Sari Salonen

HTTP EVÄSTEIDEN UHKAT TIETOSUOJASELOSTEIDEN NÄKÖKULMASTA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2022

TIIVISTELMÄ

Salonen, Sari
HTTP-evästeiden uhkat tietosuojaselosteiden näkökulmasta
Jyväskylä: Jyväskylän yliopisto, 2022, 75 s.
Tietojärjestelmätiede, pro gradu -tutkielma
Ohjaaja: Siponen, Mikko

Teknologian kehittyminen ja internetin vahva läsnäolo jokapäiväisessä elämässämme on tuonut mukanaan paljon meitä hyödyttäviä lisäpalveluita ja asioita, mutta myös uhkia yksityisyydellemme. Verkkosivustojen ja palveluiden käyttäjistä kerätään jatkuvasti monenlaisia ja usein arkaluontoisiakin tietoja, muun muassa HTTP-evästeiden ja muiden vastaavien tekniikoiden avulla. Tietomme ovat verkkosivustoilla kilpailuetu ja me olemme ison uhan äärellä, jos nämä tiedot vuotavat vääriin käsiin. Maailmalla on tapahtunut viime vuosina muutamia esimerkkejä valtavista tietosuojavuodoista, joiden ansiosta nämä uhat ovat nousseet tietoisuuteemme. Vuonna 2018 voimaan tullut yleinen tietosuoja-asetus eli GDPR on myös nostanut tietoisuuteemme sen, miten paljon meistä kerätään henkilökohtaisia tietoja verkkosivustoilla asioidessamme. Tämä laki on tuonut verkkosivustoille uhkan sanktioista, jos lakia ei noudateta, mikä on omiaan turvaamaan meitä. Suureen joukkoon mahtuu kuitenkin aina joku, joka ei noudata sääntöjä. Tällöin tietomme ja niiden vuotaminen on todellinen uhka ja saattaa aiheuttaa meille taloudellisia menetyksiä, suurta vaivaa tietojen oikaisuista ja ahdistusta siitä, missä tietomme ovat ja mihin niitä käytetään.

Tämän pro-gradutyön tarkoituksena on tarkastella sitä, mitä uhkia yksityisyyden suojalle nousee esiin tietosuojaselosteiden HTTP-evästeitä koskevista kohdista. Aineistona tähän on hyödynnetty internetin kymmenen suosituimman verkkosivuston tietosuojaselosteita vuonna 2021.

Työn tavoitteena on tuoda tietoisuuteen sitä, miksi omista evästeasetuksistaan kannattaa olla kiinnostunut ja hallinnoida niitä. Tähän työhön liittyvä tutkimus on tehty laadullisena tutkimuksena ja aineistoa on käsitelty koodaten, teemoitellen, hieman tyypitellen ja kvantifioiden. Työ alkaa johdatuksella aiheeseen, teoriaosuuksilla koskien HTTP-evästeitä, tietosuojaselosteita ja näihin liittyviä lakeja ja asetuksia. Työ jatkuu esitellen tutkimuksen, siitä saadut tulokset ja lopuksi johtopäätökset.

Eväste, HTTP, tietosuojaseloste, yksityisyyden suoja, yleinen tietosuoja-asetus

ABSTRACT

Salonen, Sari
Threats of HTTP cookies from a privacy statement perspective
Jyväskylä: University of Jyväskylä, 2022, 75 pp.
Information Systems, Master's Thesis
Supervisor(s): Siponen, Mikko

The development of technology and the strong presence of the internet in our daily lives has brought us many additional beneficial services and things that make our lives easier, but it also brings digital threats closer us and to our privacy. A wide variety of information about us, the users of internet, websites, and digital services, are collected continually with for example HTTP cookies and other similar technologies. These collected pieces of information are valuable and competitive advantage to the websites, but they can be created as a sensitive information and cause harm to us by leaking into wrong hands. There have been a few big examples in media in recent years that some companies have used our information and leaked our information causing privacy issues to the owners of the leaked data. Those examples have made us more cautious and careful in the internet. In 2018, the General Data Protection Regulation came into force and that also raised our attention and awareness that our private information is collected with so many different services. This law was about to help us to make sure that companies that collect personal data are following that law and if not, there will be sanctions. There are many parties who are following the rules and keep our private information safe, but one weak link can cause us losing our private information with financial loss, a great deal of trouble and anxiety without knowing where our data is and to what it has been used for.

The purpose of this master's thesis is to study the threats to our privacy that emerge from the HTTP cookie sections of the 10 most popular domains in 2021. The aim of this study is to make us aware of why us all should be interested in cookie settings and manage them carefully. The research related to this work has been done as a qualitative study and the material has been processed by coding, thematizing, slightly typing and quantification. This work begins with an introduction to the topic, with theoretical sections on HTTP cookies, privacy statements and related laws and regulations. The work continues by presenting the study, the results obtained from it, and finally conclusions.

Cookie, HTTP, privacy notice, privacy police, GDPR

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Vuodesta 2018 voimaan tulleen yleisen tietosuojalain (GDPR) sekä erilaisten tietosuojaa rikkovien skandaalien, kuten, kuten Cambridge Analytican ja Facebookin – tai AccuWeatherin iOs-sovelluksen tietovuotoskandaalien johdosta ovat nostaneet esiin ihmisten tietoisuutta ja huolia yksityisyyden suojasta, tietosuojasta, sekä siitä, miten arvokkaita meitä itseämme koskevat tiedot ovat – etenkin silloin, jos ne menetetään. Tämän vuoksi monet ovat entistä tarkempia siitä, miten he antavat tietojaan erilaisille verkkosivustoille ja huoli tietojen menetyksestä on jatkuvasti läsnä. Olemme tottuneet päivittäin käymään ikään kuin kauppaa sen kanssa, annammeko verkkosivustolle sen haluamia tietoja, jotta pääsemme käyttämään sen tarjoamia palveluita.

Teknologia on kehittynyt nopeasti, lähentynyt jatkuvasti ihmistä ja muuttanut ihmisen ja tietokoneen välistä vuorovaikutusta yhtä tiiviimmäksi. Samalla digitaaliset hyökkäykset ovat entistä kehittyneempiä ja tietoturvaloukkaukset jatkuvasti läsnä uhkan muodossa. Yhä suurempi osa jokapäiväisestä elämästämme pyörii jollain tavalla internetin ja digitaalisen maailman ympärillä. Palveluita käytetään laajasti erilaisiin toimenpiteisiin, joita päivittäisessä elämässä tarvitsemme arjen sujuvoittamiseksi. Meistä kerätään suuri määrä tietoja verkkosivuilla ja erilaisissa palveluissa, iso osa HTTP-evästeiden ja muun vastaavien tekniikoiden turvin. Meistä kerätty yksittäinen tieto saattaa olla mitätön osa tietojamme, emmekä ole siitä yksilöitävissä. Kuitenkin tietojamme yhteen kokoamalla, yhdenkin lenkin pettäessä tietosuojan osalta muuten turvallisessa ketjussa, yksityisyytemme on vaarassa. Yksittäisistä vaarattomista ei-henkilökohtaisista tiedoista saattaa muodostua arkaluontoinen aineisto sen vuotaessa vääriin käsiin. Kokonaisuuteen vaikuttavat paitsi sivustojen ja palveluiden keräämät, myös käyttäjien itsensä niihin syöttämät tiedot.

Alun perin HTTP-evästeiden tarkoitus oli tarjota parempaa käyttökokemusta ja lisätoimintoja verkkosivustojen käyttäjille tilattomassa HTTP-protokollassa. Tänä päivänä HTTP-evästeet voivat kuitenkin olla myös uhka käyttäjän yksityisyyden suojalle. Harva lieneekään tietoinen mihin kaikkeen heidän antamiaan ja heiltä evästeiden avulla kerättyjä tietoja hyödynnetään ja luovutetaan. Käyttäjillä ei ole tarjolla välineitä, joilla ymmärtää täysin evästeiden asettamista

ja käyttämistä huolimatta (tai kenties jopa johtuen) siitä, että verkkosivustot kertovat lukuisin sivuin tekstiä sivustollaan käyttämistään evästeistä. Käyttäjien haasteena on saada täysi ymmärrys verkkosivustojen evästeiden käytöstä, jotta he voisivat tehdä tietoisen päätöksen niiden käyttämisestä ja tietojensa luovuttamisesta sivustolle. Käyttäjät tarvitsisivat monipuolisesti tietoja ja taitoja sekä aikaa tutustuakseen evästeisiin liittyviin teksteihin käyttämillään verkkosivustoilla ja siltikään heidän ymmärryksensä ei välttämättä ole kattava. Evästeisiin liittyy myös sellaisia uhkia nyt ja tulevaisuudessa, joista ei ole vielä ennakkotapauksia olemassa ja näin ollen käyttäjä ei osaa ottaa tällaisia huomioon. Useimmat myös vähättelevät tietosuojaa, haluten vain päästä käyttämään haluamaansa verkkosivustoa klikaten häiritsevät asiat tieltä pois.

Tietosuojaselosteen avulla, käyttäjällä on oikeus ja mahdollisuus saada yleiskuva siitä, kuinka hänen käyttämänsä verkkosivustot tai palvelut käsittelevät hänen henkilötietojaan. Tietosuojaselosteen evästeitä koskevan tarkoitus on tarjota verkkosivuston käyttäjille selkeässä ja ymmärrettävässä muodossa tietoa siitä, miten verkkosivusto käyttää evästeitä. Useimmat käyttäjät eivät kuitenkaan aikaisempien tehtyjen tutkimusten mukaan tutustu dokumentteihin, vaan hyväksyvät kaikki evästeet käyttöön vain saadakseen ne alta pois ja päästäkseen käyttämään sivustoa. Tietosuojaselosteet koetaan monimutkaisiksi ja kuormittaviksi eikä niiden lukeminen tutkimusten mukaan helpota kuluttajien huolta yksityisyydestä, vaan osin pahensi sitä monimutkaisen tekstin myötä. Suurin osa käyttäjistä tekee jatkuvasti kompromisseja verkkosivuston käyttämisen evästeineen ja omien yksityisten tietojensa kanssa.

Tietosuojasta ja sen toteuttamisesta lain vaatimalla tavalla on tullut myös verkkosivustojen haaste. Eri maissa on olemassa erilaisia lakeja ja direktiivejä ja oikeudellisen yhdenmukaisuuden saavuttaminen on haastavaa. Sähköisen viestinnän lainsäädännön kokonaisuuden muodostaminen on haastavaa, sillä lainsäädäntö on hajanaista ja osittain vaikeaselkoista. Lakien, asetusten ja direktiivien vyyhti on iso ja niitä kehitetään ja päivitetään jatkuvasti. Samalla teknologia kehittyy ja on haasteellista olla sekä palvelun tarjoajana että kuluttajana täydessä ymmärryksessä siitä, mitä lait ja asetukset meiltä vaativat ja mitä suojaa ne tarjoavat missäkin muodossa.

1.1 Tutkimuksen motivaatio ja tutkimusmenetelmä

Tämän pro-gradutyön aiheena on ajankohtainen ja monia koskettava aihe, josta ei löytynyt aikaisempia samankaltaisia tutkimuksia. Aikaisemmissa tutkimuksissa oli tutkittu paljon esimerkiksi evästeitä teknisestä näkökulmasta, yleistä tietosuoja-asetusta eli GDPR:ää, yksityisyyden suojaa, tietosuojaa ja sähköisen viestinnän lakeja ja asetuksia. Yksinomaan tietosuojaselostetta koskevia tutkimuksia löytyi heikosti ja ne käsittelivät pääsääntöisesti tietosuojaselostetta GDPR:n näkökulmasta tai teknisemmin, esimerkiksi tietosuojaselosteen koneellista selventämistä tai muita tapoja yksinkertaistaa sitä kuluttajalle.

Yksityisyyden suojaa uhkaavat monenlaiset tekijät digitaalisessa toimintaympäristössä. Tässä työssä paneudutaan siihen, mitä uhkia verkkosivustojen HTTP-evästeiden käyttämisestä tietosuojaselosteen perusteella nousee esiin. Työn tarkoituksena on toimia tietopankkina siitä, minkälaisten uhkien kanssa olemme päivittäin tekemisissä omaehtoisesti digitaalisessa maailmassa verkkosivustoilla asioidessamme sekä antaa hyvä perustietous HTTP-evästeistä, tietosuojaselosteista ja niitä koskevista laeista. Tutkimuksen motivaattorina on aito huoli siitä, pystyykö verkkosivustojen käyttäjä hyväksymään verkkosivuston evästeiden käyttämisen suosituilla verkkosivustoilla varauksetta ja turvallisin mielin.

Tutkimus aiheesta on tehty laadullisin menetelmin, aineistoa on käsitelty tyypitellen ja teemoitellen kvantifiointia hyödyntäen. Tämän tutkimuksen avulla pyritään tutkimaan keskeistä kysymystä: mitä uhkia yksityisyyden suojalle tietosuojaselosteiden evästekohdista nousee. Tutkimuksen aineistona on internetin kymmenen vuoden 2021 suosituimman verkkosivuston tietosuojaselosteet, sekä näiden mahdolliset muut linkitetyt evästeitä koskevat erilliset dokumentit.

1.2 Tutkimuksen rakenne ja tutkimuskysymys

Tässä työssä käydään ensin lävitse teoriaa HTTP-evästeistä, tietosuojaselosteista ja keskeisistä laeista ja asetuksista. Tämän jälkeen käsitellään sitä, miten tutkimuksen aineistoa on analysoitu, jonka jälkeen tarkastellaan tutkimuksen tuloksia ja lopuksi tehdään johtopäätökset. Työn kappaleita on pyritty jäsentelemään selkeästi sopivilla väliotsikoilla ja taulukot ja kuvat tuovat mukanaan havainnollistavaa tietoa aiheista.

Työssä keskityttiin vain yhteen tutkimuskysymykseen:

- RQ1: Mitä uhkia yksityisyyden suojalle tietosuojaselosteiden evästekohdista nousee esiin?

1.3 Tutkimustulokset

Tutkimuksen tuloksina koostettiin näkemys käyttäjää koskevista evästeiden tuomista yksityisyyden suojan uhkista verkkosivustoilla sekä ajantasaista tietoa siitä, minkälaisia tietosuojaselosteet tällä hetkellä ovat evästeitä käsittelevien kohtiensa osalta. Tuloksina nousee verkkosivuston käyttäjää koskevia evästeiden tuomia uhkia ja ajatuksia tietosuojaselosteiden kehittämiselle ja jatkotutkimuksille.

Tutkimuksessa nousi esiin seuraavia yksityisyyden suojalle huolestuttavia kohtia tietosuojaselosteiden evästeistä kertovien tekstien perusteella: kolmannet osapuolet, käyttäjän tiedot ja taidot, läpinäkyvyys, työläys ja käyttäjän suuri vastuu. Ongelmallisimmat maininnat tietosuojaselosteiden evästekohdissa liittyivät

edellä mainituista kolmansiin osapuoliin, jotka myös teorian ja aikaisempien tutkimuksien pohjalta koetaan kaikkein huolestuttavimmaksi aiheeksi käyttäjien näkökulmasta. Kolmannet osapuolet saavat käyttäjistä laajasti tietoa, myös kyseisen verkkosivuston ulkopuolella ja kolmansia osapuolia saattaa olla verkkosivustolla jopa miljoonia, jolloin käyttäjän tiedot leviävät hallitsemattomasti. Täten olisi kohtuutonta olettaa tai vaatia, että käyttäjät tutustuisivat kaikkien kolmansien osapuolien tietosuojaselosteisiin. Riski siitä, että näiden lukuisten kolmansien osapuolien joukossa on toimija, joka ei noudata hyvää tietosuojaa on merkittävä jo yksinomaan suuren määrän johdosta. Käyttäjältä vaaditaan myös paljon ymmärrystä ja osaamista, kuten kielitaitoa ja perehtyneisyyttä tekniikkaan ja teknologiaan, jotta hän voi ymmärtää tietosuojaselosteen evästekohtaa. Aineistossa olleet tietosuojaselosteiden evästeitä koskevat tiedot eivät myöskään olleet läpinäkyviä, vaan näitä oli jätetty avoimiksi, jolloin todellista kokonaiskuvaa on mahdotonta saada. Tietosuojaselosteen evästetekstien lukeminen ylipäätään on työlästä, kuormittavaa ja vaikeaselkoista, jolloin käyttäjälle jää harteilleen kohtuuttoman iso vastuu kannettavaksi verkkosivuston evästeiden käyttämisen hyväksymispäätöstä tehdessään.

2 HTTP-EVÄSTEET

Termit eväste, keksi tai cookie ovat monelle meistä tuttuja digitaalisista palveluista. Eväste terminä on käännetty englanninkielisestä termistä cookie eli suoraan suomennettuna keksi. Evästeen nimivalinnalle ei ole mitään erityistä syytä (Järvinen, 2002).

Tämä luku tarjoaa kokonaisuudessaan kattavan tietopaketin evästeistä. Tässä luvussa käydään läpi evästeiden syntyä ja historiaa, perehdytään HTTP:hen, evästeiden käyttöön ja kategorisointiin, tarkastellaan evästebannereita, suostumuksellisuutta ja turvallisuutta kuluttajien kokemuksen perusteella sekä käsitellään evästeiden hallintakeinoja. Tässä työssä termejä HTTP-eväste, keksi ja cookie käytetään synonyymisesti.

2.1 Synty ja historia

Evästeiden syntyyn liittyy olennaisesti tieto siitä, miten World Wide Web (WWW) toimii. WWW tuli yleisön tietoisuuteen vuonna 1993 ja siihen valittu selain oli Illinoisin yliopiston National Center for Supercomputing Applications (NCSA) Mosaic. Mosaic ei kuitenkaan tarjonnut tilanhallintamekanismia, joten syntyi Netscape Navigator -selain vuonna 1994. Netscapella työskennellyt Lou Montulli kirjoitti ensimmäisen evästeen ja valitsi termin ”cookie” eli ”eväste”. Evästeiden standardointiprosessi alkoi vuonna 1995, joka alkoi evästemäärityksestä ja HTTP-spesifikaatiosta Internet Engineering Task Force (IETF) -standardointiprosessista. Evästeet ratkaisivat haasteita ja sovellukset saatiin toimimaan oikein myös käyttäjän liikkuessa sivuilla. Evästeet olivat osa protokollaa, eivät sisältöä, ja evästeitä käyttävät sivustot olivat toimivampia kuin evästeitä käyttämättömät sivustot. Nykyinen evästestandardi heijastaa teknisten asioiden, persoonallisuuksien, IETF-menettelyjen, yritysten vaikutusten ja ulkoisten poliittisten vaikutusten vuorovaikutusta (Kristol, 2001).

2.2 HTTP

Evästeisiin liittyy kiinteästi HTTP (Hypertext Transfer Protocol), joka on tilaton ja yleisesti verkkopalveluita palveleva protokolla. Palvelin ei muista verkkoselaimen aikaisempaa yhteydenottoa, vaan se käsittelee jokaisen yhteydenoton erikseen. HTTP tarjoaa perustan internetille ja useimmille evästeille. Samaan aikaan evästeiden standardointiprosessin kanssa vuonna 1995 IETF teki myös HTTP-spesifikaatiota. Kun käyttäjä avaa verkkoselaimen ja napsauttaa (hyperteksti) linkkiä, käyttäjän selain muodostaa yhteyden Web-palvelimeen. Tämä palvelin tunnistaa linkkiin upotetun yksilöllisen osoitteen eli URL:n ja lähettää URL:lle pyyntöviestin, johon palvelin lähettää vastausviestin. Kun palvelin on saanut vastauksen, se katkaiseen yhteyden palvelimeen. HTTP:n lisänä toimivat HTTP-evästeet, toiselta nimeltään Web-evästeet tai vain evästeet, ovat pieniä tekstipaketteja. Kun käyttäjä vierailee verkkosivustolla, sivuston palvelin lähettää tekstipaketin eli evästeen verkkoselaimeen, jonka selain lähettää takaisin muuttumattomana, jos palvelinta käytetään uudelleen (Kristol, 2001).

Pelkkänä päätelaitteeseen lähetettävänä tekstitiedostona eväste ei sisällä henkilötietoja, eikä siitä voida tunnistaa yksittäistä käyttäjää. Kuitenkin mikäli eväste liitetään henkilötietoihin, se saattaa siten täyttää henkilötiedon määritelmän, jolloin palveluntarjoajan eli henkilötietorekisterin pitäjän on varmistettava, että se noudattaa kaikkia henkilötietoihin liittyviä velvoitteita (Yue, Xie & Wang, 2010; Kretschmer, Pennekamp & Wehrle, 2021; Innanen & Saarimäki, 2012).

2.3 Evästeiden käyttö

HTTP-evästeitä käytetään laajalti istuntojen tilojen ylläpitämiseen, käyttäjien personointiin, autentikointiin ja käyttäytymisen seurantaan. Evästeet ovat mahdollisuus palveluntarjoajille tallentaa verkkosivuston käyttäjien viestintävälineisiin tietoa käyttäjästä tai hänen käyttäytymisestään verkkosivustoilla tai palveluissa. Osaa palveluista ei voisi toteuttaa ilman evästeiden käyttöä. Evästeet ovat siis tärkeitä ja hyödyllisiä, mutta toisaalta niissä piilee myös yksityisyydensuojaan liittyviä huolia ja riskejä, sillä ne keräävät meistä valtavia tietomääriä. On lisäksi mahdollista, että käyttäjän päätelaitteelle saatetaan tallentaa haitallinen eväste, joka seuraa käyttäjää tai pyrkii esimerkiksi tunkeutumaan laittomasti tämän yksityiselämän alueelle (Kristol, 2001; Yue ym., 2010).

Web-pohjaiset sovellukset käyttävät usein evästeitä, jotta käyttäjän tilaa voidaan ylläpitää HTTP:n tilattomuudessa. Kun käyttäjä klikkaa linkkiä verkkoselaimessaan, selain muodostaa yhteyden Web-palvelimeen ja lähettää sille pyyntöviestin, johon palvelin lähettää takaisin vastausviestin. Osana tätä vastausta se voi lähettää keräämiään tietoja, eli evästeen. Evästeen vastaus voi olla mitä tahansa mitä palvelin tarvitsee, jotta se voi jatkaa siitä mihin se käyttäjän kanssa palvelimella jäi. Esimerkiksi jos käyttäjä vierailee osoitteessa www.google.fi, käyttäjän tietokoneelle tallentuu eväste, joka edellyttää, että

käyttäjän tietokone palauttaa evästeen osoitteeseen www.google.fi kun käyttäjä vierailee osoitteessa uudelleen (Kristol, 2001; Yue ym., 2010).

Evästeet helpottavat istunnollisten verkkosovellusten rakentamista, esimerkiksi siten, että käyttäjä on verkkokaupassa tehnyt itselleen ostoskorin ja painaa tahattomasti tai tahallisesti peruutusnäppäintä, jolloin käyttäjän istunto palaa edelliselle sivulle. Jos käytössä ei olisi evästeitä, käyttäjän keräämä ostoskori tyhjenisi. Evästeitä voidaan käyttää myös kirjautumistietojen tallentamiseen sivustoilla, jolloin käyttäjän ei tarvitse kirjoittaa joka vierailukerta käyttäjätunnusta ja salasanaa uudelleen. Web-sivusto voi myös käyttää evästeitä seurattakseen käyttäjää, millä sivuilla käyttäjä vierailee tietyllä sivustolla ja mitä tuotteita käyttäjä katselee. Näin sivuston ylläpitäjät ymmärtävät paremmin, kuinka käyttäjät liikkuvat ja tekevät ostoksia sivuilla. Näiden tietojen avulla on mahdollista kehittää sivustoa asiakaslähtöisempään suuntaan, esimerkiksi niin että suosituin tuote on paikoissa, josta käyttäjä sen helposti löytää (Kristol, 2001). Käyttäjäkokemuksen näkökulmasta osa evästeistä siis muodostaa välttämättömän osan nykyaikaisia verkkopalveluita.

Kun yhä suurempi osa jokapäiväisestä elämästämme pyörii internetin ympärillä ja palveluihin ladataan suuri määrä henkilötietoja, digitaalisen viestinnän yksityisyyden varmistamisesta on tullut kriittinen ja tärkeä asia. HTTP-evästeet on alun perin kehitetty tukemaan ja auttamaan sovellusten käyttäjiä, mutta lukuisten sovellusten ja niiden erilaisten evästeiden keräämisestä syntyy riski siitä, että yksityisyyden suoja on vaarassa. Esimerkiksi kolmannet osapuolet voivat hyödyntää evästeiden keräämää tietoa käyttäjän käyttäytymisen seuraamiseen ja luodakseen käyttäjäprofiileja. Lisäksi varastetut evästeet voivat aiheuttaa turvallisuusongelmia. Evästeiden kyky seurata käyttäjän selaustottumuksia ja mahdollisesti yhdistää siihen tietojasi, on evästeiden aiheuttaman tietosuojahuolen ydin. Haastavaksi ongelman tekee se, että selaustottumusten seuranta ja tietojen yhdistely voi olla tietosuojaongelman lisäksi samalla avain saumattomaan käyttäjäkokemukseen eri palveluiden välillä. Toisaalta lienee todennäköistä, että välttämättömien evästeiden keräämisen varjolla palveluntarjoajat keräävät paljon myös sellaisia yksilöiviä ja tietosuojan näkökulmasta ongelmallisia tietoja, joita ei voida perustella parantuneella käyttäjäkokemuksella. Useimmat käyttäjät joka tapauksessa eivät ymmärrä evästeitä ja jättävät huomioimatta tietosuojavaihtoehdot. Ihanteellinen tapa käyttää evästeitä olisi ottaa käyttöön ja tallentaa niitä evästeitä, jotka tallentavat käyttäjälle hyödyllistä tietoa ja poistaa käytöstä haitalliset evästeet. Esimerkiksi joidenkin evästeiden hyödyllisyyden määritteleminen on mahdollista, koska käyttäjä voi kokemuksesta havaita haittaa tai eroja käyttämällään verkkosivustolla, jos evästeitä on estetty. Toisaalta on lähes mahdotonta tietää, ovatko evästeet loppuen lopuksi haitallisia vai hyödyllisiä, sillä tietosuojaselosteet saattavat olla hyvin pitkiä ja vaikeita ymmärtää (Yue ym., 2010). Lisäksi evästeiden keräämät tiedot voivat muodostaa täysin arvaamattomia haavoittuvuuksia joskus tulevaisuudessa.

Palveluiden personointi saattaa johtaa vahingossa yksityisten tietojen vuotamiseen ja on mahdollista, että käyttäjän yksityiset tiedot kuten sähköpostiosoite, koti- ja työosoite, hakuhistoria tai tietoja yhdistelemällä aikaiseksi saadut

henkilökohtaiset tai jopa arkaluontoiset tiedot joutuvat vääriin käsiin (Sivakorn, Polakis & Keromytis, 2016).

2.4 Kategorisointi

Evästeitä voidaan luokitella kategorioittain niiden ominaisuuksien mukaan. Luokittelu voidaan tehdä voimassaoloajan, alkuperän ja käyttötarkoituksen mukaan. Tässä kappaleessa tutustutaan evästeisiin näiden kategorioiden alla kuvion 1 mukaisesti:

Tyypit	**Evästelajit**
Evästeiden voimassaoloaika	• Istuntoevästeet • Pysyvät evästeet
Evästeiden alkuperä	• Ensimmäisen osapuolen evästeet • Kolmannen osapuolen evästeet

Evästeiden käyttötarkoitus	• Välttämättömät evästeet
	  • Toiminnalliset evästeet
	• Ei välttämättömät evästeet
	  • Personointievästeet
	  • Analytiikkaevästeet
	  • Sosiaalisen median evästeet
	  • Mainontaevästeet

TAULUKKO 1 Evästeet kategorioittain

On olemassa myös selaimen ulkopuolella olevia, niin sanottuja Flash-evästeitä. Ne ovat paikallisesti jaettuja kohteita eli LSO-tiedostoja (Local Shared Object), jotka vastaavat selainevästeitä. Niitä käytetään käyttäjäkokemuksen lisäämiseksi, esimerkiksi tallentamalla verkkosivuston käyttämän Adoben Flash Playerin asetuksia eli evästeitä käyttäjän päätelaitteelle äänenvoimakkuuden tai mykistysasetusten muistamiseksi verkkosivustoilla olevan sisällön yhteydessä. Flash-evästeet eivät yksinään voi tehdä käyttäjän tietokoneella oleville tiedoilla mitään, eivätkä ne voi käyttää näitä tietoja. Niillä on oikeus päästä vain niihin tietoihin, jotka käyttäjä on antanut verkkosivustoille, eikä evästeisiin ole pääsyä muilta verkkosivustoilta. Käyttäjälle haasteena on se, että internetselaimen selaushistorian ja evästeiden tyhjentäminen saattaa olla tuttua, mutta Flash-evästeiden poistaminen ei onnistu tätä kautta, vaan ne täytyy poistaa Adoben omien asetusten kautta. Monet käyttäjät eivät ole myöskään tällaisista evästeistä edes tietoisia. Adobe kuitenkin päätti Flash Playerin käyttämisen 31.12.2020. Tämän yhteydessä käytön lopettivat myös suuret verkkosivustot, mutta joillakin

pienemmillä sivustoilla niitä saattaa vielä kohdata. Flash-evästeet saattoivat liittyä ohjelman toimintaan, mutta käytännössä niitä käytettiin myös laajasti muihin tarkoituksiin ja niissä tunnistettiin tietosuojauhkia, joten Adoben päätös ajaa palvelu alas oli ymmärrettävä (Adobe, 2021; Innanen & Saarimäki, 2012).

Edellä mainittujen lisäksi on olemassa erilaisia evästeiden kaltaisesti toimivia tekniikoita, joihin sovelletaan samanlaista sääntelyä kuin evästeisiin. Esimerkkejä samankaltaisista tekniikoista ovat HTML5:seen sisäänrakennettu tiedon varastointimekanismi, verkkokutsuihin pohjautuvat seurantatekniikat (seurantapikselit, web beaconit, tagit) tai sormenjälkitekniikoilla käyttäjän päätelaitteen tunnistaminen yksilöllisesti. Näihin erilaisiin tekniikoihin ei kuitenkaan tässä työssä keskitytä tarkemmin, muuta kuin listaten niitä tutkimuksen tulosten yhteydessä (Traficom, 2021).

2.4.1 Voimassaoloaika

Voimassaolonsa perusteella evästeitä jaotellaan kahteen eri luokkaan, joita ovat istuntoevästeet ja pysyvät evästeet, kuten taulukossa 1.

Istuntoevästeet ovat väliaikaisia evästeitä. Niillä ei ole elinikää, vaan ne tallennetaan käyttäjän tietokoneen muistiin vain siksi aikaa, kun käyttäjä käyttää verkkosivustoa tai palvelua johon istuntoeväste liittyy. Eväste poistetaan heti, kun verkkoselain suljetaan ja käyttäjän istunto päättyy. Istuntoevästeiden avulla käyttäjän on mahdollista tehdä verkko-ostoksia verkkokaupassa esimerkiksi säilyttämällä kerätty ostoskori sivustolla liikkuessa ja ostoksia valitessa. Istuntoevästeitä käytetään silloin, kun verkkosivuston tarvitsee muistaa käyttäjän toimintaa koskevia tietoja vain lyhytaikaisesti. Niiden avulla ei ole mahdollista päästä käsiksi tietoihin järjestelmän fyysisestä muistista, eivätkä ne tallenna tietoja (Yue ym., 2010; Traficom, 2022; Velagapudi & Gupta, 2019).

Pysyvät evästeet poikkeavat merkittävästi istuntoevästeistä. Ne tallennetaan tietokoneen kiintolevylle, eli järjestelmän fyysiseen muistiin. Ne pysyvät tallennettuna nimensä mukaisesti pysyvästi, eli niitä ei poisteta, vaikka verkkoselain suljettaisiin. Ne säilyvät siihen asti, kunnes ne vanhenevat tai käyttäjä itse poistaa ne tyhjentämällä verkkoselaimensa selaushistorian. Pysyvälle evästelle on määritetty aika, johon asti se on tallennettuna käyttäjän koneella, tai vaihtoehtoisesti käyttäjä voi poistaa ne itse. Selaushistorian poiston yhteydessä on kuitenkin muistettava, että samalla poistuvat kaikkien käytettyjen sivustojen asettamat evästeet, eli esimerkiksi kirjautumistietoja. Pysyviä evästeitä käytetään silloin, kun verkkosivuston täytyy muistaa pidempiaikaisesti käyttäjän mieltymyksiä esimerkiksi kielivalinnan tai sivuston ulkoasun suhteen tai kirjautumiseen tarvittava käyttäjätunnus ja/tai salasana. Niiden avulla on mahdollista tietää, onko käyttäjä käyttänyt sivustoa aikaisemmin ja myös kerätä tietoja siitä, miten ja missä sivuston osioissa käyttäjä liikkuu tai mitä sisältöjä verkkosivustosta käyttäjä on kuluttanut (Yue ym., 2010; Traficom; Velagapudi & Gupta, 2019).

2.4.2 Alkuperä

Alkuperänsä puolesta evästeet jaotellaan ensimmäisen osapuolen- ja kolmannen osapuolen evästeisiin. Erityisesti kolmannen osapuolen evästeet mielletään yleisesti uhkaksi yksityisyyden suojalle, mutta haasteita on myös ensimmäisen osapuolen evästeissä, erityisesti pysyvien evästeiden osalta (Yue ym., 2010).

Ensimmäisen osapuolen evästeet asetetaan suoraan sen verkkosivuston tai sivuston omistavan organisaation toimesta, jolla käyttäjä selaimellaan vierailee ja vain tämä sama sivusto voi lukea ne. Ensimmäisen osapuolen istuntoevästeitä käytetään eniten verkkosivustojen käyttäjien istuntotilojen ylläpitämiseen. Ne aiheuttavat suhteellisen vähän tietosuoja- tai tietoturvallisuusuhkia käyttäjille, varsinkin niiden lyhyen käyttöiän vuoksi. Tämän vuoksi on perusteltua käyttäjälle ottaa käyttöön vain ensimmäisen osapuolen istuntoevästeet (Traficom, 2022; Yue ym., 2010).

Haasteena käyttäjän yksityisyydelle ovat ensimmäisen osapuolen pysyvät evästeet, jotka voivat säilyä käyttäjän koneella vuosia, ellei niitä poisteta käyttäjän toimesta. Jotkut näistä evästeiden mahdollistamista toimista ovat käyttäjälle hyvin hyödyllisiä, kuten asetusten muistaminen, mutta riskinä on käyttäjän toimintaa seuraavat evästeet. Ensimmäisen osapuolen pysyviä evästeitä on mahdollista kaapata tai manipuloida pitkäaikaisilla hyökkäyksillä, kuten sivustojen haavoittuvuuksia hyväksikäyttävillä hyökkäyksillä. Verkkoselainten puutteet voivat aiheuttaa käyttäjälle riskin, että hyökkääjillä on mahdollisuus varastaa ja käsitellä tietokoneen kiintolevyllä sijaitsevia evästeitä (Yue ym., 2010).

Haastavin asia vain ensimmäisen osapuolen hyväksymisessä on pysyvien evästeiden käsittely. Verkkoselainten toiminnot ovat hyvin rajalliset, kuten vain kaikkien ensimmäisen osapuolen pysyvien evästeiden automaattinen hyväksyminen tai estäminen (Yue ym., 2010).

2.4.3 Käyttötarkoitus

Sähköiseen viestintään pohjautuvissa palveluissa ja erilaisilla verkkosivustoilla käyttäjistä voidaan kerätä monenlaisia tietoja. Näitä ovat esimerkiksi IP-osoite, erilaiset laite- ja mainostunnisteet, tietoa millä sivustolla on vierailtu ja milloin, sisältöjen käytön seuranta ja tuotteiden oston seuranta. Yksittäisinä tietoina nämä eivät muodosta käyttäjää yksilöivää henkilötietoa, mutta mitä laajemmin tietoja kerätään ja yhdistellään, sitä todennäköisemmin niiden perusteella käyttäjä on mahdollista yksilöidä. Etenkin silloin kun tietoja kerätään profilointi-, kohdennus- ja vaikuttamistarkoituksessa, tietojen yhdistely ja henkilötietojen muodostuminen on todennäköistä. Joissain tapauksissa kerätyistä tiedoista voi muodostua jopa arkaluontoisia henkilötietoja, jotka voivat olla hyvin yksityiskohtaisia (esimerkiksi henkilön terveystiedot) (Kretschmer ym., 2021; Yue ym., 2010).

Osa evästeistä on välttämättömiä sivuston toiminnan kannalta, mutta eivät kaikki. Tällöin ne jakautuvat ei-toiminnallisiin tai toiselta nimeltään ei-välttämättömiin evästeisiin ja toiminnallisiin evästeisiin. Ei-pakollisten ja pakollisten evästeluokkien välillä olevat rajat voivat olla joskus häilyviä ja niitä voi olla haastavaa

erottaa toisistaan. Näiden lisäksi evästeet jakautuvat käyttötarkoituksena mukaan myös muihin evästetyyppeihin, jotka on kuvattu kuviossa 1 (Yle, 2021).

Välttämättömät evästeet ovat yleensä ensimmäisen osapuolen asettamia ja istuntokohtaisia eli vain kyseinen verkkosivusto voi asettaa ja lukea niitä ja ne poistuvat, kun käyttäjä sulkee selaimen. Tällaisia evästeitä ei voi poistaa käytöstä, koska ne ovat tärkeitä verkkosivuston perustoiminnoille eli ilman niitä verkkosivusto eivät toimi. Välttämättömien evästeiden avulla mahdollistettavia toiminnallisuuksia ovat esimerkiksi kirjautuminen sivuston suojattuihin osiin, ostoskorin sisällön muistaminen verkko-ostoksia tehdessä ja lomakkeiden täyttäminen. Välttämättömien evästeiden käyttämiseen ei ole pakko lain mukaan pyytää verkkosivuston käyttäjän suostumusta, mutta kyseisten evästeiden käytöstä olisi suotavaa kertoa (Traficom, 2022).

Välttämättömät evästeet ovat siis toiminnallisia evästeitä, joiden ansiosta verkkosivusto toimii oikein. Kun verkkosivusto asettaa käyttäjälle asennusevästeen tiedon säilyttämistä varten, on kyseessä toiminnallinen eväste. Tämä voi olla esimerkiksi valinta siitä, millä kielellä sivusto tulisi käyttäjälle näyttää. Tällaisia toiminnallisia evästeitä ei voida käyttää yksittäisen käyttäjän tunnistamiseen (Kretschmer ym., 2021).

Osa toiminnallisista evästeitä pystyy tunnistamaan yksilön, jolloin kyseessä on seurantaeväste. Seurantaevästeet ovat käytössä, kun esimerkiksi käyttäjä kirjautuu johonkin verkkopalveluun. Tällöin käyttäjän verkkopalvelin lähettää selaimelle merkkijonon, joka palautetaan jokaisen myöhemmän pyynnön yhteydessä, todistaakseen että sama käyttäjä tekee kyseiset pyynnöt. Seurantaeväste tunnistaa muun muassa sivuston suositun sisällön ja sen voi antaa käyttäjällä erityisiä yksilöityjä suosituksia. Seurantaevästeiden avulla on myös mahdollista kerätä yksityiskohtaisia tietoja käyttäjien käyttäytymisestä tietojen analysoimista varten. Kaikenlaisista toiminnallisista evästeistä on ilmoitettava käyttäjälle. Kuitenkaan niiden käyttämisen suostumus ei ole välttämätöntä, jos palveluntarjoaja voi osoittaa, että kerättyjen tietojen kerääminen on ehdottoman tarpeellista (Kretschmer ym., 2021).

Ei-välttämättömiä evästeitä kutsutaan myös ei-toiminnallisiksi evästeiksi. Nämä ovat evästeistä kiistanalaisempia, sillä ne eivät palvele mitään verkkosivuston toiminnallista tarkoitusta eli sivusto toimii käyttäjälle oikein ilman näiden asettamista. Ei-välttämättömien evästeiden tarkoituksena on kerätä verkkosivuston käyttäjän käyttäytymisestä ja mieltymyksistä tietoa. Tällaisia ovat seurantaevästeet, tilastointi- ja analytiikkaevästeet, personalisointievästeet, kohdentamisevästeet sekä markkinointievästeet, jotka on esitelty myös kuviossa 1 (Kretschmer ym., 2021; Yle, 2021).

Personointievästeitä kutsutaan myös mieltymysevästeiksi, sillä niiden avulla verkkosivuston on mahdollista muistaa esimerkiksi sen, millä kielellä käyttäjä haluaa verkkosivuston toimivan tai muistaa käyttäjän käyttäjätunnus ja salasana eri sivuston käyttökertojen välillä. Personointievästeiden ansiosta on mahdollista seurata, millä sivustoilla käyttäjä on vieraillut, mitä sisältöjä tämä on katsellut ja näiden tietojen ansiosta näyttää käyttäjälle hänen aikaisempiin kiinnostuksensa kohteisiin perustuvaa sisältöä (Traficom, 2022).

Analytiikkaevästeiden tarkoituksena on kerätä tietoa siitä, miten käyttäjä käyttää verkkosivustoa. Analytiikkaevästeet laskevat esimerkiksi sivulatauksia, mittaavat sivuston latausaikoja ja sitä, miten sivustolla liikutaan (Traficom, 2022).

Sosiaalisen median alustat käyttävät evästeitä, joita kutsutaan sosiaalisen median evästeiksi. Ne mahdollistavat julkaistujen sisältöjen näyttämisen, tykkäys- ja jakotoimet tai ne voivat liittyä myös esimerkiksi sosiaalisen median alustan käyttäjätunnuksen kirjautumiseen ja siihen liittyvän käyttäytymiseen, kuten kommentointiin (Traficom, 2022).

Mainontaevästeiden avulla on mahdollista kerätä tietoja käyttäjän kiinnostuksen kohteista seuraamalla käyttäjän verkkokäyttäytymistä. Näin käyttäjälle voidaan kohdentaa tämän käyttäytymisen perusteella kohdennettuja mainoksia. Mainontaevästeitä käyttävät verkkosivustot ovat kritisoineet käyttäjän luvan kysymistä verkkosivuston evästeiden asettamisesta, sillä se on nähty uhkana mainostajien liiketoimintamallille. Kritiikkiä mainontaevästeet ovat saaneet myös käyttäjien profiilien kokoamisesta. Tämä on uhka käyttäjän yksityisyydelle, erityisesti käytettäessä kolmannen osapuolen evästeitä, jolloin käyttäjä ei ole enää tietoinen siitä, kenelle hänen tietojaan päättyy (Traficom, 2022).

2.5 Evästebannerit

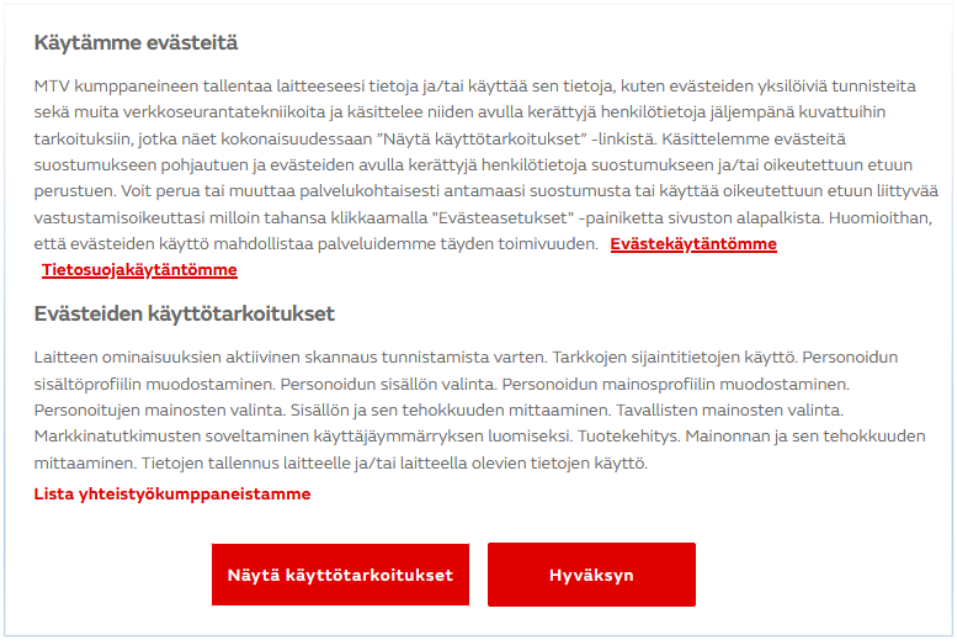
Evästebannerit ovat tulleet internetin käyttäjille viime vuosien aikana hyvinkin tutuiksi ja näkyviksi. Aina kun käyttäjä avaa verkkoselaimen ja vierailee verkkosivustolla, näytölle avautuu pyyntö käyttäjän suostumuksen antamisesta evästeisiin liittyen, jossa käyttäjää pyydetään yleensä joko hyväksymään tai hylkäämään evästeet. Kretschmerin ym. (2021) mukaan tämä johtuu siitä, että vuonna 2009 astui voimaan muutos sähköisen viestinnän tietosuojadirektiiviin, eli niin sanottuun ”Evästedirektiiviin”. Tämän myötä verkkosivustoille alkoi ilmestyä bannereita ja ponnahdusikkunoita, joita kutsutaan evästebannereiksi. Evästebannereiden tehtävä on tiedottaa verkkosivuston käyttäjää verkkosivuston evästekäytännöistä. Joskus ne tarjoavat myös mahdollisuuden hylätä tietyt evästeet tai ottaa käyttöön vain välttämättömät evästeet. Evästebannerit toimivat yleisesti vuorovaikutuksellisella tavalla, jolloin käyttäjän on oltava vuorovaikutuksessa bannerin ilmoittamien tietojen kanssa, ennen kuin hän pääsee verkkosivustoille. Evästebannereita on kolmea eri tyyppiä, jotka on eritelty tarkemmin taulukossa 2. Esimerkit kuvallisina kyseisistä bannereista, löytyvät kuvioista 1, 2 ja 3.

Evästebannerissa ei saa olla valmiiksi rastitettuja ruutuja tai oletusvalintoja ”hyväksy kaikki evästeet” kohdissa, vaan käyttäjän täytyy itse tehdä valinta. Suostumuksen täytyy olla erillinen toimi, joka on vapaaehtoinen, tietoinen, yksiselitteinen ja yksilöity tahdonilmaisu. Evästebannereiden eli pop-up-ikkunoiden avautuminen on mahdollista estää käyttäjän internetselaimen asetuksista. Tällöin verkkosivusto tai palvelu saa käyttää vain välttämättömiä evästeitä, sillä käyttäjä ei ole antanut virallista suostumustaan muiden evästeiden käyttöön. Evästebanneri voi evästeasetusten lisäksi sisältää yksityiskohtaisempiakin tietoja

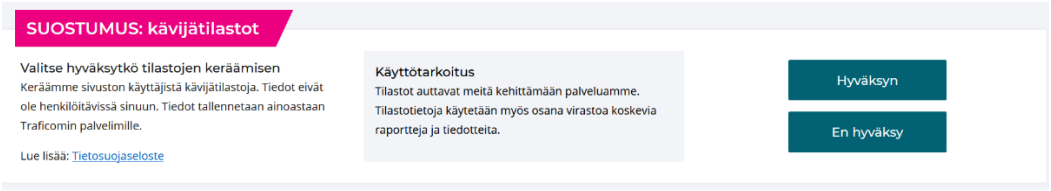
tai esimerkiksi linkin tarkempiin tietoihin palvelun evästeistä tai yksityisyyskäytännöistä eli tietosuojaselosteeseen (Traficom, 2021).

	Evästeseinät (kuvio 1)	Binääribannerit (kuvio 2)	Monivalintabannerit (kuvio 3)
Tarkoitus	Ainostaan ilmoittavat evästeiden käytöstä.	Tarjoaa käyttäjälle vaihtoehdon evästeiden käytöstä verkkosivustolla.	Tarkempi valintamahdollisuus käyttäjälle hallita tai hylätä verkkosivuston käyttämiä evästeitä.
Käyttäjän valinnat	Mahdollisuus napsauttaa hyväksymispainiketta suostumuksen ilmaisemiseksi.	Mahdollisuus hylätä evästeet yleisesti. Tietosuojaselosteesta selviää, mitkä evästeet hylkäämisellä hylätään ja mitkä ovat vielä asettamatta.	Verkkosivustosta riippuen on erilaisia tarkkuustasoja vaihdellen muutamasta kategoriasta jokaisen seurantaosapuolen tarkkaan luettelointiin.
Oletus	Vaikka käyttäjä ei napsauta hyväksymispainiketta, evästeitä asetetaan silti.	GDPR:n mukaan suostumus voidaan antaa vain ymmärrettävällä tavalla, jotta käyttäjä varmasti tietää, mitkä evästeet ovat välttämättömiä ja mitkä seurantaevästeitä, jotka asetetaan vain käyttäjän suostumuksella.	Seurantaeväste asetetaan usein ennen kuin käyttäjälle näytetään suostumuslomake. Sen sijaan että tarjotaan kieltäytymismahdollisuus henkilötietojen keräämisestä, jätetään vain personoitu sisältö pois.
Rajoitukset ja haasteet	Verkkosivustot eivät voi tehdä tietojen käsittelyä suostumuksen perusteella, sillä käyttäjälle ei anneta tasavertaista valintamahdollisuutta.	Käyttäjä ei pääse asettamaan vain ns. hyviä evästeitä ja jättämään pois haluamiaan evästeitä, vaan valinta on joko tai. On myös helpompaa hyväksyä kaikki evästeet kuin hylätä ne laajamittaisesti.	Harhaanjohtava luokittelu valinnalle. Käyttäjä ei voi olla varma, ettei häntä seurata, vaikka hän valitsisi kaikista konservatiivisimmat evästeasetukset.

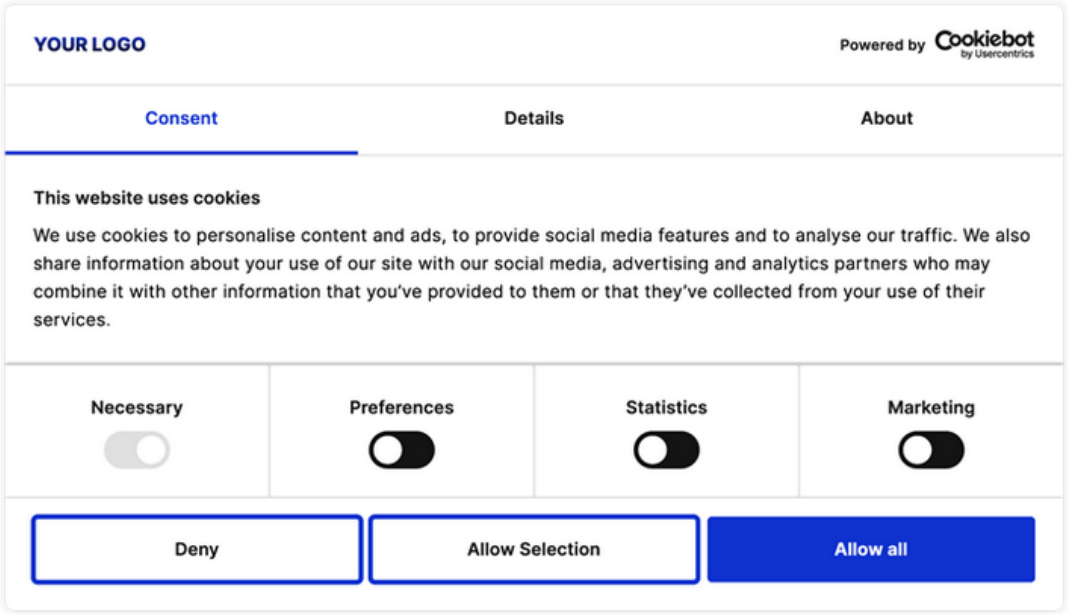
TAULUKKO 2 Evästebannerityypit



KUVIO 1 MTV Uutiset (2022) verkkosivuston evästeseinä



KUVIO 2 Traficom (2022) verkkosivuston binääribanneri



KUVIO 3 Cookiebot (2020) verkkosivuston esittelemä monivalintabanneri

2.6 Suostumuksellisuus

Sähköisen viestinnän tietosuojadirektiiviä muutettiin nykyiseen muotoonsa vuonna 2009 niin sanotulla evästedirektiivillä, jonka mukaan edellytys evästeiden käytölle on käyttäjän suostumus. Evästeistä tai muusta verkkosivuston tai palvelun tietojen käyttämisestä tai tallentamisesta, joka edellyttää käyttäjän suostumuksen antamista, on informoitava ymmärrettävällä ja kattavalla tavalla. Suostumusta ei tarvitse pyytää välttämättömien evästeiden asettamiseksi tai jos tietojen tallennuksen tarkoitus on toteuttaa viestin välitystä viestintäverkoissa tai tietojen tallennus on välttämätöntä sellaisella palvelulle, jota käyttäjä on pyytänyt. Tällöinkään tietojen tallentaminen ja käyttäminen ei ole vapaata, vaan sallittu vain ja ainoastaan palvelun vaatimassa laajuudessa (Traficom, 2021).

Palveluntarjoajan vastuulla on käyttäjän suostumuksen pyytäminen ja evästeisiin liittyvien tietojen antaminen asianmukaisesti ja oikea-aikaisesti silloin, kun käyttäjän saapuu verkkosivustolle tai avaa palvelun. Palveluntarjoajan on huolehdittava siitä, että muita evästeitä kuin välttämättömiä ei aseteta käyttäjän päätelaitteeseen ennen kuin käyttäjä on tehnyt evästeiden käyttöä koskevat valinnat. Suostumuksen on oltava yleisen tietosuoja-asetuksen mukainen, jotta se on pätevä ja sen on oltava aktiivinen tahdonilmaisu, eli suostumusta ei voi antaa jättämällä vastaamatta kysymykseen. On tärkeää, että kieltäytyminen on yhtä helppoa kuin suostumuksen antaminen eli suostumuksen antaminen ei-välttämättömien evästeiden käyttöön ei saa olla yksinkertaisempaa kuin niiden käyttämisen kieltäminen. Esimerkkinä evästebannerissa suostumusmekanismin valikossa voidaan esittää hyväksy kaikki (kaikki ei-välttämättömät evästeet voidaan ottaa käyttöön) ja sen rinnalla valinta jatkaa vain välttämättömillä evästeillä. Tällainen tekee suostumuksen ja kieltäytymisen mahdollisuuden vaihtoehdot tasapäisiksi ja yhtä helpoiksi. Näiden lisäksi käyttäjän tulee halutessaan saada tehdä tarkempia valintoja erityyppisten evästeiden suhteen. Suostumuksen pyytävä mekanismi ei saa kohtuuttomasti estää ja häiritä käyttäjän pääsy sivustolle tai palveluun ja jos käyttäjä ei tee valintoja evästeiden suostumusmekanismiin, sivuston täytyy oletuksena käyttää vain välttämättömiä evästeitä (Traficom, 2021).

Haasteena edellä mainitun tasa-arvoisen valinnan vaateen toteutumiselle on, että sitä kierretään laajasti tekemällä kaikkien evästeiden valitsemisesta tarkoituksellisesti todennäköisempää kuin vain välttämättömien valinnalla, vaikka ne teknisesti ottaen olisivatkin yhtä helposti klikattavia. Tähän vaikutetaan hahmotuksellisilla keinoille, esimerkiksi korostamalla ”Hyväksy kaikki evästeet” -valintapainikkeen taustaväriä kirkkaalla vihreällä, siinä missä ”Hyväksy vain välttämättömät evästeet” -valintapainikkeesta tehdään tätä haaleampi. Käyttäjä, joka pyrkii vain nopeasti pääsemään evästevalinnoista eroon, tulee usein klikanneeksi kaikkien evästeiden keruun hyväksymisen ilman tietoista aietta siihen, eikä tämän välttämättä tämän huomattuaankaan usein palaa etsimään, miten valinnan voisi muuttaa.

Suostumuksen teosta tallentuu suostumuksen teon ajanhetki, miten suostumusta pyydettiin, mitä tietoja suostumuksen antamista varten annettiin sekä

tarpeelliset tunnistetiedot (kenen toimesta ja miltä laitteelta suostumus annettiin). Palveluntarjoajan on kyettävä jälkikäteen osoittamaan saamansa suostumus, mutta tietoja ei tule tallentaa enempää kuin on välttämätöntä suostumuksen todistamiseksi. Jos palvelun evästeissä tehdään muutoksia, suostumus tulee pyytää uudelleen (Traficom, 2021).

Suostumus tulee myös voida peruuttaa milloin tahansa yleisen tietosuoja-asetuksen mukaan ja peruuttamisen tulee olla käyttäjän kannalta yksinkertainen. Suostumuksen peruuttamisen jälkeen palveluntarjoaja ei saa keinotekoisesti heikentää tarjoamansa palvelun tasoa saadakseen käyttäjältä täysimuotoisen suostumuksen evästeiden käyttämiseen. Joidenkin evästeiden kieltäminen saattaa kuitenkin johtaa käyttäjän kannalta palvelutason heikkenemiseen. Tämä voi näkyä esimerkiksi oletuksena vääränä verkkosivuston kielivalintana tai käyttäjälle suunnatun mainonnan ollessa olennaisesti huonompaa. Peruuttamisen täytyy myös olla sellainen, että sillä on tosiasiallinen vaikutus, jolloin esimerkiksi poistetaan tai ylikirjoitetaan laitteelle aiemmin tallennettuja tietoja (Traficom, 2021).

2.7 Turvallisuus

Verkkosivustojen evästeet keräävät paljon tietoja käyttäjistään ja niitä on käytetty laajasti vuodesta 1994 alkaen. Globalisaatio ja nopea teknologinen muutos ovat aiheuttaneet sen, että kansalaisten on mahdollista jakaa tietoa käyttäytymisestään ja mieltymyksistään ja tämä tieto voi levitä maailmanlaajuisesti yritysten ja organisaatioiden saataville (Poritskiy, Oliveria & Almeida, 2019).

Evästeiden tarkoitus oli alun perin paremman käyttökokemuksen ja lisätoimintojen tarjoaminen, mutta ne ovat muovautuneet sisältämään myös käyttäjien yksityisyyttä uhkaavien tietojen keräämistä. Erityisesti kolmannen osapuolen evästeet ovat tässä suhteessa ongelmallisia. Verkkosivustojen on tiedotettava käyttäjille evästeiden käytöstä, mutta kaikille käyttäjille ei ole selvää mitä evästeiden käyttö heidän kohdallaan tarkoittaa. Alan tutkimukset osoittavat, että tietosuojaselosteet ovat tehottomia, sillä käyttäjät eivät täysin ymmärrä niiden sisältöä voidakseen tehdä tietoisia ja valistuneita päätöksiä evästeiden käytöstä (Kulyk, Hilt, Gerber & Volkamer, 2018).

Teknologian nopea kehitys ja sen lähentyminen ihmistä ovat muuttaneet ihmisen ja tietokoneen välistä vuorovaikutusta ja nykytilanteessa tietoturvallisuus ja yksityiset tiedot ovat jatkuvasti uhattuna. Hyökkäykset ovat entistä kehittyneempiä ja tietoturvaloukkaukset koskevat niin yksityisiä henkilöitä kuin organisaatioitakin. Henkilötietojen vuotaessa niitä voidaan käyttää laittomiin tarkoituksiin aiheuttaen vakavaa haittaa tietojen omistajalle. Kristol (2001) teki tutkimuksen, jossa selvitettiin missä määrin kuluttajat välittävät siitä, että verkkosivustot seuraavat heidän tekemisiään. Tutkimus on tehty jo vuonna 2001 ja tällöin tuloksena oli, että käyttäjät hylkäsivät vain alle 1 % evästeistä yli miljardilla sivun katselukerralla. Tämän tutkimuksen mukaan selittävänä tekijänä on usein käyttäjien puutteellinen ymmärrystä evästeistä, joka näkyy ainakin seuraavilla kolmella tavalla:

- Käyttäjä ei tiedä evästeistä
- Käyttäjä tietää evästeistä, mutta ei ymmärrä niiden toimintaa
- Käyttäjä tietää evästeistä ja niiden toiminnasta, mutta ei välitä ja olettaa, että tietoja keräävät tahot suojelevat tietoja ja että viranomaismääräykset estävät väärinkäytökset

Useimmat käyttäjät vastustavat ajatusta, että verkkosivusto käyttää evästeitä, erityisesti jos verkkosivusto käyttää kolmansia osapuolia. Kuluttajat haluavat kuitenkin päästä ensisijaisesti käyttämään verkkosivustoa, hyväksyen evästeet, vaikka he ajatuksen tasolla niitä vastustavatkin (Kristol, 2001).

Hui, Teo & Lee (2007) tekemän tutkimuksen mukaan, useimmat ihmiset paljastivat henkilökohtaisia tietojaan verkkosivustolle huolimatta siitä, olivatko he lukeneet tai ymmärtäneet tietosuojaselostetta ja yksityisyyden suojan tarkoituksen. Kuitenkin tietosuojalausuntoja lukevat ihmiset luovuttavat tietonsa todennäköisemmin, päästäkseen asioimaan haluamallaan verkkosivustolla.

Evästeitä käytetään paljon jatkuvan todentamisen apuna. Tämä johtuu siitä, että HTTP on tilaton ja se saavuttaa tilallisen toiminnan käyttämällä evästeitä. Yksi kriittisimmistä alueista, jossa käyttäjän yksityisyys saattaa olla uhattuna, on istunnonhallinta. Kun käyttäjä todentaa itsensä verkkosivustolle, järjestelmä pitää käyttäjän todennettuna järjestelmän kanssa tapahtuvan vuorovaikutuksen ajan ilman uudelleentunnistusta käyttäjän liikkuessa sivustolla. Tällaiset sivustot luottavat evästeisiin jatkuvan todennuksen ensisijaisena lähteenä ja evästeet ovat herkkiä hyökkäyksille. Hyökkääjällä on käytössään laaja valikoima tekniikoita sovellusistunnon väärentämiseen, esimerkiksi istunnon kiinnitys, evästeen varastaminen tai sovellusistunnon väärentäminen. Esimerkiksi varastettua evästettä voidaan käyttää haitallisen istunnon perustamiseen. Istunnon kestoaika on optimoitava, sillä lyhyt istuntoaika on haasteellinen käyttäjälle, koska se kirjaa käyttäjän herkästi ulos sivustolta kesken toiminnan. Pidempi istuntoaika tekee kuitenkin istunnosta myös haavoittuvamman, sillä hyökkääjälle jää enemmän aikaa tehdä haitallisia toimia (Alizai, Tahir, Murtaza, Tahir & Mcdonald-Maier, 2019).

Muita tunnettuja evästeiden toiminnallisuuksien haasteita yksityisyydelle ovat Velagapudi & Gupta (2019) mukaan:

- *Evästeiden luottamuksellisuus*. Evästeet sisältävät yleensä käyttäjän henkilötietoja. Nämä tiedot paljastuvat, jos evästeet siepataan lähetyksen aikana tai varastetaan ennen kuin ne tallennetaan verkkoselaimeen.

- *Evästeiden eheys*. Yksi tärkeimmistä huolenaiheista on eheys, sillä se estää luvatonta käyttäjää kirjoittamasta suoritettavaa evästettä uudelleen. Jos evästeen sisältöä on muutettu todentamisen yhteydessä, todennus epäonnistuu. Jos eheyttä ei ole varmistettu, on mahdollista, että hyökkääjä saa todennustietoja käsiinsä muuntamalla evästettä.

- *Evästeiden tunnistettavuus*. Hyökkääjä voi esiintyä laillisena käyttäjänä lähettämällä sivustolle käyttäjältä varastettuja evästeitä. Tämän vuoksi evästeiden salaus on tärkeää ja se estää laitonta käyttäjän manipulointia.

- *Evästeiden tietosuoja*. Käyttäjän yksityisyyden ja anonymiteetin varmistaminen on erittäin tärkeää ja evästeet sisältävät usein juuri käyttäjän henkilökohtaisia tietoja. Istuntojen on seurattava käyttäjän tietoja vain lyhyen ajan ja istunnon päätyttyä evästeet tulee poistaa. EU:n tietosuojakäytäntöjen mukaan evästeet eivät pääse käsiksi käyttäjän henkilötietoihin, ilman suostumusta. Mikäli näitä tietoja rikotaan, on luvassa valtavia sakkoja.

- *Evästeiden turvallisuusongelmat*. Verkkopalvelimet tunnistavat käyttäjän ja käyttäjän tilan evästeiden avulla. Tällöin käytössä on evästeitä, jotka sisältävät käyttäjän tietoja, muun muassa: nimet, korttitiedot ja tapahtumat. Kun nämä evästeet kirjoitetaan yksinkertaiseen tekstitiedostoon, jota kuka tahansa voi lukea, on meillä käsissämme evästeiden suurin huolenaihe.

Sivakorn ym. (2016) ovat tutkineet, kuinka helposti hyökkääjät voivat kaapata käyttäjän istunnon ja paljastaa esimerkiksi käyttäjän tunnistetiedot sisäänkirjautumistiedot HTTP-evästeiden avulla. Monet suuret verkkosivustot käyttävät yhä salamaatonta yhteyttä eli HTTP:tä, vaikka tarjolla olisi turvallisempi vaihtoehto HTTPS (Hypertext Transfer Protocol Secure). HTTPS on HTTP-protokollan ja TLS/SSL-protokollan yhdistelmä, jonka avulla tiedon siirto internetissä on suojatumpaa.

Palveluntarjoajat uhraavat usein käyttäjiensä turvallisuutta käytettävyyden sijaan, mikä voi johtua mahdollisista kustannusten noususta tai verkon sisäisten toimintojen menettämisestä. HTTPS:n käyttämisen pakottamisella voitaisiin vähentää hyökkäyspintaa, mutta se ei suojaisia kaikkia käyttäjiä, sillä kaikki verkkosivustot eivät tue sitä. On myös huomioitava, että eri selaimilla, kuten Chromella ja Firefoxilla, on lukuisia osia, jotka paljastavat käyttäjän evästeet. Lisäksi vaikka verkkosivusto käyttää HTTPS:ää käyttäjän sisäänkirjautumisen suojaamiseen, kaikki sivustot eivät jatka kirjautumisen jälkeen HTTPS:n käyttämistä, vaan osa siirtyy HTTP:hen. Tällöin käyttäjän kirjautumistiedot on edelleen mahdollista poimia salaamattomasta liikenteestä (Englehardt, Reisman, Eubank, Zimmerman, Mayer, Narayanan & Felten, 2015).

Varastetut HTTP-evästeet voivat antaa hyökkääjille esimerkiksi mahdollisuuden rekonstruoida käyttäjän Google-hakuhistorian, saada selville käyttäjän osoitteen Google-hauista ja mahdollisesti myös salakuunnella käyttäjää Ne voivat myös käyttää tilin toimintoja suorasti, kuten lähettämällä sähköpostia käyttäjän tililtä tai epäsuorasti esimerkiksi vastaanottamalla käyttäjän henkilökohtaisia kyselytuloksia hakukoneelta. Ne antavat mahdollisuuden päästä yksityisiin ja arkaluontoisiin käyttäjätietoihin ja ne voivat myös kiertää autentikointivaatimukset ja saada pääsyn suojattuihin tilitoimintoihin (Sivakorn ym., 2016).

2.8 Evästeet kuluttajien kokemana

Tietosuojaselosteen evästekohdan ja sen mahdollisten evästeitä koskevien liitteiden tarkoituksena on tarjota käyttäjille selkää ja ymmärrettävää tietoa evästeiden käytöstä verkkosivustolla. Käyttäjien tueksi evästeiden tietojen keräämisen tulisi olla läpinäkyvää, jotta käyttäjä ymmärtää mihin evästeiden avulla kerättyjä tietoja käytetään. Vaikka tietosuojaseloste on saatavilla, Kulykin ym. (2018) tutkimuksen mukaan käyttäjät eivät todennäköisesti tutustu siihen ja vain hyväksyvät evästebannerin pois, jotta pääsevät käyttämään sivustoa. Käyttäjien mielestä tietosuojaselosteet ovat myös liian monimutkaisia ja niitä harvoin luetaan tai ymmärretään. Vaikka tietosuojaselosteen idea on olla selkeästi ymmärrettävä, sitä tasoa ei olla ihan vielä saavutettu (Kulyk ym., 2018). Lienee realistista olettaa, että selvästi ymmärrettävää tasoa tuskin nähdäänkään ilman merkittäviä kulttuurillisia tai lainsäädännöllisiä muutoksia, joissa keskiöön otettaisiin käyttäjä ja tarpeiden palveleminen.

Kulykin ym. (2018) tutkimuksessa todetaan, että monet ihmiset suhtautuivat lähtökohtaisesti negatiivisesti evästeiden käyttöön ja olivat huolissaan yksityisyydestään. Vaikka tietosuojaseloste sisälsi myönteisiä lausuntoja evästeiden käytöstä, osa suhtautui edelleen epäluuloisesti lausuntoihin evästeiden käytöstä ja olivat epäluuloisia. Tutkimuksen mukaan osallistujat suhtautuivat erityisen negatiivisesti evästeisiin, jos kolmannet osapuolet oli mainittu. Kuitenkin kun tutkimuksessa osallistujille näytettiin tietosuojaselostetta ja heiltä kysyttiin, poistuisivatko he sivustolta sen perusteella, ei huomattavaa poistumista huomattu negatiivisesti evästeisiin suhtautuneiden joukosta. Sama tapahtui myös silloin, kun mukana oli maininta kolmansien osapuolien evästeistä. Isoimpana tekijänä käyttäjien päätöksissä olivat sivuston ominaisuudet, sillä halu päästä käyttämään sivustoa sai monet käyttäjät sallimaan evästeet todennäköisimmin. Osa käyttäjistä ei ollut tietoisia evästeiden mahdollisista yksityisyyteen liittyvistä seurauksista tai heillä oli väärinkäsityksiä siitä, mitä evästeiden asettaminen ja niiden tietojen kerääminen heidän kohdallaan merkitsee. Käyttäjät yrittivät ikään kuin päästä eroon evästebannerista ja päästä käyttämään sivustoa hyväksymällä evästeet. Monet myös hyväksyivät evästeiden käytön välttämättömänä pahan asioidessaan verkossa. Jotkut halusivat, että heihin kohdennetaan personoituja mainoksia, joten he halusivat, että heidän tietojaan käytetään henkilökohtaisen mainonnan kohdentamiseen. Monet kokivat, että he saavat kattavamman kokemuksen sivustolta evästeet sallimalla eli että se on heille hyödyksi ja he löytävät tarvittavat palvelut tai tuotteet helpommin. Negatiivisia tunteita näissä henkilöissä herätti se, että tietosuojaselosteessa puhuttiin heidän tietojensa myymisestä.

Kulyk ym. (2018) toteavat, että suuri osa käyttäjistä teki siis jatkuvasti kompromisseja verkkosivuston käyttämisen ja sen evästeiden ja oman yksityisyytensä kanssa. Iso osa käyttäjistä piti evästebanneria vain häiriönä surffauksessa sen sijaan, että he ajattelisivat sen tarjoavan tärkeää tietoa, johon olisi syytä kiinnittää huomiota. Tällöin he vain napsauttivat ikkunan pois jatkaakseen

surffausta lukematta tietoja tarkemmin. Enimmäkseen evästeet myös hyväksyttiin kuin hylättiin. Tuloksiin vaikuttivat myös, kuinka luotettavaksi osallistujat sivuston kokivat, kuinka tuttu se oli ja mitä palveluita se tarjosi käyttäjilleen. Mitä luotettavampi ja tutumpi, sitä useammin osallistujat napsauttivat hyväksymisen päästäkseen käyttämään sivustoa. Useat osallistujat vastasivat todennäköisyyden sille, että he avaisivat tietosuojaselosteen saadakseen lisätietoja hyväksymistään evästeistä, olevan alhainen. Vastaajat kokivat hyötyvänsä enemmän sivuston tuomista tiedoista tai eduista, joten he jatkoivat sivuston käyttämistä evästeistä huolimatta. Jotkut myös luulivat, että evästeitä ei käytetä lainkaan silloin, kun he eivät nimenomaisesti suostuneet siihen ja jättivät siten evästebannerin huomiotta ja odottamaan näytölle. Tämä käsitys saattaa kuitenkin olla monen verkkosivuston kohdalla väärä ja osa evästeistä asetetaan ilman hyväksyntää. Samanaikaisesti monet tutkimukseen osallistuneista väittivät olevansa huolissaan evästeiden tietosuojasta, erityisesti palveluntarjoajan avoimuudesta kertoa todenperäisesti, miten palveluntarjoaja käyttää evästeiden avulla kerättyjä tietoja.

2.9 Hallintakeinot

Yue ym. (2010) toteavat että verkkoselaimet itsessään eivät ole turvallisia ja käteviä evästeiden hallintamekanismeja, vaan parasta olisi erillinen evästeiden hallintajärjestelmä, joka on helppokäyttöinen ja se tarjoaa käyttäjälleen minimaalisella tietosuojariskin. Tällaiselle hallintajärjestelmälle olisi kova kysyntä, sillä nykyinen selainten käyttämä menetelmä on käyttäjälle monimutkainen. Kokeellisen hallintajärjestelmän haasteena oli tunnistaa hyödylliset evästeet hyödyttömistä ja tärkeimmäksi mittaustulokseksi nousi tarpeettomien pysyvien evästeiden käytöstä poisto käyttäjien puolesta tietosuoja- ja turvallisuusriskien vähentämiseksi. Tällainen järjestelmä auttaisi käyttäjää hallitsemaan automaattisesti evästeiden käyttöä, auttaen käyttäjää löytämään sopivan tasapainon helpon käytön ja tietosuojariskien välillä.

Yhtenä vaihtoehtona on pohdittu koulutusta käyttäjille, jotta he olisivat tietoisia yksityisyyden suojastaan ja osaisivat käyttäytyvä verkossa suojaten yksityisyyttään. Olisi tärkeää, että käyttäjät osaisivat tehdä perustoimenpiteet, kuten tallennettujen evästeiden poistaminen tai evästeiden estäminen. Tämän lisäksi, mikäli käyttäjän mielenkiinto riittää, voisi olla tarjolla mahdollisuus kehittyneempien työkalujen käyttöön ja seurantaa estävän selainlaajennusten käyttöön (Kulyk ym., 2018). Myös internetin palveluntarjoajat voisivat osallistua yksityisyyden suojan turvaamiseen tarjoamalla käyttäjilleen mahdollisuuden ottaa käyttöön väliaikainen IP-osoite joka kerta, kun he muodostavat yhteyden (Kristol, 2001).

Vaihtoehtona voisi olla myös koneellisesti luettavat tietosuojaselosteet, joista merkittävin on ollut vuonna 2002 käyttöönotettu P3P (Platform for Privacy Preferences Project). Se tarjoaa käyttäjille yksinkertaisen, automatisoidun tavan hallinta henkilökohtaisten tietojensa käyttöä vierailemillaan nettisivuilla. Palvelu ei kuitenkaan yleistynyt, sillä palveluntarjoajat eivät saaneet sitä laajalti käyttöön

järjestelmän monimutkaisuuden ja vapaaehtoisuuden vuoksi ja Microsoft on lopettanut palvelun tukemisen Windows 10:stä eteenpäin (Kretschmer ym., 2021). On olemassa selainlaajennuksia, kuten Privee tai PrivacyGuide, jotka tarjoavat käyttäjälle lyhyitä yhteenvetoja tietosuojakäytännöistä. Haasteena on kuitenkin, että niiden täytyy luottaa käyttäjien ylläpitämään verkkopalveluiden tietokantaan ja vastaaviin tietosuojakäytäntöihin. Nämä vaativat vapaaehtoisten manuaalista työtä, jonka vuoksi ne eivät skaalaudu hyvin. Jos taas tiedon talteenotto on automatisoitu, saattaa syntyä virheille alttiita yhteenvetoja. Yksityiskäytännöt ovat erityisen haasteellisia tietosuojaselosteen automatisoidun analyysin yhteydessä, sillä ne ovat monimutkaisia ja moniselitteisiä. Niiden sanamuodot saattavat olla tarkoituksellisesti moniselitteisiä ja verkkosivuston tarjoajien – sekä toimintaperiaatteiden että oikeudellisten asiakirjojen osalta – tulkinta voi johtaa erilaisiin tuloksiin, jopa alan asiantuntijoiden keskuudessa (Kristol, 2001).

Eräs ratkaisu voisi olla Velagapudi & Gupta (2019) tekemän tutkimuksen mukaan evästeiden salausmekanismi. Suojattu salausmekanismi mahdollistaisi satunnaisen avaimen luomisen jokaiselle uudelle evästeelle tai vanhan evästeen päivittämiselle. Tämä korvaisi aiemman, vanhaan salausmekanismiin sidotun salausavaimen ja salaisi siten evästearvot perusteellisesti. Kun palvelin vastaanottaisi salatun evästeen, se etsisi avainta tietokannasta. Tällaisen mekanismin etuna olisi se, että kertakäyttöisen avaimen käyttö jokaiselle evästeelle rajoittaisi hyökkäyksiä. Sen haittana olisi palvelimen ylikuormitus, joka syntyisi avaimen etsinnästä käytettäessä vanhalla avaimella salattua evästettä ennen uuden evästeen vastaanottamista. Tällöin palvelin hylkäisi tapahtuman ja salauksen purkumekanismin luottamuksellisuus kärsisi, sillä toiston estomekanismia ei olisi taattu, koska kahdella identtisellä evästeellä salaus murtuisi kummalla vain (Velagapudi & Gupta, 2019).

3 TIETOSUOJASELOSTEET

Tämä luku käsittelee tietosuojaselosteita. Ensin käydään läpi niiden yleistä perustietoa, minkä jälkeen tarkastellaan aikaisemmin tehtyjä tutkimuksia tietosuojaselosteista ja nostetaan esiin tietosuojaselosteisiin liittyviä tunnettuja haasteita.

3.1 Yleistä tietosuojaselosteista

Tietosuojasta on tullut haaste yrityksille ja sosiaalisen verkostojen tarjoajille erityisesti digitaalisessa maailmassa. Yritykset käyttävät väistämättä käyttäjien henkilötietoja tarjotakseen heille kohdennettuja palveluita tai tuotteita, monien sovellusten ja palveluiden liiketoimintamallien käytännössä rakentuessa tämän käyttäjätiedon varaan (Kretschmer ym., 2021). Esimerkiksi musiikkiteollisuus (Youtube, SoundCloud, yms.) käyttää käyttäjiensä selaushistoriaa tarjotakseen käyttäjälle sitä musiikkia, josta he ovat kiinnostuneita. Tällaisissa tilanteissa kuluttajille on kerrottava heidän tietojensa käytöstä. Teknologia on tarjonnut mahdollisuuksia markkinoille tavoittaa entistä suurempi yleisö, kerätä henkilökohtaisia tunnistetietoja, verkkosivustojen selausten tietoja ja istuntohistoriaa ja muuta vastaavaa saatavilla olevaa kuluttajatietoa. Markkinointiyritykset käyttävät hyväkseen kehittyneitä tekniikoita kerätäkseen tietoja henkilöistä ja hyödyntääkseen niitä henkilökohtaisen markkinoinnin ja mainosten tarjoamiseen. Käyttäjien tiedoista onkin tullut merkittävä kilpailuetu (Parvaneh, Vijayanta, Amin & Sepideh, 2018).

Verkkosivustojen velvollisuus on paljastaa ja kertoa käyttäjille avoimesti, läpinäkyvästi ja selkeästi, millaisia tietoja he keräävät käyttäjästä ja miksi keräystä tehdään. Nämä tiedot tulee olla kerrottu ymmärrettävällä ja yksityiskohtaisella tavalla tietosuojaselosteessa. Tietosuojaselosteen avulla, käyttäjällä on oikeus ja mahdollisuus saada yleiskuva siitä, kuinka hänen käyttämänsä verkkosivustot tai palvelut hyödyntävät hänen henkilötietojaan (Kretschmer ym., 2021; Parvaneh ym., 2018).

Tietosuojaselosteen tarkoituksena on tiedottaa käyttäjille verkkosivuston käytännöistä ja menettelyistä, jotka liittyvät sivuston tietojen keräämiseen, käyttöön, jakamiseen, pääsyyn, teknologian turvallisuuteen ja käyttöön tietojen keräämisen (evästeiden) osalta, kun käyttäjä vierailee verkkosivustolla. Hyvän ja selkeän tietosuojakäytännön ansiosta käyttäjä voi valita, mitkä osat heidän henkilötiedoistaan voidaan jakaa ja mitkä kolmannet osapuolet voivat päästä käsiksi heidän henkilötietoihinsa (Jafar & Abdullat, 2009).

Usean tutkimuksen mukaan, kun käyttäjä käyttää verkkosivustoa, hän yleensä haluaa päästä käyttämään verkkosivustoa tai palvelua ja hyppää tai ohittaa tietosuojaselosteen sitä lukematta. Tietosuojaseloste näyttäytyy käyttäjälle pitkänä tekstinä, täynnä laillista ammattikieltä, jota tavallinen käyttäjä ei ymmärrä (tai yrittää edes harvoin lukea, kenties osin tästä johtuen). Ne sisältävät myös moniselitteistä kieltä, joka heikentää tietosuojaselosteen tarkoitusta sekä samalla myös verkkosivuston arvoa käyttäjälle. Tietosuojaselosteen ohittaessaan käyttäjä saattaa huonontaa henkilökohtaisiin tarpeisiinsa sopivaa verkkosivuston tai palvelun personointia, vain suostumalla kaikkiin häntä koskeviin pyyntöihin. Käyttäjä saattaa jossain vaiheessa havahtua siihen, että järjestelmä tietää hänestä hyvin paljon ja tuottaa hyvin henkilökohtaisia tuloksia. Käyttäjälle saattaa tulla tällöin kokemus siitä, että järjestelmä tietää hänestä liikaa ja pohdinta siitä, mitä järjestelmässä tapahtuu ja miten omat tiedot siellä kulkevat, saattaa alkaa. Käyttäjä saattaa tällaisen pohdinnan äärellä palata aiemmin ohittamaansa tietosuojaselosteeseen, lukien sen tällä kertaa aiempaa huolellisemmin (Garcia-Barrios, Hemmelmayr & Leitner, 2009; Parvaneh ym., 2018).

Tietosuojaselosteen tulee varmistaa, että käyttäjät saavat ymmärrettävässä muodossa tietoja siitä, miten heidän tietojaan käytetään. Usein siitä yhteinen kieli lakimiesten, teknikkojen ja käyttäjien välillä kuitenkin puuttuu. Haaste on myös tietosuojaselosteen laatijalla, sillä on monimutkaista saavuttaa oikeudellinen yhdenmukaisuus yksityisyyteen liittyvien EU-direktiivien, eri maiden lakien, yritysten sisäisten käytäntöjen ja käyttäjien näkökulmien kanssa. Myös pelkästään hyvä tietosuojalausunto, ei takaa hyvää yksityisyyttä, eikä sen hyvää noudattamista. Käyttäjät usein tietävät sen, että käyttääkseen tiettyä palvelua tai sivustoa, heidän täytyy olla valmiita antamaan itsestään henkilökohtaista tietoa ja tutkimusten mukaan useimmat käyttäjät ovat täysin valmiita tekemään niin (Garcia-Barrios ym., 2009; Parvaneh ym., 2018). Kiinnostava kysymys lienee kuitenkin, voidaanko käyttäjien olettaa ymmärtävän riittävässä laajuudessa kaikkien näiden tietojen luovuttamiseen liittyviä mahdollisia uhkia.

3.2 Tutkimukset tietosuojaselosteista

Vuonna 2018 tehdyssä Kretschmerin ym. tutkimuksessa todettiin, että vain hyvin harva käyttäjä lukee tietosuojakäytäntöjä ja kaikkien niiden selosteiden lukemiseen, joita käyttäjä kohtaa, kuluisi keskimääräisellä kuluttajalla aikaa satoja tunteja vuodessa. Lisäksi Parvaneh ym. (2018) tekemässä tutkimuksessa todetaan, että käyttäjät jättävät useimmiten tietosuojakäytännöt huomiotta. Jos niitä ei

jätetä huomiotta, käyttäjä ei silti ymmärrä tietosuojaselostetta tietosuojakäytäntöjen monimutkaisuuden vuoksi.

Arcand, Nantel, Arles-Dufour ja Vincent (2007) totesivat myös, että jo pelkkä tietosuojaselosteen läsnäolo vaikuttaa myönteisesti koettuun yksityisyyden tietojen hallintaan. Sillä, että käyttäjä luki tietosuojaselosteen, ei välttämättä ollut positiivista vaikutusta yksityisyyden hallinnan ja kokemuksen tunteeseen, sillä käyttäjä ei ymmärtänyt lukemaansa. Lisäksi, jos kuluttaja luki tietosuojaselosteen, se ei rauhoittanut kuluttajaa, vaan niistä heräsi epäilyksiä ja ahdistusta, sillä kuluttajat tulivat tietoisiksi omien tietojensa herkkyydestä ja niistä koskevista uhkista. (Arcand ym., 2007).

Jafar & Abdullat (2009) tutkivat käyttäjien ymmärrystä tietosuojakäytäntöihin sadalla eri verkkosivustolta, jotka keskittyivät henkilökohtaisiin tunnistetietoihin. Heidän tutkimuksensa mukaan, tutkimuksen verkkosivustoja käyttävät miljoonat ihmiset päivittäin ja suuri osa näistä on haavoittuvassa asemassa. Esimerkiksi heidän tutkimuksensa mukaan, 47 % käyttäjistä ei ole korkeakoulututkintoa ja noin 20 % käyttäjistä on alaikäisiä. Jafar ja Abdullat tutkivat Google, Yahoon, Myspacen ja Facebookin tietosuojalausuntojen luettavuutta. Yleinen päätelmä oli se, että Yahoo:ta lukuun ottamatta, tietosuojaselosteiden tietosuojakäytäntöjen ymmärtäminen vaati vähintään 2-vuoden korkeakouluopintojen suorittamisen. Pääkysymys tutkimuksessa oli se, onko verkkosivuston mahdollista tarjota oikeudellisesti sitova ja ymmärrettävä lausunto, jonka suurin osa käyttäjistä ymmärtää. Yahoo oli näistä neljästä ainoa, joka onnistui tarjoamaan selkeän ja ytimekkään tietosuojaselosteen, ilman että käyttäjän tarvitsi olla muuten kuin peruskoulun käynyt. Tämä todistaa sen, että suuri yritys, jolla on monia toisiinsa liittyviä tahoja, voi tarjota ja ylläpitää laillisesti sitovaa tietosuojakäytäntöä, joka ei ole monimutkainen, suurikokoinen tai vaadi korkeakoulutasoisia opintoja. Yritysten tulee pyrkiä yksinkertaistamaan tietosuojakäytäntöjään siten että tietosuojaselosteen lukeminen on helppoa. On kuitenkin huomautettava, että tutkimus on tehty vuonna 2009 ja tämän jälkeen on tullut voimaan uusia lakeja ja asetuksia.

Garcia-Barrios ym. (2009) ovat artikkelissaan pohtineet ratkaisuehdotusta, jonka avulla voisi olla mahdollista kuroa umpeen kuilua yksityisyyden ja personointiin liittyvien järjestelmien välillä. Pyrkimyksenä on, että lailliset yksityisyysongelmat ja niiden seuraukset olisivat käyttäjien ymmärrettäviä ja hallittavissa. Haasteena oli löytää tasapainoinen ratkaisu, jossa oli täydellinen lainmukaisuus, kattavat yksityisyyteen liittyvät ominaisuudet sekä käyttökelpoinen muotoilu. Ottamalla käyttöön dynaamisia ja käyttäjäystävällisiä mekanismeja, saaden aikaan vuorovaikutusta yksityisyysasetusten kanssa, voisi olla mahdollista ratkaista osittain yksityisyyteen liittyviä ongelmia.

Tutkijat ehdottavat ratkaisuksi mukautuvaa tietosuojaselostetta, joka auttaa tunnistamaan ja ymmärtämään tietosuojaongelmien ratkaisemisen ongelmallisia kohtia käyttäjää mukailevassa järjestelmässä. Isoin haaste on ymmärrettävyys: käyttäjien täytyisi helposti ymmärtää miten heidän tietojaan käytetään, mutta yrityksen täytyisi silti yrittää piilottaa laskennallinen monimutkaisuus ja yrityssalaisuudet niin, etteivät ne ole kilpailijoiden saatavilla. Mukautuva

tietosuojalausunto rakentaisi tähän tukevan oikeudellisen kehyksen, jossa käyttäjän tulisi hyväksyä ensin alkuperäinen tietosuojalausunto käyttääkseen järjestelmää. Tässä olisi vaihtoehtoina eri tasoja, kuten: yksityinen, suositeltu, julkinen ja mukautettu. Tämän valinnan jälkeen järjestelmä tunnistaisi ristiriitoja tämän alkuperäisen tietosuojalausunnon ja käyttäjän kohtaamien tietosuojalausuntojen kanssa (Garcia-Barrios ym., 2009).

Tietosuoja-analyytikot ovat pohtineet eri tapoja auttaakseen käyttäjiä ymmärtämään tietosuojakäytäntöjä selkeämmin. Tavoitteena olisi tehdä tietosuojaselosteesta ytimekäs ja kattava, tarpeeksi lyhyt luettavaksi ja täysin ymmärrettävä. He käyttivät tekstin luokittelua ja koneoppimista luokitellakseen kappaleita tietosuojaselosteesta. Tämä auttaisi käyttäjää tarkastamaan tietosuojaselosteen jäsennellysti ja huomaamaan helposti ne kappaleet, jotka heitä kiinnostavat. Epävarmuutta on kuitenkin vielä sen suhteen, noudattavatko palveluiden tarjoajat tosiaan tietosuojakäytäntöjä tietosuojaselosteen mukaisesti. Analyytikot kokeilivat koneellisesti tietosuojaselosteen osien jakamista alaryhmiin, tehden lukemisen käyttäjälle hyvin organisoiduksi ja auttaen löytämään asiaankuuluvan osan tietosuojakäytännöistä. Jos käyttäjä on esimerkiksi kiinnostunut henkilötietojensa keräämisestä, hän voi etsiä tämän alaluokan ja löytää siitä kaikki henkilötietojen keräämiseen liittyvät seikat jäsenneltynä. Jatkossa tutkijoilla on pyrkimys automatisoida tietosuojakäytäntöjen poimiminen, rakentaakseen suuremman tietojoukon uutta tutkimusta varten, jotta voidaan varmistaa tulosten tarkkuus ja paikkansa pitävyys. He myös ehdottavat tietosuojakäytäntöjen yhdenmukaistamista, jotta kuluttajan olisi helppoa löytää häntä kiinnostavat kohdat ilman erillistä ohjelmaa, joka lukee tietosuojaselosteita lävitse ja perkaa niitä jatkuvasti (Parvaneh ym., 2018).

Sigmundin (2021) tutkimuksessa tutkittiin käyttäjien motivaatiota tietosuojaselosteiden lukemiseen. Suurimmaksi ongelmaksi nostettiin, että käyttäjät eivät alkuaankaan lue tietosuojaselosteita. Vaikka ne olisivat siis kirjoitettu hyvin, ei tällä välttämättä ole minkäänlaista vaikutusta. Suurin osa (74 %) ohittaa tietosuojakäytännöt niitä lukematta. Tietosuojaseloste koetaan kuormittavaksi ja se aiheuttaa negatiivisia tunteita. Vaikeasti luettava ja monimutkainen tietosuojaseloste on siis merkittävä este sen lukemiselle.

Tietosuojaselosteilla pyritään vähentämään käyttäjien epäluuloja yksityisiin tietoihinsa liittyviä huolia kohtaan, mutta tähän tarkoitukseen ne ovat liian monimutkaisia ja epämääräisiä, eivätkä käyttäjät siis halua yleensä lukea niitä. Kuluttajat kokevat ylikuormitusta ja maailmasta on tulossa liian monimutkainen, eivätkä käyttäjät pysty sisäistämään kaikkea päätöksentekoon tarvittavaa tietoa. Kuitenkin sen olemassaolon havaittiin lisäävän halukkuutta paljastaa tietoja, maksaa tuotteista ja palveluista sekä tukea luottamusta. Vastaajat myös näkivät tietosuojaselosteissa enemmän suojaa kuin mitä niissä todellisuudessa oli, mutta samalla pitivät niitä riittämättöminä vastaamaan juuri heidän yksityisyytensä suojaan liittyviin tarpeisiinsa.

Käyttäjät haluavat jakaa henkilötietojaan täysin vapaaehtoisesti, sillä he käyttävät monipuolisesti erilaisia sovelluksia, jotka keräävät heidän henkilötietojaan, rakentaen käyttäjälle profiilia ja ostostyyliä sekä tarjoten laadukasta

kohdennettua mainontaa. Monet myös käyttävät teknologioita, jotka loukkaavat heidän yksityisyyttään, eivätkä he välitä tietosuojakäytännöistä. Tämä ei kuitenkaan tarkoita sitä, että he luopuvat yksityisyydestään, vaan he tuntevat itsensä neuvottomiksi kaikkien tietoselosteiden keskellä. Käyttäjät eivät myöskään ymmärrä, miten heidän tietojaan voidaan hyödyntää, sillä tämä edellyttäisi teknistä ja sosiologista asiantuntemusta (Sigmund, 2021).

Sigmundin (2021) tutkimuksessa todetaan, että tarvitsisimme toisenlaisen vaihtoehdon kuin tietosuojaselosteen, joka turvaisi yksityisyyden ja tietojen asianmukaisen käsittelyn ja olisi ymmärrettävä peruskuluttajalle. Tarvitsisimme yleismaallisia sääntöjä tietosuojalausuntojen laatimiseen, jotka tasapainottaisivat nykyistä tilannetta, vaikka ne eivät pystyisikään kunnioittamaan yksilöllisiä eroja. Tutkimuksessa ehdotetaan, että käyttäjän valinnan tulee olla täsmällinen, yksiselitteinen, ymmärrettävä, helppokäyttöinen eikä liian täynnä tietoa. Tietosuojaseloste voisi siis olla eriytetty eri käyttäjien ja heidän haluamansa turvatason mukaan. On myös olemassa käyttäjien luottamusta lisääviä mekanismeja, jotka varmistavat käyttäjien henkilökohtaisten tietojen turvallisuuden, kuten esimerkiksi kolmannen osapuolen sertifikaatit, taloudelliset korvaukset tai vaikkapa taloudelliset korvaukset tietosuojaloukkauksista.

3.3 Tietosuojaselosteiden haasteet

Useat ponnahdusikkunat sivustoilla kertovat kuluttajalle evästeiden käyttämisestä ja tarjoavat jonkinlaista mahdollisuutta valita vain välttämättömät evästeet tai ei-välttämättömät evästeet tai mahdollisesti mukauttaa evästeasetuksia tarkemmin. Lisätietoja evästekäytännöistä on saatavilla tietosuojaselosteesta tai tietosuojan kohdalta. Tietosuojaselosteesta löytyy tarkemmin oma kohtansa evästeille tai sitten käyttäjä ohjataan uudelle sivustolle, jossa kerrotaan evästeistä tarkemmin. Tämän työn tutkimuksessa perehdyttiin siihen, millä tasolla tietosuojaselosteiden evästekohdan ymmärrettävyydessä oltiin vuoden 2021 kymmenen eniten vieraillun sivuston osalta.

Yhteenvetona nykyisissä tietosuojaselosteissa todetaan olevan monia haasteita. On selkeästi olemassa paradigma, jonka mukaan kuluttajat ovat huolissaan yksityisistä tiedoistaan palveluita käyttäessään, mutta eivät kuitenkaan halua esteitä ja hidasteita palvelun käytölle. Kuluttajat pääosin ohittavat tietosuojaselosteen sitä lukematta. Aikomus tai motivaatio tietosuojaselosteen lukemiselle ei ole myöskään korkealla, sillä se aiheuttaa negatiivisia ja kuormittavia tunteita. Silloinkin, kun kuluttajat päätyvät lukemaan tietosuojaselosteen, sen ei koeta tuovan lisäarvoa, sillä se on pitkä, vaikea ymmärtää ja vaatii joltain osilta myös muutaman vuoden korkeakoulutasoista tutkintoa tai vastaavaa ymmärrystä. Yksityisyys on selkeästi haaste ja maailman monimutkaisuus ja toiminta ylittävät ihmisen kyvyn ymmärtää se.

Kuluttajat haluavat olla vallassa yksityisyytensä ja henkilötietojensa turvallisuudesta, kun he tekevät esimerkiksi ostoksia verkkosivustoilla. Luottamus ja sen puute ovat merkittävät tekijä ostopäätöksen tekemisessä. Mikäli kuluttaja

kokee, että hänellä on kontrolli omiin yksityisiin tietoihinsa verkkosivustolla, se lisää luottamusta vaikuttaa positiivisesti ostopäätöksen lukitsemiseen. Joten luottamus ja yksityisyys liittyvät vahvasti toisiinsa, kun kuluttajat käyvät verkkokauppaostoksilla. Yritykset ovat tämän tiedon varjolla keskittyneet käyttämään tietosuojalausuntoja. Haasteita kuluttajille tuo se, että tietosuojalausunnot ovat joka sivustolla eri muodossa, sisältäen eriasteista hallintaa henkilötietojen hallinnassa. Käyttäjät ovat täysin riippuvaisia siitä, kuinka oikeudenmukaisesti yritykset todella käsittelevät heidän tietojaan ja käyttäjät ovat joka päivä sen valinnan edessä, valitsevatko he palvelun käyttämisen, sillä ehdolla, että heillä on mahdollista luovuttaa yksityisiä tietoja itsestään. Tämä on käyttäjille panostavaa ja tiedon määrä ja riskien läsnäolo on kuormittavaa. Tietosuojaselosteen pitäisi vähentää käyttäjien pelkoa henkilökohtaisia tietojaan kohtaan, mutta asia ei kuitenkaan ole niin (Arcand ym., 2007).

4 KESKEISET LAIT JA ASETUKSET

Euroopan Unionin (EU) tietosuojan toteutumisesta määrätään EU:n perusoikeuskirjassa. Sen mukaan jokaisella on oikeus henkilötietojensa suojaan, itseään koskevien tietojen tarkasteluun ja tarvittaessa myös niiden oikaisuun. Henkilötietojen suojan maininta perusoikeuskirjassa mahdollistaa sen, että EU:lla on erityinen oikeusperusta antaa säädöksiä tämän perusoikeuden turvaamiseksi (Euroopan unionin neuvosto, 2022).

Kaikkia EU:ssa toimivia yrityksiä alkoivat koskea samat tietosuojasäännöt, kun yleinen tietosuoja-asetus (GDPR) tuli voimaan toukokuussa 2018. Yhtenäinen ja ajantasainen tietosuojalainsäädäntö on tärkeää, sillä sen avulla taataan henkilötietojen suoja perusoikeutena, mahdollistetaan digitaalitalouden kehittyminen ja tehostetaan rikollisuuden ja terrorismin torjuntaa. Sen avulla vahvistetaan yksilön oikeudet ja tietojen käsittelijän velvollisuudet sekä varmistetaan sääntöjen noudattaminen ja asetetaan sanktiot noudattamattomuudesta. Keskeisin EU:n henkilötietoja koskeva säädös on vuonna 1995 käyttöön otettu tietosuojadirektiivi (Euroopan unionin neuvosto, 2022).

Nopea teknologinen kehitys on tuonut omat haasteensa henkilötietojen suojaamisen saralla. Tiedon keräämisen määrä on kasvanut valtavasti ja tietoja jaetaan paljon enemmän kuin ennen, jopa maailmanlaajuisesti. Digitalisaation edistämiseksi on taattava korkeatasoinen henkilötietojen suoja ja tietojen vapaa, mutta suojattu liikkuminen (Euroopan unionin neuvosto, 2022).

Internet on jatkuvassa muutoksessa ja uusia tekniikoita ja palveluita syntyy jatkuvasti, luoden sekä mahdollisuuksia että uhkia. Internet on suunniteltu yksinkertaiseksi ja avoimeksi viestintäkanavaksi ja sen avoin luonne mahdollistaa viestin tehokkaan ja laaja-alaisen välittämisen ympäri maailman. Samalla myös mahdollisuus väärinkäytöille ja uudenlaisille rikoksille on läsnä. On mahdollista, että rikolliset tahot saavat internetin kautta tietoja haltuunsa, yksityishenkilön tietoja käytetään häntä vastaan tai levitetään ympäriinsä. Tietoverkkojen käyttö, teknologian läsnäolo ja kaikkialla oleva internet on muuttanut toimintaympäristöä samalla myös uhkaavaksi. Osaa internetin alkuajoilta olevista teknisistä ratkaisuista ei ole suunniteltu tietoturvalliseksi internetin nykyiseen

käyttöympäristöön. Sähköisen viestinnän lakien ja asetuksien tarkoituksena on tuoda turvaa yksilölle, sillä riskejä internetin käytössä on (Innanen & Saarimäki, 2012).

Sähköisen viestinnän lainsäädännön kokonaisuuden muodostaminen on haastavaa, sillä siihen liittyvä lainsäädäntö on hajanaista ja se on osin vaikeaselkoista. Lait ja asetukset koskevat yhteiskunnan kaikkia toimijoita, joten niiltä voitaisiin edellyttää selkeyttä ja ymmärrettävyyttä. Tämä ei kuitenkaan toteudu, sillä lakien vyyhti on iso, osittain päällekkäinen ja vaikeaselkoinen niin sisällöltään kuin termistöltäänkin. Uusia lakeja tulee jatkuvasti ja vanhoja päivitetään. Tämä muutos johtuu nopeasta teknologian kehittymisestä sekä siitä, että internet on jatkuvasti ympärillämme, tallentaen jatkuvasti uutta tietoa meistä. Sähköisen viestinnän lainsäädäntöä Suomessa on hajautettu moniin eri lakeihin ja tässä työssä käsittelen niistä evästeiden kannalta tärkeimpiä. Näitä ovat perustuslaki, laki sähköisen viestinnän palveluista, tietosuojalaki ja GDPR, jonka yhteydessä lakia on tutkittu tässä työssä vielä tarkemmin nimenomaan evästeiden näkökulmasta. Muita mainittavia lakeja, joita tässä työssä ei ole käsitelty, ovat verkkotunnuslaki, laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista sekä sähkökauppalaki, joiden käsittely ei tuo lisäarvoa tämän työn aiheen käsittelylle (Innanen & Saarimäki, 2012).

4.1 Yksityisyyden suoja ja perusoikeudet

Yksityisyys on alun perin määritetty oikeudeksi olla yksin. Uudemmassa käsitteen määritelmässä yksityisyys on saanut kontekstuaalisemman luonteen. Yksityisyyttä koskevat huolet eivät ole uusia sillä yritykset ovat keränneet asiakastietoja jo vuosikymmeniä. Kuitenkin teknologian ja internetin kehittymisen myötä on ilmaantunut uusia haasteita yksityisyydelle ja kuluttajien tietoja voidaan kerätä, seurata ja jakaa ja he voivat tietämättään menettää hallinnan yksityisten tietojensa levittämiseen. Internetin suurin uhka kuluttajien mielestä on yksityisten tietojen hallinnan menetys. Tämän vuoksi on ryhdytty lainsäätäjien puolesta tarjoamaan kuluttajille oikeudenmukaisia tiedotuskäytäntöjä verkossa. Vaikka huoli yksityisyydestä on globaali, silti suhteellisen harva kuluttaja on ryhtynyt konkreettisiin toimiin suojatakseen tietoturvansa verkossa ja harva lukee tietosuojakäytäntöjä lainkaan. Tästä syntyy paradoksi, sillä kuluttajilla on suuri huoli yksityisistä tiedoistaan verkossa ja silti heillä on vähäinen kiinnostus lukea tietosuojaselosteita. (Arcand ym., 2007).

Yksityisyys on kansainvälisen luettelon ihmisoikeuksista vaikein määritellä, sillä se vaihtelee kontekstin ja ympäristön mukaan. Erityisesti tieto- ja viestintätekniikan alalla, yksityisyyden käsite liittyy hyvin tiiviisti tietosuojan eli yksityisyyden suojan käsitteeseen. Termiä tietosuoja kutsutaankin toisinaan myös yksityisyyden suojaksi. Yksityisyyden suoja tarkoittaa ihmisen henkilötietojen ja henkilökohtaiseen toimintaan liittyvien tietojen keräämisen ja käsittelyn rajoittamista siten, ettei henkilön yksityisyys vaarannu. Tietosuojaan yksityisyyteen liittyvät kysymykset ovat nousseet esille jatkuvasti kehittyvän teknologian,

sähköisen kaupankäynnin, markkinoinnin ja kansallisen turvallisuuden vuoksi. Tietosuojan ja yksityisyyden asiat koskevat meitä kaikkia. Joudumme päivittäin tekemisiin yksityisyyden kanssa, asioidessamme verkkosivustoilla, sovelluksissa, internetissä, kaupassa tai viranomaisten kanssa. Matkapuhelinoperaattoriimme seuraa liikkeitämme, kaupungilla kulkiessamme tallennumme kauppojen valvontakameroihin, liikenteessä autojamme valvovat kamerat ja sähköisestä toiminnastamme jää aina jälki (Järvinen, 2002; Garcia-Barrios ym., 2009).

Yksityisyys on jatkuvasti elämässämme läsnä kaikilla henkilökohtaisen elämän osa-alueilla ja kanssakäymisessämme yritysten ja yksilöiden kanssa. Yksityisyydellä on useita määritelmiä ja tulkintoja, eikä sitä siten ei ole helppo määritellä yksiselitteisesti. Kaksi teemaa nousee kuitenkin esiin yksityisyyttä määritellessä: miten yksityisiin tietoihin pääsee ja mihin niistä pääsee käsiksi sekä yksilön hallinta omia tietojaan kohtaan. Yksityisyys on joka tapauksessa jokaisen ihmisen perusoikeus, eli se on turvattava riittävin keinoin (Leite, dos Santos & Almeida, 2021; Marino, 2021).

Garcia-Barrios ym. (2009) mukaan yksityisyys on rajojen sääntelyä ja siihen vaikuttavat myös yksilöiden kokemukset ja odotukset. Yksityisyys on siis yksilön oikeus pitää yllä omaa henkilökohtaista tilaansa, johon muut ihmiset ja organisaatiot eivät saa luvatta puuttua. Yksityisyyden käsite jaetaan tutkijoiden kesken usein neljään käsitteeseen:

1.) Kehon yksityisyys ja koskemattomuus
2.) Henkilökohtaisen käyttäytymisen yksityisyys (mukaan lukien arkaluontoiset asiat, kuten esimerkiksi poliittinen toiminta, seksuaalisuus, uskonto)
3.) Henkilökohtaisen viestinnän yksityisyys (mukaan lukien kuuntelu)
4.) Henkilötietojen yksityisyys (tietojen yksityisyys ja tietosuoja)

Eurooppalaisessa kontekstissa oikeus yksityisyyteen on pitkälle kehittynyt ja säännelty EU:ssa. Myös Taloudellisen Yhteistyön ja Kehityksen Järjestö (OECD) on antanut yksityisyyden suojaa koskevat suosituksensa. Suosituksiin kuuluu seitsemän periaatetta, jotka ovat:

1.) *Huomautus*. Käyttäjälle tulee ilmoittaa hänen tietojen keräämisestään.

2.) *Tarkoitus*. Käyttäjän tietoja tulee kerätä vain ilmoitettuun tarkoitukseen.

3.) *Suostumus*. Käyttäjän tietoja ei saa luovuttaa ilman käyttäjän suostumusta.

4.) *Turvallisuus*. Kerätyt tiedot on suojattava väärinkäytöksiltä.

5.) *Luovuttaminen*. Käyttäjälle tulee ilmoittaa, kuka hänen tietojaan kerää.

6.) *Pääsy*. Käyttäjän tulee päästä käsiksi tietoihinsa ja pystyä korjaamaan epäkohtia

7.) *Vastuuvelvollisuus*. Tietojen kerääjät ovat kerätyistä tiedoista vastuussa

Oikeudellinen yhteensopivuus yksityisyyden suojatoimien kanssa riippuu Euroopan maan lakien paikallisesta täytäntöönpanosta. OECD:n suositukset eivät kuitenkaan ole sitovia, joten tietosuojalait käytännössä vaihtelevat eri puolilla Eurooppaa. Euroopan komissio halusi yhtenäistää tietosuoja-asetusta ja antoi direktiivin koskien yksilöiden suojelua henkilötietojen käsittelyssä ja tietojen vapaata liikkuvuutta (Garcia-Barrios ym., 2009). Tämä direktiivi on kuitenkin korvattu GDPR:llä, joka tuli voimaan vuonna 2018.

Teknologia on antanut sysäyksen yksityisyyden määritelmän päivittämiseen tai muuttamiseen ja sen rooli on viime aikoina korostunut yksityisyyden määrittelemisessä. Teknologinen kehitys uhkaa yhteiskunnallisia normeja, jolloin voidaan pohtia, riittävätkö olemassa olevat oikeudelliset suojat suojaamaan yksilöitä yksityisyyden loukkauksilta. Teknologian kehityksen myötä kehittyvät kuitenkin myös keinot yksityisyyden turvaamiseen. HTTP-yhteys, tietosuojakäytäntöjen uusiminen ja kehittäminen ja eettinen tiedonkeruu ja tiedon käyttäminen ovat esimerkkejä verrattain viimeaikaisesta kehityksestä. Täytyy myös muistaa tasapaino, sillä kaikki verkossa tapahtuva seuranta ei ole pahantahtoista. Kaikki käyttäytymisen seuranta ei ole toivottua, mutta loppuen lopuksi käyttäjän pitäisi pystyä itse pohtimaan ja räätälöimään yksityisyyteensä liittyvät valinnat ja päättää haluavatko he, että heidän käyttäytymistään seurataan. Käyttäjien vastuulle jää yksityisyyden räätälöinti itse siten, että he saavat juuri itselleen mahdollisimman personoidun näkymän, kuitenkaan vaarantamatta heille tärkeitä yksityisiä asioita ja pitäen kokonaisuuden hallinnassaan (Marino, 2021).

Evästeiden määrittely saattoi olla ensimmäinen IETF-standardi tekniikan ja yksityisyyden risteyksessä, joka on saanut laajaa julkista huomiota. Vuonna 1996 Yhdysvaltain liittovaltion kauppakomissio (FTC) kutsui koolle kokouksen, jossa aiheena oli kuluttajien yksityisyys. Kokouksen työpöydälle liittyi olennaisesti WWW:n käyttö ja siihen liittyvät tietosuojakäytännöt ja kuluttajien valinnaismahdollisuudet henkilötietojen käytön suhteen. Tämän kokouksen seurauksena alettiin keskustella yksityisyysasetusten mekanismista ja syntyi P3P, jonka kehitys on kuitenkin lopetettu, eikä se koskaan levinnyt isosti sen vaikeuden ja monimutkaisuuden vuoksi. Erilaisista direktiiveistä, laeista ja asetuksista on hyötyä ylipäätään vain silloin, kun niitä noudatetaan. Emme voi koskaan varmuudella tietää, päätyvätkö tiedot myös varsinaisen käyttötarkoituksensa ulkopuolelle vai käytetäänkö niitä laittomasti. Lisäksi tietosuoja voi pettää väärinkäsityksen tai inhimillisen erehdyksen seurauksena (Kristol, 2001).

Yksityisyys on jatkuvasti esillä teknologian kehityksen myötä ja esimerkiksi tietovuotoja tapahtuu jatkuvasti. Verkon käyttäjät ovat yleisesti ottaen huolestuneita yksityisyydestään ja tarvitsisivat selkeitä ohjeita ja käytösmalleja yksityisyytensä suojaamiseksi. Käyttäjät tekevät jatkuvasti kauppaa yksityisyytensä kanssa asioidessaan verkossa, eikä selkeitä ratkaisumalleja ole tarjolla. Käyttäjä joutuu jokaisella verkkosivustolla erilaisen valinnan eteen, eivätkä käyttäjät usein lue tai ymmärrä lukemaansa tietosuojaselostetta. Tällä hetkellä olisi kova

tarve saada teknologinen ratkaisu, jossa verkon käyttäjä voisi määrittää yksityisyytensä rajat ja tämä määritys toimisi ja turvaisi johdonmukaisesti kuluttajaa internetin käytön aikana.

Perustuslain mukaan julkisen vallan on turvattava perusoikeuksien ja ihmisoikeuksien toteutuminen, eikä tämä rajoitu vain valtion ja yksilön väliseen suhteeseen, vaan myös yksilöiden keskinäisiin suhteisiin. Tässä työssä tarkastellaan nimenomaan perusoikeuksien toteutumista sekä muita lakeja ja asetuksia sähköisen viestinnän näkökulmasta (Innanen & Saarimäki, 2012).

Jokainen taho, joka toimii sähköisen viestinnän parissa, joutuu ottamaan huomioon ajantasaisen lainsäädännön ja ottamaan perusoikeudet huomioon. Perusoikeuksien korostettu oikeudellinen asema tekee niiden huomioonottamisen välttämättömäksi. Ne eivät ole vain lakeja, vaan ne toimivat myös yhteyskunnallisten arvojen ilmaisijoina ja ovat yhteiskunnan perusarvoja, joiden täytyy toteutua myös sähköisessä viestinnässä. Internet on keskeinen väline, jonka avulla omia perusoikeuksia on mahdollista toteuttaa. Se mahdollistaa yhteiskunnallisen osallistumisen, mielipiteiden vaihdon, poliittisen vaikuttamisen ja julkaisutoiminnan, jotka edesauttavat sananvapauden ja demokratian toteutumista. Internet ylittää rajat ja auttaa kulttuurien välisessä vuorovaikutuksessa ja kommunikoinnissa. Kun tarkastellaan perusoikeuksia sähköisen viestinnän näkökulmasta, saadaan hahmotettua, kuinka monimutkaisesta kokonaisuudesta onkaan kyse (Innanen & Saarimäki, 2012).

Perustuslaissa on turvattu yksityiselämän suoja, joka on sähköisen viestinnän näkökulmasta yksi keskeisimmistä perusoikeuksista. Yksityisyys määritellään yleensä oikeudeksi olla yksin, eli jokaisen yksityiselämä, kunnia ja kotirauha on turvattu ja henkilötietojen suojasta säädetään tarkemmin omalla lailla ja yksityiselämää suojataan myös kansainvälisten sopimuksien turvin (Jafar & Abdullat, 2009).

Lähtökohtana yksityiselämän suojalle on se, että yksilöllä tulee olla oikeus elää omaa elämäänsä ilman viranomaisten tai muiden ulkopuolisten tahojen mielivaltaista tai aiheetonta puuttumista yksityiselämään. Sähköisen viestinnän näkökulmasta erityisesti henkilötietojen suoja korostuu, mahdollistaen perusoikeuksien toteuttamisen. Muita tärkeitä kohtia ovat viestinnän luottamuksellisuus, sananvapaus, omaisuudensuoja ja sivistykselliset oikeudet (Innanen & Saarimäki, 2012).

4.2 Laki sähköisen viestinnän palveluista

Laki sähköisen viestinnän palveluista on tullut voimaan 1.1.2015 ja osa siitä osittain myöhemmin. Tätä pro-gradutyötä kirjoittaessa keväällä vuonna 2022 lakia oli päivitetty 27 kertaa sen voimaan tulosta lähtien, joista kaksi viimeisintä muutosta on tullut voimaan 1.1.2022. Finlexin (2014) mukaisesti ”Lain tavoitteena on myös turvata sähköisen viestinnän luottamuksellisuuden ja yksityisyyden suojan toteutuminen.” Sähköisen viestinnän palveluista annetun lain luvussa 24 on säädetty sähköisestä suoramarkkinoinnista ja evästeistä. Lain pykälässä 205 § on

säädetty evästeiden käyttämisestä. Sen mukaan eväste on pieni tietojoukko, joka mahdollistaa käyttäjän tekemien toimintojen seuraamisen mahdollisuuden tietyn selainistunnon aikana sähköisissä palveluissa (Finlex, 2014).

Tämän lain mukaan palveluntarjoajan on lupa tallentaa evästeitä käyttäjän päätelaitteelle ja käyttää evästeiden tietoja, mikäli käyttäjä on antanut suostumuksena. Palvelun tarjoajan on myös tarjottava käyttäjälle kattavat tiedot ymmärrettävässä muodossa tietojen käytön tarkoituksesta ja niiden tallentamisesta (Finlex, 2014; Voutilainen, 2020).

Evästeiden avulla digitaalisen palveluntarjoajan on mahdollista saada käyttäjästään tietoa mm. käyttäjän toiminnasta, linkkien käyttämisestä ja muista palvelussa tehdyistä valinnoista. Evästeitä on erilaisia ja niitä voidaan tallentaa käyttäjän laitteelle selainistunnon ajaksi (istuntoevästeet) tai pidempiaikaisesti (pysyvät evästeet). Evästeitä käytetään digitaalisissa palveluissa teknisen toteuttamisen takia sekä käyttäjien toimien seuraamiseksi, joita he digitaalisessa palvelussa tekevät. Evästeiden tarkoituksena on kerätä tietoa palvelun käyttäjämääristä, kehittää sähköisiä palveluita tietojen avulla ja kohdentaa markkinointia. Jos digitaalinen palveluntarjoaja käyttää pysyviä evästeitä ja käyttäjä palaa uudelleen samaan palveluun, palvelin voi pyytää tältä evästeeltä tallennettuja tietoja selaimelta. Pysyvän evästeen avulla on mahdollista identifioida tietty päätelaite ja tietoja käyttäjän aiemmasta käytöstä voidaan yhdistää mahdolliseen tulevaan käyttöön. Jos palvelun käyttäjä on antanut palveluun itsestään identifiointitietoja aiempien vierailujensa aikana, voidaan henkilö ja hänen käyttäytymisensä yksilöidä täysin (Voutilainen, 2020).

Kun käyttäjä alkaa käyttämään jotain digitaalista palvelua tai palaa siihen uudelleen, digitaalisen palvelun verkkopalvelin lähettää käyttäjän selaimelle evästettä koskevan tallentamispyynnön. Jos käyttäjä ei nimenomaisesti estä evästeen käyttöä, selain hyväksyy sen käyttämisen. Evästeiden käyttö täytyy nimenomaisesti hyväksyä, eli käyttäjä antaa suostumuksen evästeille. Suostumuksen hankkiminen on laissa säädetty palveluntarjoajan hoidettavaksi. Suostumuksen täytyy olla yksiselitteinen, eikä esimerkiksi hyväksyminen arvontaan ole suostumus asettaa evästeitä käyttäjän päätelaitteelle. Suostumuksesta on tultava ilmi evästeiden toiminta-aika ja kolmansien osapuolien mahdollisuus käyttää evästeiden tietoja (Voutilainen, 2020).

Sähköisen viestinnän palvelun lain pykälän 205.2 §:n mukaan suostumusta ei tarvitse pyytää silloin, kun sähköiseen palveluun on tunnistauduttava. Tunnistautuneen istunnon hallintaa varten digitaalinen palvelu joutuu tallentamaan evästeitä käyttäjän selainistunnon hallinnoimiseksi ja varmistaakseen sen turvallisen käytön. Tällöin eväste vain välittää viestiä ja istunto voidaan hoitaa turvallisesti ja sujuvasti tunnistautuneena uloskirjautumiseen saakka. Suostumusta evästeen käyttöön ei tarvitse pyytää myöskään silloin, kun evästeen käyttö on välttämätöntä. Tällöin evästeen käyttäminen mahdollistaa juuri sellaisen palvelun tarjoamisen, kuin mitä käyttäjä on nimenomaisesti pyytänyt. Sähköisen viestinnän palveluista annetun lain 205.3 §:n mukaan evästeiden tallentaminen ja käyttö on siis sallittua ainoastaan palvelun vaatimassa laajuudessa. Sillä ei

myöskään saa rajoittaa yksityisyyden suojaa enempää kuin on välttämätöntä (Voutilainen 2022; Finlex, 2014).

Evästeiden käyttämistä ja tallentamista käyttäjän päätelaitteelle on mahdollista hallinnoida ja rajoittaa selainohjelmiston asetuksien kautta. Kun käyttäjä on asettanut selaimelleen asetukset, niiden käyttäminen tai käyttämättä jättäminen ei tarkoita suostumusta evästeiden tallentamista varten käyttäjän päätelaitteelle. Näiden asetusten käyttäminen ei ole suostumus evästeiden tallentamiselle, vaan erillinen suostumus on silti saatava (Voutilainen, 2020).

4.3 Sähköisen viestinnän luottamuksellisuuden valvonta

Suomessa sähköisen viestinnän luottamuksellisuutta valvoo Liikenne- ja viestintävirasto Traficom. Se opastaa luottamuksellisuuden toteutumisessa ja evästeiden hyvissä käytännöissä sekä palvelun käyttöä kuvaavien tietojen tallentamisessa ja käytössä. Tämä valvonta kattaa myös evästeiden sekä muiden palvelun käyttöä kuvaavien tietojen tallennuksen käyttäjän päätelaitteelle ja päätelaitteella olevien tietojen käytön. Traficomin opastus sisältää valvovan viranomaisen näkemyksen lainmukaisista ja hyväksyttävistä evästekäytännöistä ja opastus on laadittu yhteistyössä toimivaltaisen tietosuojavaltuutetun viranomaisen kanssa (Traficom, 2021).

Traficom opastaa palveluntarjoajia, jotka käyttävät verkkosivuillaan ja sähköisen viestinnän palveluissaan evästeitä tai niiden kaltaisia tekniikoita. Traficom (2021) antaa ohjeistuksen, joita palveluntarjoajan pitäisi evästeiden kannalta huomioida:

- Mitä evästeitä sivustolla tai palvelussa käytetään
- Evästeiden luokittelu kyseisen palvelun näkökulmasta välttämättömiin ja ei-välttämättömiin
- Käyttäjille selkeän ja ymmärrettävän tiedon tarjoaminen palvelun evästeistä ja niiden käyttötarkoituksesta
- Suostumuksen oikeanlaiseen ei-välttämättömien evästeiden käyttöön

4.4 Yleinen tietosuoja-asetus (GDPR)

Tietosuoja sai näkyvyyttä ja tietoisuutta yhteiskunnassa muutamien lähivuosien tapahtumien johdosta. Viime vuosina suurta julkisuutta henkilötietojen käsittelyyn liittyvät tapaukset, kuten Cambridge Analytican ja Facebookin skandaali sekä AccuWeatherin iOs-sovelluksen tietojen välitys, ovat herättäneet kansalaisten huomion ja keskustelua liittyen yksityisyyteen internetissä. Nämä tapaukset osoittavat monimutkaisten palveluekosysteemien laajuuden sekä lukuisten

toimijoiden osallistumisen tietojen yksityisyyteen vaikuttaviin toimiin (Kretschmer ym., 2021).

Tällaisia ekosysteemejä on nykyään kaikkialla ja teknologinen kehitys on muuttanut niitä jatkuvasti monimutkaisemmiksi. Palveluekosysteemi määritellään suhteellisen itsenäiseksi, itsesäätyväksi resursseja integroivien toimijoiden järjestelmäksi, joita yhdistävät yhteiset institutionaaliset järjestelyt ja keskinäinen arvon luominen palveluiden vaihdon kautta. Siinä siis yhdistyvät useiden palveluntarjoajien palvelut ja taustapalveluita käytetään eri tarkoituksiin, kuten mainostamiseen, taustapalveluihin, verkostojen integrointiin ja niin edelleen. Kun käyttäjä tekee päätöksen käyttää palvelua, se voi johtaa siihen, että useat osapuolet voivat käsitellä hänen tietojaan. Tämä on käyttäjälle monimutkaista ja nämä voivat johtaa käyttäjän yksityisyyden kannalta ongelmallisiin tilanteisiin (Kurtz, Semmann & Schulz, 2018).

Cambridge Analytican Facebook-käyttäjätietojen väärinkäyttö on vain yksi näkyvä tapaus. Tässä tapauksessa 87 miljoonan Facebookin käyttäjään vaikutti Facebookissa julkaistun sovelluksen yksityisyyttä loukkaava pääsy käyttäjätietoihin. Sovellus pystyi hyödyntämään monenlaisia tietoja itse käyttäjältä ja tämän ystäviltä ja toimitti tiedot kolmannelle osapuolelle Cambridge Analyticalle. AccuWeatherin tapauksessa sen iOs-sovellus välitti käyttäjän laitetiedot ulkopuoliseen taustapalveluun, joka sai tietää käyttäjän sijaintitiedot, vaikka käyttäjä olisi kieltänyt sovellusta käyttämästä sijaintipalveluita. Kolmas osapuoli käytti sijaintitietoja hyväkseen kohdistaakseen markkinointia (Kurtz ym., 2018).

Näiden isojen tapausten seurauksena ihmisten luottamus verkkopalveluihin, erityisesti sosiaalisiin verkostoihin, jotka keräävät suoraan henkilöön liittyviä tietoja, on horjunut. EU:n laajuinen tietosuojadirektiivi, jonka tarkoituksen oli suojella yksilön yksityisyyttä, on ollut voimassa jo vuodesta 1995. Tämä ei kuitenkaan sovellu nykypäivän verkkoekosyystemeihin, sillä tietojen keräys, tallennus ja niiden käyttö on lisääntynyt jyrkästi. Tietosuojadirektiiviä on myös noudatettu heikosti sen noudattamatta jättämisen vähäisistä sanktioista johtuen. Tämän johdosta syntyi GDPR eli yleinen tietosuoja-asetus, joka otti käyttöön sitovat yksityisyyttä koskevat säännöt kaikissa EU-maissa vuodesta 2018. Sen täytäntöönpano pyrkii vahvistamaan vastuuta tietojen käsittelijöiden toimiin liittyen.

Suomessa GDPR:n soveltaminen alkoi toukokuussa 2018. On osoitettu, että jopa 70 % maailman miljoonasta suosituimmasta verkkosivuostosta käyttää jonkinlaista seurantaa, johon GDPR vaikuttaa. Lain voimaantulolta on odotettu paljon, jotta näitä yksityisyyden kannalta ongelmallisia tilanteita voitaisiin paremmin ratkaista. GDPR pyrkii takaamaan henkilöiden hallinnan omien tietojensa käsittelyssä. Lisäksi se sisältää systeemisen tietosuojan elementtejä. Lain tarkoituksen on suojella yksityisyyttä digitaalisessa maailmassa ja siten palveluekosysteemeihin liittyen tietosuojan muodossa (Kretschmer ym., 2021).

Kansalaisten henkilötietojen suoja on perusoikeus, joka on kirjattu yleismaailmalliseen ihmisoikeusjulistukseen. Henkilötietojen suojaa ei pidetty välttämättömänä ennen yleistä tietosuoja-asetusta (GDPR). Sen tarkoituksena on yksityisten henkilöiden parempi henkilötietojensa hallitseminen sekä yritysten tasapuoliset toimintaedellytykset. GDPR hyväksyttiin Euroopan parlamentin

toimesta vuonna 2016 ja sitä alettiin soveltamaan kahden vuoden siirtymäajan jälkeen 25.5.2018. Lain tarkoituksena on säännellä henkilötietojen keräämis-, käsittely- ja hallintaprosessia ja se koskee kaikkia Euroopan Unionin (EU) yrityksiä ja organisaatioita, jotka pitävät hallussaan tai käsittelevät henkilötietoja toiminnassaan. Laki ulottuu myös kolmansien maiden yrityksiin, jotka tarjoavat tavaroita tai palveluita EU:n kansalaisille. EU:n jäsenvaltiot saavat vapaasti soveltaa GDPR:ää tiukemmin, jos he niin haluavat. Se määrittelee tietosuojan ja yksityisyyden vähimmäistason EU:ssa. (Poritskiy ym., 2019; Kretschmer ym., 2021; Leite ym., 2021).

> ”GDPR kattaa laajan alueen näkökohtia, jotka liittyvät tietojen käsittelyyn ja yksityisyyteen. Se tarjoaa erityisesti laillisen kehyksen, jossa määritellään seu raamukset rikkomistapauksissa, ja se kattaa kaikki vaiheet, jotka liittyvät henkilö tietojen keräämiseen, käyttöön, suojaamiseen ja vuorovaikutukseen EU:ssa.” (Kretschmer ym., 2021).

GDPR toi mukanaan kaikkiin EU-maihin merkittäviä muutoksia kansalaisten suojeluun henkilötietojen käsittelyssä, asettamalla uusia velvoitteita kansalaisille, yrityksille ja muille julkisille organisaatioille. GDPR vaikuttaa myös EU:n ulkopuolelle sijoittuneeseen yritykseen, joka tarjoaa tavaroita tai palveluita yksityishenkilöille EU:ssa, valvoen heidän toimintaansa EU:ssa. GDPR:n toteuttaminen on haaste yrityksille, aiheuttaen yrityksille oikeudellisia, teknisiä ja organisatorisia muutoksia. Kaikkien toimialojen on tunnettava GDPR ja sovellettava sitä toiminnassaan (Poritskiy ym., 2019).

GDPR:n avulla pyrittiin korjaamaan Euroopassa olevia tietosuojastandardeja tuoden merkittäviä muutoksia EU:n tietosuojalainsäädäntöön. Sen avulla otettiin käyttöön korkealaatuiset tietosuojastandardit koko EU:ssa. GDPR:n osana on sisällytetty vaatimukset käyttäjän suostumuksesta ennen tämän henkilötietojen käsittelyä, oikeus tulla unohdetuksi ja oikeus vastustaa häntä koskevien tietojen käsittelyä. Se myös vahvistaa kansallisten lakien sisällä olevia oikeuksia, kuten tiedonsaanti-, oikaisu- ja poistamisoikeutta sekä avoimuutta (Kretschmer ym., 2021).

Poiketen kaikista muista aikaisemmista direktiiveistä GDPR sisältää sitovia seuraamuksia kuten sakkoja, mikäli sen sääntöjä rikotaan tai jätetään noudattamatta. Sakkojen suuruus on enintään 4 % vuotuisista tuloista tai 20 miljoonaa euroa. EU:n jäsenvaltiot saavat vapaasti määrittää lisäsakkoja rikkomuksista niin halutessaan. Rikkomuksista ja noudattamattomuuksista seuraava sakkokäytäntö on omiaan pitämään huolen siitä, että GDPR:ää noudatetaan. Sen noudattamatta jättämisestä saattaa seurata suurta taloudellista menetystä (Kretschmer ym., 2021).

4.4.1 Henkilötietojen käsittely

Oikeus henkilötietojen suojaan perustuu ihmisoikeuksien yleismaailmalliseen julistukseen ja siihen kirjattuihin perusihmisoikeuksiin. Henkilötietojamme tulee suojata, sillä ne ovat tietoja yksityiselämästämme (Leite ym., 2021).

GDPR:n mukaan henkilötiedot kattavat kaikki tiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön. Tällainen henkilö voidaan tunnistaa joko suoraan tai välillisesti, viittaamalla johonkin tunnistetietoon, joita ovat ainakin:

- Nimi
- Tunnistenumero
- Verovelvollisen numero
- Sijaintitieto
- Verkkotunniste
- Yksi tai useampi tekijä, jotka ovat ominaisia fyysiselle, fysiologiselle, geneettiselle, henkiselle, taloudelliselle, kulttuurilliselle tai sosiaaliselle identiteetille.

(Poritskiy ym., 2019; Leite ym., 2021).

GDPR:n mukaan henkilötietoja on käsiteltävä läpinäkyvästi yksityisyyttä, perusoikeuksia, -vapauksia ja -takuita kunnioittaen. Se on muuttanut merkittävästi tapaa, jolla henkilötietoja säilytetään. Useat kansalliset organisaatiot ja konsulttiyritykset ovat määrittäneet joukon käytäntöjä, jotka käyttöönottamalla organisaatiot tulevat noudattaneeksi GDPR:ää (Poritskiy ym., 2019).

Henkilötietojen käsittelyyn liittyy GDPR:n mukaan muutamia perusperiaatteita. Ensinnäkin henkilötietojen käsittelyn tarkoitusten on oltava yksiselitteisiä ja laillisia. Tarkoitukset on myös määriteltävä sen yhteydessä, kun henkilötietoja kerätään. Käsittelyn tarkoituksen tulee olla tietojen omistajan tiedossa ennen kuin niiden käsitteleminen aloitetaan. Toiseksi GDPR määrittelee perusperiaatteen tietojen minimoinnista. Tietojen minimointi tarkoittaa sitä, että henkilötietojen on oltava riittäviä, olennaisia ja rajoitettu vain siihen, mikä on tarpeen ennalta määrättyjä tarkoituksia varten. Tämän vuoksi henkilötietoja on kerättävä mahdollisimman vähän eikä tarpeetonta tai ylimääräistä tietoa tule kerätä. Tiedot tulisi myös salata ja anonymisoida siten, että ne takaavat tietosuojan toteutumisen.

GDPR määrittelee myös tarkkuusperiaatteen, eli kerättyjen tietojen on oltava yhteisiä ja ajantasaisia. Mikäli tiedot ovat virheellisiä tai vanhentuneita, tietojen oikaisu on suoritettava ilman viivyttelyä. Lisäksi tietoja tulee säilyttää vain sen ajan, joka on tarpeen niiden tarkoitusten kannalta ja jota varten niitä käsitellään. Rekisterinpitäjän on suunniteltava ja pystyttävä perustelemaan tietojen säilytysajat ja ne on myös dokumentoitava. Tarkkoja säilytysaikoja ei ole määritelty, vaan rekisterinpitäjän vastuulla on arvioida tietojen säilytysaika ja tarpeellisuus kysymyksessä olevaa käyttötarkoitusta varten. Henkilötietojen omistajalla on oikeus pyytää henkilötietojensa poistamista ja ne on poistettava tämän pyynnön myötä ilman aiheetonta viivytystä. Tiedot tulee myös hävittää, kun niiden käsittelylle ei ole enää perusteita (Leite ym., 2021; Traficom, 2021).

4.4.2 Arkaluontoiset tiedot

Poritskiy, Oliveira & Almeida (2019) tutkimuksen mukaan GDPR:n 9. artiklassa on määritelty ja lueteltu tiedot, jotka ovat arkaluontoisia. Niitä kutsutaan erityisiksi tietoluokiksi ja niitä koskevat erityiset käsittelyehdot. Arkaluontoisten tietojen käsittely voi aiheuttaa merkittäviä riskejä henkilön perusoikeuksille ja -vapauksille. Tämän johdosta arkaluontoisten tietojen käsittely on kiellettyä muutoin kuin tietojen haltijan antaessa nimenomaisesti suostumuksensa käsittelyyn tai jos se on välttämätöntä merkittävän yleisen edun kannalta. Arkaluontoisia tietoja GDPR:n mukaan ovat:

- Henkilötiedot, jotka paljastavat rodun, etnisen alkuperän, poliittiset mielipiteet ja uskonnolliset tai filosofiset vakaumukset
- Jäsenyys ammattiliitossa
- Geneettiset ja biometriset tiedot
- Terveyteen liittyvät tiedot ja
- Henkilön seksuaalista elämää tai suuntautumista koskevat tiedot

(Leite ym., 2021; Poritskiy ym., 2019).

4.4.3 Vaikutusarviointi yksilön oikeuksiin ja vapauksiin

GDPR sisältää myös säännön, jonka tavoitteena on arvioida vaikutuksia yksilöiden oikeuksiin ja vapauksiin tietyn tietojenkäsittelyn toimesta. Sen avulla voidaan välttää vakavat haitat jo ennen kuin tietojenkäsittelyprosessi aloitetaan. Käyttäjälle on GDPR:n myötä syntynyt uusia oikeuksia. Näitä ovat:

- Tietojen siirrettävyys toiseen organisaatioon
- Oikeus unohtaa tai poistaa tiedot ja
- Oikeus vastustaa (esim. tietojen profilointia)

Näiden lisäksi GDPR vahvistaa oikeuksia, jotka on kirjoitettu maiden kansallisiin lakeihin. Näitä oikeuksia ovat:

- *Tiedonsaantioikeus (GDPR kohdat 13 ja 14)*. Näissä kohdissa määritellään oikeudet tiedonsaantiin ja pääsyoikeus tietoihin. Tärkeää on, että tietojen haltijaa ei saa estää pääsemästä tietoihinsa käsiksi. Lisäksi pääsyn tulee olla maksutonta sekä helppoa. Jos tietojen haltijan tietoja siirretään kolmanteen maahan tai kansanväliseen organisaatioon, tietojen haltijan on saatava tietoonsa hänen tietojensa asianmukaiset suojaustoimenpiteet.

- *Oikaisuoikeus (GDPR kohta 16)*. Tietojen haltijalla on oikeus ilman aiheetonta viivytystä saada pääsy tietoihinsa ja oikaista häntä itseään koskevia virheellisiä tietoja.

- *Poistamisoikeus (GDPR kohta 17).* Tietojen haltijalla on oikeus peruuttaa suostumuksensa ja vastustaa häntä koskevien tietojen käsittelyä ilman erityistä syytä tai jos käsittely ei ole GDPR:n mukaista.

- *Avoimuus*. Läpinäkyvät, ymmärrettävät ja kattavat tiedot siitä, miten tietojen haltijan tietoja tullaan käsittelemään.

(Poritskiy ym., 2019).

4.4.4 Tietosuojan toteuttaminen

Leite ym. (2021) mukaan GDPR määrittelee myös tietosuojavastaavan roolin. Tietosuojavastaavan nimityksen on perustuttava siihen, että kyseisellä henkilöllä on rooliin tarvittavia ammatillisia ominaisuuksia tai tietosuojalainsäädännön ja -käytännön asiantuntemusta. Tietosuojavastaavan rooli keskittyy viiteen olennaiseen tehtävään, joita ovat:

1. Tiedotus ja neuvonta tietosuojavastaavan velvollisuuksista
2. Organisaation tietojenkäsittelyn valvonta
3. Tietosuojavaikutusten arvioinnin toteuttamisen valvonta
4. Henkilötietojen käsittelyä koskevien pyyntöjen yhteyshenkilönä toimiminen
5. Yhteistyön toteuttaminen tietosuojaviranomaisten kanssa

Kaksi tärkeää termiä on noussut esiin liittyen tietosuojaan ja yksityisyyteen internetissä GDPR:ää toimeenpannessa. Käyttäjien henkilötietojen yksityisyyden suojaamisen varmistamiseksi on otettava käyttöön turvatoimenpiteitä ja organisatorisia tekniikoita, jonka avulla henkilötietoja koskevan prosessin alkuvaiheilla pystytään saamaan kontrolli siitä, että varmistetaan henkilötietojen suoja ja että tarvittavat toimenpiteet on tehty.

Tietosuojan tulisi olla sisäänrakennettua, jolloin yksityisyyden tulee olla hallinnassa projektin, tuotteen tai palvelun kehittämisessä jo ohjelmistoa suunnitellessa, kehittäessä ja sitä luodessa. Sisäänrakennettu tietosuoja ei koske vain ohjelmiston suunnitteluvaihetta, vaan se on sisällytettävä koko kehitys-, testaus- ja toteutusprosessiin. Yritysten tulisi sisällyttää yksityisyys perusarvoihinsa vahvistaen sitoutumistaan etikkaan ja avoimuuteen. Hyvällä tietosuojalla on seitsemän periaatetta, joiden toteutumiseen liittyy myös käyttäjän antaman suostumus henkilötietojen käsittelyyn oikeilla ja ajantasaisilla tiedoilla ja varmistetaan käyttäjän oma pääsy ja hallinta tietoihinsa (Leite ym., 2021):

1. Ennakointi ja ennaltaehkäisy
2. Oletuksena yksityisyys
3. Yksityisyys on sisällytetty jo suunnitteluun

4. Täysi toiminnallisuus
5. Alusta loppuun turvallisuus
6. Läpinäkyvyys ja avoimuus
7. Kunnioitetaan käyttäjien yksityisyyttä

4.4.5 GDPR ja evästeet

GDPR:ssä on määritelty myös evästeiden toimintaa, sillä ne liittyvät olennaisesti tietosuojaan ja henkilötietojen käsittelyyn. Palvelun käyttäjälle on kerrottava selkeästi ja ymmärrettävästi, mitä tietoja hänestä kerätään ja mihin tietoja käytetään. Palvelun tarjoaja saa kerätä vain välttämättömiä tietoja palvelun tarjoamisen kannalta. GDPR edellyttää, että kaikki evästeitä käyttävät yritykset jättäisivät evästeiden asettamisen automaattisesti pois päältä ja ne aktivoituvat vasta sitten, kun käyttäjä päättää, mitä tietoja hän haluaa jakaa antaen vapaaehtoisen suostumuksen (Leite ym., 2021).

4.4.6 Vaikutukset teknologiaan

Toukokuussa 2018 GDPR:n käyttöönoton myötä yritykset ovat ottaneet käyttöön uusia menettelytapoja yksityisten henkilöiden tietojen keräämiseksi, tallentamiseksi ja suojaamiseksi. Tämä muutos vaikutti erityisesti ohjelmistosuunnitteluyrityksiin. GDPR:n soveltamisella onkin ollut perustavanlaatuisia vaikutuksia ohjelmistosuunnitteluyritysten sisäisiin prosesseihin ja ohjelmistokehitysmallien eri vaiheisiin. Jo projektin suunnittelun alkuvaiheessa on tehtävä päätöksiä sovellusten pyytämien ja tallentamien henkilötietojen määrästä ja tyypistä sekä suunniteltava suojausmekanismit näiden tietojen suojaamiseksi, jolloin noudatetaan sisäänrakennettua tietosuojaa. Tietosuojavastaavan on tärkeää osallistua projekteihin heti alusta pitäen, jotta voidaan tunnistaa ja minimoida projektiin liittyvät turvallisuus- ja tietosuojariskit. Heti alkuvaiheessa on myös luotava suunnitelma tietojen haltijoiden suostumuksen saamiseksi ja dokumentoitava kaikki tarkasti. Lopuksi on panostettava testaamiseen henkilötietojen käsittelyn näkökulmasta (Leite ym., 2021).

Teknisestä näkökulmasta haasteena on käyttäjäystävällisyys tämän henkilötietojen hallinnassa. Käyttäjälle pitäisi luoda miellyttävä käyttökokemus ja samalla sisällyttää palveluun kaikki GDPR:n asettamat velvoitteet. Ohjelmiston käyttöönotto- ja toimitusvaiheessa haasteita liittyy tietojen poisto-, auditointi- ja tietomurtoilmoitusmekanismeihin (Leite ym., 2021).

GDPR vaikuttaa tekoälyn, pilvilaskennan ja lohkoketjun kehitykseen, sillä näitä prosesseja tukevat algoritmit vaativat korkean prosenttiosuuden tehokkuudesta ja tarkkuudesta, jotka saadaan henkilötietojen analysoinnista. On siis ennustettu, että uusien teknologioiden kehittämien ja soveltaminen EU:ssa hidastuu merkittävästi tulevina vuosina. Pienillä start-up yrityksillä on haasteena GDPR:n vaatiman minimitason toteuttaminen, siinä isoille yrityksille keskeisempi ongelma on tietojen poistaminen. GDPR tuo mukanaan myös etuja, sillä

hyvin toteutettuna se on omiaan lisäämään kuluttajien luottamusta ja sitä kautta edistää myynnin kasvua ja tuottaa kilpailuetua (Poritskiy ym., 2019).

4.5 Tietosuojalaki

Yleistä tietosuoja-asetusta täydentää Suomessa tietosuojalaki. Sen tarkoituksena on täsmentää ja täydentää yleistää tietosuoja-asetusta ja sen kansallista soveltamista luonnollisten henkilöiden henkilötietojen käsittelyn näkökulmasta. Laki on tullut voimaan 1.1.2019, jolloin se kumosi vanhan henkilötietolain. Tietosuojalainsäädännön valvontaviranomainen Suomessa on tietosuojavaltuutettu ja hänen toimivaltansa, tehtävänsä ja valtuutensa säädellään tässä laissa. Laki turvaa oikeuden jokaiselle saattaa asia tietosuojavaltuutetun käsiteltäväksi, jos henkilötietojen käsittelyä koskevaa lainsäädäntöä on rikottu. Tietosuojavaltuutettu voi myös lähteä omatoimisesti tutkimaan henkilötietojen käsittelyn lainmukaisuutta laajoine tiedonsaantioikeuksineen. Laki säätelee myös sen noudattamattomuudesta seuraavien uhkasakkojen määräytymistä, siinä missä muut asiaan liittyvät rikolliset toimet rangaistaan rikoslain mukaan (Finlex, 2018; Lexia, 2018).

Tietosuojalaki sääntelee tiettyjä henkilötietojen käsittelyyn liittyviä erityistilanteita ja seuraamusmaksuja. Tietosuojalain keskeiset henkilötietojen käsittelyä koskevat velvoitteet tulevat sellaisenaan tietosuoja-asetuksesta. Jäsenvaltioilla on oikeus antaa täydentävää tietosuojalainsäädäntöä siltä osin kuin tietosuoja-asetus antaa siihen liikkumavaraa. Tietosuojalaki täsmentää ja täydentää tietosuoja-asetusta, eikä se muodosta itsenäistä lakia vaan sitä sovelletaan rinnakkain tietosuoja-asetuksen kanssa. Se täydentää myös muuta henkilötietojen käsittelyyn liittyvää lainsäädäntöä, esimerkiksi työntekijöiden tietojen käsittelyä koskevaa työelämän tietosuojalakia ja julkisuus- ja luottotietolakia (Lexia, 2018).

Tietosuojalaki sääntelee myös lapsille tarjottavien tietoyhteiskunnan palveluiden ikärajaa. Jos lapsi on alle 13-vuotias, hänellä täytyy olla vanhempien suostumus henkilötietojen antamista edellyttävien palveluiden käyttämistä varten ja palvelun tarjoajan eli rekisterinpitäjän velvollisuus on tarkistaa, että vanhempien suostumus on olemassa ja voimassa. Ikäraja on linjassa muiden pohjoismaiden kanssa (Lexia, 2018).

Suomessa on runsaasti erityislainsäädäntöä ja säädöksiä, jotka koskevat henkilötietojen käsittelyä. GDPR:n johdosta myös Suomen lainsäädäntöön tehtiin isoja muutoksia, jotta omat lakimme olisivat yhdenmukaisia EU-sääntelyn kanssa. Henkilötunnuksen käsittely on sallittua vain rekisteröidyn suostumuksella, mistä laissa on annettu yksityiskohtainen selvitys, tai jos henkilötiedon käsittelystä säädetään lailla. Lisäksi henkilötunnusta saa käsitellä tietyissä laeissa mainituissa erityistilanteissa, kuten silloin kun henkilön yksiselitteinen yksilöiminen on tärkeää jonkun laissa suoritettavan tehtävän suorittamista, henkilön oikeuksien ja velvollisuuksien toteuttamista tai historiallista tai tieteellistä tutkimusta varten. Henkilötunnusta saa käsitellä luottoa hakiessa, perinnässä, vakuutus-, luottolaitos-, maksupalvelu-, vuokraus- ja lainaustoiminnassa, luottotietotoiminnassa, terveydenhuollossa, sosiaalihuollossa ja muun sosiaaliturvan

toteuttamisessa tai virka-, työ- ja muita palvelussuhteita ja niihin liittyviä etuja koskevissa asioissa. Henkitunnusta on oikeus käsitellä myös osoitetietojen päivitystä ja työsuhdetta koskevissa asioissa. Kaikkia henkilötietojen käsittelyyn osallistuvia henkilöitä sitoo lain nojalla vaitiolovelvollisuus niiden käsittelyyn liittyvistä asioista, eikä tietoja saa käyttää omaksi tai toisen hyödyksi tai vahingoksi. Henkilötietoja ei myöskään saa tarpeettomasti merkitä henkilörekisterin perusteella tulostettuihin tai laadittuihin asiakirjoihin (Finlex, 2018; Lexia, 2018).

Tietosuojalainsäädäntö siis lähinnä täsmentää tietosuoja-asetusta. Uuden tietosuojalain myötä viranomaisen toimivaltaa tietosuoja-asetuksen valvonnassa on saatettu ajan tasalle ja Suomen näkökulmasta lainsäädäntö haluttiin päivittää GDPR:n voimaantulon vuoksi ja että lakimme olisivat yhtenäisiä EU:n sääntelyn ja lakien kanssa.

4.6 Sähköisen viestinnän tietosuojadirektiivi

EU:n tietosuojadirektiivi antaa edelleen tietosuojalainsäädännön kannalta tärkeitä perusmääritelmiä. Näitä ovat Kretschmerin ym. (2021) mukaan:

- Henkilötiedoiksi määritellään kaikki tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyvät tiedot
- Henkilötietoja koskeva osapuoli on rekisteröity
- Henkilötietoja käsittelevä osapuoli on rekisterinpitäjä

Vuonna 2002 hyväksyttiin tietosuoja- ja sähköisen viestinnän direktiivi, joka tunnetaan myös nimellä sähköisen viestinnän tietosuojadirektiivi. Tämä direktiivi perustuu tietosuojadirektiiviin ja jalostaa sitä verkon tietoliikenteeseen, tietoisen suostumuksen käsitteen ollessa olennainen osa sitä. Tietoinen suostumus velvoittaa palvelujen ilmoittamaan loppukäyttäjälle, millaisia tietoja käyttäjien laitteelle tallennetaan, kun palvelua käytetään. Erityisesti se velvoittaa antamaan tietoja evästeistä: millaisia tietoja käyttäjien laitteille tallennetaan ja mihin tarkoitukseen tietoja käytetään. Direktiiviin tuli muutos vuonna 2009. Tämä velvoittaa, että loppukäyttäjän on nimenomaisesti suostuttava, ennen kuin tietoja voidaan tallentaa heidän laitteilleen. Tämä muutos on antanut kuluttajille mahdollisuuden peruuttaa henkilötietojensa säilyttämiseen ja käsittelyyn liittyvän suostumuksen milloin tahansa. (Kretschmer ym., 2021).

4.7 Sähköisen viestinnän tietosuoja-asetus

Vuodesta 2017 alkaen sähköisen viestinnän tietosuoja-asetuksesta on ollut olemassa lakiesitys, joka ei ole tullut toistaiseksi voimaan tätä pro-gradutyötä tehtäessä. Sen tarkoituksena on päivittää sähköisen viestinnän tietosuojadirektiiviä, täydentäen GDPR:ää. Se sisältää tarkempia säädöksiä erityisistä palveluista ja

käyttäjän seurantateknologioista, sillä GDPR:ää ei ole suunniteltu kattamaan sähköistä viestintää. Lakiesityksen oli tarkoitus tulla voimaan GDPR:n rinnalla, mutta esitys on edelleen työn alla. Tällä hetkellä asetuksen asiat on määritelty löyhästi tietosuojadirektiivissä. Lakiesityksen käsittelyn viivästymisen syynä on EU:n jäsenvaltioiden erimielisyydet asetukseen liittyen (Kretschmer ym., 2021).

5 TUTKIMUS

Tässä luvussa on esitelty tämän pro-gradutyön tutkimus kokonaisuudessaan. Aluksi kerrotaan tutkimuksen ja pro-gradutyön tarkoituksesta, aikaisemmista aihetta koskevista tutkimuksista, tutkimusprosessista ja tutkimusideasta, tutkimusmenetelmästä ja aineistosta sekä aineistonkeruusta ja -rajauksesta. Luvussa tarkastellaan myös sitä, miten laadullisen tutkimuksen aineisto on analysoitu, mikä sen tarkoitus on ja miten aineistoa on lähestytty ja ryhdytty analysoimaan tulosten aikaansaamiseksi. Tavoitteena on, että työn lukija pystyy seuraamaan analyysin etenemistä läpinäkyvästi ja pääsemään syvemmälle siihen.

5.1 Tarkoitus, idea ja rajaus

Tutkimuksen tarkoituksena on edistää tietämystä ja ymmärrystä tietyllä alalla ja johtaa uuden tiedon luomiseen. Tämän työn tarkoituksena on tuoda informaatioteknologian alalle uutta tietoa tietosuojaselosteiden sisältämästä tiedosta koskien HTTP-evästeitä ja niiden tuomia uhkia. Työn teoriaosuus käsittelee tutkimukseen liittyviä aiheita perusteellisesti varmistaen sen, että tutkimuksen lähtökohdat on ymmärretty ja että tutkija on ajan tasalla aiheeseen liittyvästä tiedosta. Teoriaosuuden tarkoitus on antaa tutkimuksen analyysille näkökulmia, herätellä lisäpohdintaa aiheesta ja auttaa tulosten tulkinnassa. Teoria on toiminut tässä työssä ikään kuin suunnannäyttäjänä, selkeyttäen työn tekijälle sen, kuinka laaja kirjo eri aiheita sivuaa pääaihetta eli tietosuojaselosteen evästeosuutta. Teoriaosuutta varten on aiheesta ja sen läheltä tutkittu kirjallisuutta, verkkosivustoja, tieteellisiä artikkeleita ja aiemmin tehtyjä tutkimuksia. Tutkimuksen tekemisessä on noudatettu moraalisia ja eettisiä periaatteita, jotta tutkimus on rehellinen ja tutkijan oma tekemä ja jotta lähteisiin on viitattu oikein.

Tutkimusidea on saanut lähtönsä tämän pro-gradutyön tekijän todellisesta pohdinnasta ja huolenaiheesta sekä kiinnostuksen kohteesta. Tutkimuksen aihe on relevantti ja uskon, että moni jakaa tällä hetkellä huolenaiheen yksityisyytensä vaarantamisesta verkkopalveluita käyttäessään ja tulokset ovat siten

yleisemminkin kiinnostavia.

Tutkimus on rajattu siten, että vastaus tutkimuskysymykseen on mahdollista löytää tutkimukseen valitusta aineistosta valitun tutkimusmenetelmän avulla tutkijan työlle asettaman tutkimusaikataulun sisällä ilman, että aineistossa syntyy liikaa toistoa. Esimerkiksi isojen yhtiöiden tietosuojaselosteet ovat osin samoja toisen ison yhtiön kanssa, kuten esimerkiksi YouTube on osa Googlea. Tutkimusongelma on haluttu pitää yksiselitteisenä ja selkeänä sisältäen vain yhden kysymyksen (Günther & Hasanen, 2022).

5.2 Aiemmat tutkimukset aiheesta

Työn teoriaosuutta kirjoittaessa ja aihetta tutkiessa kävi ilmi, että aihetta on tutkittu aikaisemmin monesta eri näkökulmasta. Tuoreimpia tutkimuksia aiheesta tai sen läheltä ovat tutkimukset liittyen yleiseen tietosuoja-asetukseen eli GDPR:ään ja sen tuomiin muutoksiin digitaalisessa maailmassa. Evästeitä on tutkittu monipuolisesti vuosien varrella, mutta teknologia, tieto ja lait koskien evästeitä ovat muuttuneet viime vuosina paljon, joten tässä työssä pyrittiin tutkimaan tuoretta aineistoa aiheesta ja hyödyntäen vanhemmista töistä vain muuttumatonta perusteoriaosuutta. Vanhempia töitä käytettiin myös hyödyksi muutosten aikajanan näkemyksen luomiseksi. Evästeitä on tutkittu aiemmin uhkien näkökulmasta, mikä on jo hyvin lähelle tätä tutkimusta, mutta niistä puuttui kuitenkin näkökulma, joka yhdistäisi mukaan myös käyttäjän ymmärryksen ja tietosuojaselosteen. Yksityisyydestä ja yksityisyyden suojasta on tehty useita tutkimuksia eri näkökulmista ja tässä työssä keskityttiin tutkimaan sitä digitaalisen maailman ja evästeiden näkökulmasta.

Tietosuojaselosteet sen sijaan ovat verrattaen uusi asia, sillä yleisen tietosuoja-asetuksen eli GDPR:n voimaantulo vuonna 2018 sai valtavan sysäyksen niiden käyttämiselle. GDPR ei suoraan velvoita tietosuojaselosteen laatimista. Jos verkkosivusto kerää tai käsittelee henkilötietoja, tällöin kirjallinen kuvaus henkilötietojen käsittelystä tulee laatia ja sen tulee olla esillä verkkosivuston käyttäjälle. Tätä selostetta kutsutaan tietosuojaselosteeksi. Tietosuojaselosteesta löytyi jonkin verran tutkimuksia, joissa kaikissa oli hyvin samankaltainen sanoma kuluttajien käyttäytymisestä niiden suhteen. Osa tutkimuksista oli hyvin teknisiä, sillä oli kehitetty myös ohjelmistoja käsittelemään tietosuojaselosteen tekstiä. Tietosuojaselosteista puuttui selvästi suora näkökulma suhteessa evästeisiin ja niiden asetuksiin verkkosivustoilla, mihin keskityn tässä työssä. Uskon, että tämä tutkimus kokonaisuudessaan luo uutta tietoa ja mahdollisesti myös uusia näkökulmia ja ideoita uusille tutkimuksille ja jatkokehityksen kohteille.

5.3 Tutkimusprosessi ja tutkimusidea

Tässä tutkimuksessa on edetty tieteellisen tutkimuksen prosessissa asteittain

edeten tutkimusideasta tutkimusaiheen perehtymiseen, tutkimussuunnitelman tekemiseen, aineiston keräämiseen ja analysointiin sekä tutkimuksen raportoimiseen. Prosessin eri vaiheet ovat olleet vuorovaikutuksessa keskenään, jolloin edeltävä vaihe on vaikuttanut seuraaviin ja prosessin edetessä on välillä palattu taaksepäin muuttamaan työn rajausta. Tutkimuskysymys on pidetty mielessä koko tutkimuksen tekemisen ajan ja sen sanamuotoa on aineiston keruuvaiheessa hieman muunnettu vastaamaan paremmin tutkimuksen ydintä. Tämän tutkimuksen tekstin on tarkoitus olla läpinäkyvä ja ymmärrettävässä muodossa. Tutkimuksessa pyritään kulkemaan punaista lankaa pitkin, vetäen aihe lopuksi tiiviisti yhteen. Kuljettu reitti pyritään perustelemaan selkeästi, jotta tutkimuksesta saa oikean ja luotettavan näkemyksen aiheeseen (Günther & Hasanen, 2022).

5.4 Tutkimusmenetelmä ja aineisto

Tutkimus toteutettiin laadullisena tutkimuksena. Tutkimusmenetelmä valikoitui siksi, että tutkimusaihetta haluttiin tutkia syvällisesti ja aihe on melko uusi, joten samanlaista tutkimusta ei ollut tehty aikaisemmin. Työssä haluttiin myös ymmärtää aiheen inhimillistä näkökulmaa, jolloin laadullinen tutkimusmenetelmä oli oikea valinta (Myers, 2019).

Laadullinen tutkimus koostuu monenlaisista lähestymistavoista ja tutkimusperinteistä, joilla on erilaisia oletuksia sekä todellisuuden luonteesta että siitä, minkälaisin keinoin sitä on hyvä analysoida. Laadullisessa tutkimuksessa kirjoitetaan tutkimusraportissa auki ne keskeiset valinnat, joihin on päädytty ja kuvataan noudatetut toimintatavat. Laadullisen tutkimuksen aineiston kirjo on laaja ja sen käsittelemiseen on olemassa vaihtelevia käytäntöjä. Vaihtoehtoja on monia, eikä tieteenala varsinaisesti aseta rajoituksia sille, millaista aineistoa voi käyttää. Aineiston valinnan ja analyysitavan valinnan välillä ei myöskään ole mitään ehdottomia kytkentöjä, vaikka joillekin aineistoille on tarjolla tyypillisiä analyysitapoja – tai toisin päin, jotkin analyyttiset viitekehykset suosivat tiettyjä aineistotyyppejä (Günther & Hasanen, 2022).

Laadullisessa tutkimuksessa aineistot voivat siis olla erilaisia riippuen tutkimuksen tavoitteista. Tässä työssä haluttiin valikoida aineistoksi primaaristi itse kerätty aineisto käyttämällä julkisesti saatavilla olevaa kirjallista materiaalia. Kirjalliset materiaalit voidaan jakaa yksityisiin dokumentteihin ja joukkotiedotuksen tuotteisiin. Joukkotiedotusta ovat esimerkiksi mielipidekirjoitukset ja lehtijulkaisut. Yksityiset dokumentit sen sijaan ovat esimerkiksi päiväkirjoja, puheita ja muistelmia. Tässä tutkimuksena aineistona ovat julkisesti saatavilla olevat verkkosivustojen tietosuojaselosteet sekä evästeisiin liittyvät verkkosivustojen julkiset dokumentit. Nämä dokumentit luokitellaan joukkotiedotuksen tuotteisiin, sillä ne ovat avoimia tietoja, jotka ovat kaikkien saatavilla (Tuomi & Sarajärvi, 2018).

5.5 Aineistonkeruu ja -rajaus

Tutkimusongelmaan haettiin vastaus itse kerätyn aineiston avulla. Aineisto oli valmiina olemassa ja se oli tekstimuodossa olevaa verkkosivustoilla julkisesti nähtävää tietoa. Tutkimuksen tarkoitus oli koskettaa mahdollisimman monia, joten tämän vuoksi aineistoksi valittiin nimenomaan suosittuja sivustoja. Aineisto kerättiin ja luettiin huolellisesti, minkä jälkeen siitä nostettiin esiin yhteisiä piirteitä ja huolenaiheita. Aineisto kerättiin suoraan valikoiduilta sivustoilta alkaen tietosuojaselosteesta, josta päädyttiin usein erilliselle, sivuston käyttämistä evästeistä kertovalle sivulle (Günther & Hasanen, 2022).

Aineisto päädyttiin rajaamaan kymmenen suosituimman verkkosivuston tietosuojaselosteisiin kautta maailman vuonna 2021. Tällä rajauksella pyrittiin varmistamaan riittävä määrä aineistoa mutta silti punnittu työmäärä. Lisäksi aineistoon haluttiin saada riittävästi vaihtelevuutta ja ehkäistä päällekkäisten tietojen esiintyvyyttä. Isommassa otoskoossa päällekkäisyyksiä olisi varmasti tullut enemmän, siinä missä valikoidulla otoksella päällekkäisyyksiä ilmeni vain yhdessä kohtaa. Aineiston määrällä pyrittiin myös siihen, ettei aineistoon tutustuminen jää pintapuoliseksi, vaan analyysiin on saatu tarpeeksi materiaalia tuoden siihen syvyyttä ja oivaltavuutta. Käytetty aineisto löytyy kokonaisuudessaan liitteestä 1, johon on merkitty yksityiskohtaisesti tietosuojaselosteen version päivämäärä, linkki siihen ja mahdolliset muut linkit tietosuojaselosteen evästekohdasta ohjattuihin lisäsivustoihin.

Aineiston keräämistä varten saadut ajankohtaiset vuoden 2021 tiedot 10 suosituimmasta verkkosivustosta saatiin Cloudflaren verkkosivustolta Radar-palvelusta. Cloudflare (2021) verkkosivuston Radar -palvelu kerää jatkuvasti erilaista dataa ympäri maailman ja erittelee internet-liikennettä maittain. Palvelu näyttää dataa esimerkiksi internet-liikenteen määrästä ja laadusta, kyberhyökkäyksistä ja suosituimmista sivustoista ja nettiselaimista aikavälillä 24 tuntia – 30 vuorokautta. Cloudflaren koostettua dataa löytyy viitattuna useista eri uutismedioista ja sivustoa voidaan pitää luotettavana. Cloudflaren mukaan vuonna 2021 koko maailman 10 suosituinta verkkosivustoa olivat:

1.) TikTok.com
2.) Google.com
3.) Facebook.com
4.) Microsoft.com
5.) Apple.com
6.) Amazon.com
7.) Netflix.com
8.) YouTube.com
9.) Twitter.com
10.) WhatsApp.com

Näiden sivustojen tietosuojaselosteiden evästekohdat mahdollisine evästedokumentteineen toimivat tämän työn tutkimuksen aineistona.

5.6 Laadullinen tutkimus

Tutkimustyypiltään laadullinen tutkimus on empiiristä ja siinä on kyse empiirisen analyysin tavasta argumentoida ja tarkastella havaintoaineistoa. Laadullisessa tutkimustyössä useimmiten käytetty analyysimenetelmä on sisällönanalyysi, joka on laadullisen tutkimuksen perusanalyysimenetelmä. Sisällönanalyysi keskittyy siihen, mistä aiheista, asioista ja teemoista aineisto kertoo. Se soveltuu lähes kaikkiin laadullisen tutkimuksen analyyseihin, sillä se on menetelmänä väljä. Tässä tutkimuksessa käytettiin analyysimenetelmänä sisällönanalyysiä, sillä kyseessä on laadullinen tutkimus. Sisällönanalyysi voi olla joko aineisto- tai teorialähtöistä. Tämä tutkimus oli aineistolähtöistä, teoriaosuuden tukiessa aiheen syvempää ymmärrystä ja syvällisen analyysin ja pohdintojen muodostamista. Tavoitteena oli nostaa esille samankaltaisuuksia tietosuojaselosteiden evästekohdasta ja tutkia missä määrin evästeiden lisätietoja pystyi saamaan selville (Tuomi & Sarajärvi, 2018).

5.7 Aineiston analysointi

Laadullisen aineiston analysoinnin tarkoitus on tiivistää ja jalostaa aineisto käsitteelliseen ja teoreettiseen muotoon. Sen tekemiseen ei ole olemassa mitään yleispätevää kaavaa, ohjetta tai mallia, vaan analyysin pitäisi olla sellainen, että siitä pitäisi saada aikaan informaatioarvoa ja päästä aineiston avulla aiheeseen syvemmälle eli tehdä tulkintaa. Aineistoa tulisi tulkita analyyttisesti ja tulkita tehtyjä havaintoja oman ajattelun tukemana. Laadullista analyysia voi tehdä monen eri menetelmän avulla. Analyysimenetelmä tarkoittaa konkreettista tapaa, jolla aineistoa käsitellään eli analysoidaan (Günther ym., 2022).

Erilaiset lähestymistavat ohjaavat analyysitavan valintaa. Erilaisia lähestymistapoja ovat realistinen tarkastelu, sosiaalinen konstruktionismi sekä fenomenologiseen, hermeneuttiseen tai eksistentiaaliseen tapaan pohjaava analyysi. Tässä tutkimuksessa hyödynnettiin realistista tarkastelutapaa, jossa ollaan kiinnostuneita aineiston sisällöstä ja mitä aineistossa kerrotaan tutkittavasta aiheesta. Tämä analyysimenetelmä on sopusoinnussa tutkimusongelman ja käytettävän aineiston kanssa. Perinteisiä välineitä laadullisen tutkimuksen sisällönanalyysin muodoista ovat koodaaminen, teemoittelu ja tyypittely, joista kaikkia näistä kolmesta hyödynnettiin tässä tutkimuksessa (Günther, Hasanen & Juhila, 2022)

Teemoittelu on laadullisen analyysin perusmenetelmä. Sen avulla tutkimusaineistosta pyritään kiteyttämään keskeisiä aihepiirejä eli teemoja. Teemoiksi voidaan nostaa sellaisia asioita ja aiheita, jotka toistuvat tutkimusaineistossa. Teemoittelun aineiston hankintamuotona on usein teemahaastattelu,

mutta muitakaan aineistonhankinnan menetelmiä ei ole suljettu pois. Tässä tutkimuksessa käytettiin aineistomuotona tekstiä, joka sopii hyvin myös teemoittelun aineistoksi. Käytännössä teemoittelulla pilkotaan aineistoa ja järjestetään sitä erilaisten aihepiirien mukaan ja sen tarkoituksena on nostaa esiin olennaisia aiheita tutkimusongelman kannalta. Teemojen muodostamisessa voidaan käyttää apuna koodausta ja kvantifiointia. Koodaus toimii teemoittelussa eräänlaisina osoitteina ja sen yksikköinä voi toimia esimerkiksi sanat, lauseet, rivit, kappaleet tai tekstiosiot. Koodausta voi tehdä erilaisilla merkitsemistavoilla (Silius, 2018).

Tässä tutkimuksessa käytettiin näitä elementtejä siten, että aineisto koodattiin tekstiosioittain siten, että erilliseen tekstitiedostoon kerättiin erilaiset teemat, joihin aineistosta haluttiin saada vastauksia. Tämän jälkeen itse aineisto pilkottiin näiden teemojen alle. Näin ollen tehtiin aineistolähtöistä koodaamista, tutustuen ensin aineistoon ja miettien millaisia koodauksia aineistoon voitaisiin liittää. Koodausrunkoa täydennettiin koodausprosessin aikana, sillä aineistosta löydettiin lisää kiinnostavia ja olennaisia asioita prosessin aikana. Kvantifiointia käytettiin tässä tutkimuksessa kuvailemaan ryhmien välisiä eroja laskelmien ja niistä piirrettyjen kuvioiden muodossa (Silius, 2018).

Toisena laadullisen analyysin perusmenetelmänä käytettiin tässä tutkimuksessa tyypittelyä. Sen avulla tutkimusaineistosta nostettiin esiin aineistolle tyypillisiä (ja muutamia epätyypillisiä keskimääräisistä poikkeavia) tyyppejä eli ryhmiä. Tyypittelyä käytettiin muodostamaan mahdollisimman yleisiä tyyppejä kvantifioiduin menetelmin käsitellystä aineistosta työstämällä aineistoa aktiivisesti, erityisesti pyrkien tiivistämään sitä (Silius, 2018).

Tämän tutkimuksen aineiston analyysi on siis aloitettu tutustumalla aineistoon. Aineiston tutustumisen jälkeen aiheesta muodostettiin ennakkokäsitys, jonka perusteella varsinainen sisällönanalyysi aloitettiin. Käytännössä aineistoa luettiin, aineiston sisältöä pohdittiin ja rakennettiin siitä kokonaiskuva, jotta saatiin tehtyä päätös siitä, mitä lähdettiin tutkimaan. Aineistoa ei tarvinnut erikseen käsitellä ja muuttaa tekstimuotoon, vaan se oli tekstimuotoisena välittömästi tutkittavissa ilman välivaiheita.

Sisällönanalyysin seuraavassa vaiheessa joko luokitellaan, teemoitetaan tai tyypitellään aineisto. Analysoinnissa pyrittiin järjestämään aineistoa ja tutkia millaisia teemoja ja asioita sieltä nousi esiin ja mitä tulkintoja näiden perusteella voitiin tehdä. Lisäksi yleisimpiä esiintyviä tyyppejä tyypiteltiin tässä vaiheessa. Tämän tutkimuksen mukaiseen teemoitteluun päädyttiin tutkimusaineistoa lukemalla ja etsimällä samankaltaisia tieto-osioita teksteistä, jotta voitiin suorittaa vertailua ja analysointia, tutkimuskysymys mielessä pitäen. Analyysiprosessi eteni tämän jälkeen ajattelulla, kirjaamalla havaintoja ylös ja kirjoittamalla. Analyysin perusteella pohdintaa aiheesta voitiin yksityiskohtaisista huomioista yleisiin huomioihin ja pyrittiin tulosten läpinäkyvyyteen (Günther ym., 2022; Tuomi & Sarajärvi, 2018).

6 TULOKSET

Tässä osiossa käsitellään tutkimuksen tuloksia. Ensin paneudutaan siihen, millaisia perusteita verkkosivustot kertovat evästeiden käyttämiselle. Tämän jälkeen tarkastellaan tietosuojaselosteiden perustietoja, tekniikoita ja teknisiä tietoja, kolmansia osapuolia, evästeiden poistamista ja hallintaa. Lopuksi vastataan tutkimuskysymykseen.

Tämän tutkimuksen mukaan eri verkkosivustojen tietosuojaselosteet ovat jokainen yksilöllisiä. Ne eivät noudata mitään samaa kaavaa siten, että samanlainen osuus, esimerkiksi kertominen evästeiden käyttämisestä, löytyisi aina tietystä paikasta. Tämä yksistään helpottaisi lukijaa löytämään itseään kiinnostavat tai huolettavat kohdat. Jokainen seloste piti lukea yksilönä ja löytää sieltä etsimällä haluttuun teemaan sopivia asioita. Tämä osin myös rajasi tutkimustuloksia, sillä asioiden seikkaperäisyys vaihteli laajasti sivustojen välillä. Tältä osin tiettyjä tärkeitä yksityiskohtia, esimerkiksi kolmansien osapuolien lukumäärää tai käytettyjen evästeiden lukumäärää ei voitu kvantifioida ja taulukoida mielekkäästi. Tutkimusaineistossa havaittiin myös yksi toistotapaus: 10 suosituimman verkkosivuston joukosta YouTube on osa Googlea ja YouTube viittasi palvelussaan suoraan Googlen tietosuojaselosteeseen. Aineiston käsittelyssä kumpikin on siis käsitelty omana yksikkönään, vaikka ne käyttävät samaa tietosuojaselostetta.

6.1 Perusteet evästeiden käyttämiselle

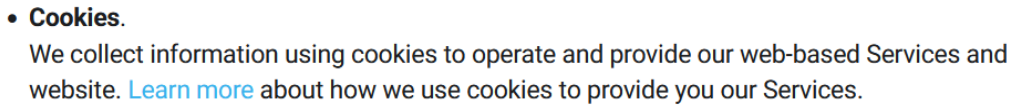
Verkkosivustoilla oli hyvin samankaltaisia perusteluita sille, miksi ne käyttävät evästeitä. Tutkimuksen tuloksena syntyi lista, joka esittelee kaikki löydetyt perustelut verkkosivustojen evästeiden käyttämiselle:

- Käyttökokemuksen parantaminen
- Käyttäjän asetusten ja määritysten muistaminen
- Käyttäjän ymmärtäminen

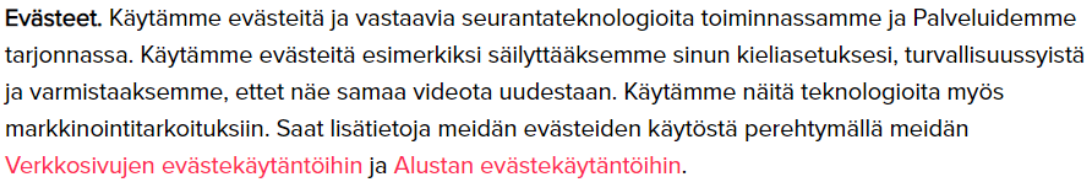
- Käyttäjän suojaaminen
- Turvallisen käyttökokemuksen varmistaminen (petosten torjunta, tietoturva)
- Mainonnan ja markkinoinnin kohdentaminen ja räätälöinti (henkilökohtaisen sisällön tarjoaminen)
- Palveluiden kehittäminen käyttäjätiedon perusteella
- Palveluiden käytön analysointi, ymmärrys ja parantaminen
- Käyttäjävuorovaikutuksen ymmärtäminen
- Palvelun tehokkuus ja toiminnallisuus
- Käyttäjän todentaminen
- Tilastointi (esimerkiksi mainoskampanjan toimivuus)
- Palautteen saaminen
- Kolmansien osapuolten tarkoitukset

6.2 Tietosuojaselosteen perustiedot

Tutkimuksen tuloksena kävi ilmi, että pelkkä tietosuojaseloste itsessään ei antanut kuin kahdessa tapauksessa kymmenestä (Microsoft ja Netflix) kaikkea evästeisiin liittyvää tietoa. Lopuissa kahdeksassa tietosuojaseloste kertoikin evästeistä vain hyvin lyhyesti omana alaotsikkonaan. Tämän otsikon alla oli linkkimuotoinen sana, josta lukija ohjattiin lukemaan lisätietoja evästeistä erillisestä selosteesta (esimerkit kuvioissa 4 ja 5). Joissakin tapauksissa (TikTok ja Facebook) joutui lukemaan 2 erillistä evästeselostetta, sillä TikTokilla oli erilliset evästeselosteet myös sen käyttämälle alustalle ja Facebookin osana taas toimii Instagram, jonka evästeseloste kuuluu myös Facebookin evästeselosteeseen.



KUVIO 4 Tietosuojaselosteen evästekohta

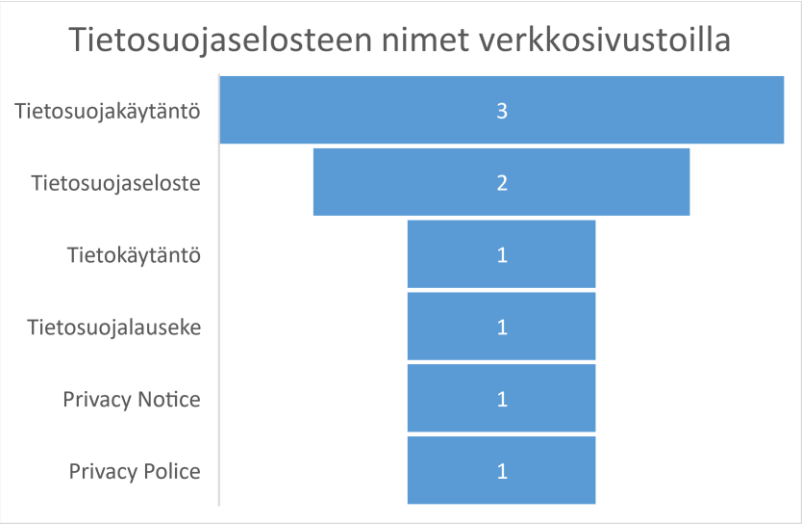


KUVIO 5 TikTokin tietosuojaselosteen evästekohta

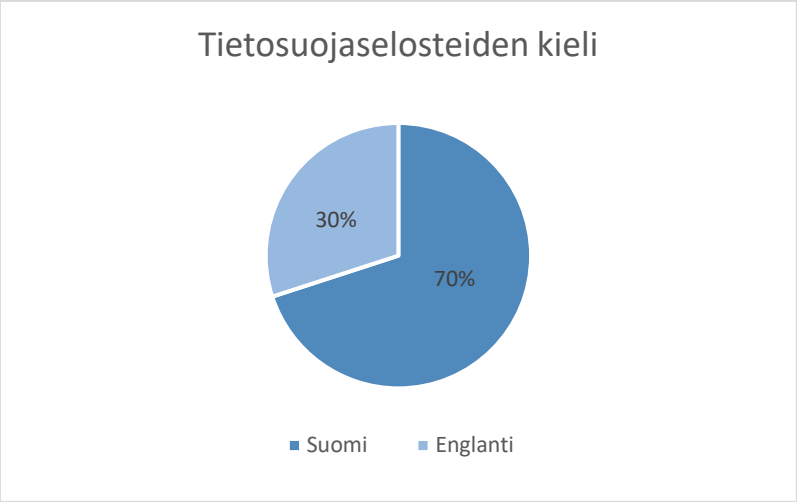
Myös nimeämiskäytännöt vaihtelivat laajasti. Erillinen, evästeistä kertova seloste kulki seuraavilla nimityksillä:

- Web Cookies Policy
- Miten Google käyttää evästeitä
- Evästeet ja muut tallennustekniikat
- Evästekäytäntö
- Evästeiden käyttö
- How Cookies are used on Twitter
- Cookies

Myös tietosuojaselosteella oli monia nimiä niin suomeksi kuin englanniksikin, joista yleisimmäksi tutkimusaineiston perusteella nousi tietosuojakäytäntö. Kaikki nämä nimet tarkoittavat kuitenkin samaa asiaa, jota käsitellään tässä työssä nimellä tietosuojaseloste. Kuvio 6 esittää jakaumaa eri nimien kanssa. Se myös havainnollistaa sen, kuinka montaa erilaista nimeä samasta asiasta tavallinen verkkosivustojen käyttäjä kohtaa. Jos etsii aina vain tietosuojaselostetta, tietoa ei välttämättä löydy, etenkään jos tietosuojaseloste on saatavilla vain englanniksi. Kuvio 7 osoittaa, kuinka valtaosa eli tässä otosmäärässä 70 % tietosuojaselosteista oli tarjolla suomeksi, mutta 30 % oli saatavilla vain englanniksi. Tavalliselta verkkosivustojen kuluttajalta vaaditaan siis myös sujuvaa englannin kielen taitoa yleensä ja erityisesti evästeisiin liittyvän termistönsä puolesta. Yhdessä tapauksessa (TikTok) tarjolla oli suomenkielinen tietosuojaseloste, jonka evästekohdasta oli linkki erilliseen evästesivustoon ja alustan käyttämiin evästeisiin, jotka olivat molemmat englanniksi.

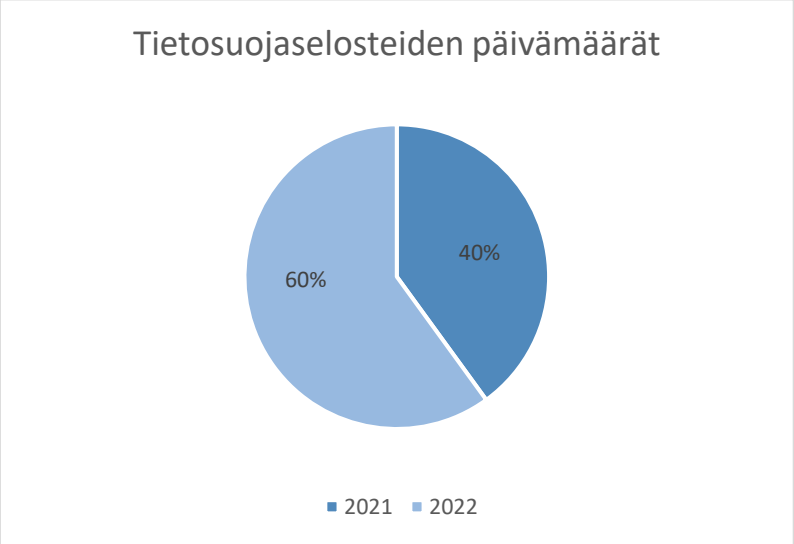


KUVIO 6 Tietosuojaselosteen nimet verkkosivustoilla



KUVIO 7 Tietosuojaselosteiden kieli

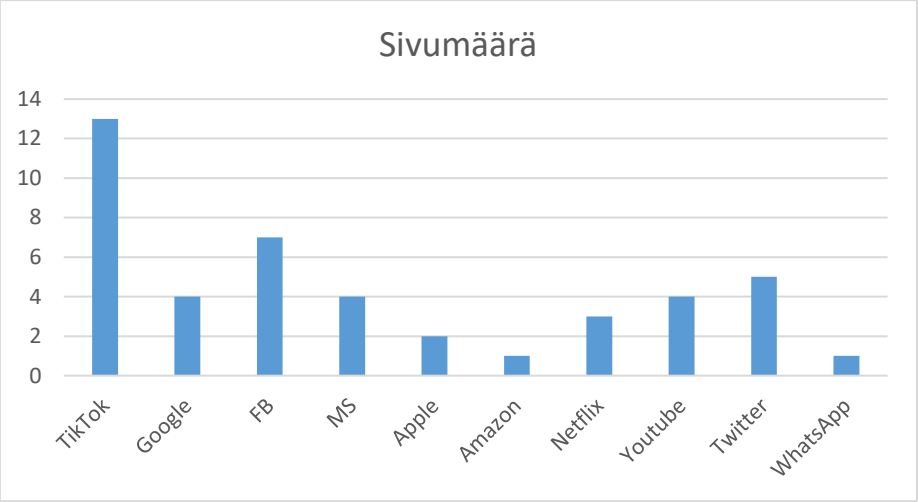
Tietosuojaselosteessa oli kaikissa selvästi nähtävillä päivämäärä, jolloin sitä oli viimeksi päivitetty. Päivämäärä näkyi joko heti dokumentin alussa, tai sen lopussa hyvin selkeästi ilmaistuna omalla rivillään. Ainoa sivusto, joka oli maininnut ja linkannut dokumentin loppuun aikaisemman voimassa olleen tietosuojaselosteen oli Netflix.



KUVIO 8 Tietosuojaselosteiden päivämäärät

Luettavan tekstin määrässä oli isoja vaihteluita. Yhdessä tapauksessa (TikTok) sivumäärä lähes tuplaantui, sillä palvelun käyttämällä alustalla oli oma evästedokumenttinsa. Osalla oli myös hyvin lyhyitä tekstejä, joista löytyi maininnat kiinnostavista asioista mutta ilman yksityiskohtaisia selvityksiä. Näin oli Amazonilla ja WhatsAppilla eikä vielä erillisiä lisälinkkejä evästeistä tarkemmin löytynyt. Tutkimuksessa tutkitun luettavan tekstin määrä arvioitiin sivumääränä, joka tekstistä tulisi tulostettaessa. Tulosteiden leipätekstit olivat tekstikokoa 11pt

- 12pt. Tulosteet on koostettu ottamalla sivustoilta sivuston tarjoamalla muotoilulla tuloste. Tietosuojaselosteesta tulostettavaksi määriteltiin evästeitä koskeva tekstiosuus ja mahdolliset lisäsivustot, eli käytännössä kaikki kohdat, joissa kerrottiin evästeistä. Kuvio 9 osoittaa sivumäärien suuren vaihtelun. Kaikista lyhyimmät, vain yhden sivun mittaiset tekstit olivat Amazonilla ja WhatsAppilla, kun taas TikTok vei pisimmän tekstiosuuden voiton 13 sivulla. Luettavien sivujen keskiarvoksi saatiin tutkimusaineiston perusteella 4,4 sivua.



KUVIO 9 Sivumäärä

6.3 Tekniikat ja tekniset tiedot

Kaikki sivustot kertoivat käyttävänsä evästeitä. Yhdeksän kertoi käyttävänsä evästeiden lisäksi myös muita vastaavia tekniikoita. Vain WhatsAppin tietosuojaselosteessa tai evästeselosteessa ei löytynyt mainintaa muista evästeitä vastaavista tekniikoista. Yleisimmäksi mainittiin pikselit ja paikallinen tallennus, kuten esimerkiksi selaimen verkkotallennus, sovellustietojen välimuistit, tietokannat ja palvelinlokit. Jäljitteet olivat yleisiä ja ainoana sivustona Microsoft mainitsi myös LSO- eli Flash-evästeiden käytön sekä Silverlight-sovelluksen tallennustilana. Näiden lisäksi mainittiin SDK:t. 4 sivustoa mainitsi muutaman esimerkin evästeitä vastaavista tekniikoista, päättäen lauseen esimerkiksi: ”…ja muita vastaavia tekniikoita.” jättäen avoimeksi sen, mitä näillä muilla tekniikoilla tarkoitettiin.

5 sivustoa (Google, YouTube, Facebook, Microsoft ja Twitter) olivat kertoneet avoimesti ja teknisesti, minkä nimisiä evästeitä sivusto käyttää ja mikä tarkoitus milläkin evästeellä on. Esimerkkinä tarkemmasta selvityksestä toimii kuvio 10, jossa on ote Microsoftin asettamista evästeistä. Huomionarvoisesti Microsoft toteaa, ettei luettelo ole kuitenkaan kattava, eli lukija pysty saamaan varmuutta siitä, kuinka paljon ja minkälaisia evästeitä Microsoft asettaa kokonaisuudessaan. Myös Facebook (kuvio 11) antaa esimerkkejä millaisia evästeitä voidaan asettaa eri vaiheissa verkkosivuston käyttöä, mutta lista ei ole kattava, vaan

esimerkinomainen. Samoin Twitter esittelee luettelon yleisimmin käytetyistä evästeistä, mutta ei suinkaan kaikista.

Jotkin yleisesti käyttämämme evästeet on lueteltu alla. Tämä luettelo ei ole kattava, vaan sen tarkoituksena on kuvata tärkeimpiä syitä evästeiden asettamiselle. Jos vierailet jossakin sivustossamme, sivusto asettaa jonkin seuraavista evästeistä tai ne kaikki:

- **MSCC**. Sisältää useimpien Microsoftin ominaisuuksien käyttäjävalinnat.
- **MUID, MC1 ja MSFPC**. Tunnistaa yksilöivät selaimet, jotka vierailevat Microsoftin sivustoissa. Näitä evästeitä käytetään markkinointitarkoituksiin, sivustoanalyyseihin ja muihin toimintaan liittyviin tarkoituksiin.
- **ANON**. Sisältää Microsoft-tilistäsi muodostetun yksilöivän ANID-tunnisteen, jota käytetään mainontaan, mukauttamiseen ja toimintaan liittyviin tarkoituksiin. Sitä käytetään myös säilyttämään valintasi estää kiinnostuksen kohteisiin perustuva mainonta Microsoftilta, jos olet valinnut eston liittämisen Microsoft-tiliisi.
- **CC**. Sisältää maakoodin, joka päätellään IP-osoitteestasi.
- **PPAuth, MSPAuth, MSNRPSAuth, KievRPSAuth, WLSSC, MSPProf**. Auttavat todentamaan sinut, kun kirjaudut sisään Microsoft-tililläsi.
- **MC0**. Havaitsee, ovatko evästeet käytössä selaimessa.
- **MS0**. Tunnistaa tietyn istunnon.
- **NAP**. Sisältää maasi, postinumerosi, ikäsi, sukupuolesi, kielesi ja ammattisi salatun version (jos ne tunnetaan) Microsoft-tiliprofiilisi perusteella.
- **MH**. Näkyy yhteispalvelusivustoissa, joissa Microsoft toimii yhteistyössä mainostajan kanssa. Eväste määrittää mainostajan, jotta oikea mainos valitaan.
- **childinfo, kcdob, kcrelid, kcru, pcfm**. Sisältää tietoja, joita Microsoft-tili käyttää sivuillaan suhteessa lasten tileihin.
- **MR**. Microsoft käyttää tätä evästettä MUID-eväs teen nollaamiseen tai päivittämiseen.
- **x-ms-gateway-slice**. Määrittää yhdyskäytävän kuormituksen tasaamiseksi.
- **TOptOut**. Tallentaa valintasi olla vastaanottamatta Microsoftin toimittamaa kiinnostuksen kohteisiin perustuvaa mainontaa. Tarvittaessa asetamme tämän evästeen oletusarvoisesti, ja se poistetaan, kun anna luvan kiinnostuksesi kohteisiin perustuvaan mainontaan.

KUVIO 10 Microsoftin asettamien evästeiden listaus

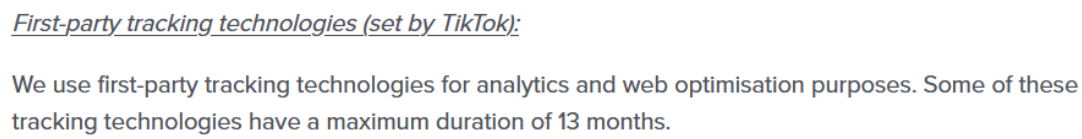
Todennus

Käytämme evästeitä tilisi vahvistamisessa ja sisäänkirjautumisajan määrittämisessä. Tarkoituksenamme on helpottaa Meta-tuotteiden käyttöä, tarjota asianmukainen käyttökokemus ja näyttää osuvia ominaisuuksia.

Esimerkiksi: Käytämme evästeitä pitämään sinut kirjautuneena, kun siirryt Facebook-Sivulta toiselle. Evästeet auttavat meitä myös muistamaan selaimesi, jotta sinun ei tarvitse kirjautua Facebookiin yhä uudelleen ja voit kirjautua Facebookiin helpommin kolmannen osapuolen sovelluksista ja verkkosivustoista. Käytämme esimerkiksi ”c_user”- ja ”xs”-evästeitä muun muassa tähän tarkoitukseen, ja niiden elinkaari on 365 päivää.

KUVIO 11 Facebookin esimerkit evästeistä

Evästeiden kestoaika jää suurimmassa osassa arvoitukseksi. TikTok, Facebook, Google ja YouTube ovat maininneet kategorioittain evästeiden maksimikestoajat kuvion 12 tapaan. Tämän lisäksi Google ja YouTube, joita koskee sama tietosuojaseloste, mainitsivat löyhästi kategorioittain evästeiden kestoaikoja. Puolet eli 50 % tutkimusaineistosta ei kuitenkaan mainitse evästeiden kestosta lainkaan.



KUVIO 12 TikTok evästeiden kestoaikaesimerkki

6.4 Kolmannet osapuolet

Kaikki sivustot käyttivät kolmansia osapuolia. Osa, esimerkiksi WhatsApp ja Apple mainitsivat vain, että palvelussa käytetään kolmansia osapuolia ilman lisäselvityksiä tai syitä kolmansien osapuolien käyttämiselle. Muissa aineiston verkkosivustoista (80 %) kuvausta kolmansien osapuolien käyttämisestä oli hieman enemmän ja yksityiskohtaisiakin selosteita löytyi. Esimerkiksi Microsoft listasi nimeltä kaikki kolmannet osapuolet. Tutkimuksen tuloksena saatiin kattava listaus siitä, miksi verkkosivustot käyttävät kolmansia osapuolia. Yleisimmät syyt olivat mainonta, markkinointi ja tietojen analysointi. Tuloksena esitellään kattava listaus siitä, mitä syitä kokonaisuudessaan kolmansien osapuolien käyttämiselle mainittiin:

- Analytiikka
- Suorituskyky
- Mainonta
- Markkinointi
- Mittaus
- Analyysipalvelut
- Sisällön toimittaminen
- Tietojen kerääminen selaimesta
- Tietojen kerääminen laitteesta
- Tiettyjen ominaisuuksien tarjoaminen
- Palveluiden parantaminen
- Sosiaalisen median palvelut

Kolmansien osapuolien käyttämisen yhteydessä 5 verkkosivustoa (Tiktok, Google, YouTube ja Twitter) mainitsivat kolmansien osapuolien määrän viitteellisesti. Googlella ja YouTubella määrä oli 2 miljoonaa ja TikTokilla lyhyt lista isoista yrityksistä, kuten Facebook ja Google Analytics. Twitter mainitsi löyhästi kolmansiksi osapuoliksi vain Google Analyticsin ja sellaiset toimijat, jotka

käyttävät integroituja Twitterin palveluita verkkosivustoillaan. Puolella tutkimusaineiston verkkosivustoista (50 %) mainintaa ei ollut lainkaan, mutta silti kaikki käyttivät kolmansia osapuolia ja olivat maininneet tämän.

6.5 Evästeiden poistaminen ja hallinta

Tutkimuksen tuloksena kaikki verkkosivustot antoivat selkeästi yhteystiedon, johon käyttäjä voi olla yhteydessä tietosuojaselosteen asioista yleensä ottaen tai evästeisiin liittyen. Yhteystieto oli annettu sähköpostiosoitteen muodossa tai linkkinä yhteydenottolomakkeeseen.

Kaikki tutkimuksessa mukana olleet verkkosivustot antoivat tietosuojaselosteessa tai evästeitä koskevissa lisädokumenteissa ohjeistuksen siitä, miten evästeitä ja niiden asettamista voidaan hallita. Ohjeistukset vaihtelivat palvelusta riippuen. Kaikki muut paitsi Twitter, eli 90 % verkkosivustoista, mainitsivat evästeiden hallinta- tai poistotyökaluksi käyttäjän käytössä olevan selaimen asetukset. Yksityiskohtaisempia ohjeistuksia löytyi Microsoftilta sen omien selainten, kuten Microsoft Edgen ja Internet Explorerin hallintaan ja Applelta sen omaan Safari-selaimen hallintaan. Myös käytetyn laitteen asetuksia kehotettiin muokkaamaan ja Google ja YouTube mainitsivat incognito-tilan käyttämisen verkossa selaamiseen.

Kaikki muut verkkosivustot paitsi Google ja YouTube antoivat jonkinlaiset varoitukset evästeiden poistamiseen tai hallintaan liittyen. Mainintoja evästeiden poistamisesta tai rajoittamisesta löytyi seuraavasti:

- Jotkin evästeet ovat välttämättömiä palvelun käyttämiselle
- Tiettyjä palvelun osia, mukaan lukien lisäominaisuudet, ei välttämättä voi käyttää ilman evästeitä
- Muut palvelun osat eivät ehkä toimi oikein
- Evästeiden käyttöä rajoittavat työkalut voivat vaikuttaa hallintotoimiin
- Sisään kirjautuminen ei ole mahdollista
- Evästeiden mukaan määräytyvät asetukset menetetään
- Et voi lisätä ostoskoriin tuotteita tai siirtyä tuotteiden maksuun
- Palvelu ei tue *do not track* -selainvaihtoehtoa

6.6 Vastaus tutkimuskysymykseen

Tässä tutkimuksessa haluttiin vastaus seuraavaan tutkimuskysymykseen:

> Mitä uhkia yksityisyyden suojalle tietosuojaselosteiden evästekohdista nousee esiin?

Tutkimuksessa nousi esiin seuraavia listassa mainittavia huolestuttavia kohtia, joiden voidaan katsoa olevan selkeä riski yksityisyyden suojalle. Näitä kaikkia käsitellään tarkemmin omissa alaluvuissaan:

- Kolmannet osapuolet
- Käyttäjän tiedot ja taidot
- Läpinäkyvyys
- Työläys
- Käyttäjän vastuu

6.6.1 Kolmannet osapuolet

Huolestuttavia kohtia löytyi enimmäkseen tietosuojaselosteiden kolmansien osapuolien käyttämisen osioista. Tutkimuksessa kävi ilmi se, että kolmannet osapuolet saavat käyttäjistä laajasti tietoa, seuraten käyttäjää myös kyseisen verkkosivuston ulkopuolella. Kolmannen osapuolten käyttämisten kohdassa oli mainintoja, joissa esimerkiksi Facebook ja Twitter mainitsivat avoimesti seuraavansa käyttäjän toimintaa kaikilla verkkosivustoilla, vaikka käyttäjä olisi kirjautunut ulos palvelusta. Google ja YouTube mainitsi käyttävänsä lisäksi myös luetettuja yrityksiä tietojen käsittelijöinä mainiten sen, että ne eivät kuitenkaan ole virallisia yhteistyökumppaneita. Tällaisessa tapauksessa herää huoli siitä, kuka on lopulta vastuussa mahdollisista tietovuodoista tai väärinkäytöksistä, jos virallista sopimusta yhteistyöstä ei ole tehty. Google ja YouTube vakuuttavat, että yhteistyössä toimivat yritykset noudattavat heidän tietosuojakäytäntöjään ja asiaankuuluvia yksityisyys- ja tietosuojamenetelmiä. Lisäksi ne toteavat, etteivät ne jaa tietoja, joista käyttäjä olisi tunnistettavissa, ellei käyttäjä niin pyydä, mainiten kuitenkin myös sen, että käyttäjän ei-henkilökohtaisia tietoja voidaan jakaa julkisesti yhteistyökumppaneille. Tässä ei-henkilökohtaisten tietojen vapaassa jakamisessa piilee riski ei-henkilökohtaisten tietojen yhdistelystä, jolloin niistä saattaa muodosta henkilökohtaisia tai jopa arkaluontoisia tietoja. Microsoft mainitsee, että sen kolmannen osapuolen yritykset hyödyntävät käyttäjätietoja tietosuojakäytäntöjensä mukaisesti, mutta tietosuojaselosteessa kerrotaan kuitenkin myös avoimesti, että nämä yritykset saattavat kerätä ja yhdistellä käyttäjän tietoja ja toimia eri sivustoissa, sovelluksissa ja verkkopalveluissa. Kuten teoriaosuudessa todettiin, tietojen yhdistelystä saattaa muodostua henkilökohtaisia tai jopa arkaluontoisia kokonaisuuksia käyttäjästä.

Myös kolmansien osapuolien valtava lukumäärä aiheuttaa huolia, sillä tarkkaa listausta ei ollut aina saatavilla. Käyttäjän ei ole mahdollista olla täysin varma siitä, kuka hänen tietojaan käyttää tai saa haltuunsa, sillä tutkimusaineiston mukaan kolmansia osapuolia saattaa olla useita satoja tai jopa miljoonia, joiden joukossa on valtavan isoja toimijoita. Jos käyttäjä haluaisi todella olla varma siitä, miten hänen tietojaan käytetään kolmansien osapuolien toimesta, tulisi hänen tutustua kaikkien kolmansien osapuolien tietosuojaselosteisiin. Tämän vaatiminen yksittäiseltä käyttäjältä ei olisi paitsi kohtuutonta, vaan joissakin tapauksissa jopa mahdotonta kolmansien osapuolten suuren määrän johdosta. Lisäksi olisi hyvä olla olemassa myös tietosuojaselosteen tai evästeestä kertovan

lisäselosteen aikaisempi versio, kuten esimerkiksi Netflixin tapauksessa tietosuojaselosteen lopussa oli suora linkki aikaisempaan voimassa olevaan tietosuojaselosteeseen. Tämä toisi käyttäjälle läpinäkyvyyttä ja mahdollisuuden tarkastella vierekkäin tietosuojaselosteiden eri versioita.

Positiivisena esimerkkinä nousi esiin Netflix, joka kertoi avoimesti, kuinka eräät kolmannen osapuolen sivustot ja sovellukset ovat heidän verkkosivustollaan käytössä, mutta kerätyt tiedot tietosuojataan. Tietosuojauksessa alkuperäinen tieto muutetaan joksikin toiseksi arvoksi, jotta alkuperäinen tieto ei paljastu. Kolmas osapuoli voi verrata tietosuojattua tunnusta oman tietokantansa tunnuksiin ja verrattu tunnus löytyy tietokannasta vain, jos käyttäjä on käyttänyt samaa tunnusta (esimerkiksi sähköpostiosoite) sekä Netflixissä, että kolmannen osapuolen palveluissa. Tällainen tietojen salaaminen herättää käyttäjässä luottamusta siihen, että yritys tekee konkreettisia toimia sen eteen, että käyttäjän yksityiset tiedot olisivat turvassa, vaikka niitä kerätäänkin ja luovutetaan eteenpäin.

6.6.2 Käyttäjän tiedot ja taidot

Verkkosivustojen ja palveluiden käyttäjiltä odotetaan sujuvaa englannin kielen taitoa, sillä tietosuojaselosteista osa on tarjolla vain englanniksi, kuten myös evästeisiin liittyvät jatkosivustot. Englannin kielen sujuva osaaminen, erityisesti evästeisiin liittyvän termistön ja käsitteiden kanssa, täytyy olla sujuvaa, jotta käyttäjän on mahdollista ymmärtää annetut tiedot verkkosivustojen ja kolmansien osapuolien asettamista evästeistä.

Jotkin tietosuojaselosteista antoivat teknisiä tietoja, millaisia evästeitä he käyttävät ja mihin tarkoituksiin. Vain harva mainitsi, kuinka kauan asetetut evästeet ovat voimassa. Evästeiden tiedot olivat kaikissa ne mainitsevissa verkkosivustoissa vain esimerkinomaisia, eli täydellistä listausta ei löytynyt yhdeltäkään sivustolta. Käyttäjällä ei siis ole edes mahdollisuutta perusteellisia tietoja käytetyistä evästeistä, ja osa sivustoista myös vaati käyttäjältä alan syvempää ymmärrystä, jotta evästeen käyttötarkoitus olisi mahdollista ymmärtää. Lisäksi verkkosivustot käyttivät muita vastaavia tekniikoita käyttäjän tietojen keräämiseen, eli tietoja eivät kerää vain evästeet. Muista tekniikoista mainitaan avoimesti, kuinka niitä käytetään, mutta ei yksilöidä tarkemmin millä tavoin. Poikkeuksen tähän muodostivat tietyt tekniset ratkaisut, joiden ymmärtäminen vaatisi kuitenkin peruskäyttäjää selvästi syvempää asiantuntemusta.

6.6.3 Läpinäkyvyys

Tutkimuksessa nousi esiin myös huoli siitä, miten tietoja jätettiin avoimeksi. Kuten edellä olevassa kappaleessa mainittiin, täydellistä listausta käytetyistä evästeistä ja niiden kestosta ei ollut saatavilla. Mainittuna oli vain yleisimmin käytettyjä evästeitä, usein esimerkinomaisesti. Muidenkin vastaavien tekniikoiden kohdalla lauseet päätettiin hyvin avoimesti todeten vain, että verkkosivustolla käytetään niitä. Tämä jättää paljon arvailun varaa tarkemmista tekniikoista ja niiden toimintaperiaatteista.

6.6.4 Työläys ja käyttäjän vastuu

Käyttäjälle annetaan hyvin paljon vastuuta, jos hän sallii evästeiden käyttämisen verkkosivustoilla. Käyttäjän tulisi jaksaa lukea tarkasti keskimäärin 4,4 sivua joko suomen- tai englanninkielistä, osin teknistä ja vaikeaselkoista tekstiä. Tämän lisäksi käyttäjän tulisi avata linkki tai linkkejä, joiden takana lisätiedot evästeistä löytyvät, ja lukea myös ne. Tämä vaatisi usein käytännössä myös uuden oppimista, sillä mikäli käyttäjä kohtaa uusia termejä, hänen tulisi tutustua niihin saadakseen riittävän ymmärryksen esimerkiksi muista evästeitä vastaavista tiedonkeräystekniikoista. Käyttäjän täytyisi siis käytännössä opiskella muut evästeitä vastaavat tekniikat, perehtyä niihin ja varmuuden vuoksi olettaa niiden kaikkien olevan käytössä, sillä kuvaukset vastaavista tekniikoista oli jätetty avoimiksi.

Käyttäjän tulisi myös huomioida, mikäli tietosuojaseloste saa päivityksen ja lukea tämä uusi päivitetty versio siten, että hän voisi vertailla sen kohtia vanhaan tietosuojaselosteeseen ja näin ollen löytää tekstin seasta muutokset. Lisäksi, jotta käyttäjällä olisi varmuus siitä, mihin hänen tietonsa oikein menevät ja mihin niitä käytetään, hänen tulisi tutustua kaikkiin kolmansien osapuolien tietosuojaselosteisiin ja niiden mahdollisiin evästedokumentteihin. Tämä on käytännössä mahdoton tehtävä ja käyttäjä hukkuu tietosuojaselosteiden suohon. Käyttäjä on siis mahdottoman tehtävän äärellä yrittäessään hahmottaa todellista kokonaiskuvaa ja sitä verkostoa, johon hänen tietonsa menevät ja jossa niitä käytetään, jos hän sallii evästeiden käyttämisen vierailemallaan sivustolla. Käyttäjän vastuulla on selvittää itse valtava määrä tietoa ja helposti herääkin epäilys siitä, tietävätkö isot yritykset, kuten Google todellisuudessa sen, kenelle kaikille tiedot käyttäjästä päätyvät. Lienee paikallaan myös kysyä, kenellä on vastuu siitä, jos joku ei noudata tietosuojaselostetta ja vuotaa tiedot vääriin käsiin? Nämä ovat isoja ja merkittäviä kysymyksiä, joihin ei tässä tutkimuksessa saada vastausta.

7 JOHTOPÄÄTÖKSET

Verkkosivustojen käyttäjillä on käsissään hirvittävä vastuu ja riski siitä, että evästeet salliessaan heidän tietonsa joutuvat vääriin käsiin tai niitä käytetään vääriin tarkoituksiin. Käyttäjän tietoja saatetaan yhdistellä tai jakaa kolmansille osapuolille tai yhteistyökumppaneille tai jopa epävirallisille yhteistyökumppaneille, jolloin käyttäjällä on todellinen haaste saada muodostettua käsitystä hänen tietojensa keräämisen ja käsittelyn laajuudesta. Käyttäjä myös käytännössä kuormittuu kohtuuttomasti työstä, johon hänet on valtuutettu tietosuojaselosteen lukuja ymmärtämisprosessissa liitteineen. Seurauksena voi olla, ettei käyttäjä lue jatkossakaan tietosuojaselosteita ja ikään kuin allergisoituu niitä kohtaan.

Tutkimuksen tuloksena löydettiin merkittäviä uhkia käyttäjän yksityisyyden suojalle. Sen myötä nousi vahvana esiin huomio siitä, että käyttäjät tarvitsisivat konkreettista tukea, apuvälineitä ja tietoa kahlatessaan päivittäin turvallista reittiään läpi tietosuojaselosteiden maailmassa ja pohtien hyväksyvätkö he sivustojen tarjoamat evästeet vai eivät.

Verkkosivustot käyttävät välttämättömiä evästeitä toimiakseen oikein, mutta ne asettavat myös käyttäjän suostumuksella lukuisia määriä ei-välttämättömiä evästeitä. Tällöin verkkosivustot sekä niiden käyttämät kolmannet osapuolet hyödyntävät käyttäjiensä tietoja kilpailuetunaan mahdollisimman paljon tietoja keräillen ja jopa yhdistellen. Tietosuojaselosteen tarkoitus olisi lieventää näitä pelkoja, kuitenkaan siinä usein onnistumatta. On selkeästi olemassa paradigma, jonka mukaan kuluttajat ovat huolissaan yksityisistä tiedoistaan, mutta kuitenkaan he eivät halua esteitä ja hidasteita palvelun käytölle. Kuluttajat pääosin ohittavat tietosuojaselosteen sitä lukematta. Myös aikomus tai motivaatio tietosuojaselosteen lukemiselle ei ole korkealla, sillä se aiheuttaa negatiivisia ja kuormittavia tunteita. Silloinkin, kun kuluttajat päätyvät lukemaan tietosuojaselosteen, sen ei koeta tuovan mitään lisäarvoa tai turvallisuuden tunnetta. Verkkosivustot käsittelevät tietoja käyttäjän silmiltä piilossa, jolloin todellista konkretiaa tietojen keräämisestä, käsittelystä ja luovuttamisesta ei ylipäätään synny. Yksityisyys on selkeästi haaste ja ongelma ja maailman monimutkaisuus ja toiminta ylittävät ihmisen kyvyn ymmärtää se.

Tämän pro-gradutyön tutkimuksen tuloksina saatiin muodostettua ajantasainen näkemys siitä, miten jokainen tietosuojaseloste, sen evästeosuus ja evästeisiin mahdollisesti linkitetyt tiedostot ovat jokainen omanlaisia yksilöitään ilman johdonmukaista jäsentelyä ja rakennetta. Tutkimuksen tuloksina saatiin koostetusti tutkimusaineiston, eli 10 suosituimman verkkosivuston vuonna 2021 tietosuojaselosteiden evästeosuuksista faktoja, vastaus tutkimuskysymykseen sekä jatkotutkimusaiheita ja kehitysideoita. Esille aineistosta ja sen käsittelystä nousivat erityisesti seuraavat havainnot:

- Harvassa tapauksessa evästeitä koskevia tietoja oli vain tietosuojaselosteessa, yleensä vaadittiin avaamaan lisälinkki tai -linkkejä
- Tietosuojaselosteella ja erillisellä evästeselosteella on vaihtelevia nimiä
- Suurin osa tietosuojaselosteista liitteineen oli suomeksi, mutta englantia oli myös pakko osata
- Tietosuojaselosteet liitteineen olivat ajantasaisia ja kaikki niistä oli päivätty vuosina 2021–2022
- Tietosuojaselosteiden eväisteitä koskevien osuuksien pituus vaihteli suuresti, keskiarvon ollessa 4,4 sivua
- Kaikki tutkivat sivustot käyttivät evästeitä ja lähes kaikki myös muita evästeitä vastaavia tekniikoita käyttäjien tietojen keräämiseen
- Puolissa verkkosivustoista oli evästelistaus, mutta yksikään näistä ei ollut kattava
- Evästeiden kestoaikaa ei ollut suurimmassa osassa mainittu lainkaan
- Kaikki käyttivät kolmansia osapuolia ja niiden määrä saattoi olla valtava, jopa miljoonia
- Yhteystiedot lisätietojen saamiseksi löytyivät kaikilta
- Kaikki ohjeistivat evästeiden hallintaan tai poistoon, mutta laatu ja ohjeistuksen syvyys vaihteli merkittävästi
- Suurin osa ”uhkasi” käyttäjää, jos evästeet poistetaan käytöstä

Tässä työssä haluttiin saada vastaus tutkimuskysymykseen, jonka avulla selvitettiin, mitä uhkia yksityisyyden suojalle tietosuojaselosteiden evästekohdista nousee esiin. Tutkimuksen avulla kävi ilmi, että huolestuttavimmat maininnat tietosuojaselosteiden evästekohdissa liittyivät kolmansiin osapuoliin, jotka myös teorian ja aikaisempien tutkimuksien pohjalta koetaan kaikkein huolestuttavimmaksi aiheeksi käyttäjien näkökulmasta. Kolmannet osapuolet saavat käyttäjistä laajasti tietoa, myös kyseisen verkkosivuston ulkopuolella ja kolmansia osapuolia saattaa olla verkkosivustolla jopa miljoonia, jolloin käyttäjän tiedot leviävät hallitsemattomasti. Riski siitä, että miljoonien kolmansien osapuolien joukossa on joku, joka ei noudata hyvää tietosuojaa on merkittävä. Käyttäjältä vaaditaan myös erilaisia tietoja ja taitoja ja perehtyneisyyttä tekniikkaan ja teknologiaan, jotta hän voi ymmärtää tietosuojaselosteen evästekohtaa. Tiedot eivät myöskään olleet läpinäkyviä, vaan tietosuojaselosteen evästeitä koskevia lauseita jätettiin avoimiksi, jolloin todellista kokonaiskuvaa oli mahdotonta saada. Tietosuojaselosteen evästetekstien lukeminen oli myös työlästä ja kuormittavaa ja

käyttäjälle annetaan kohtuuttomalta tuntuva vastuu vaikeaselkoisen tekstin ymmärtämisen suhteen.

Tutkimuksen perusteella suositellaan aivan jokaisen verkkosivustojen käyttäjän pohtivan käyttämiään verkkosivustoja ja tutustumaan käyttämiensä sivustojen tietosuojaselosteisiin evästeiden osalta mahdollisine liitteineen, huolimatta siitä, että se saattaa olla työlästä. Silti valistuneen mielipiteen muodostaminen siitä, hyväksyäkö evästeet vai ei, on kaikki dokumentit läpi lukienkin haastavaa. Välttämättömät evästeet ovat edellytyksenä verkkosivuston toiminnalle, mutta ei-välttämättömien evästeiden hyväksymistä on suositeltavaa harkita. Tarvitsisimme verkkosivustojen käyttäjinä ja kuluttajina edes jonkinlaisia apuvälineitä tai tietoja – tai yksiselitteistä yksityisyyden suojaa koskevaa lainsäädäntöä turvaamaan lukuisia päivittäin tekemiämme evästeiden suostumuspäätöksiä. Pelkästään hyvä lainsäädäntö tai kattavat, selkeät ja ymmärrettävät tietosuojaselosteet eivät luo täyttä turvaa eivätkä ne yksistään takaa hyvää yksityisyyttä. Riskinä onkin, että verkkosivustojen tuottaja ei noudata sääntöjä, huolimatta tästä seuraavista sanktioista.

7.1 Tutkimuksen luotettavuus

Tässä pro-gradu työssä toteutettu tutkimus oli laadullinen ja sen luotettavuuden arviointiin voidaan soveltaa tietyin osin reliabiliteetin ja validiteetin käsitteitä. Olennaista laadullisessa tutkimuksessa on arvioida tutkimuksen uskottavuutta ja luotettavuutta. Tämä tutkimus ja sen tulokset ovat yleistettävissä ja ne ovat siirrettävissä.

Laadullisen tutkimuksen tulokset eivät saa olla sattumanvaraisia ja tutkimuksessa käytetyillä menetelmillä on voitava tutkia sitä, mitä tutkimuksessa on tarkoitus tutkia. Tutkimuksessa käytettyjen käsitteiden on sovelluttava tutkimusongelman ja aineiston sisältöihin. (Saaranen-Kauppinen & Puusniekka, 2006c; Saaranen-Kauppinen & Puusniekka, 2006b; Jyväskylän yliopisto, 2021).

Laadullisen tutkimuksen reliabiliteetin arviointiin voi soveltaa kolmea kohtaa, joita ovat erityisen reliaabeliuden arviointi eli missä olosuhteissa jokin metodi on luotettava ja johdonmukainen, ajallinen reliaabelius eli mittausten tai havaintojen pysyvyys eri aikoina ja johdonmukaisuus tuloksissa. Tutkimus on tehty siten, että se olisi mahdollisimman luotettava ja johdonmukainen heti aineiston keräämisestä alkaen, käyden aineistoa systemaattisesti lävitse. Aineisto on sellainen, että tutkijalla ei ole ollut aineiston keräämiseen vaikutusta tai omat mielipiteet eivät ole vaikuttaneet aineiston keräämiseen, vaan se on kerätty verkkosivustojen virallisista paikoista tasapuolisesti samalla metodilla aloittaen tietosuojaselosteen evästekohdan läpikäymisestä ja seuraten siinä mahdollisesti annettuja evästeisiin liittyviä lisälinkkejä. Tutkimus on ajallisesti reliaabeli eli havaintojen keräämisen aika ei ole vaikuttanut tuloksiin. Tulokset ovat johdonmukaisia, sillä aineisto ja tulokset on analysoitu saman tutkijan toimesta samanlaisilla metodeilla. Tämän tutkimuksen aineiston teksteistä on sen analysoinnin aikana pyritty tekemään perusteltuja ja aukikirjoitettuja kategorisointeja ja

koodauksia, mikä lisää luotettavuutta. Tutkimuksen luotettavuuden perusteena on se, että tutkimuksen tekijä ei ole millään tavalla vaikuttanut siihen, minkälaista tutkimusaineistoa on saatu, vaan kaikki aineisto on ollut valmiina julkisesti ja tasapuolisesti saatavilla. Luotettavuuden yhtenä mittarina on se, että tutkitut aineistot ovat mahdollisimman tuoreita, mikä toteutui hyvin tässä tutkimuksessa (Saaranen-Kauppinen & Puusniekka, 2006b).

Validiteetissa kyse on siitä, onko tutkimus pätevä, onko se perusteellisesti tehty ja ovatko saadut tulokset ja tehdyt päätelmät oikeita. Tämä tutkimus on tehty siten, että se olisi mahdollisimman pätevä, perusteellisesti tehty ja saadut tulokset ja tehdyt päätelmät olisivat mahdollisimman paikkaansa pitäviä. Haasteena validiteetille oli aineiston osittainen vaikeaselkoisuus ja jokainen aineiston osa oli uniikki ja omanalaisensa, jolloin samankaltaisuuksien löytäminen oli osin haastavaa. Kaikesta aineistosta ei myöskään löydetty tarkempia tietoja joillekin etsityille asioille, mikä on kuitenkin mainittu avoimesti tulosten kohdalla. Yhden aineiston osan toistuminen oli haaste validiteetille, mutta koska kyseessä oli tutkitusti suomen suosituimpien sivustojen 10 parhaan lista ja aineiston osat olivat molemmat omia verkkosivustojaan, tämä hyväksyttiin aineiston analysoinnissa. Nämä aineiston yksiköt käsiteltiin siis ominaan, mainiten kuitenkin, että ne käyttävät samaa tietosuojaselostetta liitteineen (Saaranen-Kauppinen & Puusniekka, 2006c).

7.2 Jatkotutkimusehdotukset

Jatkotutkimusaiheena tämän tutkimuksen perusteella suositellaan tietosuojaselosteen mallin rakentamista siten, että kaikkien verkkosivustojen tietosuojaselosteet noudattaisivat samaa mallia. Tämä helpottaisi käyttäjää löytämään tiedot ja vertailemaan niitä eri sivustojen kesken. Käyttäjän täytyy pystyä punnitsemaan omien tietojensa antamisen päätöstä tasavertaisin keinoin, joita ei tällä hetkellä ole saatavilla. Toisena ehdotuksena jatkotutkimusaiheesta on lähestyä yrityksiä henkilökohtaisella yhteydenotolla, kysyen tarkempia selvityksiä evästeiden käytöstä siten, että saataisiin mahdollisimman hyvin vertailtavaa ja kattavampaa tietoa eri verkkosivustojen kesken, kuin mitä tietosuojaselosteiden evästekohdissa tai erillisissä evästedokumenteissa on kerrottu.

LÄHTEET

Adobe. (2021). Adobe Flash Player EOL General Information Page. https://www.adobe.com/fi/products/flashplayer/end-of-life.html

Alizai, Z. A., Tahir, H., Murtaza, M. H., Tahir, S., & Mcdonald-Maier, K. (2019). Key-based cookie-less session management framework for application layer security. *IEEE Access*, *7*, 128544-128554.

Arcand, M., Nantel, J., Arles-Dufour, M., & Vincent, A. (2007). The impact of reading a web site's privacy statement on perceived control over privacy and perceived trust. *Online Information Review*.

Cloudflare. Popular Domains Ranking – Year in Review 2021. https://blog.cloudflare.com/popular-domains-year-in-review-2021/

Cookiebot. (2020). Cookie texts and cookie messages in the age of the privacy paradox. https://www.cookiebot.com/en/cookie-texts/

Englehardt, S., Reisman, D., Eubank, C., Zimmerman, P., Mayer, J., Narayanan, A., & Felten, E. W. (2015, May). Cookies that give you away: The surveillance implications of web tracking. In *Proceedings of the 24th International Conference on World Wide Web* (pp. 289-299).

Euroopan unionin neuvosto. (2022). Tietosuoja EU:ssa. https://www.consilium.europa.eu/fi/policies/data-protection-reform/

Finlex. (2014). Laki sähköisen viestinnän palveluista. https://www.finlex.fi/fi/laki/ajantasa/2014/20140917

Finlex. (2018). Tietosuojalaki. https://www.finlex.fi/fi/laki/ajantasa/2018/20181050#L1P1

Garcia-Barrios, V. M., Hemmelmayr, A., & Leitner, H. (2009, September). Personalized systems need adaptable privacy statements! How to make privacy-related legal aspects usable and retraceable. In *2009 Second International Conference on Advances in Human-Oriented and Personalized Mechanisms, Technologies, and Services* (pp. 91-96). IEEE.

Günter, K., Hasanen, K. & Juhila, K. (2022). Johdanto: Analyysi ja tulkinta. Tietoarkisto. https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/analyysitavan-valinta-ja-yleiset-analyysitavat/analyysi-ja-tulkinta/

Günther, K. & Hasanen, K. (2022). Tutkimuksen suunnittelu. Tietoarkisto. https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/laadullisen-tutkimuksen-prosessi/tutkimuksen-suunnittelu/

Hui, K. L., Teo, H. H., & Lee, S. Y. T. (2007). The value of privacy assurance: An exploratory field experiment. *Mis Quarterly*, 19–33.

Innanen, A. & Saarimäki, J. (2012). Internetoikeus. Porvoo 2012: Bookwell. Oy

Jafar, M. J., & Abdullat, A. (2009). Exploratory analysis of the readability of information privacy statement of the primary social networks. *Journal of Business & Economics Research (JBER)*, *7*(12).

Jyväskylän yliopisto. (2021). Koppa – Tutkimuksen toteuttaminen. https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/tutkimusprosessi/tutkimuksen-toteuttaminen#tutkimustulosten-luotettavuus

Järvinen, P. (2002). Tietoturva & yksityisyys. Porvoo 2002: WS Bookwell.

Kretschmer, M., Pennekamp, J., & Wehrle, K. (2021). Cookie banners and privacy policies: Measuring the impact of the GDPR on the web. *ACM Transactions on the Web (TWEB)*, *15*(4), 1-42.

Kristol, D. M. (2001). HTTP Cookies: Standards, privacy, and politics. *ACM Transactions on Internet Technology (TOIT)*, *1*(2), 151–198.

Kulyk, O., Hilt, A., Gerber, N., & Volkamer, M. (2018). this website uses cookies": Users' perceptions and reactions to the cookie disclaimer. In *European Workshop on Usable Security (EuroUSEC)*.

Kurtz, C., Semmann, M., & Schulz, W. (2018). Towards a framework for information privacy in complex service ecosystems.

Leite, L., dos Santos, D. R., & Almeida, F. (2021). The impact of general data protection regulation on software engineering practices. *Information & Computer Security*.

Lexia. (2018). Uusi kansallinen tietosuojalaki tarkentaa henkilötietojen käsittelyyn liittyviä velvoitteita. https://www.lexia.fi/fi/uusi-kansallinen-tietosuojalaki/

Marino, B. (2021). Privacy concerns and the prevalence of third-party tracking cookies on ARL library homepages. *Reference Services Review*.

MTV Uutiset. (2022). MTV Uutiset, aina ajankohtaisimmat aiheet. https://www.mtvuutiset.fi/

Myers, M. D. (2019). Qualitative Research in Business and Management.

Parvaneh, S., Vijayanta, J., Amin, R. & Sepideh, G. (2018). Automated Approach to Improve IoT Privacy Policies.

Poritskiy, N., Oliveira, F., & Almeida, F. (2019). The benefits and challenges of general data protection regulation for the information technology sector. *Digital Policy, Regulation and Governance*.

Saaranen-Kauppinen, A. & Puusniekka, A. (2006a). KvaliMOTV - Menetelmäopetuksen tietovaranto. Tampere: Yhteiskuntatieteellinen tietoarkisto. https://www.fsd.tuni.fi/menetelmaopetus/kvali/L3_3.html

Saaranen-Kauppinen, A. & Puusniekka, A. (2006b). KvaliMOTV - Menetelmäopetuksen tietovaranto. Tampere: Yhteiskuntatieteellinen tietoarkisto. https://www.fsd.tuni.fi/menetelmaopetus/kvali/L3_3_2.html

Saaranen-Kauppinen, A. & Puusniekka, A. (2006c). KvaliMOTV - Menetelmäopetuksen tietovaranto. Tampere: Yhteiskuntatieteellinen tietoarkisto. https://www.fsd.tuni.fi/menetelmaopetus/kvali/L3_3_1.html

Sigmund, T. (2021). Attention Paid to Privacy Policy Statements. *Information (Basel), 12*(4), 144. https://doi.org/10.3390/info12040144

Silius, K. (2018). Teemoittelu ja tyypittely. Tampereen teknillinen yliopisto: hypermedialaboratorio. https://docplayer.fi/9898776-Teemoittelu-ja-tyypittely.html

Sivakorn, S., Polakis, I., & Keromytis, A. D. (2016). The cracked cookie jar: HTTP cookie hijacking and the exposure of private information. In *2016 IEEE Symposium on Security and Privacy (SP)* (pp. 724-742). IEEE.

Traficom. (2022). Evästeet. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/evasteet?toggle=Mit%C3%A4%20ev%C3%A4steet%20ovat%20ja%20mit%C3%A4%20niill%C3%A4%20tehd%C3%A4%C3%A4n%3F&toggle=Ev%C3%A4steiden%20tyyppej%C3%A4

Traficom. (2021). Evästeet ja muut käyttäjien päätelaitteille tallennettavat tiedot sekä näiden tietojen käyttö – Opas palveluntarjoajille. https://www.traficom.fi/sites/default/files/media/file/Ev%C3%A4steohjeistus_palveluntarjoajille.pdf

Velagapudi, S. L., & Gupta, H. (2019, November). Privacy, Security Of Cookies In HTTP Transmission. In *2019 4th International Conference on Information Systems and Computer Networks (ISCON)* (pp. 22-25). IEEE.

Voutilainen, T. (2020). *Digitaalisten palvelujen sääntely*. Alma Talent.

Yle. (2021). Digitreenit: Mitä nettisivujen evästeet oikein tekevät? Onko ne pakko hyväksyä? https://yle.fi/aihe/artikkeli/2020/02/22/digitreenit-mita-nettisivujen-evasteet-oikein-tekevat-onko-ne-pakko-hyvaksya

Yue, C., Xie, M., & Wang, H. (2010). An automatic HTTP cookie management system. *Computer Networks*, *54*(13), 2182–2198.

LIITE 1 AINEISTO

Aineisto

Nro	Nimi	Tietosuojaselosteen sijainti	Päivätty	Lisäsijainnit evästeistä tarkemmin
1	TikTok	https://www.tiktok.com/legal/privacy-policy-eea?lang=fi	5.12.2021	https://www.tiktok.com/legal/tiktok-website-cookies-policy?lang=en
				https://www.tiktok.com/legal/cookie-policy
2	Google	https://policies.google.com/privacy?hl=fi	10.2.2022	https://policies.google.com/technologies/cookies?hl=fi
3	Facebook	https://www.facebook.com/privacy/explanation/	4.1.2022	https://www.facebook.com/policies/cookies/
				https://help.instagram.com/1896641480634707?ref=ig
4	Microsoft	https://privacy.microsoft.com/fi-fi/privacystatement	1.4.2022	Ei
5	Apple	https://www.apple.com/legal/privacy/fi/	27.10.2021	https://www.apple.com/fi/legal/privacy/fi/cookies/
6	Amazon	https://www.amazon.com/gp/help/customer/display.html/?nodeId=468496	12.2.2021	https://www.amazon.com/gp/help/customer/display.html/?nodeId=201890250
7	Netflix	https://help.netflix.com/legal/privacy	1.1.2022	Ei
8	YouTube	osa Googlea, sama tietosuoja-asetus kuin Googlella	10.2.2022	sama kuin Googlella
9	Twitter	https://twitter.com/en/privacy	19.8.2021	https://help.twitter.com/en/rules-and-policies/twitter-cookies
10	WhatsApp	https://www.whatsapp.com/legal/privacy-policy-eea	10.3.2022	https://www.whatsapp.com/legal/cookies