VAASAN YLIOPISTO
KAUPPATIETEELLINEN TIEDEKUNTA

TALOUSOIKEUS

Veli-Matti Ämmälä q87629

TIETOSUOJA SÄHKÖISESSÄ KAUPASSA

Talousoikeuden

pro gradu -tutkielma

VAASA 2011

Sisällysluettelo **sivu**

VAASAN YLIOPISTO

Kauppatieteellinen tiedekunta

Tekijä:	Veli-Matti Ämmälä
Tutkielman nimi:	Tietosuoja sähköisessä kaupassa
Ohjaaja:	Brita Herler
Tutkinto:	Kauppatieteiden maisteri
Oppiaine:	Talousoikeus
Linja	Yritysjuridiikka
Aloitusvuosi:	2007
Valmistumisvuosi	2011 **Sivumäärä:** 74

TIIVISTELMÄ

Tutkimuksessa tarkastellaan tietosuojaa ja sen tasoa sähköisessä kaupassa. Asioimisen ja kaupan käynnin lisääntyminen Internetissä on johtanut siihen, että kuluttajien on luovutettava henkilötietoja verkossa toimiville yrityksille. Seurauksena on ollut väärinkäytöksiä, ja siksi ihmisten huoli omasta tietosuojastaan on kasvanut. Myös uusien sähköisten palveluiden ilmestyminen markkinoille on tuonut mukanaan tietosuojaongelmia. Koska Internet on maailmanlaajuista, on yhteisten sääntöjen ja lakien laatiminen ollut haasteellista. Tutkimuksessa pyrin hahmottamaan nimenomaan kuluttajan tietosuojaa Suomessa, Euroopan unionin alueella ja Yhdysvalloissa.

Arvioin tutkimuksessa tietosuojaa oikeusdogmatiikan näkökulmasta. Hahmotan tietosuojaa tämän jälkeen alan kirjallisuuden perusteella niin kuluttajan kuin myös verkossa toimivan yrityksen näkökulmasta. Tarkoituksena on luoda lukijalle mahdollisimman yhtenäinen kuva tietosuojasta ja siitä, millaisin toimenpitein yritysten tulee huolehtia asiakkaidensa tietoturvasta. Lainsäädännöllä saadaan yritykset suojelemaan keräämiään henkilötietoja verkossa ja asettamalla ne korvausvelvollisiksi, saadaan nostettua luottamusta verkossa asioimista kohtaan. Tästä huolimatta ei tule luottaa sokeasti tietoturvan toteutumiseen verkossa, vaan on myös itse huolehdittava omasta tietosuojasta.

AVAINSANAT: Tietosuoja, sähköinen kauppa, tietoturva

LYHENTEET

HetiL	Henkilötietolaki 22.4.1999/524
SVTSL	Sähköisenviestinnän tietosuojalaki 16.6.2004/516
617/2009	Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista
458/2002	Laki tietoyhteiskunnan palveluiden tarjoamisesta
HE 36/2009	Hallituksen esitys laiksi vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista
412/1974	Vahingonkorvauslaki
EU	Euroopan unioni
ETA	Euroopan talousalue
ETY	Euroopan yhteisöjen tuomioistuin
KOM (97)157)	Euroopan parlamentin ja neuvoston elektronisen kaupankäynnin aloite
KOM 2008:614	Ehdotus Euroopan parlamentin ja neuvoston direktiivi kuluttajan oikeuksista
Direktiivi 2000/31/EY	Direktiivi tietoyhteiskunnan palveluja, erityisesti sähköistä kaupankäyntiä, sisämarkkinoilla koskevista tietyistä oikeudellisista näkökohdista
Direktiivi 2002/58/EY	Direktiivi henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla
Direktiivi 95/46/EY	Direktiivi yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta
Direktiivi 1999/93/EY	Direktiivi sähköisiä allekirjoituksia koskevista yhteistyön puitteista
AB 1950	Asembly bill 1950 -säännös

AB 68	Online Privacy Protection Act of 2003 –laki
E-Sign Act	Electronic Signature in Global and National Commerce Act
FTC	Federal Trade Comission
SB 27	Shine the hight –laki
UETA	Uniform Electronic Transactions Act
UNCITRAL	United Nations Comission on International Trade Law
USC	United States Constitution

1. JOHDANTO

Perheet ja yritykset käyttävät yhä enemmän Internetiä asioiden hoidossa. Sen merkitys maksuliikenteen välittäjänä ja ostosten tekemisessä on kasvanut viimeisen vuosikymmenen aikana valtavasti. Ihmiset, jotka suhtautuivat Internetiin skeptisesti, ovat joutuneet myöntämään, että se on hyödyllinen arkipäivän asioiden hoidossa. Ei ole ihme, että yritysten mielenkiinto tuottaa palveluja tällä alueella on suuri. Yritysten ei ole helppo vastata ihmisten alati kasvaviin vaatimuksiin ja huolehtia samalla elektronisen kaupan turvallisuudesta ja asiakkaiden tietosuojasta.

Elektronisella kaupankäynnillä tarkoitetaan Internetin välityksellä verkossa tapahtuvaa sähköistä kauppaa. Tarkoituksena on saattaa yhteen ostaja ja myyjä. Euroopan komissio on määritellyt sähköisen kaupan seuraavasti: ”Sähköinen kaupankäynti tarkoittaa sähköistä yritystoimintaa. Se perustuu datan sähköiseen käsittelyyn ja siirtoon. Sähköisen kaupankäyntiin sisältyy monia erilaisia osia, joita ovat mm. tuotteiden ja palveluiden sähköinen myyminen, digitaalisen sisällön välittäminen verkon kautta, sähköiset tilisiirrot, sähköinen osakekauppa, sähköiset huutokaupat, julkiset hankinnat, suorakuluttajamarkkinointi ja myynnin jälkeiset palvelut.” [1]

Kun ostaja haluaa ostaa materiaalisia tuotteita, on kyseessä epäsuora sähköinen kaupankäynti. Internetistä ladattavien maksullisten ohjelmien, niin sanottujen immateriaalituotteiden, ostaminen on taas suoraa sähköistä kaupankäyntiä. Kun tässä tutkimuksessa käytän käsitettä ”sähköinen kaupankäynti”, viittaan molempiin edellä mainittuihin. Yhteistä näille molemmille sähköisen kaupan tyypeille on korkea tietosuojan ja yhteyden vaatimustaso. Jos sähköisessä kaupassa liikuteltaessa rahaa, on ensiarvoisen tärkeää varmentua osapuolten henkilöllisyydestä tietojen salauksesta ja suojauksesta. Tämä on ensimmäinen askel siirryttäessä toteuttamaan tilausta tai maksutapahtumaa.

[1] Eurooppalainen elektronisen kaupankäynnin aloite, KOM(97)157).

1.1 Tutkimuskohteen kuvaus

Tietoturvallisuus muodostaa olennaisen edellytyksen Internetissä käytävälle kaupankäynnille. Usein myyjäyritys mainostaa itseään ja myytäviä tuotteitaan näkyvästi eri sivustoilla saadakseen näin mahdollisia ostajia vierailemaan omilla sivustoillaan. Monesti nämä vierailijat päätyvät tekemään kauppaa sellaisen yrityksen kanssa, josta he eivät tiedä muuta, kuin mitä yritys itse omilla nettisivustoillaan kertoo. Internet on maailmanlaajuinen ja sinne mahtuu paljon laillisia ja rehellistä kauppaa harjoittavia yrityksiä, mutta valitettavan paljon myös epärehellisiä toimijoita. Usein näillä on tarkoitus vain rahastaa asiakkaita ja jättää sovittu palvelu tai tuote toimittamatta. Lisäksi on niitä, jotka pyrkivät varastamaan asiakkaiden henkilö- ja maksutietoja ja yritysten asiakastietorekistereitä. Asiakkaan on arvioitava, onko se verkkokauppa, jossa hän haluaa asioida luotettava. Tämä koskee erityisesti niitä tilanteita, joissa on luovutettava omia tietoja.

Kun ostaja on tehnyt ostopäätöksen ja valinnut haluamansa tuotteen, tulee hänen ja myyjän tehdä sähköinen sopimus, joka on verrattavissa tavalliseen myymälässä tehtävään sopimukseen. Usein myös maksu tapahtuu tässä yhteydessä. Vaihtoehtoina myyjä voi tarjota ostoksen maksamista luottokortilla tai myyjän sivustolta suoraa linkkiä ostajan nettipankkiin, jossa ostaja tekee ostosopimuksen mukaisen tilisiirron myyjän pankkiin. Osapuolina sähköisessä kaupassa voi olla ostajan ja myyjän lisäksi molempien pankit, mahdollisesti luottokorttiyhtiö ja nettipalvelinta ylläpitävä yritys, jolta myyjäyritys on ostanut kyseisen verkkokaupan ylläpitopalvelun.

Sähköinen kaupankäynti on nykyään erittäin laajaa ja nopeasti kasvavaa. Sen merkitys yrityksille ja kuluttajille lisääntyy kaiken aikaa. Yhä useammalla ihmisellä ympäri maailmaa on mahdollisuus käyttää ja hyödyntää Internetin mahdollistamia palveluja. Tämä sähköisen aikakauden ympäristö, jossa elämme, painostaa yrityksiä kehittelemään yhä uusia tuotteita ja palvelukokonaisuuksia, joita on mahdollisuus kaupata verkossa. Tämä ilmiö vain lisää entisestään elektronisen kaupan merkitystä kauppapaikkana. Nykyään voi ostoksia tehdä omalta kotikoneelta, kannettavalta tietokoneelta puistossa tai mobiilimatkapuhelimella vaikkapa taksissa. Tällainen innovatiivisuuteen rakentuva verkkoympäristö mahdollistaa yrityksille yhä vain laajenevat markkinat ja samalla kuluttajille helposti lähestyttävän

kauppatapahtuman. Mutta uusia palveluita kehitettäessä myös ympäristö on tietosuojan kannalta entistä haavoittuvaisempi. Mikäli yritys haluaa olla mukana elektronisen kaupan kehityksessä ja saada itselleen siitä hyötyä, tulee sen panostaa tähän kehittyvään ja kaiken aikaa muuttuvaan Internet-ympäristöön.

Epäilemättä sähköisen kaupankäynnin merkitys yrityksille on kasvamassa. Sähköisestä kaupankäynnin liikevaihdosta vain noin 15 % on kuluttajakauppaa ja loput 85 % yritysten välistä B to B kaupan. Silti juuri kuluttajakaupassa yrityksille on tärkeää onnistua ja voittaa asiakkaiden luottamus, sillä se on päivittäin esillä lehdissä ja mukana ihmisten jokapäiväisessä arjessa. Erityisesti kuluttajille tietosuojamurroista aiheutuneita vahinkoja uutisoidaan näyttävin otsikoin mediassa. Juuri negatiiviset kokemukset ja uutiset jäävät kuluttajien mieleen valitettavan hyvin. [2]

Kuluttajille sähköinen kaupankäynti on tuonut myös monia hyötyjä. Se on saattanut jokaisen kuluttajan saataville tuotteita ja palveluja, joita aikaisemmin oli mahdollisuus saada vain suurkaupungeista. Myös hintojen on yleisesti todettu laskeneen sähköisessä kaupassa, sillä kyseissä kauppatapahtumassa jää usea välikäsi pois verrattuna siihen, että vastaava tuote ostetaan tavallisesta myymälästä. Sähköisen kaupan merkitys kuluttajalle on ennen kaikkea siinä, että tuote on helppo ostaa kotoa käsin, sen saa nopeasti kotiovelle ja hinta on edullinen.

Yhteiskunta edesauttaa myönteisen ilmapiirin kehittymistä sähköiselle asioimiselle, kun se ohjaa kansalaisiaan toimimaan yhä enemmän sähköisessä verkossa tarjoamalla siellä omia julkisia palvelujaan. Esimerkkinä mainittakoon veroviraston luoma mahdollisuus, että yksityishenkilö voi tehdä veroilmoituksen verkossa. Samalla yksityinen sektori panostaa koko ajan enemmän sähköiseen liiketoimintaan. Kun sähköisen asioimisen tulee koko ajan lähemmäksi kaikenikäisten ihmisten arkea, on siitä lyhyt matka siirtyä käyttämään myös yritysten tarjoamia maksullisia palveluja ja tekemään sähköistä kauppaa. Elektroninen liiketoiminta ja sitä kautta myös sähköinen kauppa lisääntyy mitä ilmeisimmin tulevaisuudessa ja verkkokaupan merkitys kauppapaikkana kasvaa.

[2] Aalto 2000: 13–14

Koska elektroninen kauppa on maailmanlaajuista, on käytettävien sääntöjen yhdenvertaistaminen ensiarvoisen tärkeää. Verkkopalveluiden rajaaminen vain tietyn valtion alueelle on lähes mahdotonta, koska sama palvelu on käytettävissä ympäri maailmaa eri valtioissa, myös niissäkin valtioissa, joissa suhtautuminen yksityisyyden ja henkilötietojen suojaan voi poiketa merkittävästi siitä, mihin olemme tottuneet.[3] Valtiot ja erilaiset kansalaisjärjestöt ovat vaatineet tietoturvallisuudelle yhteisiä sääntöjä ja minimitasoa suojelemaan yrityksiä ja kuluttajia. Tällaisena aktiivisesti vaikuttavana järjestönä voidaan mainita Internet Society. Tarkoituksena on ollut saada verkossa toimijoille minimiturvataso, jota olisi mahdollisuus myös kehittää edelleen teknologian niin salliessa.

Vaikka tietosuojalle ei ole yleisesti hyväksyttyä määritelmää on Laine kuvaillut sen kirjassaan seuraavasti: ”Tietosuojalla tarkoitetaan rekisteröidyn, kuten sähköisen kaupan asiakkaan, tarpeelliset henkilötiedot on saatu laillisesti, niitä käsitellään sähköisen kaupan rekisterissä oikein, eikä niitä käytetä tai luovuteta edelleen vastoin rekisteröidyn tahtoa tai hänen tietämättään”.[4] Keinoja, joilla voidaan pyrkiä estämään luvaton tunkeutuminen muiden järjestelmiin, täytyy kehitellä kaiken aikaa ja pyrkiä näin varmistamaan sähköisen kaupan luotettavuus. Erilaisilla salausmenetelmillä pyritään parantamaan turvallisuutta. Sähköinen allekirjoitus, joka on sarja turvallisuusominaisuuksia ja joita on vaikea toteuttaa muulla tavoin, on esimerkki varsin luotettavasta varmenneesta. Vaikka ongelmat sähköisessä kaupassa ovat globaaleja, kaikki valtiot eivät suhtaudu yhtä myönteisesti salausohjelmien yleiseen käyttöön ottoon, vaan vetoavat valtion turvallisuuteen. Tämä vaikeuttaa globaalien yhteisten sääntöjen muodostamista.

Suomea on usein pidetty tietoyhteiskunnan edelläkävijämaana, mutta viime aikoina tämä maine on saanut kolhuja mediassa kerrottujen tietomurtojen vuoksi. On uutisoitu, kuinka Suomi on jäänyt jälkeen kehityksestä eikä tietoliikenneturvallisuus ole tästä poikkeus. Puolustustaloudellisen suunnittelukunnan TIHA-ryhmä totesi raportissaan, että Suomesta puuttuvat lähes kokonaan tietoliikenneturvallisuuteen, tietojärjestelmien turvallisuuteen

[3] KOM 2008:614.

[4] Laine 2001: 166.

sekä tietoturvaloukkausten ja ongelmien havaitsemiseen ja ratkaisemiseen liittyvät operatiiviset toiminnot. [5]

Suomesta puuttuu yksinomaan tietoturvallisuutta ja kaikkia sen ulottuvuuksia käsittelevä yleislaki. Tietoturvallisuutta koskevia normeja löytyy sen sijaan hajallaan eri säädöksissä. Sähköisessä kaupassa asiakkaan on vaikea selvittää omia oikeuksiaan tilanteessa, jossa kuluttajan tiedot päätyvät vääriin käsiin. Verkossa sähköistä kauppaa harjoittavan yrityksen on otettava toiminnassaan ja asiakkaiden tietoja suojatessaan huomioon muun muassa sähköisen viestinnän osalta viestinnän tietosuojalaki, laki yksityisyydensuojasta tai henkilötietolaki. Lisäksi yrityksen toimintaa säätelee Euroopan yhteisön säätämä sääntelymekanismi.

Koska tietosuojan ydinaluetta ovat yksityisyyden suojaaminen ja henkilötietojen käsittelyn toimintatavat, tulee yrityksen toiminnassaan täyttää edellä mainittujen säädösten vaatimukset. Näin myyjä pyrkii luomaan sähköiselle kaupalle ja asiakkaalle turvallisen ympäristön. Sähköiseen kauppaan liittyvien rikosten rangaistuksista säädetään rikoslaissa. Riippuen siitä kuinka tietosuojaa on rikottu, selventävä säädös rangaistuksesta on etsittävä henkilörekisteririkoksia, tieto- ja viestintärikoksia koskevista luvuista. Merkitystä vahingonkorvausta harkittaessa on myös sillä, onko teko tahallinen vai huolimattomuudella aiheutettu.[6] Maksuvälinepetoksista löytyy myös oma lukunsa.

Suomessa sähköisen viestinnän tietosuojaa valvoo liikenne- ja viestintäministeriö. Sähköisen viestinnän tietosuojalain tarkoituksena on turvata sähköisen viestinnän luottamuksellisuus ja edistää viestinnän tietoturvaa ja palvelujen kehittymistä. Tavoitteena on löytää keinoja, joilla ministeriö pyrkii lisäämään tietosuojaa sähköisessä kaupassa.

Samalla kun sähköinen kaupankäynti on lisääntynyt nopeasti ja sen suosio on kasvanut kaikenikäisten Internetin käyttäjien keskuudessa, ovat myös siihen liittyvät ongelmat lisääntyneet. Puhuttaessa kaikesta siitä hyödystä, mitä sähköinen kaupankäynti voi tarjota, ei voi unohtaa asian toista puolta. Asioidessamme verkossa olemme alttiina monille tietoturvallisuuttamme uhkaaville tekijöille. Usein tietoturvaongelmia on paisuteltu eri medioissa

[5] Laine 2001: 155
[6] Neuvonen 2008: 72 -73

turhankin paljon. On kuitenkin totta, että tietomurrot ja väärinkäytökset ovat selvästi lisääntyneet ja näin kuluttajien tuntema pelko Internetin käyttöä kohtaan on ainakin osin perusteltua. Todennäköisyys joutua väärinkäytöksen kohteeksi on hyvin pieni verrattuna esimerkiksi siihen, että maksaa ravintolalaskun ulkomailla luottokortilla.

Luottamus on minkä tahansa kauppasopimuksen syntymisen peruspilareita. Sähköisessä kaupassa kuluttajien luottamus vastapuoleen ja viestinnän luottamuksellisuus korostuvat, kun ostaja ei voi fyysisesti nähdä vastapuolta. Tietoturva on erityisen tärkeä osatekijä kaupan molemmille osapuolille. Tilastokeskus teki vuoden 2000 alussa yrityskyselyn, jonka mukaan 30 % vastanneista 1700 suomalaisesta yrityksestä piti tietoturvallisuutta yleensä Internetin ja erityisesti sähköiseen kauppaan liittyvänä esteenä. Vain 6 % yrityksistä ei pitänyt Internetin tietoturvaa ongelmallisena. [7]

Jotta sähköinen kauppa toimii, täytyy molemminpuolisen luottamuksen olla kunnossa, mutta millä keinoin luottamus tietosuojaan voidaan rakentaa elektronisessa kaupassa? Yrityksen kannalta on erittäin tärkeää, että sen tietoturvajärjestelmät ovat moitteettomassa kunnossa ja ajan tasalla. Yrityksen maine luotettavana verkkokauppana on oltava myös yleisön tiedossa. Kuluttajat valitsevat mielellään kaupan, jonka he tuntevat jo entuudestaan ja jonka he mieltävät luotettavaksi toimijaksi. Yrityksen hyvä brändi edesauttaa sitä voittamaan asiakkaiden luottamuksen sähköisessä kaupassa.

Sähköisessä kaupassa tietoturvallisuus konkretisoituu normaalisti vasta tilaus- ja maksutilanteessa. Kun asiakas luovuttaa myyjälle henkilötietojaan tehdessään tilausta tai maksaessaan esimerkiksi luottokortilla, saa myyjä haltuun ostajan tietosuojalainsäädännön piiriin kuuluvia tietoja. Sähköisessä kaupassa nämä tiedot on tarkoitettu vain myyjän käyttöön, jotta tämä voi suorittaa sovitun palvelun. Liikkuessamme sähköisessä verkossa ja tehdessämme siellä ostoksia ongelmana on, että luovuttaessamme henkilötietoja tai luottokorttitietoja, joku kolmas taho pääsee käsiksi näihin luottamuksellisiin tietoihin ja käyttää niitä väärin. Rikollisten käsissä henkilöturvatunnus tai luottokorttitiedot voivat aiheuttaa suuria vaikeuksia ja rahallisia menetyksiä.

[7] Laine 2001: 131

Sähköisessä kaupassa turvallisuus voi vaarantua myös muusta syystä kuin ulkopuolisen luvattomasta tunkeutumisesta järjestelmään. Virheitä voi sattua verkkokaupan puolella. Järjestelmissä ja tietokoneohjelmissa voi ilmetä vika, puute tai palvelukatkos, joka mahdollistaa pääsyn järjestelmään ja asiakastietoihin. Asiakkaan tulee muistaa, että hän on myös itse vastuussa omasta tietoturvallisuudestaan. Verkossa tietoturva on aina suhteellista, ja asiakas voi parantaa omaa tietosuojaansa tekemällä oman osansa, ettei hänen tietonsa päätyisi vääriin käsiin. Tällä keinolla hän voi pyrkiä minimoimaan oman vastuunsa mahdollisen tietomurron sattuessa.

Tässä tutkimuksessa syvennyn sähköisen kaupankäynnin turvallisuuteen tietosuojanäkökulmasta. Kuinka voimme siis varmistua sähköistä kauppaa käydessämme, että luovuttamamme tiedot eivät altistu kyseiselle riskille? Entä jos tietosuoja pettää ja esimerkiksi luottokorttitiedot päätyvät vääriin käsiin? Kuinka voimassa oleva lainsäädäntömme turvaa oikeuksiamme? Kuka korvaa syntyneet vahingot vai jäävätkö ne asiakkaan omaksi tappioksi?

1.2 Tutkimusongelma ja rajaus

Tutkimuksessa tarkastelen asiakkaiden tietosuojan turvaamista sähköisessä kaupassa. Tarkastelun näkökulmana on muun muassa vastuukysymysten selvittäminen tilanteessa, jossa asiakkaan henkilötietoja tai maksuvälinetietoja päätyy väärinkäyttäjien haltuun. Tutkin, kenen on vastuu, jos tiedot päätyvät rikollisten haltuun verkkokaupan huolimattomuudesta tai asiakkaan omasta huolimattomuudesta.

Tarkoituksena on myös havainnollistaa, kuinka ammattimaista toimintaa henkilötietojen ja maksutietojen varastaminen ja väärinkäyttäminen voi olla. Rikollisilla on nykyään käytössään laitteita ja järjestelmiä, joilla he kykenevät purkamaan esimerkiksi verkkokaupan käyttäjien henkilötietosuojaus-järjestelmän. Tarkoituksena ei ole perehtyä järjestelmien teknisiin ominaisuuksiin vaan antaa lukijalle kuva sähköiseen kauppaan liittyvästä tietosuojariskin vakavuudesta sekä ottaa selvää, kuinka lainsäätäjä on ottanut omissa säädöksissään huomioon sähköisen kaupan haavoittuvuuden rikolliselle toiminnalle.

Lisäksi sivuan kevyesti vastuuaihetta eli millaisia vastuita osapuolilla eli asiakkaalla ja myyjäyrityksellä on korvata ja vastata syntyneistä vahingoista. Millä perusteilla sähköisessä kaupassa osapuolille asetetaan velvoitteita ja missä vastuut määritellään?

Tarkastelussa on tietosuojan loukkaus asiakkaan näkökulmasta. Lisäksi pyrin ottamaan selvää tietosuojaloukkauksen vaikutuksista yritykseen, josta tiedot ovat päätyneet kolmannen osapuolen haltuun. Tutkimuksessa selvitän, millaisilla keinoilla myyjän on mahdollista ja toisaalta myös velvollisuus suojautua ja suojata asiakkaiden tietoja. Lainopillisesta näkökulmasta tutkimusmetodina käytän voimassa olevaa oikeutta lähestyessäni tutkimuskohdetta ja -ongelmaa.

Lisäksi selvittelen laajaa suosiota varmenneena saaneen sähköisen allekirjoituksen pätevyyttä ja käytettävyyttä sähköisessä kaupassa. Sähköinen kauppa rajoittuu harvoin vain oman maan - tässä tapauksessa Suomen - omille markkinoille. Tästä syystä on tarpeellista selvittää, millainen suoja ostajalla on Euroopan yhteisön alueella vastaavissa tietosuojaongelmissa kuin Suomessa. Kuinka yhtenäinen vaatimustaso Euroopan yhteisön alueella on asetettu eri maissa toimiville sähköistä kauppaa harjoittaville yrityksille.

Lisäksi tarkastelen, millainen tietosuojataso kuluttajalla on Yhdysvalloissa. Se on syytä ottaa tutkimukseen mukaan, koska alue käsittää varsin merkittävän osan sähköisestä kaupasta: suuri osa sähköisestä kaupasta tapahtuu verkkokauppojen kanssa, jotka toimivat Yhdysvalloissa. Tutkimuksessa tarkastelu on rajattu nimenomaan Euroopan yhteisön ja Yhdysvaltojen alueelle, koska ne itsessään käsittävät erittäin suuren markkina-alueen. Suomalaisesta näkökulmasta voidaan olettaa, että suuri osa sähköisestä kaupasta rajoittuu juuri näiden kahden talousalueen sisälle.

Tutkimuksessa pääpaino on sähköisen kuluttajakaupan tietosuojassa ja sen osapuolten -myyjän ja ostajan- velvollisuuksissa ja oikeuksissa. Tarkastelussa rajaan ulkopuolelle tietosuojan piiriin kuuluvan tiedon muunlainen käyttömahdollisuus yrityksen liiketoiminnassa.

1.3 Tutkimuksen lähteet

Suomessa ei ole tietoturvasta erillistä yleislakia tai muuta sääntelyä. Tietoturvaa koskevaa lainsäädäntöä löytyy usean muun lain kohdista. Työssäni hyödynnän oikeuskirjallisuutta ja ajantasaista lainsäädäntöä. Myös lakien esitöitä käytetään hyväksi, jotta saadaan selville, mitä lainsäätäjä on tarkoittanut säädetyssä laissa.

Tutkimuksen kannalta merkittävimmät säädökset löytyvät sähköisen viestinnän tietosuojalaista (SVTSL) ja henkilötietolaista (HeTiL). Myös Suomea velvoittava Euroopan unionin lainsäädäntö, muun muassa tietosuojaa ja sähköistä kauppaa koskevat direktiivit, ovat hyödyllisiä tässä tutkimuksessa. Yhdysvaltojen lainsäädäntöön olen perehtynyt käyttämällä voimassa olevaa lainsäädäntöä ja alan kirjallisuutta.

Peruslähdeaineistona tutkimuksessa käytän kirjallisuutta. Oikeuskirjallisuutta hyödynnän, jotta saataisiin käytännönläheisempi näkökulma tarkasteltaessa tutkimuksessa käsitellyn aiheen lainsäädäntöä. Käytän sähköistä kauppaa käsittelevää kirjallisuutta ja aiheeseen liittyviä artikkeleita käytetään, jotta saataisiin kuva sähköisen kaupan ominaispiirteistä. Kun tarkistan sellaisia tietoja, jotka liittyvät tietosuojan ja tietoturvan järjestämiseen palveluntarjoajan näkökulmasta olen käyttänyt lähteenä Kettusen ja Fileniuksen kirjoittamaa teosta Elektroninen kaupankäynti. Verkkokaupan tietosuojasta ja siihen liittyvistä toimintamahdollisuuksista olen hakenut tietoa alan kirjallisuudesta. Lähteenä olen hyödyntänyt myös lehdissä julkaistuja aiheeseen liittyviä ajankohtaisia asiantuntijakirjoituksia.

1.4 Tutkimuksen rakenne ja eteneminen

Tutkimuksen johdannossa esittelen tutkimuksessa käsiteltävää aihealuetta yleisesti ja tutkimuksen tavoitteita ja rajauksia. Lisäksi selvitän tutkimuksen merkitystä kuluttajille ja yrityksille. Lopuksi esittelen, millainen on tutkimuksen rakenne, kuinka se etenee ja kuinka tutkimuksessa on hyödynnetty lähteitä.

Tutkimuksen toisessa pääluvussa perehdyn lainsäädäntöön, joka säätelee tietosuojan piiriin kuuluvien tietojen keräämistä, hyödyntämistä, siirtämistä ja

hallussapitoa. Tietoturvaa ja tietosuojaa tarkastelen Suomen lainsäädännön ja Suomea velvoittavan Euroopan yhteisön normiston sekä Yhdysvaltain lainsäädännön näkökulmasta. Luvussa määritellen pakottavan lainsäädännöllisen normiston, jolle sähköistä kauppaa harjoittavan yrityksen tietosuojanhallinnan tulee perustua. Tarkastelen, kuinka olemassa olevat velvoitteet ja kirjoitetut ja kirjoittamattomat säännöt turvaavat ja ennalta ehkäisevät esimerkiksi henkilötietojen väärinkäytöksiä. EU-direktiivien ja Suomen lainsäädännön lisäksi luvussa tukeudutaan hallituksen esityksissä ilmeneviin tietoihin.

Kolmannessa luvussa selvittelen, millainen on kuluttajan tietosuoja voimassa olevan lainsäädännön perusteella. Tarkoituksena on hahmottaa taustalla olevia syitä sääntelylle ja selventää, millaisia velvollisuuksia on sähköisen kaupan pitäjällä, kun se tekee kauppaa sähköisessä muodossa. Millainen tietoturva palveluiden järjestäjien tulee rakentaa suojelemaan esimerkiksi henkilö- ja tilitietoja? Käyn läpi tekijöitä, joista molempien osapuolten tulee huolehtia, jotta sähköisessä kaupassa syntyisi turvallinen ostotapahtuma. Tässä luvussa käsittelen myös niitä tekijöitä, joiden perusteella asiakkaalla on mahdollisuus saada vahingonkorvausta tietojen luvattomasta käytöstä. Luvussa hyödynnän Juha Laineen teosta Verkkokauppaoikeus. Luvussa kerrotaan myös sähköisen tunnistamisen muodoista ja niiden merkityksestä. Erityisesti kuvaan ”vahvan tunnistamisen” edellytyksiä, sen vahvuuksia ja käytettävyyttä. Luvussa käsitellyt tunnistamiseen liittyvät asiat perustuvat suurelta osin Euroopan unionin säätämään sähköisten allekirjoitusten direktiiviin ja Yhdysvaltojen UETA -mallilakiin sekä E-Sign Act -lakiin.

Neljännessä luvussa käsittelen henkilötietojen hallussapitoa, niiden siirtämistä EU-jäsenvaltioiden välillä ja niiden siirtämistä kolmansiin maihin. Millaisilla lainsäädännön perusteilla palveluntarjoaja voi pitää tietoja hallussaan ja käsitellä niitä? Luvussa selvennän, millaisia oikeuksia yrityksellä on siirtää rekisteritietojaan EU-alueella toisessa maassa olevalle toimijalle ja millaisia vaikutuksia tällä on lainsäädännön näkökulmasta. Luvussa on enimmäkseen käytetty hyödyksi Juha Laineen teosta Verkkokauppaoikeus sekä Markus Salmisen teosta Tietosuoja sähköisessä liiketoiminnassa.

Viidennessä luvussa perehdyn sähköisen kaupankäynnin uusimpaan haasteeseen. Luvussa tutustutaan mobiilipalveluiden erityispiirteisin tietosuojan kannalta. Millaisia vaikutuksia sillä on asiakkaan tietoturvaan ja

kuinka lainsäädäntö suhtautuu muun muassa mobiililaitteella suoritettuun asiakkaan tunnistamiseen.

Tässä toiseksi viimeisessä luvussa pyrin osoittamaan tietosuojajärjestelmän heikkouksia. Luvussa kuvaan myös niitä haasteita, joihin sähköisen kaupankäynnin tulee vastata eli keinoja, joita rikolliset käyttävät saadakseen haltuunsa käyttäjien tietoja. Lopuksi pohdin, millaisilla ennaltaehkäisevillä toimilla voitaisiin tietoturvaa parantaa. Luvussa on hyödynnetty Tietosuoja-lehden materiaalia.

Tutkimuksen viimeisessä luvussa tarkastelen tuloksia ja teen niiden perusteella johtopäätöksiä. Pyrin tiivistämään, millaisen tietoturvatason lainsäädäntö takaa meille ja millaista tietojen suojaa meillä on oikeus odottaa palveluiden tarjoajilta sähköisessä kaupankäynnissä.

2. SÄHKÖISEN KAUPANKÄYNNIN KEHITYS

Tietoverkossa tapahtuva sähköinen kauppa on kansainvälistä. Usein sopimuksia tehdään sellaisen osapuolen kanssa, joka on toisessa maassa, jopa toisella puolen maapalloa. Tämän vuoksi kuluttajaa suojaava lainsäädäntö voi poiketa totutusta oman maan kuluttajansuojasta. Ei voida olla varmoja, millainen suoja kuluttajalle kuuluu sopimukseen sovellettavan lain perusteella. Voidakseen valvoa omia etujaan osapuolten on tiedettävä minkä maan lainsäädäntöä sopimukseen sovelletaan. [8]

Sopimuksen osapuolet voivat omilla toimillaan vaikuttaa omaan oikeudelliseen asemaansa. Erityisesti kuluttaja voi vaikuttaa omaan asemaansa perehtymällä kyseiseen sopimukseen sovellettavan lain tarjoamaan kuluttajansuojaan. Tietoisuus omista oikeuksista koskien henkilö ja muita salassa pidettäviä tietoja on ensiarvoisen tärkeää.

2.1. EU-direktiivit

Euroopan unionin myötä ovat sen jäsenmaiden kuluttajansuojasäädökset lähentyneet huomattavasti toisiaan. EU on panostanut sähköisen kaupankäynnin pelisääntöjen yhtenäistämiseen alueellaan.[9] Se on asettanut tavoitteiksi luoda vapaa ja tehokas markkina-alue eli poistaa kaupan esteitä ja lisätä tiedon vapaata liikkumista. Tarkoituksena on ollut lisätä yritysten halukkuutta käydä kauppaa yli rajojen sekä lisätä kuluttajien luottamusta sisämarkkinoihin. Pyrkimyksenä on ollut näin edistää taloudellista kasvua alueella. Samalla yksilöiden tietosuojasta sähköisessä kaupassa on pyritty huolehtimaan.[10] EU on laatinut useita sen kaikkia jäsenmaita velvoittavia direktiivejä yhtenäistämään kuluttajien tietosuojaa ja henkilötietojen käsittelyä sähköisessä kaupassa. Seuraavassa tarkastelen lyhyesti niitä direktiivejä, jotka käsittelevät sähköiseen kaupankäyntiin liittyvää tietoturvaa.

[8] Luhtasela 2007: 269.
[9] KOM 2010:348. Vihreä kirja.
[10] KOM 2008:614 lopullinen.

2.1.2. Henkilötietojen suoja

Henkilötietodirektiivillä 95/46/EY Euroopan parlamentti ja neuvosto on pyrkinyt tietoturvallisuuden parantamiseen asettamalla henkilörekisterinpitäjä, esimerkiksi verkkokauppa, vastuuseen henkilötietojen suojaamistoimenpiteiden järjestämisestä eli tietojen turvallisesta säilytyksestä ja käsittelystä. Direktiivin tavoitteena on turvata yksilöille heidän perusoikeutensa ja erityisesti heidän oikeutensa yksityisyyteen henkilötietojen käsittelyssä. Samalla sen tavoite on huolehtia henkilötietojen vapaasta liikkuvuudesta jäsenvaltioiden välillä. Sähköisessä kaupassa tietosuojan piiriin kuuluvien tietojen joutuminen vääriin käsiin on usein harmillista, mutta myös vahingollista sille, jonka tiedot päätyvät väärinkäyttäjien haltuun. Kuluttajan ja palveluntarjoajan omien intressien mukaista on tietää, mitkä tiedot luetaan tietosuojan piiriin ja näin sopeuttaa omia toimintoja sen mukaan. Euroopan parlamentin ja neuvoston direktiivissä 95/46/EY:ssä on määritelty henkilötieto käsite:

"Henkilötiedoilla tarkoitetaan kaikenlaisia tunnistettua tai tunnistettavissa olevaa 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.” [11]

Direktiivin johdannosta ilmenevillä määritelmillä henkilötietojen käsite laajenee. Niiden perusteella henkilötiedoiksi määritellään kaikki kohtuullisesti saatavissa olevat tiedot palveluntarjoajalta itseltään tai mistä tahansa muualta. Merkitystä on siis sillä, kyetäänkö tiedot yhdistämään luonnolliseen henkilöön. Direktiivin mukaan tunnistetiedot määritellään henkilötiedoiksi, jos rekisteröity on tunnistettavissa luonnolliseksi henkilöksi. Selaillessamme Internetiä ja tehdessämme ostosopimuksen sähköisessä kaupassa tallentuu meidän toimista koneelle evästeitä, jotka myös ovat direktiivin perusteella luettavissa henkilötiedoiksi.

Asioidessamme verkossa tulemme luovuttaneeksi itsestämme tietoja vaikkapa täyttäessämme tilauslomaketta verkkokaupassa. Jotta palveluntarjoajalla olisi

[11] Direktiivi 95/46/EY:6.

oikeus käyttää saamiaan tietoja, tulee yksilön ensiksi antaa sille suostumus. Tämä onkin tavallisesti edellytys sopimuksen syntymiselle. Direktiivi asettaa kuitenkin edellytykset myös sille informaatiolle, mitä verkkokaupan tulee yksilölle antaa.[12]

Komissio velvoittaa jäsenvaltiot säätämään kansallisen lakinsa henkilötietoja suojaavalla tavalla. Direktiivissä säädetään tietojen laatua koskevat periaatteet. Yksilöstä saatujen tietojen tulee olla laillisesti hankittuja, niitä tulee käsitellä asianmukaisesti ja niitä saa säilyttää vain sen ajan, kuin on tarpeen sen perusteella, miksi ne on kerätty. Tietojen tulee olla oikeita ja virheelliset tiedot on oikaistava tai poistettava palvelunharjoittajan rekisteristä. Tämän lisäksi direktiivissä on tietojen käyttötarkoitukseen liittyvät periaatteet, joita verkkokaupan tulee noudattaa:

a) henkilötietoja käsitellään asianmukaisesti ja laillisesti,

b) henkilötiedot kerätään tiettyä nimenomaista ja laillista tarkoitusta varten, eikä niitä myöhemmin saa käsitellä näiden tarkoitusten kanssa yhteen sopimattomalla tavalla,

c) henkilötiedot ovat asianmukaisia, olennaisia eivätkä liian laajoja siihen tarkoitukseen, mihin ne on kerätty ja missä niitä myöhemmin käsitellään,

d) henkilötiedot ovat täsmällisiä ja tarvittaessa päivitettyjä; on tehtävä kaikki mahdollinen sen varmistamiseksi, että niihin tarkoituksiin nähden virheelliset tai puutteelliset tiedot, joita varten tiedot kerättiin tai joissa niitä myöhemmin käsitellään, poistetaan tai oikaistaan,

e) henkilötiedot säilytetään muodossa, josta rekisteröity on tunnistettavissa ainoastaan sen ajan, kuin on tarpeen niiden tarkoitusten toteuttamista varten, joita varten tiedot kerättiin tai joissa niitä myöhemmin käsitellään.[13]

Direktiivissä rekisterinpitäjä velvoitetaan huolehtimaan henkilötietojen suojelemisesta teknisten ja organisatoristen toimenpitein. Palveluntarjoajan hallussa olevien henkilötietojen on oltava turvassa luvattomalta käsittelyltä ja siirtämiseltä. Mikäli näin ei ole, on siitä seurauksena korvausvastuu.

[12] Pöysti 1999: 437.
[13] Direktiivi 95/46/EY:6.

Kuluttajalla on direktiivin perusteella oikeus saada palveluntarjoajalta eli rekisterinpitäjältä korvaus aiheutuneesta vahingosta. Vahinko voi olla aineellista ja taloudellista, mutta myös henkistä kärsimystä. Korvauksen edellytyksenä on, että kuluttajalle on aiheutunut vahinkoa tietosuojan piiriin kuuluvien tietojen laittomasta käsittelystä tai käytöstä. Vahingonkorvausperusteet määräytyvät kunkin kansallisen vahingonkorvauslainsäädännön mukaan.[14] Palveluntarjoajalla on todistustaakka vapautuakseen korvausvastuusta eli sen pitää näyttää toteen, ettei tietojen joutuminen vääriin käsiin ole johtunut sen järjestelmissä olevista tietoturva-aukoista tai huolimattomuudesta. Komissio on myös velvoittanut jäsenvaltiot laatimaan sanktiot direktiivin säädösten noudattamatta jättämisestä ja rikkomisesta.

EU:n pyrkimyksenä on edistää alueellaan vapaata tietojen kulkua ja vapaata tietojen siirtämistä jäsenvaltioiden välillä. Yhteinen EU-lainsäädäntö toki turvaa lähes yhtäläisen tietosuojatason koko EU-alueella. Rekisterinpitäjän on lupa luovuttaa tietoja alueen ulkopuolelle kolmansiin maihin vain, jos kyseisessä maassa taataan tietosuojan riittävä taso. Kyseinen direktiivi 95/46/EY velvoittaa, että jäsenvaltiot myös asettavat erillisen valvojanviranomaisen valvomaan direktiivin toteutumista sekä tarvittaessa lopettamaan direktiivin vastaisen toiminnan. [15]

2.1.3. Sähköisten palvelutarjoajien velvollisuudet

Komissio on säätänyt sähköisen viestinnän tietosuojadirektiivin 2002/58/EY, jota sovelletaan erityisesti sellaisten henkilötietojen käsittelyssä, jotka liittyvät sähköisten viestintäpalveluiden tarjoamiseen verkossa. Direktiivi täydentää suurelta osin henkilötietodirektiiviä 95/46/EY, mutta muutamia sähköisen kaupan tietosuojaa koskevia yksityiskohtia on hyvä mainita. Direktiivi velvoittaa sähköisten viestintäpalveluiden tarjoajan seuraavaan:

”Yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajan on toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet varmistaakseen tarjoamiensa palvelujen turvallisuuden, verkon turvallisuuden

[14] Luhtasela 2007: 334.
[15] Direktiivi 95/46/EY:6.

osalta tarvittaessa yhdessä yleisen viestintäverkon tarjoajan kanssa. Näillä toimenpiteillä on voitava varmistaa riskiin suhteutettu turvallisuustaso ottaen huomioon uusin tekniikka ja toimenpiteiden käyttöönottokustannukset."

Palveluntarjoaja velvoitetaan myös informoimaan käyttäjää, jos palvelun käyttöön liittyy erityinen riski. Direktiivissä määritellään tietoturvaan liittyvä termi "liikennetiedot" eli tiedot, joita käsitellään sähköisessä viestintäverkossa välitettävää viestintää tai laskutusta varten. Direktiivillä kielletään kaikenlainen henkilötietojen tai liikennetietojen sieppaaminen ja väärinkäyttö.[16]

2.1.4. Sähköinen kaupankäynti

Komission päämääränä on sähköisen kaupankäynnindirektiivillä 2000/31/EY ollut, että sen jäsenvaltiot huolehtivat kansallisella lainsäädännöllä tietoyhteiskuntapalveluiden turvallisuudesta mukaan lukien sähköinen kauppa. Väärinkäytökset on pyrittävä estämään ja lopettamaan mahdollisimman nopeasti lain mahdollistamilla turvaamistoimenpiteillä. Lainsäädännön edellyttämillä oikeussuojakeinoilla pyritään varmistamaan, että asianosaisille ei koidu taloudellisia vahinkoja tai muuta haittaa.[17]

Jäsenvaltiot on velvoitettu järjestämään tehokas valvonta, jotta direktiivin velvoittamat säädökset toteutuvat ja niitä noudatetaan. Mikäli verkkokauppapalveluidentarjoajat pitävät henkilötietorekisteriä, niiden on ilmoitettava itsestään direktiivissä vaaditut tiedot mukaan lukien, kuinka palveluntarjoaja on järjestänyt kuluttajien tietosuojan ylläpidon ja säilytyksen. Kuluttajan kannalta on myönteistä, että jäsenvaltioiden on yhtenäistettävä lain edellyttämiä vaatimuksia juuri yksilön tietosuojan turvaamiseksi. Kansallisten valvontaviranomaisten on toimittava yhteistyössä ja pyrittävä neuvomaan ja auttamaan toisen maan valvontaviranomaista tai yksittäistä kuluttajaa sähköisessä kaupassa ilmenevissä ongelmissa.

[16] Direktiivi 2002/58/EY.
[17] Direktiivi 2000/31/EY.

2.2. Suomen lainsäädäntö

Suomen lainsäädännössä on perustuslailla ja eduskunnan säätämillä erityislailla pyritty turvaamaan yksilön tietosuoja tämän toimiessa verkossa. Lainsäädännössä on otettu huomioon Euroopan unionin säätämät Suomea velvoittavat direktiivit. Näin on saatu aikaan yksilön oikeuksia turvaava sekä palveluntarjoajia velvoittava säännöskokoelma. Tarkastelen seuraavassa lyhyesti tietosuojan kannalta keskeisiä lakeja sekä yksilöä ja palveluntarjoajaa koskevia oikeuksia ja velvoitteita.

2.2.1. Tietosuojan yleislaki

Sähköisenkaupan tietosuojan piiriin kuuluvien yksilön henkilötietojen käsittelystä säädetään henkilötietolailla (523/1999). Henkilötiedoilla tarkoitetaan luonnollisen henkilön ominaisuuksia tai elinolosuhteita kuvaavia merkintöjä esimerkiksi henkilötunnusta. Henkilötiedoksi on laajasti katsottuna luettava kaikki henkilöön yhdistettävissä oleva tieto, jota palveluntarjoaja toiminnassaan käsittelee. Laki velvoittaa rekisterinpitäjältä henkilötietoja käsiteltäessä huolellisuutta, tietojenkäsittelyn suunnitelmallisuutta sekä käyttötarkoitussidonnaisuutta. Lisäksi tällä on informaatiovelvollisuus kertoa tietoja itsestään sekä toimintatavoista ja periaatteista, jotka koskevat henkilötietojen käsittelyä. Rekisterinpitäjän on tehtävä tarpeelliset tekniset ja organisatoriset toimet rekisteröityjen asiakkaittensa henkilötietojen suojaamiseksi. Rekisterinpitäjälle on asetettu vahingonkorvausvelvollisuus, mikäli rekisteröidylle koituu taloudellista tai muuta vahinkoa ja se johtuu rekisterinpitäjän lain vastaisesta henkilötietojen käsittelystä.[18]

[18] 523/1999. Henkilötietolaki.

2.2.2. Tiedonantovelvollisuus

Laki 458/2002 perustuu Euroopan parlamentin ja neuvoston sähkökauppadirektiiviin, jonka tarkoituksena on edistää sähköistä kaupankäyntiä sisämarkkinoilla. Sähköisen kaupankäynnin tietosuojan kannalta laissa säädetään palveluntarjoajan velvollisuudesta antaa tietoja itsestään, sopimusta koskevien sähköisten muotovaatimusten täyttämisestä ja välittäjänä toimivien palveluntarjoajien vastuuvapaudesta. Laissa määrätään sellaisen viranomaisen asettamisesta, jolle kuuluu muun muassa edellä mainittujen velvoitteiden noudattamisen valvonta sekä kuluttajien informointi muun muassa tietosuojaa koskevissa asioissa. Suomessa kyseinen viranomainen on Viestintävirasto, jonka puoleen kuluttaja ja yritys voivat ongelmatilanteissa kääntyä.[19] Lain perusteella esimerkiksi verkkokaupalla on yleinen tiedonantovelvollisuus. Palveluntarjoajan tulee ilmoittaa nimi, osoite sijoittautumisvaltiossa, yhteystiedot, yritys- ja yhteisötunnus tai muu vastaava tunnus. Lisäksi lailla säädetään seikoista, joita palveluntarjoajan on ilmoitettava kuluttajalle tilauksen yhteydessä. Lain perusteella verkkokaupan tulee lähettää tilauksen tekijälle myös vastaanottoilmoitus tilauksesta. Kyseisellä lailla on pyritty lisäämään kuluttajan turvallisuutta oston ja tilauksenteon yhteydessä. Kun kuluttaja saa lain määräämät tiedot palveluntarjoajasta, hänellä on paremmat edellytykset muodostaa käsitys osapuolen luotettavuudesta sopimuskumppanina.[20]

2.2.3. Tietoturvasta huolehtimisen velvoite

Sähköisen viestinnän tietosuojalaki (516/2004) on sähköisen viestinnän yleislaki alueella mutta myös erityislaki henkilötietojen käsittelystä verkossa. Sitä sovelletaan mm. verkossa tapahtuvaan viestintään. Se sisältää velvoitteita lähinnä palveluntarjoajalle, jotta tämä voisi järjestää tietoturvan kannalta turvallisen palvelun. Tarkoitus on varmistaa yksityisyyden suojan toteutuminen sekä viestinnän tietoturva, jolla laissa tarkoitetaan hallinnollisia ja teknisiä toimia. Näiden avulla palveluntarjoajan pitää kyetä varmistamaan, että

[19] Viestintävirasto.

[20] 458/2002. Laki tietoyhteiskunnan palvelujen tarjoamisesta.

tietosuojapiiriin kuuluvat luottamukselliset tiedot ovat vain niihin oikeutettujen saatavilla. Laki velvoittaa teleyrityksiä ja palveluidentarjoajia huolehtimaan palveluidensa turvallisuudesta. Velvoite edellyttää palveluntarjoajilta toimia, joilla toiminnan ja tietoliikenteen turvallisuus, laitteiston ja ohjelmien ja rekistereiden turvallisuus kyetään varmistamaan. Lain mukaan esimerkiksi laitteisiin ja järjestelmiin pääsyä on valvottava, tietojen ja järjestelmien luvaton käyttö estettävä ja tiedot ja järjestelmät suojattava tietoturvaa vaarantavilta tekijöiltä. Lisäksi laissa kielletään tunnistetietojen suojauksen purkavan järjestelmän hallussapito tai käyttäminen, poikkeustapauksia lukuun ottamatta.[21]

Laissa on säädetty rangaistuksista, jotka rikoslain mukaan seuraavat viestintäsalaisuuden loukkaamisesta. Sähköisen viestinnän tietosuojalain perusteella se joka tahallaan

1) rikkoo laissa säädettyä teknisen suojauksen purkavan järjestelmän tai sen osan hallussapitoa, maahantuontia, valmistusta tai levittämistä koskevaa kieltoa,
2) laiminlyö laissa säädetyn velvollisuuden huolehtia palvelujensa tai tunnistetietojen ja paikkatietojen käsittelyn tietoturvallisuudesta,
3) käsittelee tunnistetietoja tai paikkatietoja laissa säädetyn vastaisesti,

on tuomittava sähköisen viestinnän tietosuojarikkomuksesta sakkoon, jollei teosta muualla laissa säädetä ankarampaa rangaistusta. Rangaistus ei lain mukaan seuraa, jos rikkomus on vähäinen.[22]

2.2.4. Vahva tunnistaminen ja sähköinen allekirjoitus

Lain 617/2009 tarkoituksena on luotettavan sähköisen asioinnin mahdollistaminen.[23] Se sisältää edellytyksiä, joita tunnistusmenetelmällä tulee olla, jotta se on vahva. Lisäksi se säätää vaatimuksia palveluntarjoajalle. Lain toteutumista valvoo Viestintävirasto. Menetelmälle asetettujen vaatimusten lähtökohtana on huolellinen esitunnistaminen esimerkiksi poliisin myöntämistä

[21] Niskanen 2010: 518 – 521.
[22] 516/2004. Sähköisen viestinnän tietosuojalaki. Katso myös HE 125/2003.
[23] 617/2009. Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista.

henkilöllisyyden osoittavista asiakirjoista. Tunnistusmenetelmän on voitava yksiselitteisesti tunnistaa tunnistusvälineen haltija tietyksi henkilöksi. Menetelmän tulee olla myös turvallinen ja luotettava, kun otetaan huomioon tekniikan ja sen kehityksen mahdollistamat tietoturvauhat.

Vahvan sähköisen tunnistamisen tulee perustua vähintään kahteen seuraavista: salasanaan tai johonkin muuhun sellaiseen, minkä tunnistusvälineen haltija tietää; sirukorttiin tai vastaavaan tunnistusvälineeseen, joka haltijalla on hallussaan; sormenjälkeen tai muuhun ominaisuuteen, joka yksilöityy tunnistamisvälineen haltijaan. Esimerkkinä vahvasta tunnistamisesta on sähköinen allekirjoitus, joka liittyy yksiselitteisesti sen allekirjoittajaan ja joka on vain hänen valvonnassaan. Myös kirjautuminen eräisiin viranomaispalveluihin henkilön pankkitunnuksilla on viranomaisen keino tunnistaa yksilö vahvasti. Tämä menetelmä onkin lisännyt kuluttajien luottamusta verkkopalveluiden käyttöä kohtaan.[24] Hallituksen esitöistä käy ilmi, että myös oikeustoimen tekemiseen tarvittava tahdonilmaisu voidaan saada aikaan vahvan tunnistamisen menetelmällä, ellei oikeustoimella ole erityisiä muotovaatimuksia. [25]

Laissa on kerrottu tunnistusvälineen haltijan eli esimerkiksi kuluttajan vastuusta tilanteessa, jossa tunnistusvälinettä on käytetty luvatta haltijan tietämättä tilanteessa, jossa se on kadonnut tai varastettu, ja se on johtunut haltijan huolimattomuudesta tai haltija on luovuttanut itse tunnistusvälineen tai hän on laiminlyönyt velvollisuuden ilmoittaa sen katoamisesta. Edellä mainitun kaltaisissa tilanteissa on haltija itse vastuussa syntyneistä vahingoista. Esimerkkinä voidaan mainita tilanne, jossa henkilö huolimattomuuttaan kadottaa verkkopankkitunnuksensa ja kolmas taho pääsee niihin käsiksi ja niiden avulla kirjautuu verkkopankkiin.[26]

[24] Niskanen 2010: 457
[25] Aato 2000: 61 -70. Katso myös HE 36/2009.
[26] 617/2009. Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista.

2.3. Tietosuojalainsäädäntö Yhdysvalloissa

Liitovaltion lainsäädäntö poikkeaa huomattavasti siitä, mihin olemme tottuneet Euroopan unionin alueella ja sitä kautta Suomessa. Yhdysvalloista puuttuu yhtenäinen liitovaltiotason lainsäädäntö, joka turvaisi kuluttajien henkilötietoja ja tietoturvaa. Oikeudellinen sääntely koostuu pääasiassa jokaisen osavaltion omasta lainsäädännöstä, mikä tekee kokonaisuudesta rikkonaisen. Käytännössä tietosuojasääntely perustuu liittovaltion rajoittuneisiin säännöksiin, tuomioistuinten oikeuskäytäntöön, osavaltioiden omaan lainsäädäntöön sekä yritysten itsesäätelyyn.[27]

Liittovaltion tietosuojaa koskeva sääntely on laadittu koskemaan yksittäisten ongelmien ratkaisemiseen, minkä takia sen soveltaminen on vaikeaa. Käytännössä ainoa kaikkia osavaltioita koskeva tietosuoja-laki on henkilötietojen keräämisestä alle 13-vuotiailta. Laki ei anna suojaa sitä vanhemmille henkilöille, mikä tekee siitä varsin rajoittuneen. Yritysten itsesäätely tietoturva-asioissa on edennyt yritysten omien intressien mukaan eikä esimerkiksi kuluttajien etuja silmälläpitäen. Tämän lisäksi Yhdysvalloista puuttuu yleinen tietosuojan valvontaviranomainen, jonka pääasiallisena tehtävänä meillä on ajateltu olevan kuluttajien etujen valvominen ja edistäminen. Liittovaltion lainsäädäntö ei kyseistä viranomaista vaadi ja sen vuoksi se on jokaisen osavaltioiden oman harkinnan varassa.[28]

Kalifornian osavaltio on kehittänyt omaa tietosuojalainsäädäntöä turvaamaan kuluttajien henkilötietoja ja asettanut yrityksille lainsäädännöllisiä velvollisuuksia huolehtia henkilötiedoista. Kalifornian tietosuojalainsäädäntö parantaakin huomattavasti kuluttajien henkilötietoihin kohdistuvaa tietoturvaa. Osavaltio on myös perustanut neuvoa-antavan tietosuojaviranomaisen palvelemaan kuluttajia. Kalifornian lainsäädäntöä voidaan pitää tällä oikeuden alalla liittovaltion edistyksellisimpänä. Sillä onkin varsin suuri merkitys koko Yhdysvaltojen tietosuojalainsäädäntöön koska osavaltio on talousalueena varsin suuri. Osavaltion säännökset koskevat määrällisesti erittäin suurta osaa sähköisen kaupan alalla toimivista yrityksistä, käsittäen niin kalifornialaiset kuin myös muissa osavaltioissa toimivia yrityksiä, jotka keräävät tietoja tai joilla on tietokannoissaan henkilötietoja kalifornialaisista henkilöistä.

---

[27] Luhtasela 2007: 351-352.

[28] Luhtasela 2007: 352-357.

Näin ollen Kalifornian tietosuojalainsäädäntö on tärkeässä roolissa harjoitettaessa sähköistä kauppaa Yhdysvalloissa. Tämän vuoksi syvennyn tutkimuksessani liittovaltion tason lainsäädännön lisäksi Kalifornian osavaltion tietosuojalainsäädäntöön.

2.3.1. Henkilötietojen kerääminen alle 13-vuotiailta

Ainoa kaikkia osavaltioita velvoittava henkilötietoja turvaava tietosuojalaki on Children's online privacy protection act -laki. Sen on tarkoitettu sovellettavaksi tilanteissa, joissa alle 13-vuotailta henkilöiltä kerätään tietoja Internetissä. Laki säädettiin 1998 koskemaan verkkosivustoja, jotka toimivat Yhdysvalloissa, tai ulkomailla olevia sivustoja, jotka pyrkivät saamaan yhdysvaltalaisten lasten henkilötietoja. Erikoisuutena laissa on, että tavallisten lasta koskevien henkilötietojen lisäksi, myös lapsen huoltajan henkilötiedot luetaan laissa tarkoitetuiksi henkilötiedoiksi. Tähän sisältyy henkilön yhteystiedot ja muut tiedot, joiden avulla yhteydenotto on mahdollista.

Lainsäätäjä on velvoittanut yritykset huolehtimaan henkilötietojen luotettavasta käsittelystä, säilyttämisestä sekä niiden yleisestä luottamuksellisuudesta. Yrityksillä on itsellään velvollisuus järjestää kohtuulliset tietoturvatoimenpiteet, joiden avulla kerätyt tiedot pysyvät turvassa. Tätä tehostaakseen lainsäätäjä on asettanut sähköisen kaupan omistajan vastuuseen tietoturvallisuuden järjestämisestä. Yrityksiä velvoittavia toimenpiteitä valvomaan on laissa asetettu Federal Trade Comission (FTC). FTC:n tehtävänä on myös kyseisen lain tulkitseminen ongelmatilanteissa ja sen täydentäminen.[29]

Children online privacy protection act -laki säätää, että verkkokauppojen tulee saada ennen lapsen henkilötietojen keräämistä lapsen huoltajan lupa tietojen keräämiseen. Yritys saa kuitenkin kerätä huoltajaa koskevat tiedot lapselta hankkiakseen luvan huoltajalta. Kerättävien tietojen on oltava määrällisesti oikeassa suhteessa siihen tarkoitukseen, mihin niitä tullaan käyttämään sekä käyttötarkoitukseen nähden relevantteja. Lisäksi kerättyjä tietoja saa käyttää vain ennalta ilmoitettuun tarkoitukseen. Mikäli alkuperäinen tietojen käyttötarkoitus kuitenkin muuttuu oleellisesti, on lupa henkilötietojen käyttöön hankittava uudestaan.

[29] USC: Chap. 91 Sec. 6502

Lain perusteella huoltajalla on oikeus tarkistaa lapsen antamat tiedot sekä kieltää niiden käyttö ja vaatia niiden poistamista rekisteristä, sillä automaattista velvollisuutta yrityksellä ei ole tietojen poistamiseen. Laki asettaa myös verkkosivustoille varsin laajan informaatiovelvollisuuden. Yrityksen tulee ilmoittaa selkeästi sivustoillaan ja suoraan lapsen huoltajalle kerättävien tietojen keräykseen, käyttöön ja tietojen eteenpäin välittämiseen liittyvät periaatteet.[30]

Children online privacy protection act -laki turvaa lasten henkilötiedot varsin tehokkaasti asettamalla verkkokaupan vastuuseen lain vastaisista toimista. Samalla liittovaltion ainoa tietosuojalaki huolehtii vain alle 13-vuotiaiden lasten henkilötiedoista ja jättää suurimman osan sähköisiä palveluja käyttävistä ihmisistä täysin vaille tietosuojaa. Tämä on merkittävä puute kuluttajien tietosuojassa. Lisäksi se, että laki ei edellytä yritystä poistamaan rekisteristä henkilötietoja, joita se ei enää käytä voidaan pitää tietoturvauhkana rekisteröidylle. Samalla kyseinen laki koskettaa vain murto-osaa sähköisenkaupan yrityksiä.[31]

2.3.2. Tietojen luvattoman käytön estäminen

Kalifornian osavaltiossa säädetty Asembly bill 1950 -säännös velvoittaa yritykset turvaamaan ulkopuolisilta sellaiset henkilötiedot, jotka ne ovat saaneet haltuunsa sähköisen kaupankäynnin yhteydessä. Yrityksen tulee itse arvioitava ja ratkaistava, millaisilla tietosuojausratkaisuilla henkilötiedot ovat suojassa luvattomalta käytöltä ja paljastumiselta.

Suojattavaksi henkilötiedoiksi säännöksessä luetaan muun muassa nimi, henkilötunnus, pankki/luottokortin tai tilinumero. Huomattavaa on, että yrityksen on hävitettävä edellä mainitut tiedot, mikäli se ei enää niitä tarvitse. Yritykset on velvoitettu myös takaaman, että tietosuojantaso jatkuu, mikäli henkilötiedot luovutetaan laillisesti kolmannelle osapuolelle.[32]

AB 1950 säännös parantaa kuluttajien tietosuojan tasoa sähköisessä kaupassa, mutta samalla se luo velvoitteita sähköisen kaupan alan yrityksille. Yritysten

[30] USC: Chap. 91.
[31] Luhtasela 2007: 352-357.
[32] California Civil Code: Sec. 1798.81.5.

tulee huolehtia rekistereidensä tietoturvasta, mutta säännös jättää suojauksen tason määrittelemisen yritysten itsensä päätettäväksi. Valvontaviranomaisen puuttuessa tämä merkitsee suurta pelivaraa suojauksen käytännön toteutuksessa ja sen seurauksena henkilöiden tietoturvassa.[33]

2.3.3. Henkilötietojen luovutus

Kaliforniassa 1.1.2005 voimaan astunut Shine the hight -laki (SB 27) säätelee henkilötietojen luovuttamista eteenpäin suoramarkkinointitarkoituksessa. Laki antaa kuluttajalle oikeuden saada tietää, mikäli yritys on kuluvan vuoden aikana luovuttanut henkilötietoja tai muita tietoja kolmannelle osapuolelle suoramarkkinointitarkoitukseen. Lisäksi kuluttajan tulee saada tietää tietoja saaneen yrityksen toimiala. Lain velvoittamina yrityksien on järjestettävä asiakkaille mahdollisuus kysyä itseään koskevia tietoja sekä annettava kyseiset tiedot kuluttajille 30–150 vuorokauden kuluessa. [34]

Verkkokaupalle on laissa annettu mahdollisuus välttää kyseinen, melko vaativa tiedonantovelvollisuus. Tällöin yrityksen tulee ilmoittaa verkkosivuillaan, ettei luovuta henkilötietoja ilman asiakkaan lupaa (opt-in), jolloin sen tulee tarjota asiakkaalle mahdollisuus kieltää tietojen luovuttaminen (opt-out) kolmannelle osapuolelle.[35]

Lain seurauksena kuluttajilla on periaatteessa mahdollisuus seurata omien henkilötietojen siirtoja. Valitettavana poikkeuksena laissa on, ettei se koske alle kaksikymmentä henkeä työllistäviä sähköisen kaupan alan yrityksiä. Näin se jättää melkoisen aukon tietosuojan toteutumiselle.[36]

2.3.4. Informointivelvollisuus

AB 68 on laki, josta käytetään nimitystä Online Privacy Protection Act of 2003 ja joka on laadittu Kalifornian osavaltiossa henkilötietoja kerääville

[33] Luhtasela 2007: 358-360.
[34] California Civil Code: Sec. 1798.83.
[35] Tieke 2003
[36] California Civil Code: Sec. 1798.83.

verkkokauppayrityksille. Sen tehtävänä on säädellä tietosuojakäytäntöjen julkistamista ja velvoittaa yritykset noudattamaan niitä.

Laki määrää verkkokaupan julkistamaan verkkosivuillaan tietosuojakäytäntönsä henkilötietojen keräämisestä. Sähköisenkaupan tulee myös informoida asiakkaitaan, mikäli kerättäviä henkilötietoja mahdollisesti tullaan luovuttamaan kolmannelle osapuolelle. Laki määrittelee henkilötiedoiksi minkä tahansa tiedon, jonka perusteella henkilöön voidaan ottaa yhteyttä. Näitä ovat esimerkiksi sähköposti- ja kotiosoite.[37]

AB 68 – laki ei käytännössä lisää kuluttajien henkilötietojen tietosuojatasoa, vaan velvoittaa sähköisenkaupan yritykset informoimaan asiakkaitaan, kuinka tietoturvasta on yrityksessä huolehdittu. Valitettavasti yritykset käyttävätkin usein lain tuomaa informointivelvollisuutta lähinnä markkinointitarkoituksessa edistääkseen omaa yrityskuvaa luotettavana verkkokauppana. Lain pääasiallisena pyrkimyksenä on kuitenkin avoimuuden lisääminen sähköisessä kaupankäynnissä. [38]

2.3.5. Tuomioistuinten oikeuskäytäntö

Tilanteissa, joissa kuluttajan tietosuojaa on loukattu sähköisen kaupankäynnin yhteydessä eikä voimassa olevasta lainsäädännöstä ole apua, voidaan turvautua oikeuskäytäntöön. Useissa osavaltioissa on runsaasti aiheeseen liittyvää oikeuskäytäntöä, muttei suoranaisesti verkossa tapahtuvasta kaupankäynnistä, mikä tekee oikeuskäytännön soveltamisesta mutkikasta.

Henkilön tietosuojaan kohdistuneen loukkauksen perusteella on mahdollista nostaa kanne osavaltion tuomioistuimessa. Kanneperusteena on yksityisyyden loukkaus, jonka voidaan katsoa koskevan useita henkilötietosuojan piiriin kuuluvia loukkauksia esimerkiksi henkilöllisyyden anastamisesta, tietojen luvatonta julkaisemisesta ja keräämistä.[39] Olemassa oleva oikeuskäytäntö antaa kuluttajalle mahdollisuuden suojella henkilötietojaan, mutta on kuitenkin

[37] California Business and Professions Code: Sec. 22577 & 22575.
[38] Luhtasela 2007: 360-363.
[39] Luhtasela 2007: 363-364.

käytännössä haasteellinen, sillä henkilön on kyettävä osoittamaan toteen haitan aiheutuminen.

2.3.6. Sähköisenkaupan yritysten itsesäätely

Yhdysvalloissa on käytössä yrityksien itsesäätelyjärjestelmä tietosuojan edistämiselle. Kalifornian osavaltiossa yritysten on pakko julkistaa tietosuojakäytäntönsä ja sitoumuksensa asiakkailleen. Tämä on myös FTC:n antama suositus kaikille sähköisenkaupan yrityksille Yhdysvalloissa.

FTC valvoo, että käytäntönsä julkaissut yritys myös noudattaa ilmoittamiaan käytäntöjään. ”Perusteen tietosuojakäytäntöjen rikkomuksia vastaan FTC:lle tarjoaa FTC Act -lain viides pykälä, jossa kielletään sopimattomat ja harhaanjohtavat toimet ja käytännöt kaupan alalla. Tähän liittyen FTC tulkitsee väärien tietojen antamisen kuluttajien tietojen keräämisen syystä tai tietojen käyttämisestä muodostavan FTC Actissa kielletyn harhaanjohtavan käytännön.” [40]

FTC on myös julkaissut sähköisenkaupan yrityksille tietosuojan edistämisen kannalta seuraavat tärkeät periaatteet: ilmoitus-, valinta-, tiedonsaanti ja turvallisuusperisaatteet. Käytännössä kuitenkin harva verkkosivusto on sitoutunut käyttämään FTC:n julkaisemia periaatteita.[41]

2.3.7. Sähköinen allekirjoitus Yhdysvallat

Yhdysvaltojen lainsäädännössä on säädetty sähköisestä allekirjoituksesta kahdessa eri laissa: E-sign act -laki (Electronic Signatures in Global and National Commerce Act) vuodelta 2001[42] ja UETA –mallilaissa (Uniform Electronic Transactions Act) vuodelta 1999.[43] Molemmat lait on tarkoitettu sovellettavaksi sähköiseen kauppaan ja sopimusten solmimiseen. Lisäksi

[40] Luhtasela 2007: 364.
[41] Luhtasela 2007: 364-365. Katso myös FTC 2000 b: 12 -13 & 35- 38.
[42] USC: Chap. 96. Sec.7001 & 7002.
[43] Uniform Electronic Transactions Act.

noudatetaan UNCITRAL:n sähköisen kaupankäynnin mallilakia.[44] Molemmissa liittovaltion laeissa sähköisen allekirjoituksen määritelmä on kirjoitettu mahdollisimman laajaksi. Tarkoituksena on ollut välttää tiukkaa ohjeistusta ja näin luoda mahdollisuus monenlaisille sähköisen allekirjoituksen tekniikoille. Sähköisen allekirjoituksen pääasiallisena tehtävänä, kuten perinteiselläkin allekirjoituksella, on osoittaa sopimuksen hyväksyntä verkkokaupassa. UETA-mallilaissa ”sähköisenä allekirjoituksena pidetään sähköistä symbolia, ääntä tai prosessia, joka on liitetty tai on loogisesti liitetty sähköiseen tietoon ja jota käytetään allekirjoitustarkoituksessa.”[45]

Lainsäädäntö on jättänyt mahdolliseksi luoda allekirjoitus millä tahansa menetelmällä. Lain perusteella allekirjoituksesta käy niin nimi sähköpostiosoitteessa kuin hiiren näpäytys tietyssä kohtaa verkkosivua. Allekirjoituksen tulee vain täyttää sille UETA-laissa annettu tehtävä eli ilmaista henkilön tahto hyväksyä allekirjoitettu teksti. Sähköinen allekirjoitus on haluttu rinnastaa mahdollisimman lähelle perinteistä käsintehtyä allekirjoitusta, ja tämän takia lainsäädäntö on välttänyt asettamasta sille erityisiä muotovaatimuksia.

Lähtökohtana Yhdysvaltain lainsäädännössä on antaa sähköiselle allekirjoitukselle sama oikeusvaikutus kuin tavanomaiselle käsin kirjoitetulle. Koska määritelmän on laaja, on lain oikeusvaikutuksen käytännön toteutus hyvin tilannesidonnainen. Yhtenä kriteerinä pidetäänkin, että allekirjoituksen tulee olla selvästi yhdistettävissä sen antajaansa.[46] Oleellisena osana vahvaan tunnistamiseen liittyy varmuus siitä, että allekirjoituksen antajan henkilöllisyys kyetään varmentamaan. Liittovaltion lainsäädännössä ei tästä kuitenkaan ole säädäntöä, mikä jättää mahdollisuuden varsin erilaisille varmennekäytännöille. Eräissä osavaltioissa on säädetty asiasta ja määrätty varmennepalveluiden tarjonta luvanvaraiseksi, mikä mahdollistaa alan valvomisen.[47]

Liittovaltion lainsäädännössä ei ole mainintaa kuluttajan tai yritysten vastuusta mahdollisten väärinkäyttötapausten ilmetessä. Tämä jättää epäselväksi korvausvelvollisuuden syntymisen perusteet Yhdysvalloissa.[48]

---

[44] UNCITRAL 1998: Art 7.
[45] Luhtasela 2007: 306-307.
[46] Uniform Electronic Transactions Act: Sec 7 & 5.
[47] USC: Chap.96 Sec.7001.
[48] Luhtasela 2007: 309.

2.4. Tietosuojan eroavaisuudet EU:ssa ja Yhdysvalloissa

Henkilö- ja muiden salassa pidettävien tietojen suoja voi poiketa huomattavasti EU:n ja Yhdysvaltojen välillä. Alueiden hallinnollinen ja oikeusjärjestelmien erilaisuus ovat vaikuttaneet tietosuojan kehitykseen sähköisen kaupan alalla. EU on pyrkinyt luomaan yhtenäisen alueen lainsäädännöllisesti, ja tämän vuoksi kuluttaja voi EU:n alueella olettaa saavansa samanlaisen oikeussuojan tiedoilleen jäsenmaasta riippumatta.[49] Yhdysvalloissa liittovaltio on jättänyt tietosuojaa koskevan lainsäädännön lähes kokonaan osavaltioiden tehtäväksi, mikä vaikeuttaa kuluttajan mahdollisuutta ennakoida, millainen oikeusturva hänen luovuttamillaan tiedoillaan on siinä osavaltiossa, jossa palveluntarjoaja toimii.

Olemassa oleva oikeus rakentuukin suuressa määrin osavaltiokohtaiseen lainsäädäntöön ja oikeustapauksiin, jotka ovat erittäin tapauskohtaisia ja sen vuoksi haasteellisia soveltaa käytäntöön. Kuluttajan kannalta mahdollisten ongelmien ratkaisut ovat ennalta arvaamattomia. Poikkeuksena tietosuojan kannalta on jo edellä mainittu Kalifornian osavaltio. Osavaltio on lainsäädännöllään velvoittanut alueellaan toimivat verkkokaupat takaamaan lähes vastaavan tietosuojan keräämilleen henkilö ja muille salassa pidettäville tiedoille kuin EU:n alueella toimiva palveluntarjoaja.

Euroopan unionin alueella on lainsäädännöllä määrätty erityinen valvontaviranomainen huolehtimaan ja neuvomaan kuluttajia ja yrityksiä tietosuoja-asioihin liittyvissä kysymyksissä.[50] Väärinkäyttötilanteissa viranomainen neuvoo ja ohjaa kuluttajaa tai yritystä kuinka toimia, jos salassa pidettäviä tietoja on käytetty väärin.[51] Yhdysvalloissa lainsäädäntö ei tällaista viranomaista vaadi, mikä aiheuttaa sen, että verkossa asioivien tulee itse olla huolellinen ja selvillä omista oikeuksistaan antaessaan henkilötietojaan. Avun saaminen tai löytäminen väärinkäyttötilanteissa voi olla erittäin haastavaa. Ainoa valvontaviranomainen on liittovaltion asettama Federal Trade Comission, ja senkin tehtävän on valvoa vain Children online privacy protection act -lain noudattamista yrityksissä sekä tulkita lakia

[49] Warma: 29. Tietosuoja 3/2010
[50] Direktiivi 95/46/EY
[51] Direktiivi 2000/31/EY

ongelmatilanteissa.[52] Pitää myös muistaa, että tämä laki antaa suojaa vain Yhdysvaltain kansalaisille. Kyseinen valvontaviranomainen antaa suojaa hyvin pienelle määrälle verkkopalvelujen käyttäjiä. Poikkeuksena tästä on kuluttajan eduksi Kalifornian osavaltio, joka on perustanut kuluttajien avuksi neuvoa antavan tietosuojaviranomaisen.

Tietosuojan lähtökohtana voidaan pitää Euroopan unionissa henkilötieto-direktiiviä. Se määrittelee tarkasti henkilötietokäsitteen ja sen tarkoitus on edistää niin henkilöiden tietoturvaa kuin yritysten liiketoimintaa ja helpottaa henkilötietojen vapaata liikkuvuutta unionin alueella. Yhdysvalloista puuttuu vastaavanlainen laki, joka määrittelisi yksiselitteisesti henkilötiedot ja joka koskisi koko liittovaltiota. Liittovaltiossa ei ole myöskään lakia, jolla nimenomaan pyrittäisiin turvaamaan henkilö tai muita salassa pidettäviä tietoja. EU:ssa, henkilötieto- ja monilla muilla direktiiveillä on pyritty turvaamaan yritysten keräämien henkilötietojen käsittely ja säilyttäminen.

Kalifornian osavaltio on säätänyt AB 1950 -säännöksen, jolla se velvoittaa sähköisen kaupan yritykset huolehtimaan kerätyistä henkilötiedoista ja niiden turvallisesta käsittelystä ja säilyttämisestä. EU-alueen yrityksillä on vastaavanlainen velvoite ja se perustuu erityisesti direktiiviin sähköisestä kaupasta.[53] Direktiivistä poiketen AB 1950 -säännös jättää tietosuojaa koskevat turvajärjestelmäratkaisut yrityksen itsensä päätettäviksi ja vaille valvontaviranomaista. EU:n alueella taas valvontaviranomaisen tehtävänä on valvoa kyseisten tietoturvaratkaisujen riittävyys. Tämä on huomattava etu kuluttajan tietoturvan kannalta.

Kuluttajan asioidessa Kalifornialaisen verkkokaupan kanssa on osavaltion säätämä Online Protection Act of 2003 -laki hyödyllinen. Se ei säädä, millä lailla yritysten tulee keräämistään tiedoista huolehtia, mutta se velvoittaa yritykset julkaisemaan ne käytännöt, kuinka ne tosiasiallisesti henkilötietoja käsittelevät ja säilyttävät. Kuluttajan on siis erityisen tärkeää tutustua kunkin yrityksen tietoturvakäytäntöselosteeseen ja päättää sen pohjalta, onko verkkokauppa turvallinen. Tämä laki siis velvoittaa yritykset vain noudattamaan niiden itsensä ilmoittamia tietosuojaa koskevia käytäntöjä. Myös EU:n alueella yritykset on velvoitettu ilmoittamaan vastaavat käytännöt mutta lainsäädäntö myös vaatii yrityksiltä tietyn minimitason toimenpiteistä, joilla henkilötiedot

[52] USC: Chap.91 Sec.6505
[53] Direktiivi 2000/31/EY

tulee suojata. [54]

Varsin merkittävänä erona EU:n ja Yhdysvaltojen välillä voidaan pitää kysymystä korvausvelvollisuudesta tietosuojan piiriin kuuluvien tietojen väärinkäytöksistä sähköisessä kaupassa. Yhdysvaltain liitovaltion lainsäädännössä ei ole mainintaa yritysten korvausvastuusta henkilötietoihin kohdistuneesta väärinkäytöksestä.[55] Euroopan unionin lainsäädännössä korvausvastuu kuitenkin löytyy muun muassa henkilötietodirektiivistä.[56]

”Käytännössä merkittävä ero Euroopan unionin ja Yhdysvaltojen välillä on siinä, että direktiivit luovat lainsäädännöllisesti yhdenmukaisen alueen jäsenvaltioiden sisälle, jossa säännökset soveltuvat sekä julkiseen että yksityiseen sektoriin ja joiden soveltamista valvoo kansallinen viranomainen, jolle kansalainen voi valittaa oikeudenloukkauksesta”. Yhdysvalloissa ei ole yhdenmukaista ja vastaavaa koko liittovaltiota koskevaa lainsäädäntöä henkilötietosuojasta eikä valvontaviranomaista.[57]

[54] California Business and Professions Code & Direktiivi 2000/31/EY.
[55] Luhtasela 2007: 309
[56] Direktiivi 95/46/EY
[57] Warma: 27. Tietosuoja 4/2004

3. TIETOSUOJA JA TUNNISTAMINEN SÄHKÖISESSÄ KAUPASSA

Tietosuojan tarkoituksena on taata palvelun käyttäjälle turvallinen ja luotettava ympäristö asioida verkossa. Tietoturva pyrkii turvaamaan tietosuojan piiriin kuuluvat käyttäjän tiedot. Kuluttajalle tietosuoja sähköisessä kaupankäynnissä perustuu tutkimuksen aikaisemmissa kappaleissa esiteltyihin Euroopan unionin määrittelemiin direktiiveihin ja Suomen lainsäädäntöön, joiden pohjalta palveluntarjoajan tulee toimia. Lisäksi sähköisenkaupan globaalin luonteen vuoksi myös Yhdysvaltojen lainsäädäntö tulee ottaa huomioon, sillä useat käyttämämme verkkokaupat toimivat Yhdysvalloissa.

Koska Suomesta puuttuu varsinainen tietosuojalaki, voidaan tietosuojaa ja sähköistä kauppaa käsittelevistä eri laeista saada varsin kattava lainsäädäntö ja turva suojelemaan kuluttajantietoja verkossa. Tietoturva rakentuu varsin pitkälle palveluntarjoajaa velvoittavaan lainsäädäntöön ja siihen, kuinka tämän tulee rakentaa tietoturvaseikat palvelussaan niin, että se takaa lain edellyttämän vähimmäistason. Yhdysvalloissa tietosuoja taas perustuu varsin vähäiseen tietosuojalainsäädäntöön sekä liike-elämän omaan itsesäätelyyn, minkä takia kuluttajan oma aktiivisuus henkilötietojen turvaamisessa on tärkeää. Voidaankin ajatella, että koko tietosuoja rakentuu eräänlaisesta kolmikannasta: lainsäädännöstä, teknisistä ratkaisuista sekä asiakkaan omasta toiminnasta verkossa.

3.1. Palveluntarjoajan velvollisuudet

Lainsäädännön perusteella tietosuojan voidaan sanoa olevan sitä, että kuluttajan tiedot on saatu laillisesti, niitä käsitellään, säilytetään ja luovutetaan lain edellyttämällä tavalla eikä mitään edellä mainittua tehdä asiakkaan tietämättä tai vastoin tämän tahtoa. Kuluttajan henkilötiedot ja luottokorttitiedot ovat tietosuojakäsitteeseen sisältyvää informaatiota, josta palveluntarjoajan tulee huolehtia.[58] Lainsäädännön perusteella palveluntarjoaja velvoitetaan teknisin ja organisatoristen ratkaisuin varmistamaan, ettei

[58] Viemerö: 34 -37. Tietosuoja 1/2009

yksikään ulkopuolinen voi murtautua tietokantoihin ja päästä käsittelemään, vahingoittamaan tai siirtämään asiakkaiden henkilö- tai tilitietoja.[59]

Palveluntarjoajan tulee kyetä seuraamaan ja kontrolloimaan kaikkia tietoihin tehtyjä muutoksia ja varmistaa niiden oikeellisuus.[60] Koska tavoitteena on, että yritykset täyttäisivät lain velvoitteet ja pyrkisivät kaiken aikaa kehittämään tietoturvaansa, on lainsäätäjä asettanut rekisterinpitäjät vahingonkorvaus- ja rangaistusvastuuseen. Mikäli asiakkaan tiedot joutuvat vääriin käsiin ja tästä aiheutuu asiakkaalle taloudellista tai muuta vahinkoa, on palveluntarjoajan korvattava vahingot.[61] Edellyttäen, että palveluntarjoaja on laiminlyönyt velvoitteensa järjestää ajanmukainen tietosuojantaso tai huolimattomuuttaan mahdollistanut tietosuojavarkauden.[62]

Yhdysvalloissa palveluntarjoajan velvollisuudet ovat kuitenkin rajallisemmat. Myös liittovaltiossa palveluntarjoajan tulee suojata tiedot tietosuojajärjestelmin, mutta yrityksen oma asia on, kuinka se sen toteuttaa, ja tämä erottaa sen meidän säännöksistämme. Kalifornian osavaltiossa palveluntarjoajan velvollisuudet huolehtia asiakkaidensa tietosuojasta ovat lähempänä eurooppalaisia ja suomalaisia velvoitteita. Huomattavia eroja kuitenkin on tietoturvajärjestelyiden vaatimuksissa ja vahingonkorvausvelvollisuudessa.[63] Tämän takia voidaankin olettaa, että kuluttaja saa helpommin suojaa väärinkäyttötilanteissa, jos hän on asioinut verkkokaupan kanssa, jota velvoittaa Euroopan unionin lainsäädäntö.

3.2. Asiakkaan tietoturvatoimenpiteet

Lainsäätäjä on asettanut tietoturvan järjestämiseksi velvoitteita lähinnä palveluntarjoajalle. Tästä huolimatta kuluttajan on omilla toimenpiteillään hyvä ennalta ehkäistä väärinkäytösten riskiä. Internet on täynnä erilaisia toimijoita, minkä vuoksi verkkokauppa on syytä valita huolellisesti ja selvittää sen kotipaikka ja osoite.[64] Laki 485/2002 säätää palveluntarjoajalle ns.

[59] Laine 2001: 137 & Salminen: 30 -32. Tietosuoja 2/2010.
[60] Aato 2000: 55-70.
[61] 412/1974. Vahingonkorvauslaki. Katso myös KKO 1998:85 & KKO 1999:127.
[62] Luottamus, Tietoturva, Sähköiset palvelut & Niskanen 2010: 519 -520.
[63] Luhtasela 2007: 358-360.
[64] Linden: 22 -23. Tietosuoja 1/2009.

informaatiovelvollisuuden eli sen on ilmoitettava itsestään, muun muassa nimi, osoite, sijoittautumisvaltio, yhteystiedot ja yritystunnus ja sen, miten on huolehtinut henkilötietojen käsittelystä eli millainen on verkkokaupan tietoturvallisuuspolitiikka.[65]

Asioidessaan yhdysvaltalaisen verkkokaupan kanssa tulee kuluttajan muistaa, että lainsäädäntö poikkeaa esimerkiksi Suomen vastaavasta. Antaessamme henkilötietoja yritykselle on meidän hyväksyttävä, että tietojamme voidaan siirtää tai myydä eteenpäin. Lisäksi antamamme tiedot jäävät yrityksen verkkokaupan rekisteriin, sillä lain luomaa velvollisuutta niiden poistoon EU:n tavoin ei Yhdysvalloissa ole. Tämän vuoksi asiakkaan on ennen omien tietojen antamista myös hyvä perehtyä palveluntarjoajaan, sen mahdollisesti ilmoittamiin tietoturvakäytäntöihin ja välttää tarpeettomien yksilöintitietojen luovuttamista. Syytä on myös ottaa huomioon eurooppalaisten ja yhdysvaltalaisten tietosuojajärjestelmien ja oikeuskulttuurien erot.[66]

Nostaakseen tietosuojantasoa kuluttajan täytyy huolehtia oman tietokoneensa tietoturvasta. On hyödyllistä pitää käyttämänsä Internet-selaimen tietoturvapäivitykset ajan tasalla ja asetukset palveluun sopivina. Kuluttaja voi parantaa omaa turvallisuuttaan toimimalla oikein ja ottamalla huomioon verkossa olevat tietosuojariskit.[67]

3.3. Sähköinen allekirjoitus ja vahva tunnistaminen

Tietosuojan kannalta erittäin merkittävä asia on käyttäjän luotettava tunnistaminen. Tunnistaminen pienentää huomattavasti esimerkiksi identiteettivarkauksien riskiä sähköisessä kaupassa. Asiakkaat onkin tunnistettava sähköisissä palveluissa, jos asiakkaan ja yrityksen välillä tehdään merkityksellisiä oikeudellisia toimia tai toimilla on taloudellista merkitystä. Sähköistä allekirjoitusta käytetäänkin useissa sähköisissä verkkokaupoissa täyttämään samaa tehtävää kuin perinteinen allekirjoitus. Käsite on erittäin laaja ja sen vuoksi sähköiseksi allekirjoitukseksi voidaan lukea esimerkiksi seuraavat menetelmät:

---

[65] Laki tietoyhteiskunnan palvelujen tarjoamisesta (458/2002) & Laine 2001: 170.
[66] Laine 2001: 189.
[67] Aalto 2000: 70- 75 & Niskanen 2010: 477.

1. asiakkaan nimi tilauslomakkeessa,
2. sähköpostiosoite viestin lopussa,
3. skannattu henkilön käsinkirjoitettu allekirjoitus,
4. verkkosivuston tietokoneelle jättämä eväste,
5. digitaalinen allekirjoitus, joka perustuu salaustekniikkaan ja sertifiointiin,
6. allekirjoitus, joka on tallennettu sellaiseen muotoon, että se voidaan tallentaa magneettijuovalle,
7. biometrinen allekirjoitus, jossa henkilö tunnistetaan tietokoneen avulla esimerkiksi sormenjälkien tai DNA:n avulla.[68]

Henkilötietojen, tili- tai luottokorttitietojen yhteydessä on erityisen tärkeää varmistua asiakkaan henkilöllisyydestä. Tällöin käytettävän tunnistusmenetelmän luotettavuuteen on kiinnitettävä erityistä huomiota.[69] Kehittynyt sähköinen allekirjoitus on vahva tunnistusmenetelmä, jolla on vastaavat oikeusvaikutukset kuin perinteisellä fyysisellä allekirjoituksella. Se on siis vahva tunnistusmenetelmä. Euroopan unioni on säätänyt sähköisten allekirjoitusten direktiivin 1999/93/EY, jolla se on asettanut vaatimukset, jotka kehittyneen sähköisen allekirjoituksen tulee täyttää:

a) sen tulee liittyä yksiselitteisesti sen allekirjoittajaan
b) sillä on voitava yksilöidä allekirjoittaja
c) se on luotu keinoilla, jotka allekirjoittaja voi pitää yksinomaisessa valvonnassaan
d) se on liitetty sen kohteena olevaan tietoon siten, että tiedon mahdollinen myöhempi muuttaminen voidaan havaita.[70]

Menetelmän täyttäessä edellä mainitut vaatimukset voidaan puhua vahvasta sähköisestä tunnistamismenetelmästä. Myös Suomen lainsäädännöstä löytyy kriteerit vahvalle sähköiselle tunnistamismenetelmälle. [71] Asiakkaan todellinen

[68] Simons & Simons 2001: 27-28.
[69] Viemerö: 30-31. Tietosuoja 4/2009
[70] Direktiivi 1999/93/EY.
[71] Niskanen 2010: 466-467.

henkilöllisyys voidaan sen avulla varmistaa ja hänet voidaan yksilöidä tietyksi henkilöksi luotettavasti. Menetelmää pidetään vastaavan tasoisena kuin henkilöllisyyden varmistaminen henkilöllisyysasiakirjoista. Esimerkki vahvasta sähköisestä tunnistusmenetelmästä on verkkokaupan mahdollisuus tunnistaa asiakas tämän omilla verkkopankkitunnuksillaan, minkä jälkeen tilauksen tai maksun suorittaminen on turvallista. Myös julkinen sektori, muun muassa Kela, varmistaa henkilöllisyyden verkossa kyseisellä menetelmällä.[72]

Kuluttajan tietosuojan turvallisuuden kannalta vahva tunnistamismenetelmä on suotava, mutta sen yleistyminen ei ole ollut kovinkaan nopeaa.[73] Yhtenä syynä tähän on sen aiheuttamat taloudelliset kustannukset palveluntarjoajalle, vaikka toisaalta verkkokaupan luotettava maine onkin kilpailutekijä sähköisessä liiketoiminnassa. Valitettavan useilla palveluntarjoajilla on verkossa käytössään menetelmä, jolla ei voida varmistaa käyttäjien henkilöllisyyttä luotettavasti. Tällaisesta menetelmästä käytetään nimeä heikko tunnistaminen ja sen laajamittainen käyttö onkin palvelusta riippumatta tietosuojariski.[74]

3.4. Sähköinen allekirjoitus Euroopan unionissa ja Yhdysvalloissa

Sähköiselle allekirjoitukselle säädetty päätehtävä on sama niin Euroopan unionin jäsenmaissa kuin Yhdysvalloissa eli osoittaa sopimuksen hyväksyminen. EU:ssa on pyritty varsin tarkasti säätelemään sähköistä allekirjoitusta, niiden turvallisuuteen ja luotettavuuteen perustuen. Heikko ja vahva tunnistaminen, joista jälkimmäinen saa saman oikeusvaikutuksen kuin normaali käsin tehty allekirjoitus. Yhdysvalloissa lainsäädäntö määrittelee sähköisestä allekirjoituksesta huomattavasti yleisemmällä tasolla, ja kaikille sen eri muodoille annetaan sama oikeusvaikutus. EU:ssa on katsottu tärkeäksi varmistaa allekirjoituksen antajan henkilöllisyys, kun taas Yhdysvalloissa on painotettu itse allekirjoituksen merkitystä ja sitovuutta.

Suurimpana eroavaisuutena EU:n ja Yhdysvaltojen välillä on, että EU:n alueella tunnistusmenetelmän on yksiselitteisesti tunnistettava tunnistusvälineen haltija tietyksi henkilöksi. Yhdysvalloissa ei ole kyseisestä asiasta lainkaan yhtenäistä

[72] Niskanen 2010: 458.
[73] Salminen 2009: 92-93.
[74] Castren: 22- 23 & Luhtasela 2003: 153. Lisensiaattitutkimus.

sähköistä kauppaa koskevaa liitovaltion tasoista lainsäädäntöä.

Eroa on myös vastuukysymyksissä. Tilanteessa, jossa sähköistä allekirjoitusta on käyttänyt väärin, joku kolmas osapuoli, on EU:n laeissa säädetty korvausvelvollisuudesta ja siitä, milloin itse tunnistusvälineen haltija vapautuu vastuusta.[75] Yhdysvalloissa ei ole lainsäädäntöä vastuu- ja korvauskysymyksistä.[76]

Vahva tunnistaminen, millä tässä yhteydessä tarkoitetaan sähköistä allekirjoitusta, on lähtökohdiltaan varsin samanlainen Euroopan unionin alueella ja Yhdysvalloissa. Molemmissa on toivottu sähköisen tunnistamisen yleistyvän sähköisessä kaupassa ja lisäävän kuluttajien ja yritysten luottamusta verkkokauppaan. Euroopan unioni ja Yhdysvallat ovat kuitenkin painottaneet lainsäädännössä hieman eri kohtia, mistä seuraa eroja. On vaikea todeta, kumpi on henkilön tietosuojaturvallisuuden kannalta edistyneempi järjestelmä.

[75] Direktiivi 1999/93/EY.

[76] USC: Chap. 96. Sec.7001 & 7002 & Uniform Electronic Transactions Act.

4. HENKILÖTIETOJEN HALLUSSAPITO JA SIIRTO

4.1. Henkilötietojen hallussapito EU:ssa

Useimmissa verkossa tapahtuvissa kaupankäyntitilanteissa jää asiakkaasta monia tietoja yrityksen rekistereihin: henkilötietoja, tilitietoja, osoitetietoja ja muita sellaisia tietoja, joita lain mukaan on käsiteltävä turvallisesti. Yrityksen tulee huolehtia näistä henkilötiedoista ja lailla turvallisesti käsiteltäviksi säädetyistä tiedoista. Tietojenkäsittelyn hyödyntämisen, käsittelyn ja turvallisen säilyttämisen tulee tapahtua yrityksen ennalta tekemän suunnitelman mukaan. Yrityksen hallussa olevien tietojen on oltava oikeita, kokonaisia ja tarkoituksenmukaisia. Tarvittaessa rekisterinpitäjän tulee tarkistaa asiakkaan ilmoittamat tiedot, kuten henkilöturvatunnus väestötietojärjestelmästä. Väärät tai puutteelliset tiedot on poistettava rekisteristä.

Henkilötietolaissa kuluttajalle annetaan myös oikeus tarkistaa omat tiedot, jotka yrityksellä on hallussaan rekisterissä. Kerättävien henkilötietojen tulee olla yrityksen toiminnassa tarpeellisia, ja syy niiden keräämiseen on kerrottava myös asiakkaalle.[77] Verkkokaupassa ostotapahtuman yhteydessä kerätyt tiedot ovat usein tarpeellisia tavaran toimittamisen ja maksamisen perusteella. Tilanteessa, jossa säilyttämiselle ei ole enää perusteita, on yrityksen hävitettävä tiedot, sillä käyttämättömät rekisterissä olevat kuluttajan henkilötiedot ovat riski tietosuojankannalta. [78]

4.2. Henkilötietojen hallussapito Yhdysvalloissa

Euroopan unionin lainsäädännöstä poiketen Yhdysvalloissa ei ole liittovaltiotason lainsäädäntöä, jolla säädeltäisiin henkilötietojen tai muiden arkaluontoisten tietojen, kuten pankkitilin tai luottokorttien numerojen hallussapitoa. Tämän vuoksi sähköistä kauppaa koskeva tietosuojalainsäädäntö on tältä osin osavaltiokohtaista ja keskitynkin tutkimuksessa Kalifornian osavaltion sähköistä kauppaa koskevaan lainsäädäntöön.

[77] Viemerö: 34-37. Tietosuoja 1/2009

[78] Laine 2001: 167-171.

Kaliforniassa samoin kuin EU:ssa, yritysten tulee henkilötietoja käsiteltäessä noudattaa ennalta julkaisemiaan tietoturvakäytäntöjään. Sähköisessä kaupassa saadut henkilötiedot on suojattava riittävin tietoturvaratkaisuin paljastumiselta ja luvattomalta käytöltä. Sähköisessä kaupassa tarvittavien tietojen on oltava tarpeellisia toimintojen mahdollistamiseksi eikä niitä saa kerätä asiakkailta enempää, kuin on tarpeellista toimintojen onnistumiseksi.

Yhdysvalloissa on poikkeuksena koko liittovaltiota koskeva Children's privacy protection act -laki, joka suojaa kaikkia alle 13-vuotiaiden lasten henkilötietoja ja asettaa verkkosivuston omistajan vastuuseen tietoturvatoimintojen järjestämisestä. Lain noudattamista valvoo FTC. Lain seurauksena alle 13-vuotiailla lapsilla on lähes vastaava tietosuoja kuin EU:n kansalaisella. Laki on poikkeus, sillä yli 13-vuotiailla henkilöillä ei Yhdysvalloissa ole vastaavaa henkilötietosuojaa juuri missään osavaltiossa.

Erona EU:n alueella toimivalla sähköisen kaupan alan yrityksellä ja yhdysvaltalaisella on, ettei jälkimmäisellä ole velvollisuutta tarkistaa annettujen tietojen oikeellisuutta. Children's privacy protection act –lain velvoittamien yritysten tulee kuitenkin tarjota lasten huoltajille mahdollisuus tarkistaa lasta ja itseään koskevat tiedot. Laki myös mahdollistaa huoltajalle oikeuden kieltää tietojen käyttö ja määrätä tiedot poistettavaksi rekisteristä. Tämä oikeus on automaattinen Yhdysvalloissa vain alle 13-vuotiaille lapsille sekä heidän huoltajilleen. Kaliforniassa laki velvoittaa yritykset poistamaan kaikkien asiakkaiden henkilö- ja luottokorttitiedot, mikäli ne ovat käyneet tarpeettomiksi.[79]

Viime aikoina Yhdysvalloissa on tiedostettu ongelmat tietosuojalainsäädännössä, ja liittovaltiossa onkin vireillä useita lakeja, jotka toisivat parannuksia henkilötietojen tietosuojaan. The Leahy Bill-nimellä tunnetun lakiehdotuksen on tarkoitus koskea yrityksiä, jotka käsittelevät suuria määriä henkilötietoja. Lain pyrkimyksenä on velvoittaa yritykset laatimaan tietoturvaohjeistukset, jotka sisältäisivät muun muassa hallinnolliset ja tekniset toimenpiteet henkilötietojen turvaamiseksi. Näiden toimenpiteiden tulisi olla riittävät suhteessa henkilötietojen määrään ja luonteeseen. Kyseinen laki velvoittaisi yritykset myös kouluttamaan henkilöstöään henkilötietojen käsittelyyn ja suorittamaan tarkastuksia tietojen käsittelyprosessien toimivuudesta. Velvoitteiden laiminlyönneistä seuraisi sakkoa, jonka määrä

[79] Luhtasela 2007: 365-370.

voisi nousta huomattavan suureksi. Liittovaltio aikoo myös kiristää nykyisten sääntöjen valvontaa. Erityisesti FTC:n on tarkoitus tehostaa lakien, muun muassa safe harbor -järjestelmän noudattamista. Voidaan siis todeta, jos lakiehdotukset toteutuvat, ollaan Yhdysvalloissa ottamassa merkittäviä askeleita henkilötietojen suojelemiseksi. Merkittävää on myös se, että ensimmäisen kerran yritykset voisivat saada rangaistuksia laiminlyönneistä.[80]

4.3. Tietojen siirtäminen EU-alueella

Sähköisenkaupan globaalin luonteen vuoksi yritysten on mahdollista ja usein välttämätöntä toimia useilla eri markkinoilla. Tämän takia eteen voi tulla tilanne, jossa halutaan siirtää jo valmiina olevat asiakastiedot toiseen maahan siellä olevalle toimijalle. Euroopan unionin sisällä on yrityksen laillista siirtää henkilötietoja jäsenvaltiosta toiseen vastaavalla tavalla ja samoin perustein, kuin tekisi tämän yhden jäsenmaan sisällä.[81] Tietoja siirtävän rekisterinpitäjän ei tarvitse tehdä siirrosta erillistä ilmoitusta tietosuojavaltuutetulle, jos siirto tapahtuu jäsenvaltiosta toiseen.

Henkilötietojen siirto Euroopan unionin ulkopuolelle kolmansiin maihin poikkeaa käytännöltään huomattavasti EU:n sisällä tapahtuvasta asiakastietojen siirrosta.[82] Henkilötietoja luovutettaessa tai siirrettäessä toiseen maahan on merkitystä sillä, kumpaa tarkoitetaan. Siirrettäessä henkilötietoja on todellisuudessa kyse toimeksiannosta, jossa toimeksisaaja käsittelee tietoja toimeksiantajan lukuun. Tietoja käsitellään samoin, kuin toimeksiantaja olisi itse käsittelemässä tietoja. Oikeudet käsitellä henkilötietoja perustuvat oikeudet alun perin saaneen oikeuksiin. Edellä mainitusta voidaan mainita tilanne, jossa toimeksiantaja yritys siirtää tietoja tietojenkäsittelypalveluja tarjoavalle yritykselle esimerkiksi laskutusta varten.

Tilanteessa, jossa yritys luovuttaa henkilötiedot, täytyy vastaanottajan olla itsenäinen rekisterinpitäjä. Tällä täytyy siis olla omat itsenäiset oikeudet toimia henkilötietojen käsittelijänä. Luovutuksen saaja ei siis automaattisesti suorita henkilötietojen käsittelyä luovuttajalle, vaan voi itse hyödyntää tietoja omassa

[80] Warma: 40–41. Tietosuoja 4/2010.
[81] EYT: C-101/01.
[82] Laine 2001: 185 -187 & Viemerö 2009: 80.

liiketoiminnassaan. Henkilötietojen luovuttamiseen täytyy olla rekisteröidyn suostumus tai esimerkiksi asiakassuhteen perusteella asiallinen peruste. Asiakkaan henkilötietojen käsittelyyn sovelletaan sen maan lakia, jossa käsittely tapahtuu.[83] Vaikka kaikkia EU:n jäsenmaita velvoittavat samat direktiivit, on henkilötietojen käsittelyssä silti kansallisia eroja.[84]

4.4. Tietojen siirtäminen Yhdysvalloissa kolmannelle osapuolelle

Yhdysvaltain lainsäädäntö ei tee eroa henkilötietojen siirrosta osavaltioiden välillä, vaan se säätelee vain tietojen siirtämistä kolmannelle osapuolelle. Voidaankin olettaa tietojen siirtämisen osavaltioiden välillä vastaavan Euroopan unionissa tapahtuvaa tietojen siirtämistä jäsenvaltioiden välillä. Lainsäädäntö velvoittaa yrityksen kertomaan etukäteen, mikäli se luovuttaa henkilötietoja kolmannelle osapuolelle. Tämän lisäksi asiakkaan sitä kysyessä yritys on velvollinen kertomaan jos se on siirtänyt asiakasta koskevia tietoja eteenpäin, mitä tietoja ja millä toimialalla kyseinen yritys toimii. Samalla yrityksen pitää varmistaa, että tietosuojataso säilyy myös kolmannen osapuolen toimessa.[85]

4.5. Henkilötietojen siirtäminen EU:n ja Yhdysvaltain välillä

Kuluttajien henkilötietosuojan parantamiseksi yritys, jonka tarkoituksena on siirtää asiakkaidensa henkilötietoja Euroopan unionin talousalueen ulkopuolelle, tarvitsee tietoja yrityksen ja kohdemaan tietosuojajärjestelyistä. Erityisesti Euroopan ja Yhdysvaltojen välisen vilkkaan kaupan seurauksena on niiden välillä käytössä niin sanottu safe harbor -järjestely, joka astui voimaan vuonna 2000.[86] Sen tarkoituksena on taata tiedon vapaa liikkuvuus Euroopan unionin ja Yhdysvaltojen välillä. [87]

---

[84] Salminen 2009: 31, 47- 48, 83- 86.
[85] Luhtasela 2007: 361-363.
[86] Safe harbor-kotisivut.
[87] Warma: 27. Tietosuoja 1/2004.

Safe harbor –järjestelmän toimintaperiaatteena on, että Yhdysvaltojen kauppaministeriö (U. S Department of Commerse) pitää luetteloa yrityksistä, jotka ovat sitoutuneet noudattamaan safe harbor -periaatteita. Euroopan unionin komissio ja Yhdysvaltojen kauppaministeriö ovat yhdessä hyväksyneet nämä yksityisyyden suojaa ja tietoturvaa koskevat seuraavat periaatteet:

1) notice – yrityksen tulee informoida rekisteröityä siitä, mitä tietoja kerätään ja mihin niitä käytetään

2) choice – rekisteröidyllä tulee olla oikeus kieltää tietojensa luovuttaminen kolmannelle osapuolelle

3) access – rekisteröidyllä tulee olla mahdollisuus tarkistaa omat tietonsa

4) security – rekisterinpitäjän on huolehdittava riittävästä tietoturvasta

5) transfer – rekisterinpitäjän tulee informoida rekisteröityä luovutuksesta ja varata hänelle tilaisuus kieltää luovutus

6) enforcement – rekisterinpitäjän tulee huolehtia siitä, että riippumaton toimielin tutkii rekisteröidyn valitukset moitittavasta toiminnasta tai väärinkäytöksistä[88]

Edellä mainitut periaatteet vastaavat suurelta osin eurooppalaisilta yrityksiltä vaadittavia tietoturvatoimenpiteitä. Järjestely onkin luonut selkeät säännöt tietojen siirrolle ja niiden käsittelylle EU:n ja Yhdysvaltojen välillä. Järjestelyn oletetaan näin takaavan riittävän suojan henkilötietojen siirrolle maiden välillä. Ongelmana voidaan pitää sitä, että liittyminen järjestelmään on vapaaehtoista yhdysvaltalaisille yrityksille ja siksi järjestelmään liittyneiden yritysten lukumäärä on jäänyt varsin vaatimattomaksi. Vuonna 2006 siihen oli liittynyt 1100 yritystä.[89] Yhdysvaltain kauppaministeriö pitääkin listaa myös organisaatioista, jotka ovat ilmoittaneet sitoutuvansa periaatteisiin, mutta ovat myöhemmin jättäneet niitä noudattamatta.[90] On muistettava, että kyseinen järjestelmä ei ole kuitenkaan ainoa keino yrityksille siirtää henkilötietoja.

[88] Tietosuojavaltuutetun toimisto.
[89] Luhtasela 2007: 347–348.
[90] Laine 2001: 187-189.

Henkilötietojen siirto EU:n alueelta Yhdysvaltoihin on mahdollista myös sopimuslausekkein, jos yritys ei kuulu Safa harbor -järjestelmään.[91]

4.6. Henkilötietojen siirto EU:n ja ETA-alueen ulkopuolelle

Euroopan unionin pyrkimyksenä on edistää sähköistä kauppaa helpottamalla henkilötietojen siirtoa alueellaan. Käytännössä henkilötietodirektiiviin mukainen tietojen siirto niin jäsenvaltioiden kuin Euroopan talousalueeseen (ETA) kuuluvien maiden välillä tapahtuu samoin perustein kuin Suomen sisällä. Lainsäädännöllä EU on halunnut suojata kansalaistensa henkilötietoja rajoittamalla voimakkaasti keinoja tietojen siirtämiseen EU-alueen ulkopuolelle kolmansiin maihin. Valtiota, jonka lainsäädäntö on varsin puutteellinen henkilötietojen ja yksityisyyden suojelemiseksi eikä näin ollen pysty tarjoamaan direktiivin 95/46/EY mukaista suojaa, kutsutaan tässä yhteydessä kolmanneksi maaksi.[92] Pyrkimyksenä on rajoituksin torjua tietojenkäsittelyä koskevaa säännösten kiertämistä siirtämällä tietojenkäsittely valtioihin, joissa on heikompi tietosuojataso. Henkilötietodirektiivin mahdollistamat rajoitukset ovat varsin perusteltuja, sillä sähköisessä kaupassa käsitellään ja siirretään valtavia määriä henkilötietoja.

Tietojen siirtäminen EU:n ja ETA-alueen ulkopuolelle on henkilötietolain 22 §:n mukaan mahdollista vain, jos kyseisessä maassa taataan tietosuojan riittävä taso. Usein on syytä olettaa, että kehitysmaissa tietosuojaan liittyvä lainsäädäntö ja yleinen suhtautuminen henkilötietojen ja yksityisyyden suojaan poikkeaa merkittävästi omastamme.[93] Tietosuojatason riittävyyttä tietyssä maassa arvioi rekisterinpitäjä ja tietosuojavaltuutettu. Arviointi tulee tapahtua kokonaisvaltaisesti, jolloin otetaan huomioon muun muassa seuraavat seikat: siirrettävien tietojen luonne, käsittelyn tarkoitus, alkuperämaa ja luovutuksen kohdemaa. Lisäksi tulee arvioida kohdemaan yleiset ja alakohtaiset säännökset, käytännesäännöt ja noudatettavat tietoturvatoimet.[94] Mikäli tietosuojavaltuutettu toteaa jonkin valtion lainsäädännön ja käytännöt

[91] Direktiivi 95/46/EY. Katso myös Rautanen: 16. Tietosuoja 1/2001.
[92] Direktiivi 95/46/EY
[93] Castren: 35. Tietosuoja
[94] 523/1999. Henkilötietolaki. Katso myös Warma: 27. Tietosuoja 4/2004.

riittäviksi, on esimerkiksi verkkokaupalla oikeus siirtää henkilötietoja kyseiseen maahan.[95]

Euroopan yhteisön komissio on pidättänyt myös itsellään oikeuden arvioida tietosuojantason riittävyyttä kolmansissa maissa. Arviointi tapahtuu tapauskohtaisesti komiteamenettelyssä, jossa komissio henkilötietodirektiivin 31 artiklassa kuvatussa menettelyssä toteaa, että tietyssä valtiossa on riittävä yksityisyyden suoja henkilötietojen käsittelyssä tai sitten ei ole. Menettelyllä komissio tulee jakaneeksi kolmannet maat turvallisiksi tai ei-turvallisiksi henkilötietojen siirron ja käsittelyn osalta. Komission päätökset kolmannen maan suhteen ovat jäsenvaltioita velvoittavia ja artiklassa 31 jäsenvaltiot ja komissio velvoitetaan informoimaan toisiaan, jos ne arvioivat jonkin maan tietosuojatason riittämättömäksi

Komissio on päättänyt, että tietosuojantaso on riittävä henkilötietojen siirtämiseen seuraaviin maihin: Argentiina, Guernsey, Färsaaret, Jersey, Unkari, Kanada, Maansaaret ja Sveitsi. [96] Näiden maiden lisäksi EU:lla ja Yhdysvalloilla on keskinäinen järjestely Safe Harbor, joka pyrkii takaamaan riittävän tietosuojatason henkilötietojen käsittelyssä. Järjestelmästä on kirjoitettu laajemmin aikaisemmin tässä tutkimuksessa.

4.6.1. Poikkeukset

Rekisterinpitäjällä on mahdollisuus siirtää henkilötietoja kolmansiin maihin muutamin poikkeuksin, vaikkei maiden lainsäädäntö täyttäisikään henkilötietolain 22 §:n edellytyksiä. Henkilötietolain 23 §:ssä on lueteltu muun muassa seuraavat poikkeukset:

1) rekisteröity antaa yksiselitteisen suostumuksensa siirtoon;
2) siirto on tarpeen rekisteröidyn toimeksiannosta tai rekisteröidyn ja rekisterinpitäjän välisen sopimuksen toimeenpanemiseksi tai sopimusta edeltävien toimenpiteiden

[95] Salminen 2009: 83 -84.
[96] Direktiivi 95/46/EY 25

toteuttamiseksi rekisteröidyn pyynnöstä, esimerkiksi varattaessa lentolippua asiakkaalle;[97]

3) rekisterinpitäjä antaa sopimuslausekkein tai muutoin riittävät takeet rekisteröityjen yksityisyyden ja oikeuksien puolesta, eikä komissio ole todennut takeita riittämättömiksi;

4) siirto on tarpeen tai lain vaatima tärkeän yleisen edun turvaamiseksi, puolustukseksi tai ratkaisemiseksi. [98]

Koska edellä mainitun kaltaiset tapaukset ovat poikkeuksia, yleiseen käytäntöön tulee näitä perusteluita tulkita tiukasta. [99] Komission perustaman tietosuojaryhmän mukaan poikkeukset koskevat suurimmalta osin tilanteita, joista rekisteröidylle aiheutuvat riskit ovat vähäisiä. Jos tämän lisäksi tietojen siirtämisestä aiheutuva muu etu ylittää rekisteröidyn oikeuden yksityisyyteen ja näin ollen siirto on mahdollinen.[100]

4.6.2. Sopimuslausekkeet

Tilanteessa, jossa komissio tai tietosuojaviranomainen on todennut tietyn valtion tarjoaman yksityisyyden suojan ja tietosuojatason riittämättömäksi, on vielä yksi mahdollisuus saada henkilötietoja siirretyksi. Verkkokauppa voi siirtää tietoja kolmannessa maassa olevalle rekisterinpitäjälle, jos tämä takaa sopimuslausekkein, että tietosuojantaso ja turvaamistoimet täyttävät tai ylittävät henkilötietodirektiivin vaatimukset.[101] Kyseisten lausekkeiden täytyy taata rekisteröidylle vastaava yksityisyyden ja perusoikeuksien suoja, kuin rekisteröidyllä oli ennen henkilötietojen siirtoa.

Kolmansiin maihin sopimuslausekkein tapahtuvat siirrot ovat mahdollisia komission eriävästä arviointipäätöksestä huolimatta, sillä sopimuksen osapuolina ovat elinkeinonharjoittajat. Tekemässään komiteamenettelyssä komissio arvio vain kyseessä olevan valtion lainsäädäntöä tietosuojan ja

---

[97] EYT: C-318/04
[98] Salminen 2009: 90 -91.
[99] Luhtasela 2007: 350.
[100] Tietosuojalautakunnan ratkaisu 2009.
[101] 524/1999. Henkilötietolaki.

yksityisyyden näkökulmasta eikä yksittäisiä yrityksiä. Sopimuksen osapuolena ei siis milloinkaan ole valtio. Itse sopimustekstin tulee olla yksityiskohtainen ja mukailtava henkilötietodirektiivin ja henkilötietolain säädöksiä ja täytettävä niissä ilmenevät velvoitteet kussakin tapauksessa.[102] Koska henkilötietosiirto perustuu tällaisiin sopimuslausekkeisiin, osapuolet sitoutuvat noudattamaan sopimuksesta ilmeneviä velvoitteita sekä soveltuvin osin vastaanottajan maassa säädettyjä lakeja.

Komissio on kuitenkin pidättänyt itsellään oikeuden kieltää tietojen siirto sopimuslausekkein ehkäistääkseen väärinkäytöksiä. Edellytyksenä kieltoon on, että komissio tai jäsenvaltio ilmaisee asianmukaisesti perustellun vastalauseen henkilöiden yksityisyyteen ja perusoikeuksiin ja vapauksiin viitaten. Tämän johdosta komission on suoritettava asianmukaiset toimenpiteet 31 artiklan 2. kohdassa mainitun menettelyn mukaisesti. Menettelyn perusteella komissio voi todeta, etteivät kyseiset sopimuslausekkein annetut takeet ole riittäviä turvaamaan rekisteröityjen henkilötietoja.[103]

Yritysten tekemien virheiden välttämiseksi komissio on hyväksynyt mallisopimuslausekkeita. Näitä mallilausekkeita käyttämällä osapuolet voivat luottaa siihen, että ne antavat hyväksyttävät takeet tietosuojan turvaamisesta.[104] Kyseiset lausekkeet antavat verkkokaupalle oikeuden siirtää henkilötietoja laillisesti EU:n ja ETA-alueen ulkopuolelle.[105]

4.6.3. Valvonta

Henkilötietojen siirtämisen valvonta on käytännössä varsin vaikeaa, ellei jopa mahdotonta. Komissio on huomauttanut jäsenvaltioita ja niiden valvontaviranomaisia kansainvälisten tietojen vähäisestä valvonnasta.[106] Valvontaviranomaisten on kuitenkin vaikeaa saada tietoa kaikista siirroista, sillä pakollinen ilmoitusvelvollisuus henkilötietojen siirrosta on rekisterinpitäjällä itsellään. Rekisterinpitäjän tulee siis ilmoittaa komissiolle tai tietosuojavaltuutetulle mahdollisesta tietojen siirrosta EU:n ja ETA-alueen

[102] Viemerö 2009: 84
[103] Direktiivi 95/46/EY
[104] Komission päätös 2000/497/EY
[105] Rautanen: 23 -24. Tietosuoja3/2001
[106] Komission kertomus: 2003/265:19

ulkopuolelle vähintään 30 päivää ennen siirtoa. Tämän lisäksi verkkokaupan tulee ilmoittaa julkaisemassaan rekisteriselosteessaan, mikäli se siirtää henkilötietoja kolmansiin maihin.[107] Tämä tieto verkkokaupan asiakkaidenkin siis tulisi saada tietää. On kuitenkin ymmärrettävää, että valvonta on vaikeaa ja väärinkäytökset tällä saralla ovat mahdollisia.[108]

Valvonnan lisäksi ongelmia on aiheuttanut tietojen siirron käsite, jota on pidetty epämääräisenä ja tulkinnanvaraisena. Euroopan yhteisöjen tuomioistuin katsoi tapauksessa EY-101/01, että henkilötietojen julkaiseminen verkossa niin, että tiedot ovat myös kolmannessa maassa saatavilla, ei ole lainvastaista eikä sitä katsottu tietojen siirroksi kolmansiin maihin. Todennäköisesti tietojen siirto muulla tavoin on kuitenkin lainvastaista.[109]

[107] 523/1999. Henkilötietolaki.
[108] Castren: 35. Tietosuoja 1/2008.
[109] EYT: C 101/01.

5. MOBIILIKAUPANKÄYNNIN TIETOSUOJA

5.1. Mobiilipalvelut

Ostoksien tekeminen tietokoneella Internetin välityksellä on useimmille ihmisille jo tuttua. Tämän niin sanotun perinteisenä muotona tunnetun sähköisen kaupankäynnin edut ja haitat ovat tai ainakin niiden pitäisi olla ihmisten tiedossa. Uusi askel tässä kehittyvässä sähköisessä ympäristössä on mobiililaitteen avulla tehtävä kauppa. Siinä, missä sähköinen asioiminen on mielletty riippuvaiseksi tietokoneesta ja siihen kytketystä Internetistä, on mobiilikaupankäynnin etuna sen paikkariippumattomuus. Mobiilikaupankäynnillä tarkoitetaan siis palveluiden tarjoamista, joita toteutetaan tietotekniikan ja langattoman televiestinnän avulla.[110]

Mobiilipalveluiden tarjoaminen on valtaisa houkutus sähköisen kaupan yrityksille, sillä mobiililaite seuraa sen käyttäjää lähes kaikkialle, ja näin palvelut ovat koko ajan henkilön saatavilla. Alan toimijat kehittelevätkin uusia mobiilipalveluja tarjottavaksi asiakkailleen.[111] Nykyään on mahdollista jo tilata maksullisia soittoääniä, lukea lehtiä, ladata aikaa parkkimittariin tai jopa lainata rahaa matkapuhelimen välityksellä. Uusimpana, vielä kehitteillä olevalla palvelulla asiakkaan olisi mahdollista maksaa pienimuotoisia ostoksia puhelimellaan, jolloin tekstiviesti toimisi eräänlaisena luottokorttina.[112]

Palveluiden tarjonta lähentelee siis jo samaa kuin perinteisellä sähköisen kaupan puolella. Valitettavasti myös ongelmat ovat vähintäänkin vastaavat ja kuluttajien tietoisuus niistä taas vajavainen. Liikenne- ja viestintäministeriön perustama kehittämisohjelma ”Luottamus ja tietoturva sähköisissä palveluissa” julkaisi raportissaan 2.6.2005, että mobiilipalveluissa on tietoturvauhkia ja niihin tulee suhtautua vakavasti.[113] Mobiilipalveluissa esiintyvistä turvallisuusuhkista ehkä haasteellisimpina voidaan pitää käyttäjän luotettavaa tunnistamista ja luovutettujen tietojen luottamuksellisuutta. Pääpiirteittäin turvallisuusuhat ovat samat kuin perinteisen Internetissä harjoitettavan sähköisen kaupan puolella.

---

[110] Terämaa: 11-13. Tietosuoja 4/2000.
[111] Paananen 2000: 49- 55.
[112] Salminen: 6. Kauppalehti / 233.
[113] Komonen: 29. Tietosuoja 4/2005.

5.2. Sovellettava lainsäädäntö

Lainsäätäjä on ottanut huomioon teknisen kehityksen, ja sen vuoksi lainsäädäntö on säädetty teknologianeutraaliksi. Tarkoituksena on, että säännökset ovat sovellettavissa riippumatta toimintatavasta, siis siitä, millä tavalla sähköistä kauppaa toteutetaan. Mobiilikaupankäynnissä henkilötietojen ja yksityisyyden suoja perustuvat samaan EU-lainsäädäntöön ja Suomen lakiin kuin perinteinen sähköinen kauppa. Yleislakina henkilötietojen käsittelyssä sovelletaan henkilötietolakia ja noudatetaan sen asettamia velvoitteita. Tämän lisäksi mobiilipalveluita tarjoavan yrityksen tulee ottaa toiminnassaan huomioon sähköisen viestinnän tietosuojalaki, laki tietoyhteiskunnan palveluiden tarjoamisesta sekä laki vahvasta sähköisestä allekirjoituksesta. Edellä mainitut lait asettavat huomattavia haasteita palveluiden tarjoajille, joiden pitää toiminnassaan kyetä tunnistamaan asiakas luotettavasti, mikä luonnollisesti on asiakkaan etu, koska se lisää turvallisuutta.

Huomion arvoista on se, ettei palvelun tarjoaminen mobiililaittein lisää merkittävästi tietosuojaan liittyviä vaatimuksia yritykselle.[114] Lähtökohtana on, että yrityksen tulee täyttää samat velvoitteet tietosuojan turvaamisen osalta, tarjosi se palvelua mobiilipalveluna tai perinteisenä verkkokauppana Internetissä. Sähköistä kaupankäyntiä harjoittavan yrityksen tulee aina kerätessään, käsitellessään, säilyttäessään ja siirtäessään henkilötietoja ottaa huomioon tietosuojalainsäädäntö ja sen velvoitteet, joita olen aikaisemmin tutkimuksessa käsitellyt.[115] Näin ollen myös vastuu korvausvelvollisuudesta asiakkaiden henkilötietojen väärinkäytösten osalta on sama mobiilipalveluita tarjoavalle yritykselle.[116]

5.3. Tunnistaminen

Varsin haasteellista mobiilikaupankäynnissä on ollut järjestää lain 617/2009 edellyttämä käyttäjän luotettava tunnistaminen. Mobiilipalveluiden kasvavan suosion myötä teleyritykset ovat kiinnostuneet kehittämään uudenlaisia

[114] Terämaa: 11. Tietosuoja 4/2000.
[115] Ämmälä 2011: 25, 28 & 29.
[116] 523/1999. Henkilötietolaki.

tunnistusmenetelmiä perinteisten rinnalle. Yksi menetelmä jota pidetään erittäin luotettavana, on menetelmä jossa tunnistukseen käytetään kahta eri verkkoa: käyttäjän tunnistaminen tapahtuu matkapuhelimella käyttämällä puhelinverkkoa ja itse asiointi verkkokaupassa tehdään perinteisesti Internetissä.[117]. Tällä menetelmällä pyritään tuomaan vaihtoehto luotettavalle tunnistamiselle suorittamalla perinteisessä sähköisessä kaupankäynnissä tunnistus mobiililaitteella.

Tietosuojan kannalta kenties luotettavin tunnistuskeino on viranomaisten luoma kansalaisvarmenne.[118] Tässä vielä kehitteillä olevassa mobiili-varmenneessa on mahdollista laittaa matkapuhelimen SIM-korttiin henkilötodistus ja näin käyttää mobiililaitetta tunnistamisessa. Kyseinen ratkaisu olisi sen luotettavuuden takia erityisen kiinnostava vaihtoehto nimenomaan niin paljon käytetyille pankkitunnuksille.[119] Toistaiseksi suosituin tunnistusmenetelmä myös mobiilikaupankäynnissä on juuri pankkitunnukset.[120]

Nimenomaan puutteellinen tunnistaminen on yleensä ollut syynä väärinkäytöksiin mobiilipalveluissa. Identiteettivarkauksia on tapahtunut tilanteissa, joissa matkapuhelimen välityksellä on otettu lainaa niin sanotuilta pikavippifirmoilta. Tapauksissa lainan hakijan tunnistaminen on perustunut vain tämän ilmoittamaan henkilötunnukseen ja teleoperaattorin liittymätietoihin. Mikäli nämä ovat täsmänneet, henkilön on todettu olevan se henkilö, jonka väittää olevan. Tämän puutteellisen tunnistamisen seurauksena lainanottaja on saanut lainaa tekeydyttyään toiseksi henkilöksi tämän tiedoilla. Korkein hallinto-oikeus on kuitenkin katsonut 3.4.2009 antamassaan ratkaisussaan, että lainanhakija on tunnistettava luotettavasti henkilötietolain nojalla ja voimassa oleva laki sähköisestä allekirjoituksesta edellyttää samaa palvelun tarjoajilta.[121]

Tietosuoja mobiilikaupankäynnissä on lähtökohdiltaan vastaava kuin perinteissä sähköisessä kaupassa. Sitä veloittaa sama lainsäädäntö, ja kuluttajaa suojaavat samat säännökset ja viranomaiset mahdollisissa ongelmatilanteissa.

---

[117] Männikkö: 34 -35. Tietosuoja 2/2008
[118] Paananen 2000: 54
[119] Rautavuori: 18 -20. Tietosuoja 4/2010
[120] Männikkö: 34. Tietosuoja 2/2008
[121] KHO 2010: 1568/1/09

Käytännössä kuluttajan ja yrityksen tulee kuitenkin ottaa huomioon, ettämobiili palveluiden käyttämä tekniikkaa ja järjestelmät eivät ole vielä täysin luotettavia tietosuojan kannalta. Tämä on hyödyllistä muistaa käytettäessä mobiilipalveluita ja varsinkin luovutettaessa siellä omia henkilötietoja.

6. SÄHKÖISEN KAUPANKÄYNNIN HAASTEITA

Samalla kun sähköinen asioiminen verkossa on lisääntynyt nopeasti, ovat myös väärinkäytökset Internetissä yleistyneet. Verkossa tapahtuneen rikoksen, kuten petoksen tai kunnianloukkauksen, kohteeksi on kuluneen vuoden aikana joutunut 70 000 suomalaista. Yhtenä tekijänä voidaan pitää sitä, että kaikki kuluttajat eivät suhtaudu tietosuojauhkiin vakavasti, vaan luovuttavat tietojaan varsin helposti yrityksille varsinkin, jos yritykset tarjoavat tietoja vastaan jotain hyötyä. Tutkimusten mukaan erityisesti nuoret ja samalla suurin Internetin käyttäjäryhmä on luottavainen toimiessaan verkossa, eikä ole huolissaan omasta tietosuojastaan.

Kuluttajille ja yrityksille kuuluvat salassa pidettävät tiedot, kuten henkilötiedot ja pankkikorttinumerot, ovat nykyään täyttä kauppatavaraa Internetin ns. pimeillä markkinoilla. ”Internet on osoittautunut erinomaiseksi tunnistetietojen, ennen kaikkea henkilötunnusten, yhteystietojen sekä luottokorttitietojen lähteeksi.” [122] Esimerkiksi verkkokaupan asiakasrekisteristä luovutetun pankkitilinumeron arvo voi nousta lähes 1000 dollariin kappaleelta.[123]Ei siis ole ihme, että laittomuudet tällä alalla ovat lisääntyneet viime vuosina hurjaa vauhtia. Yhdysvalloissa CSI:n ja FBI:n tekemä tutkimus Computer Crime and Security Survey paljasti, että yritysten omat työntekijät tekevät rikkomuksista suurimman osan noin 80 % kuten tietojen luvattomana käyttönä tai petoksina.[124]

Käyttäjätunnuksia kerätään nykyään muun muassa erilaisilla haittaohjelmilla. Usein käyttäjä vahingossa lataa vakoiluohjelman koneellensa, joka aktivoiduttuaan kerää kaikki käyttäjän koneelle syöttämät tiedot mukaan lukien salasanat ja verkkopankkitunnukset ja lähettää ne Internetin kautta eteenpäin keräilypalvelimelle. Näin kuluttajatiedot voivat päätyä vääriin käsiin.[125] Näille varastetuille tiedoille on olemassa omat markkinat. Kyseiset tiedot ovat ostettavissa seuraavin hinnoin: luottokorttinumero >30 $,

[122] Heinonen: 22. Tietosuoja 2/2005.
[123] Kenneth 2010: 5-5, 5-7.
[124] Laaksonen 2006: 282.
[125] Husa: 10-12.

pankkitilinnumero 10- 1000 $, sähköpostiosoitteen salasana 1- 100 $ ja henkilötunnus 5- 7 $.[126]

Yksi koko ajan yleistyvä tietoverkkorikollisuuden muoto on ”hakkerointi”, joka laissa tunnetaan nimikkeellä tietomurto. Koska myös hakkerointi voi kohdistua henkilötietorekistereihin, on siitä hyvä mainita tässä yhteydessä. Rikoslain 38 luvun 8 momentin mukaan sellainen henkilö syyllistyy tietomurtoon, ”joka käyttämällä hänelle kuulumatonta käyttäjäntunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja, taikka sellaisen järjestelmän erikseen suojattuun osaan.”

6.2. Keinot vastata haasteeseen

Keinoja parantaa yksityisyyden suojaa on kehitelty ja koko ajan kehitellään erilaisia teknologisia ratkaisuja, joiden avulla henkilötietojen varastaminen voidaan tehdä vaikeaksi tai mahdottomaksi. Nämä teknologiset ratkaisut ovat avuksi nimenomaan edellä mainittuja haittaohjelmia vastaan. Yksi mainitsemisen arvoinen menetelmä on nimeltään Platform for Privacy preferences. Sen avulla käyttäjä voi arvioida jonkin tietyn yrityksen yksityisyydensuoja toimintaperiaatteita. Tarkoituksena on, että käyttäjä vertaa yrityksen toimintaperiaatteita omiinsa ja tekee sen perusteella ratkaisun, onko sivusto niin turvallinen, että omia henkilötietoja uskaltaa luovuttaa.[127] Haasteena on kuitenkin se, että kyseisten suojaratkaisujen käyttö on täysin käyttäjästä tai palvelun tarjoajasta riippuvaista eikä näin ollen vielä kovin yleistä.

Osalle sähköisten palvelujen käyttäjistä luottamus toista osapuolta kohtaan voi olla vaikeaa kenties jo tapahtuneiden väärinkäytöstapausten vuoksi. Tällöin oman luottokorttinumeron antaminen netissä voi olla vaikeaa. Tämän vuoksi jotkin yritykset ovat luoneet järjestelmiä, joilla on mahdollista asioida verkkokaupoissa ja maksaa ostoksia luottokortilla ilman, että verkkokauppa saa tietoon asiakkaan luottokorttinumeroa. Tällaisen kolmikantajärjestelmän on

[126] Kenneth 2010: 5-5 – 5-7.
[127] Komission tiedonanto 2007:228/2-luku.

kehitellyt muun muassa luottokorttiyhtiö Visa.[128] Se toimii eräänlaisena luotettavana välikätenä asiakkaan ja verkkokaupan välillä ja huolehtii maksun välityksestä ilman, että asiakkaan tietoja siirretään verkkokaupalle. Vastaavanlaisten järjestelmien käyttö ja yleistyminen sähköisessä kaupassa edistää huomattavasti ”varovaisten” asiakkaiden luottamusta.

Yksi sähköisen kaupan haasteista on sitä säätelevän lainsäädännön ajan tasalla pitäminen. Valitettavasti lainsäädäntö ja seurantatekniikka eivät ole kuitenkaan pysyneet haittaohjelmien kehityksen perässä. Lisäksi uudet tekniset ratkaisut luovat uusia muotoja sähköiselle kaupalle, kuten viime aikoina kovalla vauhdilla kasvava mobiilikaupankäynti. Tämä luo uusia haasteita tietoturvasta huolehtiville tahoille. Uuden tekniikan ja uusien sovellusten ilmestyessä on verkkorikollisten selvittäminen haasteellista eikä aina edes mahdollista ja syyllisyyttä voi olla mahdotonta todistaa. Tämän takia on hyvä panostaa tietoturvasta huolehtimiseen ja haittavaikutusten minimoimiseen.[129] Tämän lisäksi yritykset ja ihmiset olisi saatava tiedostamaan paremmin tietosuoja ja siihen kohdistuvat riskit.[130] Tällä saralla viranomaisilla riittää vielä töitä, sillä esimerkiksi vuonna 2004 tietosuojavaltuutetun tekemässä kyselyssä 50 % suomalaisista yrityksistä myönsi, ettei oikeastaan edes tunne tietosuojalainsäädäntöä eikä näin ollen sen velvoitteita.[131]

On siis selvää, että kaikki sähköisen kaupan alan yritykset tulee saada sisäistämään tietosuojan merkitys ja sitä koskeva lainsäädäntö. Näin tietoturva tällä saralla kasvaisi ja niin tahalliset kuin tahattomatkin väärinkäytökset saataisiin vähenemään. Sama pätee kuluttajiin, joiden tulisi kiinnittää huomiota omaan tietosuojaansa ja oikeuksiinsa. Euroopan unionin komission teettämän kyselyn perusteella 81 % vastanneista kertoi tuntevansa tietosuojan puutteellisesti, huonosti tai erittäin huonosti.[132]

Kun median uutisoi laajoista tietoturvamurroista, saadaan ihmisten huomio kohdistumaan tietosuojaan. Vuonna 2007 julkaistussa uutisessa kerrottiin 80 000 käyttäjätunnuksen ja salasanan joutuneen vääriin käsiin. Ne oli saatu haltuun hyödyntämällä juuri tietoturvassa ilmenneitä heikkouksia.

---

[128] Viemerö 2009: 221.
[129] Männikkö: 9. Tietosuoja 1/2010 & 7. Tietosuoja 4/2009.
[130] Linden: 22 -23. Tietosuoja 1/2009
[131] Eurobarometri 226
[132] Komission tiedonanto 2007: 87

Vastaavanlaisten tapausten johdosta ovat kuluttajat alkaneet arvioida verkkopalveluita tarjoavien toimijoiden luotettavuutta.

Nykyään Internetissä palveluja tarjoava yritys voi osoittaa, että sen tietoturvaratkaisut ovat tietosuojasäännösten mukaisia, ja käyttää tätä hyväksi mainonnassaan. Yritys voi todistaa sen sille myönnetyllä EuroPrise -tietosuojasertifikaatilla. Yritys voi saada sertifikaatin kahdeksi vuodeksi kerrallaan sertifiointiviranomaiselta.[133] Toinen keino kasvattaa kuluttajien luottamusta yritystä kohtaan on tietosuojatarkastukset, jotka Yhdysvalloissa ovat varsin yleisiä mutta käsitteenä Suomessa vielä melko tuntematon. Toiminnan periaatteena on, että ulkopuolinen konsulttiyritys suorittaa puolueettoman tarkastuksen, miten jokin yritys on huolehtinut henkilötietojen käsittelystä. Tarkoitus on selvittää, onko yritys huolehtinut lainmukaisista velvoitteista ja toimiiko se lain edellytysten mukaan.[134] Tällainen tietosuojatarkastus olisi mahdollista suorittaa myös viranomaisten toiminnasta ja rekistereistä. Viranomaiset voisivat näin edesauttaa sähköisen asioimisen luottamusta julkisissa palveluissa ja toimia esimerkkinä. Joka tapauksessa tällaisten laatua ilmaisevien tekijöiden toivotaan lisäävän luottamusta ja tietysti turvallisuutta sähköisessä asioimisessa.

[133] Vanto: 29.
[134] Viemerö 2009: 226.

7. JOHTOPÄÄTÖKSET

Elektronisen kaupankäynnin kasvulle on erityisen tärkeää osapuolten välinen luottamus. Euroopan unioni ja oma lainsäädäntömme on luonut säännöt, perusteet, joihin sähköisen kaupankäynnin tulee alueellamme perustua. Yhdysvalloissa liittovaltio ja eräät osavaltiot ovat lainsäädännöllä pyrkineet suojaamaan henkilötietoja verkossa. Kun palvelujaan verkossa tarjoavat yritykset toimivat näiden sääntöjen mukaan, on luottamuksen kasvulle sähköisessä kaupassa edellytykset.

Lainsäädäntömme perusteella verkkokaupan tulee käsitellä huolellisesti kaikkia antamiamme tietoja. Merkitystä ei ole sillä, vaikka verkkokauppa, jonka kanssa asioimme, olisi toisessa EU-jäsenvaltiossa, koska valtioita velvoittavat samat direktiivit. Tämän vuoksi asiakkaalla on perustellut syyt olettaa, että tietoja käsitellään yhtä turvallisesti, kuin oman maan lakien mukaan toimiva palvelujen tarjoajakin tekisi. Yhdysvalloissa lainsäätäjän näkökulma on ollut huomattavasti väljempi tietosuojaa kohtaan. Siellä henkilötietojen käsittely, säilyttäminen ja eteenpäin siirtäminen poikkeavat huomattavasti eurooppalaisesta käytännöstä. Yhdysvalloissa asiaa on lähestytty ennemminkin yritysten näkökulmasta asiakkaiden tietosuojan kustannuksella.

Yhdysvalloissa onkin uskottu markkinoiden itsesääntelyyn ja haluttu välttää liike-elämän velvoitteita. Samalla taas Euroopan unionissa on pyritty yhdistämään nämä kaksi hyvää eli edistää sähköisen kaupan toimintaa ja tietojen vapaata liikkuvuutta sekä henkilöiden tietosuojaa. Asiakkaan onkin syytä pitää Yhdysvaltalaisen verkkokaupan kanssa asioidessaan mielessä tämän mahdollisesti erilaiset tietosuojakäytännöt. Hyödyllistä onkin tutustua kuinka yritys itse kertoo huolehtivansa keräämistään asiakkaiden tiedoista. Huomattava merkitys on myös sillä missä osavaltiossa kyseinen yritys on rekisteröity. Kalifornian osavaltiossa rekisteröityneen yrityksen tietosuojakäytännöt vastaavat lähes EU-lainsäädännön velvoitteita.

Tutkimuksen johdannossa esitettyyn kysymykseen, kuinka voimme olla varmoja, että tietomme ovat turvassa, ei ole veden pitävää keinoa. Lainsäädäntö velvoittaa verkossa toimivat yritykset toimimaan lain mukaan ja näin se pyrkii suojelemaan kuluttajien ja yritysten salassa pidettäviä tietoja. Kuitenkin lainsäädännön edellytykset ovat rajoitetut tapauksissa, joissa jokin

taho pyrkii määrätietoisesti varastamaan henkilötietoja. Tällöin asiakkaan tulee myös omilla tietoturvatoimenpiteillään huolehtia tietosuojastaan. Ensisijaisen tärkeää on harkita kaupankäyntitilannetta ja -osapuolta tietosuojan kannalta. Asiakkaan omaan harkintaan jää, luottaako hän kyseiseen toimijaan. On syytä olla huolellinen, kun valitsee palveluntarjoajaa ja perehtyä sen itsestään antamaan informaatioon. Turvallisuus ja luottamus rakentuvat siis voimassa olevaan lainsäädäntöön ja käyttäjän omiin ratkaisuihin. Näistä ratkaisuista merkittävimmät ovat verkkokaupan luotettavuuden arviointi ja huolehtiminen tietokoneen tai mobiililaitteen tietoturvaratkaisuista.

Tutkimuksen alussa esitin kysymyksen, kuka on velvollinen korvaamaan väärinkäytöksen seurauksena syntyneet taloudelliset vahingot? Lähtökohta on, että väärinkäyttäjä korvaa syntyneet vahingot, mutta viime kädessä rekisterinpitäjä on aina vastuussa ja näin ollen korvausvelvollinen. Tilanteessa, jossa asiakas joutuu tietojensa väärinkäytön kohteeksi ja kärsii taloudellista tai muuta vahinkoa, esimerkiksi jos henkilö- tai tilitietoja on käyttänyt hyväksi kolmas osapuoli, on palveluntarjoaja viime kädessä velvollinen korvaamaan asiakkaalle koituneet vahingot. Näin ollen kuluttajan asema on tältä osalta turvattu. Asiakkaan oikeus korvaukseen on omiaan lisäämään asiakkaan luottamusta. Samalla se edesauttaa verkkokauppojen mielenkiintoa kehitellä yhä turvallisempia järjestelmiä turvatakseen rekisterinsä ja tietonsa niitä uhkaavilta tekijöiltä. Verkkokaupan kannalta nykyaikaisen tietoturvan järjestäminen on merkittävä kilpailutekijä, jota voidaan hyödyntää markkinoinnissa.

On kuitenkin syytä muistaa Euroopan unionin ja Yhdysvaltojen varsin erilaiset suhtautumiset vastuukysymyksiin ja korvauksiin. Yhdysvalloista puuttuu nimittäin säädökset vahingonkorvauksista, jos asiakas on kärsinyt taloudellista vahinkoa. Tämän seurauksena korvauksen saaminen lainsäädännön perusteella on oletettavasti vaikeampaa Yhdysvalloissa kuin esimerkiksi Suomessa. Lainsäätäjä on nähnyt vahingonkorvausvelvollisuuden lisäksi tärkeänä säätää lainrikkojalle lisäseuraamuksia. Teon vakavuuden mukaan väärinkäytöksestä voi vahingonkorvausvelvollisuuden lisäksi seurata rikoslain perusteella sakkoa tai vankeutta.

Voidaan tiivistetysti sanoa, että sähköisen kaupan tietosuoja on melko ”hauras”. Se on varsin haavoittuvainen väärinkäytöksille, jotka vaikuttavat koko sähköisen kaupan maineeseen. Tietosuojaa turvaamaan on luotu

lainsäädäntö ja valvontaviranomaiset, joilla on tarkoitus vahvistaa tietosuojaa alueellaan. Tekniset tietoturvaratkaisut ja käyttäjien tilanneharkinta tukevat lainsäädäntöä ja näin tämä kolmikanta pyrkii turvaamaan ihmisten ja yritysten tietosuojaa elektronisessa kaupankäynnissä. Hyvä tietosuoja rakentuu siis näistä kolmesta tekijästä. Sähköinen kauppa kasvaa koko ajan ja tekniikka kehittyy. Siksi turvallisuustekijöitä pitää päivittää ja kehittää taukoamatta. Näin luottamus sähköistä kaupankäyntiä kohtaan lisääntyy. Tietosuojasta huolehtimisella on alati kasvava merkitys sähköisen kaupan kehitykselle.

LÄHDELUETTELO

Euroopan unionin lainsäädäntö:

Euroopan neuvoston (1999) direktiivi 1999/93/EY sähköisiä allekirjoituksia koskevista yhteisyön puitteista

Euroopan neuvoston (1995) direktiivi 95/46/EY yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta

Euroopan neuvoston (2002) direktiivi 2002/58/EY henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla

Euroopan neuvoston (2000) direktiivi 2000/31/EY tietoyhteiskunnan palveluja, erityisesti sähköistä kaupankäyntiä, sisämarkkinoilla koskevista tietyistä oikeudellisista näkökohdista

Euroopan parlamentin ja neuvoston elektronisen kaupankäynnin aloite (1997), KOM (97)157).

Euroopan komission päätös (2004) 2001/497/EY vaihtoehtoisen mallisopimuslausekkeiden ottamiseksi käyttöön henkilötietojen kolmansiin maihin siirtoa varten

Euroopan parlamentin ja neuvoston (2008) direktiivi ehdotus 2008:614 lopullinen

Suomen lainsäädäntö:

Henkilötietolaki 22.4.1999/523

Laki tietoyhteiskunnan palveluiden tarjoamisesta 5.6.2002/458

Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 7.8.2009/617

Sähköisen viestinnän tietosuojalaki 16.6.2004/516

Hallituksen esitys (36/2009) laiksi vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista.

Hallituksen esitys (125/2003) laiksi sähköisen viestinnän tietosuojasta.

Rikoslaki 19.12.1889/39

Vahingonkorvauslaki 31.5.1974/412

Yhdysvaltain lainsäädäntö:

United States Constitution

Uniform Electronic Transactions Act

California Civil Code

California Business and Professions Code

Kirjallisuus:

Aalto, Antti, Virpi Halonen, Juote, Taru, Järvinen, Vilho & Wihuri, Pauli (2000) Sähköinen liiketoiminta. Jyväskylä: Gummerus Kirjapaino Oy. ISBN 951 -8993 -77-7.

Castren, Kirsi (2008). Henkilötietojen luovutus. Tietosuoja 1/2008.

Castren, Kirsi (2010). Yksi tunnus monta palvelua. Tietosuoja 1/2010.

Heinonen, Risto (2005). Identiteetin väärinkäytökset lisääntyvät Internetin käytön myötä. Tietosuoja 5/2005.

Husa, Ari (2010). Tietoturva on yhä paljon käyttäjän varassa. Tietosuoja 1/2010.

Kenneth C Laudon & Carol Guercio Traver (2010). E- Commerce 2010 Business. Technology. Society. Pearson. 4 Part. ISBN 10: 0 -13 -509078 -4

Kettunen, Sami & Marko Filenius (1998). Elektroninen kaupankäynti. Jyväskylä: Gummerus kirjapaino Oy. 195 s. ISBN: 952-5159-35-3.

Kulla, Heikki (2002). Viestintäoikeus. Vantaa: WSOY. 372 s. ISBN: 951-670-068-3.

Laaksonen, Mika, Nevasalo Terho & Tomula Karri (2006). Yrityksen tietoturvakäsikirja. Helsinki: Oy Nordprint Ab. 324 s. ISBN: 951-37-4701-8.

Laine Juha (2001). Verkkokauppaoikeus. Helsinki: WSOY. ISBN: 951 -670 -039-X.

Linde, Suvi (2010). Ei tuurilla vaan taidolla. Tietosuoja 1/2009.

Luhtasela, Harri (2007). Sähköisen kuluttajakaupan sääntely Euroopan unionissa ja Yhdysvalloissa. Vaasan yliopiston julkaisu. 445s. ISBN: 978-952-476-189-5.

Luhtasela Harri (2003). Sähköisen kuluttajakaupan oikeudellinen sääntely. Talousoikeuden lisensiaattitutkimus. Vaasa.

Männikkö, Päivi (2008). Mobiili tunnistaminen tekee tuloaan. Tietosuoja 2/2008.

Männikkö, Päivi (2010). Luottamusta keräämässä. Tietosuoja 1/2010.

Neuvonen, Risto (2008). Viestintäoikeuden perusteet. Helsinki: Talentum. 227 s. ISBN: 978-952-14-1271-4.

Niskanen, Maarit (2010). Oikeusjärjestys osa 3. Rovaniemi: Lapin yliopiston oikeustieteellisiä julkaisuja. ISBN: 978-952-484-360-8.

Paananen, Vesa-Matti, Jukka Kolari & Veistola Pekka (2000) Wap ja mobiili tulevaisuus. Jyväskylä: Gummerus kirjapaino Oy. 126 s. ISBN: 952-5344-07-x.

Pöysti, Tuomas (1999). Tehokkuus, informaatio ja eurooppalainen oikeusalue. Helsinki: Hakapaino OY. 538 s. ISBN: 951-45-8831-2.

Rahnasto, Ilkka (2002). Internet-oikeuden perusteet. 3. uudistettu painos. Vantaa: Talentum Media Oy. ISBN: 952 -14 -0647 –X.

Rautanen, Sirpa (2000). Kansainväliset tietojen siirrot. Tietosuoja 1/2001.

Rautanen, Sirpa (2001). Mallisopimuslausekkeet helpottamaan henkilötietojen kansainvälistä siirtoja. Tietosuoja 3/2001.

Rautavuori, Marjo (2010). Mobiili-varmenne kohta markkinoille. Tietosuoja 4/2010.

Salminen, Markus (2009). Tietosuoja sähköisessä liiketoiminnassa. Talentum Media Oy. ISBN: 978 -952 -14 -1370 -4.

Salminen, Markus (2010). Verkkokaupan tietosuoja. Tietosuoja 2/2010.

Salminen, Merita (2010). Tekstiviesti toimii pian luottokorttina. Kauppalehti numero 233.

Simon & Simon (2001). E-Commerce Law Doing Business Online. Palladian Law Publishing Ltd. 296 s. ISBN: 1-902558-45-6

Vanto, Jarno (2009). Sertifioitua tietosuojaa koko EU:ssa. Tietosuoja 4/2009.

Viemerö, Mikko (2010). Tietosuoja on verkkokauppiaan etu. Tietosuoja 1/2009

Viemerö, Mikko (2009). Omat tiedot haltuun. Tietosuoja 4/2009.

Viemerö, Mikko (2009). Tietosuoja sähköisessä kaupassa ja sähköisessä viestinnässä. Helsingin kauppakorkeakoulun julkaisu. 236 s. ISBN: 978-952-488-376-4.

Warma, Eija (2004). Tietosuoja Euroopassa yksityisyys Yhdysvalloissa. Tietosuoja 4/2004.

Warma, Eija (2010). Sähköinen liiketoiminta. Tietosuoja 3/2010.

Warma, Eija (2010). Muutosta ilmassa. Tietosuoja 4/2010.

Sähköinen aineisto:

Eurobarometri 226 (2008). Data Protection in the European Union. 9 s. [online]. [25.1.2011]. Saatavana World Wide Webistä: http://ec.europa.eu/public_opinion/flash/fl_226_en.pdf

Euroopan yhteisöjen komission kertomus 265 (2003). Komission ensimmäinen kertomus tietosuojadirektiivin (EY 95/46) täytäntöönpanosta. [online]. [28.1.2011]. Saatavana World Wide Webistä: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0265:FIN:FI:PDF

Euroopan komission tiedonanto 228 (2007). Komission tiedonanto Euroopan parlamentille ja neuvostolle tietosuojan vahvistamisesta yksityisyyden suojaa parantavilla tekniikoilla. [online]. [27.1.2011]. Saatavana World Wide Webistä: http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=fi&type_doc=COMfinal&an_doc=2007&nu_doc=228

Euroopan komission tiedonanto 87 (2007). Komission tiedonanto Euroopan parlamentille ja neuvostolle tietosuojadirektiivin tehokkaampaa soveltamista koskevan työohjelman seurannasta. [online]. [26.1.2011]. Saatavana World Wide Webistä: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0087:FIN:FI:PDF

FTC (2000 b). Fair Information Practice in the Electronic Market place. A Report of Congress. [online]. Saatavana World Wide Webistä: http://www.ftc.gov/reports/privacy2000/privacy2000.pdf

Komission Vihreä kirja toimintavaihtoehdoista etenemiseksi kohti kuluttajia ja yrityksiä hyödyttävää sopimusoikeutta KOM 2010:348. [online]. Saatavana World Wide Webistä: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0348:FIN:FI:PDF

Luottamus, Tietoturva, Sähköiset palvelut. (2006). Tietoturva opas sähköisen palvelun tarjoajalle. [online]. ISBN: 952-201-789-2. (verkkojulkaisu). [20.4.2010]. Saatavana World Wide Webistä: http://www.lvm.fi/fileserver/8_2006.pdf

Safe harbor –järjestelmän kotisivut. (2011). U.S.-EU & Swiss Safe Harbor Frameworks Introduction. [online]. [27.1.2011] Saatavana World Wide Webistä: http://export.gov/safeharbor

Tieke, tietoyhteiskunnan kehittämiskeskus. (2003). Sähköisen kaupankäynnin aapinen. [online]. [10.2003]. Saatava World Wide Webistä: http://www.tieke.fi/mp/db/file_library/x/IMG/12422/file/Sahkoisenkaupankaynninaapinen.pdf

Tietosuojavaltuutetun toimisto. (2011). Yhdysvaltalainen Safe harbor –järjestelmä. [2011]. [27.1.2011]. Saatavana World Wide Webistä: http://www.tietosuoja.fi/25914.htm

UNCITRAL (1998). Model Law on Electronic Commerce with Guide to Enactment [online]. Saatava World Wide Webistä: http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf

Viestintävirasto: Viestintäviraston esittely. [online]. [27.4.2010]. Saatavana World Wide Webistä: http://www.ficora.fi/index/viestintavirasto/esittely.html

OIKEUSTAPAUSLUETTELO