

Santeri Posti

# YKSITYISYYDEN HALLINTA VERKOSSA

## Evästeet ja suostumus

Informaatioteknologian ja viestinnän tiedekunta  
Kandidaattitutkielma  
Kesäkuu 2024

# TIIVISTELMÄ

Santeri Posti: Yksityisyyden hallinta verkossa – Evästeet ja suostumus  
Kandidaattitutkielma  
Tampereen yliopisto  
Tietojenkäsittelytieteiden tutkinto-ohjelma  
Kesäkuu 2024

---

Yksityisyys on käyttäjälle digitalisoituneessa maailmassa ajankohtainen ja tärkeä asia, kun verkkosivustot tallentavat jatkuvasti evästeitä ja muuta dataa käyttäjästä. Useat verkkosivustot harrastavat käyttäjän seuranta heidän liikkuaan verkkosivuilla. Tästä syystä tutkielmassa lähdettiin selvittämään, mitkä tekijät vaikuttavat käyttäjän yksityisyyteen ja sen hallintaan. Käyttäjät kokevat yksityisyyden verkossa tärkeänä asiana, mutta eivät kuitenkaan panosta siihen tarpeeksi.

Tämän tutkielman tavoitteena on selvittää, mitä keinoja käyttäjällä on hallita yksityisyyttään verkossa. Käsittelyssä on käyttäjän asenteet, tiedot verkon yksityisyydestä, sekä käyttäjästä kerättävästä datasta. Lisäksi käsitellään evästeitä sekä niiden hyväksymistä. Tarkastelu on suoritettu pääasiassa käyttäjän näkökulmasta. Tutkielma on toteutettu kirjallisuuskatsauksena ja lähteitä on etsitty useista alan tietokannoista. Lähteitä on vertailtu ja analysoitu, jotta on saatu kokonaiskuva käyttäjien yksityisyyden hallinnasta, sekä asenteista yksityisyyttä kohtaan.

Tutkielmassa pohditaan, miten nykyinen lainsäädäntö on vaikuttanut käyttäjien yksityisyyteen verkossa. Lainsäädännöllä pyritään standardisoimaan käyttäjän oikeuksia verkossa. Tutkielmassa pohditaan lainsäädännön tuomien evästabannerien suunnittelua ja niissä käyttäjälle esiintyviä ongelmia.

Tutkielmassa käy selväksi, että kaikki sivustot eivät kuitenkaan noudata yksityisyyteen liittyvää lainsäädäntöä. Lisäksi verkkosivustot saattavat johtaa käyttäjää harhaan evästabannerien suostuttelevalla tai epäeettisellä suunnittelulla. Käyttäjien välinpitämättömyys verkon yksityisyyttä kohtaan nousee myös tutkielmassa esille. Tutkielma esittää ratkaisuksi näihin ongelmiin huomion kiinnittämistä evästabannerien suunnitteluun, sekä erityisten yksityisyydenhallintatyökalujen implementointia osaksi käyttäjän verkkoselailua. Lisäksi olisi hyvä kiinnittää huomiota käyttäjän asennoitumiseen yksityisyyden hallintaan. Voisi myös olla hyödyllistä miettiä koulutuksen lisäämistä yksityisyyteen ja verkkoselailuun liittyen.

Avainsanat: yksityisyys, evästeet, evästabanneri, käyttäjä, hallinta, suunnittelu

Tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck –ohjelmalla.

# SISÄLLYSLUETTELO

<b>1</b>	<b>Johdanto .....</b>	<b>1</b>
<b>2</b>	<b>Tutkimusmenetelmä ja käsitteitä.....</b>	<b>2</b>
<b>3</b>	<b>Yksityisyydestä digitaalisessa ympäristössä.....</b>	<b>3</b>
3.1	Lainsäädäntö	3
3.2	Evästeiden tyypit ja käyttö	5
3.3	Käyttäjän suhtautuminen yksityisyyteen verkossa	7
3.4	Käyttäjän yksityisyyden uhat	7
<b>4</b>	<b>Yksityisyyden hallinnan keinot .....</b>	<b>8</b>
4.1	Yksityisyystyökalujen suunnittelu	9
4.2	Käyttäjän näkökulma	10
<b>5</b>	<b>Pohdintaa ja yhteenveto.....</b>	<b>11</b>
	<b>Lähdeluettelo.....</b>	<b>13</b>

## 1 Johdanto

Yksityisyyden hallinta on nykyisessä digitaalisessa maailmassa tärkeää, sillä dataa kerätään käyttäjältä jatkuvasti ja paljon. Seuranta verkossa on käyttäjälle yksityisyyden uhka ja pahimmassa tapauksessa jopa turvallisuusriski. Tässä tutkielmassa käsitellään yksityisyyden hallintaa verkossa käyttäjän näkökulmaa painottaen. Tutkielma on toteutettu kirjallisuuskatsauksen muodossa. Aiheesta löytyy jo paljon kirjallisuutta ja tutkimuksia, mistä voi päätellä, että aihe on hyvinkin ajankohtainen.

Tämän tutkielman tavoitteena on selvittää, millaisia keinoja käyttäjällä on digitaalisessa ympäristössä seurata ja nähdä hänestä kerättäviä tietoja, sekä kuinka näitä kerättäviä tietoja voidaan hallita. Tutkimuksessa kartoitetaan tietojen keräämisen tarkoitusta ja pohditaan kerättävän datan käyttötarkoitusta. Tämän lisäksi pohditaan, kuinka käyttäjä voi vaikuttaa hänestä kerättävän datan määrään ja laatuun.

Käyttäjistä muodostuu massiivinen määrä dataa hänen liikkueensa verkossa sivustoilta toisille. Tämän takia käyttäjien tulisi tietää, millaisia oikeuksia heillä on kerättävään dataan. Useat yksityisyysponnahdusikkunat ja evästabannerit antavat käyttäjän vaikuttaa hänestä kerättävään dataan, mutta ponnahdusikkunat on usein suunniteltu epäselviksi, eikä käyttäjä välttämättä saa selkeästi tietää, mihin tarkoitukseen hänestä kerätään dataa ja kenellä on siihen pääsy. Tutkielmassa pohditaan käyttäjän suhtautumista yksityisyyteen, sekä miten käyttäjä itse voi vaikuttaa yksityisyyden toteutumiseen.

Digitaalisessa ympäristössä tietoa muodostuu suuria määriä jatkuvasti, joten käyttäjän oikeuksien ja hallintakeinojen tutkiminen on tärkeää, jotta yksityisyyttä ei loukata. Kuten Gerber ja kumppanit (2018) totesivat, yksityisyys on käyttäjille tärkeää, mutta siihen ei moni käyttäjä kuitenkaan aktiivisesti paneudu. Käyttäjien suhtautumiseen digitaaliseen ympäristöön vaikuttaa hänen kokemansa turvallisuuden ja ymmärryksen tunne, joten myös tästä syystä on hyvä pohtia, kuinka yksityisyyteen voi vaikuttaa omilla toimillaan (Gerber et al., 2018).

Tutkielman toisessa luvussa kerrotaan tutkimusmenetelmästä ja hakusanoista, sekä selvennetään yksityisyydelle ja verkossa liikkumiselle olennaisia käsitteitä. Kolmas luku pyrkii kertomaan yksityisyyteen liittyvistä lainsäädännöllisistä tekijöistä sekä yksityisyydestä yleisesti digitaalisessa ympäristössä. Neljännessä luvussa syvennytään yksityisyyden hallinnan työkalujen suunniteluun sekä yksityisyyden hallinnan keinoihin, joita käyttäjällä on olemassa. Lisäksi neljännessä luvussa käsitellään käyttäjän yksityisyyskäyttäytymiseen liittyviä asioita. Viides luku on yksityisyyteen liittyvää pohdintaa ja tutkielman yhteenvetoa.

## 2 Tutkimusmenetelmä ja käsitteitä

Tutkielman aihe tuli kiinnostuksesta yksityisyyteen, mutta muovautui myöhemmin muotoon yksityisyyden hallinnasta. Ensin etsin vain yksityisyyteen liittyviä artikkeleita yleisellä tasolla, mutta huomattuani hallinnan keinojen olevan käyttäjille tuntemattomia tai vähintäänkin tiedostamattomia, aloin perehtymään aiheeseen tarkemmin.

Tässä tutkielmassa on hyödynnetty useita eri lähteitä monista eri tietokannoista. Tutkielma on tehty kirjallisuuskatsauksena, jonka tarkoituksena oli etsiä mahdollisimman monipuolisesti lähteitä yksityisyydestä sekä evästeistä. Tämän lisäksi tutkin ja vertailin manuaalisesti useita eri sivustojen evästabannereita, joista sain pohjatietoa tutkielmalle. Tietoa ja artikkeleita haettiin pääasiassa ACM Digital Library -tietokannasta, IEEE Electronic Library -tietokannasta, sekä SpringerLink -tietokannasta. Tämän lisäksi tutkielmassa hyödynnettiin joitakin verkkosivuja, kuten Euroopan Unionin virallisia verkkosivuja.

Tutkielman tueksi haettiin artikkeleita erityisesti hakusanoilla ”yksityisyys”, ”evästeet”, ”GDPR”, ”evästabanneri” ja ”yksityisyys verkossa”. Näillä hakusanoilla ja niiden yhdistelmillä ei löytynyt juurikaan suomenkielisiä tuloksia, joten suurin osa artikkeleista on haettu tutkielman tueksi englanninkielisillä hakusanoilla ”privacy”, ”cookies”, ”privacy dashboard”, ”privacy pop-up”, ”design”, ”user privacy”, ”web”, ”cookie banner” ja näistä johdetuilla erinäisillä yhdistelmillä. Artikkeleita löytyi runsaasti, joten päätin rajata löytyneitä artikkeleita julkaisuvuoden perusteella. Näin sain tutkielmaan ajankohtaisinta tietoa aiheeseen liittyen. Seuraavissa kappaleissa kuvataan tälle tutkielmalle olennaisia ja tärkeitä termejä, joita tarvitaan tutkielman pohjaksi.

Evästeillä tarkoitetaan tiedostoja, joita sivustot ja sovellukset tallentavat käyttäjän laitteelle. Nämä evästeet säilyttävät käyttäjän tietoja sivustoilta ja helpottavat sivustojen käyttämistä. Ensimmäisen osapuolen evästeet ovat käytettävän verkkosivun omia evästeitä, joita sivusto kerää käyttäjältä, kun taas kolmannen osapuolen ovat käytettävän sivuston ulkopuolisia evästeitä, joiden avulla muut kuin kyseisen sivuston ylläpitäjät voivat kerätä tietoja sivuston käyttäjistä. (Euroopan unioni, 2023)

Käyttäjän saapuessa ensimmäistä kertaa uudelle sivustolle hänelle aukeaa hyvin usein *evästabanneri* (engl. cookie banner), jossa käyttäjä pääsee säätämään sivuston yksityisyysasetuksia sellaisiksi kuin käyttäjä itse haluaa. Evästabannereiden tarkoitus on vähintäänkin informoida käyttäjälle, että sivustolla tullaan keräämään käyttäjästä dataa. Näitä yksityisyysponnahdusikkunoita on monenlaisia ja niistä puhutaan lisää luvuissa 3 ja 4.

*Privacy dashboard* on erityinen yksityisyyden hallinnan työkalu, jolla käyttäjä pääsee hallitsemaan hänestä kerättyä dataa erilaisten selkeästi suunniteltujen yhteenvetojen avulla. Nämä privacy dashboardit toimivat siis yhdenlaisena yksityisyyden hallinnan keinona käyttäjälle. Privacy dashboard siis auttaa käyttäjää ymmärtämään kerättyä dataa pa-

remmin visualisoimalla sitä selkeämmin, täten luoden läpinäkyvyyttä (engl. transparency) käyttäjistä kerättyyn dataan (Herder ja van Maaren, 2020). Nämä yksityisyyden hallinnan työkalut ovat yleistymässä nopeasti, ja tunnetuimpia tällaisia työkaluja ovat Googlen sekä Microsoftin omat privacy dashboardit. Privacy dashboardille ei ole vakiintunutta suomenkielistä käännettä termiä, joten tässä tutkielmassa käytän englanninkielistä termiä.

### **3 Yksityisyydestä digitaalisessa ympäristössä**

Digitaalisessa ympäristössä yksityisyyden rajojen asettaminen on ongelma, joka koskee jokaista verkkopalveluita tai sovelluksia käyttävää yksilöä. Digitalisoituneessa yhteiskunnassa on vaikea välttää näkemästä erilaisia yksityisyyteen liittyviä kysymyksiä ja datan keräämiseen pyrkiviä evästesuostumuksia. Tämän lisäksi yksityisyyden ongelmat liittyvät myös käyttäjien asenteisiin ja osaamiseen. Acquisti ja kumppanit (2015) artikkelissaan kertovat, kuinka käyttäjien omat epävarmuudet ja tietämättömyys seurauksista aiheuttavat ongelmia liittyen käyttäjien yksityisyyteen verkossa. Aliluvussa 3.1 käsitellään verkkosivustojen yksityisyyteen liittyvää lainsäädäntöä, aliluvussa 3.2 paneudutaan evästeiden tarkoitukseen ja aliluvussa 3.3 pohditaan, miten yksityisyys verkossa näkyy käyttäjälle.

#### **3.1 Lainsäädäntö**

Datan kerääminen ja henkilökohtaisten tietojen liikkuminen on ollut epäselvää tai jopa näkymätöntä käyttäjälle vuoteen 2018 asti. Tällöin Euroopan Unioni toi voimaan EU:n sisällä voimassa olevan tietosuojalain, GDPR:n.

*GDPR* (General Data Protection Regulation) takaa henkilökohtaisten tietojen suojaamisen digitaalisessa ympäristössä, kuten verkkosivuilla liikkuesssa tai verkkokaupoissa ostoksia tehdessä. Nämä säännöt koskevat julkisia ja yksityisiä organisaatioita EU:ssa, mutta myös sen ulkopuolella olevia organisaatioita, jos ne käsittelevät EU-kansalaisten yksityistietoja (Euroopan Unioni, 2023). GDPR:n lisäksi Suomessa on oma tietosuojalaki, jonka tarkoituksena on suojata käyttäjien henkilötietoja. Tämä laki sanoo, että jos rekisterinpitäjän (verkkosivun ylläpitäjä) toimipaikka sijaitsee Suomessa, sovelletaan Suomen tietosuojalakia GDPR:n lisäksi (Tietosuojalaki 1050, 2018).

GDPR:n voimaantulosta on kulunut jo yli 5 vuotta ja sen vaikutukset näkyvät eri verkkosivustoilla käyttäjille. Näkyvimpänä osana on luultavasti evästeiden hallinta käyttäjille. GDPR vaatii, että sivustoilla kysytään suostumusta käyttäjiltä tietojen keräämisestä, sekä informoidaan kerätyn datan käyttötarkoituksista.

Suurena muutoksena GDPR toi myös vaatimuksen, jonka mukaan käyttäjän tulee pystyä pääsemään käsiksi hänestä kerättävään dataan ymmärrettävässä muodossa. Tälle

vaatimukselle eurooppalaisilla sivustoilla oli kuitenkin annettu viiden vuoden aikaraja, jonka aikana organisaatioiden pitää pystyä optimoimaan sivustonsa GDPR:n mukaisiksi.

Pöhn ja kumppanit (2023) tutkivat, kuinka helposti käyttäjä voi päästä käsiksi hänestä kerättävään dataan. He huomasivat, että sivustot toimivat hyvinkin eri tavoilla kyseisissä tapauksissa. Osa sivustoista ei toimittanut dataa ajallaan ja osa ei antanut sitä ymmärrettävässä muodossa. Vaikka ymmärrettävä muoto on tulkinnan varainen termi, ei tietokoneen ymmärrettäväksi tehtyyn muotoon pakattu data ole välttämättä käyttäjäystävällistä.

Kretschmer ja kumppanit (2021) tutkivat, miten sivustojen ylläpitäjät noudattavat GDPR:n tuomia oikeuksia käyttäjille. Artikkelissa todettiin, että vaikka sivustot noudattavat keskimäärin hyvin GDPR:n asetuksia, on sivustoilla kuitenkin paljon parannettavaa. He nostavat esille, että vaikka sivustoilla kysytään suostumusta tiedon keruuseen ja sen käsittelyyn, on evästepbannerien suunnittelu tehty niin, että käyttäjälle on hankalaa päästä käsiksi häneltä kerättävään dataan, sekä on vaikea ottaa yhteys kehenkään datan keräämisestä heränneisiin kyselyihin. Lopputulos on siis samankaltainen kuin Pöhnin ja muiden (2023) tutkimuksessa. Tämän lisäksi käyttäjä pystyy Kretschmerin ja muiden (2021) mukaan kieltäytymään datan keruusta, mutta sen tekeminen on tehty hankalaksi evästepbannerien suunnittelun avulla.

Yksityisyyslakeja siis noudatetaan suurilta osin hyvin, mutta parannettavaa myös on. Lait eivät kuitenkaan ohjaa yksityisyysponnahdusikkunoiden suunnittelua teknisiltä osin lainkaan, vaan niiden toteutus jää sivustojen ylläpitäjien vastuulle. Tästä syystä mustat mallit ja epäselvät toteutustavat ovat yleisiä näissä ponnahdusikkunoissa ja bannereissa (Htut Soe et al., 2020).

Taulukossa 1 on koottuna vuodesta 2023 vuoden 2024 maaliskuuhun asti annettujen GDPR-sakkojen määrä sekä niiden kuukausittainen summa. Taulukosta 1 näkee, että sakkoja on jaettu kymmenittäin joka kuukausi vuodesta 2023 lähtien. Tämä osoittaa, että GDPR:ää ei vielä kukaan noudateta täysin. Taulukko 1 ei kerro, mistä kaikista sakkoja on organisaatioille annettu. Kyseessä voi olla esimerkiksi verkkosivuston käyttäjien datan väärinkäyttö tai käyttäjän datan säilyttäminen määrittelemättömän ajan, kuten tuoreessa Verkkokauppa.comin tapauksessa. Tässä Verkkokauppa.comin tapauksessa kyseinen yritys ei ollut määritellyt, kuinka kauan käyttäjien dataa säilötään. Tämän lisäksi heidän sivustollaan ostosten tekeminen edellytti tunnuksen luomista verkkosivustolle, mikä on tietosuojasäännösten vastaista. (Tietosuojavaltuutetun toimisto, 2024)

Taulukko 1 GDPR Enforcement tracker, GDPR-rikkeistä määrättyt sakot 1/2023-3/2024 (GDPR Enforcement tracker, n.d.)

kuukausi	Sakkojen summa (kuukaudessa)	Sakkojen määrä (kuukaudessa)
1/2023	€ 396,440,240	43
2/2023	€ 2,644,751	35
3/2023	€ 1,464,460	48
4/2023	€ 24,607,831	41
5/2023	€ 1,208,852,640	39
6/2023	€ 50,419,060	61
7/2023	€ 3,222,220	40
8/2023	€ 3,498,480	34
9/2023	€ 356,032,120	41
10/2023	€ 18,350,120	39
11/2023	€ 3,114,920	52
12/2023	€ 10,655,200	32
1/2024	€ 32,615,640	20
2/2024	€ 4,915,500	18
3/2024	€ 1,242,800	7

Kyseisestä Verkkokauppa.comin tapauksesta, sekä sakkojen jatkuvasta jakamisesta voi päätellä, että viranomaiset seuraavat henkilörepositorien ylläpitoa aktiivisesti. Muistakin syistä sakkoja on jaettu, mutta niiden kategorisoiminen olisi liian hankalaa sekä tarpeetonta tämän tutkielman kannalta.

### 3.2 Evästeiden tyypit ja käyttö

Evästeiden käyttöä verkkosivustoilla liikuttaessa ei voi mitenkään välttää. Siksi onkin hyvä tietää, miten eri evästeet toimivat ja mitä käyttäjä voi hyväksyä pelkäämättä seurauksia. Evästeet voi jakaa kahteen eri kategoriaan, ensimmäisen osapuolen evästeet (engl. first-party cookies), sekä kolmannen osapuolen evästeet (engl. third-party cookies). Ensimmäisen osapuolen evästeet ovat verkkosivuston ylläpitäjän evästeitä, kun taas kolmannen osapuolen evästeet ovat verkkosivuston ulkopuolisilta tahoilta. Ensimmäisen osapuolen evästeiden tarkoitus on kerätä käyttäjältä dataa verkkosivuston toiminnan parantamiseksi ja käyttäjän seuraamiseksi sivustolla. Kolmannen osapuolen evästeet taas ovat usein seurantaan ja markkinointiin liittyviä evästeitä.

Kolmannen osapuolen evästeiden käytön suosio on ollut viime vuosina suuressa laskussa, kun yksityisyys verkossa on ollut kasvava puheenaihe verkossa ja sosiaalisessa mediassa. Tästä syystä markkinoijat ja muut sivustolla seuranta harjoittaneet tahot ovat alkaneet käyttää ensimmäisen osapuolen evästeitä käyttäjien toiminnan seurannassa (Munir et al., 2023). Munir kumppaneineen (2023) tutkivat, miten tämä ilmiö näkyy ja toimii verkossa. Heidän tutkimuksensa paljasti, että vaikka kolmannen osapuolen evästeistä on

kieltäytytty, varastoivat ensimmäisen osapuolen evästeet silti erilaisia seurantaan tarkoitettuja tietoja. Tämä on vastoin GDPR:n tavoitteita ja nämä rikkeet pitäisi sivuston ylläpitäjän korjata.

Tällaisten sivustojen käyttäjien ei kuitenkaan välttämättä ole käytännöllistä kieltäytyä myöskään kaikista evästeistä, sillä kaikkien evästeiden estäminen saattaa häiritä tai jopa kokonaan estää verkkosivuston käyttämisen. Tästä varoittavat myös Munir ja muut (2023). Käyttäjän keinot ovatkin tällaisissa tilanteissa vähäiset.

Kuvassa 1 on Sanoman evästabanneri, josta näkee hieman evästabannereiden ulkonäköä. Kyseisessä bannerissa on hyvä huomioida, kuinka se on suunniteltu ”työntämään” käyttäjä hyväksymään evästeet. Tämän voi huomata siitä, että bannerissa on vain vaihtoehto ”OK” ja ”Asetukset”. Kieltäytyminen ja muokkaaminen on piilotettu asetuksien taakse, mikä on hyvin yleistä näissä bannereissa.



Kuva 1 Sanoman evästabanneri (kuvakaappaus otettu 16.3.2024 sivulta [www.hs.fi](http://www.hs.fi))

Kuvan 1 bannerissa on myös annettu kohtalaisen paljon infoa käyttäjälle, mikä on toisaalta hyvä asia, mutta se saattaa myös aiheuttaa käyttäjälle tunteen ylivoimaisesta urakasta kaiken lukemiseen ja näin edistää suostumuksen hyväksymistä ilman pidempää tarkastelua tai pohdintaa. Kuvan 1 bannerista on myös hyvä huomata, kuinka Sanoman kumppanit tallentavat myös dataa käyttäjän laitteelle. Näillä kumppaneilla tarkoitetaan kolmannen osapuolen evästeitä hyödyntäviä tahoja, joiden evästeitä käytetään tässä kyseisessä tapauksessa erilaisiin mittauksiin, markkinointiin ja tuotekehitykseen. Aliluvussa 4.1 tarkastellaan evästabannerien suunnittelua tutkimuslähteiden avulla enemmän.

### 3.3 Käyttäjän suhtautuminen yksityisyyteen verkossa

Käyttäjän suhtautuminen yksityisyyteen ja sivustojen luotettavuuteen vaihtelee yksilöittäin, mutta käyttäjät kokevat yleisesti yksityisyyteen liittyvät asiat tärkeiksi. Kuitenkin vain harvoin käyttäjät yrittävät aktiivisesti suojata heiltä kerättävää dataa ja usein jopa antavat sivustojen kerätä dataa vapaaehtoisesti (Gerber et al., 2018).

Gerber ja kumppanit (2018) pyrkivät tutkimuksessaan selvittämään, mitkä asiat vaikuttavat tähän niin sanottuun yksityisyysparadoksiin ja käyttäjän tietojen suojaamiseen. Lopputuloksena todettiin, että on vaikea määrittää pätevää syytä tälle yksityisyysparadoksille, koska tutkijat usein jakavat paradoksin eri tavoilla syihin ja seurauksiin. On kuitenkin selvää, että yksityisyyden hallinnalla on suuri vaikutus käyttäjän kokemaan luottamukseen käytettävään sivustoon (Herder ja van Maaren, 2020).

Herder ja van Maaren (2020) tutkivat, miten erilaiset hallinnan työkalut vaikuttavat käyttäjien koettuun luottamukseen sivustoja ja niiden ylläpitäjiä kohtaan. Tuloksista saatiin selville, että mitä paremmin käyttäjä tietää ja kokee hallitsevansa hänestä kerättävää dataa, sitä parempi luottamus on myös käytettävään sivustoon ja sitä ylläpitävään tahoon. Kerättävän datan laatu vaikutti Herderin ja van Maarenin (2020) tutkimuksessa myös paljon käyttäjän kokemaan luottamukseen. Profilointi ja luokittelu nähtiin enemmän negatiivisessa valossa kuin normaaliin sivuston prosessointiin vaadittava data.

Kerättävän datan näkyvyys käyttäjälle on usein hyvin heikko evästabannereissa, vaikka GDPR vaatiikin datan ja sen käyttötarkoituksen esittämisen käyttäjälle selkeästi ja ymmärrettävästi. Hume ja kumppanit (2021) mainitsivat artikkelissaan, että tämä heikko näkyvyys vaikuttaa käyttäjän luottamukseen negatiivisesti. Datan huono ja epäselvä esitystapa luo käyttäjälle tunteen epävarmuudesta ja kontrollin menetyksestä henkilökohtaiseen dataan.

Kuten aikaisemmin mainittiin, yksi tietojen keräämiseen ja yksityisyyteen liittyvä uhka on käyttäjien oma asennoituminen ja välinpitämättömyys. Acquisti ja muut (2015) tarjoavat artikkelissaan havaintoja käyttäjien ymmärryksen parantamiseksi. Tämä ei tietenkään ole helppoa, sillä käyttäjien epävarmuus seurauksista yksityisyyteen ja datan keruuseen on yksilöllistä (Acquisti et al., 2015). Tämän vuoksi avoin keskustelu aiheesta on välttämätöntä asenteiden parantamiseksi.

### 3.4 Käyttäjän yksityisyyden uhat

Evästabannerit tulevat nykyään näkyviin lähes joka sivustolla internetissä ja ne antavat käyttäjälle tiedon, että dataa tullaan sivustolla keräämään. Matte ja kumppanit (2020) tutkivat, kuinka hyvin sivustot, joilla on evästabannereita, todellisuudessa noudattavat tiedon keruun suostumuksesta kieltäytymistä. Tutkimuksessa käytiin läpi 1426 sivustoa, joilla tällaiset bannerit olivat käytössä. 141 näistä sivustoista kerättiin käyttäjistä tietoja, vaikka suostumusta tiedon keruuseen ei ollut vielä annettu, kun taas 27 sivustolla suostumus tulkittiin annetuksi, vaikka käyttäjä oli kieltäytynyt evästabannerissa tiedon keruusta.

Tutkimuksessa myös todettiin, että monet evästabannerit on suunniteltu ”työntämään” käyttäjät suostumuksen suuntaan mustilla malleilla ja suunnitteluvalinnoilla. (Matte et al., 2020)

Palveluntarjoajien suunnitteluvalintojen tarkoitus on pääosin yrittää hyödyntää ja hyväksikäyttää käyttäjien tietämättömyyttä ja välinpitämättömyyttä. Acquisti ja muut (2015) haluavat tästä syystä luoda keskustelua ja tuoda esille käyttäjien verkossa harjoittaman välinpitämättömyyden aiheuttamista vaaroista yksityisyydelle.

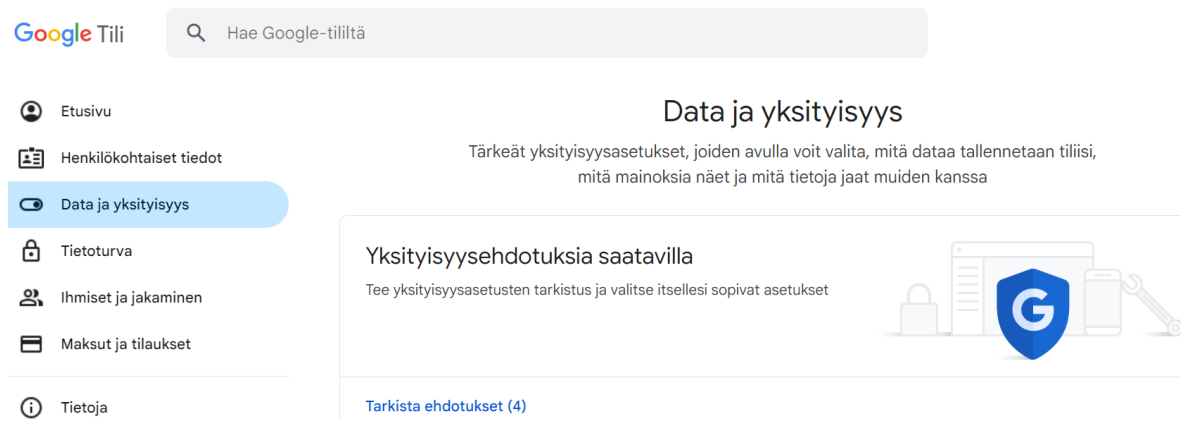
Verkossa käyttäjän yksityisyyttä uhkaavat myös paremmin piilossa olevat käyttäjän seurannan keinot. Niin sanotut näkymättömät pikselit aiheuttavat käyttäjille seurantaan liittyviä ongelmia verkkosivuilla ja jopa sähköposteissa. Näkymättömillä pikseleillä tarkoitetaan tässä tapauksessa 1x1 pikselin kuvaa, joka auttaa kolmannen osapuolen seuraajia keräämään käyttäjästä luvattomasti dataa. Nämä näkymättömät pikselit ovat nimensä mukaisesti verkkosivun käyttäjälle huomaamattomia, joten niitä on hankala torjua. Useat käyttäjät, jotka päivittäin käyttävät verkkosivuja arkisessa toiminnassaan, eivät edes tiedä tästä yksityisyyden loukkauksen ilmiöstä. Tästä syystä näkymättömiä pikseleitä ei hirveästi torjuta eikä niistä puhuta. Näkymättömät pikselit ovat nykyään hyvinkin yleisiä, vaikka kolmannen osapuolen seurannat ovat vähentyneetkin erilaisten torjuntaohjelmien kehittyessä ja yleistyessä. Ruohonen ja Leppänen (2018) ottivat tutkimuksessaan 488 verkkosivustolta kuvanäytteitä tutkittavakseen tarkoituksenaan selvittää, kuinka yleisiä näkymättömät pikselit niissä ovat. Lopputuloksena oli, että yli 30 % sivustoista oli jonkinlainen näkymätön kuva tai pikseli, minkä tarkoituksena oli luultavasti nimenomaan käyttäjän seuranta.

#### **4 Yksityisyyden hallinnan keinot**

Yksityisyystyökaluja on monenlaisia, mutta niistä yleisimmät ovat sivustojen omat evästabannerit ja yksityisyysponnahdusikkunat, sekä yleistymässä olevat privacy dashboardit. Näille suunnitteluun ei ole olemassa mitään universaaleja sääntöjä, mutta erilaisia ohjeita ja suunnitteluapuvälineitä löytyy verkosta useita. Tämän lisäksi verkkosivustojen evästabannerit saatetaan tietoisesti suunnitella käyttäjille hankaliksi, datan keruun suostumuksen saamiseksi (Htut Soe et al., 2020). Aliluvussa 4.1 keskitytään suunnittelun eri metodeihin pintapuolisesti ja pohditaan niiden hyviä ja huonoja puolia. Tämän lisäksi syvenytään evästabannerien kyseenalaiseen suunnittelupolitiikkaan. Aliluvussa 4.2 keskitytään käyttäjän näkökulmaan verkossa liikkumiseen, sekä heidän asenteidensa, että kokemustensa kautta. Nämä asenteet vaikuttavat merkittävästi yksityisyyden hallintaan käyttäjäkohtaisella tasolla.

## 4.1 Yksityisyystyökalujen suunnittelu

Raschke ja kumppanit (2018) pohtivat, mitä ongelmia ja ratkaisuja löytyy privacy dashboardeja suunnitellessa. Artikkelissa huomautetaan, että suurena ongelmana tulee alussa heti vastaan privacy dashboardin implementoinnin laajuus. Jos tavoitteena on suunnitella koko Euroopan Unionin kattava privacy dashboard, on työkalun oltava ymmärrettävä ja saavutettava monilla eri alueilla. Tämä kyseisessä työkalussa esitettävä data on saatava muotoon, joka on helposti ymmärrettävä ja muokattavissa oleva. Kuvassa 2 näkyy Googlen versio heidän privacy dashboardistaan. Kyseisellä työkalulla käyttäjä pystyy hallitsemaan hänestä verkossa kerättävää dataa, pääasiassa kuitenkin vain Googlen omissa palveluissa ja käyttäjän Google-tiliin liittyviin yksityisyysasioihin.



Kuva 2 Googlen privacy dashboard (kuvakaappaus otettu kirjoittajan Google-tililtä 13.4.2024)

Googlen työkalu on kuitenkin yritetty suunnitella suhteellisen helppokäyttöiseksi ja selkeäksi käyttäjälle. Kuten kuvasta 2 näkyy, työkalu myös suosittelee käyttäjälle joitakin yksityisyysasetuksia, jotka parantavat käyttäjän yksityisyyttä.

Raschke ja muut (2018) ehdottavat, että selkeimmän työkalun saamiseksi käyttäjältä kerättävä data tulisi kategorisoida, jotta sen visualisoiminen käyttäjälle olisi mahdollisimman helppoa. Raschke ja kumppanit käyttivät privacy dashboardin suunnittelussa hyödykseen asiantuntija-arviointia, ja lopuksi käyttäjätestausta. Näillä metodeilla heidän mielestään saadaan hyviä tuloksia yksityisyydenhallinnan työkaluja suunniteltaessa.

Osallistava tapa yksityisyydenhallinnan työkaluja suunniteltaessa tuottaa myös hyviä lopputuloksia. Humen ja kumppaneiden (2021) mukaan osallistava tapa tuo käyttäjille enemmän kontrollia työkaluja suunniteltaessa sekä myös itse lopputuotetta käytettäessä.

Mejtoft ja muut (2023) huomasivat artikkelissaan, että evästabannerin koolla ja ulkoasulla on suuri merkitys siihen, miten käyttäjä reagoi ja pitää huolen yksityisyydestään käytettävällä sivustolla. Käyttäjän luottamuksella ja mielipiteellä yrityksestä taas ei ole niin suurta vaikutusta. Evästabannerit, jotka ponnahtavat koko ruudulle, pistivät käyttäjät

enemmän miettimään valintojaan yksityisyyttä kohtaan, kun sivuston alareunaan ilmestyvät pienet bannerit (Mejtoft et al., 2023). Tästä voidaankin päätellä, että hyvin suunniteltu yksityisyysponnahdusikkuna tai evästabanneri voi vaikuttaa positiivisesti käyttäjän kokemaan yksityisyyteen ja ne pistävät käyttäjän jopa pohtimaan omaa yksityisyyttään verkossa. Tämä on suotavaa ja myös toivottavaa käyttäjien näkökulmasta.

Evästabannerit ovat tärkeitä työkaluja yksityisyyden hallinnalle ja tästä syystä myös niiden suunnitteluun pitäisi kiinnittää enemmän huomiota. Htut Soen ja hänen kumppaniensa (2020) tutkimuksessa käytiin läpi, miten käyttäjiä pyritään johtamaan harhaan ja saamaan suostumus datan keruuseen kiertämällä GDPR:n lainsäädäntöä evästabannerien suunnitteluvalinnoilla. Mustat mallit ovat näistä suunnitteluvalinnoista yleisimmät. Evästabannereissa mustien mallien tarkoitus on tuoda käyttäjälle hyvin näkyville datan keräämisen suostumuksen hyväksyminen, kun taas kieltäytyminen on yleensä joko huonosti näkyvillä tai piilotettu kokonaan. Htut Soen ja kumppanien (2020) tutkimuksessa todettiin, että heidän tutkimillaan 300 verkkosivustolla, joissa oli evästabannerit, kaikilla evästabannereilla hyödynnettiin jotakin mustien mallien keinoa. Tällaista suunnittelua kutsutaan suostuttelevaksi suunnitteluksi (engl. persuasive design) ja sen tarkoituksena on nimensä mukaisesti suostutella tai ”työntää” käyttäjää haluttuun suuntaan.

Vaikka suostutteleva suunnittelu ei ole kovinkaan käyttäjäystävällistä, se on todella yleistä varsinkin verkkosivujen evästabannereissa. Datan keruun suostumuksen piilottaminen tai vaikeasti nähtäväksi tekeminen ei varsinaisesti riko lakeja, mutta se on hyvin lähellä laittomuutta ja varsinkin eettiseltä kannalta huolestuttavaa (Mejtoft et al., 2023).

Suostumuksen kysyminen datan keräämiseksi käyttäjältä on GDPR:n myötä tullut pakolliseksi, kuten aikaisemmin on mainittu. Tästä syystä evästabannereita suunniteltiin sivustoille nopeasti GDPR:n voimaantulon jälkeen. Evästabannerien suunnittelu on kuitenkin organisaatioille ja sivustojen ylläpitäjille taas yksi lisäkulu, joten pohdittaessa evästabannerien suunnittelua tästä näkökulmasta on helppo huomata, miksi ne ovat yleisesti ottaen huonoja ja epäselviä.

## **4.2 Käyttäjän näkökulma**

Käyttäjän näkökulmasta nykyisten verkkosivustojen evästabannerit ovat epäselviä hyvästä suunnitteluyrityksistä huolimatta. Tämä johtuu osittain siitä, että on vaikea saada visualisoitua suuria määriä tietoa ja kerätyn datan tarkoituksia käyttäjälle ymmärrettävästi, kuten kuvasta 1 voi päätellä. Kuvassa 1 on käytetty vain tekstiä tiedon esittämiseen käyttäjälle, joten koko evästabanneri jää epäselväksi ja raskaslukaiseksi. Toinen syy harhaanjohtavaan suunnitteluun on se, että verkkosivustot haluavat kerätä käyttäjiltä dataa, jopa harhaanjohtavia menetelmiä hyväksikäyttämällä (Mejtoft et al., 2023). Käyttäjältä kerättyä dataa käytetään muun muassa käyttäjän seuraamiseen, sivuston toiminnan parantamiseen, käyttäjän tietojen tallentamiseen sivuston toiminnan nopeuttamiseksi sekä

verkkosivustojen personoimiseksi. Lisäksi dataa saatetaan välittää muille yhteistyökumppaneille, joita on yleensä sivustoilla suuri määrä.

Mejtoft ja kumppanit (2023) saivat tutkimuksessaan selville, että osaa käyttäjistä ärsyttää evästabannerien pakotettu valitseminen. Jotkut käyttäjät siis mieluiten jättäisivät hyväksymisen tai kieltäytymisen evästeistä kokonaan välistä, jos se on mahdollista. Joillakin verkkosivuilla tällainen huomiotta jättäminen on mahdollista, jolloin oletuksena tutkimuksen mukaan on vain pakollisten evästeiden käyttöönotto sivulla. Tällaista vaihtoehtoa toivottiin erityisesti silloin, jos verkkosivulla on tarkoitus käydä vain kerran. Mejtoftin ja muiden (2023) tutkimuksessa todettiin, että tämä voisi johtua siitä, että käyttäjien kognitio kuormittuu muutenkin paljon verkkosivuston informaatiosta, joten tämä yhden valinnan vähentäminen helpottaisi kuormaa edes vähän.

Evästeiden hyväksyminen ilman pidempää miettimistä tai pohdintaa on hyvin yleistä, sillä käytännössä joka sivustolla käyttäjän eteen ponnahtaa jonkinlainen evästabanneri. Jha ja kumppanit (2022) kirjoittivat artikkelissaan, että kaikkien sivuston evästeiden hyväksyminen saattaa aiheuttaa sivuston hidastumista ja jopa toimimattomuutta. Jha ja muut (2022) vertasivat, miten verkkosivustot käyttäytyvät ja toimivat, riippuen siitä, hyväksytäänkö evästeet vai kieltäydytäänkö niistä. Lopputuloksena oli, että hyväksyttäessä evästeet ne hidastavat sivuston toimintaa. Evästeistä kieltäytyminen saattoi artikkelin mukaan myös aiheuttaa verkkosivuston toimimattomuutta, sillä sen toimimiseen tarvittavaa dataa käyttäjältä ei saatu. Käyttäjän näkökulmasta tämä onkin huolestuttavaa, sillä evästeiden hyväksyminen ja hylkääminen molemmat saattavat aiheuttaa erilaisia ongelmia verkkosivustolla.

## **5 Pohdintaa ja yhteenveto**

Niin yritykset kuin yksityishenkilötkin hyötyvät hyvin toteutetuista evästeistä sekä avoimuudesta datan keruussa käyttäjiltä. Käyttäjät hyötyvät koetun luottamuksen kautta, kun taas yritykset ja organisaatiot saavat todennäköisesti lisää kävijöitä nousseen luottamuksen ja positiivisen kokemuksen kautta.

Käyttäjiltä kerätty data on tarpeellista ja usein myös välttämätöntä verkkosivujen toiminnallisuuden varmistamisessa käyttäjille. Käyttäjiltä kerätty data voi auttaa nopeuttamaan verkkosivuilla asiointia tai jopa räätälöidä paremman, personoidumman kokemuksen käyttäjälle. Toisaalta taas potentiaali ja vaara yksityisen datan väärinkäytölle on myös hyvin suuri (Acquisti et al., 2015).

Evästeistä kieltäytyminen kokonaan ei kaikilla verkkosivuilla ole paras ratkaisu edellä mainitusta verkkosivun toiminnallisuudesta johtuen. Munirin ja kumppaneiden (2023) artikkelissa ehdotetaan tekoälyyn perustuvaa ohjelmistoa ratkaisuksi. Tällainen ohjelma seuloisi käyttäjästä kerättävää dataa ja torjuisi sieltä käyttäjän seuraamiseen liit-

tyvää dataa. Ohjelma voisi olla hyvin implementoituna toimiva ratkaisu seurannan torjumiseksi niin, että sivusto kuitenkin toimisi ja muut ensimmäisen osapuolen evästeet olisivat käytössä. Näin varmistetaan yksityisyydestä ja pystytään silti käyttämään sivustoja evästeiden tuomien etujen kanssa.

Väärinkäyttöä ja GDPR:n noudattamista käsiteltiin useassa tähän tutkielmaan valitussa artikkelissa. Sekä Kretchmerin ja kumppaneiden (2021), että Pöhnin ja muiden (2023) artikkeleissa tultiin lopputulokseen, että organisaatiot noudattavat verkkosivullaan GDPR:ää hyvin, mutta parannettavaa löytyy. On huomioitava, että näiden kahden artikkelin kirjoittamisen välillä on kulunut noin kaksi vuotta ja GDPR:n voimaan tulemisesta yli viisi vuotta, mutta ongelmia verkkosivustoilla yksityisyyden noudattamisessa on edelleen. Aliluvussa 3.1 olevassa taulukossa 1 huomattiin, että sakkoja on jaettu kuukausittain, eikä loppua ole näkynyt maaliskuuhun 2024 mennessä. Tästä kaikesta voi vetää johtopäätöksen, että käyttäjien yksityisyyteen ja heistä kerättävään dataan liittyvät ongelmat ovat vaikeita ja niihin ei ole löytynyt lopullista ratkaisua useista pyrkimyksistä huolimatta.

Tutkielmassa on käynyt selväksi, että yksityisyyteen verkossa vaikuttaa merkittävästi käyttäjäkohtainen asennoituminen sekä käyttäjän ennakkotiedot evästeistä ja yksityisyydestä (Mejtoft et al., 2023). Vaikuttaakin siltä, että käyttäjien mielenkiinto yksityisyyasetuksiin kohtaan laskee, mitä enemmän evästebannereita ja muita ponnahdusikkunoita käyttäjän eteen hyppää verkossa liikkuesssa. Tämän lisäksi yksityisyyden hallintaan vaikuttaa myös käytössä olevat työkalut, kuten privacy dashboardit ja evästebannerit. Kuten aikaisemmin luvussa 4 todettiin, on tärkeää suunnitella evästebannerit verkkosivustoilla niin, että ne ovat mahdollisimman selkeitä käyttäjälle. Selkeys ja bannerin suuruus luovat käyttäjille lisää intoa syventyä yksityisyyteen verkossa (Mejtoft et al., 2023).

Tutkielman tekemisen aikana on siis käynyt ilmi, että käyttäjällä on useita keinoja hallita yksityisyyttään, mutta osa näistä keinoista tulee ulkopuolisilta organisaatioilta, jolloin yksityisyydenhallintatyökalujen suunnittelulla on tärkeä rooli. Suurimmaksi esteeksi käyttäjän yksityisyydelle voi kuitenkin sanoa käyttäjää itseään.

Internettiä käyttävät kaikenikäiset nykyisessä digitalisoituneessa maailmassa, tämän takia myös lapset ja nuoret tarvitsisivat enemmän tietoa aiheeseen liittyen. Koulutusta voisi lisätä jo aikaisessa vaiheessa, sillä suuri osa väestöstä kuitenkin joutuu käyttämään verkkosivuja ja olemaan tämän kautta tekemisissä evästebannereiden ja yksityisyyden kanssa. Tämä voisi ehkäistä myös käyttäjistä kerätyn datan väärinkäyttöä, kun sitä tunnistetaan paremmin. Lisätty koulutus yksityisyyteen ja verkon käytäntöihin liittyen voisi myös auttaa suunnittelemaan paremmin yksityisyydenhallinnan työkaluja ja evästebannereita. Kaikki lisähuomio verkon yksityisyyteen liittyen on kuitenkin vain hyvä asia.

Tässä tutkielmassa huomataan, että käyttäjät ovat usein kiinnostuneita suojaamaan yksityisyyttään verkossa, mutta he eivät välttämättä jaksa nähdä vaivaa sen eteen. Näin

todettiin myös Gerberin ja kumppaneiden (2018) artikkelissa. Samanlaista pohdintaa löytyi myös Mejttoftin ja kumppaneiden (2023) tutkimuksessa. Tähän motivaation puutteseen yksityisyyden suojaamiseksi verkossa voisi auttaa paremmin suunnitellut evästebannerit, joissa käyttäjiä ei välttämättä ohjattaisi tiettyyn suuntaan suostuttelevalla suunnittelulla. Myös tässä tutkielmassa mainitut privacy dashboardit voivat olla hyvä keino suojautua ei-toivotulta seurannalta verkossa. Käyttäjät voisivat myös hyötyä koulutuksesta yksityisyyden tärkeydestä verkossa, vaikka tämä onkin laajemmin hankalasti toteutettavissa, ellei käyttäjä itse ole aktiivinen asian suhteen.

Tutkielmassa käsiteltiin yksityisyyttä käyttäjän näkökulmasta ottaen huomioon käyttäjien asenteet ja verkkosivujen evästebannerien suunnittelun. Evästeet tulevat käyttäjille eteen jatkuvasti, joten tutkielmassa annetaan käyttäjille ohjeita ja tietoa yksityisyyden edistämiseen eri tavoilla. Yksityisyyden hallinnan työkalut auttavat tässä, joten niiden implementointi olisi käyttäjille suotavaa. Käyttäjien asenteet kuitenkin vaikuttavat paljon heidän yksityisyyksivalintoihinsa, joten tietoisuuden lisääminen aiheen tärkeydestä on kannattavaa. Tutkielmassa ei löydetty suoraa vastausta yksityisyyden lainsäädännön laiminlyömisestä aiheuttamaan yksityisyysongelmaan käyttäjille, vaan se vaatisi jatkotutkimusta laiminlyöntien syystä. Yksityisyyden hallinnan keinoja käyttäjällä kuitenkin riittää, kunhan asennoituminen yksityisyyteen on kunnossa.

## Lähdeluettelo

- Acquisti, A., Brandimarte, L., Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science* 347, 509–514.  
<https://doi.org/10.1126/science.aaa1465>
- GDPR Enforcement tracker, (n.d.). CMS.Law. Viitattu 13.4.2024.  
<https://www.enforcementtracker.com/?insights>
- Euroopan Unioni, (n.d.). Evästeiden käyttö. Viitattu 12.2.2024.  
[https://commission.europa.eu/cookies-policy\\_fi](https://commission.europa.eu/cookies-policy_fi)
- Euroopan Unioni, (2023). Tietosuoja ja yksityisyys verkossa. Viitattu 12.2.2024.  
[https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index\\_fi.htm](https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_fi.htm)
- Gerber, N., Gerber, P., Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, 77, 226–261. <https://doi.org/10.1016/j.cose.2018.04.002>
- Herder, E., van Maaren, O. (2020). Privacy Dashboards: The impact of the type of personal data and user control on trust and perceived risk. *Adjunct Proceedings of the*

- 28th ACM Conference on User Modeling, Adaptation and Personalization (UMAP '20 Adjunct), 6 pages. <https://doi.org/10.1145/3386392.3399557>
- Htut Soe, T., Nordberg, O. Guribye, F., Slavkovik, M., (2020). Circumvention by design - dark patterns in cookie consent for online news outlets. *In Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society (NordiCHI '20)*. Article 19, 1–12. <https://doi.org/10.1145/3419249.3420132>
- Hume, A., Ferreira, N., Cernuzzi, L. (2021). The design of a privacy dashboard for an academic environment based on participatory design. *2021 XLVII Latin American - 14- Computing Conference (CLEI)*. <https://doi.org/10.1109/CLEI53233.2021.9640155>
- Jha, N., Trevisan, M., Vassio, L., Mellia, M. (2022). The internet with privacy policies: Measuring the web upon consent. *ACM Trans. Web* 16, 3, Article 15 (August 2022), 24 pages. <https://doi.org/10.1145/3555352>
- Kretschmer, M., Pennekamp, J., Wehrle, K. (2021). Cookie banners and privacy policies: Measuring the impact of the GDPR on the web. *ACM Trans. Web* 15, 4, Article 20 (July 2021), 42 pages. <https://doi.org/10.1145/3466722>
- Matte, C., Bielova, N., Santos, C. (2020). Do cookie banners respect my choice? : Measuring legal compliance of banners from IAB Europe's transparency and consent framework. *2020 IEEE Symposium on Security and Privacy (SP)*, pp. 791-809. <https://doi.org/10.1109/SP40000.2020.00076>.
- Mejtoft, T., Vejbrinck Starbrink, N., Roos Morales, C., Norberg, O., Andersson, M., Söderström, U. (2023). Cookies and trust: Trust in organizations and the design of cookie consent prompts. *In Proceedings of the European Conference on Cognitive Ergonomics 2023 (ECCE '23)*, Article 18, 1–6. <https://doi.org/10.1145/3605655.3605668>
- Munir, S., Siby, S., Iqbal, U., Englehardt, S., Shafiq, Z., Troncoso, C. (2023). CookieGraph: Understanding and detecting first-party tracking cookies. *In Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS '23)*, 3490–3504. <https://doi.org/10.1145/3576915.3616586>
- Pöhn, D., Mörsdorf, M., Hommel, W. (2023). Needle in the Haystack: Analyzing the right of access according to GDPR article 15 five years after the implementation. *In Proceedings of the 18th International Conference on Availability, Reliability and Security (ARES '23)*, Article 91, 1–10. <https://doi.org/10.1145/3600160.3605064>
- Raschke, P., Küpper, A., Drozd, O., Kirrane, S. (2018). Designing a GDPR-compliant and usable privacy dashboard. In: Hansen, M., Kosta, E., Nai-Fovino, I., Fischer-

Hübner, S. (eds) Privacy and Identity Management. The Smart Revolution. Privacy and Identity 2017. IFIP Advances in Information and Communication Technology, vol 526. Springer, Cham. [https://doi.org/10.1007/978-3-319-92925-5\\_14](https://doi.org/10.1007/978-3-319-92925-5_14)

Ruohonen, J., Leppänen, V. (2018). Invisible pixels are dead, long live invisible pixels! *In Proceedings of the 2018 Workshop on Privacy in the Electronic Society (WPES'18)*, 28–32. <https://doi.org/10.1145/3267323.3268950>

Tietosuojalaki 5.12.2018/1050. Viitattu 12.2.2024.

<https://www.finlex.fi/fi/laki/ajantasa/2018/20181050>

Tietosuojavaltuutetun toimisto. (2024). Verkkokauppa.comille seuraamusmaksu asiakastietojen säilytysajan määrittelemättä jättämisestä – myös vaatimus asiakkaan rekisteröitymisestä oli lainvastainen. Viitattu 11.6.2024.

<https://tietosuoja.fi/-/verkkokauppa.comille-seuraamusmaksu-asiakastietojen-sailytysajan-maaritlematta-jattamisesta-myos-vaatimus-asiakkaan-rekisteroitymisesta-oli-lainvastainen>