Viestintäsalaisuuden loukkaus sosiaalisessa mediassa

30.09.2014

Marko Forss

Sisällysluettelo

Lähdeluettelo

KIRJALLISUUSLÄHTEET

Innanen, Antti – Saarimäki, Jarkko: Internetoikeus. 2., uudistettu painos. Porvoo 2012.

Lehtonen, Asko: Sähköpostin suojasta 2001. Teoksessa Oikeustieteen rajoja etsimässä. Juhlajulkaisu Juha Tolonen 15.4.2001. Turku 2001.

Neuvonen, Riku: Yksityisyyden suoja Suomessa. Viro 2014.

Nyblin, Klaus: Työelämän sähköposti. 2. painos. Helsinki 2004.

Nyblin, Klaus: Työelämän sähköposti. 3., uudistettu painos. Helsinki 2009.

Pesonen, Pirkko: Sosiaalisen median lait, Viro 2013.

Pihlajamäki, Antti: Tietojenkäsittelyrauhan rikosoikeudellinen suoja. Jyväskylä 2004.

VIRALLISLÄHTEET

HE 221/2013 vp. Hallituksen esitys eduskunnalle tietoyhteiskuntakaareksi sekä laeiksi maankäyttö- ja rakennuslain 161 §:n ja rikoslain 38 luvun 8 b §:n muuttamisesta.

HE 48/2008 vp. Hallituksen esitys Eduskunnalle sähköisen viestinnän tietosuojalain ja eräiden siihen liittyvien lakien muuttamisesta.

HE 125/2003 vp. Hallituksen esitys Eduskunnalle sähköisen viestinnän tietosuojalaiksi ja eräiksi siihen liittyviksi laeiksi.

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

HE 257/1994 vp. Hallituksen esitys Eduskunnalle tullilaiksi ja laiksi tullilaitoksesta annetun lain muuttamisesta.

HE 309/1993 vp. Hallituksen esitys Eduskunnalle perustuslakien perusoikeussäännösten muuttamisesta.

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

HE 66/1988 vp. Hallituksen esitys eduskunnalle rikoslainsäädännön kokonaisuudistuksen ensimmäisen vaiheen käsittäväksi rikoslain ja eräiden muiden lakien muutoksiksi.

PeVL 18/2014 vp. Perustuslakivaliokunnan lausunto liittyen hallituksen esitykseen tietoyhteiskuntakaareksi sekä laeiksi maankäyttö- ja rakennuslain 161 §:n ja rikoslain 38 luvun 8 b §:n muuttamisesta.

PeVL 33/2013 vp. Perustuslakivaliokunnan lausunto liittyen hallituksen esitykseen laeiksi poliisilain sekä eräiden siihen liittyvien lakien muuttamisesta.

LiVM 13/2004 vp. Liikenne- ja viestintävaliokunnan mietintö 13/2004 liittyen hallituksen esitykseen sähköisen viestinnän tietosuojalaiksi ja eräiden muiden lakien muuttamisesta.

OMML 27/2014. Oikeusministeriön mietintöjä ja lausuntoja 27/2014. Tietoverkkorikosdirektiivin täytäntöönpano.

INTERNETLÄHTEET

https://www.viestintavirasto.fi<tietoatoimialasta<katsauksetjaartikkelit<posti<postipalveluidenkehitys. Luettu 18.7.2014.

http://www.lvm.fi<vireillä<hankkeet<tietoyhteiskuntakaari. Luettu 27.5.2014.

http://www.viestintavirasto.fi/<tietoatoimialasta<tilastot<internetjapuhelin<tekstiviestit. Luettu 27.5.2014.

http://www.washingtonpost.com/blogs/worldviews/wp/2012/11/12/heres-the-e-mail-trick-petraeus-and-broadwell-used-to-communicate/. Luettu 27.5.2014.

Lehtonen, Asko 2005: Sähköpostin rikosoikeudellisen suoja kehitys muutosten paineissa. Oy Edita Ab (julkaistu aiemmin 2005 ja Edilexissä 2006). Saatavilla pdf-muodossa: <URL: http://www.edilex.fi/artikkelit/3420.pdf>. Luettu 30.04.2014.

OIKEUSTAPAUKSET

Korkein oikeus

KKO 2012:81
KKO 1992:179

Hovioikeus

Helsingin hovioikeus (14.3.2006, R 04/746)

Käräjäoikeus

Helsingin käräjäoikeus (28.03.2014, R 13/9449)

Satakunnan käräjäoikeus (07.03.2014, R 13/2029)

Unionin tuomioistuin

C-293/12 ja C-594/12 (yhdistetty). High Court (Irlanti) 27.1.2012 ja Verfassungsgerichtshof (Itävalta) 28.11.2012. Tuomio annettu 8.4.2014.

MUUT LÄHTEET

AOA 28.8.1998. Dnro 2049/4/96.

AOA 12.6.2012. Dnro 1207/2/10

Euroopan parlamentin ja neuvoston direktiivi 2006/24/EY, annettu 15. päivänä maaliskuuta 2006, yleisesti saatavilla olevien sähköisten viestintäpalvelujen tai yleisten viestintäverkkojen yhteydessä tuotettavien tai käsiteltävien tietojen säilyttämisestä ja direktiivin 2002/58/EY muuttamisesta.

LYHENNELUETTELO

AOA	Eduskunnan apulaisoikeusasiamies
EY	Euroopan yhteisö
HE	hallituksen esitys
HolhL	laki holhoustoimesta (442/1999)
LHL	laki lapsen huollosta ja tapaamisoikeudesta (361/1983)
LiVM	liikenne- ja viestintävaliokunnan mietintö
OMML	oikeusministeriön mietintöjä ja lausuntoja
PeVL	perustuslakivaliokunnan lausunto
PL	perustuslaki
PostiL	postilaki (415/2011)
RL	rikoslaki (39/1889)
SVTSL	sähköisen viestinnän tietosuojalaki (516/2004)
TL	tullilaki (1466/1994)

1 Johdanto

Luottamuksellinen viestintä, eli perinteisesti ilmaistuna kirjesalaisuus, on ollut jo vuosisatojen ajan osa länsimaista yhteiskuntaa. Suomessa kirjesalaisuus tuli perusoikeudeksi itsenäisyyden myötä, koska sitä ennen autonomian loppuaikana postitoimi oli ollut Venäjän valvonnassa. Vuoden 1917 hallitusmuodossa turvattiin kirje-, lennätin- ja puhelinsalaisuus. Nykyisin kirjesalaisuutta kutsutaan viestintäsalaisuudeksi, koska luottamuksellinen viestintä on saanut yhä enemmän uusia muotoja.[1]

> Sähköisen viestinnän myötä perinteisiä kirjeitä lähetetään yhä harvemmin. Viestintäviraston tilastojen mukaan kirjeiden määrän lasku nopeutui entisestään vuonna 2013, mutta edelleen lähetettiin noin miljardi kirjettä. Määrä väheni edellisestä vuodesta noin 6 prosentin verran. Vuonna 2012 laskujen osuus oli jopa 40 prosenttia kaikista kirjeistä, mutta näistäkin yhä suurempi osa on muuttumassa sähköisiksi, koska paperiversioista on alettu perimään erillisiä maksuja.[2]
>
> Myös sähköisessä viestinnässä tapahtuu koko ajan muutoksia viestin lähetystapojen kohdalla, koska erilaiset sosiaalisen median palvelut, kuten Facebook, Whatsapp ja Kik Messenger, ovat ajaneet viestimäärissä jo perinteisten tekstiviestien ohi. Tekstiviestien määrä lähti laskuun vuoden 2012 ensimmäisen vuosipuolikkaan jälkeen. Tuolloin tekstiviestejä lähetettiin 2 795 miljoonaa, jonka jälkeen se on laskenut tasaisesti, ollen vuoden 2013 toisella puolikkaalla 2 550 miljoonaa.[3]

Lähtökohtana viestintäsalaisuudelle on nykyään kansainvälisten sopimusten lisäksi perustuslain (731/1999) 10 §, jonka 2 momentin mukaan kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton. Perusoikeusnäkökulma on oleellinen etenkin internetiin ja sosiaaliseen mediaan liittyvässä viestinnässä. Internet on nykyään keskeinen väline kansalaiselle toteuttaa perusoikeuksiaan. Perus- ja ihmisoikeuksilla on perinteisesti pyritty suojamaan yksittäisen kansalaisen asemaa julkisen vallankäyttöä vastaan, mutta perustuslain 22 §:n mukainen velvoite koskee myös yksityisten keskinäisiä suhteita. Valtiolta vaaditaan siis aktiivisia toimenpiteitä perusoikeuksien toteuttamiseksi myös yksityisten välisissä suhteissa, jonka tärkeys on korostunut sosiaalisen median palvelujen myötä.[4]

---

[1] *Neuvonen* 2014, s. 137-138.

[2] [https://www.viestintavirasto.fi<tietoatoimialasta<katsauksetjaartikkelit<posti<postipalveluidenkehitys2013.html] (18.7.2014)

[3] [https://www.viestintavirasto.fi/tietoatoimialasta/tilastot/internetjapuhelin/tekstiviestit.html] (27.5.2014)

[4] Ks. tarkemmin sähköisestä viestinnästä perusoikeutena ja perusoikeuksien vaikutuksesta sähköisen viestintään toimintavelvoitteena teoksesta *Innanen – Saarimäki 2012*.

Viestinnän rikosoikeudellinen suoja perustuu ensisijaisesti rikoslain (39/1889, RL) 38 luvun 3 §:ään viestintäsalaisuuden loukkauksesta sekä sen törkeään tekomuotoon (RL 38:4). Merkitystä on myös tietomurron (RL 38:8) ja sen törkeän tekomuodon (38:8a) tunnusmerkistöllä. Vaitiolovelvollisuutta suojaa salassapitorikos (RL 38:1) ja salassapitorikkomus (RL 38:2). Laki yksityisyyden suojasta työelämässä (759/2004) täydentää yksityisyyden suojaa työelämässä viestinnän osalta. Sähköisen viestinnän suojaa täydentää sähköisen viestinnän tietosuojalaki (516/2004, SVTSL), jonka tarkoituksena on turvata sähköisen viestinnän luottamuksellisuus ja yksityisyys.[5] Laista löytyy rangaistussäännös, jonka mukaan voidaan tuomita sähköisen viestinnän tietosuojarikkomuksesta sakkoon (SVTSL 42). Sähköisen viestinnän tietosuojalaista löytyy keskeiset määritelmät sähköisen viestinnän osalta.

Viestintäsalaisuus koskee viestin sisältöä ja siihen liittyviä tunnistamistietoja, mutta viestin sisältämällä tiedolla ei sinänsä[6] ole vaikutusta viestin luottamuksellisuuteen. Viestintäsalaisuus koskeekin perinteisen kirjeen tai muun luottamuksellisen viestin avaamista. Myös puhelujen kuuntelu on suojattu käytävän keskustelun sisällöstä riippumatta. Sähköinen viestintä saa yhtä lailla suojaa perinteisen kirjesalaisuuden rinnalla, koska perusoikeussäännös ja siten myös viestintäsalaisuuden loukkauksen kriminalisointi on tarkoitettu välineneutraaliksi.[7]

Kirjoituksen ensisijaisena tarkoituksena on selvittää miten viestintäsalaisuutta suojataan erityisesti yksityisten tahojen, so. tilaaja tai käyttäjä, välisissä tapauksissa sosiaalisen median palveluissa. Arvioin siis lähinnä yksittäisen kansalaisen oikeutta lukea tietyn henkilön sosiaalisessa mediasta löytyvän profiilin kirjoittamia tai vastaanottamia viestejä. En esimerkiksi perehdy tarkemmin teleyritysten tai yhteisötilaajien rooliin. Tarkoituksenani ei ole myöskään käsitellä tarkemmin teon törkeää tekomuotoa, työelämään liittyvää lainsäädäntöä tai viranomaisen pakkokeino-oikeuksia. Aion tuoda esille sosiaaliseen mediaan liittyviä tulkintaongelmia sekä esittää lainsäädäntökritiikkiä. Ensin käyn kattavasti läpi viestintäsalaisuuden loukkauksen säännöksen sisällön. Kolmannessa kohdassa päästään kunnolla käsiksi sosiaaliseen mediaan liittyviin tulkintaongelmiin, vaikka niitä sivutaan tekstissä jo aikaisemmin.

---

[5] Perinteisestä kirjesalaisuudesta on säädetty postilaissa (415/2011).
[6] Viestin sisältämällä tiedolla voi olla jotain vaikutusta suojaan, koska viestintäsalaisuuden loukkauksen esitöiden *HE 94/1993 vp* (s. 149) mukaan mainos- ja massakirjeiden osalta lähetysten vähäinen suojan tarve tulisi ottaa huomioon sekä teon oikeudettomuustunnusmerkkiä arvioitaessa että rangaistusta mitattaessa.
[7] *HE 309/1993 vp*. s. 53.

2 Viestintäsalaisuuden loukkaus

Viestintäsalaisuuden loukkauksesta säädetään rikoslain 38 luvun 3 §:ssä. Luvusta löytyy myös teon törkeä tekomuoto ja sääntelyä muihinkin tieto- ja viestintärikoksiin liittyen. Viestintäsalaisuuden loukkauksen edeltäjä oli viestintärikos, josta säädettiin silloisen rikoslain 38 luvun 8 §:ssä[8]. Nykymuotoisen viestintäsalaisuuden loukkauksen esityöt ovat vuodelta 1993 ja säännös tuli voimaan 1995, joten esitöissä ei ole pystytty ottamaan huomioon täysimääräisesti sosiaalisen median mukanaan tuomia muutoksia. Säännöksen soveltamista on kuitenkin helpottanut yleisellä tasolla se, että sääntely on teknologianeutraalia, jolloin säännöstä voidaan soveltaa myös nykyaikaiseen luottamukselliseen sähköiseen viestintään sosiaalisessa mediassa. Korkeimman oikeuden ennakkopäätöksiä viestintäsalaisuuden loukkaukseen internetiin liittyen ei löydy yhtäkään[9].

Alun perin tunnusmerkistö oli jaettu kolmeen osaan, joista ensimmäinen käsitti perinteisen kirjesalaisuuden loukkaamisen täydennettynä sähköisesti tallennettua viestiä koskevalla lisäyksellä, toinen salakuuntelun ja kolmas puhelin-, lennätin tai muun telesalaisuuden loukkaamisen.[10] Viestintäsalaisuuden loukkausta muutettiin vuonna 2000, jolloin silloisen säännöksen 1 momentin 2 kohdan mukainen salakuuntelua koskeva tekotapatunnusmerkistö siirrettiin uuteen rikoslain 24 luvun 5 §:ään[11]. Tuolloin 1 momentin 3 kohdassa ollut telesalaisuuden sääntely siirrettiin 2 kohdaksi. Pykälän sisältöön ei tehty muulta osin muutoksia.

Rikoslain 38 luvun 3 §:ssä viestintäsalaisuuden loukkauksesta[12] säädetään seuraavasti:

> *Joka oikeudettomasti*
>
> *1) avaa toiselle osoitetun kirjeen tai muun suljetun viestin taikka suojauksen murtaen hankkii tiedon sähköisesti tai muulla vastaavalla teknisellä keinolla tallennetusta, ulkopuoliselta suojatusta viestistä taikka*

[8] Ks. tarkemmin säännöksen esityöt *HE 58/1988 vp.*
[9] Muitakaan viestintäsalaisuuden loukkaukseen liittyviä ratkaisuja ei löydy kuin kaksi, joita käsittelen lyhyesti tässä kirjoituksessa. Viestintäsalaisuuden loukkauksia ei ole päätynyt myöskään hovioikeuksiin juurikaan, koska tilaamani aineiston mukaan viestintäsalaisuuden loukkausta on käsitelty esimerkiksi Helsingin hovioikeudessa vain kymmenisen kertaa viimeisen kymmenen vuoden aikana.
[10] *HE 94/1993 vp*, s. 148.
[11] Ks. tarkemmin *HE 184/1999 vp*.
[12] Kirjoitushetkellä viestintäsalaisuuden loukkauksen rangaistusmaksimia suunnitellaan muutettavaksi kahteen vuoteen vankeutta. Tarkoituksena on myös muuttaa säännöstä siten, että se suojaisi myös tietojärjestelmän sisäistä luottamuksellista datan siirtoa. Uudistus liittyy tietoverkkorikosdirektiivin täytäntöön panoon, jonka osalta *OMML 27/2014* on lähetetty lausunnoille.

> *2) hankkii tiedon televerkossa välitettävänä olevan puhelun, sähkeen, tekstin-, kuvan- tai datasiirron taikka muun vastaavan televiestin sisällöstä taikka tällaisen viestin lähettämisestä tai vastaanottamisesta,*
>
> *on tuomittava* viestintäsalaisuuden loukkauksesta *sakkoon tai vankeuteen enintään yhdeksi vuodeksi.*
>
> *Yritys on rangaistava.*

Teon tulee ensinnäkin olla oikeudeton, joten esimerkiksi loukatun suostumukseen perustuva kirjeiden avaaminen tai sähköpostien lukeminen ei ole rangaistavaa. Koska viestintäsalaisuus nauttii perusoikeussuojaa, tulee loukatun suostumukseen kuitenkin suhtautua mieluummin pidättyvästi[13]. Vaihtoehtoisesti kyse voi olla myös lakiin perustuvasta oikeudesta, kuten poliisin suorittamasta telepakkokeinosta, mutta oikeudet on rajattu perustuslain mukaisesti suppeiksi[14]. Vaikka viestin sisältö ei vaikuta viestintäsalaisuuden loukkauksen täyttymiseen. on esitöissä kuitenkin todettu, että mainos- ja massakirjeiden osalta lähetysten vähäinen suojan tarve tulisi ottaa huomioon sekä teon oikeudettomuustunnusmerkkiä arvioitaessa että rangaistusta mitattaessa[15].

Oikeudettomuusvaatimuksen takia teon tulee olla tahallinen. Tahallisuutta voidaan arvioida ensisijaisesti tietomurron esitöiden perusteella, koska luottamukselliseen sähköiseen viestiin tulee päästä käsiksi suojaus murtaen.[16] Tietomurron esitöiden mukaan esimerkiksi järjestelmän satunnainen epäkunto ja siitä johtuva ulkopuolisen pääsy lukemaan luottamuksellisia viestejä, ei täytä rikoksen tunnusmerkistöä. Rangaistavaa ei myöskään ole se, että joku pääsee tai joutuu tietojärjestelmään vahingossa, esimerkiksi syöttämällä virheellisen käyttäjätunnuksen[17]. Tahallisuusvaatimuksen mukaan tekijän tulee siis tietää tunkeutuvansa tietojärjestelmään tai sen osaan oikeudettomasti[18].

> Korkeimman oikeuden ratkaisussa KKO 2012:81 oli kyse tapauksesta, jossa vartija oli avannut tutkintavangille Rikosseuraamuslaitoksesta saapuneen kirjeen, jota tutkintavankeuslain mukaan ei olisi saanut avata. Tutkintavanki vaati valtion velvoittamista suorittamaan hänelle vahingonkorvausta viestintäsalaisuuden loukkauksen aiheuttamasta kärsimyksestä. Kirjeen oli avannut erehdyksessä vankilassa harjoittelujaksoaan suorittanut vartija, joka oli tarkastanut ensimmäistä kertaa

[13] *HE 94/1993 vp*, s. 151. Ks. myös Eduskunnan apulaisoikeusasiamiehen ratkaisu 1207/2/10 12.6.2012, jossa oli kyse paperisten kirjeiden avaamisesta ja niiden skannaamisesta sähköistä jatkolähettämistä varten.
[14] Kirjesalaisuuden vahva suoja käy ilmi selkeästi myös esimerkiksi tullilain (1466/1994) esitöissä *HE 257/1994 vp*, jossa mainitaan nimenomaisesti, että vaikka tulli saa avata kirjeen ja tutkia sen sisältämää tavaran laadun, suojaa viestiä ehdoton kirjesalaisuus.
[15] *HE 94/1993 vp*, s. 149.
[16] Perinteisen kirjeen kohdalla tahallisuus näkyy kirjeen avaamisena.
[17] *HE 94/1993 vp*, s. 155.
[18] Ks. tarkemmin tietoverkkorikosten tahallisuudesta *Pihlajamäki 2004*, s. 247-259.

> vankien kirjeenvaihtoa. Vartija oli heti kirjeen avattuaan havainnut sen olevan Rikosseuraamuslaitokselta ja käsittänyt tehneensä virheen. Korkein oikeus katsoi alempien oikeusasteiden tapaan, että kyse oli erehdyksestä. Kyseessä ei siten ollut tahallinen teko, joten teko ei ollut rangaistava.
>
> Analogian mukaan myös tiedon hankkiminen sähköisestä viestistä tulee tapahtua tahallisen tietoisesti, eikä esimerkiksi vahingossa auki klikattu viesti täytä teon tunnusmerkistöä korkeimman oikeuden ratkaisun perusteella.

Oikeudettomuusvaatimuksen lisäksi säännöksestä voidaan erottaa neljä eri tekomuotoa, jotka on jaettu säännöksessä kahteen eri kohtaan. Ensimmäisessä kohdassa kriminalisoidaan a) toiselle osoitetun kirjeen tai muun suljetun viestin avaaminen ja b) tiedon hankkiminen suojauksen murtaen sähköisesti tai muulla teknisellä keinolla tallennetusta ulkopuoliselta suojatusta viestistä. Toisessa kohdassa rangaistavaksi on säädetty c) tiedon hankkiminen televerkossa välitettävänä olevan puhelun, sähkeen, tekstin, tekstin-, kuvan-, tai datasiirron taikka muun vastaavan televiestin sisällöstä sekä d) tiedon hankkiminen viestin lähettämisestä tai vastaanottamisesta.

Viestintäsalaisuuden loukkaus on asianomistajarikos, ellei rikoksentekijä rikosta tehdessään ole ollut yleistä posti- tai teletoimintaa harjoittavan laitoksen palveluksessa taikka ellei erittäin tärkeä yleinen etu vaadi syytteen nostamista (RL 38:10.2). Ennen syytteen nostamista, syyttäjän on kuultava tietosuojavaltuutettua ja tuomioistuimen on varattava tällaista rikosta käsitellessään tietosuojavaltuutetulle tilaisuus tulla kuulluksi RL 38:10.3). Myös oikeushenkilö voi olla rangaistusvastuussa viestintäsalaisuuden loukkauksesta (RL 38:12).

> Viestintäsalaisuuden loukkaus ei koske viestin hävittämistä, kätkemistä tai salaamista. Kaikki sellaiset teot, joilla viestin perille meno estetään, arvostellaan tilanteesta riippuen joko tietoliikenteen häirintänä, varkausrikoksena, vahingontekorikoksena tai hallinnan loukkauksena.[19]

Rikoslain 38 luvun 3 §:n 1 momentin 1 kohdalla suojataan viestin sisältöä, silloin kun viesti on jo lähetetty tai tallennettu suojattuna ilman lähettämistä. Suojaa saavat siis perinteinen kirje, mutta myös sähköinen viesti. Välitettävänä oleva sähköinen viesti ja sähköisen viestin tunnistamistiedot saavat suojaa 2 kohdan mukaisesti. Käyn seuraavaksi läpi jokaiset neljä tekotapaa tarkemmin.

2.1 Kirjeen tai muun suljetun viestin avaaminen

[19] *HE 94/1993 vp,* s. 152.

Tekona tunnusmerkistö tarkoittaa kirjeen fyysistä avaamista. Kyseessä on siis ns. perinteinen kirjesalaisuus. Jos kirje on jo avattu, ei kirjeen sisällä oleva viesti enää nauti kirjesalaisuuden suojaa. Jos kirjeen vastaanottaja on avannut kirjeen ja jättää sen pöydälleen, ei toinen henkilö syyllisty viestintäsalaisuuden loukkaukseen, vaikka lukisi muutoin oikeudettomasti kyseisen kirjeen sisällön. Toisaalta teon tunnusmerkistö ei edellytä itse viestin lukemista, vaan säännöksen sanamuodon mukaan pelkkä kirjeen avaaminen riittää.

Osittaista epäselvyyttä on aiheuttanut ”muun suljetun viestin” käsite ja se, tuleeko sitä tulkita laajentavasti vai suppeasti sähköisen viestinnän kannalta[20]. Esitöiden mukaan muulla suljetulla viestillä tarkoitetaan muuta lähetystä kuin kirjettä, mikäli lähetys on suljettu ja sisältää vastaanottajalle tarkoitetun viestin. Esimerkkeinä mainitaan postipakettina lähetetty asiakirjavihko, mutta rajataan tavaralähetys kirjesalaisuuden suojan ulkopuolelle. Myös suljettu atk-tallenteita sisältävä paketti saa suojaa[21]. Tämän perusteella on vaikea nähdä määritelmän ”muu suljettu viesti” koskevan muuta kuin fyysisesti lähetettävää viestiä[22]. En käsittele muun suljetun viestin sisältöä tässä kirjoituksessa sen takia tarkemmin.

2.2 Tiedon hankkiminen suojaus murtaen sähköisesti tai muulla vastaavalla teknisellä keinolla tallennetusta ulkopuoliselta suojatusta viestistä

Sähköisesti tai muulla vastaavalla teknisellä keinolla tallennetulla viestillä tarkoitetaan lähinnä ns. elektronista postia eli tietokoneesta toisen tietokoneen muistiin välitettyjä viestejä, jotka ovat vain tietyn käyttäjän tai tiettyjen käyttäjien luettavaksi tarkoitettuja. Viesti tulee olla ulkopuoliselta suojattu, eikä saatettu yleisesti vastaanotettavaksi. Suojaa saa myös sellainen viesti, joka sitä mihinkään siirtämättä tallennetaan tietokoneen muistiin tietyn henkilön tai henkilöpiirin luettavaksi. Perinteiseen kirjesalaisuuteen verrattuna rangaistavuus edellyttää myös suojauksen murtamista, jolla on pyritään tuomaan esille kirjeen fyysistä avaamista vastaavaa tapaa sähköisen viestin kohdalla.[23]

2.2.1 Sähköinen viesti

[20] Ks. tarkemmin *Lehtonen 2005*, s. 156 ja 163
[21] *HE 94/1993 vp*, s. 148-149.
[22] Näin myös *Nyblin* 2004, s. 280-281.
[23] *HE 94/1993 vp,* s. 149.

Sähköisen viestinnän tietosuojalain 2 §:n 1 momentin 1 kohdan mukaan viestillä tarkoitetaan viestintäverkossa osapuolten välillä tai vapaasti valikoituville vastaanottajille välitettävää puhelua, sähköpostiviestiä, tekstiviestiä, puheviestiä ja muuta vastaavaa sanomaa. Viestintäsalaisuuden loukkauksella suojataan sähköisen viestinnän osapuolten välillä tapahtuvaa luottamuksellista viestintää. Kyseinen sähköisen viestin suoja koskee myös sosiaalisen median palveluita. Oli sitten kyseessä kirjoitettu viesti, kuvan lähettäminen tai vaikka webkamerayhteyden kautta toteutettu viestintä, jos kyseessä on ulkopuoliselta suojattu viesti.

2.2.2 Muu tallennettu viesti

On jäänyt melko vähälle huomiolle, että suojaa saa myös viesti, joka sitä mihinkään siirtämättä tallennetaan tietokoneen muistiin tietyn henkilön tai henkilöpiirin luettavaksi. Kyseeseen voi tulla esimerkiksi intranetin tiettyyn osioon lisätty viesti, johon vain osalla henkilöistä on annettu katseluoikeus. Kyse voi olla myös kansioon tallennetusta viestistä, joka on vain tietyn henkilöpiirin luettavana, mutta viestiä ei ole missään vaiheessa nimenomaisesti välitetty osapuolille. Jotta kyseessä olisi luottamuksellinen viesti, kansion avaaminen voi vaatia esimerkiksi erillisen käyttöoikeuden tai salasanan. Viestin kertaalleen lukeminen ei vaikuta viestin suojaan. Tässä mielessä sähköisen viestin suoja eroaa perinteisestä kirjesalaisuudesta, koska jo avatun kirjeen sisältö ei enää nauti viestintäsalaisuuden suojaa. Suojaa voi saada myös pilvipalveluun[24] tallennettu viesti, johon kirjoittaja on antanut lukumahdollisuuden sähköpostilinkillä pelkästään tietyille henkilöille.

Sähköpostipalvelulla voidaan viestiä myös ilman viestin lähettämistä. Rikollisten ja terroristien keskuudessa on levinnyt laajalle tapa luoda käyttäjätili sähköpostipalveluun ja viestiä luonnoskansion kautta. Toiminta tapahtuu siten, että osapuolet avaavat yksissä tuumin yhteisen käyttäjätilin sähköpostipalveluun, jolloin molemmilla on tiedossa käyttäjätunnus ja salasana. Kun toiselle osapuolelle halutaan viestiä, kirjoitetaan luonnos, joka tallentuu käyttäjätilille, mutta viesti ei tosiasiallisesti välity mihinkään. Tämän jälkeen toinen osapuoli voi käydä lukemassa luonnoksen sähköpostipalvelusta ja jatkaa viestintää samalla tavalla kuin ensimmäinen osapuoli. Myös tällaisissa tapauksissa pelkkä luonnos nauttii käsitykseni mukaan viestintäsalaisuuden suojaa, koska kyseessä on muu tallennettu viesti.

[24] Pilvipalveluita ovat esimerkiksi iCloud, Windowsin Skydrive ja Dropbox.

> Kyseisen luonnoksien avulla viestittelyn osaavat toki muutkin kuin rikolliset. Marraskuussa 2012 uutisoitiin tapauksesta, jossa CIA:n silloisella johtajalla David Petraneuksella oli avioliiton ulkopuolinen suhde naiseen, jonka kanssa hän viestitteli yhteisen gmail-tilin kautta luonnoksilla.[25]

2.2.3 Suojauksen murtaminen

Sähköisen viestin osalta on edellytyksenä, että tieto hankitaan ”suojaus murtaen”. Viestin tulee olla teknisin keinoin suojattu ulkopuolisilta ja tiedon hankkimisen viestistä tulee tapahtua tämä suojaus murtaen.[26] Sosiaalisen median palveluissa mahdollisuuksia päästä käsiksi luottamuksellisiin viesteihin on useita. Palvelu voi olla esimerkiksi valmiina avoimena näytöllä, aueta älypuhelimen sovelluksen kautta, tunnukset on voitu saada haltuun arvaamalla tai tietomurron kautta. Käyn läpi näitä eri tekomuotoja läpi tarkemmin sosiaalista mediaa käsiteltäessä.

Suojauksen murtamisella viitataan rikoslain 38 luvun 8 §:n 1 momenttiin, jossa säädetään tietomurrosta. Rikoslain 38 luvun 8 §:n 1 momentin mukaan tietomurrosta on tuomittava se, joka ”*käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja, taikka sellaisen järjestelmän erikseen suojattuun osaan”*. Viestintäsalaisuuden loukkauksen kohdalla voidaan siis puhua sähköisen viestin osalta kahdesta erilaisesta tavasta murtaa suojaus: a) käyttämällä itselleen kuulumatonta käyttäjätunnusta tai b) murtaa turvajärjestely muutoin. Oikeuskirjallisuudessa suojauksen murtaminen on rinnastettu a-kohdan mukaisesti oven avaamiseen avaimilla, joiden käyttämiseen avaajalla ei ole oikeutta ja b-kohdan mukaisessa tapauksessa oven lukituksen väkivaltaiseen avaamiseen[27].

Käyttäjätunnuksella tarkoitetaan yksilöllisesti määriteltyä merkkiketjua, joka tietojärjestelmään pyrkivän on osattava päästäkseen järjestelmän tietoihin käsiksi. Käyttäjällä tulee siis olla tiedossa käyttäjätunnus, jolla hän pääsee kirjautumaan sisään tietojärjestelmään. Käyttäjätunnuksen tiedonsaantitavalle ei ole esitetty mitään tiettyä rajoituksia, joten se voi tapahtua esimerkiksi urkkimalla tunnukset olan yli, mutta myös pelkkä arvaaminenkin riittää täyttämään rikoksen tunnusmerkistön. Turvajärjestely voidaan murtaa tunnusmerkistön mukaisesti

---

[25] [http://www.washingtonpost.com/blogs/worldviews/wp/2012/11/12/heres-the-e-mail-trick-petraeus-and-broadwell-used-to-communicate/] (27.5.2014).
[26] *HE 94/1993 vp*, s. 149.
[27] *Pihlajamäki 2004*. s. 128.

myös muutoin, eli esimerkiksi koodimurto-ohjelmaa käyttämällä[28]. Pelkkä turvajärjestelyn satunnainen epäkunto ei riitä tunnusmerkistön täyttymiseen, vaan turvajärjestely olisi läpäistävä jollakin rikoksentekijän nimenomaisella toimella. Sanaa ”murtaa” on käytetty korostamaan perinteisestä käytöstä poiketen sitä, että turvajärjestelyn läpäisyn on oltava luvatonta. Jos sisäänkirjautuu tietojärjestelmään vahingossa toisen käyttäjätunnuksilla, ei rikoksen tunnusmerkistö täyty. Jos käyttäjätunnukset on saatu varsinaisen käyttäjän suostumuksella lainaksi, ei kyse ole rangaistavasta teosta.[29]

2.2.4 Ulkopuoliselta suojattu viesti

Sähköisen viestin osalta viestintäsalaisuuden piiriin kuuluu vain ulkopuoliselta suojatut viestit, jotka ovat tietyn käyttäjän tai tiettyjen käyttäjien luettavaksi tarkoitettua.[30] Viesti ei ole luottamuksellinen, jos se on saatettu yleisesti vastaanotettavaksi. Joka tapauksessa viestin tunnistamistiedot ovat luottamuksellisia (SVTSL 4:2).

Keskeisintä viestin luottamuksellisuuden arvioinnissa on se, onko viestin lähettäjä saattanut viestin yleisesti vastaanotettavaksi. Julkinen viesti on kyseessä esimerkiksi keskustelupalstalle kirjoitettu viesti. Vastaanottajien lukumäärällä ei ole merkitystä tarkasteltaessa viestin luottamuksellisuutta, joten esimerkiksi useammalle henkilölle lähetetty sähköposti on luottamuksellinen.[31]

2.3 Televerkossa välitettävänä oleva viesti

Viestintäsalaisuuden loukkauksen säätämisen aikoihin puhuttiin tekniikan kehittymisestä ja tuolloin tiedonsiirto tapahtui pääosin kaapeliteitse, mutta myös radiolinkkien ja satelliittien avulla. Viesti kulki nykyistä pidempään ja se oli huomattavasti helpommin kaapattavissa. Esimerkiksi poliisin radiolähetyksiin pääsi käsiksi melko helposti, koska se tapahtui salaamattoman radioliikenteen avulla.

[28] Tällöin kyseessä on monesti jo viestintäsalaisuuden loukkauksen törkeä tekomuoto.
[29] *HE 94/1993 vp*, s. 151.
[30] *HE 94/1993 vp*, s. 149.
[31] *HE 125/2003 vp*, s. 51.

> Korkeimman oikeuden ratkaisussa KKO 1992:179 oli kyse tapauksesta, jossa syytetty oli kuunnellut luvallisella radiovastaanottimella poliisiradiota ja ohjelmoinut vastaanottimen toimimaan myös automaattisen radiopuhelinverkon taajuuksilla. Korkein oikeus katsoi, että kyse ei silloisesta viestintärikoksesta, koska tiedon vastaanottamista luvallisella radiovastaanottimella ei sinänsä ollut tarkoitettu rangaistavaksi.
>
> Ratkaisusta käy ilmi selkeästi se, että viestin tulee olla suojattu ulkopuoliselta, ja vaikka viestien sisältö poliisiradioliikenteessä on varmasti erityisen arkaluontoista, ei se itsessään riitä rikoksen tunnusmerkistön täyttymiseen. Nykyään poliisiradioliikenne on salattua, jota jo suositeltiinkin esitöiden aikana luottamuksellisen viestinnän osalta.[32] Vaikka viestinnän saisi kaapattua sen ollessa välitettävänä, ei sisällöstä saa selvää.

Alkuperäisten esitöiden mukaan televiestinnällä tarkoitetaan sähkömagneettisia aaltoja hyväksikäyttäen tapahtuvaa kohdeviestintää. Televerkolla taas tarkoitetaan siirtojohtojen sekä muiden telelaitteiden ja –rakenteiden muodostamaa kokonaisuutta, jossa voidaan sähkömagneettisten aaltojen avulla välittää puheluja ja muita viestejä. Esimerkkeinä televiesteistä mainitaan tavanomaiset puhelut, sähkeet, mutta myös teksti-, kuva- ja datasiirto. Säännös koskee kuitenkin muitakin vastaavia televiestinnän muotoja ja tällä on haluttu tuoda esille säännöksen välineneutraalisuutta. Tunnusmerkistö ei edellytä suojauksen murtamista, joten riittää, kun tieto vain hankitaan oikeudettomasti. Uudenlaisen viestinnän kohdalla, tulee tarkastella etenkin viestin yksityisyyttä, arvioitaessa sen soveltumista säännöksen piiriin. Käytännössä viestin teknisellä puolella ei ole kovin suurta merkitystä tunnusmerkistön täyttymisen suhteen, vaan oleellisempaa on viestinnän yksityisyys. Televerkossa välitettävää joukkoviestintää säännös ei koske.[33]

Säännöksen soveltamisen osalta ei ole väliä, onko kyseessä yleinen vai erityinen teletoiminta. Eli mikä tahansa kohdeviestintään käytetty televerkko kuuluu säännöksen piirin. Televerkko voi muodostua jo esimerkiksi organisaation sisäisestä puhelin- ja tietoliikenneverkosta. Teletoimintaa on sekä yleistä että erityistä. Yleistä teletoimintaa harjoittavat esimerkiksi posti ja erityistä teletoimintaa pankki- ja kirjastopalvelut. Jotta teko olisi rangaistava, tulee televiestin olla nimenomaisesti välitettävänä.[34]

2.4 Tieto viestin lähettämisestä tai vastaanottamisesta

Tieto viestin lähettämisestä tai vastaanottamisesta tarkoittaa esimerkiksi tietoa siitä, mihin numeroon tietystä puhelimesta on soitettu. Säännöksen tarkoituksena on suojata viestin-

[32] *HE 94/1993 vp*, s. 151.
[33] *HE 94/1993 vp*, s. 150-151.
[34] *HE 94/1993 vp*, s. 150-151.

täsalaisuutta nimenomaan siltä osin, kun se koskee tietoa viestinnän osapuolista.[35] Kyseinen kohta koskee tunnistamistietojen suojaa, vaikka kyseistä termiä ei esitöissä käytetäkään. Esitöiden aikaan sosiaalista mediaa ei ollut vielä olemassa ja internetkin oli melko harvojen käytössä. Teknisen kehityksen myötä tunnistamistietojen tärkeys on korostunut, jonka takia käsittelen sitä tässä kirjoituksessa melko laajasti.

2.4.1 Tunnistamistiedon määritelmä

Tunnistamistiedoilla tarkoitetaan sähköisen viestinnän tietosuojalain 2 §:n 1 momentin 8 kohdan mukaan tilaajaan tai käyttäjään yhdistettävissä olevaa tietoa, jota viestintäverkossa käsitellään viestien siirtämiseksi, jakelemiseksi tai tarjolla pitämiseksi. Tunnistamistietoihin voi kuulua tietoja, jotka viittaavat muun muassa viestinnän reititykseen, kestoon, ajankohtaan tai siirrettävän tiedon määrään, käytettyyn protokollaan[36], lähettäjän tai vastaanottajien päätelaitteen sijaintiin tietyn tukiaseman alueella, lähetettävään tai vastaanottavaan verkkoon ja yhteyden alkuun, loppuun tai kestoon. Tunnistamistieto voi olla myös muoto, jossa viesti välitetään verkossa. Olennaista on, että tietojen tulee olla yhdistettävissä käyttäjään.[37]

Liikenne- ja viestintävaliokunta totesi mietinnössään sähköisen viestinnän tietosuojalakiin liittyen, että tunnistamistiedon käsitettä ei ole rajattu pelkästään viestintäverkoissa käsiteltäviin tietoihin, vaan sillä tarkoitetaan myös viestintäverkoissa olevia tietoja, joita käsitellään tiettyihin tarkoituksiin, eli viestin siirtämiseen, jakeluun ja tarjolla pitämiseen. Rajaus on tehty ennemminkin käyttötarkoituksen kuin tunnistamistiedon tarkan käsitteen määrittelemisellä. Tunnistamistiedon liian tarkalla määrittelyllä voitaisiin mahdollistaa lain kiertäminen ja aiheuttaa se, että teknologian kehityksen myötä määritelmiä pitäisi uusia liian usein. Esimerkkinä mainitaan lausuntohetkellä tapahtunut spekulointi blue tooth –teknologialla toteutetun suoramarkkinoinnin soveltumisesta sähköisen viestinnän tietosuojalain soveltamisalaan.[38]

> Kirjoittamishetkellä on vireillä lakiuudistus, jossa on tarkoitus koota yhteen keskeiset sähköistä viestintää koskevat säädökset tietoyhteiskuntakaareksi. Esimerkiksi sähköisen viestinnän tie-

[35] *HE 94/1993 vp*, s. 151.
[36] Protokolla on yhtä kuin yhteyskäytäntö. Internetissä tiedonsiirrosta huolehtii yleensä TCP-protokolla (Transmission Control Protocol). TCP/IP (Transmission Control Protocol/Internet Protocol taas on usean tietoverkkoprotokollan yhdistelmä. Muista protokollista voidaan mainita esimerkkinä VoIP (Voice over Internet Protocol), jolla voidaan siirtää ääntä reaaliaikaisesti internetissä tai muun verkon välityksellä.
[37] *HE 125/2003 vp*, s. 46.
[38] *LiVM 13/2004 vp*, s. 4-5.

> tosuojalaki tulee sisältymään tietoyhteiskuntakaareen.[39] Tietoyhteiskuntakaareen liittyen annetussa hallituksen esityksessä on määritelty käsite *välitystieto*[40], joka esityksen mukaan tarkoittaa oikeus- tai luonnolliseen henkilöön yhdistettävissä olevaa tietoa, jota viestinnän välittäjä käsittelee viestien välittämiseksi. Määritelmä vastaa sähköisen viestinnän tietosuojalain 2 §:n 1 momentin 8 kohdan määritelmää tunnistamistiedosta. Tunnistamistieto terminä sekoitetaan yleiskielessä usein erilaisiin tunnistautumiseen liittyviin palveluihin, eikä tunnistamistiedon määritelmästä ole myöskään ilmennyt riittävän selvästi se, että tilaajan tai käyttäjään yhdistettävissä oleva tieto on tullut kerätä viestinnän välittämisen yhteydessä, jotta sitä voidaan pitää tunnistamistietona. Tämän takia viestinnän osapuolena käsiteltävät tiedot eivät kuulu määritelmän piiriin, koska niitä ei kerätä viestin välittämisen yhteydessä eikä niitä siten käsitellä viestin välittämiseksi. Jos kyseessä on viestinnän osapuolena kerätty viestinnän toista osapuolta koskeva tieto, on kyse yleensä henkilötiedosta.[41]

Tunnistamistiedot erottaa henkilötiedoista tietojen liittyminen sähköiseen viestintään tai viestintäverkkojen käyttämiseen. Jos tieto on yhdistettävissä luonnolliseen henkilöön, mutta se ei liity sähköiseen viestintään tai viestintäverkkojen käyttämiseen, kysymyksessä on henkilötieto.[42] Paikkatiedon ja tunnistamistiedon ero ratkeaa tiedon käyttötarkoituksen perusteella. Jos sijainnin ilmaisevaa tietoa käytetään viestintäpalvelun toteuttamisessa, kysymyksessä on tunnistamistieto. Esimerkiksi matkaviestiverkossa tieto siitä, minkä tukiaseman alueella päällä oleva matkapuhelin on kulloisellakin hetkellä, on tunnistamistieto, koska liittymän tai päätelaitteen sijainnin ilmaiseva tieto on välttämätön viestintäpalvelun toteuttamiseksi.[43]

2.4.2 Tunnistamistiedon hankkimisajankohta

Tunnistamistietojen osalta on ollut epäselvyyttä siitä, koskeeko kriminalisointi vain välitettävänä olevaa vai jo lähetettyä viestiä. Eduskunnan apulaisoikeusasiamies otti vuonna 1998 kantaa (28.8.1998, D 2049/4/96) oppilaitoksen tietokonejärjestelmien ja tietoliikenneverkon käyttösääntöihin, eli käytännössä oppilaitoksen mahdollisuuteen käsitellä oppilaiden luottamuksellisia viestejä. Referoidessaan viestintäsalaisuuden loukkauksen tunnusmerkistöä, totesi apulaisoikeusasiamies seuraavasti: ”*Momentin 3 kohdan*[44] *mukaisena rikoksen tekomuotona on tiedon hankkiminen televiestin sisällöstä ja tällaisen viestin lähettämisestä tai vastaanottamisesta silloin, kun tieto on televerkossa välitettävänä.*”.

Nyblin ja Lehtonen ovat kritisoineet kohtaa, koska lain esitöiden ilmaisut viittaavat ennemminkin jo tapahtuneen viestinnän jälkeen tallennettuihin tunnistamistietoihin. Lehtosen mukaan ilmaisu ”hankkii tiedon viestin vastaanottamisesta” ei olisi luonteva, jos tunnusmerkistö

[39] [http://www.lvm.fi/web/hanke/tietoyhteiskuntakaari] (27.5.2014).
[40] Tämän lisäksi käsite paikkatieto tulee muuttumaan käsitteeksi sijaintitieto.
[41] *HE 221/2013 vp,* s. 95.
[42] *HE 125/2003 vp*, s. 9.
[43] *HE 125/2003 vp*, s. 47.
[44] Ratkaisuhetkellä kyseinen tunnusmerkistö löytyi 3 momentista, mutta siirrettiin myöhemmin 2 momenttiin.

koskisi vain välitettävänä olevaa viestiä.[45] He siis katsovat, että välitettävänä oleminen ei koske tunnistamistietoja. Toisaalta juuri tämä tulkinta saa aikaan sen, että tunnistamistietojen suoja onkin itse viestin sisältöä suurempi, jota on pidetty lähtökohtaisesti perusoikeussuojan ydinalueella tunnistamistietojen jäädessä sen reuna-alueelle. Käsittelen vielä tätä asiaa myöhemmin tarkemmin.

Vaikka apulaisoikeusasiamiehen tarkoituksena ei ollut käsitellä syvällisemmin juuri kyseistä asiaa ja Nyblinin ja Lehtosen tulkinta luo ongelman viestin sisällön ja tunnistamistietojen suojan välille, olen samaa mieltä Nyblinin ja Lehtosen kanssa. Kohdan voidaan siis katsoa suojaavan viestin tunnistamistietoja riippumatta siitä onko viesti välitettävänä vai ei.

2.4.3 Tunnistamistietojen yleinen perusoikeussuoja

Perustuslain 10 §:n 2 momentin mukaan luottamuksellisen viestinnän suoja koskee ensisijaisesti viestin sisällön suojaa, mutta myös tunnistamistiedot on luettu suojan piiriin, koska niiden avulla voi selvitä viestinnän osapuolet. Perustuslakivaliokunta on maininnut useissa lausunnoissaan, että tunnistamistiedot jäävät viestin perusoikeussuojan ydinalueen ulkopuolelle[46]. Tilanne on muuttunut viime aikoina siihen suuntaan, että myös tunnistamistiedot koetaan erityisen tärkeäksi perusoikeussuojan kannalta.

Perinteiseen postitoimintaan verrattuna tunnistamistiedot ovat rinnastettavissa kirjeen tai postipaketin osoite ja postileimatietoihin sekä kirjeen ja paketin kokoon ja muotoon[47]. Kirjesalaisuuteen liittyen tunnistamistiedoilla ei ole ollut missään vaiheessa erillistä suojaa. Sähköisessä maailmassa tämä suoja kuitenkin on ja viestiin tai henkilöön liittyen voidaan kerätä useita erilaisia tietoja. Melkein kaikesta jää sähköinen jälki ja tunnistamistieto voi kulkea helposti taltioitavaksi toiselle puolelle maailmaa. Tunnistamistiedot ovat myös entistä helpommin muiden kansalaisten saatavilla, esimerkiksi auki jääneen tietokoneen käyttäjätilin takia, kun aikaisemmin tähän saattoi tarvita pääsyn teleyrityksen tiloihin.

Aikaisemmin tunnistamistietojen käsittelyyn liittyvät ongelmat liittyivät lähinnä teleyrityksiin ja siihen, millä edellytyksillä teleyritykset saivat käsitellä tunnistamistietoja laskutuksen tai

[45] *Lehtonen* 2005, s. 160-161 ja *Nyblin 2004*, s. 279.
[46] Ks. esimerkiksi *PeVL 33/2013 vp*, jossa viittaukset myös vanhempiin lausuntoihin.
[47] *HE 48/2008 vp*, s. 4.

palvelun toimivuuden turvaamiseksi. Nykyään tärkeämpää on tunnistamistietojen käyttö mainonnassa, viranomaiskäytössä tai lisäarvopalveluiden tarjonnassa. Tunnistamistiedot ovat yhä suuremmassa roolissa viestinnän luottamuksellisuuteen liittyen, mutta mahdollistavat myös erittäin konkreettisen tiedon saamisen yksittäisen henkilön viestintätavoista ja viestinnän piiristä.[48]

Teleyrityksille ja lisäarvopalvelun tarjoajille sekä yhteisötilaajille on annettu sähköisen viestinnän tietosuojalaissa 3 luvussa tunnistamistietojen käsittelyoikeus esimerkiksi palvelujen toteuttamiseksi ja käyttämiseksi, laskutusta ja markkinointia sekä teknistä kehittämistä varten. Viranomaistarpeita varten tunnistamistietoja tulee säilyttää 12 kuukauden ajan[49] viestinnän päivämäärästä. Kyseisiä tietoja saa käyttää ainoastaan pakkokeinolain (806/2011) 10 luvun 6 §:n 2 momentissa tarkoitettujen rikosten tutkimiseksi, selvittämiseksi ja syyteharkintaan saattamiseksi (SVTSL 14 a).

Kyseinen tulkinta perustuu Euroopan parlamentin ja neuvoston direktiiviin 2006/24/EY, joka todettiin vastikään laittomaksi Unionin tuomioistuimen tuomiossa 8.4.2014, jossa yhdistettiin asiat C-293/12 ja C-594/12. Tuomioistuin totesi, että direktiivissä ei oltu otettu huomioon riittävällä tavalla EU:n perusoikeuskirjan 7 ja 8 artiklan kohdissa, joissa säädellään perusoikeuksiin puuttumisen mahdollisuuksista. Tuomioistuin katsoi, että ”*direktiivi sisältää laajaperäisen ja erityisen vakavan puuttumisen näihin perusoikeuksiin unionin oikeusjärjestyksessä ilman, että tällaista puuttumista olisi tarkasti rajoitettu säännöksillä, joilla voidaan taata, että se todella rajoitetaan täysin välttämättömään.*”. Tuomioistuin kritisoi myös sitä, että direktiivissä ei edellytetä, että kyseisiä tietoja säilytetään unionin alueella. Loppupäätelmä olikin, että tuomioistuin totesi direktiivin pätemättömäksi, koska suhteellisuusperiaatetta ei oltu noudatettu.

Päätöksen jälkeen perustuslakivaliokunta on ehtinyt ottaa kantaa asiaan lausunnossaan tietoyhteiskuntakaareen 19 lukuun liittyen ja todennut: ”*käytännössä sähköisen viestinnän käyttöön liittyvät tunnistamistiedot sekä mahdollisuus niiden kokoamiseen ja yhdistämiseen voivat kuitenkin olla yksityiselämän suojan näkökulmasta siinä määrin ongelmallisia, että kategorinen erottelu suoja reuna- ja ydinalueeseen ei aina ole perusteltua, vaan huomiota on yleisemmin kiinnitettävä myös rajoitusten merkittävyyteen.*”. Perustuslakivaliokunta ei kuitenkaan

[48] *Innanen – Saarimäki 2012*, s. 29.
[49] Direktiivissä 2006/24/EY säädetty vähimmäisaika on kuusi kuukautta ja enimmäiskesto 24 kuukautta.

katsonut, että tuomiosta johtuisi suoranaista estettä sellaiselle sääntelylle, jossa oikeasuhtaisuuden vaatimukset toteutetaan muilla tavoin, jota puoltaa esimerkiksi vakavan rikollisuuden torjuntaan liittyvä hyväksyttävä peruste.[50]

On täysin eri asia tallettaa tunnistamistietoja esimerkiksi markkinointitarkoituksia varten, kuin velvoittaa säilyttämään ne vakavan rikollisuuden torjumisen takia. Vaikka tunnistamistietojen säilyttämisen kieltämisellä yhtäältä lisättäisiin kansalaisen yksityisyydensuojaa, heikentäisi se samalla kansalaisen muita perusoikeuksia. Nykyään kansalaiset joutuvat melko usein rikoksen uhriksi myös sosiaalisessa mediassa, jolloin rikosten selvittäminen on huomattavasti vaikeampaa, jos tunnistamistietoja ei säilytettäisi. Esimerkiksi sosiaalisessa mediassa tapahtuneen seksuaalirikoksen saa yleensä selvitettyä epäillyn tunnistamistietojen perusteella. Yksittäistapauksessa voidaan arvioida, että uhrin perusoikeus koskemattomuuteen ja turvallisuuteen lähtökohtaisesti selkeästi tärkeämpää, kuin epäillyn oikeus luottamukselliseen viestintään. Tunnistamistietojen yleisluontoista keräämistä ei kuitenkaan voi arvioida pelkästään yksittäisen tapauksen tai rikoslajin perusteella, koska tunnistamistietoja kerätään kaikilta. Tuleekin löytää riittävä tasapaino, jossa henkilön oikeus yksityisyyteen on tasapainossa yksityisyyteen puuttumisen kanssa.

2.4.4 Tunnistamistietojen suoja verrattuna viestin sisältöön

Edellä esitetystä tunnistamistietojen perusoikeussuojan merkityksen lisääntymisestä huolimatta, on viestin ja tunnistamistietojen suojan välinen suhde ollut viestintäsalaisuuden loukkauksen kohdalla kyseenalainen. Lehtonen on kiinnittänyt tähän huomiota jo vuonna 2001, jolloin hän toi esille problematiikan tunnistamistietojen ja viestin sisällön suojan suhteen[51]. Tunnistamistietojen suoja kun näyttää säännöksessä olevan vahvempi kuin yleisesti perusoikeussuojan kannalta tärkeämpänä pidetyn viestin sisällön.

Sähköisen viestin sisällön kohdalla tieto tulee hankkia suojaus murtaen. Tekijän tulee siis nimenomaisella toimella murtautua sähköiselle alustalle, johon viesti on tallennettu. Tunnistamistietojen osalta tätä vaatimusta ei ole, joten jo pelkkä tiedon hankkiminen oikeudettomasti riittää. Toisaalta viestin sisältö saa suojaa ilman suojauksen murtamisen vaatimusta myös sil-

[50] *PeVL 18/2014 vp*, s. 6.
[51] Ks. tarkemmin *Lehtonen 2001*, s. 162-164.

loin, kun viesti on vielä välitettävänä. Tämän osalta nykytekniikka ei kuitenkaan juuri mahdollista puuttumista viestin välitettävänä olemiseen, kuin erilaisia haittaohjelmia tai teknisiä apuvälineitä käyttäen.

Säännöksen nykyrakenne onkin siten ongelmallinen, vaikka tunnistamistietojen korostettu perusoikeussuojan tarve otettaisiinkin huomioon. Jostain syystä lainsäätäjä ei ole ryhtynyt toimiin asian korjaamiseksi, eikä asiaa ole sivuttu tuoreimmissa tunnistamistietoja käsittelevissä esitöissä.

2.4.5 Tunnistamistietojen suojelutarve toisiinsa nähden

Koska viestin tunnistamistietoja ei ole määritelty tyhjentävästi, voi herätä kysymys ovatko kaikki tunnistamistiedot viestintäsalaisuuden loukkauksen sääntelyn piirissä ja mikä niiden todellinen suojelutarve perusoikeussuojan kannalta on. Esimerkiksi siirrettävän viestin koko tai protokolla ei juurikaan kerro viestinnän osapuolista mitään.

Viestintäsalaisuuden suojaa säänneltäessä oli tarkoitus ottaa kantaa, kuinka laajasti telesalaisuus koskee tietoa viestinnän osapuolista ja samalla viitattiin Eduskunnan oikeusasiamiehen päätökseen, jonka mukaan suojatun puhelinsalaisuuden piiriin kuuluu myös se, mitkä ovat puhelun tilaajan ja vastaanottajan puhelinnumerot ja heidän henkilöllisyytensä sekä puhelun tapahtuma-aika ja kesto.[52]

Esitöissä tunnistamistietojen suojaa käsitellään vain muutamalla lauseella. Lausetta ”*Säännöksen tarkoituksena on nimenomaan turvata viestintäsalaisuutta siltä osin kuin se koskee tietoa viestinnän osapuolista”* voi tulkita joko laajentavasti tai suppeasti. Suppeassa tulkinnassa säännöksellä suojattuja tunnistamistietoja ovat vain ne tiedot, jotka ovat selkeästi yhdistettävissä käyttäjään. Näitä tunnistamistietoja ovat esimerkiksi viestinnän osapuolen nimi, nimimerkki, puhelinnumero ja IP-osoite. Laajentavassa tulkinnassa säännös suojaa kaikkia viestin välittämiseen liittyviä tunnistamistietoja, riippumatta siitä, millainen mahdollisuus sen perusteella on tunnistaa viestinnän osapuoli. Tällaisia olisivat etenkin viestin sisältämän tiedon määrä ja protokolla. Näiden osalta ei yksittäisenä tietoja juuri ole mahdollisuutta yhdistää tunnistamistietoa viestinnän osapuoleen.

[52] *HE 94/1993 vp*, s. 138-139.

Käytännössä on hyvin epätodennäköistä, että viestiin ja sen sisältöön liittyen saataisiin tietoon vain yksittäinen tunnistamistieto. Niin kuin edellä tunnistamistietojen määritelmää käsiteltäessä on todettu, ei tunnistamistietojen määritelmää ole haluttu etenkään teknisen kehityksen takia rajoittaa liian tarkasti. Tämän takia kaikki tunnistamistiedot ovatkin samalla linjalla harkittaessa rikoksen tunnusmerkistön täyttymistä viestintäsalaisuuden loukkauksen kohdalla.

2.5 Rangaistava yritys

Rangaistavuuden ulottaminen yritysvaiheeseen on perusteltua, koska yrityksen ja täytetyn teon ero eräissä tapauksissa on ajallisesti pieni ja toisaalta jo yrityskin edellyttää eräiden tekotapojen kohdalla runsaasti valmistelua ja siten selvästi havaittavaa rikoksentekotahtoa. Esimerkkinä esitöissä mainitaan postilähetyksen avaaminen, vaikka teko keskeytyisikin ennen kuin lähetys on saatu kokonaan auki.[53]

Apua säännöksen yrityksen tunnusmerkistön täyttymiseen sähköisen viestinnän osalta voidaan hakea tietomurron yritykseen liittyvistä esitöistä. Rangaistavaa on jo esimerkiksi yrittää selvittää tietojärjestelmää suojaava käyttäjätunnus tai murtaa muu turvajärjestely, jos tarkoituksena on oikeudettomasti tunkeutua tietojärjestelmään.[54] Tämän perusteella viestintäsalaisuuden loukkauksen yritys voisi täyttyä siis jo siinä vaiheessa, kun tekijä on saanut selvitettyä käyttäjätunnuksen ja salasanan palveluun, jos hänen tarkoituksenaan on kirjautua sisään kyseiseen palveluun ja päästä käsiksi luottamuksellisiin viesteihin. Samalla lailla yritys voisi täyttyä siinä vaiheessa, kun tekijä pyrkii kirjautumaan käyttäjätilille arvailemalla salasanoja. Edelleen esimerkkinä voidaan mainita yritys kurkkia olan yli toisen henkilön käyttäjätunnus ja salasana.

3 Sosiaalisen median erityispiirteitä

Sosiaalisessa mediassa viestejä voidaan lähettää usealla eri tavalla. Sähköisen viestinnän tietosuojalain 1 luvun 2 §:n 1 momentin 1 kohdan mukaan viestillä tarkoitetaan viestintäverkossa osapuolten välillä tai vapaasti valikoituville vastaanottajille välitettävää puhelua, sähköpostiviestiä, tekstiviestiä, puheviestiä ja muuta vastaavaa sanomaa. Käytännössä tämä tarkoittaa

[53] *HE 94/1993 vp*, s. 152.
[54] *HE 94/1993 vp*, s. 156.

sitä, että määritelmä voi soveltua useisiin erilaisiin sosiaalisen viestinnän muotoihin. Kyseeseen voi siis tulla esimerkiksi kirjoitettu viesti, ääni, kuva, striimaus ja webkamerayhteys. Viestintäsalaisuuden loukkauksen osalta olennaista on viestin luottamuksellisuus sosiaalisessa mediassa, koska vain luottamuksellinen viesti saa suojaa.

3.1 Ulkopuoliselta suojattu luottamuksellinen viesti

Luottamuksellisten viestien lähettäminen on mahdollista useissa eri sosiaalisen median yhteisöpalveluissa, kuten Facebook tai pikaviestipalvelu Whatsapp. Webkamerayhteys taas voidaan toteuttaa esimerkiksi Skypen kautta. Suojaa saa myös pelkkä kahden henkilön välinen kuvayhteys, joten jo pelkkä toistensa tuijottaminen webkamerayhteyden kautta on suojattu. Sama koskee pelkän digitaalisen valokuvan lähettämistä ilman varsinaista kirjoitettua viestiä.

> Tällä hetkellä voimassa olevan sähköisen viestinnän tietosuojalain sääntely kohdistuu teleyrityksiin, yhteisötilaajiin ja lisäarvopalvelun tarjoajiin. On esiintynyt epäselvyyttä siitä, koskeeko sääntely myös sosiaalisen median palveluntarjoajia ja suuria internet-yhtiöitä kuten Apple, Google ja Facebook, vai onko heillä vapaammat oikeudet käsitellä palvelussaan välitettäviä ja käsiteltäviä viestejä sekä tunnistamistietoja. Tilannetta pyritään selventämään tietoyhteiskuntakaaren säätämisen yhteydessä, koska sen myötä myös erilaiset yhteisöpalvelut ja muut sosiaalisen median palvelut, joissa palvelun sisällä välitetään luottamuksellista viestintää, tulisivat selkeästi sääntelyn piiriin.[55] Tärkeää tämä on etenkin sen takia, että erilaiset sosiaalisen median palvelut ovat jo ohittaneet perinteisen viestinnän keinot.

Sosiaalisessa mediassa viestintä tapahtuu yleensä tietyn käyttäjätilin profiilin kautta. Viestintä voi tapahtua siten, että se näkyy kaikille palveluun kirjautuneille, jolloin kyse on yleensä joukkoviestinnästä, joka ei nauti luottamuksellisen viestin suojaa. Näkyvyyttä voidaan rajoittaa asetuksilla tietylle joukolle tai yksittäiselle henkilölle, jolloin viesti on monesti luottamuksellisen viestinnän piirissä. Sosiaalisen median viestintätapoja voidaan luokitella mm. seuraavanlaisesti:

1) Viesti näkyy kaikille
2) Viesti näkyy vain sisäänkirjautuneille
3) Viesti näkyy viestin kirjoittajan rajaamalle joukolle
4) Viesti näkyy viestin kirjoittajan kavereille, mutta myös heidän kavereille
5) Viesti näkyy vain tietylle yksittäiselle henkilölle

[55] *HE 221/2013 vp*, s. 62.

Julkisia viestejä voidaan 1 kohdan mukaisesti julkaista esimerkiksi keskustelupalstoilla, kuvalaudoilla, blogeissa, videoblogeissa ja verkkojulkaisujen yhteydessä olevissa kommentointiosiossa. Kommentointi voi olla mahdollista anonyymisti ilman sisäänkirjautumista, mutta osassa palveluista viestintä voi vaatia sisäänkirjautumisen. Viesti näkyy aina kaikille sivustolla vieraileville. Verkkojulkaisujen osalta viestintä voi tapahtua lisäosalla, jossa on mahdollista kommentoida omalla Facebook-profiililla tai verkkojulkaisun omalla keskustelupalstalla. Julkisia ovat myös Twitterissä lähetetyt twiitit, jotka näkyvät kaikille käyttäjille ilman sisäänkirjautumista palveluun. Ykköskohdan mukaiset viestit eivät nauti luottamuksellisen viestin suojaa, eivätkä siten kuuluu viestintäsalaisuuden loukkauksen suojan piiriin.

Jos viestien näkeminen vaatii sisäänkirjautumisen, ei se itsessään tee viestistä luottamuksellista. Esimerkkinä voidaan mainita tapaus, jossa henkilö kirjoittaa Facebookin käyttäjätilin seinälle päivityksen[56], jonka näkyvyyttä ei ole rajoitettu millään tavalla. Päivitys ei näy ilman sisäänkirjautumista, mutta jokaisella jolla on profiili Facebookissa, on mahdollisuus nähdä kyseinen viesti. Koska Facebookiin voi luoda käyttäjätilin vapaasti, on kyse ennalta rajoittamasta joukosta ihmisiä ja viesti on tulkittava julkiseksi.

Kolmoskohdan mukaisissa tapauksissa on useita erilaisia mahdollisuuksia viestiä tietylle kohderyhmälle sosiaalisessa mediassa. Kyse voi olla esimerkiksi Facebook-profiilin seinälle tehdystä päivityksestä, jonka näkyvyys on rajoitettu kaikille kaverilistalla oleville. Käyttäjä on voinut myös muodostaa kaverilistalla olijoista erillisen ryhmän, joille päivitys on tarkoitettu nähtäväksi. Facebookissa on mahdollisuus luoda ryhmiä, joihin pääsyä pystyy rajoittamaan ja sitä kautta myös viestin näkevää joukkoa. Edelleen esimerkkinä voidaan mainita ryhmäsähköpostin lähettäminen suurellekin joukolle[57] henkilöitä tai viestin lähettäminen Whatsapp-sovelluksella luodun ryhmän kesken. Myös suljettu Twitter- tai Instagram-käyttäjätili kuuluu tähän ryhmään.

Pesonen on todennut, että sosiaalisen median palvelusivuilla esitetty kommentti, kirjoitus seinällä tai profiilin tilapäivitys, ovat verkkoviestejä, mutta eivät luottamuksellisia viestejä. Pesosen mukaan ne ovat tarkoitettu avoimen vastaanottajajoukon tai ainakin usean henkilön tietoon samalla tavalla kuin tietoverkon keskustelupalstalle tai mielipidesivustolle lähetetyt

[56] Jos kyseessä on päivitys Facebookin fanisivulle, näkyy päivitys myös ilman sisäänkirjautumista ja kyseessä on 1-kohdan mukainen viesti.
[57] Vaikka luottamuksellisen viestin suojaa ei määrittele viestin vastaanottajien määrä, voidaan massapostitusten kohdalla arvioida erikseen viestin luottamuksellisuutta mainoskirjeiden tapaan.

viestit.[58] Olen Pesosen kanssa eri mieltä, koska viestit eivät ole aina tarkoitettu avoimen vastaanottajajoukon vastaanotettavaksi, eikä luottamuksellisen viestin vaatimus sisällä rajoituksia vastaanottajien lukumäärästä[59]. Lahtinen on arvioinut, että esimerkiksi kymmenille vastaanottajille lähetetty samansisältöinen sähköposti on luottamuksellinen. Esimerkkeinä hän mainitsee opiskelijaryhmälle tai työntekijöiden ammattiosastolle lähetetyn viestin[60]. Jos esimerkiksi Facebook-profiilin käyttäjällä on sata kaveria ja hän kirjoittaa seinälleen pelkästään heidän näkyville tarkoitetun päivityksen, on kyseessä luottamuksellinen viesti, koska viesti on kohdistettu nimenomaisesti kyseiselle rajatulle joukolle henkilöitä. Viestiä eivät pysty lukemaan muut kuin kaverilistalla olijat, eikä heidän lukumäärällä siis ole merkitystä. Viestiä ei myöskään pysty jakamaan suoraan palvelun jaa-toiminnolla eteenpäin yksityisyysasetusten takia, koska viesti on rajattu vain kaverilistalla olijoille. Sama koskee myös profiilin päivitykseen tulleita kommentteja, joiden osalta näkyvyys on rajattu vain päivityksen tehneen kaverilistalla olijoille. Näissä tapauksissa päivitykseen kommentoineen kaverilistalla olijat eivät siis näe kommenttia.

Vaikka viesti olisi mahdollista jakaa sosiaalisen median palvelussa suoraan eteenpäin, esimerkiksi aikaisemmin mainitulla Facebookin jaa-toiminnolla[61] omassa profiilissa tai tietyssä ryhmässä, ei sillä ole sinänsä merkitystä viestin luottamuksellisuuteen. Analogiaa voidaan hakea sähköpostin toiminnoista. Sähköpostiohjelmista löytyy yleensä erillinen valintamahdollisuus jatkolähettää saapunut sähköpostiviesti eteenpäin. Kyseinen toiminto ei kuitenkaan vaikuta saapuneen viestin luottamuksellisuuteen millään tavalla. Viestin kun pystyy kopioimaan manuaalisestikin leikkaa-liimaa -toiminnolla helposti ja lähettää eteenpäin.

> Viestin jatkolähettämismahdollisuuden osalta tulee muistaa, että henkilöllä joka toimii viestin vastaanottajana, on mahdollisuus sähköisen viestinnän tietosuojalain 3 luvun 8 §:n 2 momentin mukaan oikeus käsitellä luottamuksellisia viestejä haluamallaan tavalla. Jos henkilö esimerkiksi päivittää omalle Facebook-seinälleen vain kavereille näkyvän viestin, on kaverilistalla olevalla oikeus jakaa viestiä eteenpäin, koska hän on toiminut viestin laillisena vastaanottajana.
>
> Rajoituksen tähän voi tehdä se, että kyseessä on arkaluontoinen tieto, jolloin tietoa julkisesti tai lukuisten ihmisten saataville levitettäessä, voisi tulla kyseeseen yksityiselämää loukkaava tiedon levittäminen (RL 24:8). Rikoksen tunnusmerkistö ei tosin välttämättä täyty, jos alkuperäisen päivityksen tekijä on julkaissut tiedon julkisesti tai suurelle määrälle kaverilistalla olijoita. Viestin jatkolähettäminen voi täyttää myös kunnianloukkauksen (RL 24:9) tunnusmerkistön. Vaikka esimerkiksi pelkästä kuvan jakamisesta on tuomittu varsinaisen viestin kirjoittajan tapaan, on näissä tapauksissa tahallisuuden arviointi tärkeämmässä roolissa.

[58] *Pesonen 2013*, s. 103.
[59] *HE 125/2003 vp*, s. 51.
[60] *Lehtonen* 2001, s. 130.
[61] Teknisesti Facebookin jaa-toiminnon käyttäminen vastaa linkkaamista. Jos esimerkiksi jaettu valokuva poistetaan, poistuu kuva myös kuvan jakaneiden seinältä.

> Omaa osaansa sosiaalisessa mediassa näyttelevät myös identiteettivarkaudet. Jos viesti on lähetetty selkeästi toista henkilöä esittävälle valeprofiilille, ei viestin vastaanottajalla ole lähtökohtaisesti oikeutta välittää viestiä eteenpäin, koska viestiä ei oltu tarkoitettu hänelle (SVTL 8.2). Jos valeprofiilin haltija levittää viestiä eteenpäin, voi hän syyllistyä salassapitorikokseen (RL 38:1) tai salassapitorikkomukseen (RL 38:2).

Viestin julkisuuden kannalta suljetut ryhmät voidaan lukea joko kolmannen tai neljännen kohdan mukaisiksi. Ryhmään voi esimerkiksi päästä vain ylläpitäjän hyväksynnällä tai tietyllä salasanalla. Tällainen voi olla rekisteröitymisen ja tietyn salasanan takana oleva keskustelupalsta, tai esimerkiksi Facebookiin luotu suljettu ryhmä. Facebookin kohdalla ryhmä voi olla myös salainen, jolloin edes itse ryhmä ei näy ulkopuolisille. Voidaan ajatella tilannetta, jossa suljetussa Facebook-ryhmässä on 200 jäsentä ja yksi ryhmän jäsenistä kirjoittaa ryhmän seinälle viestin, joka näkyy vain ryhmän jäsenille. Koska ryhmään voidaan liittää kaikkien ylläpitäjien toimesta lisää henkilöitä, on kyseessä ennemminkin julkiseksi tulkittava viesti, kuin luottamuksellinen viesti. Joskin raja on hyvin häilyvä, koska viesti on mitä luultavimmin tarkoitettu vain ryhmän jäsenille. Ryhmän jäsenten määrä, ja siten viestin näkyvyys, on kuitenkin monesti useamman henkilön säädettävissä, jolloin viesti on tulkittava lähetetyksi ennemminkin ennalta määrittelemättömälle joukolle. Jos viestin kirjoittaa ryhmän ainoa ylläpitäjä, jolla on ainoana mahdollisuus hallita ryhmän jäsenten lukumäärää, tulisi kyseistä päivitystä taas pitää lähtökohtaisesti luottamuksellisena viestinä.

Luottamuksellisen viestin tulkinta muuttuu kaverilistaan verrattuna, jos kyseessä on päivitys, joka on rajattu näkyvyydeltään kavereiden lisäksi heidän kavereille. Tällöin vastaanottajat on toki rajattu viestin lähettämishetkellä tietylle rajatulle henkilöpiirille, eli kaverilistalla ja heidän kaverilistalla olijoille. Jos yksikin kaverilistalla olijoista hyväksyy uuden kaverin listalleen, näkyy viesti tämän jälkeen myös hänelle. Tämän takia kyseessä on julkinen viesti, jossa vastaanottajien joukko on ennalta määrittelemätön.

Yksittäiselle henkilölle lähetetyt viestit ovat selkeästi luottamuksellisen viestin puolella, kunhan viesti on vain suojattu ulkopuolisilta. Tällaisista voidaan mainita esimerkkeinä sosiaalisessa mediassa yksityisviestit, joita voi lähettää miltei jokaisessa sosiaalisen median palvelussa toisille käyttäjille. Esimerkiksi Twitterissä on mahdollisuus lähettää ns. direct message muille käyttäjille. Tällöin vain viestin osapuolilla on mahdollisuus nähdä viesti ja kyse on selkeästi luottamuksellisesta viestistä. Sama ominaisuus löytyy myös Whatsappista tai muista pikaviestiohjelmista.

Facebookista löytyy myös yksityisviestitoiminto, mutta tilanne muuttuu hieman monimutkaisemmaksi, jos yksityisviestiin liittää vähintään kaksi osapuolta. Kyse on sinänsä luottamuksellisesta viestistä kyseisille kahdelle henkilölle, mutta Facebookin ominaisuuksien takia kaikki kolme viestinnän osapuolta voivat liittää mukaan keskusteluun jonkun kaveripiiristään[62]. Jälkeenpäin liitetyt profiilit saavat tietoonsa myös kaikki ennen heidän liittymistä viestiketjussa kirjoitetut viestit, vaikka keskustelu onkin käyty vain noiden alkuperäisen kolmen profiilin kesken. Kahden profiilin välisessä yksityisviestinnässä tätä liittämismahdollisuutta ei siis ole. Tilanne vastaakin enemmän neloskohdan mukaista tapausta, jossa viestintä on ennalta rajoittamatonta, koska kaksi muuta käyttäjää voivat vapaasti lisätä uusia profiileja keskusteluun[63]. Se että käyttäjä ei tiedä tästä ominaisuudesta, ei tee viestinnästä luottamuksellista, vaan oletus on, että käyttäjä on tutustunut käyttämänsä palvelun ominaisuuksiin riittävällä tavalla.

3.2 Suojauksen murtaminen sosiaalisessa mediassa

Toisen käyttäjän käyttäjätunnus ja salasana on mahdollista saada haltuunsa usealla eri tavalla, mutta käyttäjätilille voi päästä käsiksi myös ilman käyttäjätunnusta ja salasanaa. Tämän takia voidaankin erottaa kaksi eri tekotapaa:

1) Käyttäjätunnus ja salasana on saatu haltuun, jonka avulla on kirjauduttu käyttäjätilille
2) Käyttäjätili saadaan käyttöön ilman käyttäjätunnusta ja salasanaa

Näiden tekomuotojen sisältä löytyy useita erilaisia tekotapoja ja niillä on oleellinen vaikutus teon rangaistavuuteen. Esittelen seuraavaksi eri mahdollisuudet näiden tekomuotojen sisällä.

3.2.1 Käyttäjätunnus hallussa

[62] Kahdenvälisessä viestinnässä tätä mahdollisuutta ei ole. Etenkin nuoret käyttävät melko usein Facebookissa mahdollisuutta käydä ryhmäkeskusteluja yksityisviestipuolella. Kyseistä toimintaa voi verrata esimerkiksi Whatsapp-sovelluksella muodostettuun keskusteluryhmään.
[63] Kyseessä on siis teknisesti eri asia kuin linkittämisessä eteenpäin, jolloin kyse olisi luottamuksellisesta viestistä, joka on vain jaettu eteenpäin.

Jos tekijällä on käyttäjätunnus ja salasana hallussa, ei yleensä synny epäselviä tilanteita suojauksen murtamisen tunnusmerkistön täyttymisen suhteen. Tällöin tekijä kirjautuu käyttäjätilille nimenomaisella toimella. Poikkeuksen tähän voi tehdä oikeudettomuusvaatimuksen takia käyttäjätilin haltijan suostumus, jolloin luottamuksellistenkin viestien käsittely on lähtökohtaisesti toisen käyttäjän toimesta sallittua.

Ongelmia voivat tuottaa tapaukset, joissa esimerkiksi Facebookin käyttäjätunnuksilla pystyy kirjautumaan johonkin toiseenkin palveluun, jolloin voi päästä käsiksi myös toisen palvelun luottamuksellisiin viesteihin. Kyseeseen voi tulla myös tapaus, jossa esimerkiksi sähköpostien joukosta löytyy linkki pilvipalveluun, johon linkki antaa käyttöoikeuden. Näissä tilanteissa tulee arvioida sitä, kuinka tarkkarajaisesti suostumus on annettu ja mitä palveluja se on koskenut. Lähtökohtaisesti suostumus olla riittävän yksilöity jokaiselle palvelulle erikseen.

> Suostumukseen voi perustua myös vanhemman oikeus lukea lapsen luottamukselliset viestit. Jos lapsi kieltää luottamuksellisten viestien lukemisen, on tilanne monimutkaisempi. Tällöin tulee arvioida huoltajan syytä lukea luottamuksellisia viestejä ja sitä minkä ikäinen lapsi on kyseessä. Laissa lapsen huollosta ja tapaamisoikeudesta (361/1983) todetaan, että lapsen holhoojan tulee turvata lapselle ikään ja kehitystasoon tarpeellinen valvonta ja huolenpito. Holhoustoimilain (442/1999) 89 §:n mukaan edunvalvojalla on ilman päämiehensä suostumusta oikeus avata vain sellaisia päämiehelleen saapuneita kirjeitä tai niihin rinnastettavia suljettuja viestejä, joiden voidaan lähettäjän nimen tai muun erityisen seikan perusteella päätellä koskevan asiaa, josta edunvalvojan tulee huolehtia. Holhoustoimilain tarkoitus on tosin lähinnä taloudellisten etujen valvonta, jonka takia holhoojan oikeus lukea luottamuksellisia viestejä sosiaalisessa mediassa ei ole selkeästi säänneltyä.
>
> Voidaan todeta, että rutiininomainen lapsen viestien lukeminen ei ole sallittua ja lastaa tulee kuulla aina ennen viestien lukemista. Jos kyseessä on lastensuojelullisen huolen herättävä tapaus, kuten epäily seksuaalirikoksesta, on holhoojalla näkemykseni mukaan tietyissä tapauksissa jopa velvollisuus lukea viestit lapsen turvallisuuden takaamiseksi. Jokaisessa tapauksessa tuleekin painottaa lapsen etua ja ratkaista teon oikeutus sen mukaan. Vaikka kaikkien perusoikeuksien rajoituksien tulisi perustua lakiin, emme voi säännellä etenkään lapsen kasvatustoimintaa ylitarkasti. Tällöin olisimme tilanteessa, jossa esimerkiksi lelun takavarikointi lapselta tai kotiarestiin määrääminen tulisi perustua johonkin tiettyyn säännökseen, koska myös näissä puututaan lapsen perusoikeuksiin.
>
> Sähköisen viestinnän tietosuojalaissa on myös erikseen kaksi eri poikkeusta alaikäisiin liittyen. Holhoojalla on oikeus saada alle 15-vuotiasta lasta koskevat tunnistamis- ja paikkatiedot (SVTSL 6:24.3 ja SVTSL 9:37.2).

Tietomurron esitöissä suojauksen murtamista on kuvattu siten, että tunkeutumisen tulee tapahtua järjestelmän turvajärjestely murtamalla ja turvajärjestelystä mainitaan esimerkkinä käyttäjätunnus, joka tietojärjestelmään pyrkivän on osattava päästäkseen järjestelmän tietoihin käsiksi. Käyttäjätunnus kuvataan yksilöllisesti määritellyksi merkkiketjuksi.[64]

[64] *HE 94/1993 vp*, s. 155.

Sosiaalisen median kohdalla käyttäjätunnuksen määritelmällä tarkoitetaan yleensä pelkkää sähköpostiosoitetta, profiilin nimeä tai nimimerkkiä keskustelupalstalla. Pelkällä nimenomaisella käyttäjätunnuksella on kuitenkin mahdotonta päästä käsiksi luottamuksellisiin viesteihin ja tämä osa käyttäjätunnusta onkin yleensä julkisesti esillä. Käyttäjätunnuksen käyttämiseksi tarvitaan salasana, jonka haltuun saaminen on merkittävämmässä roolissa rikoksen tunnusmerkistön täytymisen osalta. Salasana sisältyy esitöiden käyttäjätunnuksen määritelmään, koska käyttäjätunnusta ei yleensä pysty käyttämään ilman sitä. Sosiaalisen median profiilien ja nimimerkkien osalta olisi selvempää puhua käyttäjätilistä, jonka käyttämiseen tarvitaan käyttäjätunnus ja salasana. Näiden kohdalla salasana taas on selkeästi avainasemassa suojauksen murtamisen osalta.

Salasanan haltuun saamiseksi on useita erilaisia keinoja. Salasana on voitu saada haltuun esimerkiksi ns. keylogger-haittaohjelmalla, joka tallentaa tietokoneen käyttäjän näppäinpainallukset ja välittää ne eteenpäin. Salasana voidaan saada haltuun myös kalastelusivun avulla. Tällöin tekijä yleensä linkittää kohteelle sivuston, jonka kautta kirjautumalla luvataan esimerkiksi jotain taloudellisia etuja, jotta henkilö saadaan syöttämään tiedot. Tällöin puhutaan monesti jo viestintäsalaisuuden törkeästä tekomuodosta (RL 38:4), koska apuna on käytetty rikoksen tekemistä varten suunniteltua tai muunnettua tietojenkäsittelyohjelmaa tai teknistä erityislaitetta. Sen takia en käy läpi tarkemmin näitä tekomuotoja tässä kirjoituksessa.

Tietomurron tunnusmerkistön täyttää myös pelkkä salasanan arvaaminen, joka voi olla löyhän salasanan takia erittäin helppoa.[65] Tällöinkin salasanan on ollut tekijän hallussa. Jossain tapauksissa salasanaan kuuluu erillinen turvakysymys, joka voidaan näyttää, jos ei muista enää salasanaansa. Kysymys voi olla esimerkiksi ”kuka oli ensimmäisen luokkasi opettaja” tai ”lemmikkini nimi”. Kohteen sosiaalisen mediaan lataamista kuvista voi saada vihiä näihin salasanoihin, koska siellä on esimerkiksi voitu mainita lemmikkikoira nimi, johon salasana perustuu. Sama koskee myös salasanan selvittämistä kurkkimalla olan yli tai löytämällä salasana esimerkiksi muistilappuun kirjoitettuna.

3.2.2 Käyttäjätunnusta ei hallussa

[65] Valitettavan usein ihmiset käyttävät salasanoja, jotka ovat liian helposti arvattavissa. Näitä ovat esimerkiksi salasanat ”123456”, ”salasana” ja ”qwerty”.

Käyttäjätilille voi päästä myös muilla tavoin, kuin kirjautumalla nimenomaisesti käyttäjätunnuksella ja salasanalla. Tällä taas voi olla suuri vaikutus teon rangaistavuuteen. Näistä tapauksista voidaan erotella esimerkiksi seuraavat tilanteet:

1) Käyttäjätili aukeaa suoraan esille kun selain avataan
2) Käyttäjätili aukeaa älypuhelimen sovellus avaamalla
3) Käyttäjätili on valmiina auki laitteella

Ensinnäkin käyttäjätunnus ja salasana on mahdollista tallentaa selaimelle, jonka seurauksena seuraavan kerran palvelua käytettäessä käyttäjätili aukeaa suoraan. On myös mahdollista asettaa palvelu pitämään käyttäjä sisäänkirjautuneena. Esimerkiksi Facebookista löytyy tällainen ominaisuus ja vaikka selain suljetaan, aukeaa käyttäjätili auki kun seuraavan kerran selain aukaistaan ja siirrytään Facebookin sivuille.

> On myös olemassa erilaisia ohjelmia, joihin voi tallentaa eri palveluiden salasanat, jolloin ohjelmaa käyttämällä pääsee käsiksi useampaan palveluun yhdellä kirjautumisella ja ns. pääsalasanalla. Tällöin oikeudettomaan kirjautumisen ja suojauksen murtamisen problematiikka on kuitenkin samanlainen kuin edellisessä kohdassa, koska sosiaalisen median käyttäjätunnuksen käyttämiseen tarvitaan kuitenkin pääsalasana.

Viestintäsalaisuuden loukkauksen kannalta voidaan mainita esimerkkinä tilanne, jossa käyttäjä yrittää kirjautua Facebook-tililleen kirjaston yleiseltä koneelta. Edellinen käyttäjä on jostain syystä jättänyt kirjautumatta ulos palvelusta. Selvää on, että jos käyttäjä vain kirjaa edellisen käyttäjän ulos, ei hänen voida katsoa syyllistyneen viestintäsalaisuuden loukkaukseen, koska teko edellyttää tahallisuutta. Etenkin jos ei ole näyttöä siitä, että käyttäjä olisi aukaissut yksityisviestejä. Jos käyttäjä alkaa selailla käyttäjätilin sisältöä ja päätyy lukemaan yksityisviestejä, on tulkinta tahallisuuden osalta jo erilainen ja viestien lukemista voidaan pitää oikeudettomana. Teon kohdalla herää kuitenkin kysymys siitä, täyttyykö suojauksen murtamisen tunnusmerkistö.

Tähän otti kantaa Satakunnan käräjäoikeus tuomiossa (07.03.2014, R 13/2029), jonka kohdalla oli kyse tapauksesta, jossa vastaaja oli käyttänyt perheen yhteistä tablettitietokonetta ja lukenut asianomistajan yksityisviestejä Facebookista. Vastaajaa syytettiin ensisijaisesti tieto-

murrosta ja vaihtoehtoinen syyte koski viestintäsalaisuuden loukkausta[66]. Kyseinen tablettitietokone oli ollut koko perheen käytössä ja suojattu nk. pin-koodilla, mutta kyseinen koodi oli ollut jokaisen perheenjäsenen tiedossa. Vastaaja oli havainnut selaimen avattuaan avoimen välilehden, jossa asianomistajan Facebook-profiili oli ollut avoinna, jonka käyttämiseen vastaajalla ei kuitenkaan ollut oikeutta. Vastaaja oli kertonut klikanneensa yhden yksityisviestin avoimeksi. Koska vastaajan teko oli selkeästi oikeudeton, kysymys oli pelkästään siitä, täyttyykö tunnusmerkistön mukainen suojauksen murtaminen. Käräjäoikeus viittasi tuomiossaan tietosuojavaltuutetun antamaan lausuntoon, jonka mukaan vastaaja oli käyttänyt toiselle kuulumattomia käyttäjätunnuksia, eikä käyttäjätunnuksen haltuun saamistavalla ole merkitystä rikoksen täyttymisen kannalta. Siten myös avoimen profiilin selailu riitti täyttämään suojauksen murtamisen tunnusmerkistön. Vastaaja tuomittiin viestintäsalaisuuden loukkauksesta 15 päiväsakkoon.

Käräjäoikeuden päätös on ongelmallinen, koska käyttäjätunnukset eivät olleet missään vaiheessa tosiasiallisesti vastaajan hallussa tai edes tiedossa. Vastaajalla ei olisi edes ollut mahdollisuutta saada salasanaa haltuun, vaikka hän oli kirjautuneena asianomistajan käyttäjätilille. Käyttäjätilin salasanaa kun ei pysty näkemään Facebookissa, vaikka olisi sisäänkirjatuneena. Tuomiossa viitattiin tietomurtoa koskeviin esitöihin, joiden mukaan ilmaisulle ”suojaus murtaen” on annettu lavea merkityssisältö, eikä se vastaa ”murtaa” sanan perinteistä merkitystä. Kysymys on enemmin kielikuvasta, jolla on ollut tarkoitus ilmaista, että turvajärjestelyn läpäisy on luvatonta. Tuomiossa ei kuitenkaan tuotu esille sitä seikkaa, että samaisten esitöiden mukaan turvajärjestely tulee läpäistä jollakin rikoksen tekijän *nimenomaisella* toimella, eikä esimerkiksi turvajärjestelyn satunnainen epäkunto ja siitä johtuva ulkopuolisen pääsy järjestelmään kuulu säännöksen piiriin[67]. Tapauksessa vastaajalla ei ollut missään vaiheessa asianomistajan salasanaa hallussa, eikä hän tehnyt mitään nimenomaista tointa turvajärjestelyn murtamiseksi, koska käyttäjätili oli jo avoimena selaimella. Siten vastaaja ei mielestäni syyllistynyt tapauksessa viestintäsalaisuuden loukkaukseen viestin sisällön osalta. Samalla perusteella myöskään tietomurron tunnusmerkistö ei täyttynyt. Viestintäsalaisuuden loukkaus olisi voinut kuitenkin täyttyä tunnistamistietojen perusteella, joiden kohdalla riittää pelkkä oikeudeton tiedon hankkiminen. Käräjäoikeus ei kuitenkaan ottanut tunnistamistietojen suojaan mitään kantaa.

---

[66] Tietomurto siis täydentää osaltaan viestintäsalaisuutta. Tosin suojauksen murtamisen kohdalla problematiikka on samanlainen tunnusmerkistön täyttymisen suhteen, koska viestintäsalaisuuden sähköisen viestien osalta suojauksen murtamisen tekotapatunnusmerkistö vastaa tietomurron tekotapaa.

[67] *HE 94/1993 vp*, s. 155.

Toisen tekotavan kohdalla on kyse älypuhelinsovelluksesta, joiden kohdalla salasana on yleensä aina tallennettu sosiaalisen median palveluun ja käyttäjätili aukeaa automaattisesti sovelluksen kuvaketta painamalla. Tällöin tekijällä tulee olla kohteen älypuhelin hallussa. Jos älypuhelin on luvatta hallussa, ei sovelluksen käyttämisen oikeudettomuuden osalta ole epäselvyyttä. Älypuhelin voi olla hallussa myös luvallisesti, mutta ilman suostumusta käyttää sovelluksia[68]. Käyttäjätilin käyttöä sovelluksen kautta koskee kuitenkin sama ”suojauksen murtamisen” problematiikka kuin selaimelle auki jäävän käyttäjätilin osalta. Vaikka tekijä aukaisee sovelluksen oikeudettomasti, ei hän murra mitään suojausta, jos sovellus aukeaa suoraan salasanan tallentamisen seurauksena. Siten myös sovelluksen aukaistaessa kyseeseen tulee viestintäsalaisuuden loukkaus vain tunnistamistietojen osalta[69], jos sovelluksen aukaisu on ollut oikeudetonta.

Kolmantena tekotapana kyseeseen voi tulla kyseeseen tapaukset, jossa pöytätietokoneelle on unohdettu auki käyttäjätili ja kyseiset tiedot ovat suoraan käyttäjän nähtävänä.[70] Kyseessä voi olla esimerkiksi tilanne, jossa opettaja on jättänyt tietokoneensa auki ja oppilas näkee opettajan käyttäjätilin avoimena. Tai vaihtoehtoisesti tilanne, jossa aviopuoliso huomaa avoinna olevan käyttäjätilin yhteisellä tietokoneella. Jos käyttäjä ei käytä käyttäjätiliä, ei pelkkää tietokoneen näytön tarkastelua voida pitää rangaistavana tekona. Jos henkilö alkaa klikkailemaan auki käyttäjätilin eri osioita ja yksityisviestejä, on teko rangaistava vain tunnistamistietojen osalta kakkoskohdan esimerkkien mukaisesti, koska suojauksen murtamisen tunnusmerkistö ei täyty.

Arvioitaessa näyttökynnystä suojauksen murtamisen ja auki jääneen käyttäjätilin viestien katsomisen välillä, voidaan tarkastella Helsingin käräjäoikeuden antamaan tuomiota (28.03.2014, R 13/9449), jossa suojauksen murtamisen katsottiin tapahtuneen, vaikka asiasta ei ollut selkeää näyttöä. Tapauksessa oli kyse hampurilaisravintolassa tapahtuneesta teosta, jossa epäiltiin työvuoropäällikön (myöhemmin D) ja kenttäpäällikön (myöhemmin E) lukeneen työntekijän (myöhemmin A) ja hänen työtoverinsa (myöhemmin B) välisiä yksityisviestejä Facebookista. Viesteissä oli tietoa siitä, että viestit lähettänyt B oli käynyt työhaastattelussa huoltamolla

[68] Esimerkiksi puhelun soittamista varten.
[69] Älypuhelimen ja muidenkin kiinteiden koneiden ja laitteiden kohdalla voi tulla kyseeseen myös luvaton käyttö (RL 28:7)
[70] Kyseinen tekotapa voi tulla kyseeseen myös puhelimen osalta, mutta tämä on huomattavasti epätodennäköisempi vaihtoehto.

nykyisen työpaikan ilmapiiriongelmien takia. Samalla työhaastattelussa ja sitä myöten myös viesteissä oli tullut ilmi, että B:n haastattelija (myöhemmin F) oli tuntenut asianomistajan nykyisessä työpaikassa toimineen D:n ja irtisanonut hänet huoltamolta aikaisemmin. Viesteissä oli auki myös keskustelu kolmannen työntekijän (myöhemmin C) kanssa, joka oli hampurilaisravintolassa toiminut toinen vuoropäällikkö[71].

> Mielenkiintoinen tapaus on myös sen takia, että myös viestinnän toisia osapuolia B ja C, jotka eivät olleet käyttäjätilin haltijoita, kohdeltiin asianomistajana viestintäsalaisuuden loukkaukseen. Tämän perusteella tapauksissa joissa tekijä esimerkiksi murtaa suojauksen sähköpostitiliin ja katsoo yksityisviestejä, kaikkien näytöllä näkyvien viestien lähettäjät tai vastaanottajat tulisi merkitä rikosilmoitukseen asianomistajiksi. Näin ei kuitenkaan käytännössä menetellä, vaan asianomistajana kohdellaan vain käyttäjätilin haltijaa. Viestintäsalaisuuden loukkauksen esitöissä ei asianomistajuuden määräytymistä käsitellä tarkemmin, mutta silloisen hallitusmuodon 8 §:n esitöissä todetaan, että ”säännös ei suojaa vain viestin lähettäjää, vaan kyseessä on molempien viestin lähettäjien perusoikeus”[72]. Käytännössä on erittäin ongelmallista, jos esitutkinnassa kohdeltaisiin kaikkia viestinnän osapuolia asianomistajina, vaikka kyseessä olisi vain yhteen käyttäjätiliin kohdistunut rikos.

A oli kirjautunut Facebook-profiiliinsa työnantajan tietokoneella viimeisenä päivänä ennen lomansa alkua 29.10.2012 ja kertoi kirjautuneensa käyttäjätililtä pois log off-toiminnolla[73]. A:n mukaan salasana oli vain hänen mielessään, eikä kukaan muu tiennyt sitä. Todistajana käräjäoikeudessa kuultu nainen (myöhemmin G) kertoi, että työntekijän profiili oli ollut auki työpaikan tietokoneella joko 31.10.2012 tai 1.11.2012, jolloin asianomistaja oli ollut jo lomamatkalla. G oli nähnyt nähnyt asianomistajan yksityisesti lähettämän viestin alapalkissa ja toinen keskustelu saattoi näkyä alapalkissa nimenä[74]. Toinen todistaja (myöhemmin H), jota ei jostain syystä kuultu käräjäoikeudessa, oli kertonut käyttäjätilin haltijalle nähneensä työntekijän profiilin avoinna jo 30.10.2012 ja hän oli myös kirjannut asianomistajan ulos profiilistaan.

Vastaajat D ja E olivat kertoneet, että D oli lukenut työpaikan tietokoneella vain A:n ja C:n välisiä yksityisviestejä. Edelleen molemmat kertoivat yhtenevästi, että D oli lähettänyt viestin edelleen E:lle, joka oli lähettänyt viestin myös henkilöstöpäällikölle. E kertoi syyksi halun selvittää, onko hampurilaisravintolaketjua loukattu kirjoituksissa. D kertoi esitutkinnassa, että

---

[71] Kyseinen henkilö ei ollut käräjäoikeudessa asianomistajana, koska ei ollut vaatinut rangaistusta.
[72] *PeVL 309/1993 vp.*
[73] Jos palvelusta ei kirjaudu ulos, aukeaa profiili auki automaattisesti seuraavan kerran kun selain aukaistaan ja Facebookin sivut aukaistaan.
[74] Alapalkissa näkyvä keskustelu on tietynlainen Facebookin messenger-toiminto, jossa keskustelut aukeavat varsinaisen yksityisviestisivun sijaan selaimen alalaitaan. Tuomion perusteella jää osittain epäselväksi, onko keskustelu käyty kolmen hengen ryhmässä vai onko käyttäjätilin haltija avannut viestin vastaanottajina toimineiden asianomistajien kanssa kaksi yksityisviestiketjua, joissa toisessa on ollut osapuolena työntekijä ja toisessa vuoropäällikkö.

E olisi myös itse käynyt lukemassa viestin työpaikan tietokoneelta, mutta käräjäoikeudessa ei ollut asiasta enää tietoinen.

Käräjäoikeus arvioi, että asianomistajien ja todistajan kertomuksella oli tullut selvitetyksi, että [A:n] käyttäjätili olisi avattu oikeudettomasti työpaikalla. Käräjäoikeus totesi, että ”koska [A] on kirjautunut facebook-sivultaan ulos, [D:n] ja [E:n] on täytynyt jollakin tavalla murtaa [A:n] facebook-tilin suojaus, vaikkakin asiassa jää epäselväksi, miten he ovat suojauksen pystyneet murtamaan eli miten he ovat saaneet tietoonsa käyttäjätunnuksen ja etenkin tilin salasanan.”.

Vaikka kaksi todistajaa olikin kirjannut A:n käyttäjätilin ulos järjestelmästä, on melko ongelmallista, että suojauksen murtamisen osalta ei ole tarkempaa näyttöä[75]. Käräjäoikeuden mukaan suojauksen murtamiseen riittää siis näyttö siitä, että käyttäjätili on ollut avoinna todistajien mukaan kahteen eri otteeseen. Vielä ongelmallisempaa on E:n katsottiin murtaneen suojauksen, vaikka hänelle oli lähetetty D:n toimesta viestin sisältö. Ei ollut mitään näyttöä siitä, että juuri D olisi kirjautunut käyttäjätilille. Oli vain oletus, että D olisi käynyt lukemassa viestejä myös työpaikalla Nyt E:n, mutta myös D:n katsottiin molempien kirjautuneen A:n käyttäjätilille. Jos D saisi tuomion pelkän avoimen käyttäjätilin viestejä katsomalla, olisi myös todistajana toimineet G ja H tullut tuomita siitä, että he olivat nähneet käyttäjätilin viestejä[76], joka taas ei suojauksen murtamisen täyttymisen osalta ole mahdollista.

E ja D tuomittiin viestintäsalaisuuden loukkauksesta molemmat 30 päiväsakkoon. E ja D tuomittiin maksamaan yhteisvastuullisesti A:lle 500 euroa ja B:lle 800 euroa kärsimyksestä. Tuomiosta ilmenevien seikkojen perusteella E ja D olisi tullut tuomita pikemminkin joko salassapitorikoksesta (RL 38:1) tai salassapitorikkomuksesta (RL 38:2), koska he olivat lähettäneet edelleen heille kuulumattomia luottamuksellisia viestejä, eikä näyttö ollut riittävä viestintäsalaisuuden loukkaukseen.

3.3 Tiedon hankkiminen viestistä

Perinteisen kirjeen kohdalla teon tunnusmerkistön täyttymishetki ei juurikaan aiheuta ongelmia. Tunnusmerkistön mukaisesti riittää, kun kirje avataan, joten kirjeen sisältöä ei tarvitse

[75] Näyttö tosin olisi riittänyt pelkkien tunnistamistietojen suoja perusteella, koska niiden osalta ei tarvitse murtaa suojausta, mutta en käsittele asiaa tämän tuomion yhteydessä tarkemmin.
[76] Viestien eteenpäin lähettäminen ei siis vaikuta millään tavalla viestintäsalaisuuden loukkauksen tunnusmerkistön täyttymiseen.

tarkastella millään tavalla, jotta viestintäsalaisuuden loukkaus täyttyisi. Sähköisen viestin ja etenkin sosiaalisen median kannalta tilanne on hieman monimutkaisempi.

Jos käyttäjätilille on päästy tunnusmerkistön mukaisesti suojaus murtaen, ei se välttämättä vielä riitä viestintäsalaisuuden loukkauksen tunnusmerkistön täyttymiseen. Jossain sosiaalisen median palveluissa viestiosio voi olla useamman klikkauksen takana, jolloin tekijä ei ole saanut tietoa viesteistä, ennen kun on klikannut itsensä viestiosioon. Viesteistä ei myöskään tule välttämättä suoraa ilmoitusta käyttäjätilin yleiseen osioon. Koska tekijä ei ole näissä tapauksissa vielä saanut tietoa viestistä, ei viestintäsalaisuuden loukkauksen tunnusmerkistö täyty. Teko täyttää kuitenkin tietomurron (RL 38:8) tunnusmerkistön.

Sähköpostin osalta tilanne on melko selvä, koska avatessaan sähköpostipalvelun, tulee viestitkin suoraan esille ja tämän takia tekijä on saanut tiedon viestistä. Vähintään tekijä saa tietoja tunnistamistiedoista, kuten viestin lähettäjästä, joten viestintäsalaisuuden loukkaus täyttyy joka tapauksessa.

Facebookin[77] kohdalla käyttäjä saa ilmoituksen uusista viesteistä viestilogoon, jossa näkyy saapuneiden yksityisviestien lukumäärä. Vaihtoehtoisesti ilmoitus viestistä voi tulla avonaisen profiilin kohdalla alapalkkiin. Tulkitsen tunnusmerkistöä siten, että pelkkä ilmoitus viestin saapumisesta riitä täyttämään viestintäsalaisuuden loukkauksen tunnusmerkistön, koska pelkkä *tiedon hankkiminen*[78] viestistä riittää. Selvää tunnusmerkistön täyttyminen on viimeistään siinä vaiheessa, kun tekijä klikkaa yksityisviestiosion auki. Yksityisviestiosissa näkyy pieni pätkä saapunutta tai lähetettyä viestiä, joka riittää viestintäsalaisuuden loukkauksen tunnusmerkistön täyttymiseen. Facebookin kohdalla tekijä voi syyllistyä tekoon jo profiilin seinän nähtyään, jos se sisältää rajatulle joukolle lähetetyn viestin tai tunnistamistietoja, jotka on tulkittava luottamuksellisiksi.

3.4 Välitettävänä oleva viesti

Nykypäivänä on melko vaikea nähdä tilannetta, jossa sosiaalisessa mediassa välitettävänä olevaan viestiin päästäisiin käsiksi ilman jonkinlaista teknistä erikoislaitetta tai haittaohjel-

[77] Sama koskee myös monia muita sosiaalisen median palveluita, kuten Twitterin yksityisviestiosiota.
[78] Säännöksen 2 kohdan mukaisessa välitettävänä olevan viestin tekomuodossa tunnusmerkistö vaatii tietoa viestin *sisällöstä*, joten pelkkä ilmoitus viestin olemassa olosta ei riitä.

maa, jolloin kyseeseen tulee ennemminkin törkeä viestintäsalaisuuden loukkaaminen (RL 38:4). Etenkin sosiaalisessa mediassa viestin välitettävänä olemisaika on erittäin lyhyt, eikä käytännössä onnistu ilman teknisiä erityislaitteita tai haittaohjelmaa. Näiden osalta teon tunnusmerkistön täyttymisen kanssa kohdataan siis harvemmin epäselvyyksiä.

Helsingin hovioikeuden tuomiossa (14.3.2006, R 04/746) oli kyse työntekijän sähköpostin kääntämisestä toiselle henkilölle lomautuksen ajaksi ja siitä, oliko siihen annettu sähköpostitilin haltijan suostumus. Nyblinin mukaan teon rangaistavuutta perusteltiin rikoslain 38 luvun 3 §:n 1 mom 2 kohdan mukaisena tekona, jossa viestin katsottiin olevan vielä välitettävänä. Syytteen mukaan vastaaja oli ”oikeudettomasti hankkinut tiedon televerkossa välittävänä olleen televiestin sisällöstä toimiessaan [yrityksen] toimitusjohtajana määräämällä [asianomistajalle] osoitetut sähköpostit käännettäväksi toiselle henkilölle, joka oli tullut tietoiseksi näiden viestien sisällöstä”.[79]

Käräjäoikeuden tai hovioikeuden ratkaisutekstissä ei oteta kantaa mitä viestintäsalaisuuden säännöksen kohtaa arvioidaan, vaan tyydytään käsittelemään lähinnä suostumuksen puuttumista. Käräjäoikeus totesi, että ”sähköpostin käyttäjätietojärjestelmän tarkoituksena on tukea luottamuksellista viestintää siten, että sähköpostiosoitteella saapuvat viestit jaetaan niiden oikeille vastaanottajille eikä niitä muut sivulliset pääse luvatta avaamaan. Viestien kääntäminen on mahdollistanut myös viestien oikeudettoman avaamisen. Viestien kääntäminen on aiheuttanut sen, että viestejä ei ole jaettu sille vastaanottajalle, jota lähettäjä on tarkoittanut.”. Vastaaja tuomittiin viestintäsalaisuuden loukkauksesta 15 päiväsakkoon.

Vaikka kyseinen tapaus tulkittaisiin välitettävänä olevaksi viestiksi, ei sillä sinänsä ole vaikutusta viestintäsalaisuuden loukkauksen tunnusmerkistön täyttymiseen sosiaalisessa mediassa. Jos tekijä on päässyt luvatta käsiksi käyttäjätiliin, täyttyy rikos jo sen kautta. Sosiaalisen median palveluissa taas on harvemmin ominaisuutta, jossa viestit pystyisi jatkolähettämään automaattisesti eteenpäin. Siten tekomuoto koskee lähinnä vain sähköpostia.

3.5 Tunnistamistiedot sosiaalisen median palveluissa

[79] *Nyblin 2009*, s. 318- 319.

Niin kuin edellä on mainittu, on viestintäsalaisuuden loukkaus ongelmallinen tunnistamistietojen ja viestin sisällön suojan suhteen. Näyttää siis siltä, että tunnistamistiedot ovat vanhemmin suojattuja kuin itse viestin sisältö. Kyseinen asia korostuu etenkin sosiaalisen median palveluissa suojauksen murtamiseen liittyvän problematiikan takia.

Sosiaalisen median tunnistamistietojen osalta voidaan mainita esimerkkeinä Facebookissa näkyvät tunnistamistiedot. Jos viesti on kirjoitettu seinälle luottamuksellisena viestinä rajatulle kaveriryhmälle, näkyy tunnistamistietoina yleensä lähettäjän käyttäjänimi, lähetysaika ja mahdollisesti myös lähetyspaikka[80]. Vastaanottajan käyttäjänimen pystyy yleensä tarkistamaan kaveri- tai jakolistalta. Tunnistamistiedot ovat yksityisviestipuolella samat. Esimerkkinä viestintäsalaisuuden loukkauksen kannalta voidaan mainita tilanne, jossa henkilö kurkkii salaa toisen henkilön takana, joka käyttää pöytätietokoneella sosiaalisen median palvelua. Jos näytöllä näkyy luottamuksellinen viesti, voi kurkkija syyllistyä viestintäsalaisuuden loukkaukseen nähdessään oikeudettomasti tunnistamistietoja viesteistä. Rangaistavaa ei siis ole tärkeämpänä oikeushyvänä pidetyn viestin sisällön näkeminen, koska kurkkija ei murra suojausta.

Sosiaalisen median viestistä löytyvät tunnistamistiedot eivät välttämättä aina liity viestin lähettämiseen. Esimerkiksi sosiaalisessa mediassa jaetun valokuvassa olevat metatiedot, eli EXIF-tiedot, eivät yleensä ole viestintäsalaisuuden loukkauksen tunnusmerkistön mukaisesti suojattuja. Digitaalisesta valokuvasta voidaan löytää esimerkiksi paikkatieto[81], jossa kuva on otettu. Jos kuva jaetaan heti sen jälkeen eteenpäin, voi viestin lähettäjän olinpaikka käytännössä paljastua paikkatiedon kautta. Kuvan paikkatieto ei kuitenkaan liity viestin lähettämiseen, koska luonnollisesti kuvan voisi julkaista sosiaalisessa mediassa myös myöhemmin. Paikkatiedot ovat kuitenkin muutoin suojattuja, kuten myös verkkosivustojen selailemisesta kertyvät tunnistamistiedot (SVTSL 2:4.1 ja 2:4.3)

Joissakin palveluissa, kuten pikaviestipalvelu IRC[82], voi viestin lähettäjän tunnistamistietona näkyä IP-osoite. IP-osoite voi näkyä suoraan myös jossain tapauksissa keskustelupalstoilla. Vaikka viesti olisikin lähetetty julkiselle keskustelufoorumille, on viestin tunnistamistiedot salaisia, jos tähän ei ole erikseen käyttäjän suostumusta (SVTSL 2:4.2)

[80] Tunnistamistietojen saatavuus on hyvin samanlainen muissakin palveluissa.
[81] Kuvasta voi löytyä myös kuvan ottohetki, kameran tiedot ja tekijänoikeustiedot.
[82] Kyseessä siis Internet Related Chat, eikä IRC-Galleria.

4 Johtopäätökset ja säännöksen muutostarpeet

Viime vuosina on koettu suuri murros ihmisten välisessä viestinnässä, koska sosiaalinen media on noussut viestintävälineenä perinteisempien viestintämuotojen ohi. Viestinnän suoja onkin joutunut koetukselle uusien viestintämuotojen kanssa, koska ne ovat tuoneet mukanaan useita erilaisia tekotapoja. Vaikka viestintäsalaisuuden loukkauksen esityöt ovat jo yli kahdenkymmenenvuoden takaa, on säännös säilyttänyt suhteellisen hyvin asemansa tegnologianeutraalin rakenteensa takia. Ongelmiakin tosin löytyy, niin kuin tässä kirjoituksessa on tuotu jo esille.

Perinteisen kirjesalaisuuden kohdalla säännös toimii hyvin, mutta internetin ja sosiaalisen median palvelujen takia tunnistamistietojen suojelutarve on noussut. Säännös tuntuu olleen tämän osalta jopa hieman ennakoiva, koska tunnistamistietojen suoja näyttää olevan tällä hetkellä parempi kuin itse perusoikeussuojan ytimenä pidetyn viestin sisällön. Jotta näiden välille saataisiin tasapaino, yksi vaihtoehto olisikin muuttaa säännöstä siten, että myös tunnistamistietojen kohdalla tulisi murtaa suojaus sähköisen viestin tapaan. En kuitenkaan pidä tätä vaihtoehtoa toimivana.

Järkevin tapa olisi muuttaa tunnusmerkistöä siten, että suojauksen murtamisen tunnusmerkistöä muutettaisiin enemmän luvattoman käytön suuntaan, jossa käyttäjätunnuksen suojausta ei tarvitsisi murtaa, vaan pelkkä käyttäjätunnusten luvaton käyttö luottamuksellisen viestin lukemistarkoituksella riittäisi tunnusmerkistön täyttymiseen. Käytännössä tämä tarkoittaisi sitä, että jo pelkkä vahingossa auki jääneen käyttäjätilin yksityisviestien selailu tai älypuhelimen sovelluksen aukaiseminen ilman suojauksen murtamista olisi rangaistavaa viestin sisältöön, eikä tunnistamistietoihin perustuen. Tällöin rikoksen tunnusmerkistö täyttyisi aina myös tunnistamistietojen osalta, mutta teko olisi rangaistavaa ensisijaisesti viestin sisällön selvittämisen perusteella.

Säännökseen jäisi edelleen oikeudettomuusvaatimus, joka indikoi tekijän tahallisuutta selvittää viestin sisältö. Rangaistavuuden ulkopuolelle jäisivät siis edelleen tapaukset, joissa henkilö on vain sattumalta nähnyt auki jääneeltä tietokoneelta luottamuksellisia viestejä, tai aukaisee selaimen, joka näyttää ilman lisäklikkauksia suoraan luottamuksellisia viestejä.

Rikoslain 38 luvun 3 §:n 1 momentin 1 kohdan tunnusmerkistö tulisikin muotoilla seuraavanlaisesti:

”*avaa toiselle osoitetun kirjeen tai muun suljetun viestin taikka hankkii luvattomasti tiedon sähköisesti tai muulla vastaavalla tavalla teknisellä keinolla tallennetusta, ulkopuoliselta suojatusta viestistä tai välitystiedosta taikka*”.

Nykyisen tunnusmerkistöstä siis poistettaisiin sanat ”suojauksen murtaen” ja lisättäisiin sana ”luvattomasti”, joka vastaisi tekotavaltaan luvattoman käytön tunnusmerkistöä (RL 28:7) nykyisen suojauksen murtamista vastaavan tietomurron (RL 38:8) sijaan.

> Luvattoman käytön kohdalla tulisi kuitenkin mainita tunnusmerkistössä se, että sillä tarkoitettaisiin käyttäjätilin luvatonta käyttöä. Luvattoman käytön tunnusmerkistön mukaan rangaistavaa on ”käyttää toisen irtainta omaisuutta taikka kiinteää konetta tai laitetta”. Jos tekijä siis käyttää omaa tietokonettaan toisen käyttäjätilin käyttämiseen, ei kyse ole luvattomasta käytöstä käyttäjätilin haltijan osalta. Luvattoman käytön esitöissä asia ilmaistaan tietokonejärjestelmään tunkeutumisena ja ”tietokoneajan varastamisena”[83]. Jos tekijä siis esimerkiksi kirjautuu luvatta toisen henkilön Facebook-profiiliin omalla tietokoneellaan, ei hän käytä kohteen tietokoneaikaa. Kyseinen ”tietokoneaika” kun on oikeasti Facebookin palvelimien toimintaan kohdistuvaa ja kohteen käyttäjätilin tiedot ovat vain tallennettuna kyseisillä palvelimille. Asianomistajana luvattomaan käyttöön on siis oikeasti Facebook.

Edelleen 1 kohdan sana ”taikka” vaihdettaisiin muotoon ”tai” ja lisättäisiin sanat ”tai välitystiedosta taikka”. Näin viestin välitystiedot, eli viestin tunnistamistiedot, olisivat yhtä lailla suojattuja kuin itse viestin sisältö ja otettaisiin huomioon tietoyhteiskuntakaaren uusi nimitys viestin tunnistamistietoihin liittyen. Koska tunnistamistiedot olisi kriminalisoitu kyseisessä kohdassa, voisi rikoslain 38 luvun 1 momentin 2 kohdan tunnistamistietoja koskeva tunnusmerkistö ”taikka tällaisen viestin lähettämisestä tai vastaanottamisesta” poistaa. Samalla myös säännöksen rakenne paranisi, koska 1 momentin 2 kohdassa olisi kyse selkeästi vain välitettävänä olevan viestin suojasta.

Tarkoituksena ei olisi analogian mukaisesti kriminalisoida jo avatun kirjeen lukemista, mutta sähköisen viestin osalta jo avatun ja luetun viestin luvaton lukemisen kriminalisoiminen on perusteltua. Jos henkilö on aukaissut kirjeen ja hän ei halua paljastaa sen sisältöä muille, on kirje helppo hävittää ilman että siitä jää jälkiä. Toki tämä mahdollisuus on olemassa myös

[83] *HE 66/1988 vp,* s. 43.

sähköisten viestien osalta, mutta mahdollisuus, että niistä on jäänyt sähköisiä jälkiä[84], on selkeästi suurempi. Suojelun tarvetta tukee sähköisten viestien kohdalla myös mahdollinen viestien suuri määrä. Kirjeitä tekijällä ei ole hallussa yleensä kuin yksi, kun taas sähköisten viestien osalta on normaalia, että pääsemällä käsiksi toisen sähköisiin luottamuksellisiin viesteihin, niitä löytyy samalla kertaa kymmeniä tai jopa satoja. Voidaan siis todeta, että henkilön sähköisten viestien alusta vaatii laajempaa suojaa kuin yksittäinen kirje.

Sähköisen viestin suoja, silloin kun se on välitettävänä, on riittävällä tasolla internetin ja sosiaalisen median suhteen[85]. Käytännössä on mahdotonta saada sähköisen viestin sisällöstä tietoa sen ollessa välitettävänä, jollei käytetä erilaisia teknisiä apuvälineitä tai haittaohjelmia. Tällöin teko on myös yleensä tunnusmerkistöltään törkeä.

[84] Esimerkkeinä voidaan mainita mahdollisuus palauttaa älypuhelimen varmuuskopion kautta luottamuksellisia viestejä tai tilata Facebookin kaikki yksityisviestit rekisteröitymisessä käytetylle sähköpostitilille.
[85] Pois lukien aikaisemmin *OMML 27/2014* liittyvät seikat.