VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Milla Niemi

YKSITYISYYDEN SUOJA SOSIAALISEN MEDIAN PALVELUISSA YKSITYISHENKILÖN KANNALTA

Yksityisoikeudelliset perusteet ja tietoturva verkossa

Liiketalous
2019

VAASAN AMMATTIKORKEAKOULU
Liiketalous

TIIVISTELMÄ

Tekijä	Milla Niemi
Opinnäytetyön nimi	Yksityisyyden suoja sosiaalisen median palveluissa yksityishenkilön kannalta
Vuosi	2019
Kieli	suomi
Sivumäärä	54
Ohjaaja	Marika Teirfolk-Naarmala

Tämä tutkimus käsittelee yksityisyyden suojaa sosiaalisen median palveluissa yksityishenkilön kannalta. Sosiaaliseen mediaan pääsy on helppoa ja se on pyritty pitämään vapaana liiallisesta sääntelystä. Tutkimuksen tavoite on selvittää, millä tavoin käyttäjän yksityisyyttä voidaan suojata sosiaalisen median palveluissa ja millaisia uhkia sosiaalinen media voi aiheuttaa yksityisyyden suojan toteutumiselle.

Tutkimuksen teoreettisen viitekehyksen muodostavat aiheeseen liittyvä lainsäädäntö, lainvalmistelut, oikeuskirjallisuus sekä oikeustapaukset. Teoriaosuudessa käydään läpi yksityisyyden suojaa, sosiaalisen median keskeistä lainsäädäntöä sekä yksityisyyden merkitystä ja sen uhkia sosiaalisessa mediassa. Tutkimus toteutetaan lainopillisena kirjoituspöytätutkimuksena, jonka tehtävä on vastata tutkimuskysymyksiin voimassaolevien oikeuslähteiden mukaan. Tutkimuksessa tutkitaan oikeusjärjestykseen kuuluvia sääntöjä ja tulkitaan niiden sisältöä.

Tutkimuksessa käytetyn materiaalin ja siten myös tutkimustulosten perusteella voidaan todeta, että oikeudellisesti katsoen Internet ja sosiaalinen media on hyvin vaikeasti määriteltävä kokonaisuus, jossa vastuu on pääosin käyttäjällä. Käyttäjä hyväksyy palveluntarjoajan ehdot, jotka velvoittavat käyttäjää toimimaan asianmukaisella tavalla. Sosiaalisen median mahdollistamia merkittäviä ilmiöitä ovat mielipiteiden ja ajatusten jakaminen sekä ihmisten välinen yhteisöllisyys. Käyttäjän on kuitenkin aina tiedostettava riski siitä, että julkaisut voivat levitä tietoverkoissa.

Avainsanat yksityisyys, sosiaalinen media, lainsäädäntö, internet

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Oikeushallinto

ABSTRACT

Author	Milla Niemi
Title	Privacy Protection In Social Media Services from a Private Person's Wiewpoint
Year	2019
Language	Finnish
Pages	54
Name of Supervisor	Marika Teirfolk-Naarmala

This thesis studied the privacy protection in social media from a private person's viewpoint. Access to social media is easy and the general aim has been to keep it free from over-regulation. The objective of this survey was to find out how users' privacy can be protected in social media services and what kind of threats social media may cause to the actualization of the privacy protection.

The theoretical framework consists of legislation related to the thesis' subject, government proposals, legal literature and legal cases. The ethical study examines privacy policy, the key social media legislation and the importance of privacy and threats in social media. The research was conducted as a legal desk research, which mission was to answer to the set research questions based on valid legal sources. The study examined the rules of the legal system and interpreted its contents.

Based on the material used in the study and thus the results of the research it can be stated that the Internet and the social media is legally difficult to define, and clearly the responsibility lies with the user. The user accepts the terms of the service provider that oblige the user to act in an appropriate manner. The most important phenomena of the social media are sharing opinions and thoughts and interpersonal communality. The user must be aware of the risk that publications can spread through networks. The worst threats to an individual in social media are crimes concerning the dissemination of privacy information or offensive acts on an individual's honor.

Keywords privacy, social media, legislation, Internet

SISÄLLYS

1 JOHDANTO

Sähköinen viestintä sosiaalisessa mediassa on oikeudellisesti melko vaikeasti hallittava kokonaisuus. Perusoikeuksien suojaamisen ja rajoittamisen sääntely sekä asioiden tarkastelu tietosuojan näkökulmasta tuottavat usein ongelmia. Suomen perustuslaki turvaa jokaiselle perusoikeutena oikeuden yksityiselämään, kunniaan ja kotirauhaan. Esimerkiksi kirjeet, puhelut ja muut luottamukselliset viestit ovat salaisia, eikä tätä salaisuutta saa loukata. Digitaalisuus haastaa kuitenkin omalta osaltaan lainsäädännön ja se on saavuttamassa aivan uusia ulottuvuuksia. Tutkimuksen aiheena onkin selvittää yksityisyyden suojan perusteet sosiaalisen median palveluita käytettäessä, yksityishenkilön kannalta. (L 11.6.1999/731)

1.1 Tutkimuksen tausta

Yksityistietojamme löytyy hyvin paljon erilaisista digitaalisista järjestelmistä ja sosiaalisen median palveluista. Osa talletetuista tiedoista on mahdollista saada automaattisesti (osoite, asuinpaikka), toisinaan taas tietoja kertyy omien toimintojemme seurauksena (sosiaalinen media, verkkotilaukset). Internet ja sosiaalinen media on kaikki ja kaikkialla. Tietosuojaa ja tietoturvaa tulee tarkastella aivan uudesta näkökulmasta, kun käyttöympäristöt ja palvelut siirtyvät yhä enenevissä määrin sosiaaliseen mediaan. Sosiaalinen media mahdollistaa kattavan verkostoitumisen, markkinoinnin, ihmissuhteiden ylläpitämisen, ajankohtaisista asioista tiedottamisen ja jakamisen. Se on nopeampi ja tehokkaampi kuin muut medialähteet, mutta samalla myös armottomampi. (Hakola 2012)

Internetissä yksityishenkilön henkilötietojen tietosuojaa turvaa erityisesti laki sähköisen viestinnän palveluista. Muita yksityisyyden suojaa säätteleviä lakeja ovat muun muassa perustuslaki, julkisuuslaki, laki yksityisyyden suojasta työelämässä, tietoyhteiskuntakaari, henkilörekisterilaki sekä henkilötietolaki (henkilötietolaki kumottiin tietosuojalailla L 5.12.2018/1050, joka on voimassa 1.1.2019 alkaen). Lainalaisuuksista huolimatta aihe on kuitenkin ongelmallinen,

sillä yhä enenevissä määrin sivustot tallentavat, valvovat ja mahdollisesti jopa analysoivat käyttäjiensä tietoja ja toimia.

Opinnäytetyön aihevalinta muodostui syksyllä 2018, kun suoritin ammattiharjoitteluani Pohjanmaan käräjäoikeudessa. Tutkimus käsittelee aihetta yksityishenkilön kannalta, vaikka suuri osa sosiaalisen median käyttäjistä on myös yrityksiä, yhteisöjä sekä viranomaistahoja.

1.2 Tutkimuksen tavoite

Tutkimuksen tavoite on selvittää, millä tavoin yksityishenkilö pystyy suojaamaan yksityisyyttään, kun käytetään sähköisen viestinnän palveluita sosiaalisessa mediassa. Samalla pohditaan myös, mitä yksityisyyden suoja sosiaalisessa mediassa merkitsee yksityishenkilölle. Tutkimuskysymyksiä on neljä:

1. Mitä yksityisyyden suoja sosiaalisessa mediassa tarkoittaa yksityishenkilön osalta?
2. Mitkä eri tahot voivat uhata yksityishenkilön yksityisyyden suojaa sosiaalisessa mediassa?
3. Millaisia uhkia sähköinen viestintä voi aiheuttaa yksityishenkilön suojalle sosiaalisessa mediassa?
4. Miten yksityishenkilö voi turvata yksityisyyden suojaa sosiaalisen median verkossa?

Aiheesta löytyy aikaisempaa oikeustieteellistä tutkimusmateriaalia, mutta hyvin vähän. Muissa tieteissä kyseessä olevaa problematiikkaa on kuitenkin tutkittu. Eräs kattava viestintätieteiden pro gradu -tutkielma löytyy vuodelta 2009, jonka on laatinut Sirpa Hankkila Vaasan yliopistosta, humastistisesta tiedekunnasta. Pro gradu -tutkielman aiheena hänellä on ollut ”Yksityisyys sosiaalisessa mediassa – yksityisyyden riskit Vuodatus.netissä ja Facebookissa”.

Sosiaalinen media on jatkuvasti kehittyvä ja muuttuva kokonaisuus, mikä tuo osaltaan siihen jatkuvasti uusia näkökulmia ja huomioitavaa. Tutkimuksen avulla pyritään selvittämään myös sitä, miten eri kanavat suojaavat käyttäjiensä

henkilötietoja ja yksityisyyttä, sekä sitä, missä menee vastuun raja sivuston ylläpitäjän ja itse sivuston käyttäjän välillä.

1.3 Tutkimusmenetelmä ja tutkimusaineisto

Tutkimus on toteutettu lainopillisena kirjoituspöytätutkimuksena. Lainopillisen tutkimuksen tehtävä on vastata tutkimuskysymyksiin voimassaolevien oikeuslähteiden mukaan. Lainopilla tarkoitetaan siis oikeusjärjestykseen kuuluvien sääntöjen tutkimista ja niiden sisällön tulkitsemista. Lainopillisessa tutkimuksessa olennaista on myös tutkimuskohteen systemasointi eli voimassa olevan oikeuden jäsentäminen. (Husa, Mutanen & Pohjolainen 2008, 20)

Tutkimuksessa on käytetty aineistona oikeuslähteitä kuten lainsäädäntöä, hallituksen esityksiä, oikeuskirjallisuutta, lakitietopalvelu Edilexin artikkeleita sekä oikeustapauksia. Kyseiset oikeuslähteet voidaan jakaa ryhmiin niiden velvoittavuuden mukaan: vahvasti velvoittaviin, heikosti velvoittaviin sekä sallittuihin oikeuslähteisiin. Vahvasti velvoittavia ovat laki ja maantapa. Heikosti velvoittavilla puolestaan tarkoitetaan lainsäätäjän tarkoitusta ja tuomioistuinratkaisuja. Sallituiksi oikeuslähteiksi luetaan oikeustiede, oikeushistorialliset ja -vertailevat sekä reaaliset argumentit. (Husa ym. 2008, 32-33)

Tutkimuksessa käytetyt oikeustapaukset täsmentävät aiheeseen liittyviä säädöksiä sekä antavat konkreettisia esimerkkejä sosiaalisen median käytön lainalaisuuksista yksityishenkilön kannalta. Oikeustapausten avulla pyritään myös konkretisoimaan sosiaalisen median käyttäjän vastuun vakavuus, kun kyseessä ovat omat henkilötiedot tai muut yksityiset ja arkaluonteiset asiat.

1.4 Tutkimuksen rakenne

Tutkimus koostuu viidestä pääluvusta. Ensimmäisessä luvussa tarkastellaan tutkimuksen taustaa, tavoitteita, tutkimusmenetelmää ja tutkimusaineistoa sekä tutkimuksen rakennetta. Ensimmäisessä luvussa muun muassa esitellään tutkimuksen tavoitetta tukevat tutkimuskysymykset sekä analysoidaan tutkimuksessa käytettyä materiaalia. Toinen luku käsittelee yksityisyyden suojaa

ja sen käsitteen määritelmää lainsäädännön nojalla. Kolmannessa luvussa esitellään käsite ”sosiaalinen media” ja tutustutaan keskeiseen lainsäädäntöön aiheeseen liittyen. Kolmas luku tuo ilmi sen, miten useaan eri lakiin sähköisen viestinnän sääntely ja siten myös sosiaalinen media on ripoteltu.

Neljäs luku käsittelee yksityisyyttä sosiaalisen median palveluissa. Luvussa tarkastellaan oikeustapausten avulla sitä, millaisia riskejä ja uhkia sosiaalisessa mediassa voi esiintyä, miten tietoturva toteutuu sosiaalisessa mediassa ja millaisia yksityisyyteen liittyviä käytäntöjä sosiaalinen media pitää sisällään. Luvun lopussa käsitellään myös henkilötietojen jakamista sosiaalisen median verkkoympäristöissä.

Tutkimuksen viimeisessä luvussa esitellään keskeisimmät tutkimustulokset, arvioidaan tutkimuksen luotettavuutta sekä käydään läpi opinnäytetyöprosessin vaiheet ja eteneminen sekä mahdolliset jatkotutkimusaiheet.

2 YKSITYISYYDEN SUOJAN MÄÄRITTELY JA SOSIAALINEN MEDIA

Tämä luku käsittelee yksityisyyden suojaa ja sen käsitteen määritelmää. Yksityisyyden käsite kattaa yksilön oikeuden yksityiselämään sekä yksityisyyteen erilaisissa tietojenkäsittelymenetelmissä. (L 1.6.1999/731, 10 §) Tässä luvussa kerrotaan myös, mitä sosiaalisella medialla tarkoitetaan ja millaisia mahdollisuuksia se antaa käyttäjälleen.

2.1 Yksityisyyden suoja perusoikeutena

Yksityisyyden käsitettä ei ole virallisesti määritelty missään Suomen laissa tai säädöksessä, vaikka itse yksityisyyttä ilmentävätkin monet eri perusoikeudet. Vuonna 1988 yksityisyyden käsite omaksuttiin ensimmäistä kertaa Suomessa henkilörekisterilaissa. Lain perusteluissa yksityisyyden suojan voidaan todeta ilmenevän eri tilanteissa eri tavoin. Oikeus yksityisyyteen on myös tietyissä määrin suhteellista, sillä sitä koskevat vaatimukset voidaan joutua hetkellisesti kumoamaan tärkeämpien etujen vuoksi, esimerkiksi henkilörekisteriin kerättävien tietojen tai viranomaisten tarvitsemien henkilötietojen selvittämisen vuoksi. (Koskinen, Alapuranen, Heino & Lehtonen 2012, 38)

Rikoslain 24 luvun 8 §:n momentin säätämiseen johtaneessa hallituksen esityksessä (HE 19/2013) vp todetaan, että ”vain luonnollisilla henkilöillä on säännöksessä tarkoitettu yksityiselämä.” Täten tietojen levittäminen koskien oikeushenkilöä ei ole rangaistava säännöksen nojalla. Toinen huomioitava seikka on, että oikeushenkilöitä koskevien tietojen levittäminen voi joissakin tapauksissa merkitä myös luonnollisia henkilöitä koskevien tietojen levittämistä. Esityksessä mainitaan myös yksityisyyden suojan laajuuden riippuvan henkilön asemasta. Vallankäyttäjillä, julkisuuden henkilöillä ja tavallisilla ihmisillä suojan laajuus voi hieman vaihdella. Laajinta yksityisyyden suojaa nauttivat kuitenkin tavalliset kansalaiset. (HE 19/2013 vp, 38)

Yksityisyyden käsitettä tukevat lisäksi muun muassa seuraavat oikeudet: oikeus kunniaan, oikeus yhdenvertaiseen kohteluun, oikeus henkilökohtaiseen

koskemattomuuteen, oikeus ihmisarvoiseen kohteluun, oikeus turvallisuuteen sekä yhdenvertaisuus ja syrjinnän kielto sekä oikeus vaikuttaa itseään koskeviin asioihin. (Koskinen ym. 2012, 38)

Lasse Lehtosen julkaisemassa väitöskirjassa Lehtonen katsoo yksityisyyden merkitsevän yksilön itsemääräämisoikeutta, jota pidetään länsimaisessa demokratiassa koko perusoikeuksien olemassaolon edellytyksenä. Hänen mukaansa yksityisyys on yksilön oikeutta pitää itseään koskevat asiat omaa tietonaan ja poissa toisten ulottuvilta. Asia ei kuitenkaan ole niin yksiselitteinen, sillä sosiaalisessa mediassa yksilö voi jakaa tietoja itsestään, mutta haluaa silti pitää yksityisyytensä suojassa. Hankaluuksia tuottaakin se, millaista sisältöä voidaan pitää liian yksityiskohtaisena tietona jaettavaksi. (Kulla, Koillinen, Kuopus, Lavapuro, Lehtonen, Nieminen, Ollila, Pohjolainen, Pöysti, Sorvari H., Sorvari K., Tähti, Viljanen, Wallin 2002)

Luottamuksellinen viesintä ja viestintäsalaisuus kuuluvat myös lapsen perusoikeuksiin. Nykyajan sosiaalinen media on merkittävä osa mediakulttuuria, jossa lapset ja nuoret elävät. Mediakulttuurin muodostavat lukemattomat mediasisällöt, välineet ja ilmiöt, jotka vaikuttavat siihen, millaisia havaintoja lapsi maailmasta tekee. Mediakulttuuri vaikuttaa myös sekä lapsen että aikuisen ajattelutapoihin ja toimintaan. (Mannerheimin lastensuojeluliitto 2019)

Lähtökohtaisesti ihmisoikeudet ovat ikäneutraaleja, jolloin katsotaan, että myös lapsia suojaavat samat oikeudet, jotka sisältyvät ihmisoikeussopimuksiin. Lapsella on erityinen tarve suojeluun, jolloin ihmisoikeuksien voidaan katsoa olevan laajemmat kuin aikuisten ihmisoikeudet. YK:n sopimukseen on pyritty sisällyttämään kaikki lapsen aseman kannalta merkitykselliset osa-alueet ja siksi sitä voidaankin pitää lasten ihmisoikeuksien perusnormistona. (Virkkala 2016, 16)

YK:n lasten oikeuksien yleissopimuksen 13 artiklan mukaan: ”lapsella on oikeus ilmaista vapaasti mielipiteensä. Tämä oikeus sisältää vapauden hakea, vastaanottaa ja levittää kaikenlaisia tietoja ja ajatuksia yli rajojen suullisessa, kirjallisessa, painetussa, taiteen tai missä tahansa muussa lapsen valitsemassa

muodossa. Tämän oikeuden käytölle voidaan asettaa tiettyjä rajoituksia, mutta vain sellaisia, joista säädetään laissa ja jotka ovat välttämättömiä:

a) muiden oikeuksien tai maineen kunnioittamiseksi; tai

b) kansallisen turvallisuuden, yleisen järjestyksen (order public), tai väestön terveyden tai moraalin suojelemiseksi.” (LOS, artikla 13)

Viime vuosien muutokset mediaympäristöissä ovatkin herättäneet kysymyksiä lasten vanhemmille. Vaikka vanhemman onkin erityisen tärkeää tietää lapsen käyttäytymisestä ja mahdollsista ongelmista siihen liittyen, se ei oikeuta suoranaisesti katsomaan lapsen viestejä. Vanhempien on arvioitava, miten omaksua uutta ja päivittyvää tietoa lasten verkkomaailmasta, jotta he onnistuisivat suojaamaan lapsensa yksityisyyttä sosiaalisen median palveluissa.Yleinen kehotus onkin aktiivinen keskustelu vanhemman ja lapsen välillä siitä, mitä viestit pitävät sisällään esimerkiksi lähiajan tapahtumista tai muusta olennaisesta vanhemmalle kuuluvasta seikasta. (Honka 2017; Lastensuojelun keskusliitto 2016, 3)

Lapsen viestien lukeminen ei ole varsinaisesti ristiriidassa perustuslain kanssa, sillä kyseessä on yksilön turvallisuuteen liittyvä asia. Tällaisissa tapauksissa sääntelyn tulisi kuitenkin olla riittävän täsmällistä ja tarkkarajaista, jotta perusoikeuteen puuttumista voitaisiin pitää sallittuna. Lähtökohtana on kuitenkin aina pidettävä lapsen etua. (Forss 2014, 32-33)

2.2 Henkilötietosuoja

Henkilötietosuojaa voidaan pitää yhtenä yksityiselämän suojan sovellutuksena. Henkilötiedoilla tarkoitetaan luonnollista henkilöä tai hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, josta hänet voidaan tunnistaa. Sähköisessä viestinnässä ja siten myös sosiaalisessa mediassa henkilötiedoiksi luokitellaan muun muassa asiakastiedot, tunnistamistiedot ja järjestelmiin tallentuneet sähköiset jäljet eli lokitiedot. Henkilötietojen suojaa toteutetaan tietosuojalainsäädännöllä. Henkilötietojen suojalla tarkoitetaan yksilön, hänen yksityisyytensä ja tiedollisen määräämisoikeutensa suojaamista

tietosuojalainsäädännön avulla. (Koskinen ym. 2012, 41; Innanen & Saarimäki 2012, 87)

Tavallisimmat sähköisessä viestinnässä käytettävät henkilötiedot ovat nimi, sähköpostiosoite ja puhelinnumero. Useilla sivustoilla rekisteröityminen vaatii henkilötietojen täyttämistä. Henkilötietojen luovuttamista edellyttävät myös monet pikaviestisovellukset, sosiaalisen median yhteisöpalvelut sekä verkkokaupat. Henkilötietojen kerääminen, tallettaminen, järjestäminen, käyttö, siirtäminen, luovuttaminen, säilyttäminen, muuttaminen, yhdistäminen, suojaaminen, poistaminen, tuhoaminen ja muut henkilötietoihin kohdistuvat toimenpiteet luetaan henkilötietojen käsittelyksi. (Innanen & Saarimäki 2012, 87)

Euroopan parlamentin ja neuvoston asetuksen, EU 2016/679 (26):n mukaan tietosuojaperiaatteita tulee soveltaa tietoihin, jotka koskevat tunnistettavissa olevaa tai tunnistettua luonnollista henkilöä. Sosiaalisessa mediassa henkilö on useimmiten tunnistettavissa hänen itsensä antamien tietojen perusteella. Asetuksen mukaan ”luonnolliset henkilöt voidaan yhdistää heidän käyttämiensä laitteiden, sovellusten, työkalujen ja protokollien verkkotunnistetietoihin”. Tällöin käyttäjästä voi jäädä jälkiä, joita voidaan käyttää henkilöiden tunnistamiseen ja profilointiin etenkin, kun niitä yhdistetään yksilöllisempiin tunnistetietoihin sekä muihin palvelimelle toimitettuihin tietoihin. (EU 2016/679)

Yleensä henkilön sosiaalisessa mediassa oleva profiili on luotu hänen henkilökohtaisiin tarkoituksiinsa, minkä vuoksi profiilissa tapahtuva henkilötietojen käsittely ei ole aikanaan sisällytetty nyt kumotun henkilötietolain säännöksiin. Henkilökohtaisiin tarkoituksiin perustuva henkilötietojen käsittely katsotaan tavanomaiseksi käytöksi. Tavanomaisen käytös rajaus on epäselvä ja jatkuvasti muuttuva käsite teknologian kehityksen myötä. Henkilörekisteririkoksina tai -rikkomuksina ei ole katsottu tapauksia, joissa kuva on lisätty sosiaaliseen mediaan ilman kuvassa esiintyvän lupaa. (Forss 2015, 28)

2.3 Sähköisen viestinnän tietoturva ja viestien suojaaminen

Suomen lainsäädännössä ei ole määritelty ylläpitovastuuta, jossa tietyn palvelun tai profilin ylläpitäjällä olisi velvollisuus valvoa viestiliikenteen laillisuutta. Isoilla keskustelupalstoilla valvonta olisi lähes mahdotonta. Asia on ongelmallinen myös sananvapauden kannalta. (Forss 2014, 20)

Perustuslakivaliokunnan mietinnössä 14/2002 vp on lausuttu seuraavaa: ”Palstan ylläpitäjän rikosoikeudellinen vastuu voi tulla arvioitavaksi, jos tämä esimerkiksi sallii palstan muodostuvan rikollisten viestien julkaisukanavaksi.” Lausuntoihin on myös kirjattu valiokunnan pitävän merkityksellisenä sitä, että portaalien ja keskustelupalstojen ylläpitäjät seuraavat viestintäliikennettä sivustoillaan. (Perustuslakivaliokunnan mietintö 14/2002 vp, 5)

Sähköisen viestinnän tietoturvaa ja viestien suojaamista ei tueta tavallisessa sähköpostiliikenteessä. Lähtökohtaisesti sähköpostiviestit ovat salaamattomia ja niihin voidaan päästä käsiksi esimerkiksi verkkoliikennettä salakuuntelemalla. Vastuu sähköpostiliikenteessä on siis lähes aina lähettäjällä eli yksityishenkilöllä. Nykyään on kuitenkin saatavilla sähköpostin salauspalveluita, joita tarjotaan erityisesti yrityksille, joiden sähköpostiliikenteen sisältö on suurissa osin arkaluontoista tai henkilötietoja käsittelevää. Salauspalvelun avulla sähköpostiviesti voidaan lähettää salakirjoitetussa muodossa, jolloin ainoastaan viestin vastaanottaja pystyy sen avaamaan. (Viljanen 2013-2018)

Lähes kaikesta sähköisestä viestinnästä jää jälki, jota on hyvin hankalaa tai jopa mahdotonta poistaa. Yksityiselämän suojan ja luottamuksellisen viestinnän toteuttaminen sosiaalisen median maailmassa onkin erityisen hankalaa, sillä digitaalijäljet voivat olla uhkana jopa henkilön identiteetille. Sovellusten suunnitteluvaiheessa tuleekin kiinnitää erityistä huomiota luottamuksellisen viestinnän turvaamiseen sekä yksityiselämän suojan toteutumiseen. Yksityishenkilön vastuulla puolestaan on kiinnittää huomiota sovelluksen turvallisuusseikkoihin heti palvelun käyttöönottovaiheessa. (Innanen & Saarimäki 2012, 14)

2.4 Sosiaalinen media

Sosiaalinen media voidaan määritellä hyvin monella eri tavalla. Medialla tarkoitetaan pääsääntöisesti joukkoviestintää ja joukkoviestimiä. Sosiaalisuudella puolestaan tarkoitetaan viestimien yhteisöllisyyttä ja niin sanottua kollektiivista osallisuutta. Sosiaalinen media on siis Internetin palveluiden ja sovellusten luoma kokonaisuus, jossa merkittävänä osana on käyttäjien välinen kommunikaatio ja sisällön tuottaminen. Sosiaalisessa mediassa käyttäjät eivät ole ainoastaan vastaanottajan roolissa, vaan he voivat myös tuottaa materiaalia itse: kommentoida, tutustua, jakaa mielipiteitä ja sisältöä sekä verkostoitua. Sosiaalisessa mediassa tapahtuva toiminta lisää muun muassa sosiaalisuutta ja yhteisöllisyyttä. (Pesonen 2013, 21; Hintikka 2019)

Sosiaalisen median käyttäjä voi avata verkkoviestintäympäristössä käyttäjätilin ja luovuttaa henkilötietojaan ylläpitääkseen yksilöityä profiilisivua. Viestintä sosiaalisen median palveluissa voi tapahtua kahden henkilön välillä, mutta usein palvelussa tapahtuu viestintää useiden viestijöiden kesken niin sanottuna ryhmäkeskusteluna. Sosiaalisessa mediassa jaetut viestit ovat julkisessa tai yleisessä viestintäverkossa yleisölle suunnattuja sanomia, joihin myös muut voivat ottaa kantaa. (Pesonen 2013, 22)

Suurin osa sosiaalisen median palveluista on maksuttomia ja helppokäyttöisiä työvälineitä erilaisten sisältöjen tuottamiselle. Internetin keinotekoista ja virtuaalista todellisuutta asuttaa kasvava määrä suomalaisia, jotka omaksuvat itselleen niin sanottuja digitaalisia minuuksia. Ihmisen digitaalinen persoona jättää jälkensä rekisteriin talletetuista tiedoista sekä hänen itsensä jälkeen jättämistä sähköisistä jäljistä. (Heinonen 2001, 13)

Sosiaalisella medialla on katsottu olevan suora vaikutus ihmisten käyttäytymiseen, yhteiskuntaan, kulttuuriin, politiikkaan ja talouteen. Sosiaalinen media on helpottanut kansalaisten sosiaalista kanssakäymistä ja tuonut eri medioiden tuottajat ja sisällöt lähelle käyttäjää. ”Joukkotiedotus, markkinointi ja yksilöiden välinen viestintä ovat tavoitettavissa samalla foorumilla.” (Pesonen 2013, 22)

Sosiaalisen median käyttäjiä voivat olla yksityishenkilöiden lisäksi yritykset, yhteisöt ja jopa viranomaiset, jotka käyttävät sosiaalista mediaa viestinnän lisäksi markkinointiin ja erilaisiin käyttäjien toiminnanseuraamismenetelmiin. Informaatiota syötetään yhteisösivustojen seuraajille, jotka tykkäävät ja mahdollisesti myös jakavat tietoa markkinointimielessä eteenpäin. Tykkääjien lukumäärä puolestaan kertoo brändin, tuotteen tai palvelun herättämästä kiinnostuksesta. (Pesonen 2013, 25)

Internetiä ja sosiaalista mediaa ei hallinnoi mikään yksittäinen taho eikä sosiaaliselle medialle ole varsinaista kirjoitettua lainsäädäntöä. Sähköisen viestinnän lainsäädäntö, jota voidaan soveltaa myös sosiaaliseen viestintään, on hajautettu lukemattomiin eri lakeihin. Yleisesti sosiaalisessa mediassa tapahtuvaan sähköiseen viestintään liittyvät oikeudet ja velvollisuudet on osoitettu lainsäädännössä toimijan roolin mukaan, ei itse toiminnan mukaan. Keskeistä on myös tieto siitä, millaisia käsiteltävät asiat ovat. Merkittävää on, käsitelläänkö viesteissä tai muussa sosiaalisen median materian tuotoksessa henkilö-, tunniste- tai paikkatietoja. Käsiteltävien tietojen laatu määrittelee toimijan velvollisuudet ja tietojen käsittelyn perusteet sosiaalisessa mediassa. On myös huomioitava, millaisia reunaehtoja palvelun erityispiirteet asettavat palvelun tarjoajalle. (Innanen & Saarimäki 2012. s. 2,7, 37)

Ihmisten käyttäytymistä sosiaalisessa mediassa määrittelee osaltaan tapakulttuuri. Se sanelee ehdot sille, mikä on soveliasta, mikä sopimatonta, mistä voidaan puhua julkisesti tai mitä voidaan näyttää muille. Tämän päivän sosiaalisen median sisältö on hyvin avointa ja vapaata, jolloin se omaksutaan helposti osana tapakulttuuria. Kun tapakulttuuri on avoin ja säätelemätön, ihmisten on yhä helpompi tarttua sosiaalisen median kautta myös niihin asioihin, jotka eivät välttämättä sinne kuulu. (Kulla ym. 2002, 17)

Käytettäessä sosiaalisen median palveluita, henkilöjen on noudatettava kansainvälisiä ihmisoikeussopimuksia: Yhdistyneiden kansakuntien kansalais- ja poliittisia oikeuksia koskeva yleissopimus SopS 8/1976 ja Euroopan neuvoston ihmisoikeussopimus (SopS 18-19/1990). Kansainvälisiä ihmisoikeussopimuksia

tulee noudattaa myös sosiaaliseen mediaan liittyviä lakeja säädettäessä. (Pesonen 2013, 45)

3 YKSITYISYYDEN SUOJAA KOSKEVA KESKEINEN LAINSÄÄDÄNTÖ

Tässä luvussa käsitellään riskejä, lainalaisuuksia sekä tulevaisuuden tuomia muutoksia. Sosiaalisessa mediassa tapahtuvan viestinnän monipuolisuus ja kehittyneisyys voivat asettaa tietynlaisia haasteita tilanteissa, joissa tulisi soveltaa asianmukaista lainsäädäntöä.

3.1 Perustuslaki

Suomen perustuslaki turvaa jokaiselle suojan yksityiselämään, kunniaan ja kotirauhaan. Perustuslain mukaan myös kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton. (L 11.6.1997/731, 10 §)

On vaikea määritellä, mitä yksityiselämän piiriin kuuluu. Laaja-alaisesti katsoen yksilöllä on oikeus solmia ja ylläpitää vapaasti suhteita muihin ihmisiin sekä ympäristöön ja oikeus määrätä itsestään ja omasta ruumiistaan. Yksityiselämän suojaamisen piiriin kuuluvat myös yksilön oikeusturva ja yksityisyyden suoja henkilötietojen käsittelyssä. (Innanen & Saarimäki 2012, 13)

Perustuslaissa säädetyn yksityiselämän suojan osa-alueita sähköisessä viestinnässä ovat erityisesti henkilötietojen suoja ja henkilön oikeus luottamukselliseen viestintään. Tähän piiriin kuuluu myös paikkatietojen suoja, joka on hyvin hauras sosiaalisen median maailmassa, sillä suurin osa applikaatioista ja sosiaalisen median sovelluksista vaatii käyttäjän hyväksynnän paikkatietojen jakamiselle sovelluksen toimivuuden varmistamiseksi. (Innanen & Saarimäki 2012, 14)

Paikkatieto ilmaisee päätelaitteen tai liittymän maantieteellisen sijainnin. Useimmissa tapauksissa päätelaitteena toimii puhelin, joka on henkilön hallussa ja joka päivittää jatkuvaa dataa järjestelmän ylläpitäjälle käyttäjän ajantasaisesta sijainnista. Paikantaminen voidaan katsoa yksityiselämän suojaan puuttumiseksi ja paikkatietojen käsittely taas perustuslaissa turvattuun liikkumisvapauteen puuttumiseksi. Näihin sovelluksen käyttäjä antaa kuitenkin useimmiten itse luvan käyttöehtojen hyväksymisen yhteydessä. (Innanen & Saarimäki 2012, 30)

Perustuslaki säätelee suojan viestisalaisuudelle, mikä käsittää myös sosiaalisen median kautta tapahtuvan sähköisen viestinnän. Perustuslaki säätää myös kansalaisten oikeuden sananvapauteen, johon sisältyy oikeus ilmaista, julkistaa ja vastaanottaa tietoja, mielipiteitä ja muita viestejä kenenkään ennakolta estämättä. (L 11.6.1999, 12 §)

Sananvapaudella tarkoitetaan oikeutta ilmaista, julkistaa ja vastaanottaa tietoja, mielipiteitä ja muita viestejä kenenkään estämättä. Sananvapaus käsittää myös mielipidevapauden ja vapauden vastaanottaa ja levittää tietoja ja ajatuksia. Haasteellista on tietää, millaisen toiminnan katsotaan olevan tietojen levittämistä. Jokaisen yksilön henkilötietojen tulisi olla turvattu, mutta lukemattomia ovat ne uutiset ja julkaisut, joissa puhutaan henkilöistä nimillä ja mahdollisesti jopa laajemmilla henkilötiedoilla. Tällainen menettely korostuu usein esimerkiksi ajankohtaisissa, poliittisista keskustelua herättävissä kannanotoissa tai uutiskynnyksen ylittävissä yhteiskunnallisissa keskustelunaiheissa. Sosiaalisessa mediassa juuri henkilöistä nimillä puhuminen yleisön nähtäville jaetuissa julkaisuissa ja keskusteluissa on varsin yleistä. (Innanen & Saarimäki 2012, 18)

3.2 Tietosuojalaki

Tietosuoja on yksilön yksityisyyden ja luottamuksen turvaamista. Se on yksilön perusoikeus ja rinnastettavissa perustuslaissa turvattuun kotirauhaan. Tietosuojalla tarkoitetaan henkilötietojen käsittelyä, mikä perustuu aina lakiin, jota valvoo riippumaton viranomainen. Yksi tietosuojan toteuttamisen keino onkin tietoturva, jolla suojataan tietoaineistoja ja tietojärjestelmiä. (Tietosuojavaltuutetun toimisto 2019; OpiTietosuojaa.fi 2016)

Tietosuojalain tehtävä on täsmentää ja täydentää henkilötietojen käsittelystä annettua Euroopan parlamentin ja neuvoston asetusta. Vaikka sosiaalisen median varsinainen tarkoitus ei olekaan henkilötietojen käsittely, on sen osuus huomattavan suuri, kun tarkastellaan sosiaalisen median käyttäjien itsestään jakamien tietojen sisältöä. (L 5.12.2018/1050, 1 §)

Tietosuojalain 4 §:ssä säädetään henkilötietojen käsittelyn lainmukaisuudesta. Pykälän 1 momentin mukaan henkilötietoja saa käsitellä tietosuoja-asetuksen 6 artiklan 1 kohdan alakohdan mukaisesti, jos kysymys on henkilön asemaa, tehtäviä sekä niiden hoitoa julkisyhteisössä, elinkeinoelämässä, järjestötoiminnassa tai muussa vastaavassa toiminnassa kuvaavista tiedoista. Näin kuitenkin vain siltä osin, kuin käsittelyn tavoite on yleisen edun mukainen ja käsittely on oikeasuhtaista sillä tavoiteltuun oikeutettuun päämäärään nähden. (L 5.12.2018/1050, 4 §)

3.3 EU:n tietosuoja-asetus

Euroopan unioni on säätänyt direktiivejä, jotka vahvistavat muun muassa yksityiselämän suojaa. Direktiiveillä täsmennetään viestinnän suojaa, rekisteröidyn henkilötietojen suojaa, määritellään oikeuksien sisältöä sekä jäsenmaisen velvoitteita ja menettelytapoja. Keskeisiä sosiaalisen median kannalta ovat tietosuojadirektiivit, erityisesti sähköisen viestinnän tietosuojadirektiivit. Direktiivien velvoitteet on otettava huomioon kansallisessa lainsäädännössä kaikissa EU-jäsenvaltioissa. Viestintään liittyvän perus- ja ihmisoikeusjärjestelmän lähteinä toimivat kansallinen lainsäädäntö, EU-oikeus sekä kansainväliset sopimusvelvoitteet. (Pesonen 2013, 59)

Euroopan parlamentin ja neuvoston tietosuojadirektiivissä, EPNDir 2002/58/EY:ssä pyritään kunnioittamaan perusoikeuksia ja Euroopan unionin perusoikeuskirjassa tunnustettuja periaatteita. Euroopan parlamentti ja Euroopan unionin neuvosto ovat katsoneet muun muassa seuraavaa:

> *”Yhteisön yleisissä viestintäverkoissa ollaan parhaillaan ottamassa käyttöön kehittynyttä digitaaliteknologiaa, mikä asettaa käyttäjien henkilötietojen ja yksityisyyden suojaa koskevia erityisvaatimuksia. Uusien sähköisten viestintäpalvelujen käyttöönotto on luonteenomaista tietoyhteiskunnan kehittymiselle. Suurella yleisöllä on nykyisin mahdollisuus ja varaa käyttää digitaalisia matkaviestinverkkoja. Näillä digitaalisilla verkoilla on suuri kapasiteetti ja mahdollisuudet henkilötietojen käsittelyyn. Näiden palvelujen kansainvälisen kehittämisen onnistuminen riippuu osittain siitä, että käyttäjät luottavat siihen, ettei heidän yksityisyytensä ole vaarassa.” (EPNDir 2002/58/EY, (5))*

Euroopan parlamentin ja neuvoston tietosuojadirektiivi säätää myös viestinnän luottamuksellisuudesta 5 artiklassa, jonka mukaan jäsenvaltioiden tulee varmistaa kansallisella lainsäädännöllä yleisen viestintäverkon ja sähköisten viestintäpalvelujen välityksellä tapahtuvan viestinnän luottamuksellisuus. Jäsenvaltioiden lainsäädännön tulee kieltää viestinnän kuuntelu, salakuuntelu, tallennus tai muu viestinnän sieppaus tai valvonta, mikäli siihen ei ole käyttäjän nimenomaista suostumusta tai mikäli se ei ole laillisesti sallittua 15 artiklan 1 kohdan mukaisesti. Säädös ei kuitenkaan estä sellaista teknistä tallentamisesta, joka on välttämätöntä viestin välittämiselle, rajoittamatta kuitenkaan luottamuksellisuuden periaatteen soveltamista. (EPNDir 2002/58/EY, 5 artikla)

3.4 EU:n yleinen tietosuoja-asetus GDPR

Uusimpana henkilötietojen käsittelyä koskevana lakina on keväällä 2016 Euroopan parlamentin ja neuvoston päätöksillä hyväksytty EU:n yleinen tietosuoja-asetus eli GDPR (General Data Protection Regulation), joka tuli sovellettaviksi kaikkiin EU-maihin toukokuussa 2018. GDPR:n tavoitteena on vahvistaa yksilön oikeuksia ja vapauksia, lujittaa sisämarkkinaulottuvuutta ja huomioida tietosuojan globaalia ulottuvuutta. Lisäksi asetus tehostaa tietosuojasääntöjen täytäntöönpanon valvontaa sekä parantaa luottamusta online-palveluihin. Asetuksessa on kyse luonnollisen henkilön oikeudesta henkilötietojen suojaan sekä henkilötietojen vapaan liikkuvuuden takaamisesta EU-alueen sisällä. (Opitietosuojaa.fi 2018; Elinkeinoelämän keskusliitto 2018)

EU:n yleisen tietosuoja-asetuksen, GDPR:n mukaan henkilötietojen käsittely on mahdollista seuraavan kuuden eri perusteen mukaan:

1) rekisteröidyn suostumus

2) sopimus

3) rekisterinpitäjän lakisääteinen velvoite

4) elintärkeiden etujen suojaaminen

5) yleistä etua koskeva tehtävä tai julkinen valta

6) rekisterinpitäjän tai kolmannen osapuolen oikeutettu etu.

Henkilötietojen tulee olla asianmukaisia ja olennaisia niihin tarkoituksiin, joita varten niitä kerätään ja käsitellään. Henkilötietojen tulee olla myös täsmällisiä ja ajantasaisia ja niitä tulee säilyttää sellaisessa muodossa, josta rekisteröity on tunnistettavissa niin kauan kuin on tarpeen. Henkilötietoja tulee käsitellä niin, että niiden asianmukainen turvallisuus säilyy. Virheelliset henkilötiedot on poistettava ja oikaistava. (Tietosuojamalli 2017)

Kuten laki sähköisen viestinnän palveluista, myös GDPR säätää tietojenkäsittelyn perustumisesta suostumukseen. Rekisterinpitäjän tulee osoittaa, että rekisteröity on antanut suostumuksensa henkilötietojensa käsittelyyn. Sosiaalisen median palveluissa tämä on rinnastettavissa palvelun tarjoajan käyttöehtoihin. Facebookin tarjoaman Instagram -palvelun tietokäytännössä mainitaan muun muassa seuraavaa: ”Palvelumme tarjoaminen edellyttää tietojesi keräämistä ja käyttämistä”. (Tietosuojamalli 2017; Instagram 2019)

Mikäli tietojenkäsittely perustuu suostumukseen, on GDPR:n mukaan rekisterinpitäjän pystyttävä osoittamaan, että rekisteröity on antanut suostumuksen henkilötietojensa käsittelyyn. Suostumuksen antamista koskevan pyynnön on oltava erillään muista asioista, jotta se on helposti ymmärrettävissä ja saatavilla olevassa muodossa. Rekisteröity, eli yksityishenkilö, voi peruuttaa suostumuksensa koska tahansa ja peruuttamisen on oltava yhtä helppoa kuin sen antaminenkin. Kun arvioidaan suostumuksen vapaaehtoisuutta, on otettava huomioon, onko palvelun tarjoamisen tai muun sopimuksen täytäntöönpanon ehdoksi asetettu suostumus sellaisten henkilötietojen käsittelyä varten, jotka eivät ole tarpeen sopimuksen täytäntöönpanoa varten. (Tietosuojamalli 2017)

Sosiaalisen median yhteisöpalvelu Facebook määrittää tietokäytännöissään, miten se käsittelee ihmisten henkilökohtaisia tietoja. Facebook business -sivuston mukaan tietojen suojaaminen on erittäin tärkeää Facebook-yrityksille. EU:n

tietosuojalain ja yleisen tietosuoja-asetuksen noudattamiseksi muun muassa Faebook on sitoutunut kolmeen niin sanottuun arvoon:

1. läpinäkyyys

2. hallinta

3. vastuullisuus.

Yksityishenkilön kannalta läpinäkyvyydellä tarkoitetaan muun muassa ilmoituksia ja kuluttajien opetusohjelmia, joiden tehtävä on auttaa käyttäjiä ymmärtämään, miten heidän tietojaan käytetään ja millaisia vaihtoehtoja käyttäjillä on tietojensa suojaamiseksi. Hallinnalla puolestaan tarkoitetaan käyttäjien mahdollisuutta hallita omia tietojaan hallintakeskuksen kautta. Hallintakeskuksessa käyttäjä pääsee päivittämään omia yksityisasetuksiaan ja täten vaikuttamaan omaan someturvallisuuteensa. (Facebook 2019)

Osa hallintaa on esimerkiksi käyttäjätietojen siirtämisen salliminen erilaisille Facebook -sovelluksille. Tällaisissa tilanteissa käyttäjä asettaa itsensä riskialttiiksi sille, että hänen käyttäjätietojaan siirretään ulos palvelusta. Tämä puolestaan antaa yrityksille lukemattomia mahdollisuuksia muun muassa kohdennettuun markkinointiin. Vuotaneita tietoja on lähes mahdotonta saada takaisin. Käyttäjä voi ainoastaan ennaltaehkäistä tietojensa leviämisen esimerkiksi poistamalla Facebookia käyttävät ylimääräiset sovellukset, rajoittamalla julkaisujensa näkyvyyttä palvelussa sekä rajoittamalla palvelimelle antamiaan henkilötietoja ja muita yksilöiviä tietojaan. (Euroopan Unioni 2019)

Vastuullisuus käsittää Facebookin yksityisyysperiaatteet, joihin koko tietosuojakäytäntö yhteisöpalvelussa perustuu. Vastuullisuudesta huolehtii tietosuojatiimi eikä täten yksityishenkilöllä ole osa-alueeseen juurikaan vaikutusmahdollisuuksia. Facebookin tietosuojatiimi varmistaa, että palvelu dokumentoi määräysten mukaisesti. Tiimi myös tapaa säännöllisesti säädösten tekijöitä ja yksityisyyden asiantuntijoita sekä akateemikkoja ympäri maailman saadakseen palautetta ja parantaakseen käyttäjien henkilökohtaisten tietojen suojaamistapoja. (Facebook 2019)

3.5 Euroopan parlamentin ja neuvoston asetus

Luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä säätää Euroopan parlamentin ja neuvoston asetus EPNA (EU) 2016/679. Sen mukaan luonnollisten henkilöiden suojelun katsotaan olevan perusoikeus henkilötietojen käsittelyn yhteydessä. ”Euroopan unionin perusoikeuskirjan 8 artiklan 1 kohdan sekä Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT) 16 artiklan 1 kohdan mukaan jokaisella on oikeus henkilötietojensa suojaan.” (EU 2016/679, (1))

Asetuksen mukaan jokaisella tulisi olla oikeus henkilötietojen suojaan kansalaisuudesta ja asuinpaikasta riippumatta. Asetuksen tarkoituksena on tukea muun muassa vapauden ja turvallisuuden edistämistä. Tämän lisäksi se kehittää sosiaalista edistystä ja luonnollisten henkilöiden hyvinvointia. Henkilötietojen käsittelyn tulisi palvella ihmistä ja sitä tulisi tarkastella suhteessa sen tehtävään yhteiskunnassa. Sen on myös oltava oikeassa suhteessa muihin perusoikeuksiin suhteellisuusperiaatteen mukaisesti. EU:n 2016/679 asetuksessa

> *”kunnioitetaan kaikkia perusoikeuksia ja huomioidaan tunnustetut vapaudet ja periaatteet sellaisina kuin ne ovat vahvistettuina perussopimuksissa, erityisesti jokaisen oikeus siihen, että hänen yksityis- ja perhe-elämäänsä, kotiaan sekä viestejään kunnioitetaan, oikeus henkilötietojen suojaan, ajatuksen, omantunnon ja uskonnon vapaus, sananvapaus ja tiedonvälityksen vapaus, elinkeinovapaus, oikeus tehokkaisiin oikeussuojakeinoihin ja oikeudenmukaiseen oikeudenkäyntiin sekä oikeus kulttuuriseen, uskonnolliseen ja kielelliseen monimuotoisuuteen.” (EU 2016/679, (2),(4))*

Henkilötietojen suojeluun uusia haasteita ovat tuoneet mun muassa teknologian nopea kehitys ja globalisaatio. Tietokoneet ovat mahdollistaneet suurten tietomäärien käsittelyn ja tallentamisen. Henkilötietojen jakaminen ja kerääminen on kasvanut merkittävästi. Teknologia on mahdollistanut niin yksityisille, yrityksille ja viranomaisille henkilötietojen kattavan käytön jopa maailmanlaajuisesti. Tulevaisuudessa teknologia tulee helpottamaan yhä enemmän henkilötietojen vapaata kulkua unionissa sekä tiedon siirtoa kolmansiin

maihin ja kansainvälisille järjestöille. Teknologia vastaa myös henkilötietojen korkeatasoisesta suojasta. Teknologian kehityksellä on kuitenkin myös varjopuolensa: lisääntyneet rikollisuuden muodot. Tietotekniikkaan liittyvät rikokset voivat aiheuttaa yksityishenkilöille tai organisaatioille suuria taloudellisia vahinkoja ja ihmisten turvallisuutta uhkaavia tilanteita. (EU 2016/679, (6); Kalliojärvi 2016, 16)

3.6 Käyttöehdot

Sosiaalisen median palveluun kirjautumisessa on kyse niin sanotusta palvelussuhteen luomisesta. Oikeudellisesti katsoen kyse on rekisteröintisuhteesta ja henkilötietojen käsittelystä, sillä useimmissa palveluissa edellytetään henkilötietojen luovuttamista palveluntarjoajalle sovelluksen käytön varmistamiseksi. Tämän lisäksi käyttäjä tarvitsee tietoliikenneyhteyttä sekä viestintävälineitä, jolloin käyttäjällä on oltava hallussaan yhteys tietoverkon ylläpitoon. (Pesonen 2013, 133)

Käyttöehtojen tehtävä on luoda oikeuksia ja velvollisuuksia molemmille sopimusosapuolille. Lähtökohtaisesti palvelun tarjoajan on määriteltävä käyttöehdoissa, mikäli tämä vaatii itselleen joitakin käyttäjän aineistoon liittyviä oikeuksia itselleen, tai mikäli käyttäjän oikeuksia rajoitetaan palvelussa jollain tavalla. Erityisesti tietoverkossa tarjottavien palvelujen käyttöehdoissa on tärkeää määritellä, missä laajuudessa käyttäjän käyttöoikeudet linsensoidaan palvelun ylläpitäjälle. (Voutilainen & Galkin 2017, 17)

Yhteisöpalvelu Facebook sekä kuvien jakopalvelu ja sosiaalinen verkosto Instagram ovat esittäneet sivustollaan yhteisösäännöt koskien molempien palveluiden käyttöä. Sääntöjen mukaan käyttäjä saa jakaa vain sellaisia kuvia ja videoita, joihin käyttäjällä itsellään on oikeus. Sisältö, jonka käyttäjä julkaisee tilillään, on käyttäjän omistama. Sisällön on oltava aitoa, luvallista ja sellaista, mikä sopii monimuotoiselle yleisölle. Yhteisösääntöjen mukaan käyttäjien tulee toimia mielekkäällä ja aidolla tavalla sekä noudattaa lakia. Sääntöjen mukaan ”Instagram ei ole paikka, jossa tuetaan tai ylistetään terrorismia, järjestäytynyttä rikollisuutta tai viharyhmiä”. Myös seksuaalisen sisällön jakaminen ja lapsiin

kohdistuva alastomuus ja seksistinen lähestyminen ovat kiellettyjä. Säännöt kehottavat kunnioittamaan muita yhteisön jäseniä ja pitämään yllä tukea antavaa ympäristöä. Ne myös muistuttavat harkinnanvaraisuudesta etenkin uutiskynnyksen ylittävien tapausten osalta. (Instagram 2019)

Kuvien jakopalvelu Instagramin käyttäjille kohdistetut yhteisösäännöt kehottavat käyttäjiä ylläpitämään vahvaa yhteisöä ja ilmoittamaan, mikäli käyttäjä löytää palvelun sisällöstä jotakin sinne kuulumatonta. Palveluissa on käytössä myös sisäinen ilmiantovaihtoehto, jolloin käyttäjällä on mahdollisuus ilmiantaa sellaiset tilanteet, joissa rikotaan palveluntarjoajan asettamia sääntöjä. (Instagram 2019)

Esimerkillisen ilmiselvä yhteisösääntöjen vastainen teko ilmenee Pohjanmaan käräjäoikeuden ratkaisusta 19/116441, jossa vastaaja A on tuomittu sakkoihin muun muassa kunnianloukkauksesta. Tapauksessa A on esittänyt valheellisen tiedon 13-vuotiaasta B:stä julkaisemalla hänestä kuvan Facebookin suljetussa ryhmässä. Kuvan yhteydessä A on jakanut tekstin: ”Yksittäiskuva nuoresta pojasta, joka teki tappouhkauksia, kun pyydettiin poistumaan ja lopettamaan pahan teko.” Tekstissä esitetty väite tappouhkauksista ei ole pitänyt paikkansa. Syyttäjä on ehdottanut myös vaihtoehtoista syytettä yksityisyselämää loukkaavan tiedon levittämisestä. (KO:19/116441)

Tapauksessa asianomistaja B on ollut toistuvasti viettämättässä aikaa ystäviensä kanssa useilla julkisilla paikoilla, joista heitä oli pyydetty poistumaan. A oli ottanut tällaisesta tilanteesta kuvan tavoiteenaan saada mahdollisimman moni henkilöistä mahtumaan kuvaan. A oli julkaissut kuvan Facebook -ryhmään siinä toivossa, että kuva tavoittaisi B:n ja tämän ystävien vanhemmat. A on myöntänyt julkaisseensa kuvan ryhmään, jossa kuva oli ollut noin kaksi päivää. Asiassa ei esitetty selvitystä Facebook -ryhmän koosta, mutta julkaisu oli tavoittanut lukuisia henkilöitä. Julkaistusta lähikuvasta oli erotettavissa B:n kasvot. Lopulta A oli poistanut julkaisun. (KO:19/116441)

Tapaus osoittaa, että palvelun käyttöehtojen rikkomisen lisäksi tulee monissa tapauksissa sovellettavaksi myös rikoslaki, kun teko täyttää rikoslain tekotapatunnusmerkistön. Rikoslain 24 luvun 9 §:n mukaan kunnianloukkauksesta

tuomitaan se, joka esittää toisesta valheellisen tiedon tai vihjauksen siten, että teko on omiaan aiheuttamaan vahinkoa tai kärsimystä loukatulla taikka häneen kohdistuvaa väkivaltaa. Toissijaisesti vaaditusta yksityiselämää loukkaavasta tiedon levittämisestä puolestaan säädetään rikoslain 24 luvun 8 §:ssä seuraavasti: ”joka oikeudettomasti joukkotiedotusvälinettä käyttämällä tai muuten toimittamalla lukuisten ihmisten saataville estittää toisen yksityiselämästä tiedon, vihjauksen tai kuvan siten, että teko on omiaan aiheuttamaan vahinkoa tai kärsimystä loukatulla taikka häneen kohdistuvaa väkivaltaa.” (L 13.12.203/879, 8-9 §)

3.7 Laki sähköisen viestinnän palveluista

Sosiaalisen median rinnalla koko sähköisen viestinnän yksi ongelmakohdista on vaikeaselkoinen lainsäädäntö. Erityisesti sähköisen viestinnän sääntely koskee hyvin laajaa käyttäjäkuntaa, jolloin myös sen sääntelyltä voidaan edellyttää erityistä selkeyttä ja ymmärrettävyyttä. Sosiaalinen media käsittää nykyään valtaosan sähköisen viestinnän palveluista, jolloin siihen voidaan kohdistaa myös samoja edellytyksiä. Nopea muutoskehitys, monimutkaistuneet ongelmat sekä lainsäädännön yhteensovittaminen ovat kuitenkin jatkuvassa ristiriidassa tavoitellun selkeyden ja ymmärrettävyyden kanssa. (Innanen & Saarimäki 2012, 31)

Laki sähköisen viestinnän palveluista säätelee reunaehdot sähköisesti tapahtuvalle viestinnälle ja sen palvelutarjonnalle. Lain tehtävä on varmistaa viestintäverkkojen ja viestintäpalvelujen tarjonta kohtuullisin ehdoin koko maan laajuisesti. Radiotaajuuksien tehokas ja häiriötön käyttö, kilpailun sekä viestintäverkkojen ja -palveluiden teknillinen laatu- ja kehitysseuranta pyritään turvaamaan lain nojalla. Lain tavoitteena on myös turvata luottamuksellisuus ja yksityisyyden suojan toteutuminen sähköisessä viestinnässä ja siten myös sosiaalisessa mediassa. (L 7.11.2014/917, 1 §)

Yleinen käsitys on, että Internetissä tapahtuvaan toimintaan sovelletaan samaa lainsäädäntöä kuin niin sanotussa oikeassa maailmassa. Internetissä tapahtuva viestintä on kuitenkin niin monimuotoista ja kehittynyttä, että kaikkiin tilanteisiin

toimivien asetusten ja säädösten löytäminen laisäädännöstä on erityisen hankalaa. (Innanen & Saarimäki 2012, 31)

Konkreettisena esimerkkinä lainsäädännön soveltamisesta voidaan verrata kirjeen tai postipaketin osoite- ja postileimatietojen avulla saatua tunnistamistietoa Internetissä tapahtuvaan tunnistetetojen selvittämiseen. Internetin tunnistamistiedoista pystytään hyvinkin mutkattomasti selvittämään viestinnän osapuolet, ajankohta, sisältö, päätelaitteiden sijainti ja muut oleelliset seikat. Tunnistamistiedot muodostavat siis huomattavasti kattavamman kuvan henkilöiden välisestä viestinnästä, kuin postitse lähetetty kirje. (Innanen & Saarimäki 2012, 32)

Sähköisen viestinnän palveluista säädetyn lain mukaan viestinnän osapuolet voivat käsitellä omia sähköisiä viestejään, jollei laissa toisin säädetä. Viestinnän välittäjät, kuten teleyritykset voivat käsitellä sähköitse tapahtuvaa viestintää ja välitystietoja siinä määrin kuin se on tarpeellista toimivan viestinnän aikaansaamiseksi ja tietoturvasta huolehtimiseksi. Suurin osa sosiaalisen median palveluista tulee kuitenkin ulkomailta ja Kyberturvallisuuskeskuksen valvonta koskee vain tietyin edellytyksin palveluita, joita tarjotaan ulkomailta. (7.11.2014/917, 136 §; Traficomin Kyberturvallisuuskeskus 2019)

Sähköisen viestinnän palveluista annetun lain 17. luvussa säädetään sähköisen viestin ja välitystietojen käsittelystä. Lain 136 §:n mukaan: ”Viestinnän osapuoli voi käsitellä omia sähköisiä viestejään ja niihin liittyviä välitystietoja, jollei laissa toisin säädetä.” Laki koskee radioviestintää, jollaisena voidaan pitää myös sähköistä viestintää sosiaalisessa mediassa. Lain mukaan henkilö, joka on vastaanottanut sellaisen tiedon, joka ei ole hänelle tarkoitettu, ei saa ilmaista tai käyttää hyväksi viestin sisältöä ilman viestinnän osapuolten suostumusta, mikäli laissa ei ole toisin säädetty. (L 7.11.2014/917, 136 §)

Sosiaalisessa mediassa on tyypillistä, että käyttäjät jakavat sijaintitietojaan. Sijaintitietojen käsittely jää silloin palvelimelle, mutta itse käyttäjän vastuulla on niiden alkuperäinen luovuttaminen yleisön nähtäville. Laki sähköisen viestinnän palveluista säätää luvussa 20 sijaintitietojen käsittelystä ja luovuttamisesta

kolmannelle osapuolelle. Lain 160 §:n mukaan sijaintitietoja saa käsitellä lisäarvopalvelun tarjoamiseksi tai hyödyntämiseksi vain, jos käyttäjä on antanut siihen suostumuksensa. Sijaintietoja saa käsitellä vain tilanteen vaatimassa laajuudessa eikä sillä saada rajoittaa henkilön yksityisyyden suojaa enempää kuin on välttämätöntä. Kun sijaintitietojen käsittely on päättynyt, on sijaintitiedot hävitettävä tai tehtävä sellaisiksi, ettei niitä voida mitenkään yhdistää käyttäjään. Lain mukaan henkilö, joka on vastaanottanut sellaisen sijaintitiedon, joka ei ole hänelle tarkoitettu, ei saa ilmaista tai käyttää hyväksi sijaintitietoa tai tietoa sen olemassaolosta ilman viestinnän osapuolen suostumusta, tai mikäli laissa ei ole toisin säädetty. (L 917/2014, 160 §)

3.8 Laki viranomaisten toiminnan julkisuudesta

Julkisuuslaki eli laki viranomaisten toiminnan julkisuudesta säätää viranomaisten asiakirjojen ja muiden tietoaineistojen julkisuudesta ja salassapidosta sekä tiedon jakamisesta liittyvistä menettelyistä. Se sääntelee myös tiedonhallintatavan toteutumisesta viranomaisella, johon kuuluvat myös tietoturvallisuusvaatimukset. Lain mukaan jokaisella on oikeus saada tietoa viranomaisen asiakirjoista, mikäli ne ovat julkisia. Salaiseksi määräämisestä säädetään erikseen. (Oikeusministeriö 2019)

Suomen mediaympäristöä pidetään yhtenä maailman vapaimmista. Avoimuus, sananvapaus sekä yhdenvertaisen kohtelun edistäminen kuuluvat keskeisesti valtionhallinnon toimintaan ja sen luomaan 2016 vuoden viestintäsuositukseen. Viranomaiset hyödyntävät sosiaalista mediaa päivittäin hyvin monipuolisesti, sillä kanavat toimivat hyvin muun muassa asiakaspalvelutyöskentelyssä. Toisinaan viranomaiset voivat käyttää mediaympäristöä ja erityisesti sosiaalista mediaa henkilötietojen hankkimiseksi tai esimerkiksi apuna rikoksen selvittämisessä. Kysymyksiä herättääkin muun muassa se, miten suojatun järjestelmän läpi voi päästä ainoastaan viranomainen eikä yksityishenkilö. (Valtionhallinnon viestintäsuositus 2016)

Julkisuuslain mukaan viranomaisen velvollisuus on edistää tiedonsaantia ja hyvää tiedonhallintatapaa. Viranomaisen tulee huolehtia asiakirjojen, tietojärjestelmien

sekä niihin liittyvien tietojen asianmukaisesta käsittelystä, saatavuudesta ja käytettävyydestä. Usein viranomaiset pääsevät käsittelemään yksityishenkilön henkilötietoja hyvinkin yksityiskohtaisesti. Esimerkiksi rikosten selvittämisessä voidaan käyttää apuna epäillyn sosiaalisen median tilin tutkimista, televalvontaa tai telekuuntelua. Tällaiset tapaukset ovat erityisen salaisia, mutta suuri apu esitutkinnassa voivat olla esimerkiksi juuri sosiaalisen median kautta välitetyt viestit, kuvat tai muut julkaisut. Televalvonnan kohdistamista varten esitutkintaviranomainen tarvitsee virallisen luvan, mikäli epäiltyä on syytä epäillä pakkokeinolaissa määritellyin ehdoin. Esitutkintaviranomainen voi kohdistaa televalvontaa joissakin tapauksissa myös teleosoitteen tai telepäätelaitteen haltijan suostumuksella. (L 25.5.199/621, 18 §; 22.7.2011/806, 6 §, 7§)

4 YKSITYISYYS SOSIAALISEN MEDIAN PALVELUISSA

Tässä luvussa tarkastellaan sosiaalisen median riskejä ja uhkia sekä sitä, millaisia yksityisyyteen liittyviä toimenpiteitä yksilöllä on mahdollista toteuttaa sosiaalisessa mediassa. Luvussa tutkitaan myös, missä menee vastuun raja sivuston ylläpitäjän ja itse sivuston käyttäjän, eli yksityishenkilön välillä.

4.1 Riskit ja uhat sosiaalisessa mediassa

Internet ja sosiaalinen media tarjoavat monia lupauksia, joihin on helppo tarttua. Verkossa tapahtuvat viestintämahdollisuudet kehittyvät ja parantuvat koko ajan ja samalla ne lisäävät ihmisten välistä yhteisöllisyyttä ja ajatusten sekä mielipiteiden leviämistä. Pääsy sosiaalisen median palveluihin on tehty helpoksi ja se on pyritty pitämään vapaana liiallisesta sääntelystä, sensuurista tai muusta kontrollista. (Aula, Matikainen & Villi 2006, 15)

Käyttäjämäärien kasvu, viestinnän moninaisuus ja vapaus sekä kaupallisuus tuovat mahdollisuuksien lisäksi myös haasteita ja uhkia sosiaalisen median käyttäjälle. Sosiaalisen median varjopuolena voivat olla esimerkiksi väkivaltainen tai seksistinen materiaali, rikollisryhmien organisoituminen tai jopa henkirikokselliset tai terroristiset teot. Internetin ja sosiaalisen median haavoittuvuus näkyy myös epidemian tavoin leviävien virusten muodossa. Yksilöä ja yhteiskuntaa uhkaaville viruksille annetaan sekä biologisia että inhimillisiä ominaisuuksia. Virukset tai pikemminkin niiden takana olevat henkilöt väijyvät, kuuntelevat, keskustelevat ja pahimmassa tapauksessa jopa ohjaavat yksilön toimintaa oman edun tavoittamiseksi. (Aula ym. 2006, 15)

Sosiaalisen median helppous, avoimuus ja kansalaisen perusoikeuksiin kuuluva sananvapaus tuottavat toisinaan ongelmia koskien käyttäjien jakamia julkaisuja. Käyttäjien tulisikin varmistua siitä, ettei jaettava kuva, teksti tai tai muu tieto ole jaetussa materiaalissa esiintyvälle tai muulla tavoin toiselle asianosaiselle ongelma. Käyttäjän jakama kommentti, kuva tai muu sisältö voi muuttaa totaalisesti alkuperäismerkitystään, kun se esitetään uudessa yhteydessä ja

käytäjäprofiilista irrotettuna. Sosiaalisen median uhka voi siis löytyä jopa lähipiiristä. (Vantaan sanomat 2016; Pesonen 2013, 39)

Toisinaan avoin mielipiteiden ilmaisu ja avoin keskustelu voivat aiheuttaa tunnemyllerryksessä tehtyjä päivityksiä sosiaalisessa mediassa. Hätiköity johtopäätös voi aiheuttaa virheellisen tiedon jakamisen suuren ihmisjoukon nähtäväksi. Sosiaalisessa mediassa käyttäjillä on myös tapana väritellä tarinoita joko tahallisesti tai tahattomasti. Väärät olettamukset ja tiedot voivat pahimmassa tapauksessa täyttää jopa kunnianloukkauksen tunnusmerkistön. (Forss 2015, 24)

Yksityiselämää loukkaava tiedon levittäminen on määritelty rikoslain 24 luvun 8 pykälässä. Yksityiselämän loukkauksista sosiaalisessa mediassa yleisimpinä ovat esimerkiksi suurelle ihmisjoukolle jaetut tiedot henkilön mielenterveysongelmista, terveydestä tai ihmissuhdeasioista. Asia voi koskea monenlaista tietoa tai jaettuja kuvia. Kriteerinä on kuitenkin se, että teko aiheuttaa loukatulle kärsimystä, halveksuntaa tai muuta vahinkoa. (L 13.12.2013/879, 8 §)

Pohjanmaan käräjäoikeuden ratkaisu 19/103347 käsittelee yksityiselämää loukkaavan tiedon levittämistä, jossa henkilö A oli oikeudettomasti toimittanut yhteisöpalvelu Facebookissa useiden ihmisten saataville henkilöiden B,C ja D tietoja. Teot ovat olleet omiaan aiheuttamaan henkilöille vahinkoa, kärsimystä tai heihin kohdistuvaa halveksuntaa. (KO:19/103347)

Tapauksessa henkilö A oli työskennellyt paikallisella grillillä (osakeyhtiö), jonka olivat omistaneet henkilöt B,C ja D. Henkilö A oli julkaissut Facebook -tilillään tekstejä, joissa hän on ilmoittanut grillin, ja nimenomaisesti henkilöiden B,C ja D olevan hänelle velkaa maksamattomien palkkojen osalta 8.500 euroa. A oli myös maininnut julkaisussaan osakeyhtiön olevan varaton, ja että palkkasaatavat ovat ulosottoperinnässä. (KO:19/103347)

Henkilö A oli myös syyllistynyt kolmeen kunnianloukkaukseen, sillä hän oli julkaissut henkilöistä B, C ja D tekstejä Facebook -tilillään, joissa hän oli ilmoittanut asianomistajien hävittäneen omistamansa grillin irtaimistoa, pitäneen

häntä orjatyössä ja huijanneen häntä. A oli myös maininnut kirjoituksissaan henkilön D päihdeongelmasta. (KO:19/103347)

Henkilö A kiisti syytteet ja teonkuvaukset. Vastauksessaan hän totesi, ettei kysymys ollut yksityiselämää koskeva asiasta vaan oikeushenkilöä koskevasta seikasta. Hän perusteli vastaustaan, että kyseessä olivat tosiasiat, jotka eivät olleet omiaan aiheuttamaan vahinkoa tai kärsimystä asianomistajille. Kunnianloukkaus -syytteeseen hän perusteli vastauksensa sillä, että tiedot olivat levinneet vain rajalliseen piiriin ja että värikäs kielenkäyttö oli tyypillistä sosiaalisessa mediassa. (KO:19/103347)

Asianomistaja B kertoi hänen kuulleen kirjoitetuista viesteistä ystävä- ja tuttavapiiriltään. Henkilö A oli julkaissut viestit niin, että ne ovat kaikkien saatavilla. B ei ollut nähnyt itse julkaisuja, sillä A oli estänyt hänet Facebookissa. Julkaisuista oli kuitenkin saatu kuvakaappauksia, joista B oli myöhemmin nähnyt jaetut sisällöt. (KO:19/103347)

Asianomistaja C oli nähnyt julkaisut jälkikäteen asianomistaja B:lle toimitetuista kuvakaappauksista. Lisäksi työkaverit olivat puhuneet julkaisuista, ja tutut kertoneet A:n jakaneen julkaisuja julkiselle paikkakunnan Puskaradio -Facebook sivustolle. C oli sitä mieltä, että A olisi voinut kirjoittaa avoimesti yrityksestä ja sen tilanteesta, sillä grillin lopettamisesta oli kirjoitettu paikallislehdissäkin ja se oli julkista tietoa. Asianomistajien henkilökohtaisten nimien käyttö oli ollut kuitenkin sopimatonta. Viestit olivat levinneet laajalle, sillä ystävät, työkaverit, sukulaiset ja tutut olivat kyselleet C:ltä kirjoituksista. (KO:19/103347)

Vastaaja A oli estänyt asianomistaja D:n pääsyn Facebook -sivuilleen, mutta D oli nähnyt julkaisut tuttavien käyttäjätilien kautta. Viestit olivat julkisia ja julkaisun jälkeen D oli saanut useita viestejä ja kuvakaappauksia ystäviltä ja sukulaisilta A:n jakamista kirjoituksista. Kirjoitukset olivat levinneet nopeasti. Asianomistajat B, C ja D ajattelivat aluksi kirjoitusten loppuvan ajan kuluessa, kun tilanne rauhoittuu. A ei kuitenkaan lopettanut kirjoittelua, vaan jakoi niitä myös muilla Facebookin -sivustoilla kuin vain omalla tilillään. Lopulta kirjoitukset oltiin poistettu sivustoilta. (KO:19/103347)

Pohjanmaan käräjäoikeus katsoi, että henkilö A oli syyllistynyt rikoslain 24 luvun 8 §:ssä tarkoitettuun (kolmeen) yksityiselämää loukkaavaan tiedon levittämiseen sekä kolmeen rikoslain 24 luvun 9 §:ssä tarkoitettuun kunnianloukkaukseen. Käräjäoikeus tuomitsi vastaajan päiväsakkoihin. (KO:19/103347)

Tapauksessa sosiaalisen median uhka löytyi asianosaisten lähipiiristä. Ihmisellä on tapana muokata käytöstään tilanteiden mukaan ja se on ollut luonnollinen selviytymiskeino koko ihmishistorian ajan. Päivittäisiä ja vaihtuvia rooleja ylläpidetään myös sosiaalisessa mediassa, eikä se ole ongelmatonta. Sosiaalisen median yhtenä riskinä on, etteivät kaikki ole siellä rehellisin aikein. Läheiseksi tunnettu ihmissuhde voikin ilmetä valheelliseksi ja haavoittavaksi. (Arikka 2016)

4.2 Tietoturva sosiaalisessa mediassa

Kun käytetään sosiaalista mediaa, käyttäjät ovat altistuneet suostumuksestaan siihen, että muut voivat tarkkailla heihin liittyviä tietoja heidän käyttäjäprofiileistaan sekä jakamistaan verkkosisällöistä. Jokaisella sosiaalisen median palvelimella on omat käyttöehtonsa ja käytäntönsä, jotka käyttäjän tulee hyväksyä päästäkseen luomaan käyttäjätilin palveluun. Sosiaalisen median palveluissa itse sosiaalisen median viestintäpalvelun tarjoaja, muut käyttäjät, teleyritykset ja esimerkiksi sähköpostipalvelun tarjoajat pystyvät puuttumaan ja käyttäjien yksityisiin tietoihin sekä käsittelemään niitä. (Pesonen 2013, 45)

Sähköisen viestinnän palveluista säädetyn lain 33 luvun 272 momentissa säädetään toimenpiteet tietoturvan toteuttamiselle. Lain mukaan viestinnän välittäjällä ja lisäarvopalvelun tarjoajalla on oikeus ryhtyä toimiin tietoturvasta huolehtimiseksi:

> *”1) viestintäverkkojen tai niihin liitettyjen palvelujen sekä tietojärjestelmien tietoturvalle haittaa aiheuttavien häiriöiden havaitsemiseksi, estämiseksi, selvittämiseksi ja esitutkintaan saattamiseksi;*
>
> *2) viestin välittäjä tai viestin vastaanottajan viestintämahdollisuuksien turvaamiseksi; tai*

> *3) viestintäpalvelujen kautta laajamittaisesti toteutettavien rikoslain 37 luvun 11 §:ssä tarkoitettujen maksuvälinepetosten valmistelun ehkäisemiseksi".*

Lain mukaan toimenpiteet tulee toteuttaa huolellisuutta noudattaen ja ne tulee mitoittaa häiriön vakavuuteen. Toimenpiteitä toteutettaessa ei saa rajoittaa sananvapautta taikka luottamuksellisen viestin tai yksityisyyden suojaa enempää kuin on välttämätöntä. (L 7.11.2014/917, 272 §)

Viestintäverkkoihin ja viestintäpalveluihin kohdistuvista turvatoimenpiteistä säätää myös valmiuslaki. Valmiuslain 9 luvun 62 §:n mukaan liikenne- ja viestintäministeriö voi velvoittaa teleyrityksen, lisäarvopalvelun tarjoajan tai muun kuin valtion yhteisötilaajan esimerkiksi estämään tai salaamaan verkko- ja viestintäpalveluitaan. Sähköposti- tai tekstiviestien ja muiden vastaavanlaisten viestien lähettäminen, välittäminen tai vastaanottaminen voidaan estää tilapäisesti lain nojalla. Liikenne- ja viestintäministeriö voi myös ryhtyä muihin välttämättömiin toimenpiteisiin tietoturvaloukkausten torjumiseksi tai tietoturvahäiriöiden poistamiseksi. (L 29.12.2011/1552, 62 §)

Tietoverkon mahdollistamissa uusissa ympäristöissä melko yleisiä ovat identiteettivarkaudet, sillä tietoverkoissa liikkuu erittäin suuria summia pääomaa. Identiteettivarkauksissa esiinnytään toisen ihmisen henkilöllisyydellä käyttämällä jonkun muun henkilön henkilötietoja, tunnistautumistietoja, kuvia tai muuta yksilöitävää tietoa. Identiteettivarkauksille ominaista onkin toisena ihmisenä esiintyminen sosiaalisessa mediassa esimerkiksi osto- tai myyntipalstoilla. (Rikosuhripäivystys 2014; Soininen 2017, 84)

Perinteisen käsityksen mukaan identiteetti on osa yksilön henkilöllisyyttä, johon kuuluvat henkilötunnus, nimi ja muut yksilöivät tunnistusmenetelmät. Tietoverkoissa esiintyvällä sähköisellä identiteetillä tarkoitetaan puolestaan identiteettitiedon osajoukkoa, jota käytetään erottelemaan jokin tietty käyttäjää yksilöivä kokonaisuus muista. Sähköisen identiteetin muodostavat sosiaalisessa mediassa ja muissa sähköverkoissa esimerkiksi käyttäjätunnus ja salasana, nimimerkki, IP-osoite tai luottokorttinumero. (Soininen 2017, 86)

Yleensä tietoverkoissa tapahtuvat identiteettivarkaudet ovat laajoja kokonaisuuksia, jotka ovat vaatineet useita uhreja. Niin sanottu rikoksentekoväline voi olla esimerkiksi profiili tai käyttäjätili tai sähköpostitse tapahtuva huijaus. Joissakin tapauksissa itse identiteettivarkauskin voi olla tekoväline, jolloin se esiintyy törkeämmän rikoksen yhteydessä. Uhreille rikosten tuottamat seuraukset voivat olla hyvinkin suuria ja niiden rajoittaminen voi koitua erittäin hankalaksi. (Soininen 2017, 87)

Useat tietoturvaan tai sosiaalisen median riskeihin ja uhkiin liittyvät oikeustapaukset eivät ole tarkkarajaisia tai täsmällisiä, ja tyypillistä onkin, että teonkuvauksissa käytetään useita eri rikosnimikkeitä. Harkinnanvaraisia ovat myös automaattikirjautumisten seurauksena tehdyt sisäänkirjautumiset sekä sovelluskohtaiset tunnistautumiset. Seuraavaksi esittelen aiheeseen liittyvän oikeustapauksen Pohjanmaan käräjäoikeuden ratkaisusta 15/153015.

Tapauksessa vastaaja A tuomittiin sakkoihin tietomurrosta. Henkilö A oli käyttänyt henkilön B käyttäjätunnusta ja salasanaa oikeudettomasti kirjautumalla B:n Facebook-tilille. A oli myös lukenut tilillä olleita viestejä. (KO:15/15015)

Syyttäjä oli esittänyt tapauksessa myös vaihtoehtoisen syytteen viestintäsalaisuuden loukkaamisesta: ”Henkilö A on edellä kerrotulla tavalla menetellen oikeudettomasti avannut toiselle osoitetun suljetun viestin tai suojauksen murtaen hankkinut tiedon ulkopuoliselta suojatusta viestistä.”

Vastaaja A oli kertonut kirjallisessa lausumassaan, että hän on käynyt usein henkilön B pyynnöstä tämän Facebook -tilillä. Kun A oli mennyt Facebook sivustolle omalla tietokoneellaan, hän huomasi Facebookin kirjautuneen automaattisesti henkilön B tunnuksilla palveluun. Tämä johtui siitä, ettei edellinen käyttäjä B ollut kirjautunut tililtä ulos viimeisen käyttökerran jälkeen. Vastaaja A on myöntänyt lukeneensa asianomistaja B:n viestit. (KO:15/153015)

Asianomistaja B oli kertonut käyneensä keskustelua Facebookissa A:n enon kanssa. Viesteissä oli keskusteltu A:n lapsesta ja A:sta. Vastaaja A oli saanut tietää keskustelusta ja soittanut B:lle asiasta. Asianomistaja B:n mukaan A ei ollut

voinut saada tietoa keskusteluasta muualta, kuin näkemällä viestit Facebook-tililtä. B:n mukaan vastaaja A oli myös aikoinaan auttanut B:tä Facebook -tilin luomisessa, ja että A:lla oli tiedossa B:n Facebook -tilin salasana. Käräjäoikeus oli katsonut, että tietomurron tunnusmerkistö on täyttynyt. Täten käräjäoikeus tuomitsi vastaaja A:n sakkorangaistukseen. (KO:15/153015)

Rikoslain 38 luvun 8 §:n mukaan tietomurrolla tarkoitetaan tekoa, jossa käytetään tekijälle kuulumatonta käyttäjätunnusta tai murtaudutaan oikeudettomasti tietojärjestelmään, jossa käsitellään, varastoidaan tai siirretään tietoja tai dataa sähköisesti. Tietomurrosta tuomitaan myös, mikäli tietojärjestelmästä tai sen osasta otetaan oikeudettomasti selkoa teknisen erikoislaitteen avulla, ohitetaan turvajärjestelyitä tai käytetään vilpillisesti hyväksi tietojärjestelmän haavoittuvuutta. (L 10.4.2015/368, 8 §)

Rangaistavaa on siis tunkeutua tietojärjestelmään, johon tunkeutujalla ei ole oikeuksia päästä. Tietomurrossa on kyse järjestelmän turvajärjestelyn murtamisesta. Turvajärjestelyllä voidaan tarkoittaa esimerkiksi käyttäjätunnusta, joka mahdollistaa käyttäjätilille pääsyn. Tietomurrosta rangaistaan ainoastaan, jos teko on tahallinen. Tilanteet, joissa tunkeutuminen tapahtuu luvallisesti toiselta saadulla käyttäjätunnuksella, ei lueta rangaistavaksi tietomurroksi. (Forss 2014, 244)

Tietomurron tahallisuutta tarkasteltaessa on otettava huomioon esimerkiksi niin sanotut automaattikirjautumiset, joissa käyttäjä on tallentanut salasanan valmiiksi. Kun käyttäjätiedot on tallennettu, sisäänkirjautuminen tapahtuu automaattisesti sovelluksen avauduttua. Jos ulkopuolinen käyttäjä kirjautuu heti ulos palvelusta, on vaikea nähdä, että minkään rikoksen tunnusmerkistö täyttyisi. Tällaiset tapaukset ovat tyypillisiä esimerkiksi niissä tapauksissa, joissa yhdellä tietokoneella on monta käyttäjää. (Forss 2014, 244)

4.3 Yksityisyyteen liittyvät käytännöt sosiaalisessa mediassa

Kaikilla sosiaalisen median palveluilla on käytössään omat käyttöehdot, jotka käyttäjän tulee hyväksyä rekisteröityessä palveluun. Käyttöoikeuksiin on voitu

asettaa myös tiettyjä sovellus- tai palvelinkohtaisia rajoituksia. Sosiaalisen median käyttäjän tuleekin olla erityisen huolellinen siitä, mihin hän sitoutuu. Vastuu omasta tietoturvasta ja yksityisyyden suojasta on siis näiltä osin käyttäjällä eli yksityishenkilöllä. (IPR info 2014)

Yksityisyyteen liittyvistä käytännöistä ei ole kuitenkaan aina vastuussa itse käyttäjä, sillä sosiaalisessa mediassa tietojen jakaminen myös toisesta henkilöstä on erityisen helppoa. Rikoslain 24 luvun 8 §:ssa pykälässä säädetään yksityiselämää loukkaavasta tiedon levittämisestä. Lain mukaan se, joka oikeudettomasti käyttää joukkotiedotusvälinettä tai muulla tavoin toimittaa lukuisten ihmisten saataville tietoa, vihjauksia tai kuvia toisen yksityiselämästä siten, että sillä voidaan aiheuttaa vahinkoa, kärsimystä tai halveksuntaa toiselle, on tuomittava sakkoon. (L 13.12.2013/879, 8 §)

Hallituksen esitys HE 19/2013 täsmentää Rikoslain 24 luvun 8 §:ää. Hallituksen esityksen mukaan yksityiselämän käsitteen ytimen muodostaa se, että yksilöllä tulee olla tietyn rajan sisällä ne asiat, jotka hänellä on oikeus pitää omana tietonaan niin halutessaan: ”Yksityiselämän piiriin kuuluvat etupäässä arkaluonteiset tiedot perhe-elämästä, vapaa-ajan käytöstä, terveydestä ja ihmissuhteista. Mitä merkittävämpi asia on muidenkin kuin henkilön itsensä kannalta, sitä todennäköisimmin asia ei kuulu henkilön yksityiselämän piiriin.” On myös eroteltava, mitkä yksityiselämän alueelle kuuluvista tiedoista sijoittuvat lähemmäksi niin sanottua yksityisyyden keskiötä ja mille tasolle niiden arkaluonteisuus voidaan määritellä. (HE 19/2013, 38)

Sosiaalisessa mediassa yksityiselämän suojaa voidaan loukata esittämällä tietoa, vihjauksia tai kuvia toisen yksityiselämästä. Tiedolla tarkoitetaan totuudenmukaista informaatiota toisen yksityisasioista ja henkilökohtaisuuksista. Loukkaaminen voi tapahtua myös vihjailemalla asiasta epäsuorasti. Melko yleinen tapa puuttua toisen yksityiselämään sosiaalisessa mediassa on myös kuvan julkaiseminen toisesta ilman toisen lupaa. (HE 19/2013, 38)

Henkilökohtaista informaatiota sisältävien julkaisujen rajoittaminen sekä henkilötietojen ja julkaisujen näkyvyyden rajoittaminen puolestaan ovat tekijöitä,

joihin käyttäjä voi itse vaikuttaa. Oleellista on, miten suuri ihmisjoukko pystyy näkemään viestin tai julkaisun. Mikäli viesti on julkaistu suljetussa ryhmässä tai ainoastaan kaverilistan nähtäväksi, on arvioitava julkaisun mahdollisten näkijöiden määrää. (Forss 2015, 18)

4.4 Henkilötietojen jakaminen

Koko sosiaalisen median käyttö perustuu käyttäjien henkilötietojen käsittelyyn sen eri muodoissa, joista yhteisöpalvelun tarjoajalle koostuu käyttäjiään ja heidän elämänolojaan kuvaavia henkilörekistereitä. Käyttäjien nimi, sähköpostiosoite ja ikä ovat yleisimmät palveluihin kerättävät tiedot, mutta myös arkaluonteisia tietoja saatetaan säilyttää. Lisäksi käyttäjien toimintaa seurataan. (Pesonen 2013, 90)

Sosiaalisen median sisältö perustuu hyvin pitkälti käyttäjän itsensä luomaan materiaaliin. Henkilötietojen avoin jakaminen käyttäjän yksityisyyden kannalta on riski, sillä tietojen joutuessa vääriin käsiin voivat seuraukset olla suuria. Verkossa olevien sosiaalisten palveluiden käyttö on käyttäjän oma valinta. Useimmissa palveluissa käyttäjän tulee hyväksyä käyttöehdot palvelun käytettävyyden varmistamiseksi. Henkilötietojen jakaminen on henkilötietojen käsittelyä. Henkilötietojen käsittelystä on säädetty tarkoin tietosuojalaissa. (Hintikka 2019)

Kun tutkitaan henkilötietoja, on kiinnitettävä huomiota niiden laatuun, määrään ja sijaintiin. Käyttäjä voidaan tunnistaa jopa yhdellä henkilötiedolla. Henkilötietojen määrällä on myös merkitystä, sillä käyttäjä on mahdollista tunnistaa yhdistelemällä vähemmän yksilöiviä tietoja, joista muodostuu henkilön helposti tunnistettava kokonaisuus. (Hankkila 2009, 150)

Maanmittauslaitoksen julkaiseman artikkelin ”Sosiaalinen media tarjoaa aineistoa liikkumisen tutkimukseen” mukaan somedatalla on selkeä rakenne: sosiaalisen median päivityksiin liittyy usein ajankohta, milloin päivitys on tehty, käyttäjätietoja, sisältöä kuvana tai tekstinä, hymiöitä tai linkkejä sekä tykkäyksiä ja kommentteja muilta käyttäjiltä. Yhä useammissa sosiaalisen median alustoissa ja sovelluksissa käyttäjällä on mahdollisuus jakaa myös sijaintitietojaan.

Sijaintitietoja hyödynnetään paljon tutkimuksissa ja esimerkiksi kävijälaskennoissa, mutta sijaintietojen jakaminen voi olla myös pahimmillaan riski käyttäjälle ja hänen yksityisyyden suojalleen. (Toivonen, Heikinheimo, Hiippala & Tenkanen 2017)

Henkilötietojen jakamisesta käytän esimerkkiä Korkeimman oikeuden ratkaisusta, KKO: 2018:81, jossa henkilö A oli kuvannut videon tapahtumista koskien hänen kahden lapsensa huostaanoton täytäntöönpanoa. Henkilö B oli julkaissut Internetissä videon kuvaajahenkilö A:n pyynnöstä. Videossa lasten kasvot olivat sumennettu, mutta lapset olivat kuitenkin tunnistettavissa. Korkeimman oikeuden ratkaisun mukaan videon julkaisemisen katsottiin ylittäneen hyväksyttävän rajan. Videon julkaistamista ei voitu katsoa oikeutetuksi edes sillä perusteella, että julkaisuun oli huoltajien suostumus. Täten henkilöt A ja B syyllistyivät yksityiselämää loukkaavaan tiedon levittämiseen. (KKO:2018:81)

Tapauksessa syyttäjä vaati A:lle ja B:lle rangaistusta yksityiselämää loukkaavasta tiedon levittämisestä. A ja B olivat yhdessä julkaisseet Internetissä videon heidän kahden 9-vuotiaan lapsen, henkilöiden C ja D, huostaanottotilanteesta. Henkilö A oli kuvannut videon, jossa sosiaaliviranomaiset tulevat yhdessä poliisin kanssa hakemaan lapsia kotoa. Videolla kävi ilmi, että lapset olivat lastensuojelun asiakkaita ja heidät oli huostaanotettu. Henkilö A oli toimittanut videon henkilö B:lle ja B oli sumentanut lasten kasvoja videolla. Tämän jälkeen B oli ladannut videon Youtube -kanavalle. Video oli avoin ja kaikilla oli vapaa pääsy sen katseluun. Tämän lisäksi A, B ja muut henkilöt olivat jakaneet videolinkkiä Internetissä. Kasvojen sumentamisesta huolimatta lasten henkilöllisyys ilmeni videojukaisusta asiayhteydessä. He olivat myös muutenkin tunnistettavissa. Täten syyttäjä katsoi, että ”A ja B olivat oikeudettomasti joukkotiedotusvälinettä käyttämällä tai muutoin toimittamalla lukuisten ihmisten saataville esittäneet C:n ja D:n yksityiselämästä tiedon, vihjauksen tai kuvan siten, että teko oli omiaan aiheuttamaan vahinkoa tai kärsimystä loukatulle taikka häneen kohdistuvaa halveksuntaa”. (KKO:2018:81)

Oulun käräjäokeus hylkäsi syytteet. Käräjäoikeus katsoi, että videossa ilmennyt lasten asiakkuus lastensuojeluun sekä huostaanotto olivat rikoslain 24 luvun 8 §:ssä tarkoitettuja yksityiselämää koskevia tietoja. Video sisälsi kohtauksia, joissa lasten kasvot eivät olleet sumennettuja ja videolta kuuluivat myös lasten äänet. Lasten henkilöllisyys voitiin tunnistaa myös videolla näkyvän talon ja pihapiirin perusteella. Käräjäoikeus katsoi, että video sisälsi lapsia koskevia arkaluonteisia tietoja, mutta julkaisemiseen oli ollut tapauksessa huoltajien suostumus. Vanhemman oikeuteen julkaista lasta koskevaa arkaluontoista tietoa tai suostumuksen antamista sellaiseen toimintaan, ei ollut sovellettavissa selkeää lainsäädäntöä. Asian tarkastelussa käräjäoikeus sovelsi myös rikoslain 24 luvun 8 §:n 3 momentin mukaista säädöstä ja totesi, että video käsitteli merkittävää asiaa. Videossa lasten yksityisyyttä oltiin pyritty suojaamaan kasvojen sumentamisella ja videon yhtenä motiivina oli halu herättää keskustelua lastensuojelun päätöksen täytäntöönpanosta ja käytännön toteutuksesta. (KKO:2018:81)

Syyttäjä ja lapset C ja D valittivat käräjäoikeuden ratkaisusta hovioikeuteen ja vaativat rangaistusta A:lle ja B:lle yksityiselämää loukkaavasta tiedon levittämisestä. Lisäksi syyttäjä vaati videon poistamista yleisön saatavilta. Rovaniemen hovioikeudessa syyksiluettiin yksityiselämää loukkaava tiedon levittäminen. Lisäksi hovioikeus hyväksyi käräjäoikeuden tuomion perustelut siitä, että videosta ilmeni huostaanotto ja lastensuojelun asiakkuus ja että henkilöt olivat tunnistettavissa videolta. Kuten käräjäoikeus, hovioikeus katsoi näiden seikkojen olevan yksityiselämää koskevia tietoja. (KKO:2018:81)

Hovioikeus huomioi ratkaisussaan, että vaikka lapsen vanhemmalla olikin oikeus päättää lapsensa asioista, eivät oikeudet ole rajoittamattomia ja tapauksen kaltaisissa ristiriitatilanteissa tulee ottaa huomioon myös lasten oikeudet. Videojulkaisussa oli kyse erittäin arkaluontoisen tiedon jakamisesta, joka olisi voinut olla omiaan aiheuttamaan leimaantumista tai kiusaamista lapsille. Hovioikeus totesi, että huoltajan oli täytynyt käsittää, että videotallenne koski lasten yksityisyyden suojaa ja kunnioittamista, joita huoltajan tulee huomioida. Myös videon julkaissut B oli velvollinen ymmärtämään videotallenteen arkaluonteisuus ja julkaisun aiheuttama mahdollinen uhka lasten

vahingoittamiselle, kärsimykselle ja halveksunnalle. Hovioikeuden päätöksen mukaan videon julkaiseminen ylitti selvästi hyväksyttävän rajan. Hovioikeus tuomitsi A:n ja B:n päiväsakkoihin ja video määrättiin hävitettäväksi. (KKO:2018:81)

A:lle ja B:lle myönnettiin valituslupa ja asian käsittely jatkui Korkeimmassa oikeudessa. Korkein oikeus ei muuttanut hovioikeuden tuomion lopputulosta. Korkeimman oikeuden asiaesittelyssä ilmenee videotallenteen julkaisemisen yhteydessä julkaistu lasten asuinkaupunki. Videolla näkyy lasten vastaan hangoittelu ja huuto poliisia ja viranomaisia vastaan. Lapset kannetaan autoon ja heidän kasvonsa on sumennetu. Videolla esiintyvien muiden henkilöiden kasvot ovat kuitenkin näkyvissä. Nimiä videolla ei sanota, mutta poliisin sanomana käy ilmi, että ainakin toinen lapsista on 9-vuotias. (KKO:2018:81)

Korkein oikeus totesi, että henkilön, jota tieto koskee, tulee olla tunnistettavissa, jotta voidaan puhua yksityiselämää loukkaavasta tiedon levittämisestä. ”Yksityiselämää loukkaavaan tiedon levittämiseen syyllistyy se, joka säännöksessä mainituin tavoin ja edellytyksin oikeudettomasti esittää toisen yksityiselämästä tiedon, vihjauksen tai kuvan.” Itseään koskevan tiedon esittäminen kuuluu siis jokaiselle henkilökohtaisesti ja se koskee myös lapsia. On kuitenkin selvää, ettei pieni lapsi voi päättää itsenäisesti häntä koskevien tietojen julkaisemisesta. Korkein oikeus katsoi, etteivät 9-vuotiaat lapset olisi voineet antaa pätevää suostumusta videon julkaisemisesta. Lainsäädännöstä ei löydy kieltoa, joka koskisi huoltajan lapsestaan julkaisemia tietoja. Lapsenhuoltolaki määrittelee kuitenkin sen, mitä huoltajan tulee ottaa huomioon tehdessään lasta koskevia päätöksiä. (KKO:2018:81)

Viranomaisten toiminnan kuvaamisesta korkein oikeus katsoo viranomaisten toimintatapojen esiin nostamisen olevan perusteltua, jotta viranomaisten menettelyä voidaan arvioida ja mahdollisiin epäkohtiin voitaisiin puuttua. A:n ja B:n mukaan videon julkaiseminen oli saanut aikaan keskustelua lastensuojelupäätösten täytäntöönopanosta ja käytännön toteutumisesta.

Korkeimman oikeuden mukaan video oli käsitellyt merkittävää asiaa. (KKO:2018:81)

Menettelyn hyväksyttävyyttä koskevassa punninnassa korkein oikeus katsoi A:n ja B:n menetelleen tahallisesti, sillä heidän oli täytynyt tietää videon aiheuttavan lapsille kärsimystä. A ja B ovat esittäneet kertomuksessaankin olevan tietoisia lasten huostaanoton salassapidettävyydestä ja asian arkaluonteisuudesta. (KKO:2018:81)

Korkeimman oikeuden ratkaisun perusteluiden lisäksi tapaukseen voidaan soveltaa Euroopan ihmisoikeussopimuksen 8 artiklaa, jonka mukaan jokaisella on oikeus nauttia yksityis- ja perhe-elämän kunnioitusta. Artikla koskee myös kotiin ja kirjeenvaihtoon kohdistuvaa kunnioitusta. Tapauksessa lasten yksityiselämään on puututtu, sillä heistä oli julkaistu heidän yksityiselämää loukkaavaa materiaalia. (EIS 63/1999, 8)

Suomen perustuslain mukaan jokaisella ihmisellä on oikeus yksityisyyteen. Oikeus kattaa jokaisen henkilön iästä tai sukupuolesta huolimatta. Lapsen oikeuksia tukee myös YK:n lapsen oikeuksien sopimus LOS. LOS:in 16 artiklan mukaan ”lapsen yksityisyyteen, perheeseen, kotiin tai kirjeenvaihtoon ei saa puuttua mielivaltaisesti tai laittomasti eikä hänen kunniaansa tai mainettansa saa laittomasti halventaa”. (11.6.1999/731, 10 §; LOS 16 artikla)

5 JOHTOPÄÄTÖKSET

Tämän opinnäytetyön tarkoituksena oli selvittää, millä tavoin yksityisyyttä pystytään suojaamaan käytettäessä sosiaalisen median palveluita ja mitä yksityisyyden suoja merkitsee sosiaalisen median käyttäjälle. Tutkimuksen viimeisessä luvussa esitetään keskeisimpiä tutkimustuloksia, pohditaan tutkimuksen luotettavuutta ja arvioidaan opinnäytetyöprosessia sekä etsitään aiheeseen liittyviä jatkotutkimusmahdollisuuksia.

5.1 Keskeisimmät tutkimustulokset

Tutkimuksessa käytetyn oikeudellisen aineiston sekä oikeustapausten avulla voidaan todeta, että sosiaalisella medialla on suuri vaikutus ihmisten käyttäytymiseen ja koko yhteiskuntaan. Siten myös sen käyttäjällä on suuri vastuu, sillä kyseessä ovat omat henkilökohtaiset tiedot ja yksityisasiat, mutta myös lukematon määrä mahdollisuuksia jopa yhteiskunnalliseen vaikuttamiseen. Tutkimuksessa käytetyt oikeustapaukset ovat konkreettisia esimerkkejä sosiaaliseen mediaan sovellettavan lainsäädännön ja sananvapauden tuottamasta ristiriidasta.

Internet ja sosiaalinen media on oikeudellisesti hyvin vaikeasti määriteltävä kokonaisuus, jossa vastuu on hyvin pitkälti itse käyttäjällä. Ottaessaan käyttöön sosiaalisen median palvelun, on käyttäjän useimmiten hyväksyttävä palvelun tarjoajan käyttöehdot tai yhteisösäännöt, joiden tehtävä on palvella sekä itse käyttäjää että palveluntarjoajaa. Täten verkossa olevien sosiaalisten palveluiden käyttö on käyttäjän oma valinta.

Sosiaalisessa mediassa yksityisyyden suojalla tarkoitetaan turvallista, asianmukaista ja ihmisoikeuksia tukevaa sosiaalisen median palvelun käyttöä. Yksityishenkilön on ymmärrettävä viestintäsalaisuuden merkitys ja se, ettei arkaluonteista tai toisen yksityiselämää koskevaa tietoa tule saattaa toisten ulottuville. Yksityisyyden suoja sosiaalisessa mediassa tarkoittaa tietoturvaa ylläpitävää tietoverkkojen käyttöä sekä palveluntarjoajan asettamien käyttöehtojen ja yhteisösääntöjen asianmukaista noudattamista.

Yksityishenkilön yksityisyyden suojaa voivat uhata useat eri tahot ja toisinaan uhka voi löytyä jopa tuttavapiiristä. Valitettavan yleisiä ovat tapaukset, joissa kuva on lisätty sosiaaliseen mediaan toisen käyttäjän toimesta ilman kuvassa esiintyvän lupaa. Ongelmallisia ovat myös verkossa tapahtuvat identiteettivarkaudet, virukset ja hakkerit. Tietoverkot voivat toimia alustana myös rikollisjärjestöille sekä väkivaltaisten ja seksististen materiaalien levittämiselle. Käyttäjän on myös oltava huolellinen antaessaan lupaa markkinointitarkoitukseen käytetyistä henkilö- tai profiilitiedoista.

Myös sähköinen viestintä itsessään voi aiheuttaa yksityishenkilön suojalle uhkia käytettäessä sosiaalisen median palveluita, sillä lähes kaikesta sähköisestä viestinnästä jää pysyvä digitaalinen jälki, jota on hankala poistaa. Uhkia voivat aiheuttaa esimerkiksi jaetut sijaintitiedot, joista voidaan päätellä henkilön ajantasaiset liikkeet. Uhkana voivat olla myös toisten jakamat kuvat käyttäjästä tai arkaluonteisten asioiden päätyminen julkiseen tietoon. Sosiaalisessa mediassa sähköisen profiilin taakse on helppo piiloutua ja sähköiseen tuntemattomaan minään voi olla helppo samaistua. Käyttäjäprofiilin takaa voi myös paljastua joku muu kuin henkilö, joksi hän on itsensä profiilissaan esittänyt.

Omaan yksityisyytensä suojaan käyttäjä voi vaikuttaa omien henkilötietojen ja julkaisujen näkyvyyden rajoittamisella. Sosiaalisessa mediassa oleellista on se, miten suurelle ihmisjoukolle viesti tai julkaisu näkyy. Käyttäjän on myös syytä miettiä, millaista tietoa ja materiaalia itsestään kannattaa jakaa, sillä julkaisuilla on aina riski levitä tietoverkoissa. Erityistä huolellisuutta käyttäjän tulee kiinnittää materiaaliin, jossa on osallisena myös muita, esimerkiksi ystäviä, läheisiä tai perheenjäseniä.

Käyttöehdoista ja oman käyttäjäprofiilin hallinnoimisesta huolimatta vastuu yksityisyyteen liittyvistä käytännöistä ei ole aina itse käyttäjällä, sillä tietojen jakaminen myös toisesta henkilöstä on helppoa. Lisäksi sosiaalista mediaa tai Internetiä ei hallinnoi mikään yksittäinen taho, eikä sosiaalisen median käytölle ole kirjoitettuna varsinaista lainsäädäntöä, vaan säännökset on hajautettu useisiin eri lakeihin. Tämä puolestaan aiheuttaa ristiriitaisia tunteita käyttäjillä, sillä kuten

perusoikeuksiin kuuluu, sananvapaus oikeuttaa ilmaisemaan ja vastaanottamaan mielipiteitä julkisesti. Mielipiteiden ja ajatusten jakaminen sekä ihmisten välinen yhteisöllisyys ovatkin yksi merkittävä sosiaalisen median mahdollistama ilmiö.

Kuten käyttämästäni tutkimusmateriaalista ilmenee, yksityisyyden suojaan ja yksilön kunniaan liittyvät rikokset ovat melko ilmeisiä sosiaalisen median palveluissa. Mielipiteiden jakamisella ja pahan olon purkamisella tietoverkoissa voi olla ikäviä seurauksia. Voidaan siis todeta, että sosiaalisen median käyttäjällä voi olla toisinaan haastavaa tietää, milloin rikotaan palvelun sääntöjä tai jopa kirjoitettua lainsäädäntöä. Niin sanottuna nyrkkisääntönä voidaankin pitää, ettei minkään rikoksen tunnusmerkistö täyty niin kauan, kun henkilön jakama sisältö koskee ainoastaan häntä itseään.

5.2 Tutkimuksen luotettavuus

Teorialähtöisessä tutkimuksessa luotettavuutta voidaan arvioida validiteetin ja relibiliateetin mittareilla. Validiteetilla tarkoitetaan pätevyyttä eli sitä, onko tutkimusmenetelmä mitannut sitä, mitä on ollut tarkoitus mitata. Relibiliateetti puolestaan viittaa johdonmukaisuuteen ja tulosten toistettavuuteen. (Hirsjärvi, Remes & Sajavaara 2009, 231)

Tässä työssä validiteettia voidaan mitata sillä, miten hyvin käytetty lähdemaeriaali mittaa tutkimuksen pätevyyttä. Tässä työssä validiutta on tarkennettu käyttämällä kattavasti ajantasaista lainsäädäntöä, oikeuskirjallisuutta sekä oikeustapauksia, jotka käsittelevät asetettua tutkimusongelmaa. Tutkimuksen relibiliateetti puolestaan korostuu tutkimuksessa käytettyjen aineistojen yhteneväisyyksissä ja toistuvuudessa: lähes kaikki tutkimuksessa käytetty materiaali perustuu osaltaan lainsäädäntöön. Siten voidaan myös olettaa, että tulokset olisivat edelleen samat, vaikka tutkimus laadittaisiinkin uudelleen. Täten tutkimuksen voidaan katsoa olevan reliaabeli.

5.3 Pohdinta

Opinnäytetyöprosessi sai alkunsa syksyllä 2018, jolloin suoritin oman alan suuntaavaa harjoittelujaksoani. Aihevalinta alkoi muodostua, kun työskentelin

tiiviisti tietoverkkojen kautta henkilötietojen ja henkilöiden yksityistietojen parissa. Alustava aihevalintani vaati rajaamista, ja lopullinen aihe syntyi opinäytetyöohjaajan avustuksella. Mielenkiinto aihetta kohtaan mietitytti aluksi, mutta työn edetessä aloin kiinnostua aiheesta enemmän.

Työlläni ei ollut toimeksiantajaa, mikä mielestäni mahdollisti sujuvan työskentelyn oman näkökulman rajaamana. Työn loppusuoralla aiheeseen liittyvän ajantasaisen materiaalin löytäminen tuotti hieman haasteita, sillä osa aiheeseen liittyvästä kirjallisuudesta oli melko vanhaa verraten jatkuvasti kehittyvään teknologiaan ja sen myötä myös sosiaaliseen mediaan. Prosessin aikana ilmeni myös, että osa syksyllä 2018 tutkimusmateriaalin aineistona käyttämistäni laeista oli kumottu kevääseen 2019 mennessä. Myös sosiaaliseen mediaan liittyvien oikeustapausten vähäinen määrä yllätti verraten siihen, miten yleisiä ongelmatapaukset ja jopa rikokset ovat sosiaalisessa mediassa.

Opinnäytetyöprosessin aikana sattui myös työssäni kohdalle eräs aiheeseen liittyvä rikostapaus, jossa oli kyse sosiaalisessa mediassa tapahtuneesta kunnianloukkauksesta. Tapausta käsitellessäni sain hyvinkin paljon näkemyksiä ja materiaalia aiheeseen liittyen. Tapaus on yksi tutkimuksessa käyttämistäni oikeustapauksista. Myös sosiaalisen median laaja-alainen, mutta samalla myös vaikeaselkoinen lainsäädäntö herätti mielenkiintoni perehtyä aiheeseen lähemmin.

Opinnäytetyön innoittamana sain mahdollisuuden osallistua Pohjanmaan käräjäoikeuden työryhmään, jonka tehtävänä oli laatia henkilötietosuojaohje Pohjanmaan käräjäoikeuden kansliahenkilöstön käyttöön. Ohjeessa oli oma pieni osuutensa myös sosiaaliseen mediaan liittyvillä käytännöillä, vaikka näkökulma poikkesikin hieman varsinaisesta tutkimusaiheestani.

Tutkimusprosessi on herättänyt minussa hyvin laaja-alaista pohdintaa aiheeseen liittyen. Käsite ”sosiaalinen media” on melko uusi, mutta myös jatkuvasti muutuva ja koko yhteiskuntaa koskettava ilmiö. Tämä puolestaan mahdollistaa lukemattomia jatkotutkimusaiheita, joista yksi voisi olla esimerkiksi aiheen tarkastelu palveluntarjoajan näkökulmasta. Tällä voitaisiin selvittää vielä konkreettisemmin yksilön ja palveluntarjoajan vastuun rajaa sosiaalisen median

palveluissa. Tutkimus voitaisiin suorittaa esimerkiksi haastattelututkimuksena. Eräästä tutkimuksessa käytetystä kattavasta materiaalista nousi esiin myös aihe rikosoikeudellisesta vastuusta sosiaalisessa mediassa, joka avaa myös osaltaan mahdollisuuksia hyvin mielenkiintoisten jatkotutkimusaiheiden pariin.

LÄHTEET

Aula, P., Matikainen, J. & Villi, M. 2006. Verkkoviestintäkirja. Gaudeamus Helsinki University Press / Palmenia. Helsinki.

Arikka, R. 2016. Somessa ihmisellä on vain yhdet kasvot. Viitattu 2.6.2019. http://ajatuspajalinja.fi/somessa-ihmisella-on-vain-yhdet-kasvot/

Elinkeinoelämän keskusliitto 2018. Tietopaketti yrityksille: EU:n yleinen tietosuoja-asetus ja tietosuojalaki. Viitattu 2.12.2018. https://ek.fi/mita-teemme/yrityslainsaadanto/tietosuojalainsaadanto/tietopaketti-yrityksille-on-aika-valmistautua-eun-yleiseen-tietosuoja-asetukseen/#1--Mik--on-yleinen-tietosuoja-asetus-

Euroopan parlamentin ja neuvoston direktiivi EPNDir 2002/58/EY henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (sähköisen viestinnän tietosuojadirektiivi) 12.7.2002. Lakitietopalvelu Edilexin sivuilla. Viitattu 30.5.2019. https://www.edilex.fi/eu-lainsaadanto/32002L0058#A5

Euroopan Unioni 2019. Tietosuoja ja yksityisyys verkossa. Viitattu 14.9.2019. https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_fi.htm#shortcut-1

EU 2016/769. Euroopan parlamentin ja neuvoston asetus luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus). EU oikeuden sivuilla – EUR-Lex 2016. Viitatttu 13.9.2019. https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32016R0679

Facebook business 2019. Mikä on yleinen tietosuoja-asetus (GDPR)? Viitattu 15.9.2019. https://www.facebook.com/business/gdpr

Forss, M. 2014. Fobban sosiaalisen median selviytymisopas. Helsinki. GPS Group.

Forss, M. 2015. Kotipoliisitoiminta – asianomistajan mahdollisuudet rikoksesta epäillyn tunnistamiseen sosiaalisen median avulla. Referee-artikkeli lakitietopalvelu Edilexin sivuilla. Viitattu 8.5.2019. https://www.edilex.fi/artikkelit/15906.pdf

Hakola, L. 2012. Some uhkaa ja auttaa kriisissä. Viitattu 2.9.2019. https://viestijat.fi/some-uhkaa-ja-auttaa-kriisissa/#f7da0d8e

Hankkila, S. 2009. Viestintätieteiden pro gradu -tutkielma. Vaasan yliopisto. Yksityisyys sosiaalisessa mediassa. Viitattu 20.4.2019.

HE 19/2013 vp. Hallituksen esitys eduskunnalle laeiksi rikoslain, pakkokeinolain 10 luvun 7 §:n ja poliisilain 5 luvun 9 §:n muuttamisesta. Viitattu 4.5.2019. https://www.finlex.fi/fi/esitykset/he/2013/20130019

Heinonen, R. 2001. Digitaalinen minä. Helsinki. Edita Oyj.

Hintikka, K. 2019. Jyväskylän yliopisto. Sosiaalinen media. Viitattu 6.4.2019. http://kans.jyu.fi/sanasto/sanat-kansio/sosiaalinen-media

Honka, N. 2017. Saanko lukea lapsen viestit puhelimesta vaikka väkisin? Lue asiantuntijoiden neuvot neljään esimerkkitapaukseen. Ylen uutisartikkeli Ylen sivuilla. Viitattu 19.5.2019. https://yle.fi/uutiset/3-9770056

Husa, J., Mutanen, A. & Pohjolainen, T. 2008. Kirjoitetaan juridiikkaa. Helsinki. Talentum.

Innanen, A. & Saarimäki, J. 2012. Internetoikeus. 2. uud painos. Helsinki. Edita.

Instagram 2019. Käyttöehdot. Viitattu 16.5.2019. https://help.instagram.com/581066165581870

Instagram 2019. Yhteisösäännöt. Viitattu 13.5.2019. https://fi-fi.facebook.com/help/instagram/477434105621119

KKO:2018:81. Korkeimman oikeuden ennakkopäätös. Viitattu 20.4.2018. https://korkeinoikeus.fi/fi/index/ennakkopaatokset/precedent/1543835034428.html

KO:19/103347. Pohjanmaan käräjäoikeuden tuomio. Viitattu 4.5.2019

KO:19/116441. Pohjanmaan käräjäoikeuden tuomio. Viitattu 16.5.2019

Koskinen, S., Alapuranen, L., Heino, A-M. & Lehtonen, L. 2012. Henkilötietojen käsittely työelämässä. Helsinki. Edita.

Kuukanen, T. 2018. Tietosuojavaltuutettu uudesta tiedonhakujärjestelmästä: Ihmisten pankkitietojen yksityisyys uhattuna, riskianalyysiä ei ole tehty. Yle. Viitattu 1.11.2018. https://yle.fi/uutiset/3-10451099

L 22.4.1999/523 Henkilötietolaki. Säädöstietopankki Finlexin sivuilla. Viitattu 1.11.2018. https://www.finlex.fi/fi/laki/ajantasa/1999/19990523

L 7.11.2014/9917 Laki sähköisen viestinnän palveluista. Säädös säädöstietopankki Finlexin sivuilla. Viitattu 7.4.2019. https://www.finlex.fi/fi/laki/ajantasa/2014/20140917#L2P4

L 19.12.1889/39 Rikoslaki. Säädös säädöstietopankki Finlexin sivuilla. Viitattu 16.5.2019. https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001#L24

L 11.6.1999/731 Suomen perustuslaki. Säädös säädöstietopankki Finlexin sivuilla. Viitattu 7.8.2019. https://www.finlex.fi/fi/laki/ajantasa/1999/19990731#L2P10

L 5.12.2018/1050 Tietosuojalaki. Säädös säädöstietopankki Finlexin sivuilla. Viitattu 4.4.2018. https://www.finlex.fi/fi/laki/ajantasa/2018/20181050

L 917/2014. Tietoyhteiskuntakaari. Säädös säädöstietopankki Finlexin sivuilla. Viitattu 5.5.2019. https://www.finlex.fi/fi/laki/ajantasa/2014/20140917

L 29.12.2011/1552 Valmiuslaki. Säädös säädöstietopankki Finlexin sivuilla. Viitattu 31.5.2019. https://www.finlex.fi/fi/laki/ajantasa/2011/20111552#O1

Lastensuojelun keskusliiton verkkojulkaisu 2016. Lapsen yksityisyyden suoja digitaalisessa mediassa. Viitattu 19.5.2019. https://www.lskl.fi/materiaali/lastensuojelun-keskusliitto/Lapsen_yksityisyyden_suoja_digitaalisessa_mediassa.pdf

Mannerheimin lastensuojeluliitto 2019. Mediakasvatus. Viitattu 19.5.2019. https://www.mll.fi/ammattilaisille/kouluille-ja-oppilaitoksille/mediakasvatus/

Oikeusministeriö 2019. Julkisuuslaki. Oikeus saada tietoja viranomaisen toiminnasta. Viitattu 28.4.2019. https://oikeusministerio.fi/julkisuuslaki

OpiTietosuojaa.fi 2018. EU:n tietosuoja-asetuksen velvoitteet johdolle. Viitattu 2.12.2018. https://opitietosuojaa.fi/index.php/fi/56-lainsaeaedaentoe/lait/eun-tietosuoja-asetus/23-tuleva-eu-n-tietosuoja-asetus

Pesonen, P. 2013. Sosiaalisen median lait. Viro. Meedia Zone OÜ.

Perustuslakivaliokunnan mietintö 14/2002 vp. Hallituksen esitys laiksi sananvapauden käyttämisestä joukkoviestinnässä ja eräiksi siihen liittyviksi laeiksi. Viitattu 8.5.2019. https://www.eduskunta.fi/FI/vaski/mietinto/Documents/pevm_14+2002.pdf

Soininen, H. 2017. Identiteettivarkaus kyberrikoksena – termit ja tunnusmerkistö. Referee-artikkeli lakitietopalvelu Edilexin sivuilla. Viitattu 11.5.2019. https://www.edilex.fi/defensor_legis/17548.pdf

IPR info 2014. Sosiaalisen median sudenkuopat. Viitattu 30.8.2019. https://iprinfo.fi/artikkeli/sosiaalinen_media/

Tietosuojavaltuutetun toimisto 2018. Rekisterinpitäjän oikeutettu etu. Viitattu 19.12.2018 https://tietosuoja.fi/rekisterinpitajan-oikeutettu-etu

Tietosuojavaltuutetun toimisto 2019. Henkilötietojen käsittelyn oikeusperusteet. Viitatu 9.4.2019. https://tietosuoja.fi/kasittelyperusteet

Tietosuojamalli 2017. a Henkilötietojen käsittelyä koskevat periaatteet. Viitattu 13.5.2019. https://fakta.tietosuojamalli.fi/gdpr-asetus/5-henkilotietojen-kasittelya-koskevat-periaatteet

Tietosuojamalli 2017. b Suostumuksen edellytykset. Viitattu 16.5.2019. https://fakta.tietosuojamalli.fi/gdpr-asetus/7-suostumuksen-edellytykset

Toivonen, T., Heikinheimo, V., Hiippala, T. & Tenkanen, H. 2017. Sosiaalinen media tarjoaa aineistoa liikkumisen tutkimukseen. Julkaisu Maanmittauslaitoksen sivuilla. Viitattu 20.4.2019. https://www.maanmittauslaitos.fi/tietoa-maanmittauslaitoksesta/ajankohtaista/lehdet-ja-julkaisut/positio-lehti/lehdet/some-liikkumisen-tutkimus

Traficomin Kyberturvallisuuskeskus 2019. Luottamuksellinen viestintä. Viitattu 10.4.2019. https://www.kyberturvallisuuskeskus.fi/fi/luottamuksellinen-viestinta

Valtionhallinnon viestintäsuositus 2016. Valtioneuvoston kanslian julkaisusarja 14/2016 Avoimesti, rohkeasti ja yhdessä. Viitattu 1.5.2019. https://vnk.fi/documents/10616/3541383/Valtionhallinnon-viestintasuositus-2016.pdf

Viestintävirasto 2015. Määräys 54 viestintäverkkojen ja palvelujen varmistamisesta sekä viestintäverkkojen synkronoinnista. Viitattu 1.11.2018. https://www.viestintavirasto.fi/ohjausjavalvonta/laitmaarayksetpaatokset/maaraykset/maarays54viestintaverkkojenja-palvelujenvarmistamisesta.html

Viljanen, V. 2013-2018. Suojattu viestintä. Viitattu 15.12.2018. https://www.yksityisyydensuoja.fi/suojattu-viestint%C3%A4

Virkkala, T. 2016. Oikeudellinen katsaus lapsen yksityisyyden suojaan verkossa. Viitattu 19.5.2019. https://www.lskl.fi/materiaali/lastensuojelun-keskusliitto/Lapsen_yksityisyyden_suoja_digitaalisessa_mediassa.pdf

Virtanen, L. 2009. Sähköisen viestinnän tietosuoja. Laurea ammattikorkeakoulu. Viitattu 1.1.2018.

https://www.theseus.fi/bitstream/handle/10024/3921/ONT_Virtanen.pdf?sequence=1

Voutilainen, T. & Galkin, D. 2017. Käyttäjän tiedollisten oikeuksien suhde tietoverkossa tarjottavan palvelun käyttöehtoihin. Referee-artikkeli lakitietopalvelu Edilexin sivuilla. Viitattu 5.6.2019. https://www.edilex.fi/artikkelit/18103.pdf