Isa Nyyssönen

KOLMANNET OSAPUOLET MUKANA HENKILÖ-KOHTAISEN DATAN KÄYTÖSSÄ JA VAIKUTUKSET YKSITYISYYTEEN: CASE FACEBOOK

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2023

TIIVISTELMÄ

Nyyssönen, Isa
Kolmannet osapuolet mukana henkilökohtaisen datan käytössä ja vaikutukset yksityisyyteen: Case Facebook
Jyväskylä: Jyväskylän yliopisto, 2023, 32 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja: Vuorinen, Jukka

Sosiaalinen media ja tässä tutkielmassa tarkastelun kohteena oleva Facebook on herättänyt paljon kysymyksiä, keskustelua sekä huolta käyttäjien yksityisyyden suojasta. Facebook tallentaa ja kerää valtavan määrän henkilötietoja, jotka varsinkin nopean tekniikan kehityksen ja alustaan integroitujen kolmansien osapuolien sovellusten ja palveluiden lisääntyessä on herättänyt huolta käyttäjätietojen turvallisuudesta ja yksityisyydestä. Tästä johtuen on tullut tärkeäksi tarkastella, miten Facebook käsittelee käyttäjien yksityisyyttä erityisesti henkilötietojen ja kolmansien osapuolten kanssa jaetun tiedon osalta. Tutkielman tavoitteena on siis tutkia kolmannen osapuolen osallistumisen vaikutusta Facebookin käyttäjien yksityisyyteen. Tutkielma on toteutettu kirjallisuuskatsauksena. Erityisesti tutkimuksessa selvitetään, missä tilanteissa kolmannet osapuolet pääsevät käsiksi henkilötietoihin ja mitä yksityisyyteen liittyviä haittoja siitä on seurannut. Lisäksi tutkielmassa tutkitaan, missä määrin käyttäjät ovat tietoisia ja suostuvat tietojensa jakamiseen kolmansien osapuolten kanssa. Ennen kuin yllä oleviin ongelmiin ja kysymyksiin vastataan, tutkielma määrittelee aiheeseen liittyviä käsitteitä, joita ovat sosiaalinen media ja Facebook, henkilökohtainen data, sekä yksityisyys. Facebookissa olevat kolmannen osapuolen evästeet ja niiden hyväksyminen ovat olleet merkittävässä osassa käyttäjien yksityisyyden suojan loukkaamisessa. Evästeet ovat askel vielä vakavampaan seuraukseen yksityisyyden suojaan liittyen, joita ovat tietovuodot. Aihetta on syytä tutkia, sillä Facebook on vain yksi monista sosiaalisen median alustoista ja on tärkeää tietää, miten ne voivat olla vaaraksi yksityisyydensuojalle.

Asiasanat: Facebook, Henkilökohtainen data, Kolmannet osapuolet, Yksityisyys

ABSTRACT

Nyyssönen, Isa
Third parties involved in the use of personal data and effects on privacy: Case Facebook
Jyväskylä: University of Jyväskylä, 2023, 32 pp.
Information Systems
Supervisor: Vuorinen, Jukka

The social media service Facebook has raised a lot of questions, discussions, and concerns about the protection of users' privacy. Facebook stores and collects a huge amount of personal data, which, especially with the rapid development of technology and the increase of third-party applications and services integrated into the platform, has raised concerns about the security and privacy of user's personal data. For this reason, it has become important to examine how Facebook handles user privacy, especially regarding personal data and information shared with third parties. The aim of the thesis is therefore to investigate the impact of third-party participation on the privacy of Facebook users. The thesis was carried out as a literature review. In particular, the study finds out in which situations third parties gain access to personal data and what privacy-related disadvantages have resulted from this over the years. In addition, the thesis examines the extent to which users are aware of and consent to the sharing of their data with third parties. Before answering the above problems and questions, the thesis defines concepts related to the topic, such as social media and Facebook, personal data and privacy, and third parties. The third-party cookies on Facebook and their acceptance have been a significant part of violating users' privacy protection. Cookies are a step towards an even more serious privacy consequence, which is data leaks. The topic is worth researching, because Facebook is just one of the many social media platforms and it is important to know how they can be a threat to privacy.

Keywords: Facebook, Personal data, Third parties, Privacy

TAULUKOT

SISÄLLYS

1 JOHDANTO

Ihmiset viettävät ennennäkemättömän paljon aikaa sosiaalisessa mediassa ja sosiaalisten verkostojen parissa. Poikkeus nykypäivänä on pidemminkin se, että joku ei käytä sosiaalisen median alustoja. Facebook on ollut ensimmäinen menestynyt uuden sukupolven sosiaalisen median alusta ja edelleen sovellusta käyttää yli kaksi miljardia ihmistä (Datareportal, 2023). Facebook on vuosien varrella kohdannut lukuisia tietosuojakiistoja, jotka ovat herättäneet huolta käyttäjien henkilökohtaisen datan käytöstä (Rubistein & Good, 2013). Tämän tutkielman liittyvissä artikkeleissa ja tutkimuksissa ovat korostuneet ensisijaiset huolenaiheet, joita ovat sovelluksen käyttäjien tietojen kerääminen, kolmansien osapuolten pääsy heidän tietoihinsa, yksityisyysasetusten monimutkaisuus ja Facebookin mahdollisuus valvoa käyttäjiään. Vaikka Facebook on yrittänyt puuttua näihin huolenaiheisiin, käyttäjien keskuudessa on edelleen huomattava huoli heidän henkilökohtaisten tietojensa turvallisuudesta alustalla (Sneed, 2020). Nämä huolenaiheet ovat yksi syy siihen, miksi käyttäjien olisi tarpeellista ymmärtää Facebookin käytön riskit ja ryhtyä kiinnittämään enemmän huomiota yksityisyytensä suojelemiseksi.

Facebookin luoja Mark Zuckerberg avasi sovelluksen yleisölle vuonna 2004 ja sen suosio on kasvanut siitä eteenpäin räjähdysmäisesti (Hoffmann, Proferes & Zimmer, 2018). Sovelluksen suosio alkoi nuorten keskuudessa ja korkeakoulukeskeisellä lähestymistavalla, joka mahdollisti sosiaalisen vuorovaikutuksen, henkilökohtaisen identiteetin rakentamisen sekä verkostoitumisen muihin käyttäjiin (Debatin, Lovejoy & Hughes, 2009). Nykypäivänä Facebookia voidaan pitää enemmän vanhemman sukupolven alustana, sillä uudet sosiaalisen median alustat syrjäyttävät vanhoja alustoja (Auxier & Anderson, 2021). Ongelmat ja huoli yksityisyyteen liittyen eivät ole kuitenkaan katoamassa, sillä uusissa sosiaalisen median alustoissa samat vaarat ja ongelmat yksityisyyden suojaan

liittyen ovat vielä olemassa. Henkilökohtainen data liikkuu edelleen sovelluksissa ja kolmansien osapuolten hallinnassa ja tämän vuoksi aihetta on syytä tutkia.

Sosiaalisessa mediassa käyttäjien yksityisyys on ollut suuri huolenaihe, ja tutkijat ovat tutkineet tämän ongelman eri puolia. Stiegerin, Burgerin, Bohnin ja Voracekin (2012) tutkimuksessa käytiin syitä Facebookin lopettamiselle. Tutkimukseen osallistui 34000 ihmisistä ja 95.2 prosenttia heistä kommentoivat syyksi lopettaa Facebookin käytön, oli henkilötietojen käsittely ja tämän vaikutus yksityisyyteen. Krishnamurthyn ja Willsin (2009) artikkelissa on tarkasteltu olemassa olevien sosiaalisten verkostojen tietosuoja-asetuksia ja havaittu, että näillä sivustoilla voi olla riski vuotaa yksityisiä tietoja kolmansille osapuolille. Tästä voi siis todeta, että Facebook ei ole ollut yksin tämän ongelman kanssa. Muut tutkimukset ovat osoittaneet, että käyttäjillä on vaikeuksia käyttää monimutkaisia tietosuoja-asetuksia, eivätkä he mukauta esteettömyysasetuksiaan. Lisäksi huolestuttavaa on se, että monet käyttäjät eivät ole tietoisia tietosuojasta, eivätkä muuta oletustietosuoja-asetuksiaan (Sneed, 2020).

Tämä kandidaattitutkielma keskittyy siihen, miten henkilökohtaisen datan jakaminen ja käyttö Facebookissa voi näkyä käyttäjän yksityisyydessä. Lisäksi tutkielmassa tarkastellaan kolmansien osapuolten roolia Facebookissa, sekä miten kolmannet osapuolet ovat osana yksityisyyden vaarantamisessa. Tässä tutkielmassa pyritään vastaamaan seuraaviin tutkimuskysymyksiin:

- Mitä vaikutuksia Facebookin käytöllä on ollut käyttäjien yksityisyyden suojaan?
- Mikä on kolmansien osapuolten rooli Facebook käyttäjien yksityisyyden suojassa?

Kandidaattitutkielma koostuu viidestä sisältöluvusta, jossa toisessa luvussa määritellään sosiaalisen media ja Facebook. Nämä määritelmät antavat yleiskatsauksen yhdestä pääaiheesta. Toinen sisältöluku kattaa ne tiedot, joita Facebook pystyy mahdollisesti keräämään käyttäjiltä. Kolmannessa sisältöluvussa käsitellään yksityisyys käsiteenä, sekä mitä tarkoittaa henkilökohtainen data. Määritelmien lisäksi luvussa käsitellään Facebookin käytön vaikutuksia yksityisyyden suojaan. Neljännessä pääluvussa pyritään vastaamaan tutkimuskysymyksiin aikaisempia sisältölukuja hyödyntäen.

Tutkielma on toteutettu kirjallisuuskatsauksena. Lähdeaineistoa on kerätty Google Scholarista, Jykdokista, sekä Scopuksesta, joissa hakusanoina ovat toimineet ”sosiaalinen media”, ”Facebook”, ”personal data”, ”user privacy” sekä ”third parties”. Lähdeaineisto on keskittynyt enemmän vanhempiin lähteisiin ja aiheeseen liittyviin tapauksiin, sillä Facebook alustana on kehittynyt

tietoturvallisuudessa. Facebookiin liittyvät suuret tietovuodot ovat tapahtuneet useita vuosia sitten, joten niiden syitä ja seurauksia on hyvä tutkia, jotta tulevaisuudessa vastaavanlaisilta tapauksilta voitaisiin välttyä.

2 SOSIAALINEN MEDIA JA FACEBOOK

Tässä sisältöluvussa käsitellään keskeisiä käsitteitä kirjallisuuskatsaukseen liittyen. Sosiaalinen media on laaja käsite ja tämän tutkimuksen tarkastelun kohteena on siihen kuuluva Facebook. Tämä pääluku kattaa sosiaalisen median ja Facebookin määrittelyn lisäksi taulukon tiedoista, joita Facebook mahdollisesti kerää käyttäjillään.

2.1 Sosiaalisen median ja Facebookin määritelmät

Puhuttaessa sosiaalisesta mediasta esimerkiksi keskustelun yhteydessä, se voi herättää eri tunteita ja mielipiteitä. Sosiaalinen media käsitteenä on hyvin laaja ja ihmiset näkevät ja kokevat sen eri tavalla. Joillekin sosiaalinen media tarkoittaa tiettyä verkkoalustan sovellusta esimerkiksi Instagramia tai Facebookia, toiset ajattelevat sen viestintäkeinona ja joillekin siitä on tullut työalusta ja tulojen lähde.

Sosiaalisella medialla ei ole yhtä tiettyä määritelmää, mutta se on osa nykypäivää ja siitä on paljon keskustelua ympäri maailmaa. Kaplan & Haenlein (2010) määrittelevät sosiaalisen median ryhmäksi internet-pohjaisia sovelluksia, jotka rakentuvat Web 2.0:n ideologiselle ja teknologiselle perustalle. Web 2.0 –toimintojen ilmaantuminen ja nopea leviäminen uuden vuosituhannen ensimmäisellä vuosikymmenellä mahdollisti harppauksen verkonkäytön sosiaalisessa osassa (Kaplan & Haenlein, 2010). Tämä tarkoittaa, että ihmiset voivat tehdä yhteistyötä ja kommunikoida muiden kanssa verkossa sen sijaan, että he kuluttaisivat sisältöä passiivisesti (Carrn & Hayes, 2015). Kuten aikaisemmin todettiin, sosiaalinen media on laaja käsite ja se voidaan jakaa useisiin erityiskategorioihin niiden ominaisuuksien perusteella. Näihin luokkiin kuuluvat yhteistyöprojektit, blogit, sisältöyhteisöt, sosiaalisen verkostoitumisen sivustot, virtuaaliset pelimaailmat ja

virtuaaliset sosiaaliset maailmat. Yhteistyöprojektit viittaavat alustoihin, joissa ihmiset voivat työskennellä yhdessä yhteisissä projekteissa. Blogit tarjoavat ihmisille mahdollisuuden luoda ja jakaa kirjoitettua sisältöä. Sisältöyhteisöt ovat alustoja, joissa käyttäjät voivat jakaa ja käyttää multimediasisältöä, kuten esimerkiksi Youtube ja TikTok. Sosiaalisten verkostoitumisen sivustojen avulla ihmiset voivat olla yhteydessä muihin ja edistää verkkosuhteita. Virtuaaliset pelimaailmat ovat alustoja, joiden avulla käyttäjät voivat osallistua mukaansatempaaviin online-pelikokemuksiin. Viimeisenä virtuaaliset sosiaaliset maailmat mahdollistavat käyttäjien vuorovaikutuksen toistensa kanssa avatarien kautta simuloiduissa virtuaaliympäristöissä (Kaplan & Haenlein, 2010). Internet ja teknologia ovat ehtona sosiaaliselle median olemassaololle, mutta käyttäjät luovat lopulta sen luovan sisällön.

Facebook on laajalti käytetty sosiaalisen verkostoitumisen sivusto, joka on esimerkki Web 2.0-sovelluksesta. Sosiaaliset verkostoitumissivustot, kuten Facebook, ovat verkkopohjaisia alustoja, jotka yhdistävät erilaisia tekniikoita. Näin käyttäjät voivat luoda profiileja, olla yhteydessä muihin ihmisiin ja kommunikoida keskenään. Facebook, tarjoaa erilaisia media-, tieto- ja viestintätekniikoita, joiden avulla käyttäjät voivat olla yhteydessä toisiinsa ja jakaa tietoja (Fuchs, 2011).

Facebook on ollut ihmisten saatavilla jo vuodesta 2004 lähtien. Statista.com (katsottu 13.2.2023) mukaan tammikuussa 2023 sovelluksessa oli 2.963 miljardia aktiivista käyttäjää. Facebook kuuluu laajempaan Meta Platforms Inc. yritykseen, jossa toimivat sosiaalisen verkoston alustat: WhatsApp, Instagram, Messenger ja Horizon Worlds. Meta etenee perinteisten 2D-näyttöjen lisäksi mukaansatempaaviin kokemuksiin, kuten lisättyyn ja virtuaaliseen todellisuuteen. Tämä on osa heidän pyrkimyksiään luoda sosiaalisen teknologian seuraava taso (Meta, 2023).

Facebook käsittelee valtavia määriä dataa ja siihen sisältyy paljon henkilökohtaisia tietoja ihmisistä, esimerkiksi asuinpaikka, nimi, syntymäaika ja puhelinnumero. Vaikka sovellus on suosittu ja paljon käytetty, se on saanut paljon kritiikkiä muun muassa siitä, miten käyttäjätietoja käsitellään ja mitä vaikutuksia siitä on yksityisyydelle (Quan-Haase & Young, 2010). Tästä esimerkki on Cambridge Analytica -skandaali vuonna 2018, jossa paljastettiin, että miljoonia käyttäjätietoja oli kerätty ilman käyttäjien suostumusta (Fuller, 2019).

2.2 Facebookin tallentamat tiedot

Facebook kerää, tallentaa ja jakaa dataa päivittäin. Cameron Marlow, yksi Facebookissa työskentelevistä tutkijoista on pitänyt palvelua maailman tehokkaimpana välineenä ihmiskunnan tutkimiseen (Rieder, 2013). Facebookin keräämä datan määrä on huomattavan suurta. Sen perspektiiviin saamiseksi sovelluksen tallentama ja keräävä data, esimerkiksi vuonna 2012 on kuluttanut yhdeksästä prosentista 25 prosenttiin Kanadan ja Yhdysvaltojen Internet-liikenteestä. Tämä on kattanut kuvien lataamiset, tykkäykset ja muut toiminnot Facebookissa. Näiden lisäksi Facebookin käyttäjät useimmiten ovat tietämättömiä, miten yksi päivitys etusivulle tai uuden tykkäyksen lisääminen voi kulkea tuhansia kilometrejä internet-kanavissa useiden palvelinkeskusten lävitse (Hogan, 2015).

Kuka vain pystyy luomaan Facebookiin profiilin ja sen aavaiseksi sovellus vaatii käyttäjän nimen, sukupuolen, syntymäajan sekä puhelinnumeron tai sähköpostiosoitteen. Tilin aktivoiduttua, sovelluksesta löytyy yli 20 muuta erilaista attribuuttia, joita voidaan hyödyntää Facebookissa. Tähän sisältyy enemmän henkilökohtaisia tietoja, kuten asuinpaikka, työpaikka ja koulutus. Mitä enemmän Facebookista tulee käyttäjille ”oma henkilökohtainen päiväkirja”, niin profiilia voidaan täydentää omilla henkilökohtaisilla kiinnostustenkohteilla, esimerkiksi persoonallisuuden ominaisuuksilla tai poliittisilla taipumuksilla. Facebookiin ei tarvitse kuitenkaan syöttää enempää tietoja, mitä tilin luominen vaatii, mutta Facebook kannustaa henkilökohtaisten tietojen lisäämiseen, sillä nämä tiedot voidaan syöttää käyttäjän profiiliin. Jaettavista tiedoista voi olla vaikutuksia yksityisyyden suojaan, sekä vakaviin tietosuojaongelmiin (Farahbakhsh, Cuevas, Ortiz, Han, & Crespi, 2015.) Taulukko 1 kattaa tiedot, joita käyttäjät voivat lisätä profiilin avaamisen myötä (Limba & Šidlauskas, 2018.)

Työ ja koulutus	**Työ**. Yritys (Missä olet työskennellyt?), Asema (Mikä on työnimikkeesi?), Kaupunki/Kaupunki, Kuvaus, Aikakausi. **Ammatilliset taidot**, korkeakoulu, lukio – koulu (mitä koulua kävit?), aikajakso, valmistunut, kuvaus, keskittyminen, opiskelu (opisto tai tutkijakoulu).
Asuinpaikka	**Nykyinen sijainti ja kotipaikkakunta**
Yhteystiedot ja perustiedot	**Yhteystiedot:** Puhelinnumerot, sähköposti. **Perustiedot:** Syntymäaika, syntymävuosi, sukupuoli, kielet, kiinnostuksen kohteet uskonnolliset näkemykset, poliittiset näkemykset.
Perhe ja ihmissuhteet	**Suhdestatus:** Parisuhde (sinkku, parisuhteessa, kihloissa, naimisissa, siviililiitossa, parisuhteessa, avoimessa suhteessa, ”monimutkaista”, eronnut, leski). **Perheenjäsenet:** Perheenjäsen (tytär, poika, lapsi, äiti, isä, sisar, veli, Täti, setä, veljentytär, veljenpoika, tyttärentytär...).
Yksityiskohdat	**Tietoja sinusta** (kirjoita tietoja itsestäsi). **Muut nimet** (Lisää lempinimi, syntymänimi...). **Suosikkilainaukset** (Lisää suosikkilainauksiasi).
Elämän tapahtumia	**Elämän tapahtumia:** Työ ja koulutus, Perhe ja ihmissuhteet, Koti ja asuminen, Terveys ja hyvinvointi, Matkailu ja kokemukset.
Tykkäykset	**Tykkäykset:** Elokuvat, TV-ohjelmat, musiikki, kirjat, urheilujoukkueet, urheilijat, ihmiset, ravintolat, sovellukset ja pelit…
Muut tiedot	Ystävät, valokuvat, videot, tapahtumat, ryhmät...

Taulukko 1 Kooste Facebookin kattamista tiedoista, joita käyttäjä pystyy lisäämään itsestään profiilin avaamisen jälkeen (Mukaillen Limba & Šidlauskas, 2018).

3 HENKILÖKOHTAINEN DATA JA YKSITYISYYS

Tässä sisältöluvussa määritetään henkilökohtaisen datan ja yksityisyyden käsitteet. Henkilökohtainen data on suuressa roolissa tutkimuksessa, jonka vuoksi se on tärkeää määritellä. Yksityisyys on käsitteenä moninainen, joten sen määrittäminen on tärkeää tämän tutkimuksen kannalta. Luvussa tarkastellaan myös Facebookin käytön vaikutuksia yksityisyyden suojaan.

3.1 Henkilökohtaisen datan määritelmä

Teknologian nopea kehitys on tehnyt henkilökohtaisen datan määrittelystä monimutkaista ja sen laajuutta voi olla vaikea luonnehtia (Saglam, Nurse, & Hodges, 2022). Teknologian kehitys on tuonut monia etuja yhteiskunnallemme, mutta sillä on ollut merkittävä vaikutus ihmisten yksityisyyteen. Nykyään henkilökohtaisia tietoja kerätään, käsitellään, jaetaan ja levitetään, mukaan lukien väestötiedot, lääketieteelliset tiedot, sähköpostit, valokuvat, videot ja sijaintitiedot. Näiden tietojen keräämiseen ja jakamiseen on useita syitä, kuten tutkimustai tilastotarkoitukset, palvelujen tehokkaampi tarjoaminen, sekä personisoitu mainonta. Henkilötietojen jakaminen voi kuitenkin vaarantaa henkilöiden yksityisyyden suojan ja se herättää kysymyksiä, miten henkilökohtaisia tietoja tulisi kerätä, käsitellä ja suojata (Phelps, Nowak & Ferrell, 2010).

Teknologian kehityksen myötä henkilökohtaisista tiedoista on tullut arvokas resurssi. Se on kuin valuutta, jolla on merkittävää rahallista arvoa, jota yritykset pyrkivät hyödyntämään. Yritykset pitävät henkilökohtaista dataa arvokkaana resurssina ja käyttävät erilaisia ohjelmistoja kuluttajatietojen keräämiseen (Schwartz, 2004). Tietosuojavaltuutetun toimisto (2023) määrittelee henkilökohtaisen datan niin, että kaikki tiedot, jotka koskevat suoraan tai välillisesti tunnistettavissa olevaa henkilöä ovat henkilötietoja. Tämä sisältää tiedot, jotka

yhdistettynä muuhun informaatioon voivat johtaa henkilön tunnistamiseen. Esimerkiksi henkilön nimeä, henkilötunnusta tai mitä tahansa muuta tunnistetietoa voidaan käyttää tietojen linkittämiseen kyseiseen henkilöön.

Henkilökohtaisen datan arvo ennen teknologian ja eri alustojen nousukautta ei ole ollut yhtä arvokasta, eikä tietoihin kiinnitetty yhtä paljoa huomiota. Nykyään vähittäiskauppiaille, valmistajille, palveluntarjoajille ja voittoa tavoittelemattomille järjestöille on tullut yleinen käytäntö kerätä ja käyttää kuluttajakohtaista tietoa (Phelps ym., 2010). Lupton (2018) artikkelissaan tuo esille, että henkilökohtaisesta datasta on tullut merkittävä tekijä ihmisten jokapäiväisessä elämässä ja se muokkaa ihmisten käyttäytymistä ja identiteettiä. Teknologian rooli on huomattavassa roolissa, sillä henkilökohtaisen datan käyttö on levinnyt esimerkiksi kolmansille osapuolille ja niiden käyttö ei ole enää helposti ihmisten hallittavissa.

Maailman digitalisoituessa henkilökohtaisen datan kerääminen, tallentaminen sekä analysointi on helpompaa, kuin koskaan aikaisemmin. Nykyään on usein annettava henkilökohtaisia tietoja käyttääkseen palveluita ja tuotteita, kuten sosiaalisen median alustoja, verkkokauppasivustoja sekä terveys- ja kuntosovelluksia. Nämä alustat käyttävät henkilötietojamme luodakseen yksilöllisiä kokemuksia, tarjotakseen kohdennettuja mainoksia ja suositellakseen eri personoituja tuotteita. Alustat keräävät ja tutkivat henkilökohtaisia tietoja saadakseen tietoa mieltymyksistä ja kiinnostuksen kohteista, jonka kautta he voivat tarjota räätälöidymmän ja nautinnollisemman kokemuksen. Ihmiset saattavat joutua joissain tapauksissa kysymään, missä määrin heidän tietonsa puhuvat heidän puolestaan (Lupton, 2018). Kun henkilötietoja käytetään laajasti, sen aiheuttamista turvallisuus- ja tietosuojariskeistä ollaan huolissaan. Hakkerit ja muut pahantahtoiset tahot voivat päästä laittomasti käsiksi henkilötietoihin kyberhyökkäysten ja tietoturvaloukkausten kautta. Lisäksi sekä valtiot, että yksityiset yritykset voivat käyttää henkilötietoja esimerkiksi valvontatarkoituksiin, joihin henkilöt eivät välttämättä ole suostuneet tai eivät ole heidän tiedossansa. Siksi henkilöiden tulee olla tietoisia henkilötietojensa jakamisen mahdollisista vaaroista ja ryhtyä tarvittaessa toimenpiteisiin suojellakseen henkilötietojaan. Toimenpiteisiin sisältyy vahvojen salasanojen käyttö, kaksivaiheisen todennuksen mahdollistaminen ja verkossa paljastamiensa tietojen huomioiminen. Tahosta riippumatta kaikkien henkilökohtaisen datan käsittelijöiden on velvollisuus kerätä, tallentaa ja käyttää henkilötietoja vastuullisesti ja eettisesti, sekä riittävät turvatoimenpiteet luvattoman pääsyn ja väärinkäytön estämiseksi (Purtova, 2018).

3.2 Yksityisyyden määritelmä

Yksityisyys on monimutkainen ja joustava käsite, jolla on monia erilaisia merkityksiä eri aloilla, kuten filosofiassa, laissa ja jokapäiväisessä elämässä. Erilaiset näkemykset yksityisyyden rajoista ovat johtaneet erimielisyyksiin siitä, pitäisikö yksityisyyden suojata vain moraalisesti neutraalia tai sosiaalisesti arvostettua käyttäytymistä, vai voiko se suojata myös moraalitonta toimintaa (Lukács, 2016). Yksityisyyden suojan tulisi olla jokaisen perusoikeus, mutta se ei päde kuitenkaan kaikissa tilanteissa. Esimerkiksi mediat uutisoivat rikoksen tehneistä henkilöistä, jotka ovat toimineet moraalittomasti. Näiden henkilöiden yksityisyyttä loukataan, kun heidän henkilökohtaisia tietojaan jaetaan suurelle yleisölle, luultavasti vielä ilman henkilön suostumusta.

Yksityisyyden määrittelemisestä on luotu useita teorioita ja yksi niistä on Westinin (1968), joka esiteltiin ensimmäisen kerran vuonna 1968 ja käsittelee, kuinka ihmiset suojelevat itseään rajoittamalla muiden pääsyä omiin tietoihin ja arvoihin rajoitetun ajan. Westin kehitti puitteet yksityisyyden ymmärtämiseksi kolmella tasolla: poliittisella, sosiokulttuurisella ja henkilökohtaisella tasolla. Tämän viitekehyksen ytimessä on yksilö, ja yksityisyys voidaan nähdä eräänlaisena "suojakuplana" henkilön ympärillä, joka määrittää rajan hänen ja ulkomaailman välillä. Tämä kupla ei kuitenkaan ole kiinteä, ja se voi muuttua kontekstin ja osallistuvan henkilön mukaan. Westinin (1968) mukaan yksityisyys on yksilöiden, ryhmien tai instituutioiden oikeutta valvoa itseään koskevien tietojen luovuttamista, mukaan lukien milloin, miten ja missä määrin sitä jaetaan muille. Lisäksi yksityisyys on henkilön tilapäinen ja vapaaehtoinen vetäytyminen laajemmasta yhteiskunnasta, joka saavutetaan fyysisin tai psykologisin keinoin. Altman (1990), on tutkinut yksityisyyden käsitettä eri näkökulmista ja kuten Westin, hän tarkastelee yksityisyyttä yksilön ja ryhmän käyttäytymisen sekä yksityisyyttä säätelevien mekanismien kannalta, jotka toimivat yhdessä yhtenäisessä järjestelmässä. Altman (1977) näkee yksityisyyden säätelyn dynaamisena ja dialektisena prosessina, mikä tarkoittaa, että henkilöiden vuorovaikutus muiden kanssa muuttuu sitä myötä, kuinka avoimia tai suljettuja muut henkilöt ympärillä ovat. Altmanin teoria korostaa yksityisyyden sosiaalista luonnetta, ihmisten vuorovaikutusta, heidän sosiaalista maailmaansa, fyysistä ympäristöään ja yksityisyyden kulttuurista kontekstia. Kuten aiemmin mainittu, yksityisyys on käsitteenä muuttuva ja se voi tarkoittaa henkilöille eri asioita. Se mikä yhdistää näitä kahta teoriaa yksityisyydestä on sen moniulotteisuus ja muuttuvuus.

3.3 Yksityisyyden suojaan vaikuttavat tekijät Facebookissa

Facebookin käyttäjät pystyvät lisäämään henkilökohtaisia tietojaan sovellukseen, esimerkkinä aiemmin läpikäyty taulukko 1. Facebook ei kuitenkaan pakota käyttäjiään lisäämään enempää tietoja, kuin sovellukseen pääseminen vaatii, mutta siihen kannustetaan.

Facebookin ja käyttäjän välinen suhde yksityisyyteen on paljon käyttäjästä kiinni, sillä käyttäjällä on paljon päätösvaltaa siihen, mitä tietoja sovellukseen annetaan. Grossin & Acquistin (2005) mukaan, todellisten tietosuojariskien uskotaan syntyvän, kun käyttäjät paljastavat tunnistettavia tietoja itsestään verkossa ihmisille, joita he eivät tunne tai joihin he eivät normaalisti luottaisi. Nämä ei luotettavat käyttäjät voivat käyttää hyväksi ”kaverin” tietoja, esimerkiksi kuvia tai nimeä. Näillä tiedoilla käyttäjä voi joutua identiteettivarkauden tai vainoamisen uhriksi. Tästä voidaan todeta, että Facebook voi toimia myös kolmantena osapuolena, jossa käyttäjäien oma toiminta mahdollistaa riskejä yksityisyyden suojalle. Grossin ja Acquistin (2005) ovat luetelleet kolme sidosryhmäryhmää, jotka mahdollisesti pääsevät käsiksi osallistujien henkilötietoihin sosiaalisessa verkostossa: Facebook, verkosto ja kolmannet osapuolet. Facebookilla on pääsy osallistujien tietoihin ja se voi käyttää ja laajentaa tietoja eri tavoin. Käyttäjä voi paljastaa tiedot sekä tietoisesti, että tietämättään. Kun haitalliset kolmannet osapuolet pääsevät käsiksi henkilötietoihin, yksityisyyteen liittyvät lisäriskit tulevat todellisiksi. Sosiaalisen verkostoitumisen sivustoihin liittyvät tietosuojahuolet ovat kuitenkin vieläkin merkittävämpiä, sillä ne voivat vaikuttaa ihmisen minäkuvaan ja julkiseen identiteettiin. Yksityisyyden ja henkilötietojen hallinnan menettäminen voi johtaa sosiaalisesti korjaamattomiin vahinkoihin, kuten ystävien kunnioituksen menettämiseen, salaisuuksien paljastamiseen, sosiaalisten virheiden tekemiseen tai väärän vaikutelman luomiseen (Gross & Acquisti, 2005). Erityisen vakavia näistä uhista tekee se, että yleisössä on usein ihmisiä, joiden kanssa ollaan usein vuorovaikutuksessa fyysisessä maailmassa. Tämän seurauksena näillä uhilla voi olla vakavia seurauksia yksilölle, kuten heikentää hänen ammatillista mainettansa tai sosiaalista asemaa.

4 KOLMANNET OSAPUOLET MUKANA FACEBOOK KÄYTTÄJIEN YKSITYISYYDESSÄ

Tässä sisältöluvussa perehdytään syvemmin tutkimuskysymyksiin, eli miten Facebookin käyttö on vaikuttanut yksityisyyteen, sekä taustaa siitä, miten henkilökohtaisen datan käyttö kolmansien osapuolten toimesta vaikuttaa yksityisyyden suojaan. Luku käsittelee henkilökohtaisen datan ja yksityisyyden näkökulmia kolmansien osapuolten kautta, sekä minkälaisia kolmansia osapuolia ovat tietovuodot ja evästeet. Luvun lopussa Taulukko 2 tiivistää Facebookin käytön vaikutukset yksityisyyden suojalle.

4.1 Kolmansien osapuolten rooli Facebookissa

Kolmannen osapuolen palveluilla on tärkeä rooli verkossa, koska niiden avulla ensimmäisen osapuolen verkkosivustot voivat ottaa käyttöön ominaisuuksia, kuten mainontaa, analytiikkaa ja sosiaalisten verkostojen integrointia. Facebookin kolmannen osapuolen verkkosivustojen käyttö on herättänyt myös huolta käyttäjien yksityisyydestä (Mayer & Mitchell, 2012). Chaabanen, Dingin, Deyin, Kaafarin ja Rossin (2013) tutkimuksessa, kolmannen osapuolen sovellusten tietosuojaongelmia ilmenee useista syistä. Ensinnäkin näiden sovellusten koodia hallitaan usein julkaisijan omilla palvelimilla, jotka eivät ole Facebookin hallinnassa. Tämän vuoksi Facebookin on vaikea valvoa tai hallita sovelluksen toimintaa, mikä vaikeuttaa haitallisten toimintojen estämistä. Toiseksi, kun käyttäjätietoja siirretään Facebookin palvelimilta kolmansien osapuolien sovelluksiin, käyttäjät mahdollisesti menettävät hallinnan siihen, miten heidän tietojaan käytetään ja jaetaan. Lopuksi kolmannen osapuolen sovellusten tietosuojasäädöt ovat usein rajallisia johtuen lupien karkeasta tarkkuudesta, ja sovellukset voivat näin mahdollisesti käyttää enemmän tietoja ja toimintoja, kuin ne todellisuudessa

tarvitsisivat aiotun tehtävän suorittamiseen. Tämä herättää kysymyksiä siitä, onko tämä lähestymistapa linjassa "minimioikeuksien periaatteen" kanssa, joka viittaa siihen, että vain vaadittavat vähimmäisoikeudet tulisi myöntää käsillä olevan tehtävän suorittamiseksi. Symeonidisin, Biczókin, Shirazin, Pérez-Solàn, Schroersin ja Preneelin (2017) artikkeli korostaa myös sitä, että Facebookin ulkopuoliset sovellukset, kuten suosittu Candy Crush Saga- peli, on esimerkki kolmansien osapuolen sovelluksista. Tämä ja muut sovellukset ovat olleet saatavilla Facebookin Developers Platformissa, jotka voivat käyttää henkilökohtaisia tietoja, kun käyttäjä asentaa sovelluksen. Ongelmana on, kun käyttäjän kontakti asentaa sovelluksen, se voi kerätä tietoja niin käyttäjästä, kuin hänen kontakteistaan ilman käyttäjien tietämystä tai suostumista.

Facebook toimii myös mainostajille loistavana alustana vaikuttaa kuluttajiin. Nämä kolmannet osapuolet saavat paljon henkilökohtaisia tietoja evästeiden kautta ja kohdistavat tuotteitaan personoiduilla sisällöllä ja mainoksillaan (Arias-Cabarcos, 2023). Perinteiset verkkosivustomainokset toimitetaan enimmäkseen bannerimainosten tai sponsoroitujen linkkien kautta, jotka tunnistetaan selkeästi markkinointiviestintäviesteiksi. Facebook-mainonta eroaa kuitenkin perinteisestä verkkosivustomainonnasta, koska Facebook-mainoksia ei usein voida erottaa käyttäjien sisällöstä. Useimmat Facebook-mainokset ovat suunniteltu muistuttamaan tyypillistä viestiä, mikä tekee Facebookin käyttäjien vaikeaksi erottaa mainonnan ja muun tyyppisen käyttäjien luoman sisällön (Srinvasan, 2019). Denin ja Imisen, (2018) tutkimuksessa on käynyt ilmi, että kolmannen osapuolten mainostajat saattavat olla jopa töykeitäkin hankkiessaan henkilökohtaista tietoa käyttäjiltä. Käyttäjän suostuessa jakamaan tietonsa, hän ei välttämättä ole tietoinen kaikista yksityiskohdista, sekä miten tietoja käytetään. Tämä voi johtaa epämääräisyyteen henkilötietojen käytön merkityksessä. Käyttäjä voi esimerkiksi haluta piilottaa Facebookilta tietyt arkaluontoiset tiedot, kuten poliittiset näkemyksensä, eikä välttämättä halua, että näitä tietoja käytetään mainontaan. Facebook on saattanut kuitenkin pystyä päättelemään nämä tiedot muista lähteistä ja käyttämään niitä mainontaan ilman, että käyttäjä tietää, mitä tietoja ja kolmansia osapuolia tiedot koskevat. Tämä tarkoittaa, että käyttäjä voi antaa vain yleisen suostumuksen kaikkeen mahdolliseen tietojensa käyttöön tietämättä tarkkoja yksityiskohtia niiden käytöstä (De & Imine, 2018).

4.2 Kolmansien osapuolten evästeet Facebookissa

Evästeiden käyttö internetin käyttäjien tunnistamiseen ja seurantaan on ollut pitkään käytössä. Kolmannen osapuolen evästeiden sallimiseksi on annettava lupa lisätä sisältöä verkkosivustolle. Kolmannen osapuolen sisältö pyydetään heidän palvelimeltaan ja toimitetaan evästeen mukana. Käyttäjän vieraillessaan uudelleen verkkosivustolla, eväste lähetetään sisältöpyynnön mukana. Näin sisällöntuottajat voivat muistaa verkon käyttäjien mieltymykset, kuten kieliasetukset tai ostohistorian ja räätälöidä verkkosisältöä niiden mukaisesti (Roosendaal, 2012).

Facebook käyttää kahdenlaisia evästeitä: ensimmäisen osapuolen evästeitä ja kolmannen osapuolen evästeitä. Ensimmäisen osapuolen evästeet ovat Facebookin luomia ja niitä käytetään tallentamaan tietoja, kuten kirjautumistiedot, henkilökohtaiset mieltymykset sekä käyttäjän toiminta Facebookissa. Kolmannen osapuolen evästeet luovat muut verkkosivustot. Nämä evästeet seuraavat käyttäytymistä eri verkkosivustoilla ja niitä voidaan käyttää esimerkiksi kohdistettujen mainosten esittämiseen Facebookissa (Roosendaal, 2012). Facebookin evästekäytännöt ovat muuttuneet paljon sen perustamisesta. Aluksi Facebook ilmoitti, että ei käytä evästeitä seurantaan ja tarjosi avoimuutta evästeiden käytöstä (Srinivasan, 2019.) Facebook siirtyi kiinnostuksiin perustuvaan mainontaan, ensin vuonna 2014 käyttäjilleen ja myöhemmin vuonna 2016 muille käyttäjille. Toisin sanoen Facebook alkoi seuraamaan ja profiloimaan ihmisten verkkotoimintaa verkossa. Tämän seurauksena tietosuojaviranomaiset alkoivat tutkia, kuinka Facebook käytti evästeitä mahdollisesti seuratakseen ihmisten toimintaa (Dimova, Franken, Le Pochat, Joosen & Desmet 2022). Chaabanen ym., (2012) artikkelissa on tutkittu sitä, miten kolmannen osapuolten evästeet seuraavat jatkuvasti ja tarkasti käyttäjien toimintaa verkossa. Artikkelin julkaisemisen aikaan Facebook käytti 16 evästettä aktiivisen istunnon aikana ja jokaisen tarkka rooli on vaikea erottaa. Kaksi näistä evästeistä - *d_atr ja c_user* - on kuitenkin suunniteltu erityisesti käyttäjien tunnistamiseen. D_*atr*-eväste koostuu satunnaisesta 24-merkkisestä merkkijonosta, ja se luodaan, kun käyttäjä vierailee Facebookin sivuilla. Vaikka käyttäjällä ei olisi Facebook-tiliä, hän saa silti tämän evästeen, jos hän on aiemmin vieraillut verkkosivustolla. *D_atr*-eväste on voimassa kaksi vuotta, mikä osoittaa, että Facebookilla on mahdollisuus seurata kaikkia sivustolla käyneitä käyttäjiä, myös niitä, jotka eivät ole rekisteröityneet palveluun pidemmän aikaa. Nämä käyttäjän "menneisyydestä" saadut tiedot voidaan mahdollisesti yhdistää hänen tiliinsä, kun hän lopulta rekisteröityy käyttämällä ainutlaatuista verkkoselainta. Kolmansien osapuolten evästeet voivat vaikuttaa käyttäjien yksityisyyden suojaan usealla tavalla. Evästeet voivat seurata Facebook käyttäjiä pitkään, johon liittyy muun muassa verkon selaushistoria. Tämä

voi luoda käyttäjässä epätietoisuutta henkilökohtaisen datan käytöstä ja käyttäjä voi kokea hallinnan puutetta. Käyttäjän selaushistoria liittyy läheisesti hänen henkilötietoihinsa. Sivustot, joilla käyttäjä vierailee, voivat paljastaa hänen sijaintinsa, kiinnostuksensa, ostonsa, työllisyystilanteensa, taloudelliset vaikeutensa, sairaudet ja paljon muuta. Jopa yksittäisten ladattujen sivujen tutkiminen riittää usein useiden päätelmien tekemiseen käyttäjästä (Mayer & Mitchell, 2012).

Roosendaalin (2011) artikkelissa esimerkki evästeiden käytöstä kolmansien osapuolten toimesta on Facebookin Tykkää -painike. Se on esimerkki työkalusta, jolla sisällöntuottajat voivat houkutella vierailijoita ja lisätä verkkokattavuutta. Tykkää-painiketta voidaan kuitenkin käyttää myös evästeiden asettamiseen ja käyttäjien seuraamiseen, vaikka he eivät käyttäisikään painiketta. Tämä voi luoda profiilin henkilön selauskäyttäytymisestä, joka voidaan liittää hänen Facebook-tiliinsä tai käyttää erillisen tietojoukon luomiseen. Roosendaalin (2011) mukaan, evästeiden ja yksilöllisten tunnistenumeroiden avulla Facebook voi mahdollisesti ottaa yhteyden jokaiseen verkon käyttäjään ja seurata heidän selauskäyttäytymistään. Tämä herättää huolta yksityisyydestä ja on ristiriidassa sen ajatuksen kanssa, että yksilöiden pitäisi hallita omia henkilötietojaan. Käytäntö on herättänyt huolta käyttäjien yksityisyyden suojasta. Facebookin ”tykkää”-painike, saattaakin olla Facebookin suurin keräämä tiedon lähde (Roosendaal, 2011).

Firen, Goldschmidtin ja Elovicin (2019) artikkelissa, on käsitelty erilaisia uhkia, joita käyttäjät kohtaavat käyttäessään sosiaalisen verkoston palvelemia, mukaan lukien Facebookia. Huolia ilmenee yksityisyyden loukkauksista, identiteettivarkauksista, sekä verkkokiusaamisesta. Artikkeli on jakanut sosiaalisten verkostojen uhat neljään eri kategoriaan, joita ovat klassiset uhat, nykyaikaiset uhat, yhdistelmäuhat sekä uhat, jotka kohdistuvat nuorempaan sukupolveen ja käyttävät sosiaalisia verkostoja. Kolmansien osapuolten näkökulmasta keskitytään enemmän nykyaikaisiin uhkiin, jotka keskittyvät sosiaalisten verkostojen infrastruktuuriin. Tähän kategoriaan kuuluu pienempiä kokonaisuuksia uhista ja yksi niistä on anonymisointihyökkäykset (de-anonymization attacks). Anonymisointihyökkäykset viittaavat tekniikoihin, joita käytetään sellaisten käyttäjien todellisen identiteetin paljastamiseen, jotka käyttävät pseudonyymejä (käyttäjänimijä) yksityisyytensä ja nimettömyytensä suojaamiseen sosiaalisen verkoston palveluissa. Nämä hyökkäykset käyttävät erilaisia menetelmiä, kuten seurantaevästeitä, verkkotopologiaa ja käyttäjäryhmien jäsenyyksiä paljastaakseen käyttäjän todellisen henkilöllisyyden. Tutkijat ovat osoittaneet, että kolmannet osapuolet voivat linkittää sosiaalisten verkostojen kautta vuotaneita tietoja paljastaakseen sosiaalisten verkoston käyttäjien identiteetit. Tällaiset hyökkäykset voivat vaarantaa useimpien käyttäjien yksityisyyden, koska he ovat alttiina

henkilötietojensa vuotamiselle seurantamekanismien, kuten seurantaevästeiden kautta (Fire ym., 2009).

Miksi Facebookin käyttäjät sitten jakavat henkilökohtaisia tietoja ja dataa kolmansille osapuolille ja hyväksyvät evästeet. Sneedin, (2020) artikkeli on tutkinut Facebookin läpinäkyvyyttä, joka voi olla yksi syy tälle. Facebookin tietojen läpinäkyvyys on ollut yksi suurimmista haasteista. Käyttäjät vaativat sääntelyä, koska he ovat huolissaan siitä, mitä heidän tiedoilleen tapahtuu, kun he toimittavat ne alustalle. Monet kuluttajat ovat huolissaan tietojensa läpinäkyvyyden ja hallinnan puutteesta. Tietovuodot, sekä väärien tilien luomiset ovat edelleen heikentäneet käyttäjien luottamusta Facebookin kykyyn suojata heidän tietojaan ja todentaa tilinsä. Tämä on johtanut käyttäjien luottamuksen laskuun, ja monet ovat ilmaisseet epävarmuutta henkilötietojensa turvallisuudesta alustalla (Sneed 2020). Sneedin (2020) julkaistussa artikkelissa evästeiden käytöstä käy ilmi, että käyttäjät usein hyväksyvät evästeet rutiininomaisesti ja eivät kiinnitä huomiota niihin sen enempää. Myös avoimuuden puute ja vaikeasti ymmärrettävät käyttöehdot voivat olla syitä siihen, että evästeet hyväksytään ja kolmannet osapuolet saavat näin arvokasta dataa käyttäjiltä. Lisäksi sovelluksen käyttäjän lähtökohdat kuten ikä voi olla yksi syy henkilökohtaisten tietojen jakamiselle. Brandtzægin, Lüdersin ja Skjetnen (2010) artikkelissa tutkittiin Facebookiin sisällön jakamisesta sekä miten se, miten se vaikuttaa henkilön yksityisyyteen käyttäjän iän näkökulmasta. Tutkimuksen kohteena vertailtiin nuorten ja vanhempien Facebook-käyttäjien kokemuksia ja käyttöä. Facebook tarjoaa käyttäjille tietosuojavalintoja, joilla he voivat säännellä sisältönsä jakamista. Tutkimukset ovat kuitenkin osoittaneet, että monet käyttäjät eivät käytä näitä säätimiä oikein. Lisäksi sosiaalistenverkkojen käyttöliittymä ei useinkaan ota kunnolla huomioon tietosuojaongelmia. Tulokset osoittavat, että nuoremmat ihmiset ovat vanhempiin verrattuna ammattitaitoisempia Facebookin käyttäjiä. Nuorempien ihmisten Facebookin käyttö on myös tarkoituksenmukaisempaa, sillä sähköposti, pikaviestit ja tekstiviestipalvelut ovat suurelta osin syrjäytyneet Facebookin käytön myötä (Brandtzægin ym, 2010).

4.3 Kolmansien osapuolten tietovuodot Facebookissa

Facebook, kuten monet muut teknologiayritykset, luottavat kolmansien osapuolien toimittajiin ja kehittäjiin tarjotakseen lisäominaisuuksia ja palveluita käyttäjilleen. Näillä kolmannen osapuolen toimittajilla ja kehittäjillä on usein pääsy Facebookin käyttäjätietoihin, kuten profiilitietoihin ja sosiaalisiin yhteyksiin. Jos

kolmannen osapuolen toimittaja tai kehittäjä kokee tietomurron tai muun tietoturvaongelman, Facebook-käyttäjätiedot, joihin heillä on pääsy, voivat vaarantua (Kavianpour, Ismail & Shanmugam, 2017).

Yksi uhkaavimmista yksityisyyden suojaan liittyvistä ongelmista Facebookissa ovat tietovuodot. Vuodesta 2005 tietovuodot ovat jopa kolminkertaistuneet kehittyneen tekniikan myötä, sillä datan kerääminen ja jakaminen on tehokkaampaa ja helpompaa. Sosiaalinen media on datan avainpaikka ja ihmiset jakavat itsestään henkilökohtaisia asioita, jotka voivat lopulta päätyä toisiin käsiin (Liun ym., 2018). Tietovuodot ovat yhä yleisempiä ja yhä useammat yritykset kokevat tietovuotoja, jotka vaarantavat arkaluonteisia tietoja. Näillä rikkomuksilla voi olla vakavia seurauksia, kuten taloudellisia menetyksiä, maineen vahingoittumista ja oikeudellista vastuuta (Cheng, Liu & Yao 2015). Tietovuoto tapahtuu, kun luvaton taho pääsee käsiksi arkaluontoisiin tai luottamuksellisiin tietoihin (Peretti, 2008). Tietovuotojen motiivit voivat johtua eri syistä, kuten hakkeroinnista, tietojenkalasteluhyökkäyksistä, haittaohjelmista tai jopa yksinkertaisista inhimillisistä virheistä, kuten kannettavan tietokoneen väärin sijoittamisesta tai arkaluonteisten tietojen jättämisestä näkyville julkisilla alueilla (Cheg ym., 2015). Kun tietoturvaloukkaus tapahtuu, se voi vaarantaa henkilökohtaisten ja luottamuksellisten tietojen yksityisyyden ja turvallisuuden, mukaan lukien taloudelliset tiedot, henkilötiedot, terveystiedot ja muita yksityisyyteen liittyviä tietoja. Tämä voi johtaa identiteettivarkauksiin, taloudellisiin petoksiin ja muihin vakaviin seurauksiin (Kavianpour ym., 2017).

Esimerkki Facebookin tietovuodosta on Cambridge Analytica- skandaali, jossa sovelluksen käyttäjien henkilökohtaista dataa oli käytetty heidän tietämättään. Maaliskuussa 2018 paljastettiin, että poliittinen konsulttiyritys Cambridge Analytica oli hankkinut jopa 87 miljoonan Facebook-käyttäjän henkilötiedot ilman heidän suostumustaan. Tiedot kerättiin "This Is Your Digital Life" -sovelluksella, jonka on kehittänyt tutkija nimeltä Aleksandr Kogan. Koganin sovellusta käytti noin 270 000 Facebook-käyttäjää, jotka suostuivat jakamaan tietojaan itsestään. Sovellus kuitenkin keräsi tietoja myös näiden käyttäjien ystävistä, vaikka nämä ystävät eivät olisi antaneet suostumustaan. Tämän ansiosta Cambridge Analytica- yritys pystyi keräämään tietoja kymmenistä miljoonista Facebookin käyttäjistä. Näitä vuotaneita tietoja käytettiin muun muassa poliittisten kampanjoiden auttamiseksi vuoden 2016 Yhdysvaltojen vaaleissa, mukaan lukien Donald Trump (Venturini & Rogers, 2019).

Toinen Facebookin tietovuoto tapahtui 2019, joka kosketti myös yli miljoonaa suomalaista. Kyseisessä tapauksessa 500 miljoonan Facebook-käyttäjän henkilötiedot vuotivat nettiin. Vuotaneet tiedot sisälsivät käyttäjien puhelinnumeroita, sähköpostiosoitteita, syntymäpäiviä ja muita henkilökohtaisia tietoja. Tämä oli merkittävä rikkomus, joka herätti huolta Facebookin käyttäjien tietojen

turvallisuudesta ja sai yrityksen ryhtymään toimiin tietosuojatoimenpiteiden parantamiseksi (Traficom, 2023). Molemmat yllä olevista tapauksista linkittyvät valtavan mittakaavan tietovuotoihin. Facebookin tietovuotoskandaaleissa on useita yhteisiä piirteitä. Ensinnäkin ne kaikki sisältävät luvattoman pääsyn käyttäjätietoihin ilman käyttäjän suostumusta, kuten Peretti (2008) artikkelissaan kertoi. Lisäksi ne kaikki liittyvät Facebookin turvajärjestelmien haavoittuvuuksien hyödyntämiseen. Tämä riski puoltaa Chaabanen ym., (2013) artikkelia, sillä näiden sovellusten koodia isännöidään usein julkaisijan omilla palvelimilla, jotka eivät ole Facebookin hallinnassa. Tämänkaltaiset tapaukset heikentävät käyttäjien luottamusta Facebookiin, mikä on mahdollisesti johtanut käyttäjien sitoutumisen ja luottamuksen laskuun alustaa kohtaan, kuten Sneed, (2020) aiemmin kertoi. Lopuksi joissakin tapauksissa Facebookin vastaus tietoturvaloukkauksiin on ollut myös paikoitellen hidasta tai riittämätöntä, mikä johti käyttäjien, sääntelyviranomaisten ja tiedotusvälineiden kritiikkiin (Sneed, 2020).

4.4 Facebookin käytön vaikutukset yksityisyyden suojaan

Facebookin käytön vaikutuksia yksityisyyteen on tarkasteltu usean tutkimuksen kautta ja taulukossa 2 ne ovat koottu yhteen.

Mahdolliset riskit	**Vaikutukset yksityisyyteen**	**Lähteet**
Käyttäjien välinen, sekä oma toiminta-Facebookissa	- Identiteettivarkaudet - Vainoaminen - Tietojenkalastelu - Roskaposti	Grossin & Acquistin, (2005);
Kolmannen osapuolen sovellukset	- Henkilökohtaisen datan käyttö - Hallinnan puute	Denin & Imisen, (2018); Mayer & Mitchell, (2012);
Kolmannen osapuolen evästeet	- Evästeiden pitkä seuranta-aika - Verkkotoiminnan seuranta - Hallinnan puute	Chaabane ym., (2012); Mayer & Mitchell, (2012); Dimova ym., (2022);
Kolmannen osapuolen tietovuodot	- Henkilökohtaisen datan vuotaminen - Identiteettivarkaudet - Henkilökohtaisen datan väärinkäyttö	Cheng ym., (2015); Kavianpour ym., (2017); Peretti, (2008);

	- Taloudelliset, sekä sosiaaliset menetykset	

TAULUKKO 2 Facebookin käytön vaikutukset yksityisyyden suojaan.

Facebookin käyttö ja henkilökohtaisen datan jakaminen sovellukseen antavat mahdollisuuden siihen, että yksityisyyden suoja on uhattuna. Grossin & Acquistin (2005) mukaan, käyttäjän oma toiminta sovelluksessa vaikuttaa paljon, mitä riskejä yksityisyyden suojaan kohdistuu. Facebook on avoin alusta kaikille, joten sovellukseen mahtuu myös epärehellisiä ihmisiä. Taulukon ensimmäinen mahdollinen riski yksityisyyden suojalle on käyttäjien välinen toiminta, jossa käyttäjät saattavat hyväksyä kaverikseen epäluotettavia henkilöitä, jotka siten hyödyntävät heidän henkilökohtaista dataansa. Tämän lisäksi käyttäjän oma toiminta henkilökohtaisen datan jakamisessa vaikuttaa siihen, mitä tietoja käyttäjästä voidaan kerätä. Tästä voi seurata identiteettivarkauksia, vainoamista, tietojenkalastelua sekä roskapostia.

Taulukon toinen mahdollinen riski yksityisyyden suojalle ovat kolmannen osapuolen sovellukset. Nämä sovellukset ovat kolmannen osapuolen yritysten tai yksityishenkilöiden kehittämiä ohjelmistosovelluksia, jotka ovat integroitu Facebookin kanssa. Käyttäjän asennettuaan kolmannen osapuolen sovelluksen, häntä voidaan vaatia myöntämään sovellukselle pääsy Facebook-tilitietoihinsa, jonka kautta sovellus pääsee käsiksi käyttäjän henkilökohtaisiin tietoihin (De & Imine, 2018). Tästä voi seurata käyttäjälle hallinnan puutetta omia tietojaan kohtaan. On siis tärkeää, että ladattu sovellus on luotettava, sillä jotkin kolmannen osapuolen sovellukset sisältävät haavoittuvuuksia, joita hakkerit voivat hyödyntää päästäkseen käsiksi henkilökohtaisiin tietoihin.

Taulukon kolmas kohta ja mahdollinen riski yksityisyyden suojalle ovat kolmansien osapuolten evästeet. Tutkimuksista käy ilmi, että evästeiden hyväksyminen ei näy yksityisyyden suojassa välittömästi, vaan niiden käyttö ja toiminta on ollut salakavalaa. Chaabane ym., (2012) tutkimuksessa esiin nousivat - *d_atr ja c_user* – evästeet, jotka kulkevat käyttäjän mukana pitkänkin ajan. Tämän kautta kolmannet osapuolet pystyvät mahdollisesti seuraamaan Facebook-käyttäjän verkkotoimintaa, ja kerätä sitä kautta henkilökohtaista dataa käyttäjästä. Ihmisten verkkotoiminnasta ja selaushistoriasta voidaan saada paljon henkilökohtaista tietoa. Sivustot, joilla henkilö vierailee voivat paljastaa hänen sijaintinsa, kiinnostuksen kohteet, poliittisen kannan ja esimerkiksi taloudellisen tilanteen.

Tämä voi luoda käyttäjässä epätietoisuutta henkilökohtaisen datan käytöstä ja voi kokea tästä hallinnan puutetta.

Taulukon viimeinen kohta koskee kolmannen osapuolen tietovuotoja. Tämä on niin sanottu pahin skenaario sille, mitä voi tapahtua, kun henkilökohtaista dataa on kerätty kolmansien osapuolten toimesta. Tietovuodoilla voi olla vakaviakin seurauksia yksityisyydelle. Tietovuodot ovat erilaisia ja tapauskohtaisia, sekä henkilökohtaisten tietojen määrän vuotaminen vaihtelee. Henkilökohtaisen datan väärinkäyttö voi näkyä tässäkin riskissä identiteettivarkauksina, joka on yleinen seuraus mahdollisesta tietovuodosta, jossa esiinnytään toisen ihmisen henkilöllisyydellä. Vuotaneet tiedot voivat olla hyvinkin henkilökohtaisia ja se voi aiheuttaa sosiaalisesti korvaamattomia vahinkoja. Esimerkiksi julkinen identiteetti voi kärsiä, jos henkilökohtaiset tiedot ovat tarkoitettu vain omaan käyttöön, mutta paljastuvatkin muulle yleisölle. Tietovuodot voivat aiheuttaa ihmisissä myös hallinnan puutetta, eivätkä tiedä missä määrin henkilökohtaista dataa käytetään. Tämä taas voi johtaa psyykkiseen kuormitukseen ja voimakkaaseen ahdistuksen tunteeseen.

5 YHTEENVETO JA POHDINTAA

Tämän kirjallisuuskatsauksen tarkoituksena oli selvittää miten henkilökohtaisen datan jakamisen ja käytön vaikutukset ovat näkyneet Facebook käyttäjien yksityisyyden suojassa. Lisäksi tutkimuksessa tarkasteltiin kolmansien osapuolten roolia Facebookissa sekä, miten kolmannet osapuolet ovat osana yksityisyyden vaarantamisessa. Aihetta lähdettiin tutkimaan kahden tutkimuskysymyksen avulla, jotka olivat:

1. Mitä vaikutuksia Facebookin käytöllä on ollut yksityisyyden suojaan?
2. Mikä on kolmansien osapuolten rooli Facebook-käyttäjien yksityisyyden suojassa?

Ennen tutkimuskysymyksiin vastaamista tarkasteltiin tärkeitä käsitteitä, jotka selvensivät koko kokonaisuutta. Facebook on suosittu sosiaalisen median alusta ja se on mahdollistanut käyttäjien profiilien luomisen, yhteydenpidon ja kommunikaation toisten käyttäjien kanssa erilaisten media-, tieto- ja viestintätekniikoiden avulla. Facebook on osa Meta Platforms Inc. -yritystä, joka pyrkii laajentamaan sosiaalisen teknologian seuraavalle tasolle lisätyn ja virtuaalisen todellisuuden avulla. Teknologian nopea kehitys on johtanut henkilökohtaisten tietojen laajaan keräämiseen, käsittelyyn ja jakamiseen eri palveluissa ja alustoilla. Tämä kehitys on tuonut yhteiskunnallemme monia etuja, kuten personoituja palveluja ja tuotteita, mutta samalla se on myös vaikuttanut negatiivisesti ihmisten yksityisyyden suojaan. Henkilökohtaiset tiedot ovat nykyään arvokas resurssi ja yritykset ja kolmannet osapuolet pyrkivät hyödyntämään tätä kehitystä. Tietosuojavaltuutetun toimisto määrittelee henkilökohtaiseen dataan kaikki tiedot, jotka koskevat suoraan tai välillisesti tunnistettavissa olevaa henkilöä, mukaan lukien ne tiedot, jotka yhdistettynä muihin tietoihin voivat johtaa tunnistamiseen. Yksityisyyttä tarkasteltiin Westinin (1968) ja Altmanin (1977) mukaan, jossa käsitettä pidetään muuttuvana. Tähän vaikuttaa vahvasti ympäristö ja konteksti, jossa

yksilö on. Kun ympäristöä ajatellaan tämän tutkimuksen kannalta, se painottuu enemmän digitaaliseen ympäristöön. Siitä huolimatta yksilöllä on oikeus valvoa itseään koskevien tietojen luovuttamista, mukaan lukien milloin, miten ja missä määrin sitä jaetaan muille.

Kolmannen osapuolen palveluilla on tärkeä rooli verkossa, sillä ne mahdollistavat ensimmäisen osapuolen verkkosivustojen käyttää erilaisia ominaisuuksia, kuten mainontaa. Facebookin kolmannen osapuolen sovellukset sekä evästeet ovat herättäneet kuitenkin huolta käyttäjien yksityisyydestä, sillä niiden tietosuojaongelmat ilmenevät useista syistä. Näihin kuuluvat sovellusten koodin käyttö julkaisijan omilla palvelimilla, käyttäjätietojen siirto Facebookin palvelimilta kolmansien osapuolien sovelluksiin, sekä rajoitetut tietosuojasäädökset. Facebookin ulkopuoliset sovellukset voivat myös kerätä käyttäjien tietoja ilman heidän tietämystään tai suostumustaan.

Yksityisyys ja sen loukkaaminen näkyy suurimmaksi osaksi ihmisen henkilökohtaisen datan väärinkäytöllä. Kolmannet osapuolet ovat vahvasti tässä mukana, sillä heillä on motiivit kerätä sitä, ja tulosten perusteella jopa törkeästikin. Käyttäjän jakaessa tietojaan Facebookissa, hän ei välttämättä tiedä, miten hänen tietojaan käytetään ja tämä voi johtaa epämääräisyyteen henkilökohtaisen datan käytön suhteen. Käyttäjä voi halutessaan piilottaa tietyt arkaluontoiset tiedot, mutta Facebook saattaa silti käyttää niitä mainonnassa muista lähteistä päätellen ilman käyttäjän tietämystä. Facebookin evästekäytäntö on muuttunut ja kolmansia osapuolia voidaan käyttää evästeiden avulla henkilökohtaisen datan keräämiseen. Tutkimuksessa todettiin, että yhteistyökumppanien verkkosivustoilla käytetään evästeitä, joita Facebook ei voi seurata, mutta ne silti keräävät tietoa käyttäjistä. Facebook käytti aiemmin 16 evästettä, joista kaksi, d_atr ja c_user, ovat suunniteltu käyttäjien tunnistamiseen. D_atr-eväste on voimassa kaksi vuotta ja sen avulla Facebook voi seurata kaikkia sivustolla käyneitä käyttäjiä, myös niitä, jotka eivät ole rekisteröityneet palveluun.

Facebook ja kolmannet osapuolet säilövät valtavasti henkilökohtaista dataa ja tietovuodot ovat yksi suurimmista yksityisyyden suojaan liittyvistä huolenaiheista Facebookissa, ja ne ovat yleistyneet kehittyneen tekniikan avulla. Tietovuodot voivat aiheuttaa taloudellisia menetyksiä, maineen vahingoittumista ja oikeudellista vastuuta. Tietovuotojen motiivit voivat johtua hakkeroinnista, tietojenkalasteluhyökkäyksistä, haittaohjelmista ja inhimillisistä virheistä. Kun tietoturvaloukkaus tapahtuu, se voi vaarantaa henkilökohtaisten ja luottamuksellisten tietojen yksityisyyden ja turvallisuuden.

Ei kahta ilman kolmatta. Tämä kantava teema jatkui läpi kirjallisuuskatsauksen. Sosiaaliseen mediaan ja niiden alustoihin liittyminen on lähtökohtaisesti vapaaehtoinen päätös ja pelkkä Facebookin käyttö voi olla riski yksityisyyden suojalle, mutta kolmannet osapuolet tuovat tähän lisäksi oman ulottuvuuden ja

mahdolliset riskit. Tutkimus aiheena on ajankohtainen, mutta kapea, sillä sosiaalisen median alustoja on muitakin, kuin Facebook. Tutkimusaihetta voitaisiin laajentaa muille sosiaalisen median alustoille tai vertailla muiden alustojen yksityisyyden suojaan liittyviä riskejä.

LÄHTEET

Altman, I. (1977). Privacy regulation: Culturally universal or culturally specific?. *Journal of social issues*, *33*(3), 66-84.

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *Privacy Enhancing Technologies: 6th International Workshop, PET 2006, Cambridge, UK, June 28-30, 2006, Revised Selected Papers 6* (pp. 36-58). Springer Berlin Heidelberg.

Arias-Cabarcos, P., Kjalili, S. & Strufe, T. (2023). "Surprised, Shocked, Worried": User Reactions to Facebook Data Collection from Third Parties. *Proceedings on Privacy Enhancing Technologies (PoPETs)*.

Auxier, B. & Anderson, M. (2021). Social media use in 2021. *Pew Research Center*, *1*, 1-4.

Brandtzæg, P. B., Lüders, M. & Skjetne, J. H. (2010). Too many Facebook "friends"? Content sharing and sociability versus the need for privacy in social network sites. *Intl. Journal of Human–Computer Interaction*, *26*(11-12), 1006-1030.

Carr, C. T. & Hayes, R. A. (2015). Social media: Defining, developing, and divining. *Atlantic journal of communication*, *23*(1), 46-65.

Chaabane, A., Ding, Y., Dey, R., Kaafar, M. A. & Ross, K. W. (2014). A closer look at third-party OSN applications: are they leaking your personal information?. In *Passive and Active Measurement: 15th International Conference, PAM 2014, Los Angeles, CA, USA, March 10-11, 2014, Proceedings 15* (pp. 235-246).

Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *7*(5), e1211.

Datareportal: https://datareportal.com/essential-facebook-stats (viitattu 23.3.2023)

De, S. J. & Imine, A. (2018). To reveal or not to reveal: balancing user-centric social benefit and privacy in online social networks. In *Proceedings of the 33rd annual ACM symposium on applied computing* (pp. 1157-1164)

Debatin, B., Lovejoy, J. P., Horn, A. K. & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of computer-mediated communication, 15(1), 83-108.*

Dimova, Y., Franken, G., Le Pochat, V., Joosen, W., & Desmet, L. (2022, November). Tracking the Evolution of Cookie-based Tracking on

Facebook. *In Proceedings of the 21st Workshop on Privacy in the Electronic Society, 181-196.*

Fire, M., Goldschmidt, R., & Elovici, Y. (2014). Online social networks: threats and solutions. *IEEE Communications Surveys & Tutorials, 16(4), 2019-2036.*

Farahbakhsh, R., Cuevas, A., Ortiz, A. M., Han, X., & Crespi, N. (2015). How far is Facebook from me? Facebook network infrastructure analysis. *IEEE Communications Magazine, 53(9), 134-142.*

Fuchs, C. (2011). An alternative view of privacy on Facebook. *Information, 2(1), 140-165.*

Fuller, M. (2019). Big data and the Facebook scandal: Issues and responses. *Theology, 122(1), 14-21.*

Hoffmann, A. L., Proferes, N. & Zimmer, M. (2018). "Making the world more open and connected": Mark Zuckerberg and the discursive construction of Facebook and its users. *New media & society, 20(1), 199-218.*

Hogan, M. (2015). Facebook data storage centers as the archive's underbelly. *Television & New Media, 16(1), 3-18.*

Kaplan, A. M. & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business horizons, 53(1), 59-68.*

Kavianpour, S., Ismail, Z. & Shanmugam, B. (2017). Classification of third-party applications on Facebook to mitigate users' information leakage. *In Recent Advances in Information Systems and Technologies: Volume 1 5 (pp. 144-154). Springer International Publishing.*

Krishnamurthy, B. & Wills, C. E. (2009). On the leakage of personally identifiable information via online social networks. *In Proceedings of the 2nd ACM workshop on Online social networks (pp. 7-12)*

Kyberturvallisuuskeskus: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/facebookin-vuonna-2019-varastettuja-tietoja-julkaistu-mukana-12-miljoonan-suomalaisen (viitattu 23.3.2023)

Limba, T. & Šidlauskas, A. (2018). Secure personal data administration in the social networks: the case of voluntary sharing of personal data on the Facebook. *Entrepreneurship and Sustainability Issues, 5(3), 528-541.*

Liu, L., Han, M., Wang, Y. & Zhou, Y. (2018). Understanding data breach: A visualization aspect. *In Wireless Algorithms, Systems, and Applications: 13th International Conference, WASA 2018, Tianjin, China, June 20-22, 2018, Proceedings 13(pp. 883-892). Springer International Publishing.*

Lupton, D. (2018). How do data come to matter? Living and becoming with personal data. *Big Data & Society, 5(2), 2053951718786314.*

Lukács, A. (2016). What is privacy? The history and definition of privacy.

Mayer, J. R. & Mitchell, J. C. (2012). Third-party web tracking: Policy and technology. *In 2012 IEEE symposium on security and privacy (pp. 413-427). IEEE.*

Peretti, K. K. (2008). Data breaches: what the underground world of carding reveals. *Santa Clara Computer & High Tech. LJ, 25, 375.*

Phelps, J., Nowak, G. & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of public policy & marketing, 19(1), 27-41.*

Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology, 10(1), 40-81.*

Quan-Haase, A. & Young, A. L. (2010). Uses and gratifications of social media: A comparison of Facebook and instant messaging. *Bulletin of science, technology & society, 30(5), 350-361.*

Rieder, B. (2013). Studying Facebook via data extraction: the Netvizz application. *In Proceedings of the 5th annual ACM web science conference (pp. 346-355).*

Roosendaal, A. (2012). We Are All Connected to Facebook… by Facebook!. *European Data Protection: In Good Health?, 3-19.*

Rubinstein, I. S. & Good, N. (2013). Privacy by design: A counterfactual analysis of Google and Facebook privacy incidents. *Berkeley Tech. LJ, 28, 1333.*

Saglam, R. B., Nurse, J. R. & Hodges, D. (2022). Personal information: Perceptions, types and evolution. *Journal of Information Security and Applications, 66, 103163.*

Schwartz, P. M. (2003). Property, privacy, and personal data. *Harv. L. Rev., 117, 2056.*

Sneed, M. (2020). The Key to Regulating Facebook and Data Collection Companies is Transparency. *Alb. LJ Sci. & Tech., 30, 109.*

Srinivasan, D. (2019). The antitrust case against Facebook: A monopolist's journey towards pervasive surveillance in spite of consumers' preference for privacy. *Berkeley Bus. LJ, 16, 39.*

Stieger, S., Burger, C., Bohn, M. & Voracek, M. (2013). Who commits virtual identity suicide? Differences in privacy concerns, internet addiction, and personality between Facebook users and quitters. *Cyberpsychology, Behavior, and Social Networking, 16(9), 629-634.*

Symeonidis, I., Biczók, G., Shirazi, F., Pérez-Solà, C., Schroers, J. & Preneel, B. (2018). Collateral damage of Facebook third-party applications: a comprehensive study. *Computers & Security, 77, 179-208.*

Tietosuojavaltuutetun toimisto https://tietosuoja.fi/mika-on-henkilotieto (viitattu 2.4.2023)

Venturini, T., & Rogers, R. (2019). "API-based research" or how can digital sociology and journalism studies learn from the Facebook and Cambridge Analytica data breach. *Digital Journalism*, *7*(4), 532-540.

Waldman, A. E. (2016). Privacy, sharing, and trust: The Facebook study. *Case W. Res. L. Rev., 67, 193.*

Westin, A. F. (1968). Privacy and freedom. *Washington and Lee Law Review, 25(1), 166*