautettu tai toteutettu siten, että niiden tarkoituksena on mahdollistaa tehokkaiden teknisten toimenpiteiden kiertäminen tai helpottaa sitä. Direktiivissä tarkoitetaan ’teknisillä toimenpiteillä’ tekniikoita, laitteita tai osia, jotka on suunniteltu normaalissa käyttötarkoituksessa estämään tai rajoittamaan teoksiin tai muuhun aineistoon kohdistuvia tekoja, joihin ei ole saatu lupaa laissa säädettyjen tekijänoikeuden tai tekijänoikeuden lähioikeuksien haltijalta tai direktiivin 96/9/EY III luvussa säädetyn *sui generis* -oikeuden haltijalta. Teknisiä toimenpiteitä pidetään tehokkaina, jos oikeudenhaltijat valvovat suojatun teoksen tai muun aineiston käyttöä jonkin sellaisen pääsynvalvontatoimen tai suojauskeinon avulla, jolla tavoiteltu suoja saavutetaan, ja joita ovat esimerkiksi teoksen tai muun aineiston salaus, muuntaminen tai muunlainen muuttaminen taikka kopioinnin valvontajärjestelmä.

Salausjärjestelmät luetaan ns. kaksikäyttötuotteisiin, joita voidaan käyttää sekä sotilaallisiin että siviilitarkoituksiin. EU on säännellyt kaksikäyttötuotteiden vientiä neuvoston asetuksella 2000/1334/EY, jonka taustalla on kansainvälinen yhteistyö.[39]

3.6 Tiedon luottamuksellisuutta koskevia aineellisia EU-säännöksiä

3.6.1 Pankkisalaisuus

Niin sanottuun ensimmäiseen pankkidirektiiviin[40] sisältyy aineellisia säännöksiä pankkisalaisuudesta eli pankkitoiminnan luottamuksellisuudesta. Direktiivin 12. artiklan mukaan jäsenvaltioiden on huolehdittava, että kaikki, jotka ovat tai ovat olleet toimivaltaisen viranomaisen palveluksessa tai tilintarkastajina tai asiantuntijoina toimivaltaisen viranomaisen lukuun, ovat salassapitovelvollisia. Tämä tarkoittaa sitä, ettei näissä tehtävissä mahdollisesti saatuja luottamuksellisia tietoja saa ilmaista toiselle henkilölle eikä viranomaiselle muutoin kuin tiivistetysti tai kootusti niin, ettei niistä voi tunnistaa yksittäisiä laitoksia. Direktiivissä säädetään vain valvonta- ja eräiden muiden viranomaisten välisestä ja tietojenvaihdosta ja salassapitovelvollisuudesta. Salassapitovelvollisuus koskee vain viranomaisen tehtävää hoitaessaan luottolaitoksesta tietoonsa saamia seikkoja.

3.6.2 Julkisen sektorin hallussa olevien tietojen uudelleenkäyttö

Euroopan perusoikeuskirja sisältää määräyksiä EU:n toimielinten toimintaan liittyvistä avoimuusperiaatteista. Vaikka kyse on eräällä tavalla yhteisestä eurooppalaisesta valtiosääntöperinteestä, vaihtelee viranomaistoiminnan avoimuutta ja julkisuutta koskeva lainsäädäntö jäsenmaittain, mikä heijastuu myös EU:n päätöksentekomenettelyjen avoimuutta koskevaan keskusteluun. EU on kuitenkin laatinut direktiivin (2003/98/EY) julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä. Direktiivillä on luotu julkisen sektorin asiakirjojen uudelleenkäytön ehdoille yleiset puitteet tavoitteena oikeudenmukaiset, oikeasuhteiset ja syrjimättömät ehdot tällaisen tiedon uudelleenkäytölle.

---

[39] Neuvoston asetus (EY) N:o 1334/2000, annettu 22. päivänä kesäkuuta 2000, kaksikäyttötuotteiden ja -teknologian vientiä koskevan yhteisön valvontajärjestelmän perustamisesta. Asetusta on muutettu useaan otteeseen eri tuotteiden osalta. Sääntely perustuu ns. Wassenaar Arrangement -sopimukseen, jolla 1990-luvun puolivälissä korvattiin COCOM-yhteistyö vientirajoitusten osalta.

[40] Direktiivi 77/780/ETY.

Julkinen sektori kerää, tuottaa, jäljentää ja jakelee suuria määriä eri aloja koskevaa tietoa, kuten yhteiskunnallista ja taloudellista tietoa, paikkatietoa, säätietoja, matkailutietoa, yritystietoa, patenttitietoa ja koulutukseen liittyvää tietoa. Julkisen sektorin tieto on tärkeä raaka-aine digitaalisissa sisältötuotteissa ja -palveluissa, ja siitä tulee yhä merkittävämpi sisällönlähde langattomien sisältöpalvelujen kehittyessä. Julkisen sektorin toimijat jakavat asiakirjoja täyttääkseen julkiset tehtävänsä. Tällaisten asiakirjojen käyttö muihin tarkoituksiin on direktiivin tarkoittamaa uudelleenkäyttöä. Direktiiviin ei kuitenkaan sisälly velvoitetta sallia asiakirjojen uudelleenkäyttö. Päätös uudelleenkäytön sallimisesta tai kieltämisestä jää jäsenvaltion tai asianmukaisen julkisen sektorin elimen tehtäväksi. Direktiiviä ei sovelleta tapauksissa, joissa kansalaiset tai yritykset voivat saada asiakirjan käyttöönsä vain, jos he voivat osoittaa asianomaisten tiedon saantia koskevien sääntöjen nojalla, että asia koskee erityisesti niitä.

4. Eurooppalainen tietoturva ja rikollisuuden torjunta

4.1 Euroopan neuvoston cyber crime -sopimus

Euroopan neuvoston piirissä on valmisteltu tietoyhteiskunnan rikollisuutta koskeva sopimus, niin sanottu *cyber crime* -sopimus (Budapest, 23.11.2001). Sopimuksen aktiiviseen valmisteluun osallistui Suomen lisäksi parikymmentä muuta Euroopan neuvoston jäsenvaltiota ja lisäksi tarkkailijoina muun muassa USA, Kanada ja Japani. Sopimus sisältää määräyksiä muun muassa jäsenvaltioiden velvoitteista ryhtyä lainsäädännöllisiin ja muihin toimenpiteisiin tietokonejärjestelmiä vastaan tehtyjen tai tietokoneen avulla tehtyjen rikosten torjumiseksi. Sopimuksessa on määräyksiä tällaisten rikosten tutkintaan vaadittavista toimenpiteistä ja kansainvälisestä yhteistyöstä. Sopimuksella pyritään myös tehostamaan kansainvälistä rikos- ja esitutkinta-yhteistyötä.

4.2 ENISA edistää eurooppalaista tietoturvaa

Myös EU on tehnyt työtä samalla saralla. EU-komissio antoi kesäkuussa 2001 tiedonannon ’Verkko- ja tietoturva: Ehdotus eurooppalaiseksi lähestymistavaksi’. Siinä ehdotetaan toimiksi tietoisuuden lisäämistä, eurooppalaista varoitus- ja tiedotus-järjestelmää, tekniikan tukemista, markkinasuuntautuneen standardoinnin ja sertifioinnin tukea, sääntelyjärjestelmää, tietoturvan edistämistä valtionhallinnossa sekä kansainvälistä yhteistyötä.

Nämä pyrkimykset johtivat Euroopan tietoturvaviraston ENISA:n perustamiseen vuonna 2004.[41] ENISA:n tehtävänä on eurooppalaisen tietoturvainfrastruktuurin ja -politiikan kehittäminen, viranomaisten ja yritysten avustaminen sekä alan lainvalmisteluun osallistuminen.

EU-komissio antoi vuoden 2006 toukokuussa uuden tiedonannon ’Turvallisen tietoyhteiskunnan strategia – Lisää vuoropuhelua, yhteistyötä ja vaikutus-mahdollisuuksia’.[42] Tässä tiedonannossa tarkastellaan tietoyhteiskunnan turvallisuus-uhkien nykytilaa ja määritellään, mitä toimenpiteitä verkko- ja tietoturvan

---

[41] Euroopan parlamentin ja neuvoston asetus (EY) N:o 460/2004, annettu 10. päivänä maaliskuuta 2004, Euroopan verkko- ja tietoturvaviraston perustamisesta. ENISA on lyhenne sanoista European Network and Information Security Agency.

[42] KOM (2006) 251 lopullinen, 31.5.2006.

parantamiseksi olisi toteutettava. Tiedonannossa todetaan erityisesti, että monimuotoisuus, avoimuus ja yhteen toimivuus ovat turvallisuuden olennaisia tekijöitä ja niitä olisi edistettävä. Lisäksi siinä korostetaan sidosryhmien monenvälistä vuoropuhelua eli julkisen ja yksityisen sektorin vuoropuhelua on edistettävä.

EU on tehnyt useita lainsäädäntötoimia tietoverkkorikollisuutta vastaan. Ongelmana ovat olleet erilaiset lähestymistavat tietoverkkorikoksiin, yhteistyön puute ja toimivalta-kysymykset.

4.3 Puitepäätös tietojärjestelmiin kohdistuvista hyökkäyksistä

Neuvoston puitepäätöksellä 2005/222/YOS tietojärjestelmiin kohdistuvista hyökkäyksistä tehostetaan rikosoikeudellista yhteistyötä tietojärjestelmiin kohdistuvissa hyökkäyksissä ottamalla käyttöön tehokkaita välineitä ja menettelyjä.

EU:n jäsenvaltiot totesivat Tampereella lokakuussa 1999 pidetyssä Eurooppa-neuvoston kokouksessa, että olisi pyrittävä sopimaan tiettyjen rikollisten tekojen määritelmistä ja niihin sovellettavista seuraamuksista. Huipputekniikkaan liittyvä rikollisuus oli yksi tässä luettelossa mainituista rikollisuuden muodoista.

Puitepäätöksen lähtökohtana todetaan, että sähköiset tiedonsiirtoverkot ja tieto-järjestelmät kuuluvat nykyään erottamattomasti EU:n kansalaisten elämään ja ne ovatkin EU:n taloudellisen menestyksen elinehto. Verkot ja tietojärjestelmät lähentyvät toisiaan jatkuvasti ja niiden väliset yhteydet lisääntyvät. Vaikka tämä kehitys tarjoaa monia ilmeisiä etuja, siihen liittyy huolestuttavana uhkakuvana tietojärjestelmiä vastaan suunnatun kansainvälisen hyökkäyksen mahdollisuus. Hyökkäyksissä voidaan käyttää erilaisia keinoja, kuten tietojärjestelmien luvaton käyttö, vahingollisen ohjelmakoodin levittäminen tai tietojärjestelmien ruuhkauttaminen. Hyökkäys voidaan käynnistää mistä ja milloin tahansa ja se voidaan suunnata minne tahansa. Tulevaisuudessa voi tapahtua uudenlaisia ja odottamattomia hyökkäyksiä.

Tietojärjestelmiin kohdistuvat hyökkäykset uhkaavat tietoyhteiskunnan turvallisuuden ja vapauteen, turvallisuuteen ja oikeuteen perustuvan alueen kehittämistä. Siksi niihin on varauduttava Euroopan unionin tasolla. Ongelmina pidetään seuraavia ilmiöitä:

A) Tietojärjestelmien luvaton käyttö. Tähän sisältyy tietojärjestelmään murtautuminen (eli hakkerointi) tarkoituksena käyttää tietokonetta tai tietokoneverkkoa luvatta. Keinot vaihtelevat sisäpiirin tiedon hyväksikäyttämisestä väsytysmenetelmän käyttämiseen ja salasanan sieppaamiseen. Tarkoituksena on usein (ei kuitenkaan aina) tietojen

ilkivaltainen kopioiminen, muuttaminen tai tuhoaminen. Joskus pyritään turmelemaan www-sivustoja tai käyttämään ehdollisen pääsyn palveluja maksutta.

B) Tietojärjestelmän häirintä. Ilkivaltaisissa hyökkäyksissä käytetään erilaisia keinoja aiheuttamaan tietojärjestelmien häiriöitä. Tunnetuimpia keinoja Internet-palvelujen estämiseksi tai heikentämiseksi on palvelunestohyökkäys (denial of service attack eli DoS). Tämä muistuttaa tilannetta, jossa faksilaitteet tukitaan pitkillä ja toistuvilla viesteillä. Palvelunestohyökkäysten tavoitteena on ylikuormittaa www-palvelimet tai Internet-palveluntarjoajien toimintakapasiteetti automaattisesti syntyvillä viesteillä. Hyökkäys voi kohdistua myös verkkotunnusjärjestelmän toiminnasta huolehtiviin DNS-palvelimiin tai ns. reitittimiin. Häirintähyökkäyksillä on aiheutettu vahinkoa joillekin hyvin näkyville sivustoille, kuten portaaleille. Yritykset ovat liiketoiminnassaan yhä riippuvaisempia Internet-palvelujensa saatavuudesta. Erityisen suojattomia ovat yritykset, joiden toimitusten oikea-aikaisuus riippuu niiden www-sivustojen käytettävyydestä.

C) Tietoja ilkivaltaisesti muuttavat tai tuhoavat ohjelmat. Pahamaineisin ilkivaltainen ohjelmatyyppi on virus. Ilkivaltaisia ohjelmia on muitakin. Osa niistä vahingoittaa itse tietokonetta, osa käyttää sitä hyökätäkseen muita verkossa olevia komponentteja vastaan. Eräs ohjelmatyyppi (ns. ehdollinen pommi, logic bomb) voi uinua piilevänä, kunnes jokin tapahtuma, kuten tietty päivämäärä, laukaisee sen. Tällaiset ohjelmat voivat muuttaa tai poistaa tietoja ja aiheuttaa siten suurta vahinkoa. Toiset ohjelmat vaikuttavat harmittomilta, mutta käynnistävät avaamisensa jälkeen tuhoisan hyökkäyksen (minkä vuoksi niitä kutsutaan "Troijan hevosiksi"). Toiset ohjelmat (joita kutsutaan "madoiksi") eivät saastuta muita ohjelmia, kuten virukset, vaan tekevät itsestään kopioita, jotka kopioivat taas itsensä ja lopulta lamauttavat koko järjestelmän.

D) Telekuuntelu. Viestien luvaton sieppaaminen eli telekuuntelu rikkoo käyttäjien tietoturvaa ja eheysvaatimuksia. Telekuuntelua kutsutaan myös "nuuskimiseksi".

E) Naamioituminen. Tietojärjestelmät tarjoavat uusia mahdollisuuksia väärän identiteetin omaksumiseen eli naamioitumiseen ja tähän perustuviin petoksiin.

Puitepäätöksen mukaisesti rikosoikeudellisesti rangaistavaa on laiton tunkeutuminen tietojärjestelmään, laiton järjestelmän häirintä (tietojärjestelmän toiminnan tahallinen törkeä estäminen tai keskeyttäminen dataa syöttämällä, siirtämällä, vahingoittamalla, tuhoamalla, turmelemalla, muuttamalla tai poistamalla tai saattamalla datan käyttökelvottomaksi) sekä laiton datan vahingoittaminen. Kaikissa tapauksissa teon on oltava tahallinen, jotta sitä voidaan pitää rikollisena tekona. Myös yllytys ja avunanto edellä mainittuihin tekoihin tai yritys tehdä niitä ovat rangaistavia. Jäsenvaltioiden on säädettävä mahdollisuudesta määrätä edellä mainituista teoista tehokkaita, oikeasuhteisia ja varoittavia rikosoikeudellisia seuraamuksia.

Se, että rikos on tehty yhteisessä toiminnassa 98/733/YOS tarkoitetun rikollisjärjestön puitteissa tai että hyökkäys on aiheuttanut vakavia vahinkoja tai vaikuttanut haitallisesti olennaisiin etuihin, katsotaan koventamisperusteeksi. Jos taas rikoksesta koituneet vahingot ovat vähäiset, tuomioistuin voi lieventää tuomiota.

Tämän lisäksi puitepäätöksessä on ehdotus arviointiperusteista, joilla määritetään oikeushenkilön vastuu ja mahdolliset seuraamukset silloin, kun oikeushenkilön vastuu on ilmeinen (tilapäinen tai pysyvä liiketoimintakielto, tuomioistuimen päätös lopettaa toiminta, julkisista varoista myönnettävien etuuksien menetys jne.).

Jokainen jäsenvaltio vastaa muun muassa alueellaan tehdyistä ja oman kansalaisensa tekemistä teoista. Jos useat jäsenvaltiot katsovat olevansa asiassa lainkäyttövaltaisia, niiden on pyrittävä yhteisesti keskittämään oikeudelliset menettelyt yhteen jäsenvaltioon. Yhteistyön tehostamiseksi jäsenvaltioiden on toimitettava toisilleen asian kannalta merkitykselliset tiedot. Tätä varten kunkin jäsenvaltion on nimettävä ympärivuorokautisesti toimivia yhteyspisteitä.

4.4 Muita keskeisiä puitepäätöksiä

Eurooppalaista yhteistyötä täydentää myös tietokonerikollisuuden alalla eurooppalainen pidätysmääräys ja jäsenvaltioiden välinen luovutusmenettely (neuvoston puitepäätös 2002/584/YOS). Puitepäätöksellä nopeutetaan ja yksinkertaistetaan näihin liittyvää menettelyä korvaamalla poliittinen ja hallinnollinen menettely oikeudellisella menettelyllä.

Tietoverkot voivat toimia myös terroritekojen kanavana, jolla haavoitetaan yhteiskunnan elintärkeitä toimintoja. Syyskuun 11. päivän 2001 terrori-iskujen jälkeen Euroopan unioni on tehostanut terrorismin torjuntaan liittyviä toimia. Neuvosto onkin hyväksynyt puitepäätöksen 2002/475/YOS terrorismin torjumisesta, jonka tavoitteena on lähentää jäsenvaltioiden lainsäädäntöä laatimalla vähimmäissäännöt, jotka koskevat terroritekojen tunnusmerkkejä. Tunnusmerkkien lisäksi puitepäätöksessä määritellään terroritekojen seuraamukset, jotka jäsenvaltioiden on sisällytettävä kansalliseen lainsäädäntöönsä. YK:n puitteissa on laadittu yleissopimus terrorismin rahoituksen tukahduttamisesta ja EU on antanut samassa asiassa suosituksen. Neuvosto on myös vahvistanut omat turvallisuussääntönsä, jossa terrorismin uhka huomioidaan.

4.5 Direktiivi viestintätietojen säilyttämisestä

EU:n lainsäädäntöelimet antoivat maaliskuussa 2006 direktiivin[43], jossa yleisesti saatavissa olevien sähköisten viestintäpalvelujen tai yleisten viestintäverkkojen tarjoajat velvoitetaan tallentamaan teletunnistetietoja sen varmistamiseksi, että kyseisiä tietoja voidaan käyttää erityisesti kunkin jäsenvaltion kansallisessa lainsäädännössä vakavaksi rikollisuudeksi määritellyn rikollisuuden tutkintaa, selvittämistä ja syyteharkintaa varten. Direktiiviä ei sovelleta sähköisen viestinnän sisältöön eikä sähköistä viestintäverkkoa käyttämällä haettuihin tietoihin eli esimerkiksi Internet-sivuihin. Jäsenvaltioiden on varmistettava, että direktiivin 5. artiklassa yksityis-kohtaisesti määritellyt tietoluokat säilytetään vähintään kuuden kuukauden ja enintään kahden vuoden ajan viestinnän päivämäärästä. Direktiivi on implementoitava 1.9.2007 mennessä, mutta Internet-tietojen osalta voidaan velvoitteiden toteuttamista lykätä 18 kuukaudella aina vuoteen 2009 asti. Useimmat jäsenmaat ovat tehneet lykkäystä koskevan julistuksen neuvoston päätöspöytäkirjaan.

Direktiivin artikla 7 sisältää yksityiskohtaiset velvoitteet tietoturvan osalta, jotka ovat yksityiskohtaisemmat kuin sähköisen viestinnän tietosuojadirektiivissä 2002/58/EY. Tallennusdirektiivin mukaan tallennettujen tietojen on nautittava samanlaista tietoturvaa kuin muidenkin palveluntarjoajan hallussa olevien tietojen. Palveluntarjoajan on säännöin huolehdittava mm. tietoihin pääsyn valvonnasta ja oikeuksista. Lisäksi on huolehdittava, että tieto pysyy eheänä ja viranomaisen saavutettavana. Direktiivissä tarkoitetun määräajan päätyttyä tallennetut tiedot on hävitettävä.

[43] Direktiivi on nimeltään Euroopan parlamentin ja neuvoston direktiivi 2006/24/EY, annettu 15. päivänä maaliskuuta 2006, yleisesti saatavilla olevien sähköisten viestintäpalvelujen tai yleisten viestintäverkkojen yhteydessä tuotettavien tai käsiteltävien tietojen säilyttämisestä ja direktiivin 2002/58/EY muuttamisesta. Tämä direktiivi valmisteltiin aluksi puitepäätöksenä. Kaikki jäsenvaltiot eivät ole hyväksyneet lainsäädännön kuulumista ns. ykköspilariin ja direktiivin laillisuus ollaan saattamassa Euroopan yhteisöjen tuomioistuimen tutkittavaksi.

5. Muuta kansainvälistä sääntelyä

5.1 OECD ja tietojärjestelmien turvallisuus

OECD on julkaissut tietoverkkojen ja tietojärjestelmien tietoturvaohjeiston (**OECD Guidelines for the Security of Networks and Information Systems**). Kyse on yleisistä periaatteista, jotka tietotekniikan kanssa toimivien tulisi ottaa huomioon. Toimijoiden tulisi tiedostaa riskit, tehdä riskikartoituksia ja selvittää mahdollisuudet riskien pienentämiseen. Tietoturvan tulisi muodostaa keskeisen osan tietojärjestelmien suunnittelussa. Johtamisjärjestelmien tulisi pyrkiä kokonaisvaltaisuuteen ja dynaamisuuteen eli pyrkiä huomioimaan kaikki toiminnan tasot, pyrkiä ennalta-ehkäisyyn ja toimintojen jatkuvaan tarkkailuun. Kunkin toimijan tulisi tiedostaa vastuunsa kokonaisuudesta. Myös tuleviin uhkiin tulisi varautua. Toiminnan ajoitus ja yhteistyö ovat tärkeitä uhkien torjumisessa. Toimijoiden tulisi kunnioittaa toistensa oikeutettuja tarpeita. Verkkojen turvallisuuden tulisi olla yhteen sovitettavissa demokraattisen yhteiskunnan arvojen kanssa.

5.2 OECD ja tietosuoja

Toinen merkittävä OECD:n ohjeisto on yksityisyyden suojan, erityisesti tietosuojan, turvaaminen rajat ylittävissä tiedonsiirroissa (**OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**). Tämä ohjeisto sisältää kahdeksan tietosuojaperiaatetta, jotka soveltuvat kaikkiin teknisiin yhteyksiin ja kaikkeen tietoon. Tietosuojaa koskevilla yleisperiaatteilla on merkityksensä uusia tekniikoita, kuten biometrisiä menetelmiä käyttöönotettaessa.

5.3 OECD ja salauspolitiikka

OECD on myös antanut suosituksen tiedonsiirron salauspolitiikan yleisohjeiksi vuonna 1997. Tuossa suosituksessa pyritään edistämän salausjärjestelmiin liittyvien tuotteiden kauppaa.

5.4 GATT/TRIPS ja yrityssalaisuuksien suoja

Kauppapoliittisen GATT-sopimuksen teollis- ja tekijänoikeuksia koskeva TRIPS-sopimus sisältää määräyksiä, jotka velvoittavat ylläpitämään suojaa myös yritys-salaisuuksille. TRIPS vaatii allekirjoittajamaita suojaamaan paljastamattoman tiedon

(undisclosed information). Tällaisen tiedon on oltava salaista eli se ei saa olla yleisesti tunnettua tai helposti saavutettavaa sellaisille henkilöille, jotka kuuluvat kyseisenlaista tietoa normaalisti käsittelevien henkilöiden piiriin. Tiedolla on lisäksi oltava kaupallista arvoa salaisuutensa vuoksi ja tiedon omistajien on suoritettava kohtuullisia toimia tiedon salassa pitämiseksi.

GATT-järjestelmään kuuluvien maiden on suojattava paljastamaton tieto muiden käytöltä ilman tiedon omistajan suostumusta, jos tiedon käyttö on vastoin rehellisiä kaupallisia toimintamuotoja. Kolmas osapuoli on saatettava vastuuseen tiedon käytöstä tapauksissa, joissa kolmas osapuoli on tiennyt tiedon alkuperän tai ollut törkeän huolimaton tämän seikan suhteen.

TRIPS-sopimus velvoittaa jäsenmaat luomaan tehokkaat oikeussuojakeinot yritys-salaisuuksien suojaksi, mukaan lukien pakkokeinot, vahingonkorvausseuraamuksen sekä tilapäiset keinot keskeyttää oikeudenloukkaus ja säilyttää todistusaineistoa.

6. Standardit ja muu tietoturvaohjeistus

6.1 Kansainvälinen tietoturvajohtamisstandardi BS7799

Standardeilla tarkoitetaan yleisesti asiakirjaa, joka muodostaa vakioidun teknis-hallinnollisen eritelmän aihepiiristään, ja jonka on hyväksynyt yleisesti tunnustettu standardisointiorganisaatio tai jonka markkinoilla toimijoiden yhteenliittymä on hyväksynyt.

Kansainvälisesti yleisesti käytetty tietoturvajohtamisstandardi BS7799 eli **British Standard for Information Security Management** on vuodelta1995 ja on, kuten nimikin sanoo, brittiläistä alkuperää. Standardi käsittää kaksi osaa, joista ensimmäinen koskee yleistä turvallisuuskäytäntöä ja toinen konkreettisia turvallisuusprosesseja. Standardi oli alun perin Englannin kauppa- ja teollisuusministeriön DTI:n turvallisuus-käytännesääntöjen uudelleenjulkaisu, joka muuttui ISO17799-standardiksi. BS7799:n kakkosversio kuitenkin ilmestyi vuonna 2002 ja tällä kertaa lyhenne tarkoitti tieto-turvallisuuden johtamisjärjestelmää. Kakkosversiosta tuli lopulta ISO27001-standardi lokakuussa 2005 eikä kakkosversio ole enää käytössä sellaisenaan standardina. On kuitenkin laadittu myös kolmosversio, joka kulkee nimellä BS7799–3:2005 *Information security management systems – Guidelines for information security risk management* eli kyse on eräänlaisesta ISO27001-standardin käyttöohjeistosta, joka kattaa kaikki riskien hallinnan vaiheet.

6.2 ISO/IEC27001-standardi

ISO27001 on eritelmä tietoturvan johtamisjärjestelmää (ISMS = *Information Security Management Systems*) varten. Standardin virallinen otsikko on "*Information Technology – Security Techniques – Information Security Management Systems – Requirements*". ISO/IEC27001-standardi on 34-sivuinen asiakirja, joka toimii kolmannen osapuolen suorittaman sertifioinnin perustana. Standardi käsittää johdannon, soveltamisalan, määritelmät, normatiiviset viittaukset, johtamisjärjestelmän, johtamisvastuun, johtamista koskevan arvioinnin ja kehittämisen.

6.3 Yhteiset kriteerit

On olemassa erillinen tekninen standardi ISO/IEC15408/1999 osa 1–3 tieto-järjestelmien ja tuotteiden tietoturvaominaisuuksien arvioimiseksi. Tuotteet arvioidaan normaalisti kehitys- tai tuotantoketjun osana. Yhteisiä kriteerejä voidaan käyttää myös tietoteknisten eritelmien rakenteena, ”kielioppina” ja luettelona käyttäjän tietoturvaa koskevien teknisten vaatimusten kuvaamiseksi.

6.4 Tietoturvavaatimukset corporate governance- ja tilintarkastussäännöissä

Sitä mukaa kun yhteisiä standardeja on kehitetty mm. sertifiointia varten, on luotu käyttökelpoinen menetelmä ja mittapuu tietoturvaa koskevien vaatimusten asettamiseksi sopimusneuvotteluihin, yrityksen sisäistä tarkastusta ja yritysten yleisiä hallintoperiaatteita silmällä pitäen.

Tietoturvaa koskevat nimenomaiset viittaukset *corporate governance* -säännöissä, joilla pörssiyritysten hallintotapaa kehitetään, ovat edelleen harvassa. Tietoturvasta huolehtiminen on joka tapauksessa yksi osa sääntöjen edellyttämää yrityksen riskien hallintaa, mikä taas on osa yrityksen valvontajärjestelmää. Toimiva riskienhallinta edellyttää siinä käytettyjen periaatteiden määrittämistä, mikä voi käsittää myös yrityksen tietoturvaperiaatteet. Tietoturvan huomioon ottamiseen on kuitenkin kiinnitetty erityistä huomiota mm. Yhdysvalloissa ja jotkut alan toimijat käyttävät tässä yhteydessä käsitettä *information security governance*. Yritysten omatoiminen tietoturvapolitiikka toimiikin vaihtoehtona lakisääteisille velvoitteille, joiden ongelmana on se, että vain osa yrityksen tietoaineistosta on sellaista, että siihen liittyy yleisen edun mukaista suojatarvetta.

Kansainvälinen laskenta-alan järjestö IFAC (International Federation of Accountants), jossa toimii IAASB-lautakunta (International Auditing and Assurance Standards Board) julkaisee kansainvälisiä tilintarkastusstandardeja. Vuodelta 2004 peräisin oleva *International Standard on Auditing 401 – Auditing in a Computer Information Systems Environment* liittyy myös tietoturvaan. Tämän standardin tarkoituksena on luoda yhtenäisiä menettelytapoja tilintarkastuksen toimittamiseen tietokoneistetussa ympäristössä. Standardissa tilintarkastajaa kehotetaan hankkimaan tieto informaatio-järjestelmien toiminnasta sekä niiden käytöstä tilintarkastuksessa arvioitavien tietojen hankinnassa. Tilintarkastajan on myös selvitettävä, kuinka tietojen käsittely yrityksessä tapahtuu eli onko se keskitettyä vai hajautettua sekä kuinka saavutettavaa mikäkin tieto on.

ERI MAITA KOSKEVAT KATSAUKSET

Edellä on käyty läpi kansainvälisellä ja EU-tasolla tehtyä yhteistyötä tietoturvallisuuden ja tietosuojan alalla. Seuraavassa luodaan katsaus Suomen, Ruotsin, Norjan, Tanskan, Saksan, Viron ja Venäjän lainsäädäntöön. Näistä kuusi ensiksi mainittua maata on EU-maita, joiden lainsäädäntö on EU-säännösten myötä pitkälle harmonisoitu selvityksen kohteena olevalla alueella. Tarkoituksena on tuoda esille keskeisten EU-säädösten implementoinnin lisäksi sääntelyssä olevia kansallisia erityispiirteitä. Suomen osuus on muita maita pitempi ja seikkaperäisempi. Esitys on vain pääpiirteitä kuvaileva, minkä vuoksi on korostettava kansallisten juristien erityisasiantuntemuksen tarvetta yksityiskohtaisemman ja tarkemman tiedon saamiseksi, milloin se on tarpeen.

Aluksi tarkastellaan kunkin maan perustuslainsäännöksiä, joissa yksityisyyden suojaa koskevat säännöt on yleensä kirjattuina. Sen jälkeen tarkastellaan tietoturvan sääntelyyn ja kehittämiseen liittyviä toimia kussakin maassa. Missään tutkittavana olevassa maassa ei tietoturvaa koskevaa lainsäädäntöä ole koottu yksiin kansiin. Toisaalta tietoturvan merkitys tiedostetaan kaikissa näissä maissa, usein osana kansallista informaatioyhteiskuntastrategiaa.

Viimeisiä vuosia ovat leimanneet kansainvälisesti ja kansallisesti taistelu terrorismia ja järjestäytynyttä rikollisuutta vastaan. Pakkokeinoja koskevat säännökset ovat tyypillisesti kansallisessa toimivallassa olevia säännöksiä, joita on paikoin käyty läpi viranomaistoiminnan erityispiirteitä koskevissa kolmansissa jaksoissa.

Kunkin katsauksen neljäs jakso käsittelee julkisen ja yksityisen organisaation hallussa olevaa tietoa koskevaa lainsäädäntöä. Viidennet jaksot käsittelevät kansallisia tietosuojasäännöksiä, viranomaisia ja näiden keskeisiä kannanottoja. Tietosuojaa koskevia säännöksiä voi olla sadoittain eri puolilla aineellista lainsäädäntöä eikä ole mielekästä käydä näitä säännöksiä läpi.

Kuudennet jaksot käsittelevät sähköisiä palveluja koskevia säännöksiä, seitsemännet sähköisiä allekirjoituksia ja tunnistamista. Kahdeksansissa jaksoissa on nostettu esille eräitä ajankohtaisia tietoturvan ja sähköisten palvelujen kysymyksiä. Viimeisenä on nostettu esiin tietoturvallisuuden yleisiin palveluihin, kuten hälytyspalveluihin ja standardointiin ja sertifiointiin liittyviä palveluja.

7. Suomi

7.1 Perustuslainsäännökset

Suomen perustuslaki uusittiin 1990-luvulla ja uusittu perustuslaki (11.6.1999/731) tuli voimaan 1.3.2000. Perusoikeuksia koskevat vuoden 1919 hallitusmuodon määräykset oli kuitenkin uusittu jo 1994.

Keskeisimpänä perusoikeutena tietoturvallisuuden kannalta voidaan pitää oikeutta yksityiselämään. Perustuslain 10 §:n mukaan jokaisen yksityiselämän kunnia ja kotirauha on turvattu: Henkilötietojen suojasta säädetään tarkemmin lailla.[44] Lisäksi pykälässä todetaan, että kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton.

Perusoikeusuudistuksen esitöiden mukaan käsite ’yksityiselämä’ voidaan ymmärtää henkilön yksityisyyden piiriä koskevaksi yleiskäsitteeksi. Tähän yksityisyyden suojaan kuuluu siis henkilötietojen suoja sekä luottamuksellisen viestin suoja. Yksityisyyden piiriin kuuluvia asioita ei kuitenkaan luetella sen enempää perustuslain kuin henkilötietolain tasolla. Tietosuojalla suojataan siis kansalaisen itsemääräämisoikeutta henkilötietojensa suhteen.

Lailla voidaan säätää perusoikeuksien turvaamiseksi tai rikosten selvittämiseksi välttämättömistä kotirauhan piiriin kuuluvista toimenpiteistä. Lailla voidaan säätää lisäksi välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä ja turvallisuustarkastuksessa sekä vapaudenmenetyksen aikana.

Perustuslain 7 §:n 1. momentti takaa jokaiselle oikeuden elämään, henkilökohtaiseen vapauteen ja turvallisuuteen. Henkilökohtaista turvallisuutta ei ollut mainittu hallitusmuodossa, mutta se vastaa kansainvälisiä ihmisoikeussopimuksia sillä sekä Euroopan ihmisoikeussopimuksen 5. artiklassa että kansalais- ja poliittisia oikeuksia koskevan yleissopimuksen 9. artiklassa on henkilökohtainen turvallisuus suojattu henkilökohtaisen vapauden yhteydessä. Vaikka kansainväliset sopimukset eivät olekaan alun perin pitäneet tietoturvallisuutta tavoitteenaan, voi Suomen perustuslain säännös saada itsenäisen tulkinnan tässä suhteessa.

---

[44] Perustuslaissa oleva delegointitapa lainsäätäjälle antaa tavallisella lailla tarkempia säännöksiä määrittää lainsäätäjän liikkumavapautta.

Tietoturvallisuus on suomalaisessa kirjallisuudessa kuvattu ”metaperusoikeutena”[45] Julkisella vallalla voidaan nähdä olevan velvollisuus edistää tietoturvallisuutta kollektiivisella tasolla ja suojata siten yhteiskunnan infrastruktuuria. Toisaalta suojattavana kohteena on erityisesti kansalaisten yksityiselämä, jolloin myös tietosuojan tason turvaaminen riittävällä tietoturvallisuudella on yhteiskunnan tehtävä. Tässä yhteydessä voidaan viitata perustuslain 22 §:ään, jossa todetaan, että julkisen vallan on turvattava perusoikeuksien ja ihmisoikeuksien toteutuminen.[46]

Perustuslain 12 § sisältää sananvapautta ja julkisuutta koskevat lainsäädännön perusperiaatteet. Niiden mukaan jokaisella on sananvapaus. Sananvapauteen liittyy oikeus ilmaista, julkistaa ja vastaanottaa tietoja, mielipiteitä ja muita viestejä kenenkään ennakolta estämättä. Tarkempia säännöksiä sananvapaudesta annetaan lailla. Viranomaisen hallussa olevat asiakirjat ja muut tallenteet ovat julkisia, jollei niiden julkisuutta ole välttämättömien syiden vuoksi lailla erikseen rajoitettu. Jokaisella on oikeus saada tieto julkisesta asiakirjasta ja tallenteesta.

Vaikka tämä jakso käsitteleekin perustuslainsäännöksiä, voidaan todeta, että laki sananvapauden käyttämisestä joukkoviestinnässä (460/2003) määrittelee tarkemmin perustuslaissa turvatun sananvapauden käyttämistä. Sananvapauslain 16 §:ssä säädetään lähdesuojasta. Yleisön saataville toimitetun viestin laatijalla sekä julkaisijalla ja ohjelmatoiminnan harjoittajalla on sen mukaan oikeus olla ilmaisematta, kuka on antanut viestin sisältämät tiedot. Julkaisijalla ja ohjelmatoiminnan harjoittajalla on lisäksi oikeus olla ilmaisematta viestin laatijan henkilöllisyyttä. Tämä oikeus on myös viestin ja julkaisijan palveluksessa olevalla henkilöllä. Toinen salassapitoa koskeva säännös on 17 §:ssä todettu verkkoviestin tunnistamistietojen luovuttaminen pakkokeinona.

---

[45] Sähköinen viestintä, tietoturvallisuus ja perusoikeudet, Lapin yliopisto, Oikeusinformatiikan instituutti, 2004, s. 30.

[46] Tapauksessa KKO 2003:36 maan ylin tuomioistuin vetosi ratkaisunsa perusteluissa yksiselitteisesti tietoturvallisuuden merkitykseen porttiskannausta koskevassa tapauksessa. Porttiskannaus on toimenpide, jolla on mahdollista selvittää tietojärjestelmän tietoturva-aukkoja ja muita heikkouksia sekä saada kohdejärjestelmästä sellaisia tietoja, joiden avulla järjestelmään voidaan murtautua. Nuori turkulainen opiskelija etsi marraskuussa 1998 porttiskannausohjelman avulla Osuuspankkikeskuksen tietojärjestelmästä avoimia välityspalvelimia. Korkein oikeus pysytti Turun hovioikeuden tuomion, jossa tekijä tuomittiin tietomurron yrityksestä. Korkein oikeus totesi tuomiolauselmassaan: ”Ottaen huomioon tietoturvallisuuden tärkeyden, teon tahallisuuden ja laadun sekä sen, että A teon tehdessään on kyennyt ymmärtämään siitä aiheutuvan vahingonvaaran, Korkein oikeus katsoo, ettei vahingonkorvauksia ole perusteltua tässä tapauksessa sovitella.”

Sananvapauden kääntöpuolena on vastuu sisällöstä. Viestintä voi olla sisältönsä vuoksi lainvastaista sillä laki tuntee lukuisia rikoksia, joiden tunnusmerkistö toteutuu viestinnän eli julkisuuteen saattamisen kautta. Näitä rikoksia kutsutaan usein sisältörikoksiksi.[47]

Lakia sovelletaan Suomessa harjoitettavaan julkaisu- ja ohjelmatoimintaan, minkä vuoksi viestintään kohdistuvia pakkokeinoja ei voi ulottaa ulkomailta käsin tapahtuvaan viestintään. Yksityisen henkilön pitäessä yllä sähköisen viestintäverkon kotisivua häneen sovelletaan vain lain vastuu-, lähdesuoja-, pakkokeino- ja seuraamusmääräyksiä. Vastaavasti toimintaan, jossa huolehditaan pelkästään julkaisun tai verkkoviestin teknisestä valmistamisesta, lähettämisestä, välittämisestä tai jakelusta sovelletaan vain lain pakkokeinoja ja seuraamusjärjestelmää koskevia määräyksiä. Laissa säädetään julkaisijan ja ohjelmatoiminnan harjoittajan velvollisuuksista.

7.2 Tietoturvan sääntely ja kehittäminen

Tietoturvaa koskevia säännöksiä sisältyy tällä hetkellä useampiin voimassa oleviin lakeihin ja asetuksiin. Viestintämarkkinalain (393/2003) 128 § (viestintäverkon ja viestintäpalvelun laatuvaatimukset) sisältää teleyrityksiin kohdistuvan yleisen tietoturvaa koskevan vaatimuksen. Viestintämarkkinalain 129 §:n perusteella Viestintävirasto voi antaa näitä vaatimuksia koskevia määräyksiä. Tietoturvaa säännellään myös henkilötietolain 32 §:ssä, sähköisen viestinnän tietosuojalain 19–21 ja 38 §:ssä ja lain viranomaisen toiminnan julkisuudesta 18 §:ssä.

Henkilötietolain 32 § lähtee velvollisuudesta tietoturvallisuustoimenpitein huolehtia yksityisyyteen kuuluvasta henkilötietojen suojasta. Vastaavanlainen velvollisuus on asetettu teleyritykselle ja lisäarvopalvelun tarjoajalle palvelujensa tietoturvasta sähköisen viestinnän tietosuojalain 19 §:ssä.

Yleinen tietoturvan normaaliajan ohjaus ja kehittäminen kuuluu lähinnä liikenne- ja viestintäministeriön, sen alaisen Viestintäviraston sekä kauppa- ja teollisuusministeriön toimialaan. Tietoturvaan kuuluvia tehtäviä kuuluu siis usean ministeriön tehtäviin, minkä lisäksi valtioneuvoston kanslialla on tehtävänsä tässä suhteessa.

Viestintävirasto valvoo sekä sähköisen viestinnän tietosuojalain, että viestintämarkkinalain noudattamista. Viestintävirasto harjoittaa myös tietoliikenneturvallisuuden

---

[47] Luettelosananvapauden käyttöön liittyvistä ns. sisältörikoksista löytyy sisäasiainministeriön poliisiosaston julkaisusta 2/2003, Internetissä julkaistavan rikollisen materiaalin rajoittamista selvittäneen työryhmän raportti, s. 10.

valvontaa (COMSEC, *communications security*) ja se voi antaa teknisiä määräyksiä sähköisen viestinnän tietosuojalain ja viestintämarkkinalain tietoturvaa koskevien säännösten noudattamisesta. Viestintäviraston tehtäviin kuuluu myös televiestinnän ja siihen liittyvän tietoturvan standardoinnin koordinointi ja kehittäminen.

Tietosuojaviranomaisten tehtävänä on valvoa henkilötietolain tietoturvasäännösten noudattamista ja edistää hyvää tiedonhallintatapaa, mihin sisältyy myös tietoturvaa koskevia vaatimuksia. Arkistolaitoksen tehtävät tietoturvan alalla keskittyvät arkistolain (831/1994) perusteella pysyvästi säilytettävien asiakirjojen säilyvyyden turvaamiseen ja sen tehtävänä on sähköisestä asioinnista viranomaistoiminnassa annetun lain 22 §:n mukaan antaa tarkempia määräyksiä hallinnon sähköisen asioinnin kirjaamisesta ja rekisteröimisestä.

Muita keskeisiä ja aktiivisia toimijoita tietoturvan alalla ovat poliisin hallinnosta annetun lain (110/1992) perusteella keskusrikospoliisi, suojelupoliisi ja muut poliisiviranomaiset sekä muun muassa Funet CERT ja Tietoyhteiskunnan kehittämiskeskus ry (Tieke). Lisäksi yksityisten yritysten itsesääntelyllä samoin kuin erilaisilla yritysten käytännön tietoturvatoimenpiteillä on keskeinen merkitys tietoturvan kehittämisen ja toteutumisen kannalta. Tietoturva-alan yhteistyötä tehdään muun muassa Yritysturvallisuuden neuvottelukunnassa, joka on Teollisuuden ja Työantajain Keskusliiton, Palvelutyönantajat ry:n sekä näiden jäsenyritysten yhteistyöorganisaatio.

Valtioneuvosto teki periaatepäätöksen kansallisesta tietoturvallisuusstrategiasta 4.9.2003.[48] Sillä halutaan lisätä kansalaisten ja yritysten luottamusta tietoyhteiskuntaan. Strategiaan on koottu linjauksia ja toimia, joilla tietoturvallisuutta ja yksityisyyden suojaa voidaan parantaa. Periaatepäätös perustuu keväällä 2003 toimikautensa päättäneen tietoturvallisuusasioiden neuvottelukunnan ehdotukseen kansalliseksi tietoturvallisuusstrategiaksi.

Kansallinen tietoturvallisuusasioiden neuvottelukunta tukee tietoturvallisuusstrategian toimeenpanoa ja seuraa sen toteutumista. Sen toimikausi on 17.10.2003–31.5.2007.

[48] VM 0024:00/02/99/1998.

7.3 Yleinen turvallisuus ja erityispiirteitä viranomaistoiminnasta

Seuraavassa keskeisimmät yleisen tietoturvallisuuden kannalta merkitykselliset määräykset:

Valmiuslaki (1080/1991, muutettu lailla 198/2000) sisältää määräyksen (33 §), jonka mukaan valtioneuvosto voi laissa tarkoitetuissa poikkeustapauksissa määrätä viestiyhteyksien käytöstä ja viestiverkkojen muutoksista. Valmiuslakia ollaan tällä hetkellä muuttamassa tietoturvan osalta.

Laki huoltovarmuuden turvaamisesta (1390/1992) koskee ennakoivia toimenpiteitä kriisien varalta. Laki on laajennettu sisältämään poikkeusolojen ohella myös ne vakavat häiriötilanteet, joissa markkinamekanismi ei tuota riittävää huoltovarmuutta. Silloin, kun kaupallinen palvelutarjonta ei tuota turvallisuuden kannalta riittävää huoltovarmuustasoa, on valtion huolehdittava tarvittavasta varautumisesta. Erityistoimenpiteitä vaativat esimerkiksi kriittisten tietojärjestelmien, tietoverkkojen ja reittien varmistaminen ja suojaukset elektromagneettista pulssia (EMP) tai mikroaaltoasetta (HPM) vastaan.

Lain turvallisuusselvityksistä (177/2002) tarkoituksena on selvityksen kohteena olevan henkilön yksityiselämän suoja ja henkilötietojen suoja huomioon ottaen 1 §:ssä tarkoitettua turvallisuusselvitysmenettelyä käyttämällä parantaa mahdollisuuksia ennakolta estää rikokset, jotka vakavasti vahingoittaisivat Suomen sisäistä tai ulkoista turvallisuutta, maanpuolustusta tai poikkeusoloihin varautumista, Suomen suhteita toiseen valtioon tai kansainväliseen järjestöön, julkista taloutta, yksityisen huomattavan arvokasta liike- tai ammattisalaisuutta tai muuta tähän rinnastettavaa erittäin merkittävää yksityistä taloudellista etua taikka edellä mainittujen etujen suojaamisen kannalta erittäin merkittävää tietoturvallisuutta.

Laki puolustustaloudellisesta suunnittelukunnasta (238/1960, muutokset 1241/1987 ja 623/1999) antaa suunnittelukunnan tehtäväksi ne selvittely-, suunnittelu- ja järjestelytehtävät, jotka ovat tarpeen maan taloudellisen puolustusvalmiuden kehittämiseksi sekä väestön toimeentulon ja talouselämän turvaamiseksi sodan taikka sodan vaaran tai maan ulkopuolella sattuneen sodan tai vaikutuksiltaan siihen verrattavan muun erityisen tapahtuman aiheuttamien poikkeuksellisten olojen aikana, kuuluvat pääsääntöisesti puolustustaloudelliselle suunnittelukunnalle. Lain 4 §:ssä velvoitetaan teollisuuslaitoksen omistajan tai haltijan ja muun elinkeinonharjoittajan tulee suunnittelukunnan kehotuksesta antaa ne tiedot henkilökunnasta, huoneistotiloista, koneista ja muista varusteista, tuotannosta ja tuotantokyvystä, sähkövoiman

käytöstä, polttoaineista, raaka-aineista ja muista tarvikkeista, varastotiloista, ostoista, hankinnoista sekä muista seikoista, jotka ovat tarpeen suunnittelukunnan työtä varten.

Suomessa pakkokeinoja koskevia määräyksiä sisältyy moniin lakeihin. Esimerkiksi viestintää koskevia pakkokeinoja sisältyy pakkokeinolain ja poliisilain lisäksi sananvapauslakiin ja lakiin tietoyhteiskunnan palvelujen tarjoamisesta. Näistä kaksi jälkimmäistä ovat keskeisiä silloin, kun viranomainen yrittää estää laitonta sisältöä.

Yksityisyyden suojaan kajoamisessa ovat puolestaan keskeisiä pakkokeinolaki ja poliisilaki, jotka sääntelevät mm. telekuuntelua, televalvontaa sekä teknistä tarkkailua. Poliisilaki puhuu tällöin tiedonhankintasäännöksistä. Pakkokeinolaki soveltuu, kun edellä mainitut toimet tehdään jo tehtyjen rikosten selvittämiseksi. Myös tullilaissa ja rajavartiolaissa on samanlaisia määräyksiä kuin poliisi- ja pakkokeinolaissa. Esitutkintaa suorittavalle viranomaiselle voidaan myöntää oikeus televalvontaan tai peräti telekuunteluun pakkokeinolaissa lueteltuihin rikoksiin epäiltyjen tutkimiseksi. Poliisilaki puolestaan lähtee tiedonhankinnasta rikosten ehkäisemiseksi tai paljastamiseksi konkreettisessa tapauksessa. Lakien määritelmät ovat käytännössä samansisältöiset ja toimenpiteiden teolle asetetut vaatimuksetkin ovat lähellä toisiaan.

Sisäasiainministeriö asetti toukokuussa 2005 työryhmän laatimaan ehdotuksen yritysturvallisuusstrategiaksi. Työryhmä, joka käsitteli muun rikollisuuden ohessa myös tietoverkkorikollisuutta, jätti mietintönsä maaliskuun 15. päivänä 2006.[49] Mietinnössä todetaan, että tietoverkkorikollisuus muodostaa erityisen uhkan yritysten tietopääomalle, sillä verkossa rikoksen toteuttaminen on usein helpompaa kuin reaalimaailmassa ja kiinnijäännin riski on verkossa pienempi. Tietojärjestelmiin kohdistuvat yritysten kohtaamat rikosilmiöt voidaan ryhmitellä toisaalta satunnaisiin hyökkäyksiin, kuten roskapostin ja virusten lähettämiseen, toisaalta kohdistettuihin hyökkäyksiin, jotka uhkaavat yritysten tietopääomaa. Tietoverkkoihin liittyvää rikollisuutta itseään on pohdittu tietoverkkorikostyöryhmän mietinnössä (OM 2003:6).

Raportissa todetaan, että tietoturvallisuuden ylläpitäminen on riskienhallintaa, joka edellyttää oikeaa uhkatietoisuutta, uhan vaikutusten arviointia, turvajärjestelmien toteutuksen säännöllistä tarkastamista ja yritykselle sopivan riskitason hyväksymistä.

[49] Elinkeinoelämän ja viranomaisten yhteinen strategia yrityksiin kohdistuvien rikosten ja väärinkäytösten torjumiseksi, Sisäinen turvallisuus, Sisäasianministeriön julkaisuja 15/2006.

7.4 Tiedon julkisuus ja salassapito

7.4.1 Viranomaistieto

Laki viranomaisen toiminnan julkisuudesta (621/1999) sisältää yleisperiaatteen, jonka mukaan viranomaisten asiakirjat ovat julkisia, jollei tässä tai muussa laissa erikseen toisin säädetä. Laissa säädettyjen tiedoksisaantioikeuksien ja viranomaisten velvollisuuksien tarkoituksena on toteuttaa avoimuutta ja hyvää tiedonhallintatapaa viranomaisten toiminnassa sekä antaa yksilöille ja yhteisöille mahdollisuus valvoa julkisen vallan ja julkisten varojen käyttöä, muodostaa vapaasti mielipiteensä sekä vaikuttaa julkisen vallan käyttöön ja valvoa oikeuksiaan ja etujaan. Laissa säädetään oikeudesta saada tieto viranomaisten julkisista asiakirjoista sekä viranomaisessa toimivan vaitiolovelvollisuudesta, asiakirjojen salassapidosta ja muista tietojen saantia koskevista yleisten ja yksityisten etujen suojaamiseksi välttämättömistä rajoituksista samoin kuin viranomaisten velvollisuuksista.

Jokaisella on oikeus saada tieto viranomaisen asiakirjasta, joka on julkinen. Laissa on asiakirjan määritelmä, joka pitää sisällään myös sähköisen muodon. Asiakirjalla tarkoitetaan 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.

Viranomaisen asiakirjalla tarkoitetaan viranomaisen hallussa olevaa asiakirjaa, jonka viranomainen tai sen palveluksessa oleva on laatinut tai joka on toimitettu viranomaiselle asian käsittelyä varten tai muuten sen toimialaan tai tehtäviin kuuluvassa asiassa. Viranomaisen laatimana pidetään myös asiakirjaa, joka on laadittu viranomaisen antaman toimeksiannon johdosta, ja viranomaiselle toimitettuna asiakirjana asiakirjaa, joka on annettu viranomaisen toimeksiannosta tai muuten sen lukuun toimivalle toimeksiantotehtävän suorittamista varten. Viranomaisen asiakirjana ei pidetä mm. viranomaisen palveluksessa olevalle tai luottamushenkilölle hänen muun tehtävänsä tai asemansa vuoksi lähetettyä kirjettä tai muuta asiakirjaa tai asiakirjaa, joka on annettu viranomaiselle yksityisen lukuun suoritettavaa tehtävää varten tai laadittu sen suorittamiseksi.

Lakia sovelletaan viranomaisissa työskentelevien sekä viranomaisten ja niiden lukuun toimivien yksityisten ja yhteisöjen välisiä neuvotteluja, yhteydenpitoa ja muuta niihin verrattavaa viranomaisten sisäistä työskentelyä varten laadittuihin asiakirjoihin vain, jos asiakirjat sisältävät sellaisia tietoja, että ne arkistolainsäädännön mukaan on liitettävä

arkistoon. Jos asiakirja kuitenkin liitetään arkistoon, viranomainen voi määrätä, että tietoja niistä saa antaa vain viranomaisen luvalla.

Lain 6 § sisältää määräyksiä siitä, milloin asiakirja tulee julkiseksi. Yritysten kannalta olennainen on hankintaa koskeva sääntö, jonka mukaan hankintaa ja urakkaa samoin kuin muuta tarjousten perusteella ratkaistavaa oikeustointa koskeva tarjouksen täydennyspyyntö ja tarjousasian käsittelyä varten laaditut selvitykset ja muut asiakirjat tulevat julkisiksi, kun sopimus asiassa on tehty. Lain 7 §:n mukaan viranomaiselle asian käsittelyä varten tai muuten sen toimialaan tai tehtäviin kuuluvassa asiassa toimitettu asiakirja tulee julkiseksi, kun viranomainen on sen saanut. Viranomaiselle toimitetut hankinta-, urakka- ja muut tarjouskilpailun perusteella ratkaistavaa oikeustointa koskevat tarjoukset tulevat 1. pääsäännön mukaan julkisiksi vasta, kun sopimus on tehty.

Viranomaisen asiakirja on pidettävä salassa, jos se on laissa säädetty salassa pidettäväksi tai jos viranomainen lain nojalla on määrännyt sen salassa pidettäväksi taikka jos se sisältää tietoja, joista on lailla säädetty vaitiolovelvollisuus.

Salassa pidettävää viranomaisen asiakirjaa tai sen kopiota tai tulostetta siitä ei saa näyttää eikä luovuttaa sivulliselle eikä antaa sitä teknisen käyttöyhteyden avulla tai muulla tavalla sivullisen nähtäväksi tai käytettäväksi. Lain 24 §:ssä on lista asiakirjoista, jotka on määrätty salassa pidettäviksi. Näistä mainittakoon seuraavat yritysten tietoturvan kannalta merkitykselliset asiakirjat:

A) asiakirjat, jotka sisältävät tietoja valtion, kunnan tai muun julkisyhteisön tai 4 §:n 2. momentissa tarkoitetun yhteisön, laitoksen tai säätiön liike- tai ammattisalaisuudesta, samoin kuin sellaiset asiakirjat, jotka sisältävät tietoja muusta vastaavasta liiketoimintaa koskevasta seikasta, jos tiedon antaminen niistä aiheuttaisi mainituille yhteisöille, laitoksille tai säätiöille taloudellista vahinkoa tai saattaisi toisen samanlaista tai muutoin kilpailevaa toimintaa harjoittavan julkisyhteisön tai yksityisen parempaan kilpailuasemaan tai heikentäisi julkisyhteisön tai 4 §:n 2 momentissa tarkoitetun yhteisön, laitoksen tai säätiön mahdollisuuksia edullisiin hankintoihin tai sijoitus-, rahoitus- ja velanhoitojärjestelyihin.

B) asiakirjat, jotka sisältävät tietoja yksityisestä liike- tai ammattisalaisuudesta, samoin kuin sellaiset asiakirjat, jotka sisältävät tietoja muusta vastaavasta yksityisen elinkeinotoimintaa koskevasta seikasta, jos tiedon antaminen niistä aiheuttaisi elinkeinonharjoittajalle taloudellista vahinkoa, ja kysymys ei ole kuluttajien terveyden tai ympäristön terveellisyyden suojaamiseksi tai toiminnasta haittaa kärsivien oikeuksien valvomiseksi merkityksellisistä tiedoista tai elinkeinonharjoittajan velvollisuuksia ja niiden hoitamista koskevista tiedoista.

Viranomainen voi antaa salassa pidettävästä viranomaisen asiakirjasta tiedon, jos tiedon antamisesta tai oikeudesta tiedon saamiseen on laissa erikseen nimenomaisesti säädetty tai se, jonka etujen suojaamiseksi salassapitovelvollisuus on säädetty, antaa siihen suostumuksensa.

Viranomainen voi salassapitosäännösten estämättä antaa tiedon toisen taloudellisesta asemasta tai liike- tai ammattisalaisuudesta, jos tieto on tarpeen yksityisen tai toisen viranomaisen laissa säädetyn tiedonantovelvollisuuden toteuttamiseksi taikka tiedot antavan viranomaisen hoidettavaksi kuuluvan korvauksen tai muun vaatimuksen toteuttamiseksi.

Laki viranomaisen toiminnan julkisuudesta toteaa 18 §:ssä erityisesti, että viranomaisen tulee hyvän tiedonhallintatavan luomiseksi ja toteuttamiseksi huolehtia asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen asianmukaisesta saatavuudesta, käytettävyydestä ja suojaamisesta sekä eheydestä ja muusta tietojen laatuun vaikuttavista tekijöistä sekä tässä tarkoituksessa erityisesti:

> 4) suunnitella ja toteuttaa asiakirja- ja tietohallintonsa samoin kuin ylläpitämänsä tietojärjestelmät ja tietojenkäsittelyt niin, että asiakirjojen julkisuus voidaan vaivattomasti toteuttaa ja että asiakirjat ja tietojärjestelmät sekä niihin sisältyvät tiedot arkistoidaan tai hävitetään asianmukaisesti, ja että asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen suoja, eheys ja laatu turvataan asianmukaisin menettelytavoin ja tietoturvallisuutta koskevin järjestelyin ottaen huomioon tietojen merkitys ja käyttötarkoitus sekä asiakirjoihin ja tietojärjestelmiin kohdistuvat uhkatekijät ja tietoturvallisuustoimenpiteistä aiheutuvat kustannukset;
>
> 5) huolehtia siitä, että sen palveluksessa olevilla on tarvittava tieto käsiteltävien asiakirjojen julkisuudesta sekä tietojen antamisessa ja käsittelyssä sekä niiden ja asiakirjojen ja tietojärjestelmien suojaamisessa noudatettavista menettelyistä, tietoturvallisuusjärjestelyistä ja tehtävänjaosta, samoin kuin siitä, että hyvän tiedonhallintavan toteuttamiseksi annettujen säännösten, määräysten ja ohjeiden noudattamista valvotaan.

Arkistolaissa (831/1994) säädetyssä järjestyksessä arkistoon siirretystä, salassa pidettäväksi säädetystä viranomaisen asiakirjasta saa antaa tietoja tutkimusta tai muuta hyväksyttävää tarkoitusta varten, jollei asiakirjan siirtänyt viranomainen ole toisin määrännyt. Tietojen antamista harkittaessa on huolehdittava siitä, että tieteellisen tutkimuksen vapaus turvataan.

Asiakirjan saaneen on annettava kirjallinen sitoumus siitä, ettei hän käytä asiakirjaa sen henkilön vahingoksi tai halventamiseksi, jota asiakirja koskee, tai hänen läheisensä

vahingoksi tai halventamiseksi taikka sellaisten muiden etujen loukkaamiseksi, joiden suojaksi salassapitovelvollisuus on säädetty.

Viranomainen voi antaa toiselle viranomaiselle tiedon salassa pidettävästä asiakirjasta, jos tiedon antamisesta tai oikeudesta tiedon saamiseen on laissa erikseen nimenomaisesti säädetty tai jos se, jonka etujen suojaamiseksi salassapitovelvollisuus on säädetty, antaa siihen suostumuksensa.

7.4.2 Yrityssalaisuuksien suoja

Yrityssalaisuuksien lainsäädännöllinen suoja ei ole kehittynyt Suomessa samassa tahdissa yrityssalaisuuksien merkityksen kanssa. Yrityssalaisuuksista ei ole Suomessa muun muassa Ruotsin ja Yhdysvaltojen tavoin yhtenäistä lakia, vaan niiden kansallinen lakisääteinen suoja perustuu lukuisiin erilaisiin ja eri aikoina säädettyihin säännöksiin, joiden säätämistausta ja oikeuspoliittiset perustelut poikkeavat toisistaan.

Yrityssalaisuuksien yleinen lakisääteinen suoja on Suomessa säädetty sopimattomasta menettelystä elinkeinotoiminnassa annetussa laissa[50] (”SopMenL”), työsopimuslaissa[51] (”TSL”) ja rikoslaissa[52] (”RL”). RL:n nykymuotoiset säännökset tulivat voimaan vuosina 1991 ja 2003, SopMenL:n vuonna 1979 ja TSL:n vuonna 2001. Säännösten soveltamiseen liittyvää oikeuskäytäntöä on kuitenkin saatavilla niukasti. Yrityssalaisuuksien puutteellista lainsäädännöllistä suojaa täsmennetään ja laajennetaan usein salassapitosopimuksin.

Koska edellä mainittujen lakien yrityssalaisuuksiin sovellettavien säännösten tunnusmerkit, lainsäädäntötausta sekä käytettävissä olevat oikeuskeinot poikkeavat toisistaan, käsitellään seuraavassa kuhunkin lakiin sisältyviä säännöksiä erikseen omana kokonaisuutenaan. Huomattavaa kuitenkin on, että tiettyyn tekoon voi soveltua useampikin laki, jolloin on ensiksi ratkaistava, minkä lain perusteella ja missä menettelyssä asia halutaan kulloinkin saada ratkaistuksi.

Vaikka edellä todetusti Suomen lainsäädännössä yrityssalaisuuksien yleisestä suojasta on säännelty kolmessa eri laissa, vain rikoslain 30:11 § sisältää yrityssalaisuuden määritelmän. Sen mukaan yrityssalaisuudella tarkoitetaan ”liike- tai ammattisalaisuutta taikka muuta vastaavaa elinkeinotoimintaa koskevaa tietoa, jonka elinkeinonharjoittaja pitää salassa ja jonka ilmaiseminen olisi omiaan aiheuttamaan taloudellista vahinkoa

---

[50] 22.12.1978/1061.

[51] 2001/55.

[52] 19.12.1889/39.

joko hänelle tai toiselle elinkeinonharjoittajalle, joka on uskonut tiedon hänelle”. Rikoslain yrityssalaisuuden käsite on siten liike- tai ammattisalaisuuden käsitettä laajempi sen kattaessa näiden ohella myös ”muun vastaavan elinkeinotoimintaa koskevan tiedon”.

Rikoslain esitöiden mukaan yrityssalaisuuden tunnusmerkkejä ovat edellä viitatun määritelmän mukaan 1) tiedon haltijan salassapitotahto, 2) salassapitointressi ja 3) tosiasiallinen salassapito. Kaikkien näiden tunnusmerkkien on täytyttävä, jotta kyseessä olisi yrityssalaisuus.

Yritysvakoilu koskee tilanteita, joissa yrityssalaisuus joutuu yhtiön hallusta oikeudettomasti ilman yhtiön myötävaikutusta. Tällöin nimenomaan tiedon oikeudeton hankinta on todettu kielletyksi ja rangaistavaksi. RL 30:4 §:n tarkoittamassa yritysvakoilussa on kyse toisen yrityssalaisuuden oikeudettomasta hankinnasta, mikäli tekijällä on ollut tarkoitus oikeudettomasti ilmaista tai käyttää yrityssalaisuutta.

RL 30:5 §:n mukaisena yrityssalaisuuden rikkomisena rangaistaan laissa nimenomaan määrätyssä asemassa olevan henkilön tässä asemassa luvallisesti saaman toisen yrityssalaisuuden oikeudeton ilmaiseminen tai käyttäminen. Yrityssalaisuuden rikkomisen tunnusmerkit, joiden kaikkien tulee täyttyä samanaikaisesti, ovat: 1) tekijä on saanut tiedon yrityssalaisuudesta laissa mainitussa luottamussuhteessa yhtiöön, 2) tekijä oikeudettomasti ilmaisee tai käyttää toiselle kuuluvaa yrityssalaisuutta ja 3) tekijän tarkoitus on hankkia itselleen tai toiselle taloudellista hyötyä tai vahingoittaa toista.

Yrityssalaisuuden rikkomisen keskeisenä erona yritysvakoiluun on, että kun yritysvakoilussa henkilö on oikeudettomasti hankkinut tiedon yrityssalaisuudesta, yrityssalaisuuden rikkomisessa henkilö on saanut siitä yrityssalaisuuden haltijan suostumuksella täysin luvallisesti tiedon. RL 30:5 §:n mukaan yrityssalaisuuden salassapitoaika on palvelusuhteen kestoaika sekä sen jälkeen kaksi vuotta. Työntekijän oman työnantajan yrityssalaisuuksien ohella säännös kattaa myös työnantajan yhteistyökumppanin yrityssalaisuudet. Kuitenkin, jotta RL 30:5 §:ää voidaan soveltaa, henkilön on tullut saada tieto yrityssalaisuudesta laissa mainitussa luottamussuhteessa eli asemassa tai tehtävässä. Yrityssalaisuuden ilmaiseminen tai käyttäminen voi kuitenkin tapahtua vasta kyseisen aseman tai tehtävän päättymisen jälkeen. Mikäli yrityssalaisuutta ei loukkaa säännöksessä mainittu henkilö tai tietoa ei ole luovutettu tälle luottamussuhteen perusteella, kyse on yritysvakoilusta.

Lisäksi yrityssalaisuuden rikkomisen tunnusmerkkinä on, että tekijällä on ollut tiedon ilmaistessaan tai sitä käyttäessään hyötymis- tai vahingoittamistarkoitus. Edellytyksenä

ei ole kuitenkaan taloudellisen hyödyn tai vahingon todellinen syntyminen, vaan riittää, että tekijällä on tällainen tarkoitus.

RL 30:6 §:n mukaisen yrityssalaisuuden väärinkäytön tarkoituksena on rangaista henkilöitä, jotka syyllistymättä itse yritysvakoiluun tai yrityssalaisuuden rikkomiseen hyödyntävät rikoksella saatuja yrityssalaisuuksia joko käyttäen niitä itse tai myymällä ne edelleen. Yrityssalaisuuden väärinkäytössä tekijällä on yrityssalaisuus tiedossaan ilman sen oikean haltijan suostumusta ennen väärinkäyttöön ryhtymistä.

RL 38:1 §:n mukaisena salassapitorikoksena rangaistaan lain, asetuksen tai viranomaisen lain nojalla määräämän salassapitovelvollisuuden vastaisesti suoritettu salassa pidettävän seikan paljastaminen tai käyttäminen omaksi tai toisen hyödyksi. Säännöksen tarkoittama salassa pidettävä tieto voi olla yksityisen tai perheen salaisuuden ohella myös yrityssalaisuus. Myös henkilötietolain ja sähköisen viestinnän tietosuojalain salassapitovelvoitteiden rikkominen rangaistaan tämän lainkohdan nojalla.

Salassapitovelvollisuutta koskeva sääntely on kaksiportainen. Rangaistussäännös on sijoitettu rikoslakiin, mutta salassapitovelvollisuuden varsinainen sisältö on jätetty täysin rikoslain ulkopuolisesta lainsäädännöstä riippuvaiseksi ja määräytyy eri laeissa ja asetuksissa olevan tai viranomaisen lain nojalla antaman määräyksen perusteella.

Salassapitorikokseen voi syyllistyä kahdella eri tavalla. Säännöksen ensimmäisessä kohdassa rangaistavaksi on säädetty pelkkä salaisuuden eli salassa pidettävä seikan paljastaminen. Vaihtoehtoisesti tunnusmerkistö voi täyttyä, mikäli henkilö pykälän toisessa kohdassa todetuin tavoin käyttää salaisuutta joko omaksi tai toisen hyödyksi.

Mikäli salassapitorikos on ollut kokonaisuutena arvioiden vähäinen, rangaistaan teko salassapitorikkomuksena (RL 38:2 §).

Laki sopimattomasta menettelystä elinkeinotoiminnassa sisältää myös yritys-salaisuuksiin liittyvää sääntelyä. Itsenäistä merkitystä SopMenL:n säännöksillä on kuitenkin erityisesti silloin, kun teko ei jostain syystä ole rikoslain perusteella rangaistava. SopMenL:n säännökset koskevat myös nimenomaan elinkeinon-harjoittajien välisiä suhteita asettaen elinkeinonharjoittajille liikesalaisuuksiin liittyviä velvoitteita, kun taas rikoslain ja työsopimuslain säännökset rajautuvat koskemaan luonnollisten henkilöiden toimintaa. Erityisestä syystä SopMenL:n mukainen kielto voidaan kohdistaa elinkeinonharjoittajan lisäksi myös tämän palveluksessa olevaan henkilöön tai muuhun, joka toimii hänen lukuunsa.

Mikäli kyse ei ole rangaistavasta teosta, voi yrityssalaisuuden taikka teknisen esikuvan tai ohjeen haltija hakea loukkaavan toiminnan kieltämistä markkinaoikeudessa. Erityistä merkitystä SopMenL:lla onkin silloin, kun halutaan kieltää elinkeinonharjoittajaa jatkamasta liikesalaisuuden taikka teknisen esikuvan tai ohjeen loukkausta.

SopMenL 4.1 §:n mukaan kukaan ei saa oikeudettomasti hankkia tai yrittää hankkia tietoa liikesalaisuudesta eikä käyttää tai ilmaista näin hankkimaansa tietoa. Säännös vastaa pitkälti RL 30:4 §:n yritysvakoilua koskevaa säännöstä. Tekijänä voi molemmissa olla joko yhtiön kilpailija tai oma työntekijä, edellyttäen, että tiedonhankinta on oikeudetonta. SopMenL:ssa kiellettyä on myös sellainen tiedonhankinta, jota ei ole suoritettu rikoslain yritysvakoilua koskevan säännöksen mukaisella erikseen luetellulla tekotavalla. Edellytyksenä ei myöskään ole, että tekijällä olisi jo tekohetkellä ollut tarkoitus oikeudettomasti ilmaista tai käyttää salaisuutta. Lisäksi SopMenL:ssa on erikseen kielletty yritysvakoilulla hankitun tiedon saman henkilön toimesta tapahtuva ilmaiseminen tai käyttäminen.

SopMenL 4.2 §:n perusteella elinkeinonharjoittajan palvelussuhteessa oleva ei saa palvelusaikanaan oikeudettomasti käyttää hyödykseen eikä ilmaista tietoonsa saamia liikesalaisuuksia, joko hankkiakseen itselleen tai toiselle etua tai toista vahingoittaakseen. Säännös vastaa RL 30:5 §:n yrityssalaisuuden rikkomista koskevaa säännöstä palvelussuhteessa olevan osalta (luettelon ensimmäinen kohta). Keskeisenä säännösten välisenä erona kuitenkin on, että SopMenL kieltää liikesalaisuuden käyttämisen ja ilmaisemisen vain palvelusuhteen aikana rikoslain ulottaessa rangaistavuuden tämän lisäksi kahteen vuoteen palvelussuhteen päättymisen jälkeen. Koska SopMenL 4 § ei erottele, onko kyse yhtiön omasta vai sen yhteistyökumppanin yrityssalaisuudesta, tulee myös yhtiön hallussa oleva yhteistyökumppanin yrityssalaisuus säännöksen nojalla suojatuksi. Kiellon vastaisen toiminnan kieltämistä voidaan vaatia kanteella markkinaoikeudessa ja vahingonkorvausta kanteella yleisessä tuomioistuimessa.

SopMenL 4.3 §:n mukaan joka elinkeinonharjoittajan puolesta tehtävää suorittaessaan on saanut tiedon liikesalaisuudesta tai jolle on työn tai tehtävän suorittamista varten uskottu tekninen esikuva tai ohje, ei saa sitä oikeudettomasti käyttää eikä ilmaista. Säännös vastaa pääosin RL 30:5 §:n yrityssalaisuuden rikkomista koskevaa säännöstä tehtävää toisen puolesta suorittavan osalta (luettelon kolmas kohta). Keskeistä säännöksen osalta on, että se asettaa ainoana säännöksenä yleisen salassapitovelvoitteen yhtiöiden välille. Erona RL 30:5 §:n lähes vastaavaan säännökseen on se, että rikoslain säännöksen koskiessa vain luonnollisia henkilöitä, voi elinkeinonharjoittajana tällöin tulla kyseeseen vain itsenäinen elinkeinonharjoittaja. Toisaalta rikoslain säännös on laajempi sen koskiessa myös muuta luottamuksellista liikesuhdetta – eli käytännössä myös sopimusneuvotteluja.

SopMenL 4.3 §:ssä on lisäksi kielletty teknisen esikuvan tai ohjeen oikeudeton käyttäminen ja ilmaiseminen, mikäli sellainen on uskottu työn tai tehtävän suorittamista varten taikka muuten liiketarkoituksessa. Teknisten esikuvien tai ohjeiden salaisuusaste voi olla liikesalaisuuksia olennaisesti alhaisempi ja tunnusmerkistö täyttyy liikesalaisuuksia helpommin. Mainittu on merkittävin ero varsinaisiin yrityssalaisuusrikoksiin ja liikesalaisuuksia koskeviin säännöksiin, jotka suojaavat vain selvästi salaista tietoa eli yritys- tai liikesalaisuuksia. Suoja koskee myös palvelussuhteen jälkeistä aikaa. Teknisten esikuvien ja ohjeiden osalta suojaa tarjotaan myös yhtiöiden välisessä suhteessa. Sääntely koskee myös elinkeinonharjoittajan omia työntekijöitä. Säännöksen mukaan liikesalaisuuden salassapitovelvollisuus koskee sitä, joka suorittaa tehtävää elinkeinoharjoittajan puolesta, kuten markkinointiyhtiö, elinkeinonharjoittajan toimeksiannosta työskentelevä mainostoimisto, arkkitehti, lakimies, tai konsultti.

SopMenL:n säännöksillä on merkitystä yhtiöiden välisen liikesalaisuuden salassapitovelvollisuuden määrittäjänä, sillä ne asettavat ainoina säännöksinä organisaatioiden tasolla yleisen yrityssalaisuuksia koskevan salassapitovelvoitteen. Mikäli kahden yhtiön välisessä liikesuhteessa ei ole solmittu salassapitosopimusta tai salassapitovelvollisuutta ei ole muulla perusteella olemassa, velvoittaa SopMenL 4.3 §:n liikesalaisuuksia vastaanottavan yhtiön pitämään tiedon salassa.

SopMenL 4.4 §:n perusteella se, joka on saanut toiselta tiedon liikesalaisuudesta, teknisestä esikuvasta tai teknisestä ohjeesta tietäen, että tämä on hankkinut tai ilmaissut tiedon oikeudettomasti, ei saa käyttää tai ilmaista sitä. Säännös vastaa pääosiltaan RL 30:6 §:n yrityssalaisuuden väärinkäyttöä koskevaa säännöstä. SopMenL:n väärinkäyttökielto on kuitenkin lisäksi ulotettu teknisiin esikuviin ja ohjeisiin, eikä kielto yrityssalaisuuden ilmaisemisen osalta edellytä hyötymistarkoitusta.

Edellä mainittujen liikesalaisuutta nimenomaisesti käsittelevien lainkohtien lisäksi SopMenL 1 §:n yleislausekkeen mukaan elinkeinotoiminnassa on kiellettyä käyttää hyvän tavan vastaista tai muutoin toisen elinkeinonharjoittajan kannalta sopimatonta menettelyä. Oikeuskirjallisuudessa SopMenL 1 §:n yleislauseketta on katsottu voitavan soveltaa lähinnä karkeissa väärinkäyttötilanteissa.

SopMenL lähtee siitä, että lainvastaisesti toimineeseen tahoon kohdistetaan kielto harjoittaa tiettyä toimintaa tulevaisuudessa. Elinkeinonharjoittajaa, joka vastoin 4 §:n säännöksiä on käyttänyt toisen liikesalaisuutta, teknistä esikuvaa tai ohjetta taikka ilmaissut sen, voidaan kieltää jatkamasta tai uudistamasta tällaista menettelyä.

Lakisääteisellä yrityssalaisuuksien suojalla on erityinen merkitys työnantajan ja työntekijän välisessä suhteessa, jota sääntelee työsopimuslaki. Työntekijän on lakiin

perustuvan työsuhteensa aikaisen lojaliteettivelvoitteen työnantajaansa kohtaan nojalla vältettävä toiminnassaan kaikkea, mikä on ristiriidassa hänen asemassaan olevalta työntekijältä kohtuuden mukaan vaadittavan menettelyn kanssa. Mainittu velvollisuus liittyy osaltaan liikesalaisuuksiin, joita loukkaavat teot on TSL 3:4 §:ssä säädetty kielletyiksi. TSL 3:4 §:n mukaan työntekijä ei saa työsuhteen kestäessä käyttää hyödykseen tai ilmaista muille työnantajansa ammatti- ja liikesalaisuuksia. Salassapitoaika rajoittuu siten työsuhteen kestoaikaan. Mikäli tieto on kuitenkin saatu oikeudettomasti, jatkuu kielto myös työsuhteen päättymisen jälkeen. Tahallisuutta ei edellytetä, vaan myös tuottamukselliset teot kuuluvat kiellon piiriin.

TSL:n vastaisesti liikesalaisuuden ilmaissut tai sitä käyttänyt on velvollinen korvaamaan työnantajalleen aiheuttamansa vahingon.[53] Työntekijän ohella vahingon korvaamisesta on TSL:n mukaan vastuussa myös se, jolle työntekijä ilmaisi tiedot, jos tiedon vastaanottaja tiesi tai hänen olisi pitänyt tietää työntekijän menettelyn oikeudettomuudesta.

7.5 Tietosuojasäännökset

7.5.1 Yleiset tietosuojasäännökset

Henkilötietolaki 523/1999 on EY-direktiiviin 1995/46/EY implementoinut henkilötietojen yleislaki, joka sääntelee henkilötietojen keräämistä, käsittelyä ja käyttöä. Henkilötietolakia täydentävät useat sektori- tai toimintokohtaiset lait. On arvioitu, että Suomessa noin 650 lakia tai asetusta sisältää tietosuojaa koskevia määräyksiä. Kuten edellä on todettu, on tietosuoja Suomessa nostettu perusoikeuden tasolle, mutta koska siitä on säädettävä tavallisella lailla, on normitulva ymmärrettävä.

Tietosuojaa koskevien lakien valvonta kuuluu pääsääntöisesti tietosuojavaltuutetulle, joskin Viestintävirastolla on tehtäviä sähköisen viestinnän tietosuojalain ja työsuojeluviranomaisilla puolestaan työelämää koskevan tietosuojalain valvonnassa.

Lain 32 §:ssä on direktiivin mukaiset tietoturvaa koskevat vaatimukset. Rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä. Toimenpiteiden toteuttamisessa on otettava huomioon käytettävissä olevat tekniset mahdollisuudet, toimenpiteiden aiheuttamat kustannukset,

[53] TSL 3:4.2 § ja 12:1.3 §.

käsiteltävien tietojen laatu, määrä ja ikä sekä käsittelyn merkitys yksityisyyden suojan kannalta. Sen, joka itsenäisenä elinkeinonharjoittajana toimii rekisterinpitäjän lukuun, on ennen tietojen käsittelyyn ryhtymistä annettava rekisterinpitäjälle asianmukaiset sitoumukset ja muutoin riittävät takeet henkilötietojen suojaamisesta edellä tarkoitetulla tavalla.

Laissa yksityisyyden suojasta työelämässä 759/2004 säädetään työntekijää koskevien henkilötietojen käsittelystä, työntekijälle tehtävistä testeistä ja tarkastuksista sekä niitä koskevista vaatimuksista, teknisestä valvonnasta[54] työpaikalla sekä työntekijän sähköpostiviestin hakemisesta ja avaamisesta. Mitä tässä laissa säädetään työntekijästä, sovelletaan myös virkamieheen sekä soveltuvin osin työnhakijaan.

Henkilötietojen käsittelyyn sovelletaan kuitenkin aina henkilötietolakia (523/1999) ja sähköisen viestinnän tietosuojalakia (516/2004), jollei tässä laissa toisin säädetä.

Pääperiaate on, että työnantajalla on oikeus hakea esille tai avata työnantajan työntekijän käyttöön osoittamaan sähköpostiosoitteeseen lähetettyjä tai työntekijän tällaisesta sähköpostiosoitteesta lähettämiä sähköpostiviestejä ainoastaan silloin, jos hän on suunnitellut ja järjestänyt työntekijälle tämän nimellä lähetettyjen ja tämän lähettämien sähköpostiviestien suojan toteuttamiseksi tarpeelliset toimenpiteet ja tässä tarkoituksessa erityisesti huolehtinut siitä, että:

1. työntekijä voi käytettävän sähköpostijärjestelmän automaattisen vastaustoiminnon avulla lähettää viestin lähettäjälle ilmoituksen poissaolostaan ja sen kestosta sekä tiedon henkilöstä, joka hoitaa poissa olevalle työntekijälle kuuluvia tehtäviä; tai
2. työntekijä voi ohjata viestit toiselle työnantajan tähän tehtävään hyväksymälle henkilölle tai toiseen omassa käytössään olevaan työnantajan hyväksymään osoitteeseen; taikka
3. työntekijä voi antaa suostumuksensa siihen, että työntekijän poissa ollessa tämän valitsema työnantajan tehtävään hyväksymä toinen henkilö voi ottaa vastaan työntekijälle lähetetyt viestit sen selvittämiseksi, onko työntekijälle lähetetty sellainen viesti, joka on selvästi tarkoitettu työnantajalle työtehtävien hoitamiseksi ja josta työnantajan on toimintansa tai työtehtävien asianmukaisen järjestämisen vuoksi välttämätöntä saada tieto.

Työnantajalla on oikeus tietojärjestelmän pääkäyttäjän valtuuksia käyttävän henkilön avulla ottaa viestin lähettäjää, vastaanottajaa tai viestin otsikkoa koskevien tietojen perusteella selville, onko työntekijälle lähetetty tämän poissa ollessa tai onko työntekijä

[54] Kameravalvontaa on käsitelty erillisenä asiakokonaisuutena jäljempänä.

välittömästi ennen poissaoloaan lähettänyt tai vastaanottanut työnantajalle kuuluvia viestejä, joista työnantajan on toimintaansa liittyvien neuvottelujen loppuun saattamiseksi, asiakkaiden palvelemiseksi tai toimintojensa turvaamiseksi muutoin välttämätöntä saada tieto, jos:

1. työntekijä hoitaa tehtäviä itsenäisesti työnantajan lukuun eikä työnantajan käytössä ole järjestelmää, jonka avulla työntekijän hoitamat asiat ja niiden käsittelyvaiheet kirjataan tai saadaan muutoin selville;
2. työntekijän tehtävien ja vireillä olevien asioiden vuoksi on ilmeistä, että työnantajalle kuuluvia viestejä on lähetetty tai vastaanotettu;
3. työntekijä on estynyt tilapäisesti suorittamasta työtehtäviään eikä työnantajalle kuuluvia viestejä siitä huolimatta, että työnantaja on huolehtinut 18 §:ssä tarkoitetuista velvollisuuksistaan, voida saada työnantajan käyttöön; ja
4. työntekijän suostumusta ei voida saada kohtuullisessa ajassa ja asian selvittäminen ei kestä viivytystä.

Jos työntekijä on kuollut tai jos hän on pysyväisluonteisesti estynyt suorittamasta työtehtäviään eikä hänen suostumustaan voida saada, työnantajalla on tietyin edellytyksin oikeus ottaa viestin lähettäjää tai vastaanottajaa taikka viestin otsikkoa koskevien tietojen perusteella selville työnantajalle kuuluvat viestit, jollei työntekijän hoitamien asioiden selville saaminen ja työnantajan toiminnan turvaaminen ole muilla keinoilla mahdollista. Jollei viestin esille hakeminen johda viestin avaamiseen, siitä on laadittava siihen osallistuneiden henkilöiden allekirjoittama selvitys, josta ilmenee, miksi viestiä on haettu, hakemisen ajankohta ja sen suorittajat.

Jos sähköisen viestin lähettäjää tai vastaanottajaa taikka viestin otsikkoa koskevan tiedon perusteella on ilmeistä, että työntekijälle lähetetty tai työntekijän lähettämä viesti on selvästi työnantajalle kuuluva viesti, jonka sisällöstä työnantajan on toimintaansa liittyvien neuvottelujen loppuun saattamiseksi, asiakkaiden palvelemiseksi tai toimintojensa turvaamiseksi välttämätöntä saada tieto eikä viestin lähettäjään tai vastaanottajaan saada yhteyttä viestin sisällön selvittämiseksi tai sen lähettämiseksi työnantajan osoittamaan osoitteeseen, työnantaja saa avata viestin erikseen luetelluissa tapauksissa tietojärjestelmän pääkäyttäjän valtuuksia käyttävän henkilön avulla toisen henkilön läsnä ollessa.

Avaamisesta on laadittava siihen osallistuneiden henkilöiden allekirjoittama selvitys, josta ilmenee, mikä viesti on avattu, miksi viesti on avattu, avaamisen ajankohta, avaamisen suorittajat sekä kenelle avatun viestin sisällöstä on annettu tieto.

Työntekijöiden valvonnan osalta voidaan todeta, että työntekijöihin kohdistuvan kameravalvonnan, kulunvalvonnan ja muun teknisin menetelmin toteutetun valvonnan tarkoitus, käyttöönotto ja siinä käytettävät menetelmät sekä sähköpostin ja muun tietoverkon käyttö kuuluvat yhteistoiminnasta yrityksissä annetussa laissa ja yhteistoiminnasta valtion virastoissa ja laitoksissa annetussa laissa tarkoitetun yhteistoimintamenettelyn piiriin. Muissa kuin yhteistoimintalainsäädännön piiriin kuuluvissa yrityksissä ja julkisoikeudellisissa yhteisöissä työnantajan on ennen päätöksentekoa varattava työntekijöille tai heidän edustajilleen tilaisuus tulla kuulluksi edellä mainituista asioista.

Yhteistoiminta- tai kuulemismenettelyn jälkeen työnantajan on määriteltävä työntekijöihin kohdistuvan teknisin menetelmin toteutetun valvonnan käyttötarkoitus ja siinä käytettävät menetelmät sekä tiedotettava työntekijöille valvonnan tarkoituksesta, käyttöönotosta ja siinä käytettävistä menetelmistä sekä sähköpostin ja tietoverkon käytöstä.

Sähköisen viestinnän tietosuojalaki 516/2004 tuli voimaan 1.9.2004. Sen tarkoituksena on lain 1 §:n mukaisesti turvata sähköisen viestinnän luottamuksellisuuden ja yksityisyyden suojan toteutuminen sekä edistää sähköisen viestinnän tietoturvaa ja monipuolisten sähköisen viestinnän palvelujen tasapainoista kehittymistä.

Sähköisen viestinnän tietosuojalailla pannaan Suomessa voimaan sähköisen viestinnän tietosuojadirektiivi 2002/58/EY. Laki on kuitenkin pidemmälle menevä ja seikkaperäisempi kuin itse direktiivi ja sisältää myös tavallisiin yrityksiin ja muihin yhteisöihin kohdistuvia määräyksiä. Lain uudistaminen on vireillä mm. yritys-salaisuuksien suojan parantamiseksi, mutta hallituksen esitystä asiasta ei ole vielä annettu.

Lakia ei sovelleta sisäisiin ja muihin rajoitetuille käyttäjäpiireille tarkoitettuihin viestintäverkkoihin, ellei näitä verkkoja ole liitetty yleiseen viestintäverkkoon. Lain 4 ja 5 §:ää eli viestin, tunnistamistietojen ja paikkatietojen luottamuksellisuutta sekä vaitiolovelvollisuutta ja hyväksikäyttökieltoa koskevia sääntöjä sovelletaan kuitenkin myös sisäisiin ja muihin rajoitetuille käyttäjäpiireille tarkoitettuihin viestintäverkkoihin, vaikka näitä verkkoja ei ole liitetty yleiseen viestintäverkkoon. Lakia ei sovelleta verkkopankkitoimintaan eikä sitä sovelleta, jos rahanpesun estämisestä ja selvittämisestä annetusta laista (68/1998) muuta johtuu.

Sähköisen viestinnän tietosuojadirektiiviä Suomessa täytäntöön pantaessa otettiin lähtökohdaksi suomalainen yleiskieli eikä direktiivin mukaiset määritelmät. Kun direktiivissä määritellään käyttäjä, määritellään laissa myös tilaaja eli oikeushenkilö tai luonnollinen henkilö, joka on tehnyt sopimuksen viestintäpalvelun tai lisäarvopalvelun

toimittamisesta. Yhteisötilaajalla tarkoitetaan puolestaan viestintäpalvelun tai lisäarvopalvelun tilaajana olevaa yritystä tai yhteisöä, joka käsittelee viestintäverkossaan käyttäjien luottamuksellisia viestejä, tunnistamistietoja tai paikkatietoja.

Direktiivissä puhutaan liikennetiedoista, kun taas laissa puhutaan tunnistamistiedoista. Tunnistamistiedolla tarkoitetaan tilaajaan tai käyttäjään yhdistettävissä olevaa tietoa, jota viestintäverkoissa käsitellään viestien siirtämiseksi, jakelemiseksi tai tarjolla pitämiseksi. Suomen perustuslakivaliokunta on katsonut lausunnoissaan[55], että myös tunnistamistiedot nauttivat luottamuksellisuuden suojaa.

Tunnistamistietoihin voi kuulua tietoja, jotka viittaavat mm. viestinnän reititykseen, kestoon, ajankohtaan tai siirrettävän tiedon määrään, käytettyyn protokollaan, lähettäjän ja vastaanottajan päätelaitteen sijaintiin tietyn tukiaseman alueella, lähetettävään tai vastaanottavaan verkkoon ja yhteyden alkuun loppuun tai kestoon. Tunnistamistiedot voivat koskea myös muotoa, jossa viesti välitetään verkossa. Tilaaja, johon tunnistamistieto voidaan yhdistää, voi olla luonnollisen henkilön lisäksi myös oikeushenkilö. Näin ollen myös oikeushenkilöt voivat nauttia luottamuksellisen viestin suojaa. Lain 4 §:n 2 momentissa todetaan, että vaikka itse viesti ei ole luottamuksellinen silloin, kun se on saatettu yleisesti vastaanotettavaksi, ovat viestiin liittyvät tunnistamistiedot, joihin luetaan myös tilaajien ja käyttäjien IP-osoitteet, kuitenkin luottamuksellisia. Tällaiset tietoihin on mahdollista päästä käsiksi vain pakkokeinona sananvapauslain 17 §:n perusteella. Myös verkkosivujen selaamisesta kertyvät tunnistamistiedot ovat luottamuksellisia (4 §:n 3. momentti).

Se, joka on ottanut vastaan tai muutoin saanut tiedon luottamuksellisesta viestistä tai tunnistamistiedosta, jota ei ole hänelle tarkoitettu, ei saa ilman viestinnän osapuolen suostumusta ilmaista tai käyttää hyväksi viestin sisältöä, tunnistamistietoa tai tietoa viestin olemassaolosta, ellei laissa toisin säädetä (5 § 1). Vastaava määräys on säädetty myös paikkatiedoista (5 § 2). Lisäksi teleyrityksen, lisäarvopalvelun tarjoajan, yhteisötilaajan tai viestintämarkkinalain 137 §:ssä tarkoitetun teleurakoitsijan palveluksessa oleva tai ollut ei saa ilman viestinnän osapuolen tai paikannettavan suostumusta ilmaista, mitä hän on tehtävässään saanut tietää viesteistä, tunnistamistiedoista ja paikkatiedoista, ellei laissa toisin säädetä. Tällainen vaitiolovelvollisuus on myös sillä, joka toimii tai on toiminut teleyrityksen, lisäarvopalvelun tarjoajan, yhteisötilaajan tai teleurakoitsijan lukuun. Tämä velvollisuus koskee siis alihankintasuhteitakin.

Sähköisen viestinnän tietosuojalaissa säännellään yksityiskohtaisesti tunnistamistietojen käsittelyä. Nämä määräykset seuraavat pitkälle direktiivin sisältöä.

---

[55] Ks. perustuslakivaliokunnan mietinnöt PeVL 3/1992 vp ja 47/1996 vp.

Käsittelyä laskutusta varten sääntelevän 10 §:n 3. momentin mukaan tietoyhteiskunnan palvelujen tarjoamisesta annetussa laissa (458/2002) tarkoitettu tietoyhteiskunnan palvelun tarjoaja voi käsitellä teleyrityksen hallinnoiman viestintäverkon välityksellä tarjottavien kuvatallenteiden, äänitallenteiden ja muiden maksullisten palvelujensa laskutusta varten välttämättömiä tunnistamistietoja ja muita laskutuksen kannalta välttämättömiä tietoja, jos tilaaja tai käyttäjä, jota tiedot koskevat, on antanut siihen suostumuksensa.

Saman pykälän 4. momentin mukaan tietoyhteiskunnan palvelun tarjoajalla on oikeus saada teleyritykseltä edellä tarkoitetut tiedot. Luovutuksen saajaan sovelletaan lain määräyksiä viestinnän luottamuksellisuudesta ja yksityisyyden suojasta, viestien ja tunnistamistietojen käsittelystä, paikkatietojen käsittelystä ja viestinnän tietoturvasta lisäarvopalvelun tarjoajan osalta. Näin annetaan tietoyhteiskunnan palvelujen tarjoajalle oikeus saada teleyritykseltä sellaiset tiedot, joiden luovuttamiseen tilaaja tai käyttäjät, jota tiedot koskevat, on antanut suostumuksensa. Teleyritys ei saa kieltäytyä tällaisten tietojen luovuttamisesta tietoyhteiskunnan palvelujen tarjoajalle. Teleyritys voi periä tietojen luovuttamisesta tietoyhteiskunnan palvelun tarjoajalta asianmukaisen maksun. Samaisessa 4. momentissa säädetään teleyrityksen ja lisäarvopalvelun tarjoajan velvollisuudesta ilmoittaa tilaajalle tai käyttäjälle, millaisia tunnistamistietoja käsitellään ja kuinka kauan niiden käsittely kestää. Tällainen ilmoittaminen voi tapahtua esimerkiksi liittymäsopimuksen tekemisen yhteydessä sopimustekstissä tai Internetissä julkaistavissa sopimusehdoissa.

Laskun määräytymiseen liittyviä tietoja on säilytettävä 5. momentin mukaan vähintään kolme kuukautta laskun eräpäivästä tai tunnistamistiedon tallentumisesta riippuen siitä, kumpi näistä ajankohdista on myöhäisempi. Tietoja ei saa kuitenkaan säilyttää enää sen jälkeen, kun saatava on velan vanhentumisesta annetun lain (728/2003) mukaan vanhentunut. Laskua koskevan erimielisyyden synnyttyä laskua koskevat tiedot on kuitenkin säilytettävä siihen saakka, kunnes asia on sovittu tai ratkaistu. Velan vanhentumisesta annetun lain 4 §:ssä säädetään yleisestä vanhentumisajasta siten, että velka vanhentuu kolmen vuoden kuluttua kyseisen lain 5, 6 ja 7 §:ssä tarkoitetusta ajankohdasta, jollei vanhentumista ole sitä ennen katkaistu.

Lain 11 §:ssä mahdollistetaan tunnistetietojen käsittely markkinointitarkoituksiin. Direktiivin määräyksistä poiketen mahdollistetaan teletietojen käsittely myös teknistä kehittämistä varten (12 §). Myös yhteisötilaaja voi käsitellä tunnistamistietoja oman toimintansa teknistä kehittämistä varten. Sähköisen viestinnän tietosuojalakia ollaan eräiltä osin uusimassa. Tarkoituksena on laajentaa 12 §:n soveltamisalaa myös toiminnan kaupalliseen kehittämiseen. Tunnistamistietojen käsittely on Suomen laissa mahdollistettu nimenomaisesti myös teknisen vian tai virheen havaitsemiseksi.

Lain 15 §:ssä on määräys, jonka mukaan teleyrityksen on tallennettava tunnistamistietojen käsittelystä yksityiskohtaiset tapahtumatiedot, joista käy ilmi käsittelyn ajankohta, kesto ja käsittelijä. Käsittelyä koskevat tapahtumatiedot on säilytettävä kaksi vuotta niiden tallentamisesta. Direktiivin ei sellaisenaan katsota edellyttävän tallettamisvelvollisuuden asettamista.

Lain 16, 17 ja 18 § sääntelevät yksityiskohtaisesti paikkatietojen käsittelyä. Paikkatiedoilla ymmärretään laissa samaa kuin sähköisen viestinnän tietosuojadirektiivissä. Direktiivi edellyttää, kuten edellä on todettu, käyttäjän ja tilaajan suostumusta paikkatietojen käsittelyyn. Suomen laissa säännellään myös paikannettavan suostumusta. Paikannettavalla tarkoitetaan sitä luonnollista henkilöä, jolla on hallinnassaan paikannettava liittymä tai päätelaite. Paikannettavalta on pyydettävä palvelukohtainen suostumus ennen kuin häntä koskevia paikkatietoja aletaan käsitellä. Suostumus voi tosin ilmetä myös asiayhteydestä. Teleyrityksen, jonka menetelmin paikannus tapahtuu, edellytetään varmistavan lähinnä sopimusteitse lisäarvopalvelun tarjoajan tai yhteisötilaajan toimien asianmukaisuuden ja luotettavuuden. Teleyrityksen tulee tuntea tarjottava paikkatietoihin perustuva palvelu ja kyetä arvioimaan lisäarvopalvelun tarjoajan noudattamien menettelyjen asianmukaisuus paikannettavan palvelukohtaisen suostumuksen pyytämisen osalta.

Lain 5. luku eli 19–21 §§, sääntelee viestinnän tietoturvaa. Teleyrityksen ja lisäarvopalvelun tarjoajan on huolehdittava palvelujensa tietoturvasta. Vastaavasti yhteisötilaajan on huolehdittava käyttäjiensä tunnistamistietojen ja paikkatietojen käsittelyn tietoturvasta. Kuten direktiivissäkin todetaan, tietoturva on suhteutettava uhkien vakavuuteen, tekniseen kehitystasoon ja kustannuksiin.

Vaikka itse lakiteksti onkin yleisluonteinen, sisältävät lain esityöt täsmällisempiä kuvauksia siitä, mitä yrityksiltä ja muilta toimijoilta käytännössä edellytetään. Hallituksen esityksessä[56] todetaan aikaisemmin mainitun mukaisesti: ”tietoturvalla tarkoitetaan laissa hallinnollisia ja teknisiä toimia, joilla varmistetaan se, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla, ettei tietoja voida muuttaa muun kuin siihen oikeutetun toimesta ja että tiedot ja tietojärjestelmät ovat niihin oikeutettujen hyödynnettävissä”.

Hallituksen esityksessä kuvataan edelleen yksityiskohtaisesti tietoturvatoimien luonnetta. Kuvaukset ja lakitekstissä olevan yleisvelvoitteen muodostavat konkreettisemman velvoitteen juuri kyseisiin toimiin, joiden toteutustapa rakentuu Viestintäviraston ohjeistuksen pohjalle. Viestintäviraston antama ohjeistus on tähän

[56] HE125/2003 vp.

mennessä koskenut vain teleyrityksiä.[57] Hallinnolliset ja tekniset toimet kohdistuvat toiminnan turvallisuuteen, tietoliikenneturvallisuuteen, laitteistoturvallisuuteen ja ohjelmistoturvallisuuteen sekä tietoaineistoturvallisuuteen.

Toiminnan turvallisuudella tarkoitetaan muun muassa sitä, että ”ylläpidetään kirjallisia ohjeita siitä, miten tietoturvavaatimukset toteutetaan, oman tietoturvan tasoa seurataan säännöllisesti, varmistetaan tietoturvavaatimusten toteutuminen käytettäessä alihankkijoita ja suojataan laitteet ja tiedostot luvatonta pääsyä ja käyttöä vastaan”. Lisäksi toiminnan turvallisuudella tarkoitetaan sitä, että ”pidetään rekisteriä kunkin järjestelmän osalta siitä, kenellä on järjestelmän käyttäjätunnuksia ja mitä oikeuksia milläkin käyttäjätunnuksella on ja valvotaan tietojen, asiakirjojen, viestintäverkkojen, laitteistojen, palvelujen ja tiedostojen tietoturvaan vaikuttavia tapahtumia niin, että tietoturvan kannalta merkittävät tapahtumat havaitaan”.

Tietoliikenneturvallisuudella tarkoitetaan muun muassa sitä, että ”viestintäverkkojen avulla välitettävät viestit ja tunnistamistiedot eivät paljastu asiaankuulumattomille ja asiaankuulumattomat eivät pääse muuttamaan tai tuhoamaan viestintäverkoissa välitettäviä viestejä”. Lisäksi tietoliikenneturvallisuudella tarkoitetaan sitä, että ”viestintäverkoissa on toiminnan kannalta riittävät todentamismenettelyt, pääsynvalvontamenettelyt ja kiistämättömyysmenettelyt, ja että asiaankuulumattomat eivät pääse tunnistamistietoihin tai käsittelyä koskeviin tietoihin”.

Laitteistoturvallisuudella ja ohjelmistoturvallisuudella tarkoitetaan muun muassa sitä, että ”käytetään sellaisia laitteistoja, tietojärjestelmiä ja ohjelmistoja, joista aiheutuva tietoturvauhka on vähäinen sekä järjestetään toiminnan kannalta tärkeiden ohjelmistojen varmuuskopiointi ja turvallinen säilytys”.

Tietoaineistoturvallisuudella tarkoitetaan muun muassa sitä, että ”järjestetään tietoaineistojen turvallinen käsittely hyvän tietojenkäsittelytavan mukaisesti, järjestetään tietoaineistojen varmuuskopiointi ja turvallinen säilytys sekä suojataan tärkeät asiakirjat, tietovarastot ja yksittäiset tiedot”.

---

[57] Viestintävirasto 9 B/2004 M, määräys tietoturvaloukkausten sekä vika- ja häiriötilanteiden ilmoittamisvelvollisuudesta yleisessä teletoiminnassa SMS 9 B, suositus määräyksen Viestintävirasto 9 B/2004 M soveltamisesta.

Viestintävirasto 11/2004 M, määräys sähköpostipalvelujen tietoturvasta ja toimivuudesta SMS 11, suositus määräyksen Viestintävirasto 11/2004 M soveltamisesta.

Viestintävirasto 47 B/2004 M, määräys teleyritysten tietoturvasta SMS 47 B, suositus määräyksen THK 47/1999 M soveltamisesta. Suositus Viestintävirasto 308/2004 S tunnistamistietojen käsittelyä koskevien tietojen tallentamisesta Viestintävirasto 48 B/2004 M, määräys viestintäverkon fyysisestä suojaamisesta SMS 48 B, suositus määräyksen Viestintävirasto 48 A/2003 M soveltamisesta.

Alihankkijoiden käytön ja siis toimintojen ulkoistamisen kannalta merkityksellinen määräys on 19 §:n 2. momentissa, jossa todetaan, että teleyritys tai lisäarvopalvelun tarjoaja vastaa tilaajille ja käyttäjille tietoturvasta myös sellaisen kolmannen osapuolen osalta, joka kokonaan tai osittain toteuttaa verkkopalvelun, viestintäpalvelun tai lisäarvopalvelun. Yhteisötilaajaa tämä koskee käyttäjien tunnistamistietojen ja paikka-tietojen osalta.

Tietoturvaloukkausten torjumiseksi ja tietoturvaan kohdistuvien häiriöiden poistamiseksi teleyrityksellä tai lisäarvopalvelun tarjoajalla tai yhteisötilaajalla ja näiden lukuun toimivalla on oikeus ryhtyä välttämättömiin toimiin 19 §:ssä tarkoitetun tietoturvan varmistamiseksi estämällä sähköpostiviestien, tekstiviestien ja muiden vastaavien viestien vastaanottaminen poistamalla haittaohjelmat viesteistä sekä toteuttamalla muut välttämättömät toimenpiteet. Kuten hallituksen esityksessä todetaan, sähköisen viestinnän tietosuojadirektiivin ei voida katsoa välittömällä tavalla edellyttävän edellä mainittuja toimia mutta ne ovat toisaalta sopusoinnussa direktiivin yleisvelvoitteiden kanssa.

Viestintään puuttuminen on luonnollisesti uhka perusoikeuksien toteutumiselle. Teleyrityksen ja lisäarvopalvelun tarjoajan sekä yhteisötilaajan on tiedostettava viestintään puuttumiseen sisältyvä uhka siitä, että toteutettavien toimien seurauksena myös toivottuja luottamuksellisia viestejä ja vastaanottajan pyytämää mainontaa voi jäädä saapumatta vastaanottajalle. Sen vuoksi lainkohdassa tarkoitetut toimet tulee toteuttaa hyvin huolellisesti ja käyttäjiä mahdollisuuksien mukaan informoiden. Toimista on pidättäydyttävä, jollei voida varmistua siitä, että toimilla saavutettava hyöty on luottamuksellisen viestin suojalle ja sananvapaudelle aiheutuvaa haittaa olennaisesti suurempi.

Lain 21 §:ssä on säädetty teleyritykselle ja lisäarvopalvelun tarjoajalle ilmoitus-velvollisuus tietoturvauhan kohdistuessa niiden palveluun. Jos tällaisen palvelun tietoturvaan kohdistuu erityinen uhka, teleyrityksen ja lisäarvopalvelun tarjoajan on ilmoitettava uhkasta viipymättä tilaajalle ja kerrottava samalla tilaajan ja käyttäjän käytettävissä olevista toimenpiteistä uhkan torjumiseksi sekä niiden todennäköisistä kustannuksista.

Teleyrityksen on ilmoitettava Viestintävirastolle verkkopalvelun ja viestintäpalvelun merkittävistä tietoturvaloukkauksista ja sellaisista niihin kohdistuvista tietoturvauhkista, joista teleyritys on tietoinen. Lisäksi teleyrityksen on ilmoitettava Viestintävirastolle palvelujen merkittävistä vikatilanteista ja häiriötilanteista. Samalla on ilmoitettava toimenpiteistä, joilla tällaisten tietoturvaloukkausten ja niiden uhkien sekä vika- ja häiriötilanteiden toistuminen pyritään estämään. Viestintävirastolle tehtävässä ilmoituksessa on lisäksi kerrottava toimista, joihin on ryhdytty edellä tarkoitettujen

tapausten johdosta ja joilla tapausten toistuminen pyritään estämään. Loukkauksen, sen uhan ja vian tai häiriön merkittävyyttä arvioitaessa on kiinnitettävä huomiota tilaajien ja käyttäjien oikeuksien suojaan, palvelun käytettävyyteen ja maantieteellisten vaikutusten laajuuteen. Ilmoitus on tehtävä välittömästi, kun asian merkittävyys on todettu. Ilmoituksesta on käytävä selkeästi ilmi, mihin toimiin asian johdosta on ryhdytty ja mahdollisuuksien mukaan myös se, miten ongelma voidaan tulevaisuudessa estää. Jos tulevaisuudessa toteutettavia toimia ei kyetä ilmoituksen yhteydessä kertomaan, ilmoitusta tulee täydentää ilman aiheetonta viivytystä.

Tietoturvan osalta laissa on määräyksiä teleyrityksen velvollisuudesta maksaa tietoturvamaksua (38 §).

Sähköisen viestinnän tietosuojalain 6. luvussa on toteutettu direktiivissä tarkoitettu puhelupalveluiden tietosuojan sääntely. Lain 22 §:ssä säännellään liittymän tunnistusta ja 23 §:ssä automaattista soitonsiirtoa. Teleyrityksen on käyttäjän pyynnöstä maksutta poistettava kolmannen osapuolen tekemä automaattinen soitonsiirto käyttäjän liittymään. Direktiivissä tämä oikeus on tilaajalla.

Laskutuksen yhteyskohtaista erittelyä koskevat tietosuojasäännöt sisältyvät lain 24 §:ään. Pääsääntö on, ettei teleyritys saa luovuttaa laskun yhteyskohtaista erittelyä kuin laskun oikeellisuuden varmistamiseksi. Tilaajalla on nimittäin viestintämarkkinalain 80 §:ssä annettu oikeus eriteltyyn laskutukseen. Prepaid-liittymiin ja kiinteisiin liittymiin, joissa tätä ongelmaa ei ole, ei poikkeusta voida siten soveltaa. Pelkkä laskun maksamisvelvollisuus ei ole sellaisenaan riittävä peruste saada täydelliset tiedot liittymästä otettujen yhteyksien numeroista silloin, kun laite on luvallisesti toisen henkilön, esimerkiksi työntekijän, hallinnassa. Yhteyskohtainen erittely on ehdotetun momentin mukaan annettava tilaajalle siten, ettei siitä voida tunnistaa viestinnän toista osapuolta. Laskussa ei saa ilmaista liittymien tunnisteiden kolmea viimeistä numeroa tai jos tunniste ei ole pelkkä numerosarja, tunniste on tehtävä muutoin sellaiseksi, ettei siitä voida tunnistaa toista osapuolta.

Puhelimella voidaan kuitenkin nykyään ostaa palveluja, joita veloitetaan puhelinlaskussa. Teleyrityksen onkin annettava tilaajalle erittely palvelutyypeittäin sellaisista yhteyksistä, joista aiheutuu tilaajalle muita kuin viestintäpalvelun käytöstä aiheutuvia maksuja. Tätä säännöstä ollaan kuitenkin parhaillaan muuttamassa.

Lain 25 §:n mukaan puhelinluettelon, muun tilaajaluettelon ja numerotiedotuksen tarjoajalla on oikeus käsitellä henkilötietoja luettelopalvelun ja numerotiedotuksen muodostamiseksi sekä niiden tarjoamista varten. Teleyrityksen on annettava tilaajana olevalle luonnolliselle henkilölle mahdollisuus maksutta kieltää tietojensa merkitseminen kokonaan tai osittain puhelinluetteloon, muuhun tilaajaluetteloon ja numero-

tiedotuspalveluun. Samoin tilaajana olevalla luonnollisella henkilöllä on oikeus maksutta kieltää ehdotetussa pykälässä tarkoitettujen yhteystietojensa edelleen-luovuttaminen. Myös yrityksellä on oikeutensa: teleyrityksen on nimittäin annettava puhelinluetteloon, muuhun tilaajaluetteloon ja numerotiedotuspalveluun merkitylle yritykselle ja muulle yhteisölle oikeus saada tietonsa tarkistetuiksi ja poistetuiksi sekä virheelliset tiedot korjatuiksi.

Lain 7 luku käsittelee suoramarkkinointia. Lain 26 §:n mukaan automatisoitujen soitto-järjestelmien sekä telekopiolaitteiden, sähköpostiviestien, tekstiviestien, puheviestien, ääniviestien ja kuvaviestien avulla toteutettua suoramarkkinointia saa kohdistaa vain sellaisiin luonnollisiin henkilöihin, jotka ovat antaneet siihen ennalta suostumuksensa. Markkinoinnin käsite on määritelty kuluttajansuojalaissa. Suoramarkkinointia ei ole esimerkiksi asiakasviestintä.

Toisaalta sähköisen viestinnän tietosuojalain 27 §:n mukaan suoramarkkinointia yhteisölle saa harjoittaa, jollei tämä ole sitä nimenomaisesti kieltänyt. Kun 26 §:n mukaan pääsääntönä on, ettei suoramarkkinointia voi lähettää luonnolliselle henkilölle ilman tämän suostumusta, mutta viestejä voi kuitenkin lähettää, jos luonnollinen henkilö toimii yhteisön puolesta tietyssä tehtävässä, johon suoramarkkinoinnilla tarjottavat hyödykkeet ja palvelut olennaisesti liittyvät, on myös tällaisella henkilöllä oikeus kieltää suoramarkkinoinnin lähettäminen. Yhteisölle on annettava mahdollisuus helposti ja ilman erillistä maksua kieltää yhteystietojensa käyttö jokaisen suoramarkkinointi-tarkoituksessa lähetetyn sähköpostiviestin, tekstiviestin, puheviestin, ääniviestin ja kuvaviestin yhteydessä. Suoramarkkinointia harjoittavan on selkeästi tiedotettava kieltomahdollisuudesta. Suoramarkkinointiin tarkoitettu sähköpostiviesti, tekstiviesti, puheviesti, ääniviesti ja kuvaviesti on voitava sitä vastaanotettaessa selvästi ja yksiselitteisesti tunnistaa markkinoinniksi.

Lain 29 §:n mukaan teleyrityksellä ja yhteisötilaajalla on oikeus käyttäjän niin pyytäessä estää edellä tarkoitetun sähköisen suoramarkkinoinnin eli lähinnä roskapostin vastaan-ottaminen. Toimenpiteet on kuitenkin toteutettava huolellisesti sekä luottamuksellisen viestin ja yksityisyyden suojaa tarpeettomasti vaarantamatta. Teleyritykselle on siis luotu oikeus tai yhteisötilaajalle suodattaa pois tietyillä kriteereillä sellaiset viestit, joita käyttäjä ei halua päätelaitteelleen silloin, kun käyttäjä on sitä pyytänyt. Hallituksen esityksessä todetaan, että käytännössä saattaa kuitenkin olla mahdotonta, että tietyissä yhteisöissä joidenkin käyttäjien viestinnästä poistetaan tietyin kriteerein ei-toivottu viestintä, mutta joidenkin viestintään ne jätetään. Tällöin suodatuskriteerit tulisi sisällyttää yhteisön sähköpostin käyttöoikeusehtoihin taikka vastaaviin sääntöihin, jotka hyväksymällä käyttäjän voitaisiin katsoa antaneen ehdotetussa pykälässä tarkoitetun suostumuksen. Käytettäessä suodattimia saattaa osa myös luottamuksellisiksi katsotuista toivotuista viesteistä jäädä saapumatta vastaanottajalle. Teleyrityksen tulisi

antaa käyttäjälle hallituksen esityksen mukaan mahdollisimman tarkat ja kattavat tiedot suodatustavasta ja siitä, mitä riskejä suodattamiseen sisältyy. Esimerkiksi sopimuksen syntymiseen ja sopimuksenaikaisiin ilmoituksiin liittyvät oikeusvaikutukset saattavat syntyä tai olla syntymättä kommunikaation jouduttua suodatuksen kohteeksi.

Esimerkkeinä muista tietosuojasäännöksiä sisältävistä laeista voidaan mainita:

Laki henkilötietojen käsittelystä poliisitoimessa (2003/761) on toimintokohtainen laki, joka sääntelee henkilötietojen käsittelyä mm. esitutkinnan yhteydessä. Valmisteluasteella on myös lakiehdotus henkilötietojen käsittelystä oikeushallinnossa www.om.fi/275771.htm.

Erityinen tietosuojasäännös on **Laki potilaan asemasta ja oikeuksista**, 785/1992, jonka 13 §:ssä säädetään potilasasiakirjojen salassapidosta, minkä lisäksi laissa säädetään rikosoikeudellisesta seuraamuksesta potilassalaisuuden rikkomistapauksissa.

7.5.2 Kameravalvonta

Suomessa ei ole yhtenäistä, nimenomaan kameravalvontaa koskevaa lainsäädäntöä. Kuitenkin yksityiselämän suoja koskee myös kameravalvontaa.

Kameravalvontaa koskevat tai sen käyttöä rajoittavat Suomessa rikoslain salakatselua ja -kuuntelua koskevat säännökset (RL 24:5–7), joita on viimeksi muutettu vuonna 2000. Lisäksi kameravalvontaa sääntelee henkilötietolaki (523/1999) ja tähän liittyen henkilörekisteririkosta (RL 38:9) koskevat säännökset. Euroopan neuvostossa on ollut valmisteilla henkilötietojen käsittelyä kameravalvonnan yhteydessä koskeva suositus. Rikoslain 24 luvun 5 § määrittää salakuuntelun oikeudettomasti teknisellä laitteella kuuntelemiseksi tai tallentamiseksi, joka kohdistuu

- keskusteluun, puheeseen tai yksityiselämästä aiheutuvaan muuhun ääneen, jota ei ole tarkoitettu hänen tietoonsa ja joka tapahtuu tai syntyy kotirauhan suojaamassa paikassa, taikka
- muualla kuin kotirauhan suojaamassa paikassa puheeseen, jota ei ole tarkoitettu hänen eikä muunkaan ulkopuolisen tietoon, sellaisissa olosuhteissa, joissa puhujalla ei ole syytä olettaa ulkopuolisen kuulevan hänen puhettaan eli tällaisen puheen kuuntelu tapahtuu salaa.

Vastaavasti salakatselu on määritetty rikoslain 24 luvun 6 §:ssä oikeudettomasti teknisellä laitteella katselemiseksi tai kuvaamiseksi, joka kohdistuu

- kotirauhan suojaamassa paikassa taikka käymälässä, pukeutumistilassa tai muussa vastaavassa paikassa oleskelevaan henkilöön, taikka
- yleisöltä suljetussa rakennuksessa, huoneistossa tai aidatulla piha-alueella oleskelevaa henkilöä tämän yksityisyyttä loukaten.

Kotirauhan suojaama alue määritellään rikoslain 24 luvun 11 §:ssä. Kotirauhan suojaamia paikkoja ovat asunnot, loma-asunnot ja muut asumiseen tarkoitetut tilat, kuten hotellihuoneet, teltat, asuntovaunut ja asuttavat alukset, sekä asuintalojen porraskäytävät ja asukkaiden yksityisaluetta olevat pihat niihin välittömästi liittyvine rakennuksineen. Myös salakuuntelun tai katselun valmistelu on rangaistavaa.

Henkilötietojen käsittelyä koskeva lainsäädäntö koskee mm. henkilötietojen keräämistä, tallettamista, käyttöä, yhdistämistä tai luovuttamista. Henkilöiden kuvaaminen ja heidän puheensa tallettaminen saattaa olla paitsi salakuuntelua ja salakatselua samalla myös henkilötietojen käsittelyä. Tällöin tietojen käsittelyssä on noudatettava henkilötietolakia, jonka rikkominen täyttää rikoslain 38 luvun 9 §:ssä tarkoitetun henkilörekisteririkoksen tunnusmerkistön. Salakuuntelulla tai -katselulla saadun aineiston hyväksikäyttö saattaa tulla rangaistavaksi myös muiden tunnus-merkistöjen perusteella, kuten yksityiselämää koskevan tiedon levittäminen (RL 24:8) tai kunnianloukkausrikoksen (RL 24:9) yhteydessä.

Rikoslain muuttamiseksi säädetyn lain (531/2000) perusteluissa todetaan, että ihmisen yksityiselämä tarvitsee suojaa tekniseltä tarkkailulta myös muualla kuin kotirauhan suojaamassa paikassa. Salakuuntelun rangaistavuuden edellytyksenä on, ettei puhe ole tarkoitettu ulkopuolisen tietoon tai ettei puhujalla ole syytä olettaa ulkopuolisen kuulevan hänen puhettaan. Silloin kun puhe on tarkoitettu nimenomaisesti keskustelua salaa tallentavan osapuolen tietoon, yksityisyyden suojan loukkausta ei voida pitää niin merkittävänä, että kotirauhankaan piirissä käytävän keskustelun tallentamista olisi syytä säätää salakuunteluna rangaistavaksi (HE 184/99). Tämä periaate soveltunee myös muualla kuin kotirauhan piirissä tapahtuvaan keskustelun tallentamiseen. Yleisellä paikalla kuvatuksi tuleminen ei ole salakatselua, sen sijaan yleisellä paikalla tapahtuva kuunteleminen voi olla salakuuntelua.

Lainsäädäntö kohtelee kameravalvontaa eri tavalla muun muassa sen mukaan, kuka valvontaa suorittaa, missä tarkoituksessa valvontaa suoritetaan, missä paikassa oleskelevaan henkilöön valvonta kohdistuu ja onko kysymyksessä pelkkä katselu vai myös kuvan tallettaminen. Jotta kameravalvonta olisi sallittua, sen tulee täyttää sekä salakatselusäännöksen että henkilötietolain asettamat edellytykset. Jos kuuntelu

liitetään valvontaan, on sen täytettävä myös salakuuntelusäännöksessä asetetut edellytykset. Siellä, missä kameravalvontaa ei salakatselusäännöksen perusteella voi harjoittaa, ei sitä voida henkilötietolain perusteella sallia. Tallettamisen jälkeistä tietojen käsittelyä sääntelee yksin henkilötietojen käsittelyä koskeva lainsäädäntö.

Henkilötietolailla ei salakuuntelusäännöksen tavoin ole alueellisia rajoja: se sääntelee missä tahansa tapahtuvaa henkilötietojen käsittelyä. Sen soveltaminen pelkkään kameran kautta tapahtuvaan katseluun ilman tietojen tallentamista on kuitenkin mahdollista.

Henkilötietolaki sääntelee henkilötietojen käsittelyä. Puheääni samoin kuin kuva on henkilötietolain mielessä henkilötieto, jos henkilö on siitä tunnistettavissa. Koska tunnistamismahdollisuudet ovat kasvaneet, myös henkilötietolain välitön soveltaminen kameravalvontaan on vastaavasti laajentunut. Kameravalvontaa voitaneenkin pitää henkilötietojen automaattisena käsittelynä.

Henkilötietolain tarkoituksena on paitsi toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietojen käsittelyssä myös edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista. Niinpä kameroiden asentaminen tulisi yleisilläkin paikoilla ja paikoilla, joihin yleisöllä on pääsy, tapahtua välttäen tarpeetonta yksityisyyden loukkaamista.

Henkilötietolain asettamat keskeiset edellytykset henkilötietojen käsittelylle kameravalvonnassa ovat seuraavat:

Missä tahansa paikassa tapahtuvan kameravalvonnan edellytyksenä on, että sen tulee olla rekisterinpitäjän toiminnan kannalta asiallisesti perusteltu. Mikä tahansa tarkoitus ja toteuttamistapa ei siis ilman muuta tee oikeutetuksi yleisellä paikallakaan tapahtuvaa kameravalvontaa. Lisäksi on noudatettava henkilötietolain mukaista huolellisuutta.

Henkilötietolaki edellyttää myös kameravalvonnasta näkyvää ilmoittamista, ellei valvontaa kohdenneta pelkästään ko. paikassa oikeudettomasti epäiltyihin. Tällaisesta ilmoituksesta olisi syytä näkyä myös se yksityisyyden suojan kannalta olennainen seikka, tallentaako kamera.

Henkilötietolainsäädäntö painottaa muutoinkin avoimuutta. Rekisterinpitäjällä on velvollisuus tarvittaessa ilmoittaa rekisteröitävälle häntä koskevien tietojen keräämisestä missä, miten ja mihin tarkoitukseen niitä kerätään. Rekisteriseloste, josta ilmenee kameravalvonnan perustiedot ja vastuuhenkilöt on oltava tarkkailtavien saatavilla. Tarvittaessa hänellä täytyy olla oikeus tarkastaa itseään koskevat tiedot.

Lisäksi henkilötietolaissa on useita muitakin säännöksiä, jotka täytyy ottaa huomioon kameravalvontaa toteutettaessa. Tällaisia ovat muun muassa tietojen suojaamisvelvollisuus ja hävittämisvelvollisuus sekä arkaluonteisten tietojen käsittelykielto.

7.6 Sähköisten palvelujen tuottaminen

Suomessa pantiin täytäntöön EU:n sähkökauppadirektiivi(2000/31/ETY) **lailla tietoyhteiskunnan palvelujen tarjoamisesta** (458/2002). Laki toistaa direktiivin periaatteet samanlaista systematiikkaa käyttäen kuin itse direktiivi. Erityiskysymyksenä säänneltiin mm. sopimuksen tekemistä sähköisesti niissä tapauksissa, joissa laki edellyttää sopimuksen tekoa kirjallisesti. Sähköinen sopimustoiminta on muissa tapauksissa katsottu mahdolliseksi sopimusvapauden myötä. Lain 12 § sisältää ne vaatimukset, joita kirjallisen sopimuksen tekeminen sähköisessä ympäristössä edellyttää.

Kuluttajansuojalakiin (38/1978) tehdyillä muutoksilla on saatettu voimaan EU:n etämyyntidirektiivin ja rahoituspalvelujen etämyyntidirektiivin säännökset. Kuluttajansuojalain 6. luvun 4 §:ään on kirjattu samat kirjallista muodon sähköistä toteuttamista koskevat vaatimukset, jotka ovat lain tietoyhteiskunnan palvelujen tarjoamisesta 12 §:ssä.

Tekijänoikeuslakiin (404/1961) tehdyillä muutoksilla on saatettu voimaan EU:n tietoyhteiskuntadirektiivi 2001/29/EY. Lainmuutoksen yhteydessä keskusteltiin suojausjärjestelmistä.

Viestintämarkkinalailla (393/2003) pantiin täytäntöön EU:n vuoden 2002 sähköistä viestintää koskeva lainsäädäntöpaketti lukuun ottamatta sähköisen viestinnän tietosuojalakia, jolla pantiin täytäntöön samaa asiaa käsittelevä direktiivi.

Verkkotunnuslaki (228/2003) sääntelee suomalaisten ”.fi”- tai ”.ax”-loppuisten verkkotunnusten myöntämistä. Lain tarkoituksena on edistää tietoyhteiskunnan palvelujen tarjoamista tietoverkossa parantamalla suomalaisten verkkotunnusten saatavuutta ja turvaamalla verkkotunnusten tasapuolinen saatavuus. Verkkotunnuksen myöntää Viestintävirasto.

Laki sähköisestä asioinnista viranomaistoiminnassa (2003/13) sisältää yksityiskohtaiset määräykset sähköisen asioinnin järjestämisestä viranomaisen kanssa, ja se käsittelee myös lainkäyttöä ja ulosottoa. Yksityiskohtana laista voidaan todeta, että asiakirjaa ei tarvitse täydentää sähköisellä tai perinteisellä allekirjoituksella, jos asiakirjassa on tiedot lähettäjästä eikä asiakirjan alkuperäisyyttä tai eheyttä ole muuten

syytä epäillä, jolloin ei tarvita valtakirjaa. Myös **hallintolaki** (434/2003) on luonnollisesti otettava huomioon sähköisessä viranomaisasioinnissa. Erityiskysymyksinä sähköisen asioinnin osalta voidaan tarkastella kiinteistökauppaa ja lainhuutoa sekä asunto-osakkeiden siirron sähköistä rekisteröintiä. Näitä koskevaa lainsäädäntöä on säädetty viime aikoina.

Muita keskeisiä lakeja ovat **laki viestintähallinnosta** 625/2001 sekä **verkkotunnus-laki** 228/2003 (muutettu 241/2005).

Sähköisten palvelujen yhteydessä voidaan esittää myös palvelujen kehittämisen kannalta merkityksellinen kysymys suojauksen purkamisen kieltämisestä. **Sähköisen viestinnän tietosuojalain** mukaan salauksen käyttö yksityisyyden suojan turvaamiseksi on mahdollista. Tilaaja ja käyttäjä voi suojata viestinsä ja tunnistamis-tietonsa haluamallaan tavalla käyttäen hyväksi sitä varten tarjolla olevia teknisiä mahdollisuuksia, jollei laissa toisin säädetä. Suojauksen toteuttamisella ei saa häiritä verkkopalvelun ja viestintäpalvelun toteuttamista tai käyttämistä.

Sähköisen viestinnän teknisen suojauksen purkavan järjestelmän tai sen osan hallussapito, maahantuonti, valmistaminen ja levittäminen on kielletty, jos järjestelmän tai sen osan ensisijaisena käyttötarkoituksena on teknisen suojauksen oikeudeton purku. Viestintävirasto voi antaa hyväksyttävästä syystä luvan poiketa tästä tarkoitetusta kiellosta.

Laki eräiden suojauksen purkujärjestelmien kieltämisestä (1117/2001) saattoi EU:n ehdollisen pääsyn direktiivin osaksi Suomen lainsäädäntöä. Laki koskee maksullisten televisio- ja radiolähetysten sekä vastaanottajan henkilökohtaisesta pyynnöstä toteutettavien etäpalvelujen teknisen suojauksen oikeudetonta purkamista. Suojauksenpurkulaissa purkujärjestelmällä tarkoitetaan laitetta, tietokoneohjelmaa tai muuta järjestelmää taikka järjestelmän olennaista osaa, jonka tarkoitus on poistaa televerkon avulla tarjottavan palvelun erityisellä teknisellä järjestelmällä toteutettu suojaus. Suomen laki ylittää direktiivin vaatimukset siltä osin, että kielto koskee myös muita kuin kaupallisessa tarkoituksessa tehtyjä oikeudettomia toimia. Suojauksen purkujärjestelmärikoksesta säädetään rikoslain 38 luvun 8a §:ssä.

Tekijänoikeuslaki (404/1961, muutettu) sisältää myös suojauksen purkua koskevia säännöksiä.

7.7 Sähköiset allekirjoitukset ja tunnistaminen

EU:n sähköisiä allekirjoituksia koskeva direktiivi implementoitiin Suomessa **lailla sähköisistä allekirjoituksista** (14/2003). Laki sisältää sen keskeisen säännön, että laatuvarmenteella varmennettu kehittynyt sähköinen allekirjoitus, joka on luotu turvallisella allekirjoituksen luomisvälineellä, muodostaa lain 18 §:n mukaisesti ainakin vastineen käsintehdylle allekirjoitukselle. Sen seikan, että kriteerit täyttävät menetelmät asetetaan oikeudellisesti samanarvoiseen asemaan kuin käsintehty allekirjoitus, ei tule vähentää muiden menetelmien oikeudellista asemaa.[58] Muilta sähköisiltä allekirjoituksilta kuin tässä lainkohdassa mainituilta ei voida kiistää allekirjoituksen asemaa ainoastaan sillä perusteella, että allekirjoitus ei ole lainkohdassa mainittujen kriteerien mukainen. Tätä direktiivin 1999/93/EY artiklan 5 (2) mainittua sääntöä ei ole otettu Suomen lakiin sen vuoksi, ettei sen toteaminen ole välttämätöntä sopimusvapauden ja vapaan tuomioistuinten todistusteorian vallitessa.

Väestörekisterikeskus toimii sähköisistä allekirjoituksista annetun lain mukaisena laatuvarmentajana. Väestörekisterikeskuksen toimintaa tässä suhteessa sääntelevät useat lait.[59]

Sähköisen tunnistamisen ja allekirjoitusten osalta on laajassa käytössä pankkien TUPAS-standardi, joka perustuu muuttuvien salasanojen käyttöön.[60]

Biometriikan käyttöön myös yksityisoikeudellisissa transaktioissa on pohdittavana EU:n biometrisiä passeja koskevan direktiivin implementoimisen lisäksi.[61]

---

[58] Myös lain 18 §:ssä tarkoitettu allekirjoitus voidaan kiistää. Tällainen kiistäminen voi perustua normaalisti lähinnä muihin kuin teknisiin ominaisuuksiin, kuten allekirjoittamaan pakottamiseen tai organisaation sisäiseen toimivallan puuttumiseen. Oikeudellista estettä ei sinänsä ole myöskään esimerkiksi allekirjoituksen luomisvälineen turvallisuuden osalta, mutta on vaikeampaa, jos standardien vaatimukset on täytetty. Laissa tarkoitettua laatuvarmentajaa voi kohdata kiistämistilanteessa vahingonkorvausseuraamus, ellei tämä näytä toimineensa huolellisesti.

[59] Henkilörekisterilaki (471/1987), väestötietolaki (507/1993, muutos 299/2003), jossa säädettiin uusi 20 § varmenteiden tiedoista ja 23 § hakumenettelystä, henkilökorttilakiin (829/1999) tehtiin muutos 300/2003, jolla sisällytettiin säännökset sähköisestä henkilökortista.

[60] TUPAS, Pankkien tunnistuspalvelu asiointipalveluntuottajille, Palvelun kuvaus ja palveluntuottajan ohje, Versio 2.0, 13.6.2002, Suomen Pankkiyhdistys.

[61] Ks. myös liikenneministeriön teettämä selvitys Sähköisen tunnistamisen menetelmät ja niiden sääntelyn tarve, LVM 44/2003.

7.8 Tietoturva ja sähköiset palvelut aineellisessa lainsäädännössä

7.8.1 Pankkitoiminta ja rahanpesu

Pankkitoiminta edellyttää näin ollen asiakkaan luottamusta siihen, että hänen taloudelliset ja yksityiset asiansa pidetään salassa. Asiakkaan kannalta pankkisalaisuus on osa perustuslailla kaikille taattua yksityisyyden suojaa. Pankkisalaisuus ei kuitenkaan rajoitu suojaamaan vain yksityisiä ihmisiä vaan se ulottuu myös yhteisöihin. Aluksi pankkisalaisuusperiaatetta noudatettiin vain moraalisten sääntöjen tukemana tavanomaisena oikeutena. Laintasolla pankkisalaisuudesta säädettiin Suomessa ensimmäisen kerran vuonna 1970 voimaan tulleissa pankkilaeissa.

Pankkitoiminnan kehittyessä pankkisalaisuuden merkitys on kasvanut ja siitä on tullut yksi rahoitusalan häiriötöntä toimintaa turvaava tekijä. Pankkisalaisuuden noudattaminen on siten myös yleisen edun mukaista. Toisinaan yleinen ja yksityinen etu saattavat kuitenkin joutua ristiriitaan ja eräissä tapauksissa onkin katsottu, että pankkisalaisuuden on väistyttävä yleisen edun tieltä. Nämä poikkeustapaukset on määritelty lailla. Poikkeussäännöksinä niiden tulkinnan on oltava suppeaa.

Luottolaitoksen yksityis- ja yritysasiakkaan pankkitiedot ovat lähtökohtaisesti pankkisalaisuuden piiriin kuuluvia tietoja, joita ei ilman asiakkaan suostumusta saa luovuttaa kenellekään. **Luottolaitostoiminnasta annetun lain** (1607/1993) 94 §:ssä määritellään pankkisalaisuuden tarkka sisältö. Pankkitietojen lisäksi salassa pidettäviä ovat kaikki asiakkaan taloudellista tilannetta, henkilökohtaisia oloja ja liike- tai ammattisalaisuutta koskevat tiedot. Luottolaitosten lisäksi vastaavia määräyksiä on sijoitusrahastolaissa (48/1999) sekä laissa rahoitus- ja vakuutusryhmittymien valvonnasta (44/2002).

Suomen Pankkiyhdistyksen antamien pankkisalaisuusohjeiden mukaan salattavia ovat kaikki sellaiset tiedot, joiden perusteella asiakas voidaan yksilöidä. Pankkisalaisuus ei siten koske mm. asiakasryhmästä annettavia tietoja, ellei niitä voida liittää tiettyyn pankin asiakkaaseen. Yksittäistä asiakasta koskevia salassa pidettäviä tietoja ovat mm. luottoa haettaessa saadut tiedot kannattavuuslaskelmista ja liikesopimuksista sekä toimintajärjestelmistä ja tuotteista. Salassapitovelvollisuus ulottuu sekä pysyvään että tilapäiseen asiakassuhteeseen eikä se rajoitu vain pankin ja asiakkaan välisiin pankkiasioihin, vaan käsittää myös tämän suhteen ulkopuolelle jäävät tiedot, jos ne on saatu pankkiasioiden yhteydessä. Samoin salassapitovelvollisuus ulottuu tietoihin, jotka on saatu toiselta pankilta. Lähtökohtaisesti salassa pidettäviä ovat kaikki sellaiset tiedot, joiden osalta pankin asiakkaalla voidaan katsoa olevan salassapitotahto.

Pankkisalaisuus ei koske vain asiakassuhteen aikana, vaan myös ennen asiakassuhdetta ja sen jälkeen asiakkaasta saatuja tietoja.

Poikkeuksen salassapitovelvollisuuteen tekevät tiedot, jotka 94 §:n 2. momentin mukaan on annettava viranomaiselle. Syyttäjä- ja esitutkintaviranomaisten tietojensaantioikeudesta on luottolaitoslakiin otettu erityismaininta. Pykälässä viitataan eri viranomaisia koskeviin muiden lakien säännöksiin, joiden nojalla ko. viranomaisella on tietojensaantioikeus.

Jotta pankkisalaisuus voisi toteutua, on pankkien noudatettava toiminnassaan tietoturvaperiaatteita. Rahoitustarkastuksen standardi 4.4b ’Operatiivisten riskien hallinta’ sisältää tätä koskevat pääperiaatteet. Tuossa standardissa todetaan, yleisten määritelmäosien jälkeen, että tietojärjestelmiin pääsyä on valvottava. Myös tietojärjestelmissä käsiteltävien tapahtumien kiistämättömyys sekä keskenään kommunikoivien osapuolten tunnistaminen ja todentaminen on hoidettava asianmukaisesti. Lisäksi tietojärjestelmissä käsiteltävät tapahtumat pitää voida aukottomasti jäljittää.

Valvottavan (eli pankin) yleisen tietoturvallisuuden tason ja eri tietojärjestelmien turvatason on oltava riittävät valvottavan toiminnan luonteeseen ja laajuuteen, tietojärjestelmien uhkien vakavuuteen sekä yleiseen tekniseen kehitystasoon nähden. Valvottavan ylin johto vastaa siitä, että valvottavalla on riittävä tietoturvallisuus.

Valvottavan tietoturvallisuuden yleisen tason on oltava sen ylimmän johdon määrittämä ja hyväksymä. Valvottavan ylimmän johdon on annettava riittävät resurssit sekä määriteltävä vastuut riittävän tietoturvallisuuden tason ylläpitämiseksi. Valvottavan on arvioitava tietoturvallisuutensa taso säännöllisesti. Mikäli valvottavan omassa organisaatiossa ei ole riittävää tietoturvallisuuden asiantuntemusta, arvio on teetettävä ulkopuolisella asiantuntijataholla. Havaittujen puutteiden korjaamiseksi on ryhdyttävä tarvittaviin toimenpiteisiin.

Valvottavan tietoturvallisuuden tason arvioinnin on perustuttava tietoturvallisuuteen liittyvien riskien säännönmukaiseen arviointiin. Riskiarvioita tehtäessä on määriteltävä, mitkä ovat valvottavan keskeiset toiminnot ja resurssit, mitkä ovat niiden uhat, kuinka haavoittuvia valvottavan toiminnot ja resurssit ovat näille uhkille sekä miten uhkat toteutuessaan vaikuttavat valvottavan toimintaan. Havaittujen riskien hallitsemiseksi on rakennettava riittävät kontrollit. Käyttöönotettavien uusien tekniikoiden ja palvelujen riskit on myös arvioitava. Tietoturvallisuusriskien arviointi on liitettävä osaksi valvottavan riskienhallintaa, jotta voidaan taata, että ylin ja toimiva johto saavat käsityksen liiketoiminnassa otettujen kaikkien merkittävien riskien yhteisvaikutuksesta.

Rahanpesun osalta on Suomessa voimassa **laki rahanpesun estämisestä ja selvittämisestä** (68/1998), jota on muutettu useaan kertaan. Lakia täydentää **sisäasiainministeriön asetus rahanpesun estämisestä ja selvittämisestä** (890/2003). Asetuksessa on määräykset henkilön tunnistamisesta. Luonnollinen henkilö on tunnistettava viranomaisen antamasta asiakirjasta tai erityisestä syystä muusta asiakirjasta, josta henkilöllisyys voidaan luotettavasti todentaa. Henkilöstä on selvitettävä täydellinen nimi ja syntymäaika sekä henkilön suomalainen henkilötunnus, jos henkilöllä tämä on ja ulkomaisen henkilön kansallisuus sekä ulkomaisen henkilön passin tai muun matkustusasiakirjan numero tai muu tunnistetieto.

Jos luonnollinen henkilö taikka hänen asiamiehensä ei ole läsnä henkilöllisyyttä todennettaessa, henkilön on tunnistauduttava sähköisesti laatuvarmennetta tai muuta tietoturvallista ja todisteellista tunnistautumistekniikkaa käyttäen. Erityisestä syystä lain mukainen ilmoitusvelvollinen voi etätunnistaa henkilön hankkimalla tämän henkilöllisyyden todentamiseksi tarvittavan selvityksen käyttämällä lähteitä, joista selvitys voidaan luotettavasti saada.

Asetuksessa on myös määräykset oikeushenkilön tunnistamisesta. Tunnistamisesta syntyneet tiedot on säilytettävä luotettavasti ja muodossa, joka mahdollistaa niiden saattamisen tarvittaessa viranomaisen käytettäviksi.

Rahanpesun torjuntaa varten on Keskusrikospoliisin Rahanpesun selvittelykeskus laatinut säännöt ’Rahanpesun torjunnan parhaat käytänteet’. Rahoitustarkastus on lisäksi laatinut standardin ’Asiakkaan tunnistaminen ja tunteminen rahanpesun, terrorismin rahoituksen sekä markkinoiden väärinkäytösten estäminen nro 2.4’.

Kuten johdantojaksosta ilmenee, rahanpesua koskeva kolmas direktiivi on implementointivaiheessa, jolloin myös kansalliset säännöt EU-maissa tulevat osin muuttumaan.

7.8.2 Hankintalainsäädäntö ja verkkolaskutus

Suomessa ollaan panemassa täytäntöön EU:n uusia hankintadirektiivejä, joista toinen on yleinen ja toinen koskee erityissektoreita, vesi- ja energiahuoltoa, liikennettä ja postipalveluja. Hallituksen esitys 50/2006 on annettu eduskunnalle keväällä 2006. Direktiiveillä mahdollistettiin sähköinen hankintatoimi, minkä lisäksi on mahdollista ottaa kansallisesti käyttöön erityismenettelyt sähköinen huutokauppa ja dynaaminen hankintajärjestelmä. Erityismenettelyiden osalta on viitattu mahdollisuuteen säätää niistä myöhemmin asetuksella.

Yleistä hankintalakia koskevan ehdotuksen 50 §:n mukaan hankintamenettelyyn liittyvät ilmoitukset ja tietojenvaihto on toimitettava hankintayksikön valinnan mukaan joko kirjeitse, telekopiolla tai sähköisiä välineitä käyttäen. Valittujen viestintävälineiden on oltava yleisesti käytettävissä, eivätkä ne saa rajoittaa toimittajien mahdollisuutta osallistua hankintamenettelyyn. Valtioneuvoston asetuksella annetaan tarkemmat säännökset hankintadirektiivin ja sen liitteessä X tarkoitetuista viestintään sovellettavista menettelytavoista sekä sähköiseen viestintään sovellettavista teknisistä ja muista edellytyksistä. Nämä määräykset mahdollistavat tietoturvan vaatimusten huomioimisen. On huomattava, ettei Suomen laissa aseteta sähköisiin allekirjoituksiin liittyviä erityisvaatimuksia tarjousten tekemiselle. Ehdotuksessa on myös salassapitoa koskeva säännös, jossa viitataan mm. lakiin viranomaisen toiminnan julkisuudesta.

Verkkolaskutus on ollut mahdollista Suomessa jo vuosia. Sähköistä laskutusta säännellään **arvonlisäverolaissa** (1993/1501, muutettu) ja **kirjanpitolaissa** (1997/336, muutettu). Suomessa oli perinteisesti katsottu arvonlisäverolain laskuja koskevien säännösten koskevan yhtä hyvin paperilla kuin sähköisestikin toimitettuja laskuja. Kirjanpitolain mukaan tositteet ja kirjanpitomerkinnät on saatu tehdä koneelliselle tietovälineelle kirjanpitovelvollisen tarvittaessa selväkieliseen kirjalliseen muotoon saatettavalla tavalla. Sittemmin on arvonlisäverolaissa todettu nimenomaisesti, että lasku voidaan toimittaa vastaanottajan suostumuksin sähköisesti. Säännös koskee niitä laskuja, jotka myyjä lakiehdotuksen mukaan on velvollinen antamaan.

Sähköiselle laskutukselle ei aseteta arvonlisäverolaissa muita erityisiä edellytyksiä. Suomi käyttää siis hyväksi 6. arvonlisäverodirektiivin (2001/115/EY) 22. artiklan 3. kohdan c-alakohdan 3. alakohdassa jäsenvaltioille annetun mahdollisuuden hyväksyä myös muulla tavoin kuin kyseisessä kohdassa määritellyin tavoin toimitetut sähköiset laskut. Muilta osinhan direktiivi asettaa vaatimukseksi sähköisten allekirjoitusten tai sähköisen tiedonsiirron eli EDI:n käytön. Suomessa ei ole katsottu verovalvonnan kannalta tai muistakaan syistä tarpeelliseksi lainsäädännössä asettaa sähköiselle laskutukselle erityisiä edellytyksiä.

7.9 Tietoturvallisuuteen liittyvät yleiset palvelut

Viestintäviraston tehtävänä on toimia kansallisena tietoturvaviranomaisena, joka harjoittaa CERT-toimintaa. CERT-FI on Viestintävirastossa toimiva kansallinen CERT-ryhmä, jonka tehtävänä on tietoturvaloukkausten ennaltaehkäisy, havainnointi, ratkaisu sekä tietoturvauhkista tiedottaminen. On yleisesti katsottu, että yrityksillä on oikeus, nimenomaisen lakivaltuutuksen puuttuessakin, informoida Viestintäviraston CERT-FI-ryhmää tietoturvauhkista ja -loukkauksista.

Suomessa ei ole kansallista viranomaista tai elintä, joka antaisi sertifikaatteja tietoturva-asioissa. Laki ei edellytä viranomaisilta sertifiointeja. Kansainväliset tietoturvastandardit ovat käytössä Suomessakin. Suomessa ei ole kehitetty kansallista, informaatioteknologiaa koskevaa tilintarkastusstandardia.

8. Ruotsi

8.1 Perustuslainsäännökset

Ruotsin perustuslaki koostuu neljästä säädöksestä, hallitusmuodosta[62], perimysjärjestyksestä, painovapausasetuksesta[63] ja ilmaisunvapausperustuslaista[64]. Nämä lait toimivat Ruotsissa poliittisen päätöksenteon pohjana ja sisältävät useita tietosuojan sekä kansalaisvapauksien ja ihmisoikeuksien kannalta merkityksellisiä määräyksiä. Lisäksi Euroopan ihmisoikeussopimus on saatettu vuonna 1994 osaksi Ruotsin lakia. Vaikka sillä ei olekaan muodollisesti perustuslain asemaa, on sillä se kuitenkin käytännössä.

Hallitusmuodon 2 § sisältää määräyksen yksityisyyden suojasta. Hallitusmuodon 2. luvun 13 § määrää, että ilmaisun- ja tiedon liikkumisen vapautta, joita painovapausasetus perustuslaillisesti suojaa, voidaan rajoittaa yksityiselämän koskemattomuuden suojaamiseksi. Hallitusmuodon 2. luvun 3 § turvaa lisäksi yksityiselämän koskemattomuuden automaattisen tietojenkäsittelyn yhteydessä.[65] Tuossa lainkohdassa todetaan, että kansalaisten henkilökohtainen koskemattomuus nauttii lailla täsmennettyä suojaa häntä koskevien tietojen rekisteröimistä automaattisen tietojenkäsittelyn välityksellä. Näin Ruotsissa on tietosuoja osin nostettu perustuslain tasolle.

Ruotsi on Euroopan Unionin ja Euroopan neuvoston jäsen ja maa on saattanut useita tietosuojaan ja tietoturvaan liittyviä kansainvälisiä sopimuksia kansallisen lainsäädäntönsä osaksi.

8.2 Tietoturvan sääntely ja kehittäminen ja yleinen turvallisuus

Ruotsissa ei ole yhtenäistä tietoturvallisuutta koskevaa lainsäädäntöä vaan alan normit ovat hajallaan eri puolilla lainsäädäntöä. Kattavia selvityksiä normistoista on kuitenkin tehty valtiovallan toimesta.

---

[62] Regeringsform SFS 1974:152.

[63] Tryckfrihetsförordning SFS 1949:105.

[64] Yttrandefrihetsgrundlag SFS 991:1469.

[65] Lain muutos 1988:1489.

Ruotsissa tehtiin vuosituhanteen vaihteessa vuonna 2000 tietoyhteiskuntapoliittinen päätös, jonka mukaan Ruotsista tulee tehdä tietotekniikan käytössä maailman johtavia maita. Jotta tämä onnistuisi, olisi luottamusta tietojärjestelmien käyttöön lisättävä. Tämän katsottiin merkitsevän myös tietoturvan kehittämistä.

Tietoturvasäännösten kehittäminen on painottunut valtakunnan turvallisuuteen. Ruotsin puolustusministeriö tilasi selvityksen, jonka osaraportti signaalisuojasta yhteiskunnan kannalta elintärkeissä laitoksissa valmistui vuonna 2003. Signaalisuojalla tarkoitetaan toimenpiteitä, joilla estetään sähköisen kommunikaation sisällön paljastuminen tai sen muuttaminen eli salausjärjestelmiä. Toimeksiantoa, joka sai nimen **InfoSäutredningen**, laajennettiin koskemaan ehdotusta siitä, kuinka Ruotsin kansallista tietoturvastrategiaa tulee kehittää ja kuinka Ruotsin tulee toimia kansainvälisessä tietoturvaa koskevassa yhteistyössä. Tämän työn tuloksena Ruotsissa valmistui vuonna 2004 kattava selvitys tietoturvasäännöksistä nimeltään **Informationssäkerhet i Sverige och Internationellt – en översikt**.[66] Selvityksessä korostettiin OECD:n tietoturvallisuutta koskevia suuntaviivoja ja niissä korostetun turvallisuuskulttuurin aikaansaamista Ruotsiin kansallisella tasolla. Toukokuussa 2005 julkaistiin kolmas osaraportti nimeltään **Säker information – Förslag till informationssäkerhetspolitik**.[67] Raportissa katsotaan kattavan tietoturvallisuuslainsäädännön olevan Ruotsissa tarpeen.

Ruotsin valtakunnan turvallisuutta silmällä pitäen on olemassa useita tietoturvaan liittyviä säädöksiä, joita ovat laki yhteiskunnalle tärkeiden laitosten suojasta[68], yleisen turvallisuuden suojaksi säädetty laki ja siihen liittyvä asetus[69] sekä valtakunnanpoliisin määräykset[70]. Yleisiä turvallisuus kysymyksiä on kartoitettu selvityksessä **Sårbarhets och säkerhetsutredning**[71]. Viranomaiset ovat myös määrittäneet tietoturvan perustasoa valtakunnan kannalta merkittävien toimintojen osalta.

Ruotsi on muiden EU-maiden tavoin pannut täytäntöön terrorismin ja tietoverkkorikollisuuden torjuntaan liittyviä EU- ja muita kansainvälisiä sopimuksia.

---

[66] SOU 2004:32.

[67] SOU 2005:42.

[68] Lagen om skydd för samhällsviktiga anläggningar 1990:217.

[69] Säkerhetsskyddslagen 1996:627 ja säkerhetskyddsförordning 1996:633.

[70] Rikspolisstyrelsens föreskrifter om säkerhetsskydd RPS FS 1996:9.

[71] SOU 2001:41.

8.3 Erityispiirteitä viranomaistoiminnasta

Ruotsin lainsäädäntö sisältää määräyksiä telekuuntelusta (*hemlig teleavlyssning*) ja televalvonnasta (*hemlig teleövervakning*) Ruotsin oikeudenkäymiskaaren (*rättegångs-balken*) luvussa 27 sekä laissa[72] pakkokeinojen käytöstä eräiden rikosten yhteydessä samoin kuin parissa erityislaissa. Näiden pakkokeinojen keskeisenä erona on, ettei televalvonnassa voida saada tietoa viestinnän sisällöstä. Telekuuntelun ja -valvonnan suorittamiselle asetettuja vaatimuksia on viime vuosina hieman lievennetty ja ne ovat jonkin verran Suomea lievemmät. Telekuuntelua voidaan suorittaa jopa yksityisessä yritysverkossa.

Ruotsin hallitus toimittaa vuosittain valtiopäiville kertomuksen telekuuntelun, televalvonnan ja kameravalvonnan käytöstä esitutkinnassa.

8.4 Tiedon julkisuus ja salassapito

8.4.1 Viranomaistiedon julkisuus

Ruotsissa on koottu julkisen lainsäädännön salassapitovaatimukset yhdeksi salaisuus-laiksi[73]. Tässä laissa säädetään julkisen viranomaisen vaitiolovelvollisuudesta ja kiellosta luovuttaa julkisia asiakirjoja. Tässä suhteessa lain määräykset sisältävät poikkeuksia perustuslainsäännöksissä (*tryckfrihetsförordning*) taatussa oikeudessa saada tieto julkisista asiakirjoista.

Laissa on kielto paljastaa salassa pidettävää tietoa suullisesti tai kirjallisesti. Laissa on myös kielto luovuttaa tietoa toiselle viranomaiselle muissa kuin laissa säädetyissä tapauksissa. Jos laissa on kielto paljastaa tietoa, ei tietoa myöskään voi käyttää sen toiminnan ulkopuolella, jota varten salaisuus on säädetty.

Tietojen arkistoinnista säädetään arkistolaissa[74]. Sen 6 § sisältää myös vaatimuksen arkiston suojaamisesta tuhoamiselta tai asiattomalta pääsyltä.

---

[72] Laki 1952:98.

[73] Sekretesslag 1980:100.

[74] Arkivlag 1990:782.

8.4.2 Yrityssalaisuuksien suoja

Ruotsissa on säädetty erityinen laki[75] yrityssalaisuuksien suojasta. Lain 1§:n mukaan tarkoitetaan yrityssalaisuudella sellaista tietoa elinkeinonharjoittajan liike- tai muussa toiminnassa, jotka tämä pitää salaisena, ja jonka paljastuminen on omiaan aiheuttamaan hänen liiketoiminnalleen vahinkoa heikentämällä kilpailunedellytyksiä. Tiedolla tarkoitetaan sekä eri tavoin dokumentoitua tietoa, mukaan lukien piirrokset, mallit ja vastaavat tekniset kuvaukset, että yksittäisten henkilöiden hallussaan pitämää tietoa jostain seikasta, vaikka sitä ei olisikaan dokumentoitu.

Laki koskee ainoastaan luvattomia yrityssalaisuuksien loukkauksia. Luvattomalla loukkauksella ei tarkoiteta sellaista tilannetta, jossa joku hankkii, hyväksikäyttää tai paljastaa elinkeinonharjoittajan yrityssalaisuuden julkistaakseen viranomaiselle tai muulle toimivaltaiselle elimelle sellaista, minkä voidaan ajatella käsittävän rikoksen, josta voi seurata vankeusrangaistus, tai jonka voi katsoa muodostavan muun vakavan väärinkäytöksen elinkeinonharjoittajan toiminnassa. Luvattomana puuttumisena ei voida myöskään pitää sitä, että joku hyväksikäyttää tai paljastaa yrityssalaisuuden, jonka hän tai joku ennen häntä on saanut tietoonsa laillisesti.

Laki tarjoaa yrityssalaisuuden loukkaamisesta sekä rangaistus- että vahingonkorvaus-seuraamuksen. Sen, joka syyllistyy 3 tai 4 §:ssä tarkoitettuun rikokseen, on korvattava rikoksen tai yritysalaisuuden hyväksikäytön ja paljastumisen aiheuttama vahinko(5 §). Joka tahallaan tai huolimattomuudella käyttää hyväksi tai paljastaa elinkeinon-harjoittajan yrityssalaisuuden, jonka hän on saanut tietoonsa liikesuhteessa tähän, on korvattava tästä aiheutunut vahinko (6 §).

Työntekijän, joka tahallaan tai huolimattomuudella käyttää hyväkseen tai paljastaa työnantajan yrityssalaisuuden, jonka on saanut tietoonsa työsuhteessa olosuhteissa, joissa hän käsitti tai hänen olisi pitänyt käsittää, ettei tietoa saa paljastaa, on korvattava toiminnastaan aiheutunut vahinko (7 §). Jos teko on tapahtunut työsuhteen päätyttyä, sovelletaan tätä lainkohtaa vain jos on erityisiä syitä. Tällaiset tilanteet korostavat salassapitosopimusten merkitystä.

Laki säätää korvausseuraamuksen myös muiden osalta. Se, joka tahallaan tai huolimattomuudella käyttää hyväkseen tai paljastaa yrityssalaisuuden, jonka tämä on käsittänyt tai hänen olisi pitänyt käsittää saaduksi haltuun laissa tarkoitetulla tavalla, on korvattava se vahinko, joka syntyy hänen menettelystään (8 §).

---

[75] Lag om skydd för företagshemligheter 1990:40.

Vastaavasti jos joku muussa tapauksessa tahallaan tai huolimattomasti käyttää hyväkseen tai paljastaa yrityssalaisuuden, jonka hän on käsittänyt tai jonka hänen olisi pitänyt käsittää paljastetun vastoin salaisuuslakia (1980:100) on tuomittava korvausvelvolliseksi.

8.5 Tietosuojasäännökset

8.5.1 Yleiset tietosuojasäännökset

Ruotsin keskeinen tietosuojalaki on henkilötietolaki[76], jolla on pantu täytäntöön EU:n henkilötietodirektiivi 95/46/EY. Laki sääntelee automatisoitujen henkilörekisterien käyttöä sekä julkisella että yksityisellä sektorilla. Laki korvasi vuoden 1973 tietosuojalain, joka oli tiettävästi ensimmäinen kattava tietosuojalaki koko maailmassa. Vanhan lain voimassaolo jatkuu siirtymäajan muodossa manuaalisten rekisterien osalta kuitenkin aina vuoteen 2007 asti.

Ruotsin tietosuojaviranomaisena toimii henkilötietolain osalta **Datainspektionen**, jonka tehtävänä on valvoa, että henkilötietojen käsittely ei johda asiattomaan puuttumiseen henkilön yksityiselämään ja että tietojenkäsittelyä koskevaa sääntelyä noudatetaan. Erityiseksi tavoitteeksi on kuitenkin asetettu, ettei tekniikan käyttöä tarpeettomasti ehkäistä.

Erityislakeja, joissa on henkilötietojen käsittelyä koskevia määräyksiä, on olemassa mm. liittyen terveydenhuoltoon[77], poliisitoimeen[78], kiinteistöverotukseen[79], Schengen-sopimuksen informaatiojärjestelmään[80], luottotietoihin[81], velan perintään[82] sekä hallintomenettelyyn[83].

---

[76] Personuppgiftslagen (yleinen lyhenne PuL) 1998:204.

[77] Lag 1998:544 om vårdregister.

[78] Polisdatalag 1998:622.

[79] Lag 2000:244 om ändring i fastighetstaxeringslagen 1979:1152.

[80] Lag 2000:344 om Schengens informationssystem.

[81] Kreditupplysningslag 1973:1173.

[82] Inkassolag 1974:182.

[83] Förvaltningslag 1986:223.

EU-direktiivin tavoin Ruotsin henkilötietolaki sisältää turvallisuusmääräyksiä henkilötietojen käsittelylle. Datainspektionen on ohjeistanut turvallisuuskysymyksiä henkilötietojen käsittelyssä joulukuussa 1999 ohjeellaan[84].

Ruotsissa ei ole lakia yksityisyyden suojasta työelämässä, vaan näitä kysymyksiä säännellään tietosuojalaissa ja erityisesti sen 4 §:ssä. Asia on kuitenkin ollut lainvalmistelun kohteena, mutta erityislainsäädäntöä ei ainakaan toistaiseksi ole säädetty.[85] Ruotsin tietosuojaviranomainen on kuitenkin äskettäin laatinut raportin asiasta.[86] Raportissa mainittujen kannanottojen mukaan työnantaja on vastuussa henkilötietojen käsittelystä työpaikalla. Työntekijöiden henkilötietoja voi käsitellä vain laissa sallimissa tilanteissa. Henkilötietojen käsittelyn tarkoitus on määriteltävä eikä käsittelyä saa suorittaa muuhun tarkoitukseen. Henkilöiden, joiden henkilötietoja käsitellään, on saatava tietää tarkoitus.

Lain sallimia tilanteita ovat 1) tilanteet, joissa työntekijä on antanut suostumuksensa käsittelyyn, 2) tilanteet, joissa työnantaja ja työntekijä ovat tehneet sopimuksen, jonka täyttämiseksi henkilötietoja käsitellään, 3) tilanteet, joissa henkilötietoja käsitellään oikeudellisen velvoitteen täyttämiseksi, 4) työntekijän tärkeän edun suojaaminen, 5) tietoja käytetään työtehtävän suorittamiseen viranomaisessa, 6) muissa tapauksissa, joissa työnantajan tai muun henkilön, jolle henkilötiedot luovutetaan, intressi on suurempi kuin työntekijän yksityisyyden suoja.

Lailla[87] sähköisestä viestinnästä on pantu täytäntöön sähköisen viestinnän tietosuojadirektiivi 2002/58/EY Ruotsissa. Tämä laki eli EkomL sääntelee kuitenkin myös viestintämarkkinakysymyksiä, sillä tällä lailla on pantu täytäntöön koko EU:n viiden tietoliikennettä koskevan direktiivin lainsäädäntöpaketti (ks. johdantojakso). EkomL:n 2 §:n mukaan henkilötietolain määräykset soveltuvat myös tietoverkkojen ja sähköisten viestintäpalvelujen käyttöön, ellei EkomL:sta muuta ilmene.

Valvonnan osalta EkomL:n valvontaviranomainen on posti- ja televiranomainen eli **Post- och telestyrelsen**, kun taas PuL:n valvonta kuuluu Datainspektionille. Toisaalta kun EkomL sisältää vain joukon erityismääräyksiä, on näillä viranomaisilla silti päällekkäistä toimivaltaa sähköisen viestinnän osalta.

---

[84] Säkerhet för Personuppgifter – Datainspektionens allmänna råd.

[85] Ks. tätä koskevaa lainvalmistelua: http://naring.regeringen.se/propositioner_mm/sou/pdf/sou2002_18a.pdf.

[86] Övervakning i Arbetslivet, Kontroll av de anställdas Internet- och e-postandvändning m.m., Datainspektionens rapport 2005:3.

[87] Lag (2000:389) om elektronisk kommunikation (lyhennne EkomL).

Ekom L:n 3 ja 4 §:n mukaan sen, joka ylläpitää yleistä sähköistä viestintäpalvelua, on ryhdyttävä varmistaakseen, että käsitellyt tiedot suojataan. Yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajan on toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet varmistaakseen tarjoamiensa palvelujen turvallisuuden, verkon turvallisuuden osalta tarvittaessa yhdessä yleisen viestintäverkon tarjoajan kanssa. Näillä toimenpiteillä on voitava varmistaa riskiin suhteutettu turvallisuustaso ottaen huomioon uusin tekniikka ja toimenpiteiden käyttöönottokustannukset. Jos verkon turvallisuuteen kohdistuu erityinen riski, on yleisesti saatavilla olevan sähköisen viestintäpalvelun tarjoajan ilmoitettava tilaajille tällaisesta riskistä, ja jos palvelujen tarjoaja ei voi vaikuttaa riskiin, mahdollisista korjauskeinoista mukaan lukien asiaan liittyvät todennäköiset kustannukset.

Lain 6. luvussa käsitellään liikenne- ja paikkatietoja direktiivin vaatimusten mukaisesti. Verkon ylläpitäjällä ja lisäarvopalvelun tarjoajalla on velvollisuus pyyhkiä pois tai tehdä liikenne- ja paikkatiedot tunnistamiskelvottomiksi sen jälkeen, kun niitä ei enää tarvita viestien välittämiseen. Tietoja, joita tarvitaan tilaajalaskutukseen tai yhteisliikenteen maksamiseen, voidaan kuitenkin säästää tietyn ajan. Tiedot, jotka koskevat henkilöä, joka on antanut suostumuksensa markkinointia tai palvelun tarjoamista varten, voidaan myös säilyttää. Suostumus voidaan kuitenkin aina perua. Liikennetiedot voidaan säilyttää myös, jos ne ovat tarpeen sähköisen tietoverkon tai viestintäpalvelun luvattoman käytön estämiseksi tai paljastamiseksi. Lain perusteluissa on todettu, että tämä käsittää liikennetietojen säilyttämisen rikos- tai siviilioikeudellisen oikeudenkäynnin käynnistämiseksi tai rikoksen selvittämiseksi tai syytteeseen panemiseksi silloin, kun tämä koskee verkon tai kyseisen palvelun laittoman käytön estämistä tai paljastamista.

Tietoja ei saa säilyttää pitempään kuin välttämätöntä tarkoituksen saavuttamiseksi eikä missään tapauksessa yli vuoden aikaa ilman perusteltua syytä, kuten että esitutkintaa tietojen perusteella on suoritettu. Liikennetietojen osalta on myös säädetty, että yleisen viestintäverkon ylläpitäjän on ilmoitettava henkilölle, jota asia koskee, minkälaisia liikennetietoja käsitellään ja kuinka kauan niitä käsitellään ilman suostumuksen pyytämistä.

Paikkatietoja, jotka liittyvät yksityishenkilöön palvelun käyttäjänä tai tilaajana, saa lain mukaan käsitellä vasta sen jälkeen, kun ne on tehty tunnistamiskelvottomiksi tai milloin tilaaja tai käyttäjä on antanut suostumuksensa niiden käyttöön. Näissäkin tapauksissa on informoitava, mitä tietoja käsitellään ja mihin tarkoitukseen niitä käsitellään. Suostumus on peruttavissa.

Lain 6. luvun 15 § ja 16 § käsittelevät tilaajatietoja ja niiden käsittelyä. Tilaajana olevalle luonnolliselle henkilölle on niiden mukaan ilmoitettava, mihin tarkoitukseen

yleisesti saatavilla olevaa tilaajaluetteloa käytetään, ennen kuin hänen tietonsa voidaan sisällyttää siihen. Jos luettelo on sähköisessä muodossa, on tilaajaa informoitava myös luettelon hakuominaisuuksista. Tässäkin yhteydessä henkilötietojen käsittely edellyttää kohteena olevan luonnollisen henkilön suostumusta.

Lain 5. luvun 7 §:ssä säännellään yleisesti saatavilla olevan puhelinpalvelun ylläpitäjän velvollisuuksia. Säännöksessä todetaan, että ylläpitäjän on varmistettava, että palvelu tai yleinen puhelinverkko, joka on kytketty kiinteään verkkoliityntäpaikkaan, täyttää kohtuulliset toiminnalliset ja teknisen luotettavuuden vaatimukset kestävyyden ja saavutettavuuden suhteen rauhan aikaisten poikkeusolojen aikana.

Lain 6. luvun 19 §:ssä määrätään, että toimintaa on harjoitettava niin, ettei pakko-keinoja koskevassa lainsäädännössä tarkoitettu telekuuntelu tai televalvonta paljastu. Telepalvelua tarjoavan on siis toimittava yhteistyössä viranomaisten kanssa näissä tapauksissa. Lainkohdassa todetaan, että sen, joka harjoittaa yhteistyövelvollisuuden alaista toimintaa, on käytettävä teknisiä apuvälineitä ja annettava henkilökohtaista tai organisatorista apua. Saman luvun 22 §:ssä on asetettu teleoperaattoreille velvollisuus luovuttaa tietyn törkeysasteen omaavien rikosten ollessa kyseessä tilaajatietoja tai liikennetietoja, jotka on muuten säädetty laissa salaisiksi. Tämä tulee kuitenkin kysymykseen vain silloin, kun operaattori ei ole jo poistanut tietoja. On huomattava, että Ruotsin on EU-maana jatkossa implementoitava EU:n direktiivi teletietojen tallettamisesta, jolloin operaattorilla on säilytysvelvollisuus kansallisen liikkumavaran puitteissa säädetyn ajan.

Ruotsissa ei siten ole erillistä sähköisen viestinnän tietosuojalakia kuten Suomessa. EkomL:n sääntely kohdistuu vain teleyrityksiin ja lisäarvopalvelun tarjoajiin eikä yhteisötilaajiin eli tavallisiin yrityksiin tai muihin organisaatioihin, jotka käsittelevät viestintäverkossaan käyttäjien luottamuksellisia viestejä tunnistamistietoja tai paikkatietoja.

Sähköisen viestinnän tietosuojadirektiivin säännöksiä on otettu kuitenkin Ruotsin markkinointilakiin[88]. Ruotsin markkinointilakia muutettiin 2004 sähköisen viestinnän tietosuojadirektiivin 2002/58/EY implementoimiseksi haittapostin lähettämiseen liittyvillä määräyksillä.

[88] Marknadsföringslagen (1995:450).

8.5.2 Kameravalvonta

Ruotsissa on kameravalvontaa säännelty yksityiskohtaisesti lainsäädännöllä. Toisaalta on olemassa laki[89] yleisestä kameravalvonnasta. Tämän lain yleisenä vaatimuksena on, että kameravalvontaa tulee suorittaa niin, että otetaan riittävästi huomioon yksityisyyden suoja. Esitutkinnassa käytettävää salaista kameravalvontaa koskee erillinen laki[90] samoin kuin pakkokeinona käytettävää kameravalvontaa varten on oma lakinsa[91]. Seuraava esitys koskee lakia yleisestä kameravalvonnasta.

Laki koskee valvontalaitteita (*övervakningsutrustning*), jolla laissa tarkoitetaan

1) TV-kameroita, muita optis-elektronisia ja niihin verrattavissa olevia laitteita, jotka on asennettu niin, että niitä voidaan liikuttamatta käyttää henkilövalvontaan, sekä erillisiä teknisiä laitteita, joilla voidaan käsitellä tai säilyttää valvontakameroilla otettuja kuvia, sekä

2) erillisiä teknisiä laitteita, joita käytetään kuunteluun tai äänen taltiointiin, joita käytetään valvontakameroiden yhteydessä.

Tieto yleisestä kameravalvonnasta on annettava selvällä tavalla, esimerkiksi kyltein. Mikäli valvontaan liittyy äänen tarkkailua, on tästäkin ilmoitettava asianmukaisesti. Tiedottamisvelvollisuus tulee ajankohtaiseksi, kun valvontalaitteisto asennetaan. Tiedottamista ei kuitenkaan tarvitse tehdä, jos yleinen kameravalvonta tapahtuu yhteiskunnalle tärkeiden laitosten suojaamiseksi annetun lain[92] perusteella tai poliisin suorittama automaattinen nopeudenvalvonta. Lääninhallitus voi erityisestä syystä myöntää poikkeuksia tiedottamisvelvollisuudesta ja voi tätä koskevassa päätöksessään asettaa poikkeukselle ehtoja. Poikkeus ei kuitenkaan koske äänen tallentamista, josta on joka tapauksessa tiedotettava.

Lupavaatimus ja siitä tehtävät poikkeukset: Valvontakameran asentaminen paikkaan, johon yleisöllä on pääsy, on myös luvanvaraista. Luvan myöntää lääninhallitus kuultuaan sitä kuntaa, jossa valvontaa harjoitetaan. Lupamenettelystä säädetään lain 15,16, 18, 19 ja 20 §:ssä. Lupaa ei kuitenkaan tarvita kaikissa tapauksissa. Näin on asian laita silloin, kun valvontakamera on asetettu ajoneuvoon liikenne- tai työturvallisuuden parantamiseksi tai kyse on Ruotsin tielaitoksen suorittamasta liikenteen tai liikennemaksujen maksamisen valvonnasta. Poikkeuksia on myös kameravalvonnasta pelikasinoissa, jos valvonnan tarkoituksena on rikosten

---

[89] Lag (1998:150) om allmän kameraövervakning.

[90] Lag (1995:1506) om hemlig kameraövervakning.

[91] Lag 1952:98 med särskilda bestämmelser om tvångsmedel i vissa brottmål.

[92] Lag 1990:217 om skydd för samhällsviktiga anläggningar.

selvittäminen tai riitaisuuksien ratkaiseminen. Tällöin poikkeus ei kuitenkaan koske äänen taltiointia. Poliisiviranomainen tai muu onnettomuuksien vaikutusten torjumisesta annetussa laissa[93] tarkoitettu pelastustoimen johtaja voi harjoittaa kameravalvontaa, joka on tarpeen onnettomuustapauksen torjumiseksi tai sen vaikutusten rajoittamiseksi. Vastaavasti poliisiviranomainen voi harjoittaa kameravalvontaa ilman lupaa, jos valvonta on tarpeen rikoksen uhkan torjumiseksi. Näitä tarkoituksia varten kameravalvontaa voi harjoittaa kuukauden ajan ilman hakemuksen jättämistä lääninhallitukseen.

Pelkkä ilmoitusmenettely: Eräissä tapauksissa riittää pelkkä ilmoitus valvontakameran asettamisesta. Kyse on tapauksista, joissa kameravalvonnan tarve on ilmeinen. Ilmoitusmenettelystä säädetään lain 17 §:ssä. Näin on asian laita silloin, kun valvontakamera asetetaan pankin tai luottomarkkinayrityksen tiloihin tai postikonttoriin, näiden sisääntulo- tai poistumisteiden läheisyyteen tai maksuautomaattien läheisyyteen, jos automaatin tarkoituksena on estää tai vähentää rikollisuutta, minkä lisäksi kameran on oltava kiinteästi asennettu ja siinä on oltava kiinteä objektiivi. Pankki- tai sijoitusmarkkinayrityksen tilat on määritelty näitä toimintoja koskevassa laissa[94] ja postikonttoritoiminta puolestaan postilaissa[95]. Kuuntelu tai äänitaltiointi voi kuitenkin tapahtua vain, kun näihin tarkoituksiin käytetty laite on aktivoitu rikosepäilyn vuoksi.[96] Ilmoituksen jälkeen valvontakameran saa asentaa kauppahuoneistoon, jos valvonnan ainoana tarkoituksena on estää tai paljastaa rikoksia, valvontakamera on kiinteästi asennettu ja varustettu kiinteällä optiikalla ja se henkilö, jonka on määrä harjoittaa valvontaa, on solminut kirjallisen sopimuksen valvonnasta suojeluvaltuutetun, suojelutoimikunnan ja työntekijöitä työpaikalla edustavan organisaation kanssa.

Kauppahuoneistolla tarkoitetaan huoneistoa, jossa kuluttajat voivat ostaa tavaroita tai palveluja tai vuokrata tavaroita, ei kuitenkaan ravintoloita tai muita ruokailuun tarkoitettuja paikkoja (*näringsställen*). Kauppahuoneistoa koskevat säännökset käsittävät myös samassa huoneistossa harjoitettavaa pankki- ja postikonttoritoimintaa. Ainoastaan kassa-alueelta tai sisään- ja ulostuloväylistä otettuja kuvia voidaan käsitellä ilman lupaa. Kuuntelu tai äänittäminen edellyttää aina lupaa.

Aineiston säilyttäminen: Silloin kun kameravalvontaa harjoitetaan paikassa, johon yleisöllä on pääsy, ei käsiteltyjen tai säilytettyjen kuvien tai tallennetun äänen kanssa

---

[93] Lag 2003:778 om skydd mot olyckor.

[94] Lag (2004:297) om bank- och finansieringsrörelse.

[95] Postlag (1993:1684).

[96] Lakimuutos 2004:442.

saa olla tekemisissä kuin ne henkilöt, joita tarvitaan valvonnan suorittamiseen. Aineistoa on käsiteltävä niin, että sen väärinkäyttö estetään.

Aineistoa saa säilyttää ainoastaan kuukauden, ellei lääninhallitus myönnä pidempää säilytysaikaa. Tätä määräystä ei kuitenkaan sovelleta, jos aineistolla on merkitystä rikoksen selvittämisessä, ja sen on kerännyt poliisiviranomainen tai aineisto on luovutettu poliisiviranomaiselle kuukauden kuluessa sen keräämisestä tai aineisto annetaan tuomioistuimelle. Kun kuva- tai äänimateriaalin säilyttäminen ei enää ole sallittua, on se tuhottava välittömästi.

Lääninhallitus valvoo lain määräysten noudattamista. Se voi mm. tarkastaa säilytettävän kuva- tai äänimateriaalin. Lääninhallituksen päätöksestä voidaan valittaa hallintotuomioistuimeen.

Laissa on asetettu vaitiolovelvollisuus niille henkilöille, jotka kameravalvonnan kautta saavat selon jonkun henkilön yksityiselämästä. Lain 26–28 §§ sisältävät säännösten rikkomisesta seuraavia rangaistussäännöksiä.

8.6 Sähköisten palvelujen tuottaminen

Edellä mainittu EkomL[97] sisältää erityisesti viestintämarkkinoita koskevia määräyksiä. Lailla on sähköisen viestinnän tietosuojadirektiivin lisäksi implementoitu neljä viestintämarkkinoita koskevaa direktiiviä. Lain tarkoituksena on antaa kansalaisille, yrityksille ja viranomaisille pääsy tehokkaaseen sähköiseen viestintään. Lailla pyritään myös turvaamaan sähköisten viestintäpalvelujen saatavuus eri puolilla maata.

Laki[98] sähköisestä kaupankäynnistä ja muista tietoyhteiskunnan palveluista puolestaan implementoi sähkökauppadirektiivin 2000/31/EY, joskin direktiivi edellytti muutoksia myös markkinointilakiin. Etämyynnistä on säädetty erillinen laki.[99]

EU:n sähköisen rahan direktiivi (2000/46/EY) on pantu täytäntöön erillisellä lailla[100], jota on vuoteen 2006 mennessä ehditty muuttaa jo kuusi kertaa.

---

[97] Lag 2003:389 om elektronisk kommunikation.

[98] Lag 2002:562 om elektronisk handel och andra informationssamhällets tjänster.

[99] Distans- och hemförsäljningslag 2005:59.

[100] Lag (2002:149) om utgivning av elektroniska pengar.

Ruotsin tekijänoikeuslakia[101] kirjallisiin ja taiteellisiin teoksiin on muutettu EU:n tietoyhteiskuntadirektiivin implementoimiseksi.

Ruotsissa ei ole lainsäädäntöä kansallisista verkkotunnuksista, vaan verkkotunnuksen rekisteröi **Internet Infrastruktur i Sverige** -niminen aatteellinen järjestö.

Ruotsissa on ns. ehdollisen pääsyn direktiivi 1998/84/EY saatettu voimaan lailla eräiden suojauksen purkujärjestelmien kieltämisestä.[102]

8.7 Sähköiset allekirjoitukset ja tunnistaminen

EU-direktiivin 1999/93/EY implementoimiseksi säädettiin Ruotsissa jo seuraavana vuonna laki[103] kvalifioiduista sähköisistä allekirjoituksista. Lain mukaan telehallintoviranomainen (Post- och telestyrelsen) ylläpitää luetteloa laatuvarmentajista, joiden tulee tehdä lain 8 §:ssä tarkoitetun ilmoituksen. Laki on sellaisenaan kuitenkin jäänyt taustalle, koska Ruotsin markkinoille ei ole laatuvarmenteita myöntäviä varmentajia.

Sähköisten allekirjoitusten käyttö ja sähköinen asiointi perustuukin Ruotsissa pitkälle ohjelmistovarmenteille. Julkinen sektori eli valtiokonttori on kuitenkin määrittänyt varmennestandardin kaupallisille toimijoille ja harjoittaa valvontatoimintaa varmentajien suhteen sikäli, kun kyse on asioinnista valtion viranomaisten kanssa. Useat pankit ovat muodostaneet yhteisen varmentajatoiminnon ja käytössä on myös sähköinen henkilökortti. Ruotsissa voi veroilmoituksen jättää ilmoituksen yhteydessä tulleita kirjautumis- ja allekirjoitussalasanoja käyttämällä mikäli ilmoittaja hyväksyy veroehdotuksen. Jos ilmoittaja haluaa tehdä muutoksia, vaaditaan kuitenkin sähköinen henkilökortti.

Ruotsissa on valmisteltu lakia, jolla implementoidaan EU biometrisiä passeja koskeva direktiivi. Biometristen tunnistamismenetelmien käyttöä työelämässä on kommentoinut Ruotsin tietosuojaviranomainen.[104] Kannanotossa käydään läpi biometristen tunnistamismenetelmien käyttö erityisesti henkilötietolain pykälien näkökulmasta. Ruotsissa on käyty aktiivista keskustelua DNA:n rekisteröinnistä.

---

[101] Lag 1960:729 om upphovsrätt till litterära och konstnärliga verk.

[102] Lag (2000:171)om förbud beträffande viss avkodningsutrustning.

[103] Lag (2000:832) om kvalificerade elektroniska signaturer.

[104] Datainspektionin tiedote 1.6.2005 ´Förfrågningar angående biometri i arbetslivet´.

8.8 Tietoturva ja sähköiset palvelut aineellisessa lainsäädännössä

8.8.1 Pankkitoiminta ja rahanpesu

Pankkisalaisuus on Ruotsissa toteutettu lainsäädäntöteitse. Ruotsin pankkitoiminta-lain[105] 10 § määrää, että henkilön asiakassuhdetta pankkiin ei saa asiattomasti paljastaa. Julkisoikeudellista toimintaa käsitellään kuitenkin viranomaistiedon julkisuutta koskevassa laissa. Laki ei sisällä tietoturvallisuutta koskevia vaatimuksia, mutta tietoturvallisuus mainitaan viranomaisen ohjeissa.[106]

Ruotsissa on ollut rajoituksia luottotietojen käsittelystä Internetissä, mutta vuonna 2003 Ruotsin korkein hallinto-oikeus lievensi niitä.

Rahanpesua vastaan on Ruotsissa säädetty laki ja asetus.[107] Asiakkaan tunnistamisen osalta säännökset viittaavat valvontaviranomaisen yksityiskohtaisempiin ohjeisiin. Valvontaviranomainen eli Finansinspektionen antoi ohjeet rahanpesun vastaisista toimista viimeksi kesäkuussa 2005.[108]

8.8.2 Hankintalainsäädäntö ja verkkolaskutus

Ruotsi on parhaillaan implementoimassa EU:n hankintadirektiivejä. Uudistuksen sisältö ei ole vielä kokonaan selvillä, mutta Ruotsi ei aseta lainsäädännössään sähköisessä muodossa olevalle tarjoukselle sähköisen allekirjoituksen vaatimusta.

Verkkolaskutus on Ruotsissa mahdollistettu lainsäädännössä. Tätä koskevia määräyksiä on arvonlisäverolaissa[109], kirjanpitolaissa[110] sekä verotuslaissa[111]. Lain muutokset ovat mahdollistaneet sen, että veroviranomainen hyväksyy sähköiset laskut sekä sen, että kolmas taho voi hoitaa laskutuksen myyjän puolesta. Sähköisen laskutuksen käyttö edellyttää, että vastaanottaja hyväksyy laskutuksen tapahtuvan

---

[105] Bankrörelselag 1987:617.

[106] Finansinspektion: FFFS 2005:1 Allmänna råd om styrning och kontroll av finansiella företag.

[107] Lag (1993:768) om åtgärder mot penningtvätt, muutettu viimeksi 2005 (409/2005) ja Förordning (2002:552) om åtgärder mot penningtvätt och finansiering av särskilt allvarlig brottslighet i vissa fall.

[108] Finansinspektion: FFFS 2005:5: Föreskrifter och allmänna råd om åtgärder mot penningtvätt och finansiering av särskilt allvarlig brottslighet i vissa fall.

[109] Mervärdesskattelag 1994:200, muutettu.

[110] Bokföringslag 1999:1078, muutettu.

[111] Skattebetalningslag 1987:483, muutettu.

sähköisessä muodossa. Vaikka uutta lainsäädäntöä valmisteltaessa keskusteltiin erilaisista teknisistä ratkaisuista verkkolaskujen alkuperän selvittämiseksi, ei Ruotsin lakiin lopulta kirjattu mitään muotovaatimuksia. Sähköiset laskut on muiden laskujen tavoin arkistoitava kymmeneksi vuodeksi. Kun arkistointi tapahtuu sähköisesti, on myös laskun lukemisessa tarvittavien teknisten menetelmien ja ohjelmien oltava saatavilla vastaavan ajan. Verkkolaskut voidaan arkistoida myös toiseen EU-valtioon, joka on kuitenkin ilmoitettava veroviranomaisille.

8.9 Tietoturvallisuuteen liittyvät yleiset palvelut

Ruotsissa on käytössä kansallinen versio SS-ISO/IEC17799 sekä SS 62 7799 tietoturvan johtamisjärjestelmistä. Sen kaksi osaa määrittävät suuntaviivat tietoturvan johtamisjärjestelmille ja sisältävät eritelmiä ja käyttöohjeita. Standardi sisältää käsitteistöä ja määritelmiä.

Ruotsin standardisointiorganisaatio **Standardiseringen i Sverige (**SIS) on laatinut vuonna 2003 käsikirjan **Handbok 550: Terminologi för informationssäkerhet**. Tietoturvaa käsittelevän SIS-työryhmän mukaan tietoturvallisuuden käsite laajan joukon käsitteitä tietoturvallisuuspolitiikasta riskienhallintaan sekä hallinnollisiin ja teknisiin toimenpiteisiin.

Ruotsin kriisienhallintaviranomainen Krisberedskapsmyndigheten (KBM) on laatinut standardin **Basnivå för informationsäkerheten** eli BITS tietoturvallisuuden perus-tasoksi.[112] Försvarets materielverk sertifioi IT-turvallisuutta yleisen turvallisuuden kannalta keskeisissä laitoksissa.

Ruotsin tilintarkastustoimintaa varten on kansainvälisestä ISA401-standardista laadittu kansallinen versio **RS 401 Revision i en datorisered informationssystemmiljö**, jota ryhdyttiin soveltamaan vuoden 2004 alusta, ei kuitenkaan aluksi julkisella sektorilla. Tämän standardin sisältöä on käyty lyhyesti läpi tämän tutkimuksen kansainvälisessä osassa. Standardin tarkoituksena on lisätä tilintarkastussektorin tietoturva- ja IT-kysymyksiä koskevaa tuntemusta.

Ruotsissa toimii useita tietoturvallisuutta koskevia hälytysryhmiä. Näitä ovat *SITIC*, *SuNET CERT* ja Soneran *TS CERT*.

---

[112] KBM Rekommederar 1/2006.

9. Norja

9.1 Perustuslainsäännökset

Norjan perustuslaki on vuodelta 1814.[113] Perustuslaki on muodoltaan hieman muista selvityksen kohdemaista poikkeava, sillä se ei sisällä nimenomaista yksityiselämän suojaa koskevaa määräystä. Lähimpänä tätä on perustuslain artikla 102, joka kieltää kotietsinnän muissa kuin rikosasioissa. Perustuslain artikla 110c puolestaan asettaa valtion viranomaisille nimenomaisen velvoitteen kunnioittaa ihmisoikeuksia.

Yksityisyyden suoja on kehittynyt oikeuskäytännön myötä. Vuonna 1952 Norjan korkein oikeus totesi, että henkilöllisyys nauttii Norjan oikeudessa suojaa ja henkilöllisyyden suoja käsittää yksityiselämän suojan. Norjan perustuslain artikla 100 takaa kansalaisille sananvapauden. Postilähetyksiä voidaan sensuroida vain julkisten viranomaisten toimesta ja oikeuden luvalla. Norja on allekirjoittanut Euroopan ihmisoikeussopimuksen sekä YK:n kansalais- ja poliittisia oikeuksia koskevan yleissopimuksen, jotka on saatettu osaksi Norjan oikeutta.[114] Norja on Euroopan neuvoston jäsen.

Norja ei ole Euroopan unionin jäsen, mutta on osa Euroopan talousaluetta, joten ns. ykköspilarin lainsäädäntö eli mm. tietosuojaa koskevat ja sähköistä kaupankäyntiä direktiivit tulevat osaksi Norjan oikeutta, mutta eivät esimerkiksi tietoverkkorikollisuutta koskevat puitepäätökset.

Vuoden 1902 rikoslain 390 § säätää rangaistavaksi yksityiselämän loukkaamisen, joka tapahtuu paljastamalla julkisesti henkilökohtaiseen tai kotielämään liittyvän seikan.

9.2 Tietoturvan sääntely ja kehittäminen

Norjassakaan ei tietoturvallisuutta koskevaa lainsäädäntöä ole koottu yksiin kansiin. Norjassa on laadittu kansallinen tietoturvastrategia nimeltään **@-Norge: Nasjonal strategi for informasjonssikkerhet**. Sen laatijoina ovat yhdessä puolustusministeriö, kauppa- ja elinkeinoministeriö sekä oikeus- ja poliisiministeriö. Näin tietoturva mielletään kansalliseksi, yli yksityisen ja julkisen sektorin rajan ulottuvaksi tavoitteeksi. Kansallinen strategia käsittää kahdeksan kohtaa, joista voidaan tässä yhteydessä

---

[113] LOV 1814-05-17 nr 00: Kongerikets Norges Grundlov, given i Riksforsamlingen paa Eidsvold den 17de Mai 1814.

[114] LOV 1999-05-21 nr 30: Lov om styrking av menneskerettighetetenes stilling i norsk rett (menneskerettsloven).

mainita joitakin. Näistä ensimmäinen ja tärkein on yhteiskunnalle kriittisen IT-infrastruktuurin suojelu saavutettavuuden, eheyden ja luottamuksellisuuden suhteen.

Toinen tämän selvityksen kannalta olennainen on tietoturvallisuutta koskevan sääntelyjärjestelmän ylläpito ja kehittäminen yhtenäisellä tavalla. Sääntelyn kohteen toimintaa tulisi helpottaa samalla kun sääntelyn tehokkuus säilytetään. Sääntely- ja muiden viranomaisten tulee vaihtaa kokemuksia ja tehdä yhteistyötä yhteisten toiminta-tapojen ja työkalujen löytämiseksi.

Mielenkiintoinen on myös ohjelmakohta, jossa IT-alalla todetaan kollektiivisesti olevan vastuu tuotteiden turvallisuusominaisuuksista ja käyttäjille ohjeistamisesta suojaus-mahdollisuuksien suhteen. Alan olisi kehitettävä tätä varten normeja tuotekehitystä varten ja käyttäjäystävällisen tietoturvallisuuden kehittämiseksi sekä ottaa vastuu omista asiakkaiden ja yhteistyökumppaneiden tietoturvallisuuden suhteen. Mikäli IT-ala ei haluaisi tätä vastuuta kantaa, on viranomaisten ryhdyttävä asianmukaisiin sääntely-toimiin tai kehitettävä käytäntöjä omassa ostopolitiikassaan.

Keskeinen on myös vaatimus, jonka mukaan kriittisiä IT-järjestelmiä tulisi suojata sertifioiduilla turvallisuusjärjestelyillä. Ohjelmassa kannustetaan tietoturvastandardien mukaisien ratkaisujen käyttöön.

Norjaan on perustettu erityinen tietoturvaviranomainen, puolustusministeriön alaisuudessa toimiva **Nasjonal sikkerhetsmyndighet**. Sen tehtävänä on rakentaa ja kontrolloida tietoturvallisuutta. Virasto raportoi puolustusministeriölle puolustusasioista mutta oikeusministeriölle muista asioista. Norjan tietosuojaviranomainen **Datatilsynet** on antanut ohjeistusta tietoturvallisuudesta.[115]

9.3 Erityispiirteitä viranomaistoiminnasta ja pakkokeinoista

Puhelinkuuntelu edellyttää Norjassa normaalisti tuomioistuimen lupaa ja lupa myönnetään alustavasti neljäksi viikoksi.[116] Laissa on joitakin poikkeuksia tuomio-istuimen myötävaikutuksen vaatimukseen nähden, erityisesti huumausainerikosten valvonnan osalta.[117] Salakuuntelu nousi Norjassa keskustelun aiheeksi ns. Lundin komission raportin julkistamisen jälkeen 1990-luvulla. Raportti käsitteli vasemmisto-

[115] Veiledning i informasjonsikkerhet for kommuner og fylker (2005).

[116] Rikosprosessilaki eli straffeprosessloven 16 a §.

[117] Ks. rikosprosessilain 216a ja 216b §§.

laisten poliittisten järjestöjen tarkkailua poliittisen kahtiajaon vuosikymmeninä. Raportin seurauksena Norjan turvallisuuspalveluiden valvontaa tehostettiin.[118]

Rikosprosessia koskevien sääntöjen lisäksi myös hallintoprosessilaki ja rikoslaki sisältävät yksityisyyden suojaa koskevia määräyksiä. Norjan rikoslaki kielsi jo vuonna 1889 henkilön yksityiselämää koskevan tiedon julkaisemisen. Rikoslaissa kriminalisoidaan sinetöidyn kirjeen avaaminen, ja rikoslain määräykset voidaan ulottaa tietoturvajärjestelyjen kuten salauksen ja suojauksen murtamiseen. Rikoslaki kieltää myös peitetyn tarkkailun ja puhelin- ja muun kuuntelun suljetuissa paikoissa.

Terrorismin vastainen taistelu on kuitenkin myös Norjassa saanut aikaan ehdotuksia poliisin toimintamahdollisuuksien laajentamisesta käsittämään myös salakuuntelun (norjaksi *romavlyttning*).[119] Huhtikuussa 2002 täydennettiin Norjan rikoslakia eräillä terrorismin torjuntaan liittyvillä säännöksillä.

Kansallisten turvallisuusviranomaisten ja yritysten välisistä yhteyksistä on Norjassa kokemuksia. Vuoden 2000 lopussa Norjan armeijan ja poliisin turvallisuusyksiköt solmivat sopimuksen maan 15 suurimman yrityksen kanssa harjoittaakseen Internetin valvontaa. Tavoitteena oli kansallisen tietoliikenneinfrastruktuurin puolustaminen. Yritysten ja viranomaissektorin yhteistyö tietoturva-asioissa on siten edennyt pitkälle myös käytännön tasolla. Valvonta muistutti FBI:n ylläpitämää Carnivore-järjestelmää Yhdysvalloissa. Carnivore valvoo kaikkea Internetin välityksellä lähetettyä tietoa.

9.4 Tiedon julkisuus ja salassapito

9.4.1 Viranomaistieto

Viranomaistiedon julkisuutta koskeva laki[120] vuodelta 1970 sääntelee viranomaistoiminnan julkisuutta. Laki takaa yleisesti viranomaisasiakirjojen ja -rekisterien julkisuuden. Poikkeuksen muodostavat parlamentin ja sen alaisten viranomaisten, kuten valtiontilintarkastajan ja oikeusasiamiehen asiakirjat. Myös jotkut kansainvälistä alkuperää olevat asiakirjat ovat salaisia samoin kuin informaatio, jonka paljastuminen voisi olla haitallista valtakunnan turvallisuudelle tai puolustukselle tai haittaisi suhteita vieraaseen valtioon tai kansainväliseen järjestöön. Ei-julkisia ovat myös viranomaiselle

---

[118] Ks. Norjan turvallisuuslaki, LOV 1998-03-20 nr 10: Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven**)**. Lakiin liittyy asiakirjojen luokitteluun liittyvä turvaohje eli *beskyttelseinstruksen*, johon liittyy IT-osa.

[119] Ks. tarkemmin raportti "*Mellom Effektivitet och Personvern*", NOU 2004:6.

[120] Lov om tillgang till offentlig information.

tehtyä kantelua koskevat asiakirjat samoin budjetin valmistelua koskevat valtiovarainministeriön asiakirjat. Erikseen on todettu, että henkilötietorekistereihin merkittyjen henkilöiden valokuvat eivät ole julkisia.

9.4.2 Yrityssalaisuuksien suoja

Norjassa ei ole erillistä yritysalaisuuksien suojaa koskevaa lakia vaan asiaa säännellään vuonna 1972 säädetyssä markkinalaissa.[121] Lain 7. artiklan mukaan henkilö, joka on saanut haltuunsa yrityssalaisuuden tai tiedon siitä ollessaan työsuhteessa, luottamustehtävässä tai liikesuhteessa salaisuuden haltijaan, ei saa käyttää yrityssalaisuutta laittomasti elinkeinotoiminnassa.

Samaa määräystä sovelletaan jokaiseen, joka on saanut hallintaansa tai tietoonsa yrityssalaisuuden sen johdosta, että toinen henkilö on rikkonut ammattisalaisuutta koskevan salassapitovelvollisuutensa tai muuten toisen henkilön lainvastaisen toimen seurauksena.

Rangaistussäännöt lain rikkomisesta ovat 17. artiklassa. Siinä säädetään korkeintaan kuuden kuukauden vankeusrangaistus lain rikkomusten johdosta. Rangaistusseuraamukset ovat siten melko lieviä. Lisäksi kyseisen artiklan 5. momentissa lisätään, että rangaistusta ei saa määrätä, milloin yrityssalaisuus on hankittu työsuhteessa tai luottamustehtävässä tai saatu henkilöltä, joka on ollut tällaisessa suhteessa ja kaksi vuotta on kulunut kyseisen aseman päättymisestä.

9.5 Tietosuojasäännökset

9.5.1 Yleiset tietosuojasäännökset

Norjan nykyinen tietosuojalaki[122], on vuodelta 2000. Sitä täydentää tietosuoja-asetus[123]. Laki perustuu EU-direktiiviin, joten sen määräykset ovat lähes kauttaaltaan samansisältöiset kuin direktiivi. Poikkeuksen muodostaa kuitenkin lain 21 §, joka koskee henkilöprofiilien käyttöä. Tuon pykälän mukaan henkilö, joka ottaa yhteyden rekisteröitävään tai tekee tätä koskevia päätöksiä perustuen tämän henkilöprofiileihin, joiden on tarkoitus kuvata käytöstä, mieltymyksiä, kykyjä tai tarpeita esimerkiksi markkinointiin

[121] Lov om kontroll med markedsføring og avtalevilkår (markedsføringsloven) nr 47 av 16. juni 1972.

[122] Lov om behandling av personopplysninger LOV 2000-04-14 nr 31.

[123] Forskrift om behandling av personopplysninger FOR 2000-12-15 nr 1265.

liittyen, rekisterinpitäjän[124] on informoitava rekisteröitävää kerääjän henkilöstä, käytetyn tiedon laadusta ja tiedon lähteestä.

Tietosuojalain 13 artikla sisältää tietoturvamääräyksen, joka perustuu EU-direktiiviin, mutta on seikkaperäisempi. Sen mukaan rekisterinpitäjän ja tiedon käsittelijän on turvattava henkilötietoja koskeva tietoturvallisuus suunniteluilla ja järjestelmällisillä toimilla luottamuksellisuuden, eheyden ja saavutettavuuden suhteen henkilötietojen käsittelyn yhteydessä. Tämän saavuttaakseen rekisterinpitäjän ja tiedon käsittelijän on raportoitava asiakirjoin tietojärjestelmästä ja turvatoimista. Asiakirjojen on oltava sekä rekisterinpitäjän että tiedon käsittelijän työntekijöiden tutustuttavissa. Myös **Datatilsynetin** samoin kuin tietosuojan oikeusturvaelimen vetoomuslautakunnan (**personvernnemnda**) on voitava tutustua asiakirjoihin. Rekisterinpitäjän, joka sallii muiden henkilöiden käsitellä henkilötietoja, on huolehdittava siitä, että nämä täyttävät myös lain vaatimukset.

Tietosuoja-asetuksen 2 luku sisältää myös tietoturvallisuutta koskevia määräyksiä. Norjan tietosuojaviranomainen Datatilsynet on julkaissut kyseisistä määräyksistä ohjeen **Sikkerhetbestemmelsene i personopplysningsforskriften med kommentarer**. Ohje soveltuu ainoastaan niissä tapauksissa, joissa henkilötietojen käsittely tapahtuu sähköisesti. Henkilötietojen manuaaliseen käsittelyyn soveltuu ainoastaan henkilötietolain 13 §:ssä oleva yleissääntö. Tietosuoja-asetus sisältää vaatimuksia johtojärjestelmistä, joita rekisterinpitäjän täytyy luoda saavuttaakseen tyydyttävän tietoturvan tason. Asetuksen vaatimukset tulee olla täytetty, ennen kuin tietojenkäsittelyyn ryhdytään.

Tärkeä osatekijä tässä suhteessa on turvajohtamisen vaatimus. On luotava turvallisuutta koskevat tavoitteet ja niitä koskeva strategia. Tavoitteita on arvioitava tarkastuksin. Rekisterinpitäjän on tehtävä riskiarviointi sen suhteen, mitä tietojen-käsittelyllä on luottamuksellisuuden, saavutettavuuden ja eheyden suhteen. Riski-arvioinnin on päädyttävä samalla hyväksyttävälle riskitasolle, jonka rekisterinpitäjä on asettanut. Tarvittaessa on määriteltävä toimenpiteet hyväksyttävän riskitason saavuttamiseksi. Ohjeisto sisältää vaatimuksia myös dokumentoinnin suhteen.

Tietosuoja-asetuksen vaatimukset ovat mittapuu, johon on viitattu muussa, toimiala-kohtaisessa viranomaissääntelyssä myös henkilötietoja yleisemmän tietoturvallisuuden saavuttamiseksi eli säännöksillä on yleisempääkin merkitystä.

---

[124] Laissa käytetään jaottelua *behandlingsansvarlig* ja *databehandler*, joista ensimmäinen vastaa rekisterinpitäjää ja jälkimmäisellä tarkoitetaan tiedon tosiasiallista käsittelijää.

Norjassa on implementoitu EU:n sähköisen viestinnän tietosuojadirektiivi 2002/58/EY sähköistä viestintää koskevalla yleislailla eli **ekomlovenilla**.[125] Tuon lain 2–7 § sisältää direktiivin tavoin yleismääräyksen, jonka mukaan liittymän tarjoajan on toteutettava riittävät turvatoimenpiteet suojatakseen liikennettä omissa verkoissaan ja palveluissaan. Kun turvallisuuden suhteen esiintyy riskejä, on palveluntarjoajan informoitava käyttäjää näistä. Vastaavasti liikennetiedot on tehtävä nimettömiksi heti, kun ne eivät enää ole tarpeen viestintä- tai laskutustarpeisiin, ellei muuta ole säädetty. Myös liikennetietojen käsittely edellyttää puolestaan palvelun käyttäjän suostumusta.

Ekomlovenin 2–9 §:n mukaan palveluntarjoajan ja pystyttäjän[126] on ylläpidettävä viestinnän luottamuksellisuutta sekä pidettävä salassa sähköisen viestinnän käyttö, mukaan lukien tiedot teknisistä järjestelmistä ja menetelmistä. Velvollisuus käsittää sen, että ryhdytään toimenpiteisiin sen varalta, etteivät muut kuin tietoon oikeutetut saisi käsiinsä tietoja. Palveluntarjoaja ja -pystyttäjä eivät saa käyttää kyseistä tietoa myöskään omaksi tai muun tahon hyväksi, poikkeuksena nimettömäksi tehty tilastotieto verkon liikenteestä, joka ei tarjoa tietoa järjestelmistä tai teknisistä ratkaisuista. Salassapitovelvollisuus ulottuu myös palveluntarjoajan, pystyttäjän tai valvonta-viranomaisen lukuun työtä tekevän henkilöön, myös kyseisten työtehtävän päättymisen jälkeen.

Luottamuksellisuutta koskeva vaatimus ei estä informaation luovuttamista syyttäjä-viranomaiselle tai poliisille salaisista puhelinnumeroista tai muusta tilaaja-informaatiosta, samoin kuin tunnistetiedoista. Sama koskee näyttöä oikeudessa. Mainittuja tietoja voi myös luovuttaa toiselle viranomaiselle lain mukaan. Viranomaiset voivat antaa määräyksiä luottamuksellisuuden suhteen.

Uusi laki merkitsi huononnusta aikaisempaan oikeustilaan verrattuna, mitä tulee yksityisyyden suojaan. Ekomloven soveltamista koskeva asetus nimittäin vaatii palveluntarjoajaa pitämään rekisteriä kaikista asiakkaistaan. Näin ollen anonyymit prepaid-liittymät eivät enää ole mahdollisia.

Norjassa ei ole erillistä lakia yksityisyyden suojasta työelämässä vaan asiaa on ohjeistettu Datatilsynetin ohjeilla.[127] Pääsääntönä on, että työnantajan halutessa lukea työntekijän sähköpostia ja muita tietokansioita tämä tarvitsee työntekijän suostumuksen tai asia ratkaistaan Norjan tietosuojalain 8 § f-kirjaimen ja EU-direktiivin tarkoittaman

---

[125] LOV 2003-07-04 nr 83: Lov om elektronisk kommunikasjon.

[126] Laissa ei ole tälle määritelmää.

[127] Ks. kannanotto *E-poster og filer*, 15.11.2004, joka on viranomaisen kotisivulla. Jotta viranomainenkin eläisi kuin opettaa, on Datatilsynet julkaissut omat sääntönsä *Datatilsynets egne retningslinjer for bruk av Internett og e-post*.

intressivertailun jälkeen. Norjalainen työnantaja voi päättää direktio-oikeutensa perusteella, että työhön liittyviin tarkoituksiin on käytettävä työnantajan tietojärjestelmiä. Työnantaja ei voi lukea kaikkea työntekijän sähköpostia. Työnantajan on laadittava säännöt tietojärjestelmän käytölle, jolloin on täsmennettävä, missä laajuudessa järjestelmää voidaan käyttää yksityisiin tarkoituksiin. Säännöissä, jotka on liitettävä yrityksen sisäisen tarkastuksen sääntöihin, on ilmaistava, missä olosuhteissa työnantaja voi lukea yksityistä sähköpostia. Lähtökohtana on, että jos tällaisia sääntöjä ei ole, ei työnantaja ole oikeutettu lukemaan työntekijän sähköpostia.

Mikäli työnantaja epäilee työntekijää epälojaaliudesta tai tämän toimivan sisäisten sääntöjen ja ohjeiden vastaisesti, voi syntyä oikeus tarkastaa työntekijän sähköposti-kirjeenvaihtoa. Viranomaisen kannanotossa todetaan, että jos työnantaja voi antaa hyviä perusteluja epäilyksille, voi asiallisten perustelujen vaatimus tarkastuksille täyttyä. Mikäli työnantajan tarkastusintressit konkreettisessa tapauksessa ovat suurempia kuin työntekijän oikeus yksityisyyteen, voidaan tarkastus suorittaa ilman työntekijän suostumusta.

Myös Norjan erityislainsäädäntö sisältää runsaasti tietosuojavaatimuksia, joita ei eritellä tässä. Poliisin ylläpitämien henkilörekisterien sääntely on nostettu esille, sillä Norjassa ei ole tätä koskevaa erityislainsäädäntöä.

9.5.2 Kameravalvonta

Vaikka kameravalvonta on myös rikosoikeudellinen ja pakkokeinolainsäädäntöön liittyvä kysymys, käsitellään sitä tässä yhteydessä osana tietosuojalainsäädäntöä. Kameravalvontaa sääntelee Norjan uusitun tietosuojalain VII luku (*Fjernsynsovervåkning*). Lain 36 §:ssä määritellään kameravalvonta tilapäisesti tai säännöllisesti suoritetuksi henkilövalvonnaksi, jota suoritetaan etäohjatulla tai automaattisella valvontakameralla (*fjernsynskamera*), valokuvaus- tai muulla laitteella. Matkapuhelimissa olevat kamerat kuuluvat myös lain piiriin. Toisin kuin Ruotsissa, eivät Norjan kameravalvontaa koskevat säännökset käsitä äänittämistä, vaan tätä koskevat periaatteet määräytyvät tietosuojalain ja rikoslain perusteella.

Kameravalvontaan sovelletaan erityismääräysten lisäksi tietosuojalain 8 § (henkilö-tietojen käsittelyn yleiset ehdot), 9 § (arkaluonteisten henkilötietojen käsittely), 11 § (henkilötietojen käsittelyn perusvaatimukset), 31 § (ilmoitusvelvollisuus valvonta-viranomaiselle) ja 32 § (ilmoituksen sisältö). Kameravalvonta rikosten selvittämiseksi on myös sallittua, eikä tällöin tarvitse täyttää lain 19 §:ssä mainittua ilmoitus-velvollisuutta eikä lain 33 §:ssä mainittua viranomaisen suostumusta arkaluonteisten henkilötietojen käsittelyyn tarvita.

Kameravalvonta sellaisessa paikassa, johon vain rajoitetulla henkilöjoukolla on pääsy, on 38 §:n mukaan sallittua vain, jos valvonnalle on erityisiä perusteita. Tämä tarkoittaa mm. työpaikoilla suoritettavaa kameravalvontaa. Tällöin työntekijöille on etukäteen tiedotettava valvonnasta. Valvonnan kohteen mielipiteelle valvonnan suorittamisesta on annettava merkitystä ratkaistaessa voidaanko valvontaa suorittaa. Mikäli kyse on valvonnan kohteen turvallisuuden ja terveyden turvaamisesta, on valvonta helpommin perusteltavissa. Esimerkkeinä toimivat tilanteet, joissa valvonnan kohteena olevassa paikassa suoritetaan terveydelle riskialtista tuotantoa, tai jos paikka voi joutua rikoksen kohteeksi, kuten pankki- tai postikonttorit. Rikoksen ehkäisy kameravalvonnan keinoin paikoissa, joissa käsitellään tai säilytetään rahaa, on myös sallittua.

Kaupoissa, kioskeissa, pankki- tai postikonttoreissa tai bensiiniasemilla tapahtuva valvontaa ei yleensä pidetä perusoikeuksiin kajoavana ja on siksi sallittua. Kyse on paljolti yleisistä odotuksista yksityisyyden vaatimuksen puuttumisesta. Sen sijaan ravintoloissa, yökerhoissa ja vastaavissa paikoissa yleisön odotukset luottamuksellisuuden suhteen ovat suuremmat eikä valvonta ole perusteltavissa kuin poikkeuksellisista syistä. Turvallisuussyyt voivat oikeuttaa järjestelyn, jossa valvonta käynnistyy uhkaavissa tilanteissa. Vastaavasti kuntosaleilla tai uima-altailla olevat valvontakamerat eivät pääsääntöisesti ole hyväksyttävissä, poikkeuksena joissain tapauksissa turvallisuussyyt. Valvontakameroilla ei kuitenkaan voida korvata kokonaan valvontahenkilöstöä, vaan kameravalvonnan on täydennettävä fyysistä valvontaa.

Pääsääntönä on, etteivät yksityiset tahot voi suorittaa valvontaa julkisilla paikoilla, kuten kaduilla ja toreilla, vaan ainoastaan viranomaiset voivat suorittaa tällaista valvontaa. Liikennevälineissä ei valvonta ole pääsääntöisesti mahdollista. Poikkeuksena ovat jälleen turvallisuussyyt, ja harkintaa on suoritettava ajan ja paikan suhteen.

Mikäli tarkoituksena on ehkäistä rikollisuutta valvonnan kohteena olevien henkilöiden taholta, kuten kavalluksia ja petoksia, on osoitettava, että väärinkäytöksiä on tapahtunut ja että väärinkäytökset ovat mittaluokaltaan riittäviä perustelemaan valvonnan.

Asuntoyhteisöissä suoritettava valvonta edellyttää yhtiökokouksen tai vastaavan elimen päätöstä.

Kameravalvonnan tuloksena syntynyt aineisto voidaan luovuttaa muille kuin käsittelyvelvolliselle vain kuvatun suostumuksella tai luovutusmahdollisuus perustuu lakiin. Valvonta-aineisto voidaan myös luovuttaa poliisille rikosten tai onnettomuuksien tutkintaa varten, ellei laissa ole säädetty erityistä vaitiolovelvollisuutta. Asetuksella voidaan luovutusmahdollisuutta kuitenkin laajentaa.

Kameravalvonnasta julkisella paikalla tai paikassa, johon vain rajoitetulla henkilöjoukolla on pääsy, on lain 40 §:n mukaan ilmoitettava kyltein tai muulla keinoin tehtävä ilmeisen havaittavaksi, että paikka on kameravalvonnassa, ja kuka vastaa valvonnan suorittamisesta.

Kameravalvonnasta on ilmoitettava tietosuojaviranomaiselle (Datatilsynet). Ilmoitus on voimassa kolmen vuoden ajan, jonka jälkeen tarvitaan uusi ilmoitus. Viranomainen kiinnittää huomiotaan mm. valvontaan osallistuvien henkilöiden määrään ja siihen, miten määräyksiä voidaan arvioida noudatettavan.

Valvonta-aineiston säilytys on suoritettava turvallisesti. Fyysiset säilytysvälineet, kuten filmit, videonauhat tai cd-levyt täytyy säilyttää lukitussa tilassa. Digitaalista valvonta-aineistoa koskevat vielä suuremmat vaatimukset, jotka koskevat sekä tietokonetta, tietoverkkoa sekä kuva-aineiston siirtoa valvontakamerasta keskuslaitteeseen. Vain organisaation turvallisuudesta vastaavilla henkilöillä voi olla pääsy aineistoon. Aineisto on tuhottava sen jälkeen, kun sillä ei ole enää käyttöä ja viimeistään seitsemän päivää nauhoittamisen jälkeen. Jos aineisto todennäköisesti tullaan luovuttamaan poliisille rikostutkintaa varten, voidaan aineistoa säilyttää 30 päivän ajan. Pankki- ja postitoimistoissa otetut valvontakuvat voidaan säilyttää kolmen kuukauden ajan. Valvonta-aineistoa ei voida luovuttaa tai näyttää ulkopuolisille kuin valvonnan kohteen luvalla. Aineiston näyttäminen Internet-osoitteessa edellyttää kaikkien tunnistettavissa olevien henkilöiden suostumusta. Poikkeuksena on luovutus poliisille.

Valvontakameroiden käyttömahdollisuus ei sisällä mahdollisuutta äänittämiseen. Äänittämistä on tarkasteltava tietosuojalain yleismääräysten sekä muun lainsäädännön, kuten rikoslainsäädännön, pohjalta. Norjan tietosuojaviranomainen Datatilsynet on antanut ohjeistusta erityisesti puheluiden kuuntelun osalta.

Muun kuin oman puhelun nauhoittaminen tai kuunteleminen on rangaistavaa Norjan rikoslain 145a §:n perusteella. Myöskään omien puhelujen nauhoittaminen ei ole ilman muuta sallittua.

Kaikki äänittäminen, joka tapahtuu sähköisten apuvälineiden avulla, kuuluu Norjassa tietosuojalain piiriin. Samoin kaikki äänittäminen, jonka tulokset järjestetään henkilörekisteriksi, josta henkilö on tunnistettavissa, kuuluu lain piiriin. Äänittäminen edellyttää joko lain sallimaa perustetta tai vastapuolen suostumusta. Äänittäminen edellyttää, että äänittämisen aihe on tarkoin määritelty ja sille on asiallinen peruste. Äänitteiden on oltava merkityksellisiä aiheen kannalta. Kun kyse on toisaalta työntekijän ja työnantajan välisestä suhteesta ja toisaalta suhteesta asiakkaaseen tai muuhun ulkopuoliseen, on lain ehtoja tarkasteltava molemmissa suhteissa.

Äänittämisestä vastuullisella henkilöllä tai organisaatiolla on tiedonantovelvollisuus. Tämä pitää sisällään sen, että äänittämisen aihe ja äänitteiden säilyttämisen kesto on selvitettävä, sikäli kuin tämä on käytännössä mahdollista. Rekisteröidyllä eli sillä, jonka puhetta on äänitetty, on oltava mahdollisuus tarkistaa äänite. Äänitteet on hävitettävä sen jälkeen kun niiden aihe on täytetty. Äänitteitä säilytettäessä on pidettävä huolta tietoturvasta. Äänittämisen edellytyksistä kertoo tarkemmin tietosuojaviranomaisen tiedote **Lydopptak og personopplysningsloven**, joka löytyy viranomaisen kotisivuilta.

9.6 Sähköisten palvelujen tuottaminen

Norjassa on pantu täytäntöön EU:n sähkökauppadirektiivi erillisellä lailla[128]. Laki lähinnä toistaa direktiivin keskeisen sisällön.

EU:n vuoden 2002 tietoliikennettä koskeva lainsäädäntöpaketti on puolestaan pantu täytäntöön yhdellä lailla[129], kuten monessa muussakin maassa. Tämä laki sisältää lähinnä sisältää paljolti markkinaoikeudellisia määräyksiä, mutta myös, kuten edellä on todettu, sähköisen viestinnän tietosuojaan liittyviä määräyksiä.

Markkinoinnin osalta Norjan kuluttaja-asiamies (**forbrukerombudet**) on antanut vuonna 2002 suuntaviivat Internet-markkinointiin. Kannanotossa viitataan Pohjois-maiden kuluttaja-asiamiesten laatimaan yhteiseen kantaan elinkeinotoiminnasta ja markkinoinnista Internetin ja muiden tietoverkkojen välityksellä. Markkinointi Internetin välityksellä on Norjassa vuoden 1972 markkinalain alaista toimintaa.

Kuluttaja-asiamies katsoo kannanotossaan mm. että markkinointi sähköpostin kautta ilman vastaanottajan ennakkosuostumusta on vastoin markkinointilain 1 §:n kanssa. Kyseinen lainkohta kieltää yrityksiä käyttämästä menetelmiä, jotka ovat kohtuuttomia tai muutoin hyvän tavan vastaisia. Tämä määräys on saanut vahvistuksen markkinalain uudessa 2b §:ssä, jossa kielletään käyttämästä kuluttajille tapahtuvassa markkinoin-nissa ilman kuluttajan etukäteen antamaa lupaa yksilöllisen viestinnän mahdollistavia tietoliikennevälineitä, kuten sähköpostia, matkapuhelimien tekstiviestipalveluja, tele-kopiolaitteita tai automaattisoittolaitteita. Ennakkosuostumusta ei kuitenkaan vaadita markkinointiin, jossa kuluttajaan otetaan yhteyttä suullisesti puhelimen välityksellä.

Kuluttaja-asiamies on lisäksi katsonut, että sopimukset jotka eivät sisällä määräyksiä asiakkaan rekisteröimisestä ja kotisivun ylläpitämisessä käytetyistä tietosuoja-

---

[128] Lov om visse sider av elektronisk handel og andre informasjonssamfunnstjenester - ”ehandelsloven” LOV-2003-05-23 nr.35.

[129] Lov om elektronisk kommunikasjon Lov 2003-07-04 nr 83 (Ekomloven).

säännöistä, voidaan katsoa olevat vastoin markkinalain 9a §:ää, joka koskee kohtuuttomien ehtojen käyttöä kuluttajakaupoissa.

Julkisten viranomaisten tarjoamien sähköisten palvelujen käyttöön soveltuu tätä koskeva asetus.[130] On myös olemassa laki ja asetus julkisista arkistoista.[131]

9.7 Sähköiset allekirjoitukset ja tunnistaminen

Norjan laki sähköisistä allekirjoituksista eli **Lov om elektronisk signatur** on vuodelta 2001. Laki perustuu EU-direktiiviin ja käyttää siten samaa käsitteistöä kuin direktiivi. Vuodelta 2003 peräisin olevassa tietoturvastrategiassa todetaan, että Norjassa tulee kehittää saatavilla oleva infrastruktuuri sähköisille allekirjoituksille ja tunnistamiselle, joka perustuisi PKI-tekniikkaan.[132] Infrastruktuuri rakennettaisiin julkisen ja yksityisen sektorin yhteistyönä. Norjaan ei ole kuitenkaan vielä syntynyt laatuvarmentajia.

Datatilsynet on ottanut helmikuussa 2006 kantaa biometristen tunnisteiden käyttöön. Henkilötietolain 12 §:n mukaan voidaan yksiselitteisiä tunnistamiskeinoja käyttää vain, kun varmalle tunnistamiselle on asiallinen tarve ja menetelmä on tarpeen tunnistamisen suorittamiseksi. Siten sormenjäljet, silmän iiris ja muut biometriset tuntomerkit kuuluvat yksiselitteisten tuntomerkkien joukkoon. Vaikka biometrisestä tunnisteesta määriteltäisiin vain koodi, soveltuvat lain vaatimukset aina, kun koodi voidaan yhdistää henkilöön.

Datatilsynet on kuitenkin katsonut, että biometriset tunnistamiskeinot ovat varmoja tunnistamiskeinoja. Norjan henkilötietolain 12 § estää käytännössä biometristen tunnisteiden yleisen käytön ja Datatilsynet onkin ilmoittanut ehdottavansa, että kyseistä lainkohtaa muutettaisiin niin, että biometrinen tunnistaminen tulisi enemmän mahdolliseksi.

Norja on kiinnostunut seuraamaan kansainvälisen työjärjestön ILO:n yleissopimusta, jolla hallitukset velvoitetaan myöntämään merenkulkijoille biometriset henkilökortit terrorismin ehkäisemiseksi.

---

[130] Forskrift om elektronisk kommunikasjon med og i forvaltningen 2004-06-25 nr. 988 i kraft 2004-07-01.

[131] Lov om arkiv og forskrift om offentlig arkiv**.**

[132] Ks. norjalainen puheenvuoro sähköisestä tunnistamisesta: Thomas *Myhr*, Regulating a European eID, A preliminary study on a regulatory framework for entity authentication and a pan European Electronic ID for the Porvoo e-ID Group, 31 January 2005.

Ks. myös suunnitelma Utbredelse av PKI-anveldelser i offentlig sektor. Strategivalg. 17.2.2005.

9.8 Tietoturva ja sähköiset palvelut aineellisessa lainsäädännössä

9.8.1 Pankkitoiminta ja rahanpesu

Norjan rahoitusalan valvontaviranomainen Kredittilsynet antoi viimeksi vuonna 2003 toimiohjeen[133] informaatio- ja kommunikaatioteknologian käytöstä. Toimiohjeessa on määräyksiä mm. riskinkartoituksesta, turvallisuudesta, katastrofivalmiuden ylläpitämisestä ja toiminnan ulkoistamisesta. Määräykset ovat yleisellä tasolla. Esimerkiksi turvallisuuden osalta todetaan, että yrityksen on luotava menettelytapoja, joilla turvataan yrityksen toiminnan kannalta merkityksellinen laitteisto, ohjelmat ja tiedot vahinkoja, väärinkäyttöä, luvatonta pääsyä ja tiedon muuttamista ja tuhoamista vastaan. Tämän lisäksi menettelytapojen on sisällettävä ohjeita informaatiojärjestelmiin pääsystä. Toimiohjeessa todetaan, että tietosuojalakiin liittyvässä asetuksessa nro 1265 (15.12.2000) määriteltyjen henkilötietojen suojelua koskevien tietoturvaohjeiden täyttäminen on riittävä toimiohjeessa olevan vaatimuksen kannalta.

Norja on pannut täytäntöön EU:n 1. ja 2. rahanpesudirektiivit ja valmistelee nyt kolmannen rahanpesudirektiivin täytäntöönpanoa. Direktiiveissä on vaatimukset asiakkaan tunnistamisesta.

9.8.2 Hankintalainsäädäntö ja verkkolaskutus

Norja on myös pannut täytäntöön julkisia hankintoja koskevat EU-direktiivit vuoden 2006 alusta voimaan tulleella lailla. Samalla myös sähköinen hankintatoimi on tulossa pitkälti mahdolliseksi. Norjassa ei ole asetettu tarjouksille sähköisiä allekirjoituksia koskevia vaatimuksia. Norjassa tullaan sähköiseen hankintatoimeen panostamaan, mikä saattaa johtaa sääntelyn kehittämiseen.

Myös Norjassa on verkkolaskutus yleistynyt huomattavasti. Toisin kuin Tanskassa, ei verkkolaskutus ole kuitenkaan pakollista julkisen sektorin kanssa käytävässä kaupassa eikä verkkolaskutuksesta ole erillistä lakia. Tällaista on kuitenkin Norjassakin pohdittu.

Verkkolaskutusta koskevat nykyiset säännöt eivät sisällä nimenomaisia teknisiä vaatimuksia.

---

[133] Forskrift om bruk av informasjons- og kommunikasjonsteknologi.

9.9 Tietoturvallisuuteen liittyvät yleiset palvelut

Norjassa voimassa oleva organisaatioiden tietoturvallisuutta sääntelevä sertifiointi-järjestelmä mahdollistaa sertifikaattien myöntämisen BS 7799 standardin (1995) 2. osan mukaisen evaluoinnin jälkeen. Kyse on lähinnä julkisen sektorin tarpeisiin kehitetystä hankkeesta.

Tietoturvallisuuteen liittyviä kansallisia hälytysryhmiä ovat NorCERT, jonka kohde-ryhmänä ovat virastot ja eräät yritykset sekä UniNett CERT, joka on tarkoitettu yliopistojen tietoverkoille.

10. Tanska

10.1 Perustuslainsäännökset

Tanskan vuodelta 1953 peräisin oleva perustuslaki sisältää kaksi yksityisyyden suojaa koskevaa määräystä. Ensinnäkin perustuslain 71 § takaa kansalaisen henkilökohtaisen koskemattomuuden. Tanskan kansalaisen vapautta ei voi riistää poliittisen tai uskonnollisen vakaumuksen vuoksi tai syntyperän johdosta.

Perustuslain 72 § määrää puolestaan kotirauhan loukkaamattomiksi. Kotietsintä, kirjeiden ja muun kirjallisen aineiston takavarikoiminen ja tutkiminen, samoin kuin postin, tietoliikenne- ja puhelinsalaisuuden murtaminen voi tapahtua ainoastaan oikeuden määräyksellä, ellei laissa ole toisin määrätty. Lainkohta soveltuu kaikkeen tietoliikenteeseen ja sähköiseen tietoon.

Kuten edellä olevasta ilmenee, tietosuojaa ei ole Tanskassa määritelty varsinaisesti perusoikeudeksi.

Tanska on Euroopan Unionin ja Euroopan neuvoston jäsen ja se on ottanut lainsäädäntöönsä useita kansainvälisiä sopimuksia tietosuojan ja tietoturvan alalla, Grönlannilla on itsehallinto ja lainsäädännön ulottuvuus Grönlantiin ilmoitetaan kunkin lain yhteydessä. Tanskalla on poikkeuksia Maastrichtin sopimuksesta liittyen Schengen-sopimukseen.

10.2 Tietoturvan sääntely ja kehittäminen

Tanskassakaan ei ole nimenomaista tietoturvalainsäädäntöä, vaan tietoturvaa koskevat määräykset löytyvät eri laeista.

Kuitenkin maan hallitus on monien muiden maiden tavoin tiedostanut tietoturvan tärkeyden. Maan tiedeministeriö on perustanut viimeksi vuoden 2006 alusta toimintansa aloittaneen Tietoturvallisuuspaneelin. Paneelin tarkoituksena on vahvistaa yleistä tietoturvallisuutta ja sen 17 jäsentä edustavat laajasti tanskalaista yhteiskuntaa sekä julkiselta että yksityiseltä sektorilta. Tietoturvallisuuspaneelin lisäksi hallituksen toimintaa sektorilla on maan teknologia neuvoston kannustama yleinen tieto-turvallisuuskeskustelu sekä maan tietotekniikka- ja telehallituksen yhteyteen perustettu tietoturvavirasto.

10.3 Erityispiirteitä viranomaistoiminnasta

Terrorismin torjunta on ollut Tanskassa lainsäätäjän huomion kohteena viime vuosina erityisesti vuoden 2001 syyskuun 11. päivän sekä vuonna 2005 Lontoossa tapahtuneiden pommi-iskujen jälkeen. Viranomaisten valtuuksia viestinnän valvontaan ja mm. kameravalvontaan on lisätty.

Tanskan oikeusprosessilain (**retspjeloven**) 71 luku käsittelee viestintäsalaisuuteen puuttumista pakkokeinoin. Tämä edellyttää oikeuden lupaa. Lain 786 §:n mukaan televerkko- ja telepalveluoperaattorien on avustettava viranomaisia rikostutkinnassa tallettamalla teleliikennettä koskevat tiedot vuoden ajan. Määräyksen soveltamisesta on antanut tarkempia määräyksiä maan tiedeministeriö. Vaatimus on koskenut tämän mukaan pienempiä Internet-palveluntarjoajiakin. Kuten muissakin EU-maissa, joudutaan Tanskassakin panemaan täytäntöön EU:n teletietojen tallettamista koskeva direktiivi 2006/24/EY, mutta tällainen velvollisuus on siis ollut olemassa jo kansalliselta pohjalta.

Vuonna 2004 hyväksytyllä lailla[134] lisättiin Tanskan rikoslakiin ja eräisiin muihin lakeihin tietotekniikkarikollisuutta koskevia kriminalisointeja koskien mm. salauksen murtamista, väärää sähköistä rahaa ja sähköisen asiakirjan väärentämistä. Lailla pannaan täytäntöön Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus sekä EU:n neuvoston puitepäätös tietojärjestelmiä vastaan suunnatuista hyökkäyksistä. Lailla annettiin poliisille oikeus määrätä tietoliikennepalvelujen tarjoajat säilyttämään sähköistä viestintää koskevat tiedot, mukaan lukien jopa viestinnän sisällön kopioimisen, korkeintaan 90 päivän ajan.

Kesäkuussa 2006 hyväksytyllä lailla[135] lisättiin Tanskan tiedusteluviranomaisten valtuuksia saada tietoja muilta viranomaisilta.

---

[134] Lov om ændring af straffeloven, retsplejeloven, markedsføringsloven og ophavsretsloven (It-kriminalitet m.v.) LOV nr 352 af 19/05/2004 (Gældende).

[135] Lov om ændring af straffeloven, retsplejeloven og forskellige andre love (Styrkelse af indsatsen for at bekæmpe terrorisme m.v.) LOV nr 542 af 08/06/2006 (Gældende).

10.4 Tiedon julkisuus ja salassapito

10.4.1 Viranomaistiedon julkisuus

Tanskalla, kuten muillakin Pohjoismailla, on pitkä historia viranomaistiedon julkisuuden suhteen sillä ensimmäinen tätä koskeva laki säädettiin jo 1865. Nykyinen laki viranomaistoiminnan julkisuudesta[136] on vuodelta 1985. On myös olemassa vuodelta 1992 peräisin oleva laki julkisista asiakirjoista. Julkisuuslaki sallii jokaisen (ei siis ole sidottu kansalaisuuteen) vaatia nähdäkseen hallinnon asiakirjoja. Viranomaisten on vastattava pyyntöön niin pian kuin mahdollista, ja mikäli asiakirjojen toimittaminen viivästyy, on viivästyksen syy ja kesto ilmoitettava.

Julkisuuslakia ei sovelleta tuomioistuimiin eikä lainsäätäjään. Siten rikosprosessiin ja lainvalmisteluun ennen parlamentille esittämistä liittyvät asiakirjat eivät kuulu lain piiriin. Myös sellaisten asiakirjojen, jotka liittyvät valtakunnan turvallisuuteen tai puolustukseen, kansainvälisiin suhteisiin, verotukseen tai julkisen talouden etuihin, voivat myös olla ei-julkisia. Lakia täydennettiin vuonna 2000 poikkeuksella, joka koskee julkisen sektorin työntekijöitä koskevaa tietoa.

Lain soveltamiseen liittyvien erimielisyyksien johdosta voidaan valittaa parlamentin oikeusasiamiehelle, joka voi antaa ei-sitovia suosituksia asiakirjoihin tutustumisen sallimiseksi. Tanskan hallitus on käynnistänyt lain uudistustyön, jossa otetaan huomioon myös informaatioteknologian vaikutukset. Direktiivi 2003/98/EY viranomaistiedon uudelleenkäytöstä on myös implementoitu Tanskassa.

10.4.2 Yrityssalaisuuksien suoja

Tanskan markkinointilaki[137] sääntelee yrityssalaisuuksien suojaa. Lain 19 §:n mukaan henkilö, joka on palvelusuhteessa yritykseen tai toimii yhteistyössä sen kanssa tai joka suorittaa tehtävää yrityksen lukuun ei saa hankkia tai yrittää hankkia tietoonsa tai haltuunsa kyseisen yrityksen yrityssalaisuuksia luvattomasti.

Jos edellä mainittu henkilö on hankkinut yrityssalaisuudesta laillisesti, hän ei saa luovuttaa ilman asianmukaista lupaa tai käyttää yrityssalaisuutta. Kielto on voimassa kolme vuotta palvelusuhteen, yhteistyön tai tehtävän päättymisestä. Näitä sääntöjä sovelletaan samalla tavoin muuhun henkilöön, jolla on laillinen ´pääsy yritystietoon.

---

[136] Lov nr 572 af 19 desember 1985 om offentlighet i forvaltning.

[137] Maerkedsfoeringsloven 1389, 21.12.2005.

Vastaavasti henkilö, jolle on työtehtävän tai muun kaupallisen syyn vuoksi uskottu teknisiä piirustuksia, eritelmiä, kaavoja, malleja tai vastaavia salaisia asiakirjoja ei saa käyttää hyväkseen mainittua materiaalia tai saattaa materiaalia muiden käytettäväksi ilman lupaa.

Kaupankäynnissä ei saa käyttää liikesalaisuutta, jos siitä on saatu tieto vastoin edellä mainittuja periaatteita.

Lain rikkomisesta seuraavista vahingonkorvaussanktioista säädetään lain 20 §:ssä. Lain vastainen toiminta voidaan kieltää oikeuden päätöksellä. Kiellon turvaksi voidaan antaa oikeuden määräyksiä. Lainkohdassa todetaan, että jokainen, joka loukkaa toisen oikeutta tai käyttää hyväkseen toisen oikeuksia lain säännösten vastaisesti, on maksettava tälle kohtuulliseksi katsottava vahingonkorvaus. Lain 30 § sisältää puolestaan rangaistus-seuraamuksen. Sen mukaan lain 19 §:n määräysten rikkomisesta rangaistaan sakolla tai vankeudella enintään kahdeksaksitoista kuukaudeksi, ellei Tanskan rikoslain 299 §:ssä ole säädetty ankarampaa rangaistusta. Kyseinen lainkohta koskee uhkapeliä.

10.5 Tietosuojasäännökset

10.5.1 Yleiset tietosuojasäännökset

Tanskan tietosuojalaki[138] on vuodelta 2000. Tällä lailla on pantu täytäntöön EU:n henkilötietodirektiivi. Laki sisältää myös direktiivin mukaiset tietoturvallisuutta koskevat määräykset, joita maan tietosuojaviranomainen **Datatilsynet** on täsmentänyt ohjeistuksellaan.[139]

Sähköisen viestinnän tietosuojamääräykset sisältyvät telelainsäädännön[140] vuoden 2003 muutoksiin, jolla direktiivi 2002/58/EY saatettiin osaksi Tanskan oikeutta.[141] Telelainsäädännön valvontaviranomaisena on **IT- og Telestyrelsen**.

Tanskan markkinointilaki[142] sisältää myös tietosuojaa koskevia määräyksiä. Lain 6 §:ään on otettu määräys nimetyille asiakkaille tarkoitetuista ei-toivotusta viestinnästä.

---

[138] Lov om behandling af personoplysningar nr 429, 31.5.2000.

[139] sikkerhetsvejledning (Vejl. nr 37 af. 2. april 2001) 16/4/2001.

[140] Lov om konkurrence- og forbrugerforhold på telemarkedet Lov nr. 418 af 31. maj 2000.

[141] Lov om ændring af lov om konkurrence- og forbrugerforhold på telemarkedet med flere love Nr. 450 af 10. juni 2003.

[142] Maerkedsfoeringsloven 1389, 21.12.2005.

Elinkeinonharjoittaja, joka on saanut asiakkaan yhteystiedot, voi markkinoida tälle tuotteitaan, ellei tämä ole nimenomaisesti kieltänyt markkinointia (ns. soft opt-in-vaihtoehto).

Työelämää ja yksityisyyttä säännellään myös henkilötietolain pohjalta eikä Tanskassa ole siten erillistä työelämän tietosuojalakia. Maan viranomaiset eivät ole ottaneet erityisen jyrkkää kantaa yksityisyyden suojaamiseksi työelämässä. Tanskan tietosuoja-laki tarjoaa työnantajalle mahdollisuuden kerätä ja jopa paljastaa henkilötietoja ilman työntekijän suostumusta, milloin tämä on välttämätöntä oikeudellisen velvoitteen täyttämiseksi, suorittaa yhteiskunnan kannalta merkityksellinen tehtävä tai täyttää laillinen tarve, joka menee työtekijän edun edelle. Työnantaja ei kuitenkaan voi, ilman työntekijän suostumusta, käsitellä tietoja rodullisesta tai etnisestä alkuperästä, uskonnollisesta tai filosofisesta vakaumuksesta, terveydestä tai sukupuolielämästä, ellei tällainen tieto ole tarpeen oikeudellisen vaatimuksen tekemiseksi tai torjumiseksi. Tietoa ammattiliittoon kuulumisesta voidaan myös käsitellä, milloin tämä on tarpeen työnantajan työlainsäädännössä määriteltyjen oikeuksien tai velvollisuuksien täyttämiseksi.

Tietosuojaa koskevaa sääntelyä on lukuisissa erityislaeissa, kuten potilastietoja ja luottokortteja koskevissa laeissa.

10.5.2 Kameravalvonta

Yleistä kameravalvontaa Tanskassa sääntelee erillinen laki[143]. Sen mukaan yritykset eivät saa tarkkailla suljetulla TV-järjestelmällä tai videovalvonnan avulla yleistä aluetta, jota käytetään tavanomaiseen liikenteeseen. Eräät sensitiiviset kohteet on rajattu pois kiellon piiristä. Kieltoa ei sovelleta huoltoasemiin, tehdaslaitoksiin, katettuihin ostoskeskuksiin, käteisautomaatteihin jne. Lisäksi lain mukaan televisiovalvonta on mahdollista yksityisten sisäänkäyntien, julkisivujen tai aitojen kohdalla, jos valvonta ei sisällä kuvien tallentamista.

Kameravalvonnan käytöstä yksityisissä tiloissa, joihin yleisöllä on pääsy, samoin kuin työpaikoilla, on tiedotettava kyltein tai muulla tavoin. Myös julkisen viranomaisen on tiedotettava kameravalvonnasta.

Julkinen tai yksityinen työnantaja voi valvoa työpaikkatiloja TV-kameralla, jos hän ilmoittaa tästä työntekijöille. Ilmoitus voidaan tehdä kyltein tai muulla selvällä tavalla, kuten toimittamalla työntekijöille kirjallinen ilmoitus valvonnasta. Valvonnalla täytyy olla

[143] lov om forbud mod tv-overvågning mv., jf. lov nr. 278 af 9. juni 1982.

kuitenkin objektiivisesti hyväksyttävä tarkoitus. Tällaisia ovat turvallisuusnäkökohdat tai väärinkäytösten estäminen. Tietosuojasäännösten mukaan taas valvonnassa syntynyt aineisto on pidettävä asiattomien ulottumattomissa ja sitä saa säilyttää vain niin kauan kuin työnantajalla on intressi säilyttää se.

Tanskan rikoslaki kieltää nimenomaisesti kameravalvonnan intimiteetin kannalta tärkeissä paikoissa, kuten suihkutiloissa.

Laki ei sisällä määräyksiä äänittämisestä, johon sovelletaan yleisiä tietosuoja-määräyksiä.

Kameravalvonnan osalta on olemassa tuomioistuinten ja viranomaisten ratkaisuja. Maan tietosuojaviranomainen on esimerkiksi katsonut, ettei ravintolaan asennetun web-kameran kuvaamaa aineistoa saa julkistaa Internetissä. Kameravalvontalain ja tietosuojalain suhde on aiheuttanut ongelmia, minkä vuoksi Tanskan oikeusministeriö on asettanut työryhmän pohtimaan asiaa.

10.6 Sähköisten palvelujen tuottaminen

EU:n sähkökauppadirektiivi on pantu täytäntöön erityislailla[144]. Laki toistaa, kuten muissakin EU-maissa voimaan pantu lainsäädännössä direktiivin keskeiset määräykset. Lakiin ei ole otettu määräystä sähköisen sopimustoiminnan sallimisesta. Myös etämyyntidirektiivi ja rahoituspalvelujen etämyyntidirektiivi on pantu toimeen

Sähköistä viestintää eli tietoliikennepalveluja on säännelty myös tietoliikenteen vapauttamispaketin yhteydessä vuosina 2003 ja 2004.

EU:n tietoyhteiskuntadirektiivi saatettiin osaksi Tanskan tekijänoikeuslakia vuonna 2003 voimaan tulleella lainmuutoksella.[145]

Sähköisistä ja muista maksuvälineistä säädetään maksuvälineitä koskevassa laissa.[146] Laki sääntelee nimetyille henkilöille annettuja käteis- ja maksukortteja, mukaan lukien prepaid-kortit. Se sääntelee muita nimetyille haltijoille osoitettuja fyysisiä tunnistamis-keinoja, ja jotka on tarkoitettu sähköisesti luettaviksi. Samoin se sääntelee koodeja ja

---

[144] Lov om tjenester i informationssamfundet, herunder visse aspekter af elektronisk handel LOV nr 227 af 22/04/2002 (Gældende).

[145] Lov om ophavsret, muutos lovbekendtgørelse nr 164 af 12/3/2003.

[146] Lov om visse betalingsmidler, muutos LBK nr 1501 af 20/12/2004 (Gældende).

biometrisiä tunnisteita, jotka on tarkoitettu henkilön tunnistamiseen sekä sähköisesti rekisteröityjä maksuvaatimuksia. Lain yleislauseke (4 § 2) toteaa, että maksujärjestelmä täytyy suunnitella tavalla, että käyttäjät voivat luottaa avoimuuteen, vapaaehtoisuuteen, turvaan väärinkäytöksiä vastaan sekä maksutapahtuman luottamuksellisuuteen.

Tanskassa tuli kesäkuussa 2005 voimaan uusi laki[147] verkkotunnuksista, joka sääntelee ”.dk”-loppuisten verkkotunnusten käyttöä. Tunnuksen myöntää **IT- og Telestyrelsen**. Aikaisemmin kyseisen verkkotunnuksen sääntely on perustunut itsesääntelyyn.

Sähköisistä viranomaispalveluista ei ole säädetty erillistä lakia, mutta avoimuutta koskevien määräysten täydentämistä on selvitetty lainvalmistelussa. Erikoista Tanskalle on, että sähköistä asiointia viranomaisen kanssa edistetään pakolla. Esimerkiksi julkiselle viranomaiselle menevät laskut on toimitettava sähköisesti (ks. jäljempänä). Tanska onkin tällä vuosikymmenellä toteuttanut systemaattisia toimia sähköiseen hallintoon (e-government) siirtymiseksi. Helmikuun 1. päivänä 2005 katsottiin kaikkien Tanskan virastojen voivan kommunikoida sähköisesti myös luottamuksellisen tiedon osalta, ja niinpä virastot voivat lähettää toisilleen kaikkea aineistoa sähköisesti.[148]

10.7 Sähköiset allekirjoitukset ja tunnistaminen

Tanskan laki[149] sähköisistä allekirjoituksista perustuu EU-direktiiviin 2000/31/EY. Tanskassa ei kuitenkaan ole laatuvarmentajia, joten monien lain määräysten soveltaminen on jäänyt teoriaksi. Maan hallitus on kiinnostunut edistämän sähköistä asiointia vaihtoehtoisella tavalla.

Teknisesti Tanska toimii samalla tavoin kuin monet muut maat. Kansalaiset saavat hallitukselta älykortin, jossa on digitaalinen ohjelmistovarmenne.[150] Juridisesti valtio ei tarjoa sähköistä identiteettiä eli kyse ei ole muodollisesti sähköisestä ID-kortista, vaikka kaikki Tanskan kansalaiset saavat henkilökohtaisen väestön keskusrekisterinumeron

---

[147] Lov om internetdomæner nr. 598 af 16/06/2006Gældende)

[148] Ks. asiakirja The Danish eGovernment Strategy 2004-06 - realising the potential

[149] Lov om elektroniske signaturer nr. 417/2000 Lakia täydentävät hallinnolliset määräykset nro 923/2000 turvallisuusvaatimuksista varmennepalveluja tarjoaville organisaatioille, joka tuli voimaan 16.10.2000, ja nro 922/2000 koskien varmennepalvelujen tarjoajien ja järjestelmän arvioijien raportoitointivelvollisuudesta tietoliikenneviranomaiselle eli *IT- og Telestyrelsenille*, joka tuli voimaan 16.10.2000.

[150] Varmenne on tyyppiä X.509.

(CPR), vaan antaa ainoastaan sähköisen allekirjoituksen kansalaisille edistääkseen käyttäjien tunnistamista julkisella sektorilla. Järjestelmä muistuttaa hyvin paljon sellaisia maita, esimerkiksi Suomea ja Viroa, jossa valtiovalta on järjestänyt PKI-pohjaisen, sähköiseen identiteettiin pohjautuvan kansalaisvarmenteen kansalaisten käyttöön.

Varmennetta voidaan käyttää mm. verohallinnon kanssa. Vuona 2005 kansalaisilla oli käytössään yhteensä 88 palvelua ja yhteensä 382 organisaation kanssa saattoi käyttää sähköistä allekirjoitusta. Kansalaisella on valittavanaan joko tunnusluvun tai sähköisen allekirjoituksen käyttö. Myös salaustoiminto on käytettävissä.

Tanskan maahanmuuttoviranomaisille on myönnetty oikeus vaatia oleskelulupaa vaativilta henkilöiltä DNA-testejä perhesiteiden selvittämiseksi.

10.8 Tietoturva ja sähköiset palvelut aineellisessa lainsäädännössä

10.8.1 Pankkitoiminta ja rahanpesun ehkäiseminen

Tanskan rahoituspalvelulain[151] yleislausekkeen tyyppinen 15 § vaatii rahoituspalveluja tarjoavan yrityksen ylläpitämään riittäviä valvonta- ja turvamekanismeja tietotekniikan hyväksikäytössä. Tanskan rahoitustarkastus on ohjeistanut tämän määräyksen noudattamista ja ottanut kantaa mm. ulkoistamiskysymyksiin kieltämällä pääsääntöisesti valvontafunktion ulkoistamisen.[152]

Tanskassa hyväksyttiin helmikuussa uusi laki rahanpesun ja terrorismin rahoituksen ehkäisemisestä[153]. Säädöksen taustalla on EU:n kolmas rahanpesudirektiivi ja se asettaa toimijoille kiristyneet vaatimukset tunnistamisen suhteen. Tanska on, kuten edellä on todettu.

10.8.2 Hankintalainsäädäntö ja verkkolaskutus

Myös Tanskassa on implementoitu EU:n uudet hankintadirektiivit, joissa sähköinen hankintatoimi on mahdollistettu. Tanskassa on jo ennen uusia direktiivejä ollut tapana saattaa direktiivit voimaan sellaisenaan ainoastaan hallituksen määräystä apuna

---

[151] Lov om finansiel virksomhed, LOV nr 501 af 07/06/2001.

[152] Vejledning af 20.2.2003 om kontrol- og sikringsforanstaltninger på it-området (it-leverandørers overholdelse af finansielle virksomheders it-sikkerhedspolitik).

[153] Lov om forebyggende foranstaltninger mod hvidvask af udbytte og finansiering af terrorisme LOV nr 117 af 27/02/2006 (Gældende).

käyttäen. Niinpä hallituksen määräyksellä nro 937, joka annettiin 16.9.2004, saatettiin tavarahankintoja, palveluita ja rakennusurakoita koskeva direktiivi 2004/18/EY osaksi Tanskan lakia, sama tehtiin erityisalojen direktiivin 2004/17/EY kohdalla hallituksen määräyksellä nro 936. Direktiivien teksti on määräysten liitteenä. EU-direktiivien kynnysarvon alittavia rakennusurakoita varten on oma lakinsa. Tanska ei ottanut käyttöön direktiivin sallimia sähköisiä huutokauppoja. Koska direktiivien teksti muodostaa suoraan lain, ei Tanskassa otettu käyttöön sähköisten allekirjoitusten käyttöä koskevia vaatimuksia tarjouksille.

Tanska on ensimmäisenä maana säätänyt velvollisuuden laskuttaa julkisia organisaatioita vain sähköisesti. Tätä koskeva laki[154] tuli voimaan 1. helmikuuta 2005 ja koskee valtiota ja sen virastoja sekä kuntia. Tanska on valinnut julkiseksi tietoliikenne-standardiksi OIOXML:n, joka perustuu UBL-standardiin. UBL (*Universal Business Language*) on ajateltu sillaksi monien olemassa olevien standardien kuten EDIFACT:in käyttäjien välillä. Se on puolestapuhujiensa mukaan kansainvälinen ja riittävän huokea myös pienille yrityksille.

Verkkolaskua lähetettäessä on noudatettava voimassaolevaa lainsäädäntöä, erityisesti tietosuojalakia. Vastuu kanavoituu tässä suhteessa lähettäjälle. Verkkolaskun käytölle ei Tanskassa ole asetettu teknisiä muotovaatimuksia, kuten sähköisen allekirjoituksen käyttö.

10.9 Tietoturvallisuuteen liittyvät yleiset palvelut

Tanskan hallitus päätti vuonna 2004, että Tanskan valtion laitosten on noudatettava yhteistä valtion tietoturvastandardia kolmevuotisen siirtymäjakson jälkeen eli vuoden 2007 alusta. Maan tiedeministeriö on asettanut tätä varten apuohjelman, joka koostuu useista implementointia tukevista toiminnoista. Standardi on kansallisesti laadittu.

Tanskassa toimii DK-CERT-niminen Computer Emergency Response Team, joka yhdessä muiden kansallisten elinten kanssa on tarkkailla tietoturvariskejä, vastaanottaa niitä koskevia ilmoituksia ja julkaista varoituksia yleisistä tietoturvauhkista kuten viruksista. DK-CERT:in kotisivuilla on runsaasti tietoturvallisuuteen liittyvää ohjeistusta ja säännöstöjä. Muita vastaavia toimintoja ovat CSIRT.DK, joka on tarkoitettu operaattori TDC:n asiakkaille ja KMD IAC, joka on tarkoitettu KMD:n asiakkaille ja paikallisviranomaisille.

---

[154] Lov om offentlige betalinger m.v. (Lov nr. 1203 af 27/12 2003).

11. Saksa

11.1 Perustuslainsäännökset

Saksan liittotasavallan perustuslaki (Grundgesetz) on vuodelta 1949, ja sitä on viimeksi muutettu Saksojen jälleenyhdistymisen yhteydessä 1990. Perustuslain 10 artiklassa turvataan kirje- ja tietoliikennesalaisuus ja poikkeuksia tästä voidaan tehdä ainoastaan lainsäännöksin. Silloin kun rajoituksen tarkoituksena on demokraattisen yhteiskunta-järjestelmän tai liittovaltion turvallisuuden turvaaminen, lainsäädännössä voidaan määrätä, ettei kajoamisen kohteeksi joutunut henkilö saa tietää toimenpiteestä, ja tuomioistuimien asemesta oikeusturvatienä toimivat liittopäivien nimeämät elimet.

Liittotasavallan perustuslakiin esitettiin sisällytettäväksi oikeutta tietosuojaan koskevaa määräystä Saksojen yhdistymisen yhteydessä, mutta tuolloin hallinnut poliittinen koalitio ei ehdotusta niellyt.

Oikeus tietosuojaan on kuitenkin kehittynyt oikeuskäytännön myötä. Vuonna 1983 ratkaistussa oikeustapauksessa, joka koski väestönlaskentalainsäädäntöä, liittovaltion perustuslakituomioistuin muodollisesti tunnusti yksilön oikeuden ”tiedolliseen itsemääräämisoikeuteen”, jota rajoittaa ainoastaan ”merkittävä julkinen intressi”. Tiedollinen itsemääräämisoikeus johdettiin perustuslain 1. ja 2. artikloista, jotka turvaavat ihmisarvoa ja yksilönvapautta ja yksilön koskemattomuutta (Persönlichkeitrecht).

11.2 Tietoturvan sääntely ja kehittäminen

Saksassakaan ei ole nimenomaista tietoturvalainsäädäntöä, vaan tietoturvaa koskevat määräykset ovat hajallaan eri puolilla lainsäädäntöä.

Kuten monissa muissa maissa, Saksassakin pidetään tietoyhteiskunnan kehittämistä keskeisenä haasteena. Liittovaltion hallitus antoi maaliskuussa 2006 maan talous- ja teknologiaministeriölle tehtäväksi laatia maalle strategia ”**Information Society Germany 2010**”. Vaikka pääpaino on tietotekniikan hyödyntäminen kaupallisesti ja hallinnollisesti, mainitaan asiakirjassa myös tietoturvallisuuden merkitys keskeisenä painopistealueena.

Saksassa on nimenomaan tietoturvallisuuskysymyksiä varten organisoitu valtion virasto **Bundesamt für Sicherheit in der Informationsteknik** (BSI).

11.3 Erityispiirteitä viranomaistoiminnassa

Perustuslain turvaamasta tietoliikennesalaisuudesta säädetään tarkemmin tietoliikennelain eli *Telekommunikationsgesetzin* 85 §:ssä. Telesalaisuus ulottuu myös yhteydenottoyrityksiin. Tietoliikennelain 86 §:ssä säädetään telekuuntelun kiellosta sekä vastaanottolaitteiden ylläpitäjän salassapitovelvollisuudesta. Vastaavasti lain 87 §:ssä säädetään ammattimaisessa tarkoituksessa tietoliikennelaitteita ylläpitävän henkilön velvollisuudesta ylläpitää teknisiä suojakeinoja mm. telesalaisuuden ylläpitämiseksi. Pakkokeinoista, myös tietoliikennettä koskevista, säädetään rikosprosessijärjestyksessä eli *Strafprozessordnungissa* (StPO). Sen määräyksiä ei tässä käydä tarkemmin läpi. Seuraavassa kuitenkin joukko keinoja, joilla Saksassa on pyritty vastaamaan mm. terrorismin uhkaan kuluneiden vuosien aikana.

Poliisin toiminnan kannalta keskeinen laki on ns. G-10-laki[155], joka asettaa rajoituksia joidenkin tietojen luottamuksellisuudelle.

G-10-lakia täydennettiin vuonna 2001 määräyksillä, jotka antavat poliisiviranomaisille oikeuden valvoa dataa sekä puhelimia. Lisäksi vuonna 2001 Saksan lainsäätäjä velvoitti kiinteän ja langattoman liittymän ylläpitäjien asentamaan, ainakin väliaikaisesti, laitteita, joka antaa poliisille ja turvallisuusviranomaisille pääsyn pääosaan saksalaisesta tiedonvälityksestä.[156] Säännökset eivät koske Internet-palveluntarjoajia.

G-10-laki sääntelee myös puhelinkuuntelua rikosten torjumiseksi tai selvittämiseksi, mikä vaatii oikeuden määräystä. Vuonna 1994 säädetyn G-10-lain muutosasetuksen perusteella maan turvallisuuspalvelulla BND:llä on oikeus kansainvälisten tietoliikenneyhteyksien pysyvään telekuunteluun terrorismin, huumekaupan tai laittoman asekaupan ehkäisemiseksi. Vuonna 1999 Saksan perustuslakituomioistuin päätti, että samaa lainsäädäntöä voidaan soveltaa myös poliittisten järjestöjen valvontaan, jos järjestöt ovat perustuslainvastaisia eikä tietoa niiden toiminnasta ole saatavissa julkista tietä.

Vuonna 2001 liittopäivät hyväksyivät myös lain, jolla poliisille ja muille täytäntöönpanoviranomaisille taattiin pääsy tietoliikenteen yhteystietoihin eli teletunnistetietoihin vakavien rikosten tutkimiseksi. Tämä mahdollisuus täydentää lain tarjoamia salakuuntelumahdollisuuksia. Lain mukaan tietoliikenneoperaattorien on luovutettava edellä mainituille viranomaisille mm. puhelujen aikaa ja kestoa, yhteysnumerot sekä

---

[155] Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses eli Gezetz zu Artikel 10 Grundgesetzes.

[156] Telekommunikations-überwachungsverordnung TKÜV, 22.1.2002.

käyttöpaikka. Tässä laissa on kuitenkin ns. sunset-lauseke eli se arvioidaan uudestaan vuoden 2007 alussa.

Saksaan säädettiin vuosikymmenen alussa antiterrorismilaki[157] joka tuli voimaan vuoden 2002 alusta. Lailla luotiin mm. oikeudellinen perusta biometrisille passeille ja henkilöllisyystodistuksille, tehostettiin viranomaisten välistä tiedonvaihtoa, annettiin turvallisuuspalvelu BND:lle oikeus saada tietoa Internet-palveluntarjoajilta, lentoyhtiöiltä ja matkatoimistoilta ja luotiin mahdollisuus puhetietokannan luomiseen sen varalta, että turvapaikkahakemuksen tekijät tunnistettaisiin äänen perusteella. Vuonna 2002 Saksan sisäministeriö julkaisi suunnitelman, jonka mukaan terrorismin vastainen taistelu johtaisi salauksen sisältävien biometristen henkilökorttien käyttöönottoon, samoin kuin sormenjälkien ja kasvontunnisteiden käyttöön. Nämä pyrkimykset jäivät kuitenkin odottamaan EU:n toimia biometrian soveltamiseksi passeissa.

Biometrisiin ominaisuuksiin kuuluu myös ihmisen geneettinen rakenne eli DNA. Saksan tietosuojaviranomaiset ovat katsoneet tärkeäksi säännellä DNA:n käyttöä väärinkäytön estämiseksi. Sen vuoksi ketään ei tulisi pakottaa geneettisiin testeihin. Geneettisen aineiston käyttö vastoin suostumusta tulisi kriminalisoida. Vaikka tämän perusteella ei ole syntynyt lainsäädäntöä, kertovat näkemykset saksalaisesta keskustelusta ajankohtaisten tunnistamiseen liittyvien ilmiöiden tiimoilta.

Vuonna 2002 säädettiin laki, jolla mahdollistettiin ns. IMSI-Catcherin käyttö liittyen henkilön paikannukseen matkapuhelimen sijainnin avulla. Viranomaisilla on oikeus saada tuomioistuimelta määräys, jonka avulla saadaan tieto henkilön puhelimen numerosta ja hänen olinpaikoistaan kuuden kuukauden ajan. Laki on osa StPO:n pakkokeinomääräyksiä.

11.4 Tiedon julkisuus ja salassapito

11.4.1 Viranomaistiedon julkisuus

Saksa oli pitkään ilman viranomaistiedon julkisuutta koskevaa yleistä lainsäädäntöä. Asiassa on tapahtunut kuitenkin äskettäin muutos, sillä julkisen tiedon osalta on säädetty äskettäin uusi viranomaistiedon julkisuutta sääntelevä laki eli *Informationsfreiheitsgesetz*, joka tuli voimaan vuoden 2006 alusta. Erityissääntelyä oli kuitenkin olemassa rekisterien ja arkistojen osalta sekä asianosaisasemassa olevien henkilöiden kohdalla. Yleinen tiedonsaantioikeus vallitsi vain ympäristötiedon osalta.

---

[157] Terrorismbekämfungsgesetz BGBI, 2002, I.

Saksassa käytiin tätä ennen keskustelua siitä, kuinka pitkälle virkasalaisuus ja tietosuoja voivat rajoittaa kansalaisen tiedonsaantioikeutta viranomaistoiminnasta.

Vaikka laki takaakin kansalaisille yleisen pääsyn viranomaistietoon, sisältää se useita merkittäviä poikkeuksia, joita tiedonvapauden puolestapuhujat ovat kritisoineet. Poikkeukset ovat voimassa silloin, kun tiedon julkistaminen vaarantaisi yleisen tai kansallisen turvallisuuden tai haittaisi kansainvälisiä suhteita. Poikkeus tehdään myös rahoitus- tai kilpailuasioita käsittelevien viranomaisten samoin kuin muiden viranomaisten kohdalla, jotka suojaavat liittovaltion fiskaalisia etuja.

Kun kyse on luottamuksellisesta liiketiedosta tai teollisoikeuksista, laki vaatii, että asianomainen yritys antaa suostumuksensa ennen kuin viranomaiset voivat julkistaa tällaista tietoa. Jos taas kyse on henkilökohtaisesta tiedosta, tietoa säilyttävän viranomaisen on ratkaistava, onko tietoa pyytävän vai tiedon kohteena olevan henkilön intressit tärkeämmät silloin kun päättää annetaanko pyytäjälle pääsy tietoon vai ei.

11.4.2 Yrityssalaisuuksien suoja

Yrityssalaisuuksien suojasta säädetään Saksassa vilpillistä kilpailua koskevan lain 17 §:ssä. Yrityssalaisuuden piiriin kuuluu kaupallisesti arvokas tieto, joka ei ole julkisesti saatavilla, ja jonka osalta se, jolle tieto kuuluu, on ilmaissut objektiivisen aikomuksen tiedon salassa pitämiseksi.

Lainkohdan 1. momentin mukaan työntekijää, oppisopimuskoulutuksessa olevaa tai muuta henkilöä, joka työsuhteen kuluessa ilmaisee ilman lupaa kolmannelle kauppa- tai teollisuussalaisuuden, joka on uskottu hänelle tai saatettu hänen tietoonsa työsuhteen puitteissa, jos hän tekee paljastuksen kilpailun tai henkilökohtaisen edun vuoksi, hyödyttääkseen kolmatta osapuolta tai vahingoittaakseen elinkeinonharjoittajaa.

Vilpillistä kilpailua koskevan lain 17 §:n 2. momentin mukaan rangaistaan samalla tavalla henkilöä, jotka yllä kuvatuista syistä hankkii luvatta kauppa- tai teollisuussalaisuuden

a) käyttämällä teknisiä keinoja,

b) luomalla salaisuuden sisältävän kopion, tai

c) irrottamalla esineen, johon salaisuus on sisällytetty.

Sama koskee henkilöä, joka käyttää tai ilmaisee toiselle kaupallisen tai teollisen salaisuuden, jonka on hankkinut tai saanut ilman lupaa sen luvatta ilmaisseelta työntekijältä tai oman tai toisen henkilön toiminnan tuloksena. Yritys on rangaistava.

Erityisen vakavissa tapauksissa, korkeintaan viiden vuoden vankeusrangaistus tai sakko voi tulla kyseeseen. Erityisen vakava tapaus on kyseessä silloin, kun tekijä salaisuutta ilmaistessaan tietää, että salaisuutta käytetään vieraassa valtiossa tai hän itse käyttää sitä vieraassa valtiossa.

Vilpillistä kilpailua koskevan lain 18 §:ssä säädetään korkeintaan kahden vuoden vankeusrangaistus tai sakkorangaistus henkilölle, joka kilpailusyistä tai henkilökohtaista hyötyä tavoitellakseen käyttää luvatta tai ilmaisee kolmannelle malleja tai teknisiä ohjeita, erityisesti piirustuksia, prototyyppejä, muotoja, leikkauksia tai reseptejä, jotka on hänelle uskottu liiketoiminnan puitteissa.

Vilpillistä kilpailua koskevan lain 19 §:ssä säädetään lisäksi vahingonkorvausvelvollisuudesta 17 ja 18 §:n mukaisten rikosten perusteella. Mikäli tekijöitä on useita, ovat he vastuussa yhteisvastuullisesti. Myös kolmas osapuoli voi joutua vahingonkorvausvelvolliseksi. Vahinkoa kärsinyt tai muu oikeudenhaltija voi hakea oikeudelta kieltomääräyksen turvakseen.

11.5 Tietosuojasäännökset

11.5.1 Yleiset tietosuojasäännökset

Saksassa on Euroopan Unionin tiukimpia tietosuojalakeja. Maailman ensimmäinen tietosuojalaki säädettiin vuonna 1970 Hessenin osavaltiossa. Saksan nykyinen tietosuojalaki (*Bundesdatenschutzgesetz*) on vuodelta 1990, ja se on viimeksi uudistettu vuonna 2002. Viimeisimmät uudistukset käsittelevät rekisteritietojen siirtoa ulkomaille, kameravalvontaa, anonyymisyyttä ja salanimen käyttöä, älykortteja, arkaluonteisen tiedon keräämistä. Laki antaa rekisteröidyille suuremmat mahdollisuudet vastustaa tiedon käsittelyä. Laki vaatii yrityksien nimeävän tietosuojavastaavan, jos yritys kerää, käsittelee tai käyttää henkilötietoja. Henkilötietoja sisältävät tietokannat on rekisteröitävä tietosuojaviranomaisessa. Rekisteröitävän suostumuksen merkitystä on korostettu.

Saksan osalta on huomattava sen liittovaltioluonne. Siksi osavaltiotasolla on säädetty esimerkiksi omat tietosuojalait ja niillä on omat tietosuojavaltuutettunsa. Kaikissa Saksan 16 osavaltiossa (*Länder*) on omat yksityiskohtaiset tietosuoja-asetukset, jotka kattavat osavaltioiden hallinnon. Osavaltiot ovat lisäksi säätäneet omat tietosuojalakinsa, jotka perustuvat EU-direktiiviin.

Sähköisen viestinnän osalta sisältyvät tietosuojamääräykset vuonna 2004 muutettuun tietoliikennelakiin eli *Telekommunikationsgesetziin*, johon yhdistettiin vuoden 2000 tietoliikennettä koskeva tietosuoja-asetus. Sisällöllisesti ei laki kuitenkaan muuttunut.

Omat tietosuojasäännöksensä sisältyvät myös informaatiopalvelulakiin eli IuKDG:hen[158]. Tämän lain 3 §:n mukaan henkilötietoja voi kerätä vain laissa suoduin valtuuksin tai asianosaisen suostumuksella. Palvelun tarjoamista ei saa tehdä riippuvaksi suostumuksen antamisesta. Suostumuksen antaminen sähköisesti on mahdollista tietyin edellytyksin. Palvelun tarjoamisessa käytettävä laitteisto on suunniteltava niin, että henkilötietojen kerääminen on mahdollisimman vähäistä.

Yksityisyyden kannalta on merkityksellinen 4 §:n määräys, jonka mukaan käyttäjälle on tarjottava oikeus sähköisten palvelujen anonyymiin tai pseudonyymin pohjalta tapahtuvaan käyttöön ja maksamiseen sen mukaan kuin tämä on käytännössä mahdollista. Asiakkaalle on tiedotettava näistä vaihtoehdoista. Palveluntarjoajan on teknisesti varmistuttava, että käyttäjä voi milloin tahansa katkaista yhteyden. Sähköisten palvelujen käyttöön liittyvät tunnistetiedot on hävitettävä, elleivät ne ole tarpeen kirjanpidollisista syistä. Käyttäjää on suojattava siltä, että muut saisivat tiedon sähköisten palvelujen käytöstä. Asiakkaan kunkin telepalvelun käyttö on käsiteltävä erikseen. Yhdistelmän saa luoda vain kirjanpidollisista syistä. Käyttäjälle on annettava tieto palvelun ohjaamisesta toiselle palveluntarjoajalle. Käyttäjäprofiilit sallitaan vain salanimien käytön yhteydessä. Salanimen käyttöön perustuvia tietoja ei saa yhdistää henkilön oikeaan nimeen perustuviin tiedostoihin.

Viranomaiset ovat tukeneet anonyymiä asiointia ja maksamista muutenkin. Vuonna 2001 Saksan liittovaltion talous- ja työministeriö esitteli tietokoneohjelman, jolla kuluttajat voisivat tehdä anonyymejä ostoja ja maksuja Internetissä. Saksassa on todettu, että Internetissä asioivat kuluttajat kantavat huolta yksityissytensä suojasta.

IuKDG:n 5 ja 6 §:ssä säännellään asiakastietojen käsittelyä. Toimittajalla on oikeus koota, käsitellä tai käyttää käyttäjän henkilötietoja tämän kanssa tehtävän sopimuksen laatimiseen tai muuttamiseen. Sopimustietojen käsittely tai käyttö neuvontaa, mainontaa, markkinatutkimusta tai palvelun kysynnän mukaiseksi suunnittelua varten edellyttää kuitenkin käyttäjän nimenomaista suostumusta. Palveluntarjoaja voi kerätä, käsitellä tai käyttää telepalvelujen käyttöä koskevia tietoja vain tarpeen mukaan mahdollistamaan palvelujen käytön (käyttötieto) tai veloittamaan palvelujen käytöstä (laskentatieto). Molempien osalta on yksityiskohtaisia määräyksiä siitä, kuinka pian tiedot on pyyhittävä pois. Tietoja ei myöskään saa luovuttaa edelleen, ellei toimittaja

[158] Ks. tästä kohta XI.6 jäljempänä.

teetä alihankintana laskentapalveluja, jolloin alihankkijan on noudatettava tele-salaisuutta. Telepalveluja koskeva lasku ei saa sisältää yksityiskohtia, jotka paljastavat palvelujen käyttöön liittyviä yksityiskohtaisia tietoja.

IuKDG:ssä on lisäksi määräyksiä käyttäjän tietojaan koskevasta tarkastusoikeudesta sekä sääntöjen noudattamisen valvonnasta. Näissä lainkohdissa on viittaukset liittovaltion tietosuojalakiin eli *Bundesdatenshutzgesetziin*.

Melkein kaikissa Saksan laeissa, jotka sisältävät määräyksiä luonnollisten henkilöiden henkilökohtaisista tiedoista ja niiden käsittelystä, on tietosuojaa koskevia määräyksiä.

Tietosuojan kehittämiseksi on Saksassa esiintynyt kunnianhimoisia pyrkimyksiä. Saksan tietosuojaviranomaiset haluavat lisätä opt-in mahdollisuuksia opt-outin kustannuksella, kehittää mahdollisuutta käyttää Internetiä anonyymisti ja varmistaa se, että henkilötietojen käyttö perustuu suostumukseen. Tietosuojalainsäädännön virtaviivaistamista tavoitellaan.

Saksan tietosuojaviranomainen on liittovaltion tietosuojatoimikunta, **Bundesbeauftragter für den Datenschutz**. Elimen tehtävänä on valitusten vastaanottaminen ja tutkiminen samoin kuin suositusten tekeminen lainsäädäntö- ja muille viranomaisille. Osavaltiotasolla Saksassa on omat tietosuojaviranomaisensa.

Tietoturvaan ja tietosuojaan liittyvänä kysymyksenä on pidetty myös haittaohjelmien ja roskapostin torjumista. Saksassa säädettiin elokuussa 2004 uusi laki vilpittömästä kilpailusta (Gesetz gegen den unlauteren Wettbewerb eli UWB). Lain 7 §:n avulla on pantu täytäntöön EU:n sähköisen viestinnän tietosuojadirektiivi. Direktiivin täytäntöön-panossa on valittu korkein kuluttajansuojan taso. Niinpä sähköpostin, faksin tai puhelimen välityksellä tapahtuva markkinointi edellyttää vastaanottajan suostumusta (opt-in-malli).

11.5.2 Kameravalvonta

Lainsäädäntöä kameravalvonnasta on osavaltiotasolla. Tulkintasyistä johtuen liittovaltiotason tietosuojalaki ei sääntele kameravalvontaa. Osavaltiotason lainsäädäntö sääntelee sekä yksityistä että muiden kuin poliisiviranomaisten suorittamaa kameravalvontaa. Yksityistä kameravalvontaa voidaan harjoittaa mm. asunnon vartioimiseen. Kamera- valvonnan käyttö on tehtävä näkyväksi. Valvonta-materiaalin säilyttäminen vaatii erityisiä syitä, konkreettista vaaraa ja aineiston säilyttämisen välttämättömyyttä tarkoituksen kannalta. Sen jälkeen kun aineisto on muuttunut tarpeettomaksi, se on hävitettävä. Mikäli kameravalvonnan tuloksena

syntyneiden tietojen käsittely on uskottu ulkopuoliselle, on valvonnan kohteita informoitava.

Kameravalvonta on Saksassa joutunut tietosuojan ja yksityisyyden suojan puolesta toimivien järjestöjen mielenkiinnon kohteeksi. Eräs näistä haastoi berliiniläisen kauppakeskuksen, jonka valvontakameran tarkkailukulma ulottui yleiselle kadulle. Videovalvontaan työpaikoilla kohdistuu vaatimuksia erityisesti yhteistoiminta-lainsäädännön taholta.

Vuonna 2002 Saksa päätti ottaa käyttöön sähköisen tiemaksujen keräysjärjestelmän. Ajoneuvoja tarkkaillaan GPS:n (*Global Positionining System*) samoin kuin matkapuhelinverkkojen avulla. Järjestelmän toteuttamiseksi säädettyä lakia täsmennettiin niin, että tietojen keruu ja käsittely on mahdollista ainoastaan laskutusta varten. Tämän jälkeen tiedot on hävitettävä ja samoin tiedot autoista, jotka eivät ole tiemaksujen piirissä, on hävitettävä. Tiemaksujen keruupaikoille on kuitenkin asennettu myös valvontakamerat ulkomaisia autoja varten. Valvontakameran tietoja verrataan keskusrekisterissä oleviin tietoihin. Käyttötarkoituksen rajauksesta huolimatta viranomaiset ovat käyttäneet järjestelmää mm. varastetun kuorma-auton jäljittämiseen.

Radiotaajuustunnisteen eli RFID:n käyttön on liittynyt Saksassa epäluuloja. Vähittäis-kauppaketju Metro otti käyttöön RFID-tarrat käyttöön 2003. Yhdistettynä sähköisesti luettavaan asiakaskorttiin, RFID-teknologia mahdollistaa kaikkien asiakkaan ostojen yhdistämisen hänen henkilöönsä. Vaikka RFID-tarrat voi deaktivoida, pysäytti Metro vuotta myöhemmin kokeilunsa sen jälkeen, kun digitaalisten palvelujen käyttäjäjärjestöt olivat esittäneet protesteja. Protestit olivat yltyneet, kun kävi ilmi, että Metro oli asentanut RFID:hen yhdistettäviä toimintoja asiakaskorttiinsa ilman kuluttajien informoimista. Asia ilmeni sen jälkeen, kun eräs järjestö oli röntgenkuvannut Metron asiakaskortin. Järjestö on sittemmin saanut varoja yleishyödyllisistä rahastoista kehittääkseen laitteen, jolla kuluttaja voisi paljastaa RFID-tunnisteita kuluttajatuotteista. Laitetta on kutsuttu yksityistäjäksi (*privatizer*).

11.6 Sähköisten palvelujen tuottaminen

EU:n sähköistä kaupankäyntiä koskeva direktiivi 2000/31/ETY pantiin Saksassa täytäntöön Elektronischer Geschäftsverkehr-Gesetz (EGG)-nimisellä lailla.[159]

[159] Gesetz über rechtliche Rahmenbedingungen für den Elektronischen Geschäftsverkehr (Elektronischer Geschäftsverkehr-Gesetz (EGG) Bundesgesetzblatt (BGBl) 2001 Teil I Nr. 70 vom 20. Dezember 2001, S. 3721.

Sähköisen viestinnän välityksellä tarjottavien informaatiopalvelujen tarjontaa on jo aikaisemmin säännellyt *Informations- und Kommunikationsdienste-Gesetz* eli IuKDG. Tämä liittovaltion laki on itse asiassa lakipaketti, joka sisältää telepalvelulain (TDG), telepalvelujen tietosuojalain (TDDSG) sekä lain sähköisistä allekirjoituksista (SigG) Tällä lailla luodaan yhtenäiset säännöt sähköisille viestintä- ja kommunikaatio-palveluille, joilla tarkoitetaan muita kuin tietoliikenneyhteyden tarjoamista tarkoittavia palveluja ja olennaisesti toimitukselliseen panokseen perustuvia palveluja. Olennaista on kuitenkin, että palvelua tarjotaan käyttäjän yksilöllisten tiedon- tai sisällöntarpeiden tyydyttämiseksi. Näin esimerkiksi sähköiset pankkipalvelut kuuluvat lain piiriin. TDG:ssä säännellään mm. palveluntarjoajan vastuuta sisällöstä. Edellä mainittu EGG, jolla on pantu täytäntöön EU:n sähkökauppadirektiivi, on eräiltä osin täsmentänyt TDG:tä ja TDDSG:tä.

Sähköistä viestintää sääntelee ns. *Mediendienste-Staatsvertrag* (MdStV) eli Saksan osavaltioiden välinen lainsäädäntösopimus, jolla säännellään mediapalveluita.[160] Mediapalvelut määritellään yleiseen käyttöön tarkoitetuiksi viestintäpalveluiksi erotuksena edellä mainituista telepalveluista. Esimerkiksi kotisivuja pidetään yleensä mediapalveluina, ellei sivun välityksellä muodosteta säännönmukaisesti kontaktia sivun ylläpitäjään, jolloin kyse on telepalvelusta. MdStV:n vastuu- ja tietosuojamääräykset muistuttavat IuKDG:tä. Poikkeuksen muodostaa kuitenkin sopimuksen 17 §, jolla säädetään, että mediapalvelujen tarjoajan on hyväksytettävä tietosuojajärjestelmänsä samoin kuin tekniset ratkaisunsa ulkopuolisella tarkastajalla.

MdStV:tä ollaan korvaamassa varsinaisella liittovaltiolailla eli *Telemediengesetzillä* (TMG). TMG korvaisi telepalvelulain TDG:n, telepalvelujen tietosuojalain TDDSG:n sekä mediapalveluja koskevan osavaltioiden sopimuksen MdStV:n. Sisältö ei muuttuisi kuin tietosuojamääräysten osalta. TMG on toistaiseksi vielä valmisteluasteella.

11.7 Sähköiset allekirjoitukset ja tunnistaminen

Lailla sähköisistä allekirjoituksista 22.5.2001 (*Signaturgesetz, SigG*) on pantu täytäntöön EU:n sähköisiä allekirjoituksia koskeva direktiivi 1999/93/EY. SigG on muodollisesti osa IuKDG:tä, ja lainmuutos 2001 teki SigV:stä velvoittavaa oikeutta eli sähköiset allekirjoitukset on ollut tunnistettava. Aikaisempi laki oli rakentunut, aivan kuten Italiankin varhainen laki, PKI-tekniikkaan perustuvien digitaalisten allekirjoitusten sääntelyä varten ja sisälsi määräyksiä myös aikaleimoista. Lakia täydentää sähköisiä allekirjoituksia koskeva asetus *Signaturverordnung* (SigV).

---

[160] Lisäksi on olemassa osavaltioiden välinen Rundfunkstaatsvertrag, joka sääntelee radio- ja TV-toimintaa.

Viranomaiset ovat pyrkineet edistämään sähköisten allekirjoitusten käyttöä. Vuonna 2002 liittohallitus päätti suunnitelmasta varustaa yli 200.000 liittovaltion viranomaista sirukorteilla, joiden avulla nämä voisivat allekirjoittaa sähköisiä asiakirjoja.

On myös tehty ehdotus kaikille työntekijöille annettavasta älykortista eli työntekijäkortista. Taustalla on ollut ajatus työnantajien kulujen vähentämisestä sosiaaliturvan osalta. Keskitettyyn tietokantaan koottaisiin tietoja nykyisestä työnantajasta, palkasta ja työskentelyajasta. Tietokantaa voisivat käyttää kaikki sosiaaliturvan parissa työskentelevät yksiköt kortinhaltijan suostumuksella. Järjestelmää ei kuitenkaan ole vielä toteutettu.

11.8 Tietoturva ja sähköiset palvelut aineellisessa lainsäädännössä

11.8.1 Pankkitoiminta ja rahanpesu

Saksan pankkitoimintaa koskeva monipuolinen lainsäädäntö säätää muiden maiden tavoin yleisestä riskienhallinnasta. Saksan pankkivalvontaviranomainen **Bundesanstalt für Finanzdienstleistungsaufsicht** täsmentää yleisiä määräyksiä yksityiskohtaisella ohjeistuksellaan (*Richtlinie* tai *Rundschreiben*). Tietosuojaa koskevat kysymykset kuuluvat Saksassa kuitenkin tietosuojaviranomaisille ja kun yleistä tietoturvallisuutta varten on oma virastonsa, ei tietoturvallisuus ole noussut pankkiviranomaisten huomion kohteeksi.

Saksassa on voimassa rahanpesun ehkäisemiseksi EU-direktiiveihin perustuva lainsäädäntö, jota ollaan uusimassa. Keskitetyn valvonnan aikaansaamiseksi pankit on velvoitettu toimittamaan valvontaviranomaiselle tietoja asiakkaistaan. Kyseessä on tieto pankkitileistä ja niiden omistajista, ei esimerkiksi transaktioista tai tileillä olevista varoista. Tieto annetaan muodostamalla sähköinen yhteys viranomaisen tietokantaan. Pankkivalvontaviranomainen voi luovuttaa tilitietoja muulle viranomaiselle erityistä prosessia noudattaen.

11.8.2 Hankintalainsäädäntö ja verkkolaskutus

Saksassa vaaditaan verkkolaskutuksessa laatuvarmenteeseen perustuvaa kehittynyttä sähköistä allekirjoitusta eli ns. kvalifioitua sähköistä allekirjoitusta. Hankintalainsäädännön osalta on kuitenkin tapahtunut muutos sikäli, että sähköisen hankintatoimen osalta on käyty keskustelua vaadittavasta sähköisen allekirjoituksen toteutustavasta. Tähän asti on vaadittu kvalifioidun sähköisen allekirjoituksen käyttöä tarjouksissa, muta nyt ollaan mahdollistamassa kehittyneen sähköisen allekirjoituksen käyttö ilman, että

se perustuisi laatuvarmenteeseen ja olisi luotu turvallisella allekirjoituksen luomismenetelmällä.

Kehittynyt sähköinen allekirjoitus on määritelty sähköisiä allekirjoituksia koskevassa direktiivissä (1999/93/EY) allekirjoitukseksi, joka liittyy yksiselitteisesti allekirjoittajaan niin, että sillä allekirjoittaja voidaan yksilöidä, ja allekirjoitus on luotu menetelmällä, jonka allekirjoittaja pitää yksinomaisessa valvonnassaan ja on liitetty muuhun sähköiseen tietoon siten, että tiedon mahdolliset muutokset voidaan havaita eli tällöin täytetään asiakirjan eheyden vaatimus.

Pitkän aikaa Saksan lainsäädännössä pidettiin kvalifioitua sähköistä allekirjoitusta vaatimuksena sen korkeamman luotettavuuden vuoksi. Myös Saksan teollisuus tuki kvalifioidun sähköisen allekirjoituksen käyttöä. Laatuvarmenteita myönsi usea laatuvarmentaja. Silti laatuvarmenteet eivät saavuttaneet niin laajaa käyttöä kuin oli otaksuttu. Vaikka sähköiselle allekirjoitukselle asetettavia vaatimuksia on lievennetty, ei kaikkia ongelmia ole vielä ratkaistu. Saksassa, kuten koko EU:ssa, on ratkaistava sähköisten allekirjoitusten yhteen toimivuuden ongelma. Jokainen tarjoaja voi käyttää omassa jäsenvaltiossaan hyväksyttyjä sähköisen allekirjoituksen menetelmiä. Vastaanottavan tahon eli hankintayksikön on siten tultava toimeen useiden erilaisten sähköisten allekirjoitusten kanssa. Vaikka muotovaatimusten lieventäminen edistääkin sähköisten menetelmien käyttöä lyhyellä tähtäimellä, aiheuttaa yhtenäisten menettely-tapojen puuttuminen kuitenkin yhteensovitusongelmia.

On lisäksi todettava, että Saksan nykyinen rakennusurakoita koskeva hankintalaki on vaatinut salausmenetelmän käyttöä tarjouksen muodollisen pätevyyden turvaamiseksi.

Saksassa hyväksytään sähköinen laskutus, mutta lainsäädännössä on sille asetettu muotovaatimukseksi kvalifioidun sähköisen allekirjoituksen käyttö. Tätä koskeva säännös on Saksan arvonlisäverolain[161] 14 §:ssä, jossa säädetään, että sähköinen laskun on allekirjoitettava Saksan sähköisiä allekirjoituksia koskevan lain[162] mukaisella sähköisellä allekirjoituksella, joka voi perustua laatuvarmenteeseen tai sitten on käytettävä elektronista tiedonsiirtoa eli EDI:ä direktiivin 2001/115/EY mukaisesti.[163]

---

[161] Umsatzsteuergesetz BGBl I 1979, 1953.

[162] Signaturgesetz BGBl I 2001 876.

[163] Säännöksesä todetaan : « *eine qualifizierte elektronische Signatur oder eine qualifizierte elektronische Signatur mit Anbieter-Akkreditierung nach dem Signaturgesetz...* ».

11.9 Tietoturvallisuuteen liittyvät yleiset palvelut

Saksassa on tuotteiden tietoturvaan liittyvien sertifiointien osalta käytössä kansainvälinen Common Criteria -standardi (ISO/IEC 15408). Saksan tietoturvaviranomaisella BSI:llä on oikeus myöntää tietoturvallisuuteen liittyville tuotteille, kuten järjestelmille ja komponenteille tietoturvallisuutta koskevia sertifikaatteja. BSI myöntää yksityisille yrityksille akkreditointeja sertifikaattien myöntämiseen liittyvien tarkastusten toteuttamiseksi.

Saksassa toimii useita tietoturvallisuuden hälytysryhmiä, joista keskeisin on *CERT-BUND*.

12. Viro

12.1 Perustuslainsäännökset

Viron nykyinen perustuslaki on vuodelta 1992. Laki tunnustaa oikeuden yksityisyyteen, viestinnän luottamuksellisuuteen sekä, ainakin osittain, tietosuojaan. Perustuslain artikla 42 toteaa, ettei valtion tai paikallisen hallinnon viranomainen voi kerätä tietoa Viron kansalaisen vakaumuksesta vastoin tämän tahtoa.

Artikla 43 lisää, että jokaisella on oikeus luottamukselliseen viestintään kirjeen, sähkeen, puhelimen tai muun yleisesti käytetyn viestintävälineen avulla Poikkeuksia voidaan tehdä vain oikeuden suostumuksella, lain määräämissä tapauksissa ja lain mukaisia menettelytapoja noudattaen rikoksen ehkäisemiseksi tai rikostutkinta-aineiston hankkimiseksi. Viestinnän kuuntelu edellyttää tuomioistuimen myöntämää lupaa. Laittomasti hankittua todistusaineistoa ei voi esittää oikeudessa.

Artikla 44 antaa oikeuden vastaanottaa tietoa, jota levitetään yleiseen käyttöön. Samainen artikla sisältää tietosuojan kannalta merkityksellisen kolmannen momentin, jonka mukaan Viron kansalaisilla on oikeus tutustua itseään koskevaan tietoon, jota valtion tai paikallishallinnon viranomaisilla on hallussaan tai joita säilytetään arkistoissa. Tätä oikeutta voidaan rajoittaa lailla muiden henkilöiden oikeuksien tai vapauksien turvaamiseksi, lasten sukutaustan suojaamiseksi tai rikoksen torjumiseksi, rikollisen kiinniottamiseksi tai totuuden selvittämiseksi oikeudenkäynnissä.

Artikla 45 sisältää ilmaisunvapautta koskevan perusoikeuden. Sen mukaan jokaisella on vapaus levittää ideoita, mielipiteitä ja muuta tietoa kirjallisesti, painettuna, kuvana tai muulla tavoin. Tätä oikeutta voidaan rajoittaa lailla yleisen järjestyksen tai moraalin suojaamiseksi samoin kuin toisen henkilön oikeuksien, vapauksien, terveyden, kunnian tai maineen suojaamiseksi. Lailla voidaan ilmaisunvapautta rajoittaa valtion ja paikallis-hallinnon viranomaisten osalta valtionsalaisuuden, liikesalaisuuden tai luottamuksellisen viestinnän suojaamiseksi silloin kun viranomaiset saavat tehtävässään tietoonsa kyseistä tietoa. Oikeutta voidaan viranomaisten osalta rajoittaa myös perhe-elämän ja yksityisyyden suojaamiseksi sekä oikeuden toteuttamiseksi.

Viron perustuslaki keskittyy edellä olevan mukaisesti kansalaisen ja viranomaisen väliseen suhteeseen. Perustuslaki puhuu monissa yhteydessä kansalaisista, mikä jättää epäselväksi sen, mikä on ulkomaalaisten tai maassa asuvan kansalaisuudet-toman venäjänkielisen väestön asema. Viron on Euroopan Neuvoston jäsenvaltio ja on ratifioinut Euroopan ihmisoikeussopimuksen.

12.2 Tietoturvan sääntely ja kehittäminen

Virossa ei ole tietoturvan osalta erityislainsäädäntöä, vaan tietoturvaa koskevat määräykset ovat hajallaan eri puolilla lainsäädäntöä. Keskeisiä säännöksiä ovat tässä suhteessa, kuten muissakin EU-maissa henkilötietodirektiivin ja sähköisen viestinnän tietosuojadirektiivin implementoinnin yhteydessä annetut määräykset.

Toisaalta Virossa on panostettu turvalliseen sähköiseen asiointiin eli voidaan sanoa, että transaktioturvallisuuden osalta maassa on tehty huomattavia investointeja.

Viro on pitkään ollut etulinjassa sähköiseen asiointiin perustuvan yhteiskunnan kehittämisessä. Taustalla on pitkälti valtion politiikka. Tuorein ilmaus informaatio-yhteiskunnan kehittämisestä on ohjelma-asiakirja **Estonian IT Policy: Towards a More Service-Centred and Citizen-Friendly State, Principles of the Estonian Information Policy 2004–2006**. Kyse on kuitenkin viisivuotissuunnitelmasta, jolla Viron valtiovalta haluaa tuoda sähköiset palvelut kaikkiin valtion virastoihin, ylläpitämällä viestintä- ja kommunikaatioteknologian käyttö Virossa vähintään keskitasolla sekä edistämällä maan IT-sektorin vientikapasiteettiä.

ICT:n käytöllä pyritään edistämään julkisen sektorin tehokkuutta. Sähköistä asiakirja-hallintaa pyritään edelleen kehittämään ja sähköinen asiakirjojen arkistointijärjestelmä luodaan. Erityinen huomio kohdistetaan Internet-viestintään erityisesti hallituksen ja paikallistason viranomaisten välillä. Sähköisiä tietokantoja kehitetään edelleen tarkoituksena turvata tiedon eheys, saatavuus ja yhteen toimivuus. Myös sähköisesti allekirjoitettujen asiakirjojen arkistointimahdollisuutta aiotaan kehittää niillä aloilla, jossa tämä katsotaan tarpeelliseksi.

Sähköistä kaupankäyntiä halutaan edistää sähköisen henkilökortin, sähköisen allekirjoituksen sekä sähköisten tunnistamismenetelmien käyttöä kehittämällä. Myös standardointia ja lainsäädäntöä halutaan kehittää.

Yhteiset turvallisuusperiaatteet informaatioteknologian käytölle halutaan kehittää. Valtiovalta perustaa yhdessä yksityisen sektorin kanssa kansallisen tietoturvaelimen toimimaan yhteistyössä EU:n toimielimien kanssa. Viranomaisen tehtävänä olisi tietoturvaan kohdistuvien hyökkäysten rekisteröinti, tiedottaminen osapuolille, turva-toimien valmistelu ja levittäminen sekä tietoisuuden lisääminen tietoturvaongelmista. Erityisenä toimenpiteenä mainitaan tieto-oikeuksien peruskirjan (**charter of information rights**) luominen. Tämä peruskirja määrittelisi yksilön suhteen erityyppiseen tietoon. Tavoitteena olisi perusoikeuksien toteutuminen sähköisessä ympäristössä.

12.3 Erityispiirteitä viranomaistoiminnasta

Erityinen **viranomaisvalvontalaki**[164] sääntelee viestintätiedon sieppaamista, peitettyä valvontaa, soluttautujien käyttöä samoin kuin poliisin ja tiedustelupalvelun tietokantoja. Valvontatoimen voi hyväksyä valvontaelimen päällikkö perustellulla päätöksellä. ’Poikkeuksellinen valvonta’ tulee kysymykseen vakavien rikosten ollessa kyseessä ja edellyttää Tallinnan hallinto-oikeuden tuomarin antamaa lupaa. Laissa on säädetty myös rangaistusseuraamus laittomasta valvonnasta. Jos kyse on tavallisesta valvonnasta, on rangaistus sakko tai vankeus enintään kolmeksi vuodeksi. Jos laiton valvontatoiminta käsittää erityistoimia, kuten salakuuntelua tai kirjeiden luvatonta avaamista, on maksimirangaistus viisi vuotta vankeutta.

Viranomaisvalvontalaki antaa kansalaisille mahdollisuuden tutustua heitä koskevaan, valvonta- viranomaisten hallussa olevaan tietoon. Viranomaisten on vastattava kolmessa kuukaudessa, jos näillä on hallussaan kansalaista koskevaa tietoa. Vuoden 2000 **tietoliikennelaki**[165] säätää, että valvontaviranomaiset voivat saada liikennetietoja kirjallisen tai suullisen pyynnön perusteella. Toisaalta palveluntarjoajien on pidettävä liikennetiedot salaisina, elleivät käyttäjät suostu niiden paljastamiseen, mikä velvollisuus seuraa nyt myös sähköisen viestinnän tietosuojadirektiivistä. Vuonna 2003 tehdyt muutokset tietoliikennelakiin velvoittavat teleoperaattorit säilyttämään liikennetiedot valvonnallisista syistä jopa kolmen vuoden ajan.

12.4 Tiedon julkisuus ja salassapito

12.4.1 Viranomaistieto

Viron **julkisuuslaki**[166] hyväksyttiin vuonna 2000 ja se tuli voimaan 1.1.2001. Laki kattaa valtion ja paikallishallinnon viranomaiset, julkisoikeudelliset oikeushenkilöt samoin kuin yksityisoikeudelliset oikeushenkilöt, jotka suorittavat julkista tehtävää esimerkiksi opetustoimen, terveydenhuollon tai muiden julkisten palvelujen suorittamisessa. Jokainen henkilö (siis myös ei-kansalainen) voi tehdä tietopyynnön ja tiedon haltijan on vastattava viiden päivän kuluessa. Tiedon luovutusta koskevat pyynnöt on rekisteröitävä. Maksuista voidaan luopua, jos pyyntö on tehty tutkimus-tarkoituksiin. Laissa on myös runsaasti määräyksiä tiedon sähköisestä esilläpidosta. Hallituksen ministeriöiden on ylläpidettävä asiakirjarekisterejä. Ministeriöiden ja muiden

---

[164] RT I 1994, 16, 290.

[165] RT I 2000, 18, 116.

[166] RT I 2000.

keskusviranomaisten, alueellisten viranomaisten ja muiden julkista tietoa säilyttävien on ylläpidettävä verkkosivuja ja luotava pääsy huomattavaan määrään tietoa verkossa. Tällaiseen tietoon kuuluvat tilastot rikollisuudesta ja talouden tilasta, viranomaisten perustavista säännöistä sekä toimintayksiköistä, viranomaisten toimenkuvista ja osoitteista, kelpoisuusehdoista ja palkkauksesta, tietoa terveydestä ja turvallisuudesta, budjetista ja budjettiehdotuksista, tietoa ympäristön tilasta, laki- ja asetusehdotuksista selitysosioineen. Edellä mainittujen virastojen ja organisaatioiden on varmistuttava, että tieto ei ole vanhentunutta, epätäsmällistä tai harhaanjohtavaa. Sähköpostin välityksellä tehdyt tiedustelut on käsiteltävä virallisina tietopyyntöinä. Lain noudattamista valvoo Viron tietosuojaviranomainen. Tämä laki kattaa EU-direktiivin 2003/98/EY vaatimukset viranomaistiedon uudelleenkäytöstä. Viranomaistiedon julkisuutta rajoittaa **laki**[167] **valtionsalaisuuksista**.

Tietokantalaki[168] säätelee viranomaisten sähköisten tietokantojen luomista ja ylläpitoa. Laki asettaa tietokantojen ylläpitämisen yleiset vaatimukset, ja se määrittelee tietojenkäsittelyn vaatimukset ja suojatoimet ja yhtenäistää tietokantojen ylläpidossa käytettyä terminologiaa. Laki mahdollistaa myös valtion tietokantarekisterin perustamisen. Valtion tietokantarekisteriin luetteloidaan valtion ja paikallishallinnon tietokannat samoin kuin yksityisoikeudellisten oikeushenkilöiden ylläpitämät, arkaluonteisia henkilötietoja sisältämät tietokannat. Näin lailla on myös yritysulottuvuus. Laissa on määritelty keskusrekisterin pääkäsittelijä, jolle on annettu tehtäväksi tehdä ehdotuksia hallitukselle, muiden tietokantojen pääkäsittelijöille ja hallituksen tieto-järjestelmistä vastaaville henkilöille. Keskusrekisterin pääkäsittelijä toimii koordinointi-viranomaisena silloin, kun tietokantoja laajennetaan, yhdistetään tai suljetaan samoin kuin tietokantojen ristiin käytöstä samoin kuin tietojenkäsittelyn tehostamisesta. Tietokantalaista erillinen laki on **arkistolaki**[169], joka sääntelee viranomaisarkistojen ylläpitoa.

12.4.2 Yrityssalaisuuksien suoja

Yrityssalaisuuksien suojaa säännellään Virossa vuodelta 1993 peräisin olevassa kilpailulaissa.[170] Lain 7 § määrittelee yrityssalaisuuden väärinkäytön epäreiluksi kilpailuksi, joka on kielletty.

---

[167] RT1 I 1999, voimaan 28.2.1999.

[168] RT1 I 1997, 28, 423, voimaan 19.4.1997.

[169] RT1 I 1998, 36/37, 552, voimaan 1.5.1998.

[170] RT I 1993, 47, 642, voimaan 1.1.1994.

Yrityssalaisuuden väärinkäyttöä on lain mukaan toisen samoilla markkinoilla toimivan yrityksen (tai muun toimijan) liikesalaisuuden käyttö kilpailuaseman parantamiseksi, jos liikesalaisuutta koskeva tieto on saatu laittomasti tai vastoin toisen, samoilla markkinoilla toimivan yrityksen kanssa tehdyn sopimuksen määräyksiä. Yrityssalaisuus määritellään tekniseksi, teknologiseksi tai muuksi yritystiedoksi samoin kuin tiedoksi liikeneuvotteluista, transaktioista, markkinatutkimuksesta tai muista olosuhteista, joiden käytöstä markkinoille osallistuva yritys määrää, ja jonka julkistaminen ei ole pakollista, ja jonka salassapidon markkinatoimija eli yleensä yritys katsoo välttämättömäksi.

Kilpailulaki ei sisällä rangaistuseuraamuksia, vaan nämä löytyvät rikoslainsäädännöstä. Kilpailulaki ei myöskään sisällä määräyksiä työntekijöiden velvollisuuksista yritys-salaisuuksien suhteen, vaan nämä velvollisuudet määräytyvät työlainsäädännön lojaliteettisäännösten perusteella.

12.5 Tietosuojasäännökset

12.5.1 Yleiset tietosuojasäännökset

Viroon säädettiin ensimmäinen tietosuojalaki vuonna 1996. Nykyinen lainsäädäntö, Viron henkilötietosuojalaki[171], jolla lainsäädäntö saatetaan henkilötietodirektiivin (1995/46/EY) mukaiseksi, on tullut voimaan 1. lokakuuta 2003 ja sitä on jo muutettu kerran sen jälkeen. Kuten on aikaisemmassa yhteydessä tullut esille, direktiivissä on tietoturvallisuutta koskeva yleinen vaatimus. Lakia valvoo tietosuojan tarkastusvirasto.[172]

Laki sähköisestä viestinnästä[173] sisältää luvussa 10 määräykset tietoturvasta ja tietosuojasta.

12.5.2 Kameravalvonta

Kameravalvontaa varten ei ole olemassa erillistä lainsäädäntöä, vaan kameravalvonnan käyttö kuuluu henkilötietosuojadirektiivin alle.

Myöskään yksityisyyden suojasta työelämässä ei ole omaa lakia, vaan siihen sovelletaan henkilötietosuojalakia.

---

[171] RT I 2003, 26,158.

[172] Vironkieliseltä nimeltään **Andmekaitse Inspektioon.**

[173] RT2 I 2004, 87, 593, voimaan 1. tammikuuta 2005.

12.6 Sähköisten palvelujen tuottaminen

Lailla tietoyhteiskunnan palvelujen tarjoamisesta pannaan täytäntöön EU:n sähkökauppadirektiivi 2000/31/EY. Siten laki sisältää määräyksiä kotivaltion valvonnasta, valvontaviranomaisista, kaupallisesta viestinnästä sekä tietoyhteiskunnan palvelujen tarjoajien vastuuvapaudesta.

Kun direktiivi velvoittaa jäsenvaltiot sallimaan sähköiset sopimukset, lain 7 § toteaa, että sopimukset palvelun tarjoajien ja vastaanottajien välillä silloin kun osapuolet eivät ole yhtä aikaa saapuvilla, on solmittava velvoiteoikeutta koskevan lain[174] 62 §:n mukaisesti.

Lailla sähköisestä viestinnästä[175] pannaan Virossa täytäntöön EU:n sääntely-järjestelmä eli vuoden 2002 direktiivipaketti. Lain tarkoituksena on luoda olosuhteet sähköisten viestintäverkkojen ja viestintäpalvelujen kehittämiselle ja turvata sähköisten viestintä palvelujen käyttäjien intressit. Lailla luodaan säännöt yleisille viestintäverkoille ja -palveluille, radiolähetyksille, radiotaajuuksien ja numeroinnin järjestämiselle, valvontajärjestelmälle samoin kuin seuraamukset lain rikkomisesta.

12.7 Sähköiset allekirjoitukset ja tunnistaminen

Laki[176] **sähköisistä allekirjoituksista** antaa sähköiselle allekirjoitukselle saman oikeudellisen merkityksen kuin käsintehdyllä allekirjoituksella on ja velvoittaa viran-omaiset hyväksymään sähköisten allekirjoitusten käytön Viron laki puhuu digitaalisista allekirjoituksista eli se on ollut selkeästi PKI-tekniikkaan perustuva laki. EU:n sähköisiä allekirjoituksia koskeva direktiivi kieltää kuitenkin varsinaisen diskriminoinnin puhtaasti sähköisen allekirjoituksen muodon perusteella. Viron laki sääntelee myös mm. aikaleimojen käyttöä.

Viron **henkilökorttilaki** säädettiin vuonna 1999. Laissa säädetään vaatimus henkilöllisyystodistuksen olemassaolosta ja todistuksen myöntämisestä Viron kansalaisille ja maassa asuville ulkomaalaisille, joihin kuuluu runsaasti maan venäläis-vähemmistön edustajia. Laki luettelee ID-kortin käyttötarkoitukset pääasiallisena henkilöllisyystodistuksena ja lailla perustetaan henkilöllisyystodistuksien valtionrekisteri.

---

[174] RT I 2001, 81, 487; 2002, 60, 374; 2003, 78, 523; 2004, 13, 86.

[175] RT2 I 2004, 87, 593, voimaan 1. tammikuuta 2005.

[176] RT I 2000, 26, 150, voimaan 15.12.2000. Lakia on täydennetty useaan otteeseen.

Sähköinen henkilökortti sisältää yleiset henkilötiedot, kuten nimen, syntymäajan, kansalaisuuden, henkilötunnuksen, kortin voimassaolon umpeutumisajan sekä kortinhaltijan käsintehdyn allekirjoituksen ja valokuvan. Virossa oleskeluoikeuden omaavien ulkomaalaisten eli erityisesti venäläisvähemmistön suhteen kortti sisältää oleskelu- ja työlupaa koskevat tiedot. Kortti sisältää myös mikrosirun, jossa on henkilökohtaisen tunnistamisen mahdollistava, varmentajan eli pankkien omistaman *Eesti Serifitseerimiskeskus A/S:n* antamat varmenteet. Varmenteita käytetään PKI-tekniikkaan kuuluvan, asymmetriseen kryptografiaan perustuvan avainparin avulla.

Sähköinen henkilökortti aktivoidaan henkilökohtaisella tunnusnumerolla eli PIN-tunnuksella, mutta tämä toiminto on ajateltu myöhemmin korvattavan biometrisillä tunnisteilla. Biometriset ominaisuudet olisivat kasvokuva ja sormenjäljet. Biometriset tunnisteet vastaisivat kansainvälisen siviili-ilmailujärjestön ICAO:n standardeja.

Virossa oli keväällä 2005 jo noin 700.000 kansalaisella sähköinen henkilökortti ja niiden levinneisyys kasvaa koko ajan. Sähköisiä allekirjoituksia käytetään runsaasti mm. tuomioistuimien ja verottajan kanssa asioitaessa. Virossa on tarjolla noin 150 sähköistä palvelua, joissa voidaan käyttää henkilökortin tunnistus- ja allekirjoitusvarmennetta. Esimerkiksi pankkilainahakemuksen voi allekirjoittaa sähköisellä allekirjoituksella. Kansalaiset käyttävät kuitenkin huomattavasti yleisemmin pankkitunnisteita ja sähköistä henkilökorttia käyttää vain noin 3 % laatuvarmenteiden piirissä olevien sähköisten palvelujen käyttäjistä. Allekirjoituskäyttöä on kuitenkin merkittävässä määrin olemassa. Allekirjoitustilanteessa tietojärjestelmä huomauttaa allekirjoittajalle, että tämän tekemällä toimenpiteellä on oikeusvaikutuksia, mikä vastaa myös kuluttajansuojatarpeisiin.

Henkilön tunnistamiseen liittyy **ihmisgeenien tutkimuslaki** vuodelta 2000. Lailla luotiin kansallinen geenitietokanta, jota käytetään sairauksien tutkimiseen. Tietokannan omistaa virolainen säätiö, mutta valtaosan hankkeen rahoituksesta tarjoaa yhdysvaltalainen yritys. Viron tutkimushanke liittyy sen tutkimiseen, miten geeniperimä vaikuttaa yksilön reagoimiseen eri lääkkeisiin.

12.8 Tietoturva ja sähköiset palvelut aineellisessa lainsäädännössä

12.8.1 Pankkitoiminta ja rahanpesu

Viron olot muistuttavat kovasti Suomea sillä maan pankkilaitos hyväksyy Suomen mallin mukaiset pankkitunnukset sekä kansalaisille jaetun sähköisen henkilökortin asiakkaan tunnistuskeinoina. Virossa on panostettu tunnistamiseen voimakkaasti minkä johdosta pankeilla on mahdollisuus tietoturvallisuuden tehokkaaseen ylläpitämiseen asiakasrajapinnassa.

EU-maana Virossa on myös käynnissä kolmannen rahanpesudirektiivin täytäntöönpano.

12.8.2 Hankintalainsäädäntö ja verkkolaskutus

Viron hankintalainsäädäntö on ollut uusittavana EU-direktiivien mukaiseksi. Sähköinen hankintatoimi oli käytössä jo ennen maan liittymistä EU:n jäseneksi ja järjestelmä meni väliaikaisesti uusiksi liittymisen myötä sillä uudet direktiivit eivät vielä tuolloin olleet valmiina.

Verkkolaskutus on myös Virossa yleistynyt. Virossa seurattiin Pohjoismaisen esimerkkiä eikä asetettu verkkolaskuille sähköisen allekirjoituksen vaatimusta. Viranomaisen kanssa asioitaessa sähköisesti on Virossa kuitenkin asetettu sähköisen allekirjoituksen vaatimus.

12.9 Tietoturvallisuuteen liittyvät yleiset palvelut

PKI-pohjaisiin sähköisiin allekirjoituksiin liittyviä palvelut ovat Virossa kehittyneet ja tarjolla on myös luotetun kolmannen osapuolen palveluja aikaleimojen osalta.

Toukokuussa 2006 aloitti toimintansa tietoturvallisuuden *CERT Estonia*, joka toimii Viron informatiikkakeskuksen (*Estonian Informatics Centre*) yhteydessä.

13. Venäjä

13.1 Perustuslainsäännökset

Venäjän perustuslaki on vuodelta 1993. Perustuslain 23 artiklan mukaan jokaisella on oikeus yksityiselämään, henkilökohtaisiin ja perheen salaisuuksiin sekä henkilökohtaisen kunnian ja maineen ylläpitämiseen. Lisäksi jokaisella on oikeus yksityisyyteen kirjesalaisuuden, puhelin- ja kaapeliliikenteen ja muiden kommunikaatiomuotojen osalta. Poikkeuksia voidaan sallia ainoastaan oikeuden määräyksellä.

Perustuslain 24 artikla lisää, että on kiellettyä koota, varastoida, käyttää ja levittää tietoa henkilön yksityiselämästä ilman hänen suostumustaan. Valtiovallan ja paikallisen itsehallinnon ja niiden virkamiesten on tarjottava kansalaisille oikeus tutustua hänen oikeuksiaan ja vapauksiaan koskeviin asiakirjoihin ja aineistoon, ellei laissa ole toisin määrätty.

Perustuslain 25 artikla määrää kotirauhan loukkaamattomaksi. Kukaan ei saa tunkeutua henkilön kotiin ilman siellä asuvan henkilön suostumusta, ellei liittovaltion laissa ole toisin säädetty tai tuomioistuin ole antanut lupaa.

Venäjä ei ole, kuten tunnettua, Euroopan unionin eikä Maailman kauppajärjestön jäsen. jäsen. Sen vuoksi Venäjän lainsäädäntökin poikkeaa rakenteellisesti olennaisesti tämä tutkimuksen muista kohdemaista sillä maassa ei ole pantu täytäntöön samanlaisia direktiivien voimaan panoja kuin muissa tutkittavissa maissa. Maan lainsäädäntötyön tavoitteena onkin ollut välttämättömän oikeudellisen infrastruktuurin luominen markkinatalouteen siirtymiseksi ja investointien edellytysten luomiseksi.

Venäjä on toisaalta Euroopan neuvoston jäsen ja on allekirjoittanut Euroopan Ihmisoikeussopimuksen. Tällä hetkellä maassa on vireillä Euroopan neuvoston tietosuojayleissopimuksen voimaansaattaminen. Perusoikeuksia ja tietosuojaa koskevat kysymykset nousevat esille myös EU:n kanssa käytävissä neuvotteluissa rajavalvonnan osalta.

13.2 Tietoturvan sääntely ja kehittäminen

Venäjällä on laadittu yleinen informaatioyhteiskuntastrategia ja tietoturvastrategia. Tammikuussa 2002 Venäjän hallitus hyväksyi liittovaltion ohjelman ”Sähköinen Venäjä” vuosiksi 2002–2010. Ohjelmassa on määräyksiä informaation etsimisen vapaudesta, tietoon saavutettavuudesta, siirrosta, tuottamisesta ja levittämisestä, samoin kuin

kaiken tietojärjestelmissä olevan, oikeudellisesti suojatun tiedon yksityisyyden suojasta. Ohjelman laatijat ovat kaavailleet lainsäädäntöä mm. tietoturvasta ja kansalaisten perustuslaillisten oikeuksien suojasta.

Tiedon luottamuksellisuuden tai yksityisyyden suojaa ei kuitenkaan ole mainittu keskeisenä ohjelmatavoitteena. Yrityssalaisuuksien suoja on kuitenkin keskeinen tavoite samoin kuin asiakirjaliikenteen sähköistäminen. Viranomaiset kiinnittävät myös huomiota mahdollisuuteen operatiivisen tutkinnan toteuttamiseen tietoverkkojen kautta.

Venäjä on, kuten tunnettua, liittovaltio, jossa on lainsäädäntöä sekä liittovaltion eli federaation tasolla sekä alueellisella tasolla. Tiedon avoimuuteen ja suojaamiseen liittyvät kysymykset on käytännössä keskitetty liittovaltion tasolle. Keskeinen säännös on Venäjän Federaation laki tiedosta, tiedon käsittelystä ja suojaamisesta on vuodelta 1995 ja lain viimeisin muutos astunut voimaan 1.1.2004.

13.3 Erityispiirteitä viranomaistoiminnasta

Venäjä on suurvalta ja ydinasevaltio, ja maassa on esiintynyt sisäisiä levottomuuksia mm. Tshetsheniassa. Valtakunnan turvallisuus ja terrorismin torjunta ovat siksi merkittäviä tietoturvakysymystenkin taustavaikuttajia. Lisäksi taustalla on turvallisuus-kysymysten keskeinen merkitys Venäjän viranomaishistoriassa.

Laki tiedosta, tiedon käsittelystä ja suojaamisesta vuodelta 1995 suojaa tiedonvälityksen vapautta. Sen mukaan puhelinkeskustelujen nauhoittaminen, sähköisen kommunikaation tarkastaminen, kirjelähetysten viivyttäminen, tarkastaminen ja takavarikoiminen ja muu puuttuminen tiedonvälityksen salaisuuteen on tapahduttava oikeuden määräyksellä.

Tiedustelupalvelujen toimintaa sääntelee **laki**[177] **operatiivisesta tutkimus-toiminnasta**. Sen mukaan myös tiedustelupalvelut tarvitsevat oikeuden määräyksen tiedonkulun vapauteen puuttuakseen. Tätä lakia muutettiin vuonna 1998, jolloin Venäjän kansanedustuslaitos eli duuma edellytti takeita yksityisyyden suojan ylläpitämiseksi. Sen vuoksi lain 5. artikla edellyttää, että tiedustelutoiminnan rakenteen on turvattava yksityiselämän suoja. Laki antaa henkilölle, joka katsoo tiedustelu-viranomaisten toiminnan loukanneen kansalaisoikeuksia, voivan valittaa oikeuteen, syyttäjälle tai ylemmälle valvontaelimelle. Venäjän Federaatioiden turvallisuuspalveluita

[177] Laki nro. 144-FZ, 12.8.1995.

koskevassa laissa[178] on samanlainen määräys, mutta se on tavallaan kumottu maininnalla, jonka mukaan määräyksistä voidaan poiketa, jos yleinen etu tai oikeus muuta vaatii. Samanlaiset laajat valtuudet annettiin myöhemmin veropoliisille, sisäministeriölle, rajavartiolaitokselle sekä useille turvallisuuspalveluille. Kuitenkin vuonna 2001 lakia muutettiin siten, että kuuntelunauhoitukset ja muu aineisto, joka on syntynyt rikosoikeudenkäynnin ulkopuolella olevaan henkilöön kohdistuneen salakuuntelun tuloksena, on tuhottava kuudessa kuukaudessa salakuuntelusta, ja asiasta on laadittava pöytäkirja. Oikeutta on puolestaan informoitava kolme kuukautta ennen kuin sen luvalla suoritettujen operatiivisten tutkimusten tulokset hävitetään.

Venäjän liittovaltion tiedustelupalvelulla (FSB) on oikeus vaatia kaikkia Venäjällä toimivia viestintäpalvelujen tarjoajia asentamaan tietokonelaitteistot ja -ohjelmat, jotka ohjaavat kaiken Internet-liikenteen FSB:n järjestelmien läpi. Vuonna 1998 tuli käyttöön SORM-2, joka edellyttää Internet-palveluntarjoajilta valvontalaitteiden asentamista samoin kuin linkkejä paikalliseen FSB:n toimistoon. Näin FSB voi suoraan päästä valvomaan Internetin käyttäjien yhteyksiä, vaikka tämä vaatiikin oikeuden lupaa. SORM-2:n käyttöönotto herätti protesteja ja erään oikeusjutun tuloksena lakia muutettiin niin, että Internet-palveluntarjoajan tulee tietää, ketä FSB kulloinkin valvoo. Valvontajärjestelmän mielekkyys on myös kyseenalaistettu.

13.4 Tiedon julkisuus ja salassapito

13.4.1 Viranomaistiedon julkisuus

Laki tiedosta, tiedon käsittelystä ja suojaamisesta vuodelta 1995 on kattava viranomaistiedon avoimuutta ja sitä koskevaa tietoturva sääntelevä laki. Tämä laki säätää, että viranomaisten hallussa oleva tietoaineisto on yleisessä käytössä, paitsi sellaiset asiakirjat, joihin pääsy on rajattu. Tällaisia ovat valtiosalaisuuksiin ja muuhun luottamukselliseen tietoon liittyvät asiakirjat. Valtionsalaisuuksien osalta on olemassa erillinen laki.[179] Venäjän Federaation lait tuntevat yli 30 erilaista luokitellun tiedon lajia ja muut säännökset kymmenkunta lisää. Arviolta 45 Venäjän Federaation lakia sisältää luokiteltua tietoa koskevia määräyksiä.

Avoimuutta koskevassa laissa säädetään, ettei ole sallittua rajoittaa erityissäännöksin pääsyä asiakirjoihin, jotka koskevat hallinnollisten elinten ja organisaatioiden, mukaan lukien itsehallinnolliset elimet, sekä sosiaalisten järjestöjen oikeudellista asemaa tai

[178] Laki nro. 40-FZ, 3.4.1995.

[179] Laki 7.7.1993.

kansalaisten oikeuksia, vapauksia ja velvollisuuksia. Toiseksi on kiellettyä rajoittaa pääsyä asiakirjoihin, jotka käsittelevät epätavallisia tapahtumia, ekologisiin, meteorologiaa, demografiaa tai terveyttä ja epidemioita koskevia tietoja tai jotka sisältävät muuta tietoa, jolla on merkitystä toimitus- ja tuotantomahdollisuuksien tai kansalaisten turvallisuuden ja talouden toiminnan kannalta. Vastaavasti hallintoelinten toimintaan liittyvät asiakirjat, jotka käsittelevät budjettivarojen käyttöä, taloudellista tilannetta ja toimitusvaatimuksia, ellei kyse ole valtionsalaisuuksiin liittyvistä asioista. Julkisia ovat aina myös edellä mainittujen hallintoviranomaisten ja muiden elinten ylläpitämissä kirjastoissa, arkistoissa ja tietojärjestelmissä ylläpidetyissä julkisissa kokoelmissa olevat asiakirjat, joilla on yleistä merkitystä tai jotka ovat oleellisia kansalaisten oikeuksien, vapauksien ja velvollisuuksien kannalta.

Lain soveltamisalaan kuuluvien organisaatioiden on lain mukaan laadittava yleisesti saatavilla olevia informaatioluetteloita omalla toimialallaan. Tietoa ja tietopalveluita koskevat luettelot ovat yleisön saatavilla veloituksetta. Kansalaisilla on oikeus saattaa kieltäytyminen tiedon luovuttamiseen oikeuden tutkittavaksi. Venäjän Federaation viranomaiset laativat luetteloita lain määräysten täytäntöön panemiseksi.

Kansalaisilla ja eri organisaatioilla on pääsy itseään koskevaan asiakirja-aineistoon, ja heillä on oikeus korjata ja täydentää sitä tiedon luottamuksellisuuden ja täydellisyyden turvaamiseksi. Heillä on lain mukaan myös oikeus tietää kuka tietoa käyttää tai on aikaisemmin käyttänyt ja mihin tarkoitukseen. Kun viranomaisen hallussa olevat, henkilöä koskevat tiedot ovat salaisia, ei määräys siten koske muiden tiedonsaanti-oikeuksia. Tietoja ylläpitävä virasto tai muu laitos vastaa siitä, että tiedon käsittelyn ehdot ja tietoon pääsyä koskevat määräykset tulevat täytetyiksi.

Laki tiedosta, tiedon käsittelystä ja suojaamisesta osa 5 sisältää määräyksiä tiedon turvaamisvelvoitteista. Koska kyse on osaltaan kansalaisia ja organisaatioita koskevien tietojen suojaamisesta viranomaisissa, ovat määräykset keskeisiä venäläisiä tietoturva-määräyksiä.

Suojaamisen tarkoituksena on estää tiedon vähentymistä, varkautta, menetystä ja väärentämistä. Samoin tarkoituksena on suojata henkilöitä, yhteiskuntaa ja valtiota. Säännöksillä suojataan tietojärjestelmiä ja tietoresursseja luvattomalta tuhoamiselta, muuttamiselta, väärentämiseltä, kopioinnilta, sulkemiselta ja muilta laittomilta puuttumisilta. Lain tarkoituksena mainitaan lisäksi omistusoikeuden turvaaminen dokumentoituun tietoon sekä kansalaisten perustuslaillisen oikeuden, joka koskee yksityisyyttä ja kansalaista koskevan tiedon luottamuksellisuutta. Lain tarkoituksena on luonnollisesti myös valtiosalaisuuksien ylläpitäminen. Erikseen todetaan vielä henkilöiden oikeuksien turvaaminen tietojärjestelmäprosessien aikana sekä tieto-järjestelmien ja tietoturvamenetelmien suunnittelussa, valmistuksessa ja käytössä.

Lain 21. artiklan mukaan kaikki dokumentoitu tieto, johon pääsy ilman lupaa aiheuttaisi vahinkoa tiedon omistajille[180], hallussapitäjillä[181] tai muille oikeutetuille, on suojattava. Laki jakaa velvoitteet viranomaisittain valtionsalaisuuksiin liittyvään informaatioon sekä muihin informaatioresursseihin, joista ensiksi mainittua sääntelee valtionsalaisuuksia koskeva laki. Laki tiedosta, tiedon käsittelystä ja suojaamisesta sääntelee kuitenkin henkilötietojen tietoturvallisuutta.

Viranomaiset, jotka hallinnoivat suojaa vaativia informaatioresursseja samoin kuin elimet, jotka tuottavat ja käyttävät tietojärjestelmiä rajoitetun tiedon käsittelyyn Venäjällä, ovat Venäjän lain alaisia. Viranomaisten vastuulla on tiedon turvaaminen sekä siihen käytetyt tietokoneohjelmat ja laitteet sekä organisatoriset määräykset, joiden mukaan suojeltava tieto käsitellään tietojärjestelmissä. Tämä vastuu täytetään Venäjän Federaation hallituksen antamien määräysten mukaan. Niiden organisaatioiden, jotka käsittelevät hallituksen omistamaa tietoa, on organisoitava omat tietoturvapalvelunsa. Informaatiota hallinnoivat organisaatiot voivat tarkastaa turvatoimet ja tarvittaessa keskeyttää tiedon käsittelyn. Tämä oikeus ulottuu myös ulkopuoliseen tiedon dokumentoidun tiedon omistajaan tai haltijaan, joka voi kääntyä asianomaisen viraston tai laitoksen puoleen ja tarkastaa, onko hänen tietonsa käsitelty tietoturvaohjeiden mukaan. Venäjän Federaation hallitus asettaa silti omat tarkastus-elimensä.

Asiakirjojen tai tietojärjestelmien omistaja tai tämän määräämä henkilö on velvollinen laatimaan tiedon käyttösäännöt, jossa määritellään tiedon sijainti, ajankohta, vastuu-henkilöt ja tiedon käsittelyjärjestelmä. Asiakirjojen tai tietojärjestelmien haltija varmistavat, että Venäjän Federaation lainsäädännön mukainen tietoturvataso saavutetaan.

Laissa todetaan nimenomaisesti, että riski ei-sertifioitujen tietojärjestelmien ja tieto-turvamenetelmien käytöstä on näiden järjestelmien ja menetelmien haltijoilla. Vastaavasti sellaisen tiedon käyttö, joka on otettu ei-sertifioidusta tietojärjestelmästä, on käyttäjän riskillä. Laissa todetaan sertifioinnin osalta ainoastaan, että asiakirjojen tai tietojärjestelmän haltija voi pyytää sertifioinnista vastaavia organisaatioita suorittamaan tarkastuksia samoin kuin antamaan neuvoja. Asiakirjojen tai tietojärjestelmän haltija on velvoitettu informoimaan informaatioresurssien tai tietojärjestelmien haltijaa kaikista tietoturvamääräysten loukkauksista.

---

[180] Tiedon, tietotojärjestelmän, teknologian tai tietoturvamenetelmän omistajalla tai haltijalla tarkoitetaan laissa jokaista, joka voi käyttää omistajan puhevaltaa näihin nähden.

[181] Tiedon, tietotojärjestelmän, teknologian tai tietoturvamenetelmän hallussapitäjä on henkilö, joilla on mainitut asiat hallussaan joko omistajan tai haltijan ominaisuudessa ja käyttää niitä oikeudellisen järjestelmän puitteissa.

Jos pääsy julkiseen viranomaisaineistoon estetään, tarjoaa laki mahdollisuuden syytteen nostamiseen. Henkilöillä, joilta evätään mahdollisuus saada julkista viranomaistietoa tai tätä oikeutta rajoitetaan, on oikeus vaatia vahingonkorvausta.

13.4.2 Yrityssalaisuuksien suoja

Liittovaltion laki[182] **yrityssalaisuuksien suojasta** sääntelee kaupallisten salaisuuksien käyttöä ja sitä, kuinka tiedon luottamuksellisuus voidaan turvata. Laki määrittelee liike- ja ammattisalaisuuden ainoastaan yleisin termein. Liikesalaisuuden haltijan tulee yksilöidä liikesalaisuutensa. Toisaalta laki luettelee tiedon, jota ei voida missään oloissa pitää yritysalaisuutena ja luetteloi tietoa, jota voidaan tilanteen mukaan pitää yrityssalaisuutena. Tällaista tietoa on mm. työntekijöiden määrä, palkitsemis-järjestelmät, työolot mukaan luettuina turvallisuusjärjestelyt, työperäiset tapaturmat, ammatilliset kuolleisuusluvut, avoimena olevat työpaikat sekä lainrikkomukset. Yrityssalaisuudet omistaa lain mukaan yritys eli työnantaja.

Venäjän lainsäädännössä turvataan yrityssalaisuuksia myös siviilikoodin ja kilpailu-lainsäädännön määräyksillä. Venäjän Federaation siviilikoodin artikla 139, joka on otsikoitu ’liike- ja ammattisalaisuudet’, määrää sellaisen liike- ja ammattisalaisuuden muodostavan tiedon olevan suojattu siviilioikeudellisin oikeussuojakeinoin, erityisesti vahingonkorvausvelvollisuuksin. Vahingonkorvausvelvolliseksi voivat joutua liike-salaisuuden haltijan työntekijät sekä kolmas henkilö, joka vastaanotti luvattomasti tiedon yrityssalaisuudesta.

Mainittu siviilikoodin artikla määrittelee kolme ominaisuutta, jotka tiedolla tulisi olla voidakseen tulla luokitelluksi liike- tai ammattisalaisuudeksi. Ensinnäkin tiedolla tulisi olla todellinen tai mahdollinen kilpailullinen arvo. Toiseksi tiedon tulee olla tuntematon ulkopuolisille sekä yleisesti lain sallimien informaatiokanavien saavuttamattomissa. Kolmanneksi tiedon omistajan tulisi suorittaa toimenpiteitä suojatakseen tiedon luottamuksellisuutta. Muussa tapauksessa tiedon omistaja ei voi näyttää, että tieto on yrityssalaisuus.

Yrityksen on lainsäädännön mukaan siten suoritettava useita toimia saadakseen tiedolle yrityssalaisuuden aseman. Ensinnäkin on luetteloitava organisaation liikesalaisuuksien piiriin kuuluva aineisto. Toiseksi yrityksen on rajoitettava pääsyä liikesalaisuuteen luomalla menettely kyseistä tietoa varten ja menettelyn noudattamisen valvontaa varten. Yrityksen on myös lueteltava henkilöt, joilla on pääsy kyseiseen tietoon. Sen lisäksi yrityksen on säänneltävä suhdetta liikesalaisuustiedon

[182] Laki nro N98-FZ, 29.7.2004.

käyttöön. Työntekijöiden osalta tämä tapahtuu työsopimusten ja liikekumppanien osalta liikesopimusten avulla. Liikesalaisuustieto on lisäksi varustettava leimalla ilmaisten tiedon omistajan. Tämä menettely on tietenkin merkityksellinen manuaalisessa muodossa säilytettävän tiedon osalta.

Venäjän lain mukaan liikesalaisuustietoon oikeutetun henkilökunnan jäsenen on noudatettava työnantajan asettamia luottamuksellisuusmääräyksiä. Henkilökunnan jäsen ei myöskään saa paljastaa työnantajan liikesalaisuutta aikana, joka on määritelty työnantajan kanssa sopimuksessa työsuhteen kestäessä, tai kolmena työsuhteen päättymisen jälkeisenä vuotena milloin sopimusta ei ole solmittu.

Työntekijän on myös korvattava työnantajalle vahinko, jonka tämä on kärsinyt työntekijän luovuttaessa tietoonsa tulleita yrityssalaisuuksia. Venäjän työsopimuslaki sisältää täsmällisempiä määräyksiä työntekijän korvausvelvollisuudesta samoin kuin rangaistusseuraamuksista. Yrityssalaisuuksien suojaa koskeva laki sisältää kuitenkin määräyksen, jonka mukaan työntekijän on korvattava vahinko, joka on syntynyt työntekijän paljastettua liikesalaisuuksia ulkopuolisille kolmen vuoden kuluessa työsuhteen päättymisestä.

Työntekijän on myös luovutettava työsuhteen päättyessä työnantajalle kaikki liike-salaisuuksia sisältävä aineisto. Työnantajan on puolestaan kiinnitettävä työntekijän huomio yrityssalaisuuden luonteeseen, työntekijän niitä koskeviin velvollisuuksiin ja rikkomuksesta seuraaviin sanktioihin.

Yrityssalaisuuksia koskeva laki velvoittaa kuitenkin yrityssalaisuuksien haltijan eli yrityksen ja/tai sen työntekijän luovuttamaan tiedon yrityssalaisuudesta valtiollisille tai kunnalliselle viranomaiselle, joka on tehnyt luovutusta koskevan perustellun pyynnön. Pyynnön on oltava asianmukaisesti muotoiltu ja allekirjoitettu ja sen on ilmaistava asiallinen ja oikeudellinen peruste samoin kuin aikaraja luovuttamiselle. Yritys voi velvoittaa työsopimuksessa työntekijän ilmoittamaan luovutusta koskevista vaatimuksista. Viranomaisiin kohdistuu vaatimuksia yrityssalaisuuksien suojaan nähden. Viranomaisten on luotava luottamuksellisuutta koskevat menettelytavat eikä näillä ole oikeutta ilman yrityssalaisuuden omistajan lupaa ilmaista salaisuutta ulkopuolisille, ei edes toisille viranomaisille.

Yritysalaisuuksia koskeva laki sääntelee poikkeuksellisesti myös yrityksen ja tämän sopimuskumppanin välisiä suhteita yrityksen luovuttaessa tälle salaisuuksiaan. Käytännössä sopimuskumppanin velvollisuudet määritellään sopimuksessa. Sopimus voi määritellä yleisen velvollisuuden olla paljastamatta toisen osapuolen liikesalaisuutta ja määritellä toisen osapuolen velvollisuudet yrityssalaisuutta koskevan tiedon suojaamiseksi. Tiedon suoja-aika voi ulottua sopimuksen muuta kestoa pitemmäksikin.

Sopimuksella on määriteltävä myös yrityssalaisuutta koskevan tiedon asema osapuolen joutuessa konkurssiin tai selvitystilaan samoin kuin sopijapuolen velvollisuus korvata vahingot jotka syntyvät tiedon sopimuksen vastaisesta luovutuksesta.

Tiedon omistajan on sopimuslausekkeiden lisäksi kohdeltava tietoa liikesalaisuutena, mikä edellyttää asianmukaisten suojelutoimien tekemistä.

Sopimuskumppani on velvollinen informoimaan liikesalaisuuden haltijaa salaisuuden paljastumisesta tai sen uhasta, on paljastumiseen syyllinen sopimuskumppani itse tai muu taho. Samoin on sopijapuolen informoitava

Yrityssalaisuuksia voidaan lisäksi suojata kilpailulainsäädännön määräysten turvin. **Laki kilpailusta ja monopolististen menettelyjen rajoittamisesta hyödyke-markkinoilla** vuodelta 1992 määrittelee sopimattoman kilpailun tieteellisen, teknisen, tuotannollisen tai kaupallisen tiedon, mukaan lukien liikesalaisuudet, hankkimiseksi ilman omistajan suostumusta. Sen lisäksi, että liikesalaisuuksien haltija voi vaatia vahingonkorvausta luottamuksellisen tiedon luvattomasta hankinnasta, käytöstä tai paljastamisesta, mainittu kilpailulaki tarjoaa hallinnollisia sanktioita oikeudenloukkaajia vastaan. Kilpailuviranomaiset voivat tällöin määrätä huomattavia sakkoja väärin-käytöksiä tehneille. Kilpailuasioista ja yritystoiminnasta vastaava ministeriö ylläpitää alueellisten toimielinten verkkoa, joka voi käsitellä yrittäjien liikesalaisuuksien rikkomista koskevia vaatimuksia. Näiden viranomaisten päätöksiin voi hakea muutosta hallinnollisista välitystuomioistuimista.

Venäjän patenttilainsäädäntö tarjoaa mahdollisuuden suojata eräät yrityssalaisuudet patentilla.

13.5 Tietosuojasäännökset

13.5.1 Yleinen tietosuojalainsäädäntö

Laki tiedosta, tiedon käsittelystä ja suojaamisesta vuodelta 1995 sääntelee myös henkilötietoja koskevia kysymyksiä yleisellä tasolla, vaikka Venäjä ei olekaan mukana Euroopan neuvoston tietosuojayleissopimuksessa. Myös henkilöön liittyvät tiedot katsotaan sen tarkoittamaksi luottamukselliseksi tiedoksi. Henkilötiedot eli tieto kansalaisista tarkoittaa raportteja tosiseikoista, tapahtumista ja elämäntavoista, jotka yksittäisen kansalaisen yksilöimisen.

Kyseisen lain mukaan on luonnollisen henkilön yksityiselämään liittyvän tiedon kerääminen, säilyttäminen, käyttö, levittäminen samoin kuin henkilökohtaiseen tai

perhesalaisuuteen liittyvän tiedon käsittely ilman asianomaisen henkilön suostumusta kielletty, ellei kyse ole tiedon käsittelystä oikeuden määräyksen perusteella tai asianomainen henkilö on antanut suostumuksensa toimenpiteeseen. Samoin viestintäsalaisuutta loukkaava tiedon kerääminen, säilyttäminen, käyttö tai levittäminen on sallittu vain erityismääräysten nojalla tai asianosaisen suostumuksin.

Henkilöä koskevaa tietoa ei saa koskaan käyttää aineellisen tai aineettoman vahingon tuottamiseen tai kansalaiselle kuuluvien oikeuksien käytön rajoittamiseen tai estämiseen. Kansalaisoikeuksien rajoittaminen, joka perustuu sosiaalista alkuperää, rotua, kansallisuutta, kieltä, uskontoa tai puoluejäsenyyttä koskevaan tietoon, on kiellettyä ja lain mukaan rajoitettua.

Luonnolliset ja oikeushenkilöt, jotka käsittelevät, keräävät tai käyttävät henkilötietoja, kantavat Venäjän Federaation lainsäädännön mukaisen vastuun tiedon keräämistä, käsittelyä ja käyttöä koskevien määräysten rikkomisesta. Myös viranomaiset voidaan saattaa oikeuskäsittelyyn. Yksityisten järjestöjen, yritysten ja henkilöiden harjoittama henkilötietojen käsittely vaatii Venäjän Federaation lainsäädännön edellyttämää lisenssiä.

Vuoden 1995 lain lisäksi henkilötietojen käsite esiintyy uudemmissa laeissa, kuten verolaissa[183], työlaissa[184] sekä Federaation laissa, joka koskee siviilistatusta.

Vuoden 1995 laki tiedosta, tiedon käsittelystä ja suojaamisesta viittaa yksityiskohtaisempaan federaation lainsäädäntöön. Seikkaperäinen tietosuojalaki on edelleen valmisteilla. Näitä koskevat ehdotukset tehtiin 1998 ja 2000, mutta asiaa on täytynyt odottaa näihin päiviin asti. Tietosuojaa koskeva lakiesitys on kevään 2006 aikana ollut käsiteltävänä Venäjän duumassa ja etenee syksyllä 2006 toiseen käsittelyyn. Taustalla on Venäjän pyrkimys ratifioida Euroopan neuvoston tietosuojayleissopimus.

Ratifioinnin esteenä saattaa kuitenkin olla muita tekijöitä, kuten se, ettei Venäjän keskushallinnossa ole tietosuojaviranomaista. Sen sijaan alueellisia tietosuojaviranomaisia esiintyy. Tietosuojakysymyksiä on käsitellyt informaatioriitoja ratkaiseva vetoomuskamari, joka oli puolioikeudellinen, lehdistön tuella toimiva elin vähän kuten kotimainen Julkisen sanan neuvostokin. Presidentti Putinin hallinto kuitenkin lopetti tämän elimen toiminnan.

---

[183] Artikla 84, Osa I.

[184] Artiklat 85-90.

Venäjällä on esiintynyt merkittäviä henkilötietoihin liittyviä väärinkäytöksiä. Esimerkiksi vuonna 2003 erään miljoonia asiakkaita palvelevan teleoperaattorin koko asiakaskuntaa koskevat tiedot varastettiin ja niitä kaupiteltiin CD-levyillä.

Erityistä sähköiseen viestintään yksityiskohtaisesti puutuvaa tietosuojalainsäädäntöä ei Venäjällä myöskään toistaiseksi ole sen enempää kuin työelämän tietosuojalainsäädäntöä.

13.5.2 Kameravalvonta

Venäjällä ei tiettävästi ole lainsäädäntöä valvontakameroiden käytöstä, koska tietosuojalaki ja sen valvontamekanismit puuttuvat.

13.6 Sähköisten palvelujen tuottaminen

Tämän tutkimuksen muista maista poiketen Venäjällä ei ole tapahtunut voimakasta sähköisiä palveluja koskevan lainsäädännön kehittämistä. Silti monia uudistuksia on tapahtunut.

Venäjällä sallittiin sähköinen sopimustoiminta vuonna 1994 tehdyn siviililakiuudistuksen yhteydessä. Sähköisistä sopimuksista ei ole erityislainsäädäntöä, mutta Venäjän kuluttajansuojalain[185] määräykset ulottuvat verkkokauppaan kuluttajien kanssa.

Verkkotunnus ”.ru” on käytössä ja sen käyttöä koordinoi yksityinen organisaatio.[186] Internet-palveluntarjoajien vastuuta välittämästään sisällöstä tai linkeistä ei ole säännelty lailla.

Maassa on kuitenkin monia erityispiirteitä. Venäjällä toimivien Internet-palveluntarjoajien on rekisteröidyttävä Venäjän tietoliikenneministeriössä. Palveluntarjoajien on lisäksi saatava viranomaisilta lupa toiminnalleen. Lisäksi kaikki tietoliikenneyritykset mukaan lukien nettikahvilat, sähköpostipalvelut ja call centerit on rekisteröitävä.[187] Venäjän Federaation laki joukkotiedotusvälineistä säätää teleteksti-, videoteksti- ja muut tietoliikenneverkot joukkotiedotusvälineiksi. Laki säätää, että kaikki Internet-kotisivut, jotka käyttävät ”.ru”-verkkotunnusta, täytyy rekisteröidä viestintäministeriössä.

---

[185] Laki nro. 2-FZ, 9.1.1996.

[186] Englanninkieliseltä nimeltään Russian Scientific Research Institute for the Development of Public Networks (“RosNIIROS)

[187] Art. 15, Laki nro. N15-FA, 16.2.1995 tietoliikenteestä, Ross Gazeta No. 39, 22.2.1995 (muutettu lailla nro N8-FA, 16.1.1999 ja lailla nro 176-FA 17.7.1999).

Venäjällä julkaistavan Internet-sisällön on oltava laadittu kyrillisin aakkosin. Yksityisten järjestöjen ja yksityishenkilöiden, jotka harjoittavat markkinointia tai tilastollista tutkimusta ja harjoittavat tiedonsiirtoa tässä yhteydessä, on hankittava toimilupa.

13.7 Sähköiset allekirjoitukset ja tunnistaminen

Venäjän laki hyväksyi sähköiset allekirjoitukset ensimmäisen kerran jo vuonna 1994, jolloin Venäjän siviililakia täydennettiin hyväksymällä sähköisten asiakirjojen avulla tapahtuvat oikeustoimet.[188] Vuonna 2002 säädettiin liittovaltion laki sähköisistä allekirjoituksista.[189] Laki perustuu julkisen avaimen järjestelmään, ja siitä käytetään nimitystä GOST. Lain perusteella viranomaiset kontrolloivat järjestelmää mm. lisensioitujen varmentajien avulla. Lailla suljetaan pois biometristen menetelmien käyttö samoin kuin käsintehtyjen allekirjoitusten sähköisten analogioiden ja digitaalisten kuvausten käyttö. Hallituksen varmennuskeskukset todentavat ja vahvistavat sähköisten allekirjoitusten kuuluvan luonnolliselle tai oikeushenkilölle, kuten yhtiölle. Tämä onkin erityispiirre Venäjän sähköisiä allekirjoituksia koskevassa laissa.

Laki on kuitenkin osoittautunut toimimattomaksi, ja Venäjän informaatioteknologia- ja viestintäministeriö on todennut lain olevan muutoksen tarpeessa sillä sen soveltamiseksi on tarvittu alemmanasteisia säännöksiä eikä laki ole sopusoinnussa muun lainsäädännön kanssa.

Venäjällä on virallinen henkilöiden tunnistusjärjestelmä. Jokaisella 14 vuotta täyttäneellä täytyy olla henkilöllisyystodistus eli sisäinen passi, jonka myöntää sisäministeriön paikallisosasto. Sisäistä passia edellytetään juna- tai lentolippujen ostamiseen. Sisäinen passi sisältää oleskelulupaleiman eli ns. *propiskan*. Vaikka propiska-järjestelmä on todettu perustuslain vastaiseksi, voi sen puuttuminen saattaa asianosaisen vaikeuksiin paikallisten viranomaisten kanssa asioidessaan ja asioita hoitaessaan. Sähköisten henkilökorttien on odotettu täydentävän ja myöhemmin korvaavan sisäiset passit. Tarkoitus on aloittaa siten, että jokainen vastasyntynyt saisi sähköisen ID:n. Tarkoitus ei kuitenkaan olisi luoda uutta, keskitettyä tietokantaa.

---

[188] Sobr.Zakonod RF, 1994, Nro. 52 FZ; Nro. 32 (täydennetty 2003), Grazhdanskii Kodeks RF, artiklat 160 ja 434.

[189] Laki nro 1-FZ digitaalisista sähköisistä allekirjoituksista, Ross. Gazeta, 6.1.2002.

13.8 Tietoturva ja sähköiset palvelut aineellisessa lainsäädännössä

13.8.1 Pankkitoiminta ja rahanpesu

Pankkitoiminta on Venäjällä ollut kehitysvaiheessa yhteiskuntajärjestelmän muutoksen jälkeen eikä tietoturvallisuuden ja tietosuojan kehittäminen pankkitoiminnassa ole noussut painopisteeksi.

Sen sijaan rahanpesun ehkäiseminen on saanut Venäjällä lainsäätäjän huomion osakseen. G7-maiden ja rahanpesun ehkäisemistä edistävä Financial Actions Task Force (FATF) painostivat Venäjää hyväksymään lain rahanpesun ehkäisemisestä. Laki rahanpesun ja terrorismin rahoituksen ehkäisemisestä tuli voimaan 1.2.2002 ja sitä on muutettu vuonna 2004. Samassa yhteydessä luotiin aikaisemmasta elimestä liitto-valtion rahoituksentarkkailupalvelu (Federal Service of Finance Monitoring, FMS).

Laissa tarkoitettujen organisaatioiden, jotka suorittavat varojen siirtoa, on tunnistettava ne henkilöt, joille ne tarjoavat palvelua. Lisäksi niiden on, raportoitava sopivilla identifiointiasiakirjoilla ne transaktiot, jotka ovat pakottavan valvonnan piirissä ja lähetettävä edellytetyt tiedot FMS:lle seuraavan työpäivän aikana. Edellytettyjä tietoja ovat transaktion luonne ja päivämäärä sekä osapuolten identifiointi. Viranomaisella on lisäksi oikeus vaatia identifikaatiota koskevaa tietoa niissäkin tapauksissa, joissa ei ole pakollista raportointia. Identifikaatioasiakirjat sekä pakollisen raportoinnin asiakirjat tulee säilyttää viiden vuoden ajan. Pankeilla ei ole oikeutta avata nimettömiä pankkitilejä.

13.8.2 Hankintalainsäädäntö ja verkkolaskutus

Venäjän julkisia hankintoja koskeva lainsäädäntö on kehitteillä. Käytössä on ollut yleisiä hankintaehtoja ja yleinen kartellilakia on sovellettu myös hankintoihin. Sähköinen hankintatoimi ja verkkolaskutus eivät ole olleet erityisen ajankohtaisia kysymyksiä, mutta sähköinen tullausmenettely Suomen ja Venäjän rajalla on edellyttänyt myös sähköisen laskun hyväksymistä tietyssä laajuudessa. Lainsäädäntöä asiasta ei kuitenkaan ole.

13.9 Tietoturvallisuuteen liittyvät yleiset palvelut

Venäjällä ei ole yleistä tietoturvallisuusviranomaista. Venäjällä toimii kuitenkin mm. *RU-CERT*-niminen Computer Security Incident Response Team, jonka perusti vuonna 1998 Russian Institute for Public Networks. RU-CERT toimii yhteistyössä muiden maiden vastaavien elimien kanssa.