Minna Jormalainen

# PIMEÄT KÄYTÄNNÖT SUOMALAISTEN VERKKOSIVUSTOJEN EVÄSTEKYSELYISSÄ

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

# TIIVISTELMÄ

Jormalainen, Minna
Pimeät käytännöt suomalaisten verkkosivustojen evästekyselyissä
Jyväskylä: Jyväskylän yliopisto, 2024, 60 s.
Tietojärjestelmätiede, pro gradu -tutkielma
Ohjaaja: Riekkinen, Janne

Tutkimuksen tarkoituksena oli selvittää, millaisia pimeitä käytäntöjä suomalaisten verkkosivustojen evästekyselyissä esiintyy. Pimeille käytännöille (eng. dark patterns) ei ole olemassa yhtä tiettyä määritelmää, mutta yleensä ne ovat keinoja, joilla palveluntarjoajat yrittävät saada käyttäjät tekemään itselleen epäedullisia valintoja. Evästekyselyissä pimeillä käytännöillä yritetään saada käyttäjä hyväksymään mahdollisimman paljon evästeitä ja luovuttamaan näin tietoja palvelun tarjoajalle. Vastaavanlaista Suomessa tehtyä tutkimusta, joka keskittyy evästekyselyissä esiintyviin pimeisiin käytäntöihin, ei löytynyt, mutta asiaa on tutkittu aiemmin muissa Euroopan maissa.

Tutkimus toteutettiin perehtymällä ensin aikaisempaan tutkimukseen pimeistä käytännöistä ja evästekyselyistä. Aikaisemman tutkimuksen perusteella laadittiin luokittelu evästekyselyissä mahdollisesti esiintyvistä pimeistä käytännöistä. Aineistona käytettiin sataa suomalaista verkkosivusto-osoitetta, joiden evästekyselyitä tarkasteltiin visuaalisesti. Aineisto analysoitiin käyttämällä aikaisemman tutkimuksen pohjalta luotua taulukkoa.

Tutkimus osoitti, että pimeitä käytäntöjä käytetään yleisesti suomalaisissa evästekyselyissä. 76 evästekyselyssä esiintyi ainakin yksi luokituksen mukainen pimeä käytäntö. Selvästi yleisin pimeä käytäntö oli keino, jossa vaihtoehdot esitettiin eriarvoisesti (73), esimerkiksi hyväksy-vaihtoehto esitetiin visuaalisesti korostetummin, kuin hylkää-vaihtoehto. Seuraavaksi eniten (44) löytyi valintojen kaskadiksi nimettyä pimeää käytäntöä. Käyttäjä ei pysty hylkäämään evästeitä yhdellä klikkauksella, vaan toiminto on piilotettu valikoiden taakse. Melkein yhtä paljon (32) esiintyi epäselvästi merkattuja liukusäätimiä. Tutkimuksen tulokset ovat samansuuntaisia kuin aikaisemmin Euroopassa tehdyissä tutkimuksissa.

Tutkimuksen perusteella voidaan päätellä, että suomalaiset evästekyselyt eivät ole millään tavalla poikkeuksellisia mitä tulee pimeiden käytäntöjen soveltamiseen. Niiden yleisyyden vuoksi käyttäjien olisi hyvä olla tietoisempia niiden olemassaolosta ja mahdollisesta vaikutuksesta valintoihin.

Asiasanat: pimeä käytäntö, eväste, evästekysely, yleinen tietosuoja-asetus, valintamuotoilu

# ABSTRACT

Jormalainen, Minna
Dark Patterns in Finnish Websites' Cookie Consent Notices
Jyväskylä: University of Jyväskylä, 2024, 60 pp.
Information Systems, Master's Thesis
Supervisor: Riekkinen, Janne

The purpose of the study was to find out what kind of dark patterns exist in cookie notices on Finnish websites. There is no single definition of dark pattern, but they are usually ways in which service providers try to get users to make choices that are unfavourable to them. Dark patterns are used in cookie banners to get the user to accept as many cookies as possible and thus disclose information to the service provider. Dark patterns in cookie banners have previously been studied in other European countries, but not in Finland.

The study was conducted by first examining previous research on dark patterns and cookie consents. Based on the previous research, a classification of potentially occurring dark patterns in cookie consents was created. One hundred Finnish website addresses were used as the material, and their cookie banners were visually examined. The material was analyzed using a table created based on previous research.

The study showed that dark patterns are commonly used in Finnish cookie banners. There was at least one classified dark pattern in 76 cookie banners. The most common dark pattern was the way in which the options were presented unequally (73) to the user, for example the accept -option was presented more visually appealing than the reject -option. The next highest number (44) was the dark pattern called cascade of choices. The reject cookies -function is hidden behind the menus. There were almost as many (32) occurrences as unmarked sliders. The results of the study are similar to previous studies conducted in Europe.

Based on the research, it can be concluded that Finnish cookie consents are not exceptional when it comes to applying dark patterns. Due to their prevalence, users should be more aware of their existence and their potential impact on choices.

Keywords: dark pattern, cookie, cookie banner, cookie notice, GDPR, nudge,

# KUVAT



# TAULUKOT

# SISÄLLYS

# 1 JOHDANTO

EU:n yleinen tietosuoja-asetus (GDPR) tuli voimaan toukokuussa 2018 (Asetus 2016/679, 2016). Sen mukaan palvelun tarjoajilla pitää olla laillinen peruste käyttäjien tietojen keräämiseksi. Tietosuoja-asetus koskee myös evästeitä ja se on yksi syistä miksi törmäämme evästekyselyihin. Palveluiden tarjoajien pitää informoida käyttäjää mihin tarkoitukseen evästeitä käytetään ja niiden tulee myös tarjota käyttäjälle mahdollisuus kieltäytyä tai hyväksyä tietty käyttötarkoitus (Bollinger ym., 2022). Myös palveluntarjoajien, jotka eivät toimi EU:n alueella tulee noudattaa asetusta, jos ne tarjoavat palveluitaan kohdennetusti EU:n kansalaisille (Krisam ym., 2021).

Mitä evästeet sitten oikeastaan ovat ja miksi niiden vaikutuksesta yksityisyyteen pitäisi olla kiinnostunut? Evästeiden avulla sivusto pystyy tarjoamaan henkilökohtaisemman kokemuksen, seuraamaan käyttäjää sekä tallentamaan ja käsittelemään tämän tietoja (F-Secure, ei pvm.; Kaspersky, ei pvm.). Koska evästeiden avulla on mahdollista tallentaa ja käsitellä käyttäjän tietoja sekä seurata käyttäjää, niiden avulla on mahdollista kerätä käyttäjästä paljon tietoja.

Evästekyselyt tai evästebannerit (eng. cookie banners) taas ovat teknisesti toteutettuja kyselyitä, joiden avulla käyttäjä pystyy hallitsemaan yksityisyysasetuksia, jotka liittyvät evästeiden käyttöön sivustolla (Kampanos & Shahandashti, 2021). Evästekyselyille ei tiettävästi ole mitään standardia, joten jokainen internet sivusto on vapaa käyttämään haluamaansa kyselyä (Kampanos & Shahandashti, 2021). Alla olevassa kuvassa on esimerkki evästekyselystä (Kuva 1.) Evästekyselyssä voi olla mahdollisuus kieltää erikseen esimerkiksi markkinointi- tai tilastolliset evästeet. Käyttäjällä ei kuitenkaan ole mahdollisuutta kieltää välttämättömiä evästeitä, koska niitä tarvitaan sivuston toiminnan takaamiseksi. Jos sivusto asettaa vain välttämättömiä evästeitä, suostumusta ei tarvita (Kyberturvallisuuskeskus, 2023), eli tällöin sivuston ei tarvitse esittää evästekyselyä.


Kuva 1. Esimerkki evästekyselystä

Koska evästeet mahdollistavat kattavan tietojen keruun käyttäjästä, palvelun tarjoajilla on kannustin houkutella käyttäjä hyväksymään mahdollisimman paljon evästeitä. Tähän yhtenä keinona ovat pimeät käytännöt (eng. dark patterns), joita palveluntarjoajat ja evästekyselyiden suunnittelijat hyödyntävät saadakseen käyttäjät hyväksymään evästeet (Martini & Drews, 2022; Soe ym., 2020; Bailey ym., 2019). Käyttäjälle evästeet voivat olla tarpeettomia tai tietoturvan kannalta jopa haitallisia (Bailey ym., 2019).

Pimeille käytännöille ei ole yhtä tiettyä määritelmää. Eräs yleisesti käytetty lähtökohta on kuitenkin, että ne käyttävät hyväkseen ihmisen psykologisia heikkouksia ja niiden tarkoituksena on palvelun tarjoajan etujen ajaminen, ei käyttäjän (Gray ym., 2018; Krisam ym., 2021; Martini & Drews, 2022). Yllä olevassa esimerkki evästekyselyssä (Kuva 1.) yksi tällainen pimeä käytäntö on ”Salli kaikki” -painikkeen vihreä väritys (Martini & Drews, 2022; Mathur ym., 2021). Sen avulla houkutellaan käyttäjää hyväksymään kaikki evästeet. Toinen pimeä käytäntö on valmiiksi valitut valintaruudut (European Commission. Directorate General for Justice and Consumers, 2022; Maier & Harr, 2020; Mathur ym., 2021). Pimeät käytännöt myös vaikuttavat ihmisten tekemiin valintoihin, esimerkiksi hyväksy -vaihtoehdon korostaminen ja oletuksena valitut valintaruudut vaikuttivat siihen hyväksyivätkö käyttäjät evästeet (European Commission. Directorate General for Justice and Consumers, 2022).

Kiinnostuin evästeistä ja pimeistä käytännöistä, koska niihin ei voi olla törmäämättä verkkosivustoja selatessa. Tarkoituksena onkin tutkia kuinka pimeät käytännöt ilmenevät suomalaisten suosimien sivustojen evästekyselyissä. Aihetta on aikaisemmin tutkittu muissa Euroopan maissa esimerkiksi Saksassa, Liettuassa ja Irlannissa (Krisam ym., 2021; Limba ym., 2021; Sheil & Malone, 2022). Vastaavaa tutkimusta ei kuitenkaan ole suoritettu suomalaisella aineistolla. Tutkimuskysymys on:

1. Millaisia pimeitä käytäntöjä esiintyy suomalaisten verkkosivustojen evästekyselyissä?

Tutkimuksen tarkoituksena on tarkastella visuaalisesti sadalta suomalaiselta verkkosivustolta löytyvää evästekyselyä ja perehtyä tarkemmin siihen millaisia pimeitä käytäntöjä näistä evästekyselyistä löytyy. Käytännössä tutkimus

suoritetaan vierailemalla sadalla suomalaisella .fi -päätteisellä sivustolla ja luokittelemalla niissä esiintyvät pimeät käytännöt.

Miksi pimeitä käytäntöjä kannattaa tutkia? Useat tutkimukset argumentoivat, että pimeistä käytännöistä on haittaa käyttäjälle tai ne ovat käyttäjän intressejä vastaan tai vaikuttavat haitallisesti käyttäjäkokemukseen (Forbrukerrådet, 2018; Gray ym., 2020; Waldman, 2020). Yksilölle aiheutuvan haitan lisäksi Mathur ym. (2021) nostavat esiin myös yhteisöllinen näkökulman. Vaikka pimeät käytännöt eivät vaikuttaisi suoraan yksilön hyvinvointiin niillä voi olla kumulatiivinen vaikutus yhteisön muihin jäseniin (Mathur ym., 2021).

Millä tavalla pimeät käytännöt ovat sitten yksilön kannalta haitallisia? Pimeät käytännöt voivat aiheuttaa kuluttajalle rahallista menetystä, ne voivat heikentää käyttäjän yksityisyyttä ja lisätä tämän kognitiivista taakkaa (Mathur ym., 2021). Rahallista menetystä kuluttajalle aiheuttaa esimerkiksi pimeä käytäntö, jossa ostoskoriin ilmestyy pyytämättä tuotteita (eng. Sneak into basket), puhelinostoksen yhteydessä ostoskoriin ilmestyy automaattisesti maksullinen näytönsuoja (Kilpailu- ja kuluttajavirasto, ei pvm.). Yksityisyyttä taas heikentävät esimerkiksi esivalitut asetukset, joissa suostutaan luovuttamaan tarpeettoman paljon tietoja (Mathur ym., 2021). Yksityisyyttä parantavat asetukset voivat puolestaan olla vaikeasti saavutettavissa (Mathur ym., 2021). Evästekyselyiden kohdalla tämä voi tarkoittaa sitä, että valinnaisista evästeistä kaikki on valittu tai että evästeiden kieltäminen on piilotettu asetusten taakse. Käyttäjien kognitiivista taakan lisääminen saattaa aiheuttaa sen, että käyttäjä valitsee helpoimman tarjolla olevan vaihtoehdon, jäämättä tarkastelemaan onko se paras (Mathur ym., 2021). Kognitiivista taakkaa voi myös lisätä se, että evästeitä ei pysty hylkäämään (Soe ym., 2020).

Yhteisön näkökulmasta pimeät käytännöt vähentävät yhteisön hyvinvointia vähentämällä kilpailua, hankaloittamalla hintojen vertailua ja heikentämällä luottamusta markkinoihin (Mathur ym., 2021). Toimivat ja tehokkaat markkinat lisäävät hintakilpailua ja innovaatioita. Yksi esimerkki pimeästä käytännöstä, joka häiritsee markkinoiden tehokasta toimintaa, on hiirenloukku (eng. roach motel). Käyttäjän on helppo sopia sopimus, mutta hankala päästä siitä eroon (Brignull ym., 2023b; Kilpailu- ja kuluttajavirasto, ei pvm.). Sopimuksen voi esimerkiksi luoda helposti verkossa, mutta siitä eroon pääsemiseksi voi joutua soittamaan asiakaspalveluun (Brignull ym., 2023a). Hintojen arviointia puolestaan hankaloittaa hintatietojen pimittäminen ostoksen loppumetreille tai niiden piilottaminen erillisen valikon taakse (Gray ym., 2018; Kilpailu- ja kuluttajavirasto, ei pvm.) Yrityksille hintojen läpinäkyvyyden parantaminen ei välttämättä ole hyödyksi ja ne saattavatkin omaksua samoja käytäntöjä kuin kilpailijansa (Gabaix & Laibson, 2006).

Marthur ym. (2021) mukaan pimeiden käytäntöjen lisääntyessä kuluttajat tulevat tietoisemmiksi niistä ja saattavat alkaa suhtautua skeptisemmin ja vastustuskykyisemmin kaikkeen sellaiseen mikä vaikuttaa pimeältä käytännöltä. Lisääntynyt skeptisyys saattaa kuitenkin johtaa siihen, että kuluttajalta menee ohi aitoja tarjouksia. (Mathur ym., 2021)

Viimeisenä yhteiseen hyvään negatiivisesti vaikuttavana tekijänä Matrhur ym. (2021) mainitsevat odottamattomat yhteiskunnalliset vaikutukset. Käyttäjät luovuttavat esimerkiksi paljon henkilökohtaisia tietoja palveluille kuten Facebookille, jotka sitten käyttävät näitä tietoja yksilöityyn markkinointiin (Mathur ym., 2021). Mainosten lisäksi tietoja voidaan käyttää muuhunkin, kuten kävi Cambridge Analytican tapauksessa, jossa tietoja käytettiin poliittisen disinformaation levittämiseen, jotta voitaisiin vaikuttaa vuoden 2016 Yhdysvaltojen presidentinvaaleihin (Mathur ym., 2021).

Aihe on siis tärkeä sekä yksilön näkökulmasta, että yhteisön näkökulmasta katsottuna. Oletuksena on, että pimeitä käytäntöjä löytyy suomalaisten verkkosivustojen evästekyselyistä ja niiden käyttö voi olla yleistäkin. Keskeistä on selvittää mitä ovat pimeät käytännöt, miten niitä voidaan luokitella ja miten ne ilmenevät evästekyselyissä. Tarkoitus on myös vertailla muualla Euroopassa tehtyjen tutkimusten tuloksia saatuihin tuloksiin.

# 2 EU:N YLEINEN TIETOSUOJA-ASETUS

Euroopan unionin yleinen tietosuoja-asetus (eng. General Data Protection Regulation, GDPR) tuli voimaan toukokuussa 2018 (Asetus 2016/679, 2016). Se on henkilötietojen käsittelyä sääntelevä laki, jota sovelletaan kaikissa EU maissa (Tietosuojavaltuutetun toimisto, ei pvm.-a). Lain tarkoituksena on yksilötasolla parantaa henkilötietojen suojaa (Tietosuojavaltuutetun toimisto, ei pvm.-a). EU-tasolla yhtenäistää tietosuojasääntelyä ja edistää EU:n sisäistä digitaalista kaupankäyntiä (Tietosuojavaltuutetun toimisto, ei pvm.-a). EU:n yleistä tietosuoja-asetusta on tärkeää tarkastella tämän tutkimuksen kannalta, koska se on yksi syistä, miksi vastaamme tulee evästekyselyitä ja se vaikuttaa myös siihen millaisia evästekyselyiden pitäisi olla.

## 2.1 EU:n yleisen tietosuoja-asetuksen vaikutus evästekyselyihin

Artiklan 6 mukaan henkilötietojen käsittelylle tarvitaan laillinen peruste (Asetus 2016/679, 2016). Yleisin peruste internet sivustolle kerätä käyttäjästä tietoja on käyttäjän antama suostumus (Bollinger ym., 2022). Suostumuksen tulee olla *"vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu"* (Asetus 2016/679, 2016). Jos rekisterin pitäjä esittää pyynnön sähköisessä muodossa, sen *"on oltava selkeä ja tiiviisti esitetty eikä se saa tarpeettomasti häiritä sen palvelun käyttöä, jota varten se annetaan"* (Asetus 2016/679, 2016 johdanto-osan kappale 32)

Sähköisen viestinnän tietosuojadirektiivi ja yleisen tietosuoja-asetuksen johdanto-osan kappale 30 määrittelevät, että suostumus edellytetään myös, kun kyseessä ovat evästeet (Bollinger ym., 2022; Asetus 2016/679, 2016; Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, 2002). Verkkosivustojen täytyy siis kertoa käyttäjilleen, mihin tarkoitukseen evästeitä käytetään ja tarjota käyttäjälle mahdollisuus kieltäytyä tietyistä käyttötarkoituksista (Bollinger ym., 2022). Myös palveluntarjoajien, jotka eivät toimi EU:n alueella tulee noudattaa asetusta,

jos ne tarjoavat palveluitaan kohdennetusti EU:n kansalaisille (Krisam ym., 2021). Kohdentamiseksi voidaan katsoa esimerkiksi kielen tai valuutan käyttö, joka on käytössä EU:ssa (Krisam ym., 2021).

Yleinen tietosuoja-asetus säätelee siis myös evästeiden käyttöä. Koch (2019) on tiivistänyt hyvin, mitä seikkoja palveluntarjoajien tulee ottaa huomioon täyttääkseen yleisen tietosuoja-asetuksen vaatimukset:

- Niiden tulee saada käyttäjän suostumus ennen evästeiden asettamista, pois lukien teknisesti välttämättömät evästeet
- Kertoa tarkasti millaista tietoa kukin eväste kerää ja mikä on sen tarkoitus selkeästi ymmärrettävällä kielellä.
- Dokumentoida ja tallentaa suostumus, jonka se on saanut käyttäjältä
- Mahdollistaa palvelun käyttö, vaikka käyttäjä kieltäytyisi tietyistä evästeistä.
- Tehdä yhtä helpoksi kuluttajan perua suostumuksensa, kuin se oli antaa ensimmäisellä kerralla.

(Koch, 2019)

Tietosuoja-asetuksen johdonmukaista soveltamista valvoo Euroopan tietosuojaneuvosto (eng. European Data Protection Board, EDPB), joka on riippumaton eurooppalainen elin (European Data Protection Board, ei pvm.-a). Se antaa myös ohjeistuksia (eng. Guidelines) EU:n tietosuojalakeihin liittyen (European Data Protection Board, ei pvm.-b). Vuonna 2020 hyväksytyssä ohjeistuksessa tietosuojaneuvosto täsmensi, millainen suostumus on lainvoimainen, kun kyseessä on evästekysely (European Data Protection Board, 2020). Palveluntarjoajat eivät voi estää käyttäjiä pääsemästä verkkosivustolle evästemuurin avulla, eli ehtona sivuston käyttämiselle ei saa olla evästeiden hyväksyminen (European Data Protection Board, 2020). Palveluntarjoajat eivät voi myöskään olettaa, että sivuston selailu jatkaminen on sama asia kuin suostumuksen antaminen. Oletuksena valitut valintaruudut evästekyselyssä eivät vastaa suostumuksen antamista oikeasti (European Data Protection Board, 2020).

## 2.2 Yleisen tietosuoja-asetuksen noudattamisesta

Kuinka hyvin sitten sivustot noudattavat EU:n yleistä tietosuoja-asetusta? Tutkimusten mukaan eivät kovinkaan hyvin, esimerkiksi vuonna 2020 julkaistussa tutkimuksessa vain 11,8 % tutkitusta 680 evästekyselytyypistä (eng. Consent Management Platform) täytti tutkijoiden asettamat vaatimukset, jotka perustuivat yleiseen tietosuoja-asetukseen (Nouwens ym., 2020). Toisessa tutkimuksessa, joka keskittyi 500 suosituimpaan saksalaiseen sivustoon, 54 % sivustoista ei täyttänyt vaatimuksia tai niiltä löytyi ainakin yksi rikkomus (Krisam ym., 2021). Kolmannessa tutkimuksessa käytiin läpi 400 evästekyselyä, jotka löytyivät eurooppalaisten suosimilta englanninkielisiltä nettisivuilta. Tämän tutkimuksen tulokset eivät olleet sen rohkaisevampia, 89 % kyselyistä ei täyttänyt lain vaatimuksia.

(Santos ym., 2021) Jotkut sivustot puolestaan käyttävät evästekyselyitä pelkästään kulissina, eivätkä välitä käyttäjän tekemistä valinnoista (Martini & Drews, 2022). Kun vedetään yhteen eri tutkimusten luvut, saadaan tulos, jonka mukaan 11,8–46 % verkkosivustojen evästekyselyistä täyttää yleisen tietosuoja-asetuksen vaatimukset.

Sääntöjen noudattamatta jättäminen ei ole kuitenkaan jäänyt huomiotta. Vuonna 2021 Ranskan tietosuojaa valvova viranomainen Commission nationale de l'informatique et des libertés (CNIL) määräsi Google LLC:lle 90 miljoonan euron sakon ja Google Ireland' lle 60 miljoonan euron sakon, koska ne eivät noudattaneet EU:n yleistä tietosuoja-asetusta ja Ranskan omaa tietosuoja lakia (CNIL, 2022a). Sakon lisäksi CNIL vaati, että ranskalaisilla käyttäjille tulee olla mahdollisuus kieltäytyä evästeistä yhtä helposti kuin hyväksyä ne (CNIL, 2022a). CNIL määräsi myös 35 miljoonan euron sakot Amazonin Euroopan osastolle, koska amazon.fr oli asettanut evästeitä käyttäjien laitteille ennen kuin käyttäjät antoivat suostumuksensa (CNIL, 2022b).

EU:n yleinen tietosuoja-asetus antaa siis raamit millä ehdoilla käyttäjän tietoja saa kerätä ja miten se tulisi tehdä. Palveluntarjoajille jää kuitenkin paljon vapauksia evästekyselyiden toteuttamisen suhteen ja usein ne kiertävät säädöksiä. Jossain tapauksissa tietosuojaviranomaiset ovat puuttuneet yritysten käytäntöihin.

# 3 EVÄSTEET

- *"-- every action leaves behind traces collected by companies for commercial purposes."* (West, 2019, s. 20)

Evästeet ovat yksi keino monien joukossa, jotka mahdollistavat sivustojen ylläpitäjille tietojen keruun sivustolla kävijöistä. Voidaankin puhua data-kapitalismista (West, 2019). Käyttäjien tietojen kaupallistaminen on mahdollistanut sen, että tieto ja sitä kautta valta, ovat jakaantuneet epätasaisesti (West, 2019). West jatkaa, että tieto ja valta kerääntyvät sille osapuolelle, jolla on pääsy dataan ja kyky analysoida sitä. Vallan epätasaisen jakautumisen vuoksi on tärkeää sekä yksilön että yhteiskunnan kannalta, että meillä on keinoja vaikuttaa siihen (Zuboff, 2019, s. 21).

Poliitikot ja lainsäätäjät siirtävät kuitenkin mielellään vastuun käyttäjille. Käyttäjien mahdollisuudet suojella yksityisyyttään ovat kuitenkin rajalliset (Baruh & Popescu, 2017). Käyttäjän voi olla vaikea ymmärtää kuinka tietoja kerätään, miten niitä käsitellään ja keille niitä luovutetaan, koska verkkosivustot käsittelevät tietoja käyttäjän silmiltä piilossa (Salonen, 2022). Voidaan myös kysyä, kuinka paljon se tieto, että yritykset seuraavat heitä ja louhivat heistä tietoja vaikuttaa käyttäjien käytökseen (Baruh & Popescu, 2017)?

Usein käyttäjää pyydetään luovuttamaan tietoja palveluiden parantamisen varjolla, tietoja voidaan kuitenkin käyttää kohdennettujen mainosten tarjoamiseen tai jopa yhteiskunnalliseen vaikuttamiseen (Mathur ym., 2021; Zuboff, 2019, s. 208–211). Esimerkiksi vuoden 2016 Yhdysvaltojen presidentinvaaleissa kerättyjä tietoja käytettiin poliittisen disinformaation levittämiseen (Mathur ym., 2021).

## 3.1 Mitä evästeet ovat ja mihin niitä käytetään?

Evästeet (eng. HTTP cookies) kehitettiin vuonna 1994 Netscape Navigator selaimen tarpeisiin (Jones, 2020). Ne ovat pieniä palvelimen lähettämiä datan kappaleita, jotka tallennetaan käyttäjän laitteen muistiin (Peters & Sikorski, 1997). Tarkemmin määriteltyinä ne ovat merkkijonoja, jotka tallennetaan tekstitiedostoina käyttäjän koneelle tämän vieraillessa sivustolla (Cahn ym., 2016; Limba ym., 2021; Peters & Sikorski, 1997). Ne varastoivat tiettyjä tietoja käyttäjästä, esimerkiksi salasanan tai ajankohdan, kun tämä vierailee sivustolla (Peters & Sikorski, 1997). Käyttäjän palatessa samalle sivustolle tämä tieto voidaan välittää takaisin palveluntarjoajalle (Peters & Sikorski, 1997). Evästeet ovat tarpeellisia esimerkiksi verkkokauppojen sivustoilla, sillä ne mahdollistavat sen, että käyttäjä voi valita tuotteita verkkokaupan eri sivuilta ja maksaa ne kaikki kerralla (Peters & Sikorski, 1997).

Evästeitä voidaan luokitella niiden teknisten ominaisuuksien perusteella: evästeen keston, tarkoituksen ja alkuperän mukaan (Koch, 2019). Kestolla tarkoitetaan joko väliaikaisia evästeitä, jotka tallennetaan selaimeen vain istunnon ajaksi tai pysyviä evästeitä, jotka säilyvät laitteen muistissa, kunnes ne poistetaan (Koch, 2019).

Tarkoitukseltaan evästeet voidaan Kochin (2019) mukaan jakaa neljään eri luokkaan. Ensimmäinen on välttämättömät evästeet, jotka varmistavat, että sivuston ominaisuudet toimivat toivotulla tavalla. Seuraavana ovat toiminnalliset evästeet, jotka mahdollistavat, että sivusto tallentaa tekemäsi valinnat, kuten minkä alueen säätiedotuksen haluat nähdä. Kolmantena ovat tilastolliset evästeet, jotka keräävät tietoa siitä, miten käyttäjät käyttävät sivustoa esim. mitä linkkejä klikattiin ja millä sivuilla vierailit. Neljäntenä ovat markkinointievästeet. Nämä evästeet seuraavat käyttäytymistäsi verkosta ja yhdistävät tietoja eri organisaatioilta ja mainostajilta tarjotakseen kohdennetumpia mainoksia. (Koch, 2019)

Alkuperältään evästeet voivat olla joko ensimmäisen osapuolen evästeitä, jotka tulevat suoraan vierailulta verkkosivulta tai kolmannen osapuolen evästeitä, jotka tulevat verkkosivuston ulkopuolelta (Cahn ym., 2016; Kaspersky, ei pvm.). Ensimmäisen osapuolen evästeet mahdollistavat mm. ostoskorin toiminnan. Kolmannen osapuolen evästeet tulevat usein dataa välittäviltä yrityksiltä esimerkiksi Datalogixilta, Epsilonilta tai mainostajilta tai käyttäjäseurantaa tekeviltä yrityksiltä esimerkiksi Google Analyticsilta (Cahn ym., 2016).

Evästeiden avulla voidaan luoda käyttäjästä yksilöllinen profiili ja kohdentaa mainontaa tämän profiilin mukaan (Peters & Sikorski, 1997). Evästeiden avulla sivustot voivat seurata, kuinka usein ole vieraillut sivustolla ja kauanko vierailusi kesti (F-Secure, ei pvm.; Kaspersky, ei pvm.). Profiilin avulla verkkosivu voi tallentaa myös käyttäjän mieltymyksen sivustolla, kuten uutissivustolla näytetään urheilu ennen politiikkaa tai käyttäjän tekemät kielivalinnat (F-Secure, ei pvm.; Kaspersky, ei pvm.).

Tietyt tahot ovat erityisen innokkaita asettamaan evästeitä. Ensinnäkin kolmannen osapuolen evästeet ovat kaksi kertaa yleisempiä kuin ensimmäisen

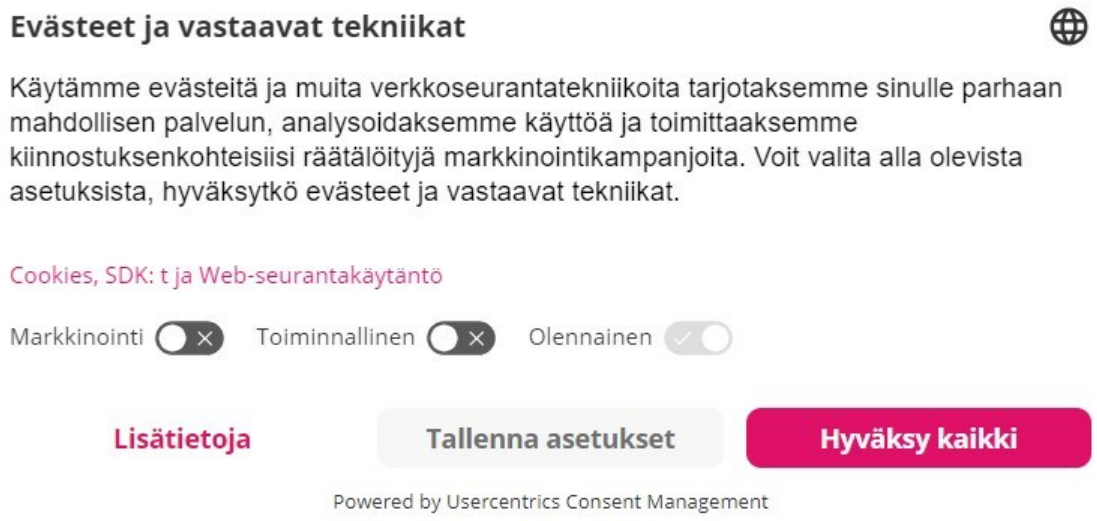
osapuolen evästeet (Cahn ym., 2016). Lisäksi pieni prosentti toimijoista on hyvin hallitsevia alalla (Cahn ym., 2016), esimerkiksi maailman miljoonan suosituimman sivuston joukosta Googlen seurantateknologiaa (eng. tracker) löytyy 75 % sivuista (Englehardt & Narayanan, 2016). Tämä on yhdenmukainen havainto sen kanssa, jonka Bailey ym. (2019) tekivät tutkiessaan, millaisia seurantateknologioita suomalaiset verkkosivustot käyttivät. He huomasivat, että ainakin 75 %:lla sivustoista oli mahdollisuus lähettää tietoja Googlelle (Bailey ym., 2019).

Kolmannen osapuolen evästeet voivat olla myös tietoturvauhka. Vuonna 2015 suomalaisella pankilla oli verkkosivullaan käytössä Google Analytics -työkalu (Bailey ym., 2019). Pankin tiedotteessa luvattiin, että kolmannen osapuolen evästeiden mukana ei siirry evästeiden tarjoajalle tietoja käyttäjästä (S-Pankki, 2015). Kirjautuessaan sivustolle demo tunnuksilla Räisänen (2015) havaitsi kuitenkin, että pankkitilin numero lähetettiin Googlelle käyttäen yksinkertaista SHA-1 salausta. Tämä salaus voitiin purkaa 0.5 sekunnissa väsytysmenetelmällä (eng. brute-force) (Räisänen, 2015). Esille nostetut tietoturvahuolet saivatkin pankin lopettamaan Google Analyticsin käytön (Pitkänen, 2015).

## 3.2 Mitä ovat evästekyselyt?

Evästekysely (eng. cookie banner, cookie consent, cookie consent banner) on teknisesti toteutettu kysely, jonka avulla käyttäjä pystyy hallitsemaan niitä yksityisyysasetuksia, jotka liittyvät evästeiden käyttöön sivustolla (Kampanos & Shahandashti, 2021). Evästekyselyille ei tiettävästi ole mitään standardia, joten jokainen internet sivusto on vapaa käyttämään haluamaansa kyselyä (Kampanos & Shahandashti, 2021).

Alla on esimerkkikuva (Kuva 2.) evästekyselystä, jossa on mahdollisuus kieltää erikseen markkinointi- tai toiminnalliset evästeet. Mahdollisuutta kieltää välttämättömät evästeet ei kuitenkaan ole, sillä niitä tarvitaan sivuston toiminnan takaamiseksi. Esimerkkinä olevassa evästekyselyssä kaikki evästeet on mahdollista hyväksyä yhdellä klikkauksella.




Kuva 2. Esimerkki evästekyselystä (Lähde: foodora.fi).

Evästekyselyt ovat tulleet myös näkyvämmäksi ja arkipäiväisemmiksi, varsinkin EU:n yleisen tietosuoja-asetuksen tultua voimaan toukokuussa 2018 (Asetus 2016/679, 2016). Yleinen tietosuoja-asetus on suoraan yhteydessä evästekyselyiden ja tietosuojaselosteiden kasvaneeseen määrään, mutta ei ole vahvoja todisteita sen tueksi, että asetus olisi vähentänyt verkossa tapahtuvaa seurantaa (Kretschmer ym., 2021). Tosin ainakin asetuksen tulessa voimaan sivustojen säädösten mukaisuus on voinut olla kyseenalaista. Degeling ym. (2019) havaitsivat tutkimuksissaan, että vaikka yli 60 % sivustoista löytyi evästekysely, useimmat eivät antaneet käyttäjille muuta mahdollisuutta kuin hyväksyä evästeet. Evästekyselyn olemassaolo sivustolla voikin antaa käyttäjälle väärän tunteen hallinnasta, jos se ei oikeasti tarjoa käyttäjälle mahdollisuutta hallita evästeitä (Degeling ym., 2019).

Hennig ym. (2022) kiinnostuivat niistä syistä, miksi palveluntarjoajat eivät noudattaneet yleisessä tietosuoja-asetuksessa evästekyselyille annettuja normeja. He lähettivät viestin 147 verkkosivustojen ylläpitäjälle, joiden evästekyselyt eivät olleet asetuksen mukaisia ja kysyivät, miksi heidän evästekyselynsä ei ollut yleisen tietosuoja-asetuksen mukainen. Valitettavasti kyselyyn ei vastannut kovin moni henkilö. Henning ym. (2022) saivat 7 vastausta, joista vain yhdessä kysely oli täytetty kokonaan. Kyselyn vastaajien selityksiin kuului mm. se, että vastaajat eivät pystyneet vaikuttamaan evästekyselyn ulkonäköön tai, että evästekyselyyn oli suunnitteilla muutoksia (Hennig ym., 2022).

Evästekyselyt ovat kuitenkin erittäin yleisiä siihen nähden, että evästekyselyä ei tarvitse esittää, jos sivusto käyttää ainoastaan välttämättömiä evästeitä (Kyberturvallisuuskeskus, 2023). Bruni (2019) huomauttaa blogitekstissään, että useat sivustot tarvitsevat evästeitä vasta, kun tämä kirjautuu sisälle verkkosivustolle. Jos sivustot vähentäisivät evästeiden käyttöä, tämä mahdollistaisi myös evästekyselyiden määrän vähentämisen. Tämä on kuitenkin epätodennäköistä evästeiden mahdollistaman tietojen keräämisen vuoksi.

# 4 PIMEÄT KÄYTÄNNÖT

Termille pimeä käytäntö ei ole yksiselitteistä selitystä, vaan tutkijat voivat käyttää sitä hieman eri tarkoituksessa. Yksi suhteellisen kattava määritelmä termille löytyy Kilpailu- ja kuluttajaviraston sivustolta:

> ”Pimeä käytäntö (dark pattern) on mikä tahansa sellainen nettisivun, ohjelmiston, mobiilisovelluksen tai muun käyttöliittymän suunnittelussa toteutettu keino, jolla saadaan käyttäjä tekemään jotain sellaista, jota hänen ei ollut alun perin tarkoitus tehdä. Kyse on siis käyttäjää manipuloivasta tai harhaan johtavasta suunnitteluratkaisusta, jolla vaikutetaan tämän tekemiin valintoihin esimerkiksi verkkosivulla. ” (Mutru, 2022)

Termin pimeä käytäntö (eng. dark pattern) kehitti Harry Brignull vuonna 2010 (Mathur ym., 2019). Määritelmä ei käytetty tieteellisessä julkaisussa vaan Brignull esitteli sen verkkosivustolla darkpatterns.org (Mathur ym., 2021). Tutustuessani tutkimusaiheeseen törmäsin useisiin erilaisiin vaihtoehtoisiin tapoihin suomentaa englanninkielinen termi ”dark pattern”. Emma Nevala (2023) oli käyttänyt pro gradu -tutkielmassaan termiä synkät suunnittelumallit. Miklos Strömberg (2020) käytti puolestaan pro gradu -tutkielmassaan suomennosta mustat mallit. Kilpailu- ja kuluttajavirasto käyttää puolestaan termiä pimeät käytännöt (Kilpailu- ja kuluttajavirasto, ei pvm.). Päädyin käyttämään tutkielmassani Kilpailu- ja kuluttajaviraston käyttämää termiä pimeät käytännöt.

Pimeän käytännön tarkoituksena on usein ohjata käyttäjää tekemään itsensä kannalta epäedullisia valintoja, kun taas yritys hyötyy (Kilpailu- ja kuluttajavirasto, ei pvm.). Ne käyttävät hyväkseen psykologista tietoa ihmisen käyttäytymisestä, kuten inhimillisen päätöksenteon heikkouksia ja tiedonkäsittelyn vinoumia (Gray ym., 2018; Mutru, 2022). Pimeistä käytännöt hyödyttävät siis yritystä ja niiden suunnittelussa käytetään hyväksi tietoa ihmisen psykologiasta.

Osa käytännöistä on selvästi lainvastaisia, joidenkin kohdalla laillisuuden arviointi edellyttää tapauskohtaista harkintaa (Kilpailu- ja kuluttajavirasto, ei pvm.). Pitää kuitenkin ottaa huomioon, että markkinointiin liittyy kuluttajan mieltymysten manipuloimista, joten keinon määritteleminen pimeäksi käytännöksi ei kerro vielä onko keino hyväksyttävä vai jotakin josta pitäisi rangaista

(Mathur ym., 2021). Koska pimeät käytännöt voivat olla laittomia, useiden maiden kuluttajansuojaviranomaiset sekä EU ovat kiinnostuneet niistä (European Data Protection Board, 2022; Forbrukerrådet, 2018; Kilpailu- ja kuluttajavirasto, ei pvm.; Laboratoire d'Innovation Numérique de la CNIL, 2019). Esimerkiksi vuonna 2021 kuusitoista eri kuluttajansuojaan keskittynyttä organisaatiota laativat valituksen Amazonista, koska se teki Prime -jäsenyyden tilauksen lopettamisesta tahallisen hankalaa (Myrstad, 2022).

## 4.1 Kuinka pimeitä käytäntöjä voidaan luokitella?

Koska termin pimeä käytäntö määritelmä riippui hieman tutkijasta, löytyy myös pimeiden käytäntöjen luokittelemiseksi erilaisia tapoja. Tarkastelemme ensin yhtä, jonka lähtökohta on Brignullin alkuperäisessä luokittelussa, jotta saadaan käsitys siitä, minkälaisia pimeitä käytäntöjä on ylipäänsä olemassa. Sen jälkeen tarkastellaan Mathur ym. (2021) luomaa taulukkoa, jossa pimeät käytännöt on jaettu yläkäsitteisiin. Viimeiseksi tarkastellaan, kuinka aikaisemmissa tutkimuksissa evästekyselyistä löytyneitä pimeitä käytäntöjä on luokiteltu.

Brignull, joka esitteli termin ensimmäisen kerran, laati myös taksonomian pimeille käytännöille (Brignull ym., 2023b). Brignullin luokittelua on laajennettu myöhemmin (Mathur ym., 2019). Yksi tällainen luokittelu on Gray ym. (2018) tekemä. He löysivät tutkimuksessaan viisi eri pääluokkaa, joihin he jaottelivat pimeät käytännöt (taulukko 1.).

TAULUKKO 1. Pimeiden käytäntöjen luokittelu Gray ym. (2018) mukaan

| **Pimeä käytäntö** | **Kuvaus** |
|---|---|
| Ruinaaminen (eng. Nagging) | Käyttäjän toiminta keskeytetään kerran tai useammin sellaisella toiminnalla, joka ei liity käyttäjän sillä hetkellä tekemään toimintaan. |
| Vaikeuttaminen (eng. Obstruction) | Tehdään toiminnasta vaikeampaa kuin sen tarvitsee olla. Tähän luokkaan kuuluvat mm. hintavertailun hankaloittaminen ja oikean rahan korvaaminen virtuaalisella. |
| Tietojen pimittäminen (eng. Sneaking) | Pimitetään, viivästytetään tai naamioidaan käyttäjälle annettavia tietoja, jotta saadaan käyttäjä tekemään valinta, jota hän ei tekisi, jos hänellä olisi enemmän tietoa. Luokkaan kuuluvat mm. piilotetut kulut, ostoskoriin ilmestyvät tuotteet, ilmaisnäytteen jatkuminen maksullisena ja toiminnon korvaaminen toisella. |
| Tiettyyn valintaa ohjaaminen (eng. Interface Interference) | Käyttöliittymän manipuloiminen niin, että se suosii/korostaa tiettyjä toimintoja. Tähän kuuluvat mm. oleellisten tietojen piilottaminen valikoihin tai pienellä kirjoitettuun tekstiin, valmiiksi valitut vaihtoehdot, tunteisiin |

| | |
|---|---|
| | vetoaminen, valheellinen hierarkia, piilomainonta ja kompakysymykset. |
| Pakotettu toiminta (eng. Forced action) | Käyttäjien on pakko suorittaa jokin toiminto, jotta he joko pääsevät käsiksi sisältöön tai voivat jatkaa tuotteen käyttämistä. Tähän luokkaan kuuluvat sosiaalinen pyramidi (sinun täytyy rekrytoida ystäväsi käyttämään palvelua), tietojen tahaton luovuttaminen ja pelillistäminen (tietyt ominaisuudet ovat saatavissa vain, jos suoritat toistuvasti tietyn toiminnon). |

Taulukosta käy ilmi, että esimerkiksi vaikeuttaminen -pimeän käytännön (eng. obstruction) toteutustapa voi vaihdella. Tuotteiden välistä hintavertailua voidaan hankaloittaa tai summat voidaan esittää virtuaalisena valuuttana, jolloin käsitys oikeasta rahan arvosta hämärtyy (Gray ym., 2018). Yhdistävänä tekijänä näille on kuitenkin tarkoitus vaikeuttaa käyttäjän toimintojen vaikeuttaminen (Gray ym., 2018).

Gray ym. (2018) käyttämä tapa, on yksi tapa luokitella pimeitä käytäntöjä ja se antaa yleiskuvan millaisia ne voivat käytännössä olla. Luokituksia on kuitenkin paljon muitakin kuin edellä esitelty, esimerkiksi seuraavat tutkijat ovat tehneet omat luokittelunsa tai luoneet oman määritelmänsä pimeille käytännöille: Conti ja Sobiesk (2010), Zagal ym. (2013), Greenberg ym. (2014), Bösch ym. (2016), Mathur ym. (2019) ja Maiera ja Harr (2020). Tutkimusta on tehty hyvinkin eri näkökulmista. Zagal ym. (2013) tutkivat pimeitä käytäntöjä peleissä. Greenberg ym. (2014) keskittyivät puolestaan prokseemiseen vuorovaikutukseen. He tutkivat kuinka etäisyys ihmisen ja kohteen välillä vaikuttaa näiden vuorovaikutukseen ja millaisia pimeitä käytäntöjä mahdollisesti käytetään hyväksi tällaisessa vuorovaikutuksessa. Bösch ym. (2016) puolestaan tutkivat yksityisyyteen liittyviä pimeitä käytäntöjä.

Mathur ym. loivat vuonna 2019 ensimmäisen kerran yläkäsitteisiin perustuvat luokat pimeille käytännöille (Mathur ym., 2019). Pari vuotta myöhemmin luokkia tarkennettiin lisäpiirteellä (Mathur ym., 2021). He tarkastelivat kuinka pimeät käytännöt muuttavat käyttäjän valinta-arkkitehtuuria (eng. choice architecture) kahdesta eri näkökulmasta. Ne joko muokkaavat käyttäjän päätösavaruutta (eng. decision space) tai manipuloivat käyttäjälle annettavaa informaatiota (taulukko 2). Marthur ym. (2019) eivät määrittele tarkemmin termiä päätösavaruus, mutta yhden määritelmän mukaan sen on käyttäjälle valittavissa olevien vaihtoehtojen valikoima (Klein ym., 2009).

TAULUKKO 2. Pimeiden käytäntöjen jakaminen yläkäsitteisiin Marthur ym.:n (2021) mukaan.

| **Vaihtoehtojen muokkaaminen** (eng. Modifying the decision space) | |
|---|---|
| Asymmetrinen (eng. Asymmetric) | Valintojen esittäminen epätasa-arvoisella tavalla |
| Rajoittava (eng. Restrictive) | Rajataan käyttäjän valintoja |

| | |
|---|---|
| Epätasa-arvoinen kohtelu (eng. Disparate treatment) | Käyttäjäryhmien eriarvoinen kohtelu |
| Piilevä (eng. Covert) | Vaikutusmekanismin piilottaminen/peittäminen/hämärtäminen käyttäjältä |
| **Informaatiovirran manipuloiminen** (eng. Manipulation of the information flow) | |
| Petollinen/Harhaanjohtava (eng. Deceptive) | Aikaansaavat virheellisiä uskomuksia, valheellisilla väittämillä tai jättämällä kertomatta tietoja. |
| Informaation pimittäminen (eng. Inforamation hiding) | Tietojen hämärtäminen tai niiden panttaaminen |

Mathurin ym.:n (2021) luokittelussa vaihtoehtojen muokkaaminen (eng. modifying the decision space) jakaantuu neljään luokkaan: asymmetriseen, rajoittavaan, epätasa-arvoiseen kohteluun ja piilottamiseen. Nämä keinot vaikuttavat käyttäjän tekemiin valintoihin muokkaamalla käyttäjälle tarjolla olevia valintoja. Informaatiovirran manipuloiminen (eng. manipulation of the information flow) jakaantuu harhaanjohtaviin pimeisiin käytäntöihin ja informaation pimittämiseen. Nämä vaikuttavat käyttäjän valintoihin manipuloimalla käyttäjille annettavaa tietoa. Molemmat keinot, käyttäjän päätösavaruuden muokkaaminen ja käyttäjälle annettavan informaation manipuloiminen, heijastelevat sitä kuinka pimeät käytännöt muokkaavat perustana olevaa valinta-arkkitehtuuria. (Mathur ym. 2021)

Asymmetriset pimeät käytännöt esittävät palvelua hyödyttävät valinnat siten, että ne on helppo huomata. Käyttäjää hyödyttävät valinnat on puolestaan piilotettu useiden klikkausten päähän tai niiden ulkonäköä on hämärretty. (Mathur ym., 2021) Tähän kuuluu esimerkiksi valintapainikkeiden suunnitteleminen eriarvoisiksi. Mathur ym. (2021) luokittelevat tähän luokkaan myös sellaiset tapaukset, jotka piilottavat käyttäjän yksityisyyttä kunnioittavat asetukset hämärien valikoiden taakse.

Rajoittavat pimeät käytännöt vähentävät tai rajoittavat käyttäjälle tarjolla olevien valintojen määrää (Mathur ym., 2021). Tällaisia ovat esimerkiksi pakotettu toiminta ja ”hiirenloukku” (Mathur ym., 2021). Pakotettu toiminta voi esimerkiksi tarkoittaa sitä, että käyttäjän on pakko hyväksyä evästeet, jotta hän pääsee etenemään sivustolle (Gray ym., 2018; Martini & Drews, 2022). ”Hiirenloukku” on palvelu, joka on helppo tilata, mutta jonka peruuttaminen on tehty hankalaksi (Kilpailu- ja kuluttajavirasto, ei pvm.).

Epätasa-arvoista kohtelua käyttäjäryhmien välillä ei ole esitetty aiemmissa määrittelyissä pimeänä käytäntönä (Mathur ym., 2021). Tämän tyyppinen pimeä käytäntö saattaa löytyä esimerkiksi peleistä. Maksukykyiset asiakkaat voivat ohittaa vaikeita kohtia pelissä maksamalla (Zagal ym., 2013). Toinen esimerkki on niin sanottu hinta epätasa-arvo (eng. price discrimination), jossa eri käyttäjiltä veloitetaan eri hinta samasta tuotteesta tai palvelusta (Hannak ym., 2014).

Vaikutusmekanismin piilottamisessa käyttäjää johdatellaan kohti tiettyä lopputulosta tai valintaa, mutta mekanismi, kuinka tämä tehdään, on piilotettu (Mathur ym., 2021). Jotkut pimeistä käytännöistä käyttävät hyväkseen kognitiivisia vinoumia toiset taas käyttävät värejä ja muotoilua ohjatakseen käyttäjiä,

esimerkiksi käyttäjille esitetään sivustolla tuote, jonka ainoa tarkoitus on saada muut vaihtoehdot näyttämään paremmilta (Mathur ym., 2021).

Harhaanjohtavat käytännöt saavat käyttäjässä aikaan vääriä uskomuksia käyttämällä valheellisia väittämiä tai jättämällä kertomatta asioita (Mathur ym., 2021). Keinot ovat yleisiä verkkokauppojen sivustoilla (Mathur ym., 2021). Tällaisia ovat esimerkiksi erilaiset tarjoukset, jotka ovat voimassa vain tietyn ajan ja käyttäjä näkee ajan kulumisen reaaliaikaisesti (Kilpailu- ja kuluttajavirasto, ei pvm.). Tämä luo käyttäjälle valheellisen tunteen kiireestä. Toinen keino on kehottaa käyttäjää kiirehtimään, koska saldoa on enää yksi jäljellä (Kilpailu- ja kuluttajavirasto, ei pvm.).

Viimeisenä on informaation pimittäminen. Siinä käyttäjälle annettavaa informaatiota vääristellään tai sen antamista pitkitetään (Mathur ym., 2021). Yksi esimerkki tällaisesta on toistuva tilaus. Tilausta tehdessä ei käy ilmi, että tilaus onkin toistuva (Gray ym., 2018). Tähän kategoriaan kuuluu myös lopullisen hinnan panttaaminen, kunnes käyttäjä on aivan tilausprosessin lopussa (eng. Hidden costs) (Brignull ym., 2023b).

Leiser (2022) huomauttaa, että Marthur ym. (2021) laatimien luokkien välillä voidaan tulkita olevan päällekkäisyyttä. Hänen mukaansa asymmetrisen luokan ja käyttäjän valintoja rajoittavan luokan välillä on päällekkäisyyttä. Valintojen esittäminen epäsymmetrisesti voidaan ajatella asettavan käyttäjälle rajoituksia, koska päätöksenteon taakka on suurempi. Leiser (2022) jatkaa, että myös piilevä -luokan ja harhaanjohtava -luokan välillä on päällekkäisyyttä. Piilevä -luokassa vaikutusmekanismi, kuinka käyttäjää ohjaillaan kohti haluttua valintaa, on piilotettu. Harhaanjohtava -luokassa tämä saavutetaan taas käyttämällä valheellisia väittämiä tai jättämällä kertomatta asioita (Leiser, 2022). Mielestäni myös asymmetrisen -luokan ja piilevä -luokan väillä on päällekkäisyyttä. Asymmetrisiin pimeisiin käytäntöihin lasketaan kuuluvaksi keinot, jotka ohjaavat käyttäjää visuaalisesti tiettyyn valintaa, mutta tämä keino voidaan laskea myös kuuluvaksi piilevä -luokkaan. Ongelmana onkin, että esimerkiksi evästekysely, jossa hyväksy -vaihtoehto on korostetumpi voi kuulua kumpaan vain luokkaan.

Millaisia mahdollisia pimeitä käytäntöjä evästekyselyissä mahdollisesti sitten ilmenee Mathur ym. (2021) luokittelun mukaan? Ne kuuluvat todennäköisesti valintaympäristöä muokkaaviin. Ongelmaksi muodostuukin se, että luokat ovat suhteellisen laajoja ja niiden välillä ilmenee päällekkäisyyttä. Luokan perusteella ei ole siis helppoa ensinnäkään määritellä pimeätä käytäntöä yksityiskohtaisesti. Toisaalta, jos pimeä käytäntö on tunnistettu, on vaikea sanoa varmasti mihin luokkaan se kuuluu. Mathur ym. (2021) luokittelu vastaakin pikemmin kysymykseen, minkä laatuisia, kuin millaisia.

## 4.2 Millaisia pimeitä käytäntöjä evästekyselyissä esiintyy?

Aikaisempaa tutkimusta, jossa olisi tarkasteltu suomalaisten sivustojen evästekyselyitä ja niiden pimeitä käytäntöjä, ei löytynyt, mutta löytyi useita, jossa oli

tutkittu asiaa toisessa Euroopan maassa. Ensin käydään läpi millaisia yleisiä havaintoja tutkijat ovat tehneet, sen jälkeen tarkastellaan kahta tapaa luokitella evästekyselyistä löytyvät pimeät käytännöt.

Kampanos ja Shahandashti (2021) analysoivat 7 500 Iso-Britannialaista ja Kreikkalaista evästekyselyä. Krisam ym. (2021) kävivät läpi 500 saksalaisten suosimien sivuston evästekyselyä. Limba ym. (2021) analysoivat 100 suosituinta sivustoa Liettuassa ja tarkastelivat niiden evästekyselyitä. Soe ym. (2020) puolestaan tutkivat 300 uutissivuston evästekyselyä Skandinaviasta, Isosta-Britanniasta ja USA:sta.

Kampanos ja Shahandashti (2021) havaitsivat tutkiessaan kreikkalaisia ja brittiläisiä sivustoja, että vaikka 60 % sivustoista tallensi selaimelle kolmannen osapuolen evästeitä vain vajaalla 50 % sivustoilla oli evästekysely tai -ilmoitus. Lisäksi he havaitsivat, että vain pieni osa sivustoista, joilla oli evästekysely, tarjosi yhtä helppoa hylkää -vaihtoehtoa kuin hyväksy -vaihtoehtoa. Lähes kaikki yrittivät saada käyttäjän hyväksymään heikommat yksityisyysasetukset ja tekivät kieltäytymisestä paljon hankalampaa (Kampanos & Shahandashti, 2021).

Samankaltaiseen tulokseen tulivat Krisam ym. (2021) tutkiessaan 500 saksalaisen sivuston evästekyselyä. Sivustoista, joilla oli evästekysely, 85 % yrtti saada käyttäjää hyväksymään evästeet visuaalisten keinojen avulla. Kun taas vain 21.5 % mahdollisti evästeiden hylkäämisen yhdellä klikkauksella (Krisam ym., 2021).

Limba ym. (2021) tutkivat ovatko liettualaiset evästekyselyt yleisen tietosuoja-asetuksen mukaisia. He havaitsivat, että jopa 92 % sivustoista asetti evästeitä ilman käyttäjän hyväksyntää. Lisäksi vain 28 %:lla sivustoista oli käytössä evästekysely, joka mahdollisti käyttäjälle valintojen tekemisen pelkän ilmoituksen sijaan ja 64 %:ssa evästekyselyistä oli valmiiksi rastitettuja kenttiä (Limba ym., 2021).

Soe ym. (2020) tutkivat löytyykö uutissivustoilta Gray ym.:n (2018) (taulukko 1.) määrittelemiä pimeitä käytäntöjä. He havaitsivat, että 297 sivustolla 300:sta oli käytössään ainakin yksi pimeä käytäntö. Eniten esiintynyt pimeä käytäntö oli vaikeuttaminen (eng. obstruction), joka tunnistettiin 43 % sivustoista. He tekivät myös havainnon, että vain viidellätoista verkkosivustolla oli käytössään mahdollisuus kieltää evästeet yhdellä klikkauksella, kun taas kaikilla niillä oli mahdollisuus hyväksyä ne yhdellä klikkauksella (Soe ym., 2020).

Soe ym. (2020) eivät ainoastaan tukeutuneet aiempaan aineistoon vaan he tekivät myös ehdotuksen, kuinka määritelmiä voitaisiin kehittää edelleen evästekyselyiden kohdalla. Alla on listaus heidän tekemistään ehdotuksista (taulukko 3.). Jotkut pimeistä käytännöistä on tunnistettu aikaisemmissa tutkimuksissa, mutta osaa ei ollut aikaisemmin määritelty (Soe ym., 2020). Ainakaan Soe ym. (2020) määrittelemille pimeille käytännöille ”Ei antonyymeja” ja ”Merkkaamattomat liukusäätimet” en löytänyt vastinetta muualta.

TAULUKKO 3. Evästekyselyissä havaitut pimeät käytännöt Soe ym. (2020) mukaan.

| **Pimeä käytäntö** | **Kuvaus** |
|---|---|
| Huomiotta jättäminen (eng. Does not count) | Sivusto asettaa evästeitä, vaikka suostumusta ei ole annettu. |
| Ei vaihtoehtoa (eng. No choice) | Linkit ja painikkeet vievät sivulle, jolla kerrotaan kuinka säätää selaimen asetuksia tai sivulle, jolla selostetaan/kerrotaan sivuston evästeistä, mutta eivät mahdollista niiden hylkäämistä. |
| Useampi kysely (eng. Multiple choice panels) | Sivustolla useampi evästekysely |
| Valintojen kaskadi (eng. Choice cascade) | Evästeet voi hylätä vain seuraamalla useita linkkejä tai painikkeita, jotka tarjoavat lisätietoja |
| Epätasa-arvoinen kysely (eng. Widget inequality) | Hyväksy ja hylkää vaihtoehdot on esitetty eri tavalla. Yleensä hyväksy -vaihtoehto on korostetumpi ja hylkää -vaihtoehto esitetään eri tavalla esimerkiksi linkkinä painikkeen sijaan. |
| Merkkaamattomat liukusäätimet (eng. Unlabeled sliders) | Liukusäätimet antavat käyttäjän valita haluamansa evästeet, mutta niitä ei ole merkitty selvästi, mikä on hyväksy/on ja mikä on hylkää/off. |
| Merkitsemätön X (eng. Unmarked X) | Kyselyn oikeassa yläkulmassa on yleensä rasti sulkemista varten, mutta mihinkään ei ole merkitty tarkoittaako sen painaminen evästeiden hylkäämistä vai hyväksymistä. |
| Ei antonyymejä (eng. No antonyms) | Selkeiden ilmaisujen puuttuminen. Sen sijaan, että käytettäisiin selkeitä vastakohtia ”Hyväksy” tai ”Salli” ilmaisuille käytetään epämääräisempiä ilmaisuja kuten ”Tallenna valinnat” tai ”Hallitse asetuksia”. |

Toinen artikkeli, josta löytyy listaus evästekyselyistä löytyvistä pimeistä käytännöistä, on Martini ja Drewsin (2022) ”*Making Choice Meaningful*”. Martini ja Drews (2022) eivät koonneet omaa ainestoaan vaan koostivat taulukon aikaisemman tutkimuksen perusteella ja se on osa Dark pattern detection -tutkimusprojektia, jota rahoittaa yksi Saksan liittovaltion ministeriöistä. Martini ja Drews (2022) luettelevat viisi erilaista pimeää käytäntöä, jotka esiintyvät evästekyselyissä: oletusvalinnat, harhaanjohtamisen, estämisen, ruinaamisen ja pakotetun toiminnan.

**Oletusvalinnassa** (eng. Preselection) tietyt valinnat on tehty käyttäjälle valmiiksi (Martini & Drews, 2022). Palveluiden toimittajat käyttävät valmiiksi valittuja valintaruutuja, liukusäätimiä tai muita elementtejä (Gray ym., 2018; Kilpailuja kuluttajavirasto, ei pvm.). Tällaisten valikkojen suunnittelijat tietävät, että käyttäjät eivät viitsi muuttaa tehtyjä valintoja, vaan jatkavat oletuksilla (Martini & Drews, 2022).

**Harhaanjohtamisella** (eng. Misdirection) yritetään saada käyttäjä hyväksymään yksityisyyden kannalta epäsuotuisat asetukset (Nouwens ym., 2020). Tämä esiintyy tyypillisesti siten, että valintapainikkeet on suunniteltu eriarvoisiksi (Kilpailu- ja kuluttajavirasto, ei pvm.; Martini & Drews, 2022). Tämän vuoksi käyttäjät voivat jättää huomiotta muita vaihtoehtoja (Martini & Drews, 2022; Utz ym., 2019)

**Estämisellä** tai tietojen piilottamisella (eng. Obstruction/ Hidden information) ei tarkoiteta tässä yhteydessä sitä, etteikö käyttäjä pääsisi etenemään sivulle, vaan sitä, että käyttäjän tielle on asetettu esteitä. Tämä tekniikka oli esitetty jo Gray ym. (2018) taulukossa. Toinen tapa ilmaista asia on tietojen piilottaminen (European Data Protection Board, 2022; Kilpailu- ja kuluttajavirasto, ei pvm.). Yksi esimerkki tästä on evästeiden kieltämisen mahdollistavan painikeen on piilottaminen toiselle tai kolmannelle tasolle, kun taas evästeiden hyväksyminen on helppoa (Graßl ym., 2021; Gray ym., 2018; Nouwens ym., 2020). Käyttäjien pitää usein valita linkki tai painike, joka on usein melkein huomaamaton päästäkseen oikeaan valikkoon (Martini & Drews, 2022).

Myös **ruinaaminen** (eng. Nagging) oli mukana Gray ym. (2018) taulukossa. Ruinaamisella tarkoitetaan tässä esimerkiksi sellaista toimintoa, jossa evästekysely esitetään yhä uudelleen, vaikka evästeistä olisi jo aiemmin kieltäydytty tai evästekysely olisi suljettu (European Data Protection Board, 2022; Gray ym., 2018).

Viimeinen käytäntö on **pakotettu toiminta** (eng. Forced action) tai evästeeste (eng. cookie wall). Tässä tapauksessa käyttäjä ei pääse jatkamaan sivustolle ennen kuin hän on hyväksynyt evästeet (Martini & Drews, 2022). Martini ja Drews jaottelevat tähän kategoriaan myös sellaiset sivustot, jotka pakottavat käyttäjän tekemään valinnat ennen kuin ne päästävät jatkamaan sivustolle, vaikka ne päästäisivät jatkamaan sivustolle käyttäjän hylätessä evästeet.

Taulukossa 4 on verrattu yhtenäisyyksiä Soe ym. (2020) ja Martini ja Drewsin (2022) luokittelussa. Ensimmäinen yhteinen on harhaanjohtaminen (Martini & Drews, 2022), joka on sisällöltään sama kuin epätasa-arvoinen kysely (Soe ym., 2020). Molemmissa käytetään hyväksi vaihtoehtojen epätasa-arvoista esittämistä. Estäminen/tietojen piilottaminen (Martini & Drews, 2022) vertautuu valintojen kaskadiin (Soe ym., 2022). Hylkää vaihtoehto piilotetaan linkin taakse, josta käyttäjä joutuu sen etsimään. Soe ym.:n (2020) ”ei vaihtoehtoa” taas on hyvin samanlainen kuin Martini ja Drewsin (2022) pakotettu toiminta. Molemmissa käyttäjällä ei ole muuta vaihtoehtoa kuin hyväksyä evästeet.

TAULUKKO 4. Evästekyselyissä esiintyvien pimeiden käytäntöjen vertailu Soe ym., (2022) ja Martinin ja Drewsin (2022) välillä.

| **Soe ym. (2022)** | **Martini & Drews (2022)** |
|---|---|
| Epätasa-arvoinen kysely | Harhaanjohtaminen |

| | |
|---|---|
| Valintojen kaskadi | Estäminen/ tietojen piilottaminen |
| Ei vaihtoehtoa | Pakotettu toiminta |

Taulukossa 5 on esitetty pimeät käytännöt, jotka erosivat Soe ym. (2020) ja Martini ja Drews (2022) kesken. Soe ym.:n (2020) löytyy viisi pimeää käytäntöä, jota ei esiinny Martini ja Drewsillä (2022). Ne ovat: huomiotta jättäminen, useampi kysely, merkkaamattomat liukusäätimet, merkitsemätön x ja ei antonyymeja. Martini ja Dresillä (2022) puolestaan mainitsevat oletusvalinnat ja ruinaamisen, joita ei ole Soe ym.:n (2020) listauksessa.

TAULUKKO 5. Eroavat pimeät käytännöt Soe ym. (2022) ja Martini ja Drewsin (2022) välillä.

| **Vain Soe ym. (2022)** | |
|---|---|
| Huomiotta jättäminen | Käyttäjän valintoja ei huomioitu oikeasti |
| Useampi kysely | Sivustolla useampi evästekysely |
| Merkkaamattomat liukusäätimet | Liukusäätimistä ei käy selkeästi ilmi, milloin asetukset ovat päällä ja milloin pois päältä. |
| Merkitsemätön X | Ei ole kerrottu merkitseekö kyselyn sulkeminen evästeiden hylkäämistä vai hyväksymistä |
| Ei antonyymejä | Hylkää termin esittäminen epäselvästi |
| **Vain Martini & Drews (2022)** | |
| Oletusvalinnat | Valmiiksi rastitetut ruudut |
| Ruinaaminen | Evästekyselyn esittäminen uudelleen, kunnes käyttäjä hyväksyy evästeet |

Soe ym. (2020) listaus perustuu pimeisiin käytäntöihin, joita he havaitsivat tutkiessaan 300 uutissivuston evästekyselyä. Heidän luokittelunsa on tarkempi siinä suhteessa, että minkälaisia pimeitä käytäntöjä ilmenee käytännössä evästekyselyissä. Martini ja Drewsin (2022) luokittelu perustuu pimeiden käytäntöjen yleiseen luokitteluun, josta he ovat nostaneet käytäntöjä ja soveltaneet niitä evästekyselyihin. Soe ym.:n (2020) ja Martini ja Drewsin (2020) artikkeleiden pohjalta voidaan laatia listaus evästekyselyissä mahdollisesti esiintyvistä pimeistä käytännöistä tutkimusta varten. Listaus ja valintaperusteet löytyvät kappaleesta 6.2 analyysimenetelmät.

# 5 TEOREETTINEN VIITEKEHYS

> "*Design is not just what it looks like and feels like. Design is how it works*" -Steve Jobs. (Walker, 2003)

Evästekyselyt ovat tietoisen suunnittelun tulos niiden on tarkoitus tarjota käyttäjälle mahdollisuus valita ne evästeet, jotka hän haluaa hyväksyä. Suunnittelijan näkökulmasta tarkoitus on saada käyttäjä hyväksymään mahdollisimman paljon evästeitä, jotta käyttäjästä saadaan kerättyä mahdollisimman paljon tietoja. Käyttäjän puolestaan joutuu harkitsemaan omia tietosuoja-asetuksiaan joka kerta, kun hän törmää evästekyselyihin. Taustalla mahdollisesti vaikuttavista teorioista käydään läpi kaksi. Ensin suunnitteluun vaikuttava valintamuotoilu ja toisen käyttäjään vaikuttava Privacy calculus -teoria.

Valintamuotoilu käsittelee sitä kuinka käyttäjiä voidaan ohjata kohti haluttuja valintoja (Thaler & Sunstein, 2021). Valintamuotoilulla pyritään yleensä ohjaamaan käyttäjiä kohti käyttäjiä hyödyttäviä valintoja esimerkiksi asettamalla hedelmät ja kasvikset paremmin tarjolle, jolloin niiden kulutus kasvaa (Hanks ym., 2013). Kun valintamuotoilua käytetään hyödyttämään palvelun tarjoajaa, kyseessä on usein pimeä käytäntö (Martini & Drews, 2022).

Käyttäjä puolestaan katsoo evästekyselyitä ja sen yksityisyysasetuksia omasta viitekehyksestään. Privacy calculus -teorian mukaan käyttäjät arvioivat hyötyjä suhteessa riskiin ennen kuin luovuttavat tietoja (Meier & Krämer, 2022). Jos hyödyt nähdään suurempana kuin riskit, käyttäjä luovuttaa tietojaan todennäköisemmin (Meier & Krämer, 2022). Toisaalta käyttäjät haluavat sujuvaa palvelua, vaikka ovat huolissaan yksityisyydensuojastaan (Salonen, 2022).

## 5.1 Valintamuotoilu

Valintamuotoilun (eng. The Nudge Theory) popularisoivat Richard Thaler ja Cass Sunstein vuonna 2008 julkaisemassaan kirjassa: *Nudge: improving decisions*

*about health, wealth, and happiness*. Virallista suomennosta teorialle en löytänyt, mutta useissa lähteissä käytettiin, joko termiä tuuppaus (Lappalainen, 2019; Ojanen, 2023; Rantalahti, 2020) tai termiä valintamuotoilu (Karumaa, 2023; Vainio, 2018). Päädyin käyttämään tässä tutkielmassa termiä valintamuotoilu, kun tarkoitetaan koko teoriaa ja termiä tuuppaus, kun puhutaan yksittäisistä muutoksista valinta-arkkitehtuurissa.

Valintamuotoilulla pyritään ohjaamaan ihmisiä kohti heitä hyödyttäviä valintoja, mutta siten, että se ei muuta taloudellisia kannustimia tai estä tekemästä muita valintoja (Thaler & Sunstein, 2008, s. 6). Valinnat ovat siis vapaaehtoisesti tehtyjä ja kaikki vaihtoehdot tarjotaan ilman ylimääräisiä kustannuksia tai vaivaa (Leal ym., 2022).

Thaler ja Sunstein (2008) puhuvat tuuppauksista (eng. nudges). Tuuppaukset ovat mitä tahansa ominaisuuksia valinta-arkkitehtuurissa (eng. choice architecture), jotka muokkaa ihmisen käytöstä odotetulla tavalla, mutta jotka ovat siis kustannuksiltaan ja ponnistuksiltaan samanarvoiset (Thaler & Sunstein, 2008, s. 6). Tuuppaukset auttavat siis suunnittelemaan valinta-arkkitehtuurin uudelleen, käyttäen tarkoituksellisia ja ennustettavissa olevia menetelmiä, joilla voidaan vaikuttaa ihmisten käytökseen (Leal ym., 2022). Menetelminä voivat olla päätöksentekoon vaikuttavien tiedostamattomien prosessien aktivointi tai käyttäjän saamiin vihjeisiin vaikuttaminen (Leal ym., 2022). Tuuppaukset siis ”tuuppavat” meitä tekemään halutun valinnan (Thaler & Sunstein, 2008, s. 6).

Valinta-arkkitehtuurin Thaler ja Sunstein (2008, s.3) puolestaan määrittelevät, sen kontekstin määrittelemiksesi, jossa ihmiset tekevät valintoja ”-- *organising the context in which people make decisions*”. Valinta-arkkitehtuuri on siis se ympäristö tai tapahtumapaikka, jossa valinnat tehdään (Leal ym., 2022; Thaler & Sunstein, 2021, s. 103–129). Millaisia keinoja voidaan sitten käyttää, jotta käyttäjät saadaan tekemään haluttu valinta? Thaler ja Sunstein (2008, s. 3) argumentoivat, että ei ole olemassa ”neutraalia” suunnittelua. Pienilläkin yksityiskohdilla voi olla merkitystä (Thaler & Sunstein, 2008, s. 3). Oletusvalinnat on yksi keino saada ihmiset valitsemaan tai oikeastaan pysymään tehdyssä valinnassa (Thaler & Sunstein, 2008, s. 8). Toinen keino on tehdä halutusta vaihtoehdosta helpoin suorittaa (Thaler & Sunstein, 2021, s. 107). Tekemällä vaihtoehdosta helposti valittava, voidaan käyttäjiä ohjata sen suuntaa (Thaler & Sunstein, 2021, s. 108–112).

Valintamuotoilun avulla voidaan siis suunnitella käyttäjän kannalta paremmin toimivia evästekyselyitä. Graßl ym. (2021) tekivät tutkimuksen, jossa he esittivät yli 200 koehenkilölle evästekyselyn. Tavallisessa tilanteessa käyttäjät hyväksyivät noin 94 % evästeistä. Tutkijat kuitenkin havaitsivat, että evästeiden hyväksymisprosentti putosi 53,2 %:n, kun tehtiin vastakkaisia suunnitteluratkaisuja kuin tavallisesti. Tällaisia olivat seurannan esto oletusvalintana, hylkää -painikkeen korostaminen tai käyttäjälle annettiin vaihtoehtoina hylkää -painike tai asetukset (Graßl ym., 2021). Suunnitteluratkaisut olivat siis päinvastaiset kuin tyypilliset hyväksy -painikkeen korostaminen, oletusvalintana valitut ruudut tai käyttäjälle annettava hyväksy tai asetukset vaihtoehto.

Käyttäjän kokemaa vaivaa voidaan myös tahallisesti lisätä. Thaler ja Sunstein (2021, s. 151–176) puhuvat järjestelmään lisättävästä kitkasta (eng. sludge).

Tehdään toisesta vaihtoehdosta niin hankala, että käyttäjä mieluummin valitsee helpomman vaihtoehdon. Thaler ja Sunstein (2021, s.170) käyttävä yhtenä esimerkkinä evästeitä. He kertovat kuinka vieraillessaan sivustolla mobiililaitteella heitä kehotetaan ensimmäisenä tekemään evästevalinnat, mutta vaikka he valitsisivat ”ei” vaihtoehdon, valinta ei kuitenkaan tarkoita, että he pääsisivät lukemaan haluamaansa artikkelia, vaan heitä kysellään loputtomasti evästeistä pienellä fontilla. He kokivat, että tällöin on vain helpompi antaa periksi ja hyväksyä evästeet, kuin ruveta kahlaamaan asetuksia (Thaler & Sunstein, 2021, s. 170).

Tämä esimerkki on hyvin samanlainen kuin Soe ym., (2022) antama esimerkki pimeästä käytännöstä valintojen kaskadi. Käyttäjä joutuu käymään läpi useita valikoita löytääkseen haluamansa asetuksen tai voidakseen kieltäytyä evästeistä. Kyseessä on siis kaksi vastakkaista ”voimaa”. Tuuppauksilla ohjataan käyttäjää kohti yhtä valintaa ja kitkan avulla pyritään estämään käyttäjää tekemästä toista valintaa.

Pimeistä käytännöistä puhutaan toisinaan pimeinä tuuppauksina (Graßl ym., 2021; Martini & Drews, 2022). Valintamuotoilun periaatteita ja oppeja käytetään tällöin pimeiden käytäntöjen suunnittelussa. Valintamuotoilulla pyritään ohjamaan käyttäjää kohti tätä hyödyttäviä valintoja. Pimeiden käytäntöjen tarkoitus on kuitenkin hyödyttää palvelun tarjoajaa.

## 5.2 Privacy Calculus -teoria

Toiseksi teoriapohjaksi otin Privacy calculus teorian. Valintamuotoilun näkökulma on suunnittelijan; kuinka suunnitella palvelu tai toiminto siten, että se saa käyttäjän toimimaan tietyllä tavalla. Kun taas Privacy calculus -teoria katsoo asiaa käyttäjän näkökulmasta ja yrittää arvioida millaisia valintoja käyttäjä tekee yksityisyytensä liittyen ja miksi.

Aikaisemmin Privacy calculus -teoria tunnettiin Behaviour calculus -teoriana ja sen juuret ovat 1970-luvulla. Tällöin keskityttiin käsitykseen yksityisyydestä ja siitä kuinka tämä käsitys on tiukasti sidoksissa konkreettisiin jokapäiväisiin tilanteisiin (Laufer & Wolfe, 1977). 2000 -luvun taitteessa ongelma nousi uudella tavalla esille, kun verkkokauppojen käyttö lisääntyi ja kauppiaille tarjoutui uudenlaisia mahdollisuuksia kerätä asiakkaistaan dataa (Dinev & Hart, 2006). Datan keräämiseen liittyykin ongelma. Se mikä näyttäytyy yrityksille arvokkaana datana, on yksityisyydensuojan kannalta ongelma kuluttajille (Culnan & Armstrong, 1999). Yksi esimerkkitapaus on amerikkalainen myymäläketju Target, joka käytti data-analytiikkaa tunnistaakseen raskaana olevat asiakkaat, vaikka he eivät tätä tietoa suoraan Targetille antaneetkaan (Duhigg, 2012).

Privacy calculus -teorian mukaan internetin käyttäjät arvioivat hyötyjä suhteessa riskiin ennen kuin luovuttavat henkilökohtaisia tietoja (Meier & Krämer, 2022). Ajatuksena on, että jos käyttäjä kokee hyötyvänsä paljon tilanteesta, hän todennäköisemmin luovuttaa tietoja. Vastaavasti, jos riskit nähdään suureksi, tietojen luovuttaminen on epätodennäköisempää. (Meier & Krämer, 2022) Tämä

heijastelee Culnanin ja Armstrongin (1999) näkemystä, jonka mukaan asiakkaat ovat valmiita luovuttamaan tietoja ja suostuvat asiakasprofiilien luomiseen, jos he tietävät, että heidän tietojaan käsitellään oikeudenmukaisesti. Evästekyselyiden tapauksessa tämä voi tarkoittaa sitä, että käyttäjät valitsevat tiukemmat asetukset, jos eivät näe hyötyä tietojen luovuttamisessa (Graßl ym., 2021).

Privacy calculus -teoriaa kohtaan kohdistuu myös kritiikkiä. Yksi tällainen on privacy paradox -näkökulma. Sen mukaan useimmat käyttäjät eivät ajattele jokapäiväisessä toiminnassaan millaisia vaikutuksia yksityisyysasetuksilla voi olla (Gerber ym., 2018). Vaikka ihmiset ovat huolissaan tietosuojasta, harva tekee asioita aktiivisesti suojatakseen dataansa ja moni luovuttaa tietojaan vapaaehtoisesti (Gerber ym., 2018). Käyttäjät esimerkiksi kertovat elämästään sosiaalisessa mediassa tai käyttävät kuntoiluun tarkoitettuja sovelluksia, mutta tekevät harvoin toimia, jotka voisivat suojata heidän yksityisyyttään esimerkiksi poistavat evästeet selaimesta (Gerber ym., 2018). Kuluttajat voivat olla siis huolissaan tietoturvasta, mutta eivät kuitenkaan halua hidasteita tai esteitä palvelun käytölle (Salonen, 2022).

Miten sitten privacy calculus -teoria liittyy evästeisiin? Evästeet keräävät tietoja meistä, kun liikumme internetissä. Eri lähteistä saatavia tietoja yhdistämällä yritykset saavat vielä enemmän tietoa meistä ja liikkeistämme netissä ja nämä tiedot ovat rahanarvoisia. Päätökset sallimmeko evästeet ovat osa yksityisyys asetuksia, joten jos näemme niiden hyväksymisessä enemmän hyötyjä kuin haittoja saatamme hyväksyä ne helpommin, esimerkiksi saatamme odottaa, että sivusto toimii paremmin, jos hyväksymme evästeet.

# 6 EMPIIRINEN OSUUS

Tutkimus suoritetaan laadullisena tutkimuksena. Aineistona käytetään sadalta suomalaiselta verkkosivustolta löytyvää evästekyselyä. Analyysi suoritetaan tarkastelemalla evästekyselyitä visuaalisesti. Pimeiden käytäntöjen luokittelussa käytetään apuna Martini ja Drewsin (2022) sekä Soe ym. (2020) artikkeleiden pohjalta luotua luokittelua.

## 6.1 Aineisto

Alun perin tutkimuksen tarkoituksena oli tarkastella sadan suosituimman suomalaisen nettisivuston evästekäytäntöjä. Yllättäen haasteelliseksi kuitenkin muodostui sellaisen listauksen löytäminen, jossa olisi lueteltu sata suosituinta suomalaista verkkosivustoa. Tutkimukset joihin perehdyin, olivat käyttäneet Amazonin ”Alexa Internet inc. ranking” -palvelua (Krisam ym., 2021; Limba ym., 2021), mutta tämä palvelu oli lopettanut toimintansa toukokuussa 2022. Maksullisia listauksia olisi kyllä ollut olemassa (esim. similarweb.com) mutta näiden ongelmaksi muodostui niiden kustannukset ja se, että ne eivät erotelleet suomalaisia sivustoja, vaan listauksesta löytyy esimerkiksi youtube.com. Lopulta löysin tutkimuksen, jossa oli käytetty lähdettä, joka oli vapaasti saatavilla. Tutkiessaan brittiläisiä ja kreikkalaisia sivustojen evästekyselyitä Kampanos ja Shahandashti (2021) olivat käyttäneet Tranco Top sites ranking (Le Pochat ym., 2019) ja suodattaneet listasta .uk ja .gr -päätteiset sivustot.

Tranco on tutkimuspainotteinen listaus nettisivuista, joka koostetaan viidestä muusta lähteestä (Le Pochat ym., 2019). Listauksessa on miljoona maailman suosituinta nettisivua, kuinka ne sijoittuvat listalla riippuu eri tilastollisista

tekijöistä (Le Pochat ym., 2019). Käytin Tranco-listausta, joka oli muodostettu 30.8.2023[1] ja sen sai ladattua CVS tiedostona (Le Pochat ym., 2019).

Listauksen löydyttyä ongelmaksi nousi mitkä sivustot listalta poimisin. Päätin käyttää vain .fi-päätteisiä sivustoja, vaikka suomalaisia sivustoja voi olla rekisteröityneen esimerkiksi .com verkkotunnuksen alle. Jätin ne kuitenkin tutkimuksen ulkopuolelle, koska niiden seulominen listasta olisi liian hankalaa.

Suomen kansallista verkkotunnuspäätettä .fi-päätettä hallinnoidaan Traficomissa (Traficom, 2019). Traficom huolehtii siitä, että fi-päätteisiin verkkotunnuksiin liitetyt verkkosivustot ja sähköpostiosoitteet toimivat kaikkialla maailmassa (Traficom, 2019). Päätetunnuksen käyttöä ei ole rajattu, vaan ”*Kaikki yritykset, yhteisöt ja yksityishenkilöt kotipaikasta riippumatta voivat rekisteröidä itselleen fi-verkkotunnuksen*” (Traficom, 2022). Tunnus haetaan verkkotunnusvälittäjän kautta, joka rekisteröi verkkotunnuksen hakijan puolesta (Traficom, 2022). Ei siis ole takeita, että .fi-pääte rajaa ulkopuolelle ulkomaalaiset sivustot. Koska Suomen .fi-päätetunnus on tuntemattomampi, oletan kuitenkin, että se ei ole laajasti muualla käytössä. Toisin kuin esimerkiksi Tuvalun .tv-pääte, jonka myyminen on tuonut saarivaltiolle ylimääräisen tulonlähteen (Lee, 2019).

Suodatin ensimmäiseksi listauksesta .fi-päätteiset sivustot. Tässä listauksessa oli kuitenkin vielä paljon virheellisiä tai puutteellisia sivujen osoitteita, esimerkiksi ensimmäinen osuma oli järjestyksessä 792 “simpli.fi”. Osoite ei kuulostanut lainkaan tutulta ja pikaisella Googlauksella selvisi, että se on Teksasissa toimivan mainostoimiston sivu. Epäilen, että yritys on valinnut .fi-päätteen, koska on kuvitellut sen liittyvän rahoitukseen (eng. finance). Epäilen samanlaisen ajatusrakenteen olleen usean kryptovaluuttasivuston takana, jotka löytyivät hakutuloksista. Poistin tuloksista vapaalla kädellä kaikki sivustot, jotka olivat joko ulkomaalaisia, koskivat kryptovaluuttoja, pyörittivät nettihotelleja, liittyivät aikuisviihteeseen tai joista ei löytynyt tietoa pikaisen googletuksen perusteella. Esimerkiksi ”spoti.fi” -haulla Google löysi kyllä paljon Spotifyyn liittyviä tuloksia, mutta ei mitään itse kyseiseen sivuun liittyvää.

Käytin sivujen valinnassa kieltä päätekijänä .fi-päätetunnuksen lisäksi. Tarkastelin, oliko verkkosivuston ja evästekyselyn sisältö tuotettu joko suomeksi tai ruotsiksi. Taulukko vierailluista sivustoista löytyy liitteestä 1. Kaikilla sivustoilla vierailtiin marraskuussa 2023. Aineistosta löytyy useita uutismedioita, eri kaupunkien sivustoja, teleoperaattoreita sekä verkkokauppoja. Mukana on sekä julkisia toimijoita että kaupallisia. Suurin osa verkkosivustoista on hyvin tunnettuja, vain muutama on selvästi tuntemattomampia.

## 6.2 Analyysimenetelmä

Käytin pimeiden käytäntöjen luokittelemiseksi Martini ja Drewsin (2022) sekä Soe ym. (2020) pohjalta koostamaani listaa (taulukko 6.). Alun perin

[1] Saatavilla: https://tranco-list.eu/list/6J33X/full

tarkoituksena oli käyttää Mathur ym. (2021) yläkäsitetaulukkoa. Se kuitenkin käsitteli kaikkia pimeitä käytäntöjä ja sen luokkien välillä oli päällekkäisyyttä. Liian moni evästekyselyistä löytyvä pimeä käytäntö voisi päätyä samaan luokkaa. Näiden seikkojen vuoksi tulin siihen tulokseen, että Mathur ym. (2021) yläkäsitteisiin perustuvat taulukko ei olisi paras mahdollinen lähtökohta tutkimukselleni. Martini ja Drewsin (2022) ja Soe ym. (2020) artikkelit puolestaan käsittelivät juuri evästekyselyissä löytyviä pimeitä käytäntöjä, jolloin on mahdollista jakaa pimeät käytännöt tarkempiin luokkiin.

TAULUKKO 6. Listaus pimeiden käytäntöjen arviointiin evästekyselyissä

| **Pimeä käytäntö** | **Kyllä/Ei** |
|---|---|
| Sivustolla useampi evästekysely | |
| Vaihtoehdot esitetty eriarvoisesti | |
| Valintojen kaskadi | |
| Merkkaamattomat liukusäätimet | |
| Merkitsemätön X | |
| Ei antonyymeja | |
| Ei vaihtoehtoa | |
| Oletusvalinnat | |

Ensimmäinen taulukon listauksessa oleva pimeä käytäntö on useiden evästekyselyiden esiintyminen samalla verkkosivulla. Tällöin käyttäjän on hankala tietää mikä kyselyistä oikeasti tallentaa käyttäjän tekemät valinnat. Toisena on vaihtoehtojen esittäminen eriarvoisesti. Tällä tarkoitetaan esimerkiksi sitä, että hyväksy-vaihtoehtoa korostetaan visuaalisesti. Kolmantena olevassa ”Valintojen kaskadissa” käyttäjä ei pysty hylkäämään evästeitä yhdellä klikkauksella vaan joutuu siirtymään esimerkiksi asetukset-painikkeen kautta toisella sivulle. ”Merkkaamattomat liukusäätimet” tarkoittaa sitä, että evästekyselyssä on liukusäätimiä, joiden avulla käyttäjä voi hallita evästeasetuksia, mutta niihin ei ole selkeästi merkattu, milloin asetukset ovat päällä ja milloin pois päältä. ”Merkitsemätön X” tarkoittaa, että evästekyselystä löytyy sulkemiseen tarkoitettu rasti (yleensä oikeassa yläkulmassa), mutta kyselyssä ei kerrota, tarkoittaako sen painaminen evästeiden hyväksymistä vai hylkäämistä. ”Ei antonyymejä” tarkoittaa, että sen sijaan, että olisi käytetty vastakkaisia ilmauksia esim. sanoille *Hyväksy* tai *Salli* on käytetty ilmauksia kuten *Tallenna valinnat* tai *Hallitse asetuksia*. ”Ei vaihtoehtoa” tarkoittaa, että käyttäjän on pakko hyväksyä evästeet, jos hän haluaa jatkaa sivustolle. ”Oletusvalinnat” tarkoittaa valmiiksi tehtyjä oletusvalintoja esimerkiksi valmiiksi rastitettuja ruutuja kuten kuvassa 1. Yhdessä evästekyselyssä voi esiintyä useampi pimeä käytäntö.

Listauksesta jäivät pois Soe ym.:n (2020) luokka ”Huomiotta jättäminen” ja Martini ja Drewsin (2022) ”Ruinaaminen”. ”Huomiotta jättäminen” jäi pois koska tutkimuksen puitteissa ei ole mahdollista tutkia asettavatko sivustot evästeitä käyttäjän kiellosta huolimatta. Martini ja Drewsin (2022) luokka ”Ruinaaminen” jäi pois, koska käytäntöä on hankala todentaa. Sen todentaminen, että

esittääkö sivusto evästekyselyn uudelleen, jos evästeitä ei hyväksytä olisi vaatinut, että sivustolla vierailua jatketaan, jos ja kunnes kysely esitetään uudestaan.

Jos sivuston ensimmäisessä käyttöliittymässä oli sekä hyväksy- että hylkää -vaihtoehto samanarvoisina ja antonyymein ilmaistuna, en lähtenyt enää tutkimaan, kuinka mahdolliset lisäasetukset oli esitetty tai miten niihin pääsi käsiksi, vaan katsoin että sivuston evästekyselyssä ei ilmennyt pimeitä käytäntöjä. Koska pidin epätodennäköisenä, että pimeitä käytäntöjä esiintyy tällöin evästekyselyssä (Kuva 3).


Kuva 3. Kuvakaappaus evästekyselystä, jossa molemmat vaihtoehdot esitetty samanarvoisina. (Lähde: yle.fi)

Rajoittavaksi toiminnaksi (ja siten pimeäksi käytännöksi) en myöskään laskenut, jos sivusto ei päästänyt etenemään ennen kuin evästevalinnat on tehty, jos käyttäjällä oli mahdollisuus kieltäytyä evästeistä. Koska rekisterinpitäjän on pyydettävä suostumus ennen tietojen käsittelyä (Tietosuojavaltuutetun toimisto, ei pvm.-c), ei sivustoilla välttämättä ole muuta mahdollisuutta kuin estää sivustolle pääsy, jotta ne saisivat käyttäjät reagoimaan evästekyselyyn. Toisaalta tämän voitaisiin laskea pimeäksi käytännöksi, koska välttämättömien evästeiden asettamiseksi ei tarvita kyselyä, joten käyttäjä voidaan pakottaa tekemään tarpeettomasti valinta.

Analyysin tekemiseen käytettiin Windows-käyttöjärjestelmää ja Google Chrome -selainta, jonka historiatiedot oli tyhjennetty ja jonka kieleksi oli valittu suomi.

# 7 TULOKSET

Tässä luvussa käydään tarkemmin läpi laadullisen analyysin tulokset. Ensin tarkoituksenani oli analysoida aineisto käyttäen Mathur ym.:n (2021) yläkäsitteisiin perustuvaa luokittelua. Ensimmäisessä kappaleessa käydään läpi, miksi ratkaisu ei toiminut. Varsinaisissa tuloksissa käydään läpi, millaisia havaintoja tehtiin ja kuinka paljon kutakin pimeää käytäntöä löytyi määrällisesti. Lopuksi tuloksia verrataan aikaisempien tutkimusten tuloksiin.

## 7.1 Ensimmäinen analyysi

Tarkoituksena oli ensin käyttää tutkimuksen pohjana Mathur ym.:n (2021) laatimaa yläkäsitteisiin perustuvaa taulukkoa (Taulukko 2.). Aineiston läpikäytyäni huomasin kuitenkin, että useimmat pimeät käytännöt menivät samaan luokkaan – asymmetrisiin pimeisiin käytäntöihin. Mathur ym.:n (2021) mukaa asymmetrisessä pimeässä käytännössä valinnat esitetään käyttäjälle eriarvoisella tavalla. Lisäksi tähän luokkaan voidaan laskea kuuluvaksi sellaiset keinot, jotka piilottavat käyttäjää suosivat asetukset valikoiden taakse (Mathur ym., 2021). Lähes kaikki kohtaamani pimeät käytännöt voitiin siis luokitella asymmetrisiksi. Lisäksi, koska luokkaan kuului asetusten piilottaminen valikoiden taakse, saattoi samassa evästekyselyssä esiintyä kaksi pimeää käytäntöä, jotka kuuluivat samaan luokkaan. Tällöin evästekyselyssä korostettiin hyväksy -vaihtoehtoa ja evästeiden hylkäys mahdollisuus oli piilotettu linkin taakse (esimerkiksi kuva 5.). Luokkien yläkäsitteisiin perustumisen vuoksi pimeitä käytäntöjä oli vaikea erottaa toisistaan. Tämän takia päädyin laatimaan taulukon Soe ym.:n (2020) ja Martinin ja Drewsin (2022) evästekyselyihin perustuvien artikkeleiden pohjalta ja käyttämään sitä tutkimukseni pohjana (taulukko 6.).

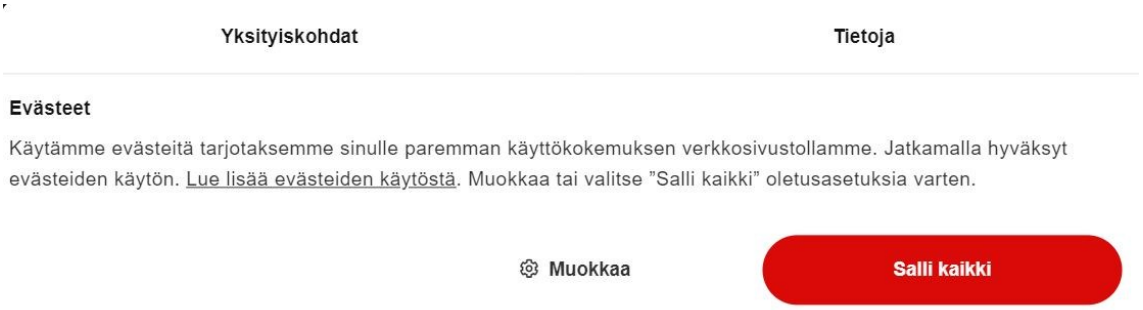
## 7.2 Tulkintaa ja havaintoja

Jokaisella sivulla vierailtiin erikseen liitteessä 1 esitetyssä numerojärjestyksessä. Ensin tarkasteltiin, oliko vaihtoehdot esitetty eriarvoisesti. Oliko sen hyväksy -painike visualisesti houkuttelevampi tai korostetumpi verrattuna muihin? Jos näin mielestäni oli, merkkasin, että sivustolla oli esitetty vaihtoehdot eriarvoisesti. Vaihtoehtojen esittäminen eriarvoisesti oli erittäin yleistä ja havaitsemistani pimeistä käytännöistä yleisin. Kyselyissä korostettiin nimenomaan hyväksyvaihtoehtoa. En tavannut yhtään evästekyselyä, jossa hylkää-vaihtoehto olisi ollut korostetumpi. Yhden sivuston kohdalla, en ollut varma oliko kyseessä pimeä käytäntö vai pelkästään esteettinen valinta. *Salli kaikki evästeet* -painike oli sinisellä pohjalla ja *Salli vain välttämättömät* –painike valkoisella (kuva 4.). Voidaan argumentoida, että evästeiden hyväksymiseen tarkoitettu painike on korostetumpi, joten laskin sen mukaan.


Kuva 4. Esimerkki epäselvästä tilanteesta onko kyseessä pimeä käytäntö. (Lähde: ilmatieteenlaitos.fi)

Seuraavaksi tarkastelin, oliko evästekyselyä mahdollista sulkea ja jos oli, oliko missään ilmoitettu tarkoittaako sulkeminen evästeiden hyväksymistä vai hylkäämistä. Evästekyselyitä ei ollut yleensä mahdollisuutta sulkea rastista. Se puuttui kyselystä yleensä kokonaan. Asetuksia klikkaamalla avautui usein uusi ikkuna, joka oli mahdollisuus sulkea rastista, mutta rastin painaminen ei sulkenut koko evästekyselyä vaan palautti käyttäjän ensimmäiseen evästekyselyyn.

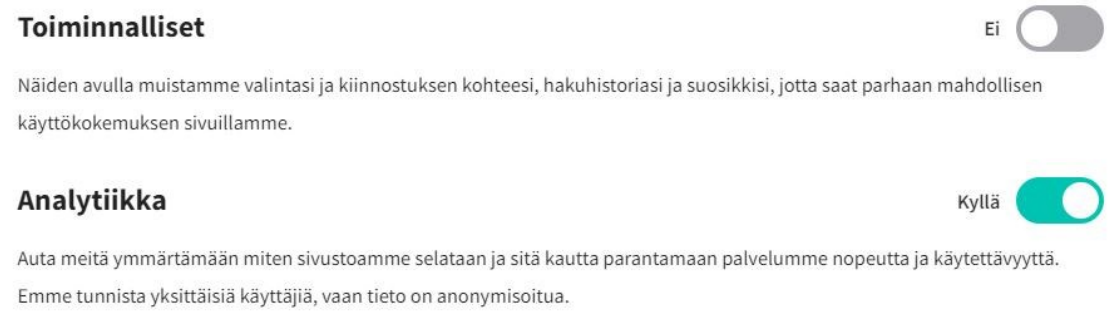
Sen jälkeen tarkastelin, pystyykö käyttäjä kieltämään kaikki, paitsi välttämättömät evästeet, ensimmäisenä ruudulle ilmestyvästä evästekyselystä. Yleisenä käytäntönä oli ohjata käyttäjä asetukset tai lisätietoja -linkin taakse, jotta evästeet pystyi kieltämään (Kuva 5). Valintojen kaskadi -pimeä käytäntö oli käytössä melkein puolella tutkittujen sivustojen evästekyselyissä.




Kuva 5. Esimerkki siitä kuinka evästeet on helppo hyväksyä, mutta niiden kieltäminen on piilotettu muokkaa -valikon taakse(Lähde: vikingline.fi)

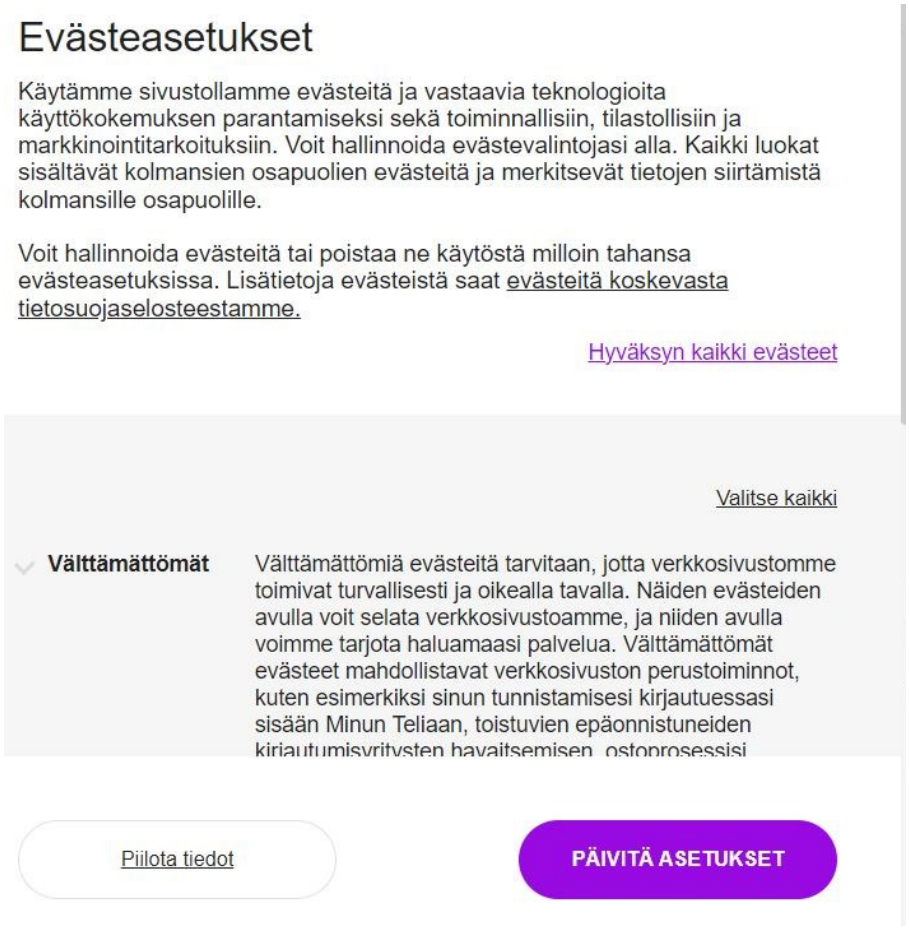
Seuraavaksi tarkastelin, millaiset vaihtoehdot löytyivät muokkaa/asetukset/lisätietoja painikkeen tai linkin takaa. Lähes kaikilta löytyi mahdollisuus säätää yksittäisiä evästeitä tai hyväksyä tai hylätä ne kokonaan. Jos evästekyselyssä oli esitetty ensimmäiset vaihtoehdot eriarvoisesti, kävin katsomassa asetuksista, löytyykö evästekyselystä merkkaamattomia liukusäätimiä, myös silloin kun toinen vaihtoehto oli muiden kuin välttämättömien evästeiden hylkääminen. Oli harvinaista, että käyttäjä olisi pystynyt säätämään asetuksia ensimmäisenä näyttöön tulevasta evästekyselystä.

Merkkaamattomien liukusäätimien tulkinta osoittautui hankalaksi. Riittääkö, että liukusäädin vaihtaa väriä? Onko värillä väliä esim. sininen verrattuna vihreä? Alla on esimerkkikuva hyvin merkatuista liukusäätimistä (Kuva 6.). Päädyin siihen ratkaisuun, että jos liukusäätimiä ei ollut merkattu mitenkään muuten kuin värein, tulkitsin ne epäselvästi merkatuiksi.



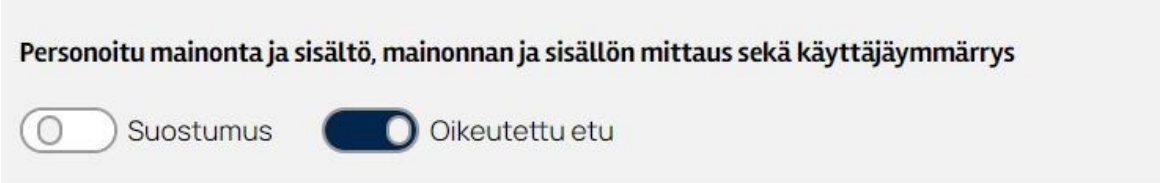

Kuva 6. Esimerkkikuva selkeästi merkatuista liukusäätimistä (Lähde: duunitori.fi)

Noin parikymmentä sivustoa ei myöskään käyttänyt antonyymejä. Ne esittivät sen sijaan evästeiden hyväksymisen vastakohtana ilmauksia kuten ”Hyväksy valitut”, ”Vahvista valinnat”, ”Päivitä asetukset”, ”Jatka valituilla”, ”Päivitä suostumus”, ”Tallenna asetukset”, ”Salli valinta”, ”Tallenna evästevalinnat”, ”Tallenna ja sulje” tai ”Tallenna muutokset” (esimerkkikuva Kuva 7.). Käyttäjälle näyttää siis siltä, että mikään vaihtoehdoista ei mahdollista evästeiden hylkäämistä. Ilmaukset jättävät käyttäjälle epäselväksi millaiset asetukset tallentuvat, ellei hän käy jokaista asetusta erikseen läpi.




Kuva 7. Esimerkki evästekyselystä, jossa ei tarjota lainkaan vaihtoehtoa, jonka avulla voisi hylätä yksiselitteisesti kaikki paitsi välttämättömät evästeet. Huomattavaa on, että tässä esimerkissä *Päivitä asetukset* -vaihtoehto on korostetumpi kuin *Hyväksyn kaikki evästeet* -vaihtoehto. Esimerkkikuva on evästekyselyn asetukset valikon takaa avautuvasta kyselystä. (Lähde: telia.fi)

Asetusten takaa löytyvät useimmiten myös valmiiksi tehdyt oletusvalinnat. Valmiiksi tehdyt oletusvalinnat olivat harvinaisempia kuin oletin. Varsinaisiin valmiiksi tehtyihin valintoihin en törmännyt kuin muutaman sivuston kohdalla. Hankalampi kysymys oli kuitenkin oikeutettu etu (eng. legitimate interest), jota löytyi varsinkin uutissivustojen evästekyselyistä oletusvalintana. (Kuva 8.)



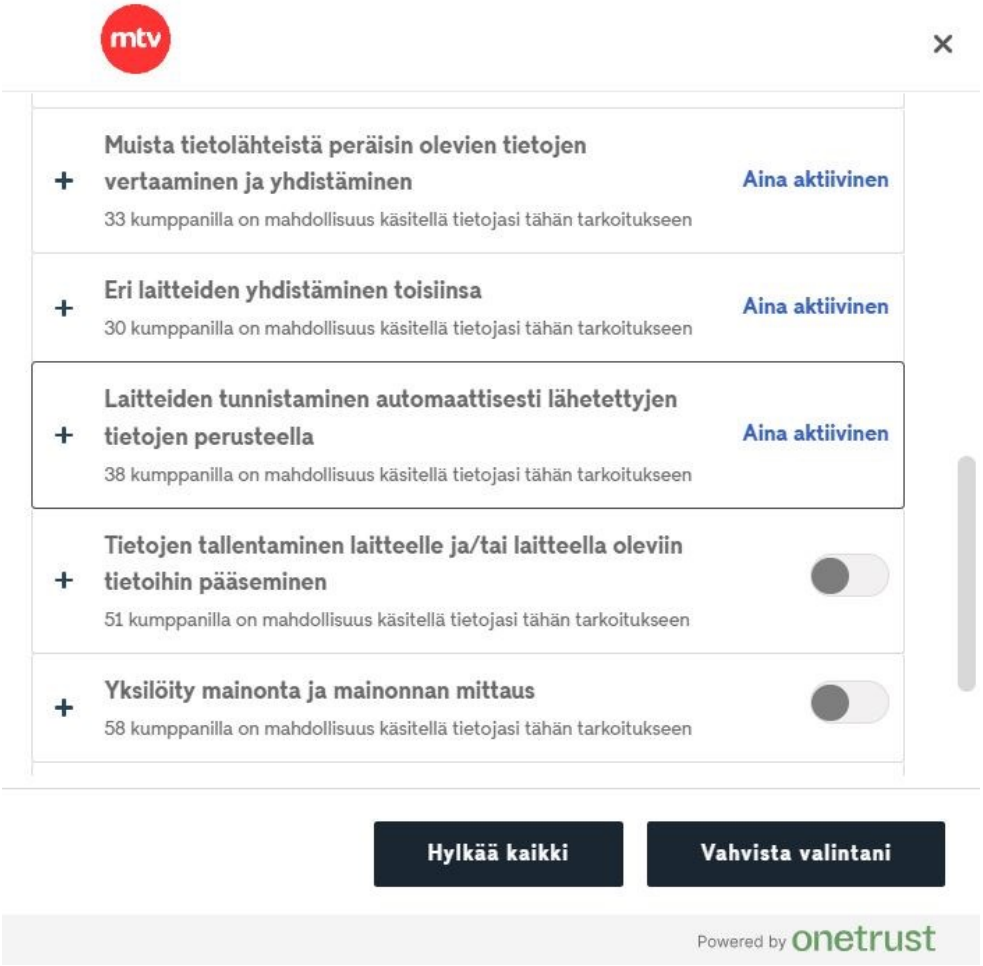

Kuva 8. Erityisesti uutisia tarjoavien sivustojen evästeasetuksista saattoi löytää valmiiksi valittuna kohdan oikeutettu etu. (Lähde: verkkouutiset.fi)

Oikeutetusta edusta on kyse, *"kun tietojenkäsittely tapahtuu asiakassuhteessa, kun se käsittelee tietoja suoramarkkinointitarkoituksissa, petoksen estämiseksi tai IT-*

*järjestelmien verkon ja tietoturvan varmistamiseksi*."(Euroopan komissio, ei pvm.) Mutta palveluntarjoajan on varmistettava, että "*oikeutetun edun mukainen toiminnasta ei aiheudu vakavaa haittaa kyseisten yksilöiden oikeuksille ja vapauksille*." (Euroopan komissio, ei pvm.) Jos näin tapahtuu, palveluntarjoajan on löydettävä toinen oikeusperusta (Euroopan komissio, ei pvm.). Tietosuojavaltuutetun toimiston sivuilta löytyy taas tieto, jonka mukaan "*Henkilötietoja ei saa käsitellä, jos rekisteröidyn edut tai oikeudet syrjäyttävät rekisterinpitäjän tai kolmannen osapuolen edun.*" (Tietosuojavaltuutetun toimisto, ei pvm.-b). Kuinka nämä oikeudet sitten määritellään? " *Rekisterinpitäjän oikeutettujen etujen vaikutus rekisteröidyn etuihin ja oikeuksiin muodostaa liukuvan skaalan. Oikeutettuun etuun liittyvät intressit voivat vaihdella merkityksettömistä melko tärkeisiin ja jopa pakottaviin, ja vaikutukset rekisteröidyn etuihin ja oikeuksiin voivat vaihdella enemmän tai vähemmän huomattavista vakaviin.*" (Tietosuojavaltuutetun toimisto, ei pvm.-b).

On siis vaikea sanoa, onko sivustoilla oikeus kerätä tietoja oikeutetun edun perusteella vai ei. Laskin kuitenkin kyseiset valmiiksi valitut oikeutetut edut oletusvalintoihin. Sillä ne sai myös kytkettyä usein pois päältä. Laskin nämä myös siksi valmiiksi tehdyiksi oletusvalinnoiksi, koska vaikka käytäntöä esiintyi uutissivustoilla, osa oli jättänyt oikeutetun edun valitsematta valmiiksi Se minulle ei selvinnyt, että jos valitsi evästeiden hylkäämisen, tarkoittiko se myös näiden valmiiksi valittujen oikeutettu etu tyyppisten evästeiden hylkäämistä.

En havainnut, että yksikään sivustoista olisi pakottanut käyttäjän hyväksymään kaikkia evästeitä. Muutamalla sivustolla osaa valinnaisista evästeistä ei saanut kytkettyä pois päältä (esimerkiksi kuva 9). Laskin nämä kohtaan ei vaihtoehtoa. Useimmilla sivustoilla käyttäjän piti tehdä evästevalinnat ennen kuin pääsi etenemään sivuille, mutta valinnat mahdollistivat evästeiden hylkäämisen. Yksi sivustoista otti kannan, jonka mukaan sivuston käyttäminen tarkoittaa evästeiden hyväksymistä. En myöskään havainnut, että yhdelläkään sivustolla olisi ollut käytössään useampia evästekyselyitä.




Kuva 9. Esimerkkikuva evästekyselystä, joka ei mahdollista kaikkien ei välttämättömien evästeiden hylkäämistä (Lähde: mtvuutiset.fi)

## 7.3 Keskeiset tulokset

Aineiston analysointiin käytettiin Soe ym.:n (2020) ja Martinin ja Drewsin (2022) artikkeleiden pohjalta laatimaani taulukkoa (Taulukko 6.). Vierailtuani sadalla sivustolla (Liite 1.) keskeisimmät tulokset on koostettu taulukkoon 7. Keskimäärin pimeitä käytäntöjä ilmeni sivuilla 2 kpl.

Pimeistä käytännöistä selvästi eniten ilmeni vaihtoehtojen esittämistä eriarvoisesti, 73 evästekyselyssä oli keino käytössä. Toiseksi eniten havaittu pimeä käytäntö oli valintojen kaskadi (44). Evästeiden hylkäämisvaihtoehto oli piilotettu linkin tai painikkeen taakse. Käyttäjä joutui siis tekemään useamman klikkauksen, jos halusi hylätä evästeet, kun taas kaikissa evästekyselyissä oli mahdollista hyväksyä evästeet yhdellä klikkauksella.

Merkkaamattomien liukusäätimien tulkinta oli välillä hieman hankalaa. Yleisin tapa indikoida, että säätimen asentoa on vaihdettu, oli sen värin vaihdos.

Koska löysin myös selkeästi merkattuja liukusäätimiä, tulkitsin pelkästään väriä vaihtavat huonosti merkityiksi. Liukusäätimet eivät kuitenkaan olleet yleisin tapa mahdollistaa käyttäjälle valintojen tekeminen, valintaruudut olivat suositumpia. Merkkaamattomia liukusäätimiä oli noin kolmasosassa (32) evästekyselyistä.

Oletusvalintana tehdyt valinnat oli perusteltu yleensä oikeutetulla edulla. Suoraa vastausta milloin sivustolla on oikeus kerätä käyttäjästä tietoja oikeutetun edun perusteella en löytänyt. Muita kuin oikeutetun edun nimissä tehtyjä oletusvalintoja en nähnyt kuin parilla sivulla. Yhteensä valmiiksi tehtyjä oletusvalintoja löytyi 20 kyselystä.

Selkeitä antonyymejä evästekyselyissään ei käyttänyt 17 sivustoa. Tallenna asetukset -tyyppisten ilmaisujen käyttäminen jättää käyttäjälle epäselväksi mitkä asetuksista hän lopulta hyväksyy. Vähiten havaitsin pimeää käytäntöä ”ei vaihtoehtoa” (3). Evästeet oli mahdollisuus yleensä hylätä. Vain muutamalla sivustolla oli oletusvalintana muita kuin välttämättömiä evästeitä, joiden valintaa ei pystynyt poistamaan. Useilla sivustoilla evästevalinnat piti suorittaa ennen kuin sivustolle pääsi etenemään. En kuitenkaan laskenut tätä pimeäksi käytännöksi, jos evästeet pystyi hylkäämään. Kaikkein käyttäjäystävällisin vaihtoehto se ei kuitenkaan ole.

Pimeitä käytäntöjä, joita en havainnut olivat ”Merkitsemätön X” ja ”Sivustolla useampi evästekysely”. Evästekyselyitä ei yleensä ollut mahdollista sulkea rastista, joten en myöskään havainnut, että tähän liittyvää pimeää käytäntöä olisi esiintynyt. Yhdelläkään sivustolla ei myöskään ollut käytössä useampaa evästekyselyä.

TAULUKKO 7. Yhteenveto kuinka paljon kutakin pimeää käytäntöä esiintyi

| **Pimeä käytäntö** | **Kpl** |
|---|---|
| Vaihtoehdot esitetty eriarvoisesti | 73 |
| Valintojen kaskadi | 44 |
| Merkkaamattomat liukusäätimet | 32 |
| Oletusvalinnat | 20 |
| Ei antonyymeja | 17 |
| Ei vaihtoehtoa | 3 |
| Merkitsemätön X | 0 |
| Sivustolla useampi evästekysely | 0 |

Tutkittuja sivustoja oli yhteensä sata. Näistä sivustoista 95 esitti evästekyselyn ja 76 evästekyselyssä esiintyi yksi tai useampi pimeä käytäntö. 19 evästekyselystä en löytänyt pimeitä käytäntöjä. Tässä joukossa korostuivat valtion ja kuntien sivustot, niissä hylkää ja hyväksy vaihtoehdot esitettiin ensimmäisessä kyselyssä samanarvoisina. Sivustoista viisi ei esittänyt evästekyselyä ja ne kaikki olivat valtiollisia toimijoita esim. vero.fi. Näillä sivustoille ei siis ilmennyt pimeitä käytäntöjä tämän luokittelun mukaan. Yhteensä sivustoja, joilla ei esiintynyt pimeitä käytäntöjä on siis 24. Pitää ottaa huomioon, että vaikka evästekyselyä

ei esiintynyt sivustot voivat asettaa silti evästeitä ns. huomiotta jättäminen, jota ei tämän tutkimuksen puitteissa tarkasteltu. Samaan konserniin kuuluvat sanomalehdet käyttivät samanlaista evästekyselyä, joten niissä kaikissa ilmenivät samat pimeät käytännöt.

Tulokset viittaavat siihen, että suomalaisten verkkosivustojen evästekyselyissä esiintyy pimeitä käytäntöjä yleisesti. Vaikka pimeät käytännöt eivät välttämättä ole lakien tai asetusten vastaisia voivat ne kuitenkin aiheuttaa käyttäjälle haittaa, evästekyselyiden tapauksessa esimerkiksi heikompina yksityisyysasetuksina.

## 7.4 Tulosten vertaaminen aikaisempiin tutkimuksiin

Tämän tutkimuksen yleisin pimeä käytäntö, vaihtoehtojen esittäminen eriarvoisesti, oli yleinen myös aiemmissa tutkimuksissa. Tässä tutkimuksessa tätä pimeää käytäntöä havaittiin 73 evästekyselyssä, koska sivustoista 95 esitti evästekyselyn, saadaan, että noin 77 % evästekyselyistä esitti vaihtoehdot eriarvoisesti. Krisam ym. (2021) tutkivat 500 saksalaisia verkkosivustoista niillä sivustoilla, joilla oli evästekysely, 85 %:lla oli tämä keino käytössään (Krisam ym., 2021). Samanlaisia tuloksia saivat Kampanos ja Shahandasti (2021). Heidän tutkimuksessaan selvisi, että 75 % kreikkalaisista evästekyselyistä ja 82 % Iso-Britannialaisista kyselyistä yritti ”tuupata” käyttäjää hyväksymään evästeet (Kampanos & Shahandashti, 2021). Liettuassa tehdyssä tutkimuksessa tämän pimeän käytännön prosenttiosuus oli paljon matalampi (28 %) (Limba ym., 2021). Pientä osuutta selittää osittain se, että vain 28 %:lla sivustoista oli käytössä sellainen evästekysely, joka mahdollisti valintojen tekemisen (Limba ym., 2021). Utz ym.:n (2019) tutkivat puolestaan 1000 sattumavaraista evästekyselyä Euroopan unionin jäsenmaista. Heidän tutkimuksessaan 57 % evästekyselyistä käytti tätä keinoa. He tosin jatkavat, että määritelmästä riippuen, määrä saattaa olla vielä suurempikin (Utz ym., 2019). Prosenttiosuudet ovat siis suhteellisen samanlaisia Liettuaa ja yleiseurooppalaista tutkimusta lukuun ottamatta. Tuloksia on verrattu taulukossa 8.

TAULUKKO 8. Vaihtoehtojen esittäminen eriarvoisesti. Vertailua alueiden välillä

| Maa tai alue | Määrä | Lähde |
|---|---|---|
| Saksa | 85 % | (Krisam ym., 2021) |
| Iso-Britannia | 82 % | (Kampanos & Shahandashti, 2021) |
| Kreikka | 75 % | (Kampanos & Shahandashti, 2021) |
| Euroopan unioni | 57 % | (Utz ym., 2019) |
| Liettua | 28 %* | (Limba ym., 2021) |

* 45 % sivustoista ei anna muuta mahdollisuutta kuin hyväksyä evästeet, 27 %:lla ei ole evästekyselyä lainkaan (Limba ym., 2021)

Mahdollisuus evästeiden hylkäämiseen piilotetaan usein valikoiden taakse. Evästeiden hylkääminen yhdellä klikkauksella oli mahdollista 56

evästekyselyssä. Myös Soe ym.:n (2020) havaitsivat tutkimuksessaan, että kaikilla verkkosivustoilla oli mahdollisuus hyväksyä evästeet yhdellä klikkauksella. Evästeiden hylkääminen puolestaan oli mahdollista vain 15:lla tutkitusta 300:sta sivustosta (Soe ym., 2020). Krisam ym. (2021) havaitsivat puolestaan tutkiessaan, että vain 21.5 % kyselyistä mahdollisti evästeiden hylkäämisen yhdellä klikkauksella. Tässä tutkimuksessa havaittu mahdollisuus hylätä evästeet yhdellä klikkauksella on selvästi suurempi kuin Soe ym.:n (2020) tai Krisam ym.:n (2021) tutkimuksessa.

Mikä voidaan tulkita liukusäätimien huonosti merkitsemiseksi, oli joidenkin kyselyiden kohdalla hieman tulkinnanvaraista. Käytäntöä löytyi 32 evästekyselystä. Samanlaisen pimeän käytännön havaitsivat Soe ym. (2020). He eivät kuitenkaan erittele tarkemmin, kuinka monella sivustolla käytäntö esiintyi. Se oli käytäntö, jonka he havaitsivat käydessään aineistoa läpi. En löytänyt mainitaan kyseisestä käytännöstä muista tutkimuksista. Tämä johtuu luultavasti siitä, että asiaan ei ole aikaisemmin kiinnitetty huomiota.

Valmiiksi tehtyjä oletusvalintoja löytyi 20 evästekyselystä. Luvussa ovat mukana myös niin sanotut ”oikeutettu etu” -valinnat, joita löytyi erityisesti uutissivustoilta. Prosenttiosuus on noin 21 % niistä sivustoista, jotka esittivät evästekyselyn. Liettualaisia sivustoja tutkiessaan Limba ym. (2021) havaitsivat, että 64 %:ssa evästekyselyistä oli valmiiksi rastitettuja kenttiä (Limba ym., 2021). Limba ym.:n (2021) tekemä havainto on siis paljon korkeampi.

Antonyymien puute tai asian ilmaiseminen epäselvästi vaivasi 17 evästekyselyä. Evästeiden hylkäämisen sijasta tarjottiin esimerkiksi asetusten tallentamista. Tämä oli toinen pimeä käytäntö, josta en löytänyt kuvausta kuin Soe ym.:n (2020) tutkimuksesta. Samalla tavalla kuin huonosti merkatuista liukusäätimistä tästäkään ei ole tarkempia lukuja, vaan se oli havainto, jonka Soe ym. tekivät tehdessään tutkimusta.

Käyttäjälle annettiin mahdollisuus hylätä evästeet lähes kaikissa tapauksissa. Tässä tutkimuksessa vain kolme sivustoa pakotti hyväksymään evästeet. Tällöin käyttäjä pakotettiin hyväksymään osa evästeitä. Piiloon voi kuitenkin jäädä se, että sivusto asettaa evästeitä käyttäjän tietämättä. Aiemmin mainitussa liettualaisessa tutkimuksessa Limba ym. (2021) mukaan vain 28 % evästekyselyistä mahdollisti käyttäjälle evästeiden hylkäämisen. Irlantilaisessa tutkimuksessa Sheil ja Malone (2022) taas havaitsivat, että 76 % evästekyselyissä oli vain hyväksy -vaihtoehto.

Pimeitä käytäntöjä, joita ei havaittu tässä tutkimuksessa, olivat useampi evästekysely samalla sivulla ja ”merkitsemätön x” eli mahdollisuus evästekyselyn sulkemiseen ilman selitystä. Näitä pimeitä käytäntöjä ei myöskään mainittu muissa kuin Soe ym.:n (2020) tekemässä tutkimuksessa. Näistä en löytänyt lukuja vertailtavaksi.

# 8 PÄÄTÄNTÖ

Päätännössä vedetään yhteen tutkimuksen tarkoitus, käytetty aineisto ja tulokset sekä käydään läpi tutkimuksen luotettavuuteen ja rajoituksiin liittyviä seikkoja. Onnistuttiinko tutkimuskysymykseen vastaamaan ja minkälaisia mahdollisia vaikutuksia tuloksilla on?

## 8.1 Tulosten koonti ja pohdinta

Tutkimuksen lähtökohtana oli evästekyselyt ja niissä esiintyvät pimeät käytännöt. Evästekyselyiden suunnitteluun ja niiden esiintymiseen vaikuttaa EU:n yleinen tietosuoja-asetus (Asetus 2016/679, 2016). Asetuksen mukaan palvelun tuottajalla tulee olla käyttäjän suostumus tämän tietojen keräämiseen ja käsittelyyn. Evästekyselyiden avulla palveluntarjoajat tallentavat käyttäjän suostumuksen. Evästeet mahdollistavat yksilöllisen profiilin muodostamisen käyttäjästä. Profiilia voidaan tämän jälkeen käyttää persoonallistettuun markkinointiin, jonka vuoksi palvelun tuottajalla on kannustin kerätä käyttäjästä mahdollisimman paljon tietoja (Zuboff, 2019, s. 208–211). Kun taas käyttäjän tulee miettiä asiaa oman yksityisyytensä kannalta (Culnan & Armstrong, 1999). Palvelun tarjoajat käyttävätkin usein pimeitä käytäntö saadakseen käyttäjät hyväksymään asetukset, jotka voivat olla käyttäjän yksityisyyden kannalta haitalliset.

Tutkimuskysymyksenä oli ”Millaisia pimeitä käytäntöjä löytyy suomalaisten verkkosivustojen evästekyselyistä?”. Kysymykseen pyrittiin vastamaan perehtymällä ensin aikaisempaan tutkimukseen ja niissä tunnistettuihin pimeisiin käytäntöihin. Tutkimuksen tuloksena havaittiin, että pimeälle käytännölle ei ole yhtä tiettyä määritelmää, mutta ne ovat usein keinoja, joilla suunnittelijat yrittävät saada käyttäjän toimimaan tämän omia etujaan vastaan. Pimeitä käytäntöjä

voidaan luokitella monella eri tavalla. Yksi kattavimmista luokitteluista on Mathur ym. (2021) luoma yläkäsitteisiin perustuva luokittelu. Sen ongelmaksi tutkimuksen kannalta paljastui kuitenkin luokkien laajuus. Se vastasi pikemminkin kysymyksen, minkä laatuisia kuin millaisia.

Päädyin luokittelemaan pimeät käytännöt käyttäen pohjana Soe ym. (2020) ja Martini ja Drewsin (2022) artikkeleita, jotka käsittelivät evästekyselyissä esiintyviä pimeitä käytäntöjä. Soe ym. (2020) olivat tutkimuksessaan havainneet myös ennen tunnistamattomia pimeitä käytäntöjä, jotka liittyivät juuri evästekyselyihin esimerkiksi sen, että sivusto esittää useamman evästekyselyn. Näiden artikkeleiden pohjalta luotiin luokittelu (taulukko 6.), jota käytettiin evästekyselyistä löytyvien pimeiden käytäntöjen tunnistamiseen. Aineistona käytettiin Trancolist.eu sivustolta saatavissa olevaa listausta miljoonasta maailman suosituimmasta verkkosivusto-osoitteesta, joka oli koostettu elokuussa 2023. Listauksesta suodatettiin ensimmäiset sata sopivaa suomalaista verkkosivustoa (liite 1.). Huomattavaa on, että sata ensimmäistä ei tarkoita sataa suosituinta. Trancon listaus on koostettu viidestä muusta eri listauksesta, käyttäen erilaisia tilastollisia parametreja (Le Pochat ym., 2019; Tranco, ei pvm.).

Teoriapohjana toimivat valintamuotoilu ja privacy calculus -teoria. Valintamuotoilu pohtii suunnittelijoiden tekemiä ratkaisuja, kun taas privacy calculus -teoria pohtii käyttäjän tekemiä valintoja. Valintamuotoilun on tarkoitus ohjata suunnittelijoita rakentamaan sellaisia ratkaisuja, jotka hyödyttävät käyttäjää (Thaler & Sunstein, 2008). Mutta sitä voidaan käyttää vastakkaiseen tarkoitukseen ja usein sitä käytetään juuri näin evästekyselyiden kohdalla. Tällöin voidaan puhua pimeistä tuuppauksista (Graßl ym., 2021). Privacy calculus -teorian mukaan käyttäjän valintoihin evästeitä valittaessa pitäisi vaikuttaa se kokeeko käyttäjä saavansa enemmän hyötyä, jos hän valitsee enemmän evästeitä (Graßl ym., 2021). Käyttäjät eivät kuitenkaan jokapäiväisessä elämässään välttämättä pohdi tällaisia valintoja (Gerber ym., 2018).

Tutkimuksessa havaittiin, että pimeitä käytäntöjä esiintyy suomalaisten verkkosivustojen evästekyselyissä. Tässä tutkimuksessa 95 sivustoa sadasta esitti evästekyselyn. Evästekyselyistä 76:ssa oli jokin luokittelun (taulukko 6.) mukainen pimeä käytäntö, joten noin 80 %:ssa evästekyselyistä esiintyi jokin pimeä käytäntö. Kolme eniten havaittua pimeää käytäntöä olivat: vaihtoehtojen esittäminen eriarvoisesti, valintojen kaskadi ja merkkaamattomat liukusäätimet.

Yleisin pimeä käytäntö oli vaihtoehtojen esittäminen eriarvoisesti, joka löytyi 73 evästekyselystä. Tämä pimeä käytäntö oli myös yleinen muissa tutkimuksissa mm. kreikkalaisista evästekyselyistä 75% käytti keinoa ja 82% Iso-Britannialaisista kyselyistä (Kampanos & Shahandashti, 2021). Luvut ovat korkeampia kuin Utz ym.:n (2019) havainto. He tutkivat 1000 sattumavaraista evästekyselyä Euroopan unionin jäsenmaista. Heidän mukaansa 57 % evästekyselyistä houkuttelee käyttäjiä hyväksymään evästeet (Utz ym., 2019). Yksi syy, miksi tulokset eroavat Utz ym. (2019) tutkimuksen tuloksista, voi olla se, että kohdennetut tutkimukset tavoittavat paremmin pimeät käytännöt tai se, että käytännöt vaihtelevat suuresti eri maiden välillä, jolloin keskiarvo on pienempi.

Vaikuttako vaihtoehtojen esittäminen eriarvoisesti sitten käyttäjien valintoihin? Bouma-Sims ym.:n (2023) tekemän tutkimuksen mukaan käyttäjien valintoihin vaikuttivat eniten ensimmäisenä esitetyt vaihtoehdot. Tämä tukee havaintoa, jonka mukaan Hyväksy -painikkeen korostaminen ja oletuksena valitut valintaruudut vaikuttivat huomattavasti siihen hyväksyivätkö käyttäjät evästeet (European Commission. Directorate General for Justice and Consumers, 2022). Voidaan siis olettaa, että käyttäjät hyväksyivät enemmän evästeistä sellaisilla sivustoilla, joilla nämä keinot olivat käytössä.

Seuraavaksi eniten, 44 evästekyselyssä, käyttäjän ei ollut mahdollista hylätä evästeitä yhdellä klikkauksella. Tämä on parempi tulos kuin Krisam ym.:n (2021) tutkimuksessa, jossa evästeet oli mahdollisuus hylätä yhdellä klikkauksella vain 21. 5% tapauksista. Soe ym. (2020) taas havaitsivat omassa tutkimuksessaan, että vain 15 sivustoa 300:sta mahdollisti evästeiden hylkäämisen yhdellä klikkauksella. Suomalaisten evästekyselyiden kohdalla tulos on siis paljon parempi, vaikka käytäntö esiintyi lähes puolessa evästekyselyistä. Evästeiden hylkäämisen hankaloittaminen lisätään Thaler ja Sunsteinin (2021) mukaan kitkaa (eng. sludge). Kun evästeiden hyväksyminen on taas helppoa, kaikilla sivustoilla oli mahdollisuus tehdä tämä yhdellä klikkauksella, saadaan aikaan tilanne, jossa on todennäköisempää, että käyttäjä hyväksyy evästeet.

Kolmanneksi eniten esiintyi epäselvästi merkattuja liukusäätimiä. Tulkitsin, että jos liukusäätimiä ei ollut merkattu muuten kuin värein, niitä ei ole merkattu selkeästi. Tulkinnan mukaan 32 sivustoa käytti keinoa. Toinen tulkinnanvarainen pimeä käytäntö, joka oli käytössä 20 evästekyselyllä oli valmiiksi tehdyt oletusvalinnat. Tulkintaa vaikeuttivat etenkin uutissivustoilla esiintynyt ns. ”oikeutettu etu” käytäntö, joka oli oletusvalintana päällä. Epäselväksi jäi, milloin sivustoilla on oikeus kerätä käyttäjän tietoja oikeutetun edun nimissä.

Muita havaittuja pimeitä käytäntöjä olivat ”ei antonyymejä” (17) ja ”ei mahdollisuutta kieltäytyä” (3). ”Ei antonyymejä” tarkoittaa tilannetta, jossa evästeiden hyväksymiselle ei ole käytetty selkeää vastakkaista ilmausta, vaan esimerkiksi kehotetaan tallentamaan valinnat. Vain muutamassa evästekyselyssä ei ollut mahdollisuutta kieltäytyä kaikista paitsi välttämättömistä evästeistä. Verrattuna Sheilin ja Malonen (2022) Irlannissa tekemään tutkimukseen, jossa 76 % evästekyselyistä oli vain hyväksy vaihtoehto, suomalaisilla sivustoilla on paljon paremmat mahdollisuudet kieltäytyä evästeistä.

Pimeitä käytäntöjä, joita tässä tutkimuksessa ei havaittu olivat useamman evästekyselyn esiintyminen samalla sivulla ja ”merkitsemätön x”. Pimeä käytäntö ”merkitsemätön x” tarkoittaa tilannetta, jossa evästekyselyn yläkulmasta löytyy rasti kyselyn sulkemista varten, mutta missään ei ole ilmoitettu tarkoittaako kyselyn sulkeminen evästeiden hyväksymistä vai hylkäämistä. Kyselyitä ei yleensä pystynyt sulkemaan rastista, enkä myöskään löytänyt sivustoa, joka olisi käyttänyt useampaa evästekyselyä.

Pimeiden käytäntöjen käyttäminen on siis suomalaisissa evästekyselyissä yleistä. Havainnot ovat samansuuntaisia muiden Euroopassa tehtyjen tutkimusten kanssa. Lukujen vaihtelevuutta voidaan selittää tutkimusten ajoituksella, maakohtaisilla käytännöillä ja kuinka tutkimus on suoritettu (esim.

automaattinen tulkinta vs. manuaalinen tulkinta). Lisäksi toiset tutkijat voivat esimerkiksi keskittyä enemmän visuaalisiin elementteihin, kun toiset painottavat sanamuotoja ja käytettävyyttä, jolloin toinen näkökulma voi jäädä huomiotta (Soe ym., 2020). Myös tulkinnat mitä tai minkälaisia pimeät käytännöt ovat tutkijakohtaisia, mikä vaikuttaa tulosten vertailtavuuteen.

## 8.2 Tutkimuksen luotettavuus

Tutkimus suoritettiin laadullisena tutkimuksena. Laadullisen tutkimuksen luotettavuuden arviointiin ei ole olemassa yksiselitteisiä ohjeita (Tuomi & Sarajärvi, 2003). Yksi tapa arvioida luotettavuutta on käydä läpi tutkimusprosessia ja arvioida tutkimuksen sisäistä johdonmukaisuutta (Tuomi & Sarajärvi, 2003). Tutkimuksen luotettavuutta on arvioitu tarkastelemalla tarkemmin tutkimuksen kohdetta ja tarkoitusta, aineistonkeruuta ja aineiston analyysiä.

Tutkimuksen kohteena olivat suomalaisten verkkosivustojen evästekyselyt ja tarkoituksena oli selvittää, millaisia pimeitä käytäntöjä näissä evästekyselyissä esiintyy. Tutkimuksen luotettavuuteen vaikuttaa aineiston pieni koko. Sadasta sivustosta koostuva aineisto ei anna kovin laajaa kuvaa evästekyselyissä esiintyvistä pimeistä käytännöistä. Tutkimuksen luotettavuutta olisi siten parantunut suurempi otanta. Pimeitä käytäntöjen määrittelemiseksi turvauduttiin laajasti aiempaan tutkimukseen. Pimeiden käytäntöjen luokittelemiseksi löytyi myös useita tapoja. Tätä tutkimusta varten kohdensin näkökulman pelkästään evästekyselyissä esiintyvien pimeiden käytäntöjen luokittelemiseksi tehtyihin määritelmiin tai luokituksiin. Vaikka käytin nimenomaan evästekyselyissä havaittujen pimeiden käytäntöjen pohjalta koostamaani taulukkoa, osoittautui tulkinta välillä hankalaksi, esimerkiksi mitä tarkoitetaan oletusvalinnoilla, entä milloin liukusäätimet on merkattu huonosti. Tulkintaa vaikeutti se seikka, että evästekyselyille ei ole olemassa mitään tiettyä standardia. Lisäksi evästekyselyiden suunnitteluun vaikuttava EU:n yleinen tietosuoja-asetus on laaja ja osin ristiriitainen.

Aineiston kerääminen ei ollut niin helppoa kuin odotin. Selkeää listausta suomalaisista verkkosivustoista ei ollut saatavissa. Tarvittava aineisto piti seuloa miljoonan suosituimman nettisivuston joukosta. Seulonnan luotettavuutta pyrittiin parantamaan käyttämällä selkeitä kriteereitä verkkosivustojen valinnassa. Aineiston vaihtelevuutta vähentää se, että joukossa oli useita sanomalehtien sivustoja, jotka käyttivät samaa evästekyselyä.

Laadullisen tutkimuksen luotettavuutta voidaan parantaa, jos kaksi tutkijaa luokittelee saman aineiston ja tuloksia verrataan tämän jälkeen keskenään (Tuomi & Sarajärvi, 2003). Tämän tutkimuksen luotettavuutta vähentää se tekijä, että aineiston on käynyt läpi vain yksi henkilö. Soe ym. (2020) huomauttavat, että pimeitä käytäntöjä on hyvin vaikea havaita automaattisesti ja jopa tutkijat voivat olla eri mieltä siitä, mitä pimeällä käytännöllä tarkoitetaan ja millaiset teot/käytännöt lasketaan niiden soveltamiseksi. Tutkimuksen luotettavuutta olisi parantanut, jos toinen tutkija olisi käynyt läpi samat evästekyselyt, käyttäen samaa

listaa ja samaa pimeiden käytäntöjen taulukkoa. Läpikäynnin jälkeen saatuja tuloksia olisi verrattu.

## 8.3 Rajoitukset

Yksi tutkimuksen rajoituksista on pieni otoskoko. Sadan sivuston evästekyselyistä tehtyä analyysia ei voi yleistää kaikkiin suomalaisiin sivustoihin. Varsinkin, kun erilaisten evästekyselytyyppien määrä oli pienempi kuin sivustojen määrä, esimerkiksi Sanoma-konserniin kuuluvat sanomalehdet käyttivät kaikki samanlaista evästekyselyä. Toinen tekijä on, että sivustot on valittu ensimmäisen reilun sadan sivuston joukosta. Useimmat verkkosivustot olivat tunnettuja ja niillä on enemmän kävijöitä, joten on todennäköisempää, että niiden evästekyselyt ja -asetukset ovat toimivampia kuin vähemmän vierailuilla sivustoilla. Isoimmilla sivustoilla on myös enemmän tietotaitoa johon nojata.

Toinen ongelma pienen otoskoon lisäksi on, että käytin vain yhtä laitetta ja yhtä selainta. On todennäköistä, että evästekyselyiden ulkoasu riippuu selaimesta ja laitteesta, esimerkiksi tietokoneen näytöllä on enemmän tilaa kuin mobiililaitteen näytöllä. Vaikka tietokoneen näyttö on suhteellisen suuri, osa evästekyselyistä oli kuitenkin esitetty niin, että esimerkiksi, jos haluaa tehdä yksittäisiä valintoja, joutuu sivupalkkia vierittämään, jos haluaa käydä kaikki vaihtoehdot läpi. Tämä on varmasti vielä hankalampaa mobiililaitteella.

Sijainnin ei pitäisi tässä tutkimuksessa olla vaikuttava tekijä, koska verkkosivustoista pyrittiin valitsemaan juuri suomalaiset. Vaikka sivustoa ylläpidettäisiin Euroopan ulkopuolella sen pitäisi noudattaa EU:n yleistä tietosuoja-asetusta, jos ne tarjoavat kohdennetusti palveluitaan EU:n kansalaisille (Asetus 2016/679, 2016). Selaimen kieleksi oli valittu suomi ja suurin osa sivustoista esitti evästekyselyn suomeksi, joukossa oli pari ruotsinkielistä.

Kolmas rajoitus on, että evästekyselyt voivat muuttua ajan myötä. Tämä on itse asiassa hyvin todennäköistä. Säädösten muutokset, tekniikan muutos ja uudistamisen tarve vaikuttavat siihen, että evästekyselyt muuttuvat. Joten tutkimus ei voikaan kuin kuvata tämänhetkistä tilannetta. Pelkästään se esitetäänkö evästekyselyitä voi muuttua. Degeling ym (2019) kävivät tutkimuksessaan läpi 6 579 eurooppalaista sivustoa joulukuun 2017 ja lokakuun 2018 välillä. He havaitsivat, että ennen EU.n yleisen tietosuoja-asetuksen tuloa voimaan 46.1%:lla sivustoista oli evästekysely tammikuussa 2018, asetuksen tultua voimaan keskiarvo nousi 62.1 %:n (Degeling ym., 2019).

Yksi ongelma on, että evästekyselyistä ja käyttäjän tekemistä valinnoista huolimatta, sivustot saattavat asettaa evästeitä joihin käyttäjä ei ole suostunut. Eli evästekyselyt eivät heijastele sivuston todellisia evästekäytäntöjä. Tämän tutkimuksen puitteissa ei ole mahdollista varmentaa millaisia sivustojen todelliset evästekäytännöt ovat.

Toinen ongelma on, että evästekyselyt eivät välttämättä tavoita sitä valintajoukkoa, joka olisi oikeasti käyttäjien valittavana. Käyttäjälle voidaan antaa yleisluontoiset valinnat kuten esimerkiksi tilastolliset evästeet. Toisaalta vaihtoehto,

jossa käyttäjälle annetaan tehdä hyvin yksityiskohtaiset valinnat, eivät välttämättä palvele käyttäjää. Törmäsin joillakin sivustoilla oleviin hyvinkin yksityiskohtaisiin evästevalintoihin, valinnoilla pystyi kieltämään evästeet toimittaja kerrallaan. Hyvin harvalla käyttäjällä on mielenkiintoa tai aikaa käydä yksittäin tällaisia asetuksia läpi.

Menetelmää voitaisiin kehittää ottamalla mukaan suurempi joukko sivustoja ja sitä kautta evästekyselyitä. Myös rajoituksiin voidaan laskea, että tulkinnan teki vain yksi henkilö. Kahden eri ihmisen tekemä tulkinta toisi eri näkökulmia asioihin.

## 8.4 Tutkimuksen implikaatioita

Pimeät käytännöt eivät ole mitenkään poikkeuksellisia suomalaisten sivustojen evästekyselyissä. Tulos on samansuuntainen kuin aiemmissa muissa Euroopan maissa suoritetuissa evästekyselyihin kohdistuvissa tutkimuksissa. Tämä voi johtaa siihen, että myös suomalaiset käyttäjät luovuttavat tarpeettoman paljon tietoja itsestään palvelun tarjoajille. Käyttäjien on myös hyvä tiedostaa keinojen olemassaolo, näin niiden vaikutusvalta vähenee.

Tutkimuksessa tuli myös ilmi, että evästekyselyt ovat erilaisia eri palveluntarjoajilla. Vain samaan konserniin kuuluvilla lehdillä oli samanlainen evästekysely. Käyttäjälle on hankalaa, kun jokainen evästekysely on erilainen. Painikkeiden paikat saattavat vaihdella ja eri sivustot käyttävät eri ilmaisuja. Tämä lisää käyttäjän kognitiivista taakkaa (Mathur ym., 2021; Soe ym., 2020).

Yksi keino kognitiivisen kuorman vähentämiseen olisi standardisoitu evästekysely. Valintapainikkeet olisivat aina samalla paikalla ja käytettäisiin samaa termistöä ja antonyymejä. Ongelmana tässä on, että vaikka saat hyvät puolet, saat myös huonot. Todennäköisesti evästekyselyn muokkausmahdollisuudet ovat rajatummat tällaisessa tilanteessa. Jos valmiissa evästekyselyssä on pimeitä käytäntöjä, ne tulevat sen mukana.

Toinen keino kognitiivisen kuorman vähentämiseen ja yksityisyyden parantamiseksi on pyrkiä vähentämään evästeiden määrää. Jos sivusto asettaa vain välttämättömiä evästeitä ei evästekyselyä tarvitse esittää. Jotkut palveluiden tarjoajat eivät välttämättä tiedä, että tämä on mahdollista. Asian tiedostaminen voisi vähentää evästekyselyiden määrää.

Tämän tutkimuksen puitteissa ei tarkasteltu käyttäjän valintojen huomiotta jättämistä eli tapausta, jossa evästeet asetetaan, vaikka käyttäjä kieltää ne. Sivustoille ei pitäisi antaa mahdollisuutta kiertää tällaista kieltoa. Ongelmana on kuitenkin se, että vaikka EU:n yleinen tietosuoja-asetus säätelee millainen evästekyselyn pitäisi olla, asetusta ei välttämättä noudateta. Toiminnan kieltäminen ei siis välttämättä toimi.

Jatkotutkimushaasteena ovat muuttuvat säädökset ja teknologia. Teknologia muuttuu jatkuvasti, jolloin evästekyselyt muuttuvat, esimerkiksi Google on lopettamassa tuen kolmannen osapuolen evästeille (Google, 2023). Pimeitä

käytäntöjä esiintyy varmasti jatkossakin ja vanhojen rinnalle tulee uusia, kun käyttäjät oppivat tunnistamaan entiset ja suunnittelijat kehittelevät uusia.

# LÄHTEET

Bailey, J., Laakso, M. & Nyman, L. (2019). Look Who's Tracking: An analysis of the 500 websites most-visited by Finnish web users. *Informaatiotutkimus*, *38*(3–4), 20–44. https://doi.org/10.23978/inf.87841

Baruh, L. & Popescu, M. (2017). Big data analytics and the limits of privacy self-management. *New Media & Society*, *19*(4), 579–596. https://doi.org/10.1177/1461444815614001

Bollinger, D., Kubicek, K., Cotrini, C. & Basin, D. (2022). Automating Cookie Consent and GDPR Violation Detection. *31st USENIX Security Symposium (USENIX Security 22)*, 2893–2910. https://www.usenix.org/conference/usenixsecurity22/presentation/bollinger

Bouma-Sims, E. R., Li, M., Lin, Y., Sakura-Lemessy, A., Nisenoff, A., Young, E., Birrell, E., Cranor, L. F. & Habib, H. (2023). A US-UK Usability Evaluation of Consent Management Platform Cookie Consent Interface Design on Desktop and Mobile. *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, 1–36. https://doi.org/10.1145/3544548.3580725

Brignull, H., Leiser, M., Santos, C. & Doshi, K. (25.4.2023a). *Deceptive Patterns - Types - Hard to cancel*. https://www.deceptive.design/types/hard-to-cancel

Brignull, H., Leiser, M., Santos, C. & Doshi, K. (25.4.2023b). *Deceptive Patterns - Types of Deceptive Pattern*. https://www.deceptive.design/types

Bruni, E. (5.6.2019). Does the Web Really Need Cookies? *WDD*. https://www.webdesignerdepot.com/2019/06/does-the-web-really-need-cookies/

Bösch, C., Erb, B., Kargl, F., Kopp, H. & Pfattheicher, S. (2016). Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns. *Proceedings on Privacy Enhancing Technologies*. https://petsymposium.org/popets/2016/popets-2016-0038.php

Cahn, A., Alfeld, S., Barford, P. & Muthukrishnan, S. (2016). An Empirical Study of Web Cookies. *Proceedings of the 25th International Conference on World Wide Web*, 891–901. https://doi.org/10.1145/2872427.2882991

CNIL. (6.1.2022a). *Cookies: GOOGLE fined 150 million euros*. Commission Nationale de l'informatique et Des Libertés. https://www.cnil.fr/en/cookies-google-fined-150-million-euros

CNIL. (28.6.2022b). *Cookies: the Council of State confirms the 2020 sanction imposed by the CNIL against Amazon*. Commission Nationale de l'informatique et Des Libertés. https://www.cnil.fr/en/cookies-council-state-confirms-2020-sanction-imposed-cnil-against-amazon

Conti, G. & Sobiesk, E. (2010). Malicious interface design: exploiting the user. *Proceedings of the 19th International Conference on World Wide Web*, 271–280. https://doi.org/10.1145/1772690.1772719

Culnan, M. J. & Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science*, *10*(1), 104–115. https://doi.org/10.1287/orsc.10.1.104

Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F. & Holz, T. (2019). We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy. *Proceedings 2019 Network and Distributed System Security Symposium*. Network and Distributed System Security Symposium, San Diego, CA. https://doi.org/10.14722/ndss.2019.23378

Dinev, T. & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, *17*(1), 61–80. https://doi.org/10.1287/isre.1060.0080

Duhigg, C. (16.2.2012). How Companies Learn Your Secrets. *The New York Times*. https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

Englehardt, S. & Narayanan, A. (2016). Online tracking: A 1-million-site measurement and analysis. *CCS 2016 - Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 1388–1401. https://doi.org/10.1145/2976749.2978313

Euroopan komissio. (ei pvm.). *Mitä tarkoittaa "oikeutettu etu"?* Noudettu 12. joulukuuta 2023, osoitteesta https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-does-grounds-legitimate-interest-mean_fi

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, Pub. L. No. 2016/679 (2016).

Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, Pub. L. No. 2002/58/EY (2002). https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX%3A32002L0058

European Commission. Directorate General for Justice and Consumers. (2022). *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation : final report.* Publications Office. https://data.europa.eu/doi/10.2838/859030

European Data Protection Board. (ei pvm.-a). *EDPB:n puheenjohtajuus | European Data Protection Board*. Noudettu 14. marraskuuta 2023, osoitteesta https://edpb.europa.eu/about-edpb/who-we-are/edpb-chairmanship_fi

European Data Protection Board. (ei pvm.-b). *Tasks and duties | European Data Protection Board*. Noudettu 14. marraskuuta 2023, osoitteesta https://edpb.europa.eu/about-edpb/what-we-do/tasks-and-duties_en

European Data Protection Board. (2020). *Guidelines 05/2020 on consent under Regulation 2016/679*. European Data Protection Board. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

European Data Protection Board. (2022). *Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them*. European Data Protection Board. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en

Forbrukerrådet. (2018). *Deceived by Design How tech companies use dark patterns to discourage us from exercising our rights to privacy*. Forbrukerrådet. https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

F-Secure. (ei pvm.). *What are cookies? | F-Secure*. Noudettu 26. syyskuuta 2023, osoitteesta https://www.f-secure.com/en/articles/cookies

Gabaix, X. & Laibson, D. (2006). Shrouded Attributes, Consumer Myopia, and Information Suppression in Competitive Markets. *The Quarterly Journal of Economics*, *121*(2), 505–540. https://doi.org/10.1162/qjec.2006.121.2.505

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

Google. (21.12.2023). *Prepare for phasing out third-party cookies | Privacy Sandbox*. Google for Developers. https://developers.google.com/privacy-sandbox/3pcd

Graßl, P., Schraffenberger, H., Borgesius, F. Z. & Buijzen, M. (2021). Dark and Bright Patterns in Cookie Consent Requests. *Journal of Digital Social Research*, *3*(1), 1–38. https://doi.org/10.33621/jdsr.v3i1.54

Gray, C. M., Chivukula, S. S. & Lee, A. (2020). What Kind of Work Do "Asshole Designers" Create? Describing Properties of Ethical Concern on Reddit. *Proceedings of the 2020 ACM Designing Interactive Systems Conference*, 61–73. https://doi.org/10.1145/3357236.3395486

Gray, C. M., Kou, Y., Battles, B., Hoggatt, J. & Toombs, A. L. (2018). The Dark (Patterns) Side of UX Design. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1–14. https://doi.org/10.1145/3173574.3174108

Greenberg, S., Boring, S., Vermeulen, J. & Dostal, J. (2014). Dark patterns in proxemic interactions: a critical perspective. *Proceedings of the 2014 Conference on Designing Interactive Systems*, 523–532. https://doi.org/10.1145/2598510.2598541

Hanks, A. S., Just, D. R. & Wansink, B. (2013). Smarter Lunchrooms Can Address New School Lunchroom Guidelines and Childhood Obesity. *The Journal of Pediatrics*, *162*(4), 867–869. https://doi.org/10.1016/j.jpeds.2012.12.031

Hannak, A., Soeller, G., Lazer, D., Mislove, A. & Wilson, C. (2014). Measuring Price Discrimination and Steering on E-commerce Web Sites. *Proceedings of the 2014 Conference on Internet Measurement Conference*, 305–318. https://doi.org/10.1145/2663716.2663744

Hennig, A., Dietmann, H., Lehr, F., Mutter, M., Volkamer, M. & Mayer, P. (2022). "Your Cookie Disclaimer is Not in Line with the Ideas of the GDPR. Why?". Teoksessa N. Clarke & S. Furnell (toim.), *Human Aspects of Information Security and Assurance* (Vsk. 658, s. 218–227). Springer International Publishing. https://doi.org/10.1007/978-3-031-12172-2_17

Jones, M. L. (2020). Cookies: a legacy of controversy. *Internet Histories*, *4*(1), 87–104. https://doi.org/10.1080/24701475.2020.1725852

Kampanos, G. & Shahandashti, S. F. (2021). Accept All: The Landscape of Cookie Banners in Greece and the UK. Teoksessa A. Jøsang, L. Futcher & J. Hagen (toim.), *ICT Systems Security and Privacy Protection* (Vsk. 625, s.

213–227). Springer International Publishing. https://doi.org/10.1007/978-3-030-78120-0_14

Karumaa, P. (1.3.2023). Palveluiden valintamuotoilun ja -arkkitehtuurin sietämätön tärkeys. *HAMK Beat*. https://blog.hamk.fi/hamk-beat/palveluiden-valintamuotoilun-ja-arkkitehtuurin-ja-sietamaton-tarkeys/

Kaspersky. (ei pvm.). *What are Cookies?* Noudettu 26. syyskuuta 2023, osoitteesta https://www.kaspersky.com/resource-center/definitions/cookies

Kilpailu- ja kuluttajavirasto. (ei pvm.). *Pimeät käytännöt*. Kilpailu- ja kuluttajavirasto. Noudettu 19. syyskuuta 2023, osoitteesta https://www.kkv.fi/kuluttaja-asiat/huijaukset/pimeat-kaytannot/

Klein, G. L., Pfaff, M. S. & Drury, J. L. (2009). Supporting a Robust Decision Space. *AAAI Spring Symposium: Technosocial Predictive Analytics*, 66–71. https://cdn.aaai.org/Symposia/Spring/2009/SS-09-09/SS09-09-013.pdf

Koch, R. (9.5.2019). *Cookies, the GDPR, and the ePrivacy Directive*. GDPR.Eu. https://gdpr.eu/cookies/

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*, *15*(4), 1–42. https://doi.org/10.1145/3466722

Krisam, C., Dietmann, H., Volkamer, M. & Kulyk, O. (2021). Dark Patterns in the Wild: Review of Cookie Disclaimer Designs on Top 500 German Websites. *Proceedings of the 2021 European Symposium on Usable Security*, 1–8. https://doi.org/10.1145/3481357.3481516

Kyberturvallisuuskeskus. (4.4.2023). *Evästeet*. Traficom. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/evasteet

Laboratoire d'Innovation Numérique de la CNIL. (2019). *IP Report: Shaping Choices in the Digital World, From dark patterns to data protection: the influence of UX/UI design on user empowerment*. Laboratoire d'Innovation Numérique de la CNIL. https://linc.cnil.fr/ip-report-shaping-choices-digital-world

Lappalainen, T. (9.9.2019). Maailmalla tuupataan nyt huolella – menetelmä toimii hyvin erityisesti julkishallinnossa. *Aalto leaders insight*. https://www.aaltoee.fi/aalto-leaders-insight/2019/maailmalla-

tuupataan-nyt-huolella-menetelma-toimii-hyvin-erityisesti-julkishallinnossa

Laufer, R. S. & Wolfe, M. (1977). Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. *Journal of Social Issues*, *33*(3), 22–42. https://doi.org/10.1111/j.1540-4560.1977.tb01880.x

Le Pochat, V., Van Goethem, T., Tajalizadehkhoob, S., Korczynski, M. & Joosen, W. (2019). Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation. *Proceedings 2019 Network and Distributed System Security Symposium*. Network and Distributed System Security Symposium, San Diego, CA. https://doi.org/10.14722/ndss.2019.23386

Leal, C. C., Branco-Illodo, I., Oliveira, B. M. do N. & Esteban-Salvador, L. (2022). Nudging and Choice Architecture: Perspectives and Challenges. *Revista de Administração Contemporânea*, *26*(5). https://www.redalyc.org/journal/840/84070847005/html/

Lee, A. (23.12.2019). Tuvalu is a tiny island nation of 11,000 people. It's cashing in thanks to Twitch. *Washington Post*. https://www.washingtonpost.com/video-games/2019/12/23/tuvalu-is-tiny-island-nation-people-its-cashing-thanks-twitch/

Leiser, M. (2022). Illuminating Manipulative Design: From "Dark Patterns" to Information Asymmetry and the Repression of Free Choice Under the Unfair Commercial Practices Directive. *Loyola Consumer Law Review*, *34*(3), 484–528.

Limba, T., Driaunys, K. & Šidlauskas, A. (2021). Use of cookies after GDPR: a case study of top Lithuanian websites. *Transformations in Business & Economics*, *20*, 93–116.

Maier, M. & Harr, R. (2020). Dark Design Patterns: An End-User Perspective. *Human Technology*, *16*(2), 170–199. https://doi.org/10.17011/ht/urn.202008245641

Martini, M. & Drews, C. (2022). Making Choice Meaningful – Tackling Dark Patterns in Cookie and Consent Banners through European Data Privacy Law. *SSRN Scholarly Paper Nro 4257979*. https://doi.org/10.2139/ssrn.4257979

Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M. & Narayanan, A. (2019). Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. *Proceedings of the ACM on Human-Computer Interaction*, *3*(CSCW), 1–32. https://doi.org/10.1145/3359183

Mathur, A., Kshirsagar, M. & Mayer, J. (2021). What Makes a Dark Pattern... Dark?: Design Attributes, Normative Considerations, and Measurement Methods. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 1–18. https://doi.org/10.1145/3411764.3445610

Meier, Y. & Krämer, N. C. (2022). The Privacy Calculus Revisited: An Empirical Investigation of Online Privacy Decisions on Between- and Within-Person Levels. *Communication Research*. https://doi.org/10.1177/00936502221102101

Mutru, M. (14.11.2022). Pimeät käytännöt: sallittua ohjailua vai kiellettyä manipulointia? *Kulma*. https://kulma.kkv.fi/2022/11/14/pimeat-kaytannot-sallittua-ohjailua-vai-kiellettya-manipulointia/

Myrstad, F. (1.7.2022). Amazon makes it easier to cancel Prime following complaints from European consumer organisations. *Forbrukerrådet*. https://www.forbrukerradet.no/siste-nytt/amazon-makes-it-easier-to-cancel-prime-following-complaints-from-european-consumer-organisations/

Nevala, E. (2023). ”Just let me buy my thing!” : A survey study on consumers’ perceptions of social influence in E-Commerce. Pro gradu –tutkielma, Jyväskylän yliopisto. https://jyx.jyu.fi/handle/123456789/87309

Nouwens, M., Liccardi, I., Veale, M., Karger, D. & Kagal, L. (2020). Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–13. https://doi.org/10.1145/3313831.3376321

Ojanen, M. (2023). *Tuuppauksesta toimeen: kohti fiksumpia valintoja ja päätöksiä*. Kaswu.

Peters, R. & Sikorski, R. (1997). Cookie monster? *Science*, *278*(5342), 1486–1487.

Pitkänen, P. (26.2.2015). Tietosuojahuolet vaikuttivat - S-Pankki lopetti Googlen käytön. *Ilta-Sanomat*. https://www.is.fi/digitoday/art-2000000884663.html

Rantalahti, E. (2020). Kulutusta tuupaten: systemaattinen kirjallisuuskatsaus tuuppauksen vaikutuksesta kestävän kuluttamisen valintoihin. Pro gradu –tutkielma, Jyväskylän yliopisto. https://jyx.jyu.fi/handle/123456789/71955

Räisänen, O. (14.4.2015). Trackers leaking bank account data. *absorptions*. https://www.windytan.com/2015/04/trackers-and-bank-accounts.html

Salonen, S. (2022). HTTP evästeiden uhkat tietosuojaselosteiden näkökulmasta. Pro gradu –tutkielma, Jyväskylän yliopisto. https://jyx.jyu.fi/handle/123456789/81955

Santos, C., Rossi, A., Sanchez Chamorro, L., Bongard-Blanchy, K. & Abu-Salma, R. (2021). Cookie Banners, What's the Purpose? Analyzing Cookie Banner Text Through a Legal Lens. *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society*, 187–194. https://doi.org/10.1145/3463676.3485611

Sheil, A. & Malone, D. (2022). Fianán, Cuacha: Irish Cookie Banners. *2022 33rd Irish Signals and Systems Conference (ISSC)*, 1–8. https://doi.org/10.1109/ISSC55427.2022.9826167

Soe, T. H., Nordberg, O. E., Guribye, F. & Slavkovik, M. (2020). Circumvention by design - dark patterns in cookie consent for online news outlets. *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*, 1–12. https://doi.org/10.1145/3419249.3420132

S-Pankki. (25.2.2015). *Google Analytics -palvelun käyttö S-Pankin verkkopalveluissa | S-Pankki.fi*. https://web.archive.org/web/20190906101353/https://www.s-pankki.fi/fi/tiedotteet/2015/google-analytics--palvelun-kaytto-s-pankin-verkkopalveluissa/

Strömberg, M. (2020). Ärsyttääkö ohjailu?: Fenomenografinen analyysi käyttäjien kokemasta ohjailusta verkkopalveluissa. Pro gradu –tutkielma, Tampereen yliopisto. https://trepo.tuni.fi/handle/10024/120394

Thaler, R. H. & Sunstein, C. R. (2008). *Nudge: improving decisions about health, wealth, and happiness*. Yale University Press.

Thaler, R. H. & Sunstein, C. R. (2021). *Nudge: the final edition* (Updated edition). Penguin Books.

Tietosuojavaltuutetun toimisto. (ei pvm.-a). *EU:n tietosuoja-asetus - usein kysyttyjä kysymyksiä*. Tietosuojavaltuutetun toimisto. Noudettu 18. syyskuuta 2023, osoitteesta https://tietosuoja.fi/gdpr

Tietosuojavaltuutetun toimisto. (ei pvm.-b). *Rekisterinpitäjän oikeutettu etu*. Tietosuojavaltuutetun toimisto. Noudettu 12. joulukuuta 2023, osoitteesta https://tietosuoja.fi/rekisterinpitajan-oikeutettu-etu

Tietosuojavaltuutetun toimisto. (ei pvm.-c). *Rekisteröidyn suostumus*. Tietosuojavaltuutetun toimisto. Noudettu 7. marraskuuta 2023, osoitteesta https://tietosuoja.fi/rekisteroidyn-suostumus

Traficom. (10.1.2019). *Muut kuin fi-verkkotunnukset*. Traficom. https://www.traficom.fi/fi/viestinta/fi-verkkotunnukset/muut-kuin-fi-verkkotunnukset

Traficom. (14.9.2022). *Näin hankit fi-verkkotunnuksen*. Traficom. https://www.traficom.fi/fi/viestinta/fi-verkkotunnukset/nain-hankit-fi-verkkotunnuksen

Tranco. (ei pvm.). *A research-oriented top sites ranking hardened against manipulation - Tranco*. Noudettu 21. syyskuuta 2023, osoitteesta https://tranco-list.eu/

Tuomi, J. & Sarajärvi, A. (2003). *Laadullinen tutkimus ja sisällönanalyysi* (1.-2.painos). Tammi.

Utz, C., Degeling, M., Fahl, S., Schaub, F. & Holz, T. (2019). (Un)informed Consent: Studying GDPR Consent Notices in the Field. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 973–990. https://doi.org/10.1145/3319535.3354212

Vainio, L. (24.11.2018). *Viikon ilmiö: Mitä on valintamuotoilu? -*. http://www.valintamuotoilijat.com/viikon-ilmio-mita-on-valintamuotoilu/

Waldman, A. E. (2020). Cognitive biases, dark patterns, and the 'privacy paradox'. *Current Opinion in Psychology*, *31*, 105–109. https://doi.org/10.1016/j.copsyc.2019.08.025

Walker, R. (30.11.2003). The Guts of a New Machine. *The New York Times*. https://www.nytimes.com/2003/11/30/magazine/the-guts-of-a-new-machine.html

West, S. M. (2019). Data Capitalism: Redefining the Logics of Surveillance and Privacy. *Business & Society*, *58*(1), 20–41. https://doi.org/10.1177/0007650317718185

Zagal, J. P., Björk, S. & Lewis, C. (2013). Dark Patterns in the Design of Games. *Foundations of Digital Games 2013.* https://urn.kb.se/resolve?urn=urn:nbn:se:ri:diva-24252

Zuboff, S. (2019). *The age of surveillance capitalism: the fight for the future at the new frontier of power*. Profile Books.

# LIITE 1. LISTAUS SIVUSTOISTA

| nro. | osoite |
|---|---|
| 1. | elisa.fi |
| 2. | iltalehti.fi |
| 3. | foreca.fi |
| 4. | google.fi |
| 5. | yle.fi |
| 6. | helsinki.fi |
| 7. | hs.fi |
| 8. | is.fi |
| 9. | mtvuutiset.fi |
| 10. | veikkaus.fi |
| 11. | tori.fi |
| 12. | seiska.fi |
| 13. | lippu.fi |
| 14. | aalto.fi |
| 15. | oikotie.fi |
| 16. | ilmatieteenlaitos.fi |
| 17. | vauva.fi |
| 18. | motonet.fi |
| 19. | kanta.fi |
| 20. | oulu.fi |
| 21. | utu.fi |
| 22. | posti.fi |
| 23. | jyu.fi |
| 24. | tuni.fi |
| 25. | hel.fi |
| 26. | lahitapiola.fi |
| 27. | kauppalehti.fi |
| 28. | elisaviihde.fi |
| 29. | lut.fi |
| 30. | mikrobitti.fi |
| 31. | op.fi |
| 32. | finland.fi |
| 33. | telia.fi |
| 34. | kela.fi |
| 35. | vr.fi |
| 36. | vero.fi |
| 37. | uef.fi |
| 38. | ts.fi |
| 39. | mtv.fi |
| 40. | dna.fi |
| 41. | abo.fi |
| 42. | aamulehti.fi |
| 43. | zalando.fi |
| 44. | kaleva.fi |
| 45. | traficom.fi |
| 46. | nordea.fi |
| 47. | valtioneuvosto.fi |
| 48. | gigantti.fi |
| 49. | ouka.fi |
| 50. | uusisuomi.fi |
| 51. | suomi.fi |
| 52. | prisma.fi |
| 53. | turku.fi |
| 54. | vtt.fi |
| 55. | sanoma.fi |
| 56. | talouselama.fi |
| 57. | suomi24.fi |
| 58. | k-ruoka.fi |
| 59. | finlandabroad.fi |
| 60. | foodora.fi |
| 61. | s-kaupat.fi |
| 62. | almamedia.fi |
| 63. | hsl.fi |
| 64. | vasabladet.fi |
| 65. | verkkouutiset.fi |
| 66. | tekniikkatalous.fi |
| 67. | terveyskirjasto.fi |
| 68. | sokoshotels.fi |
| 69. | vikingline.fi |
| 70. | ksml.fi |
| 71. | finder.fi |
| 72. | savonsanomat.fi |
| 73. | finnkino.fi |
| 74. | finlex.fi |
| 75. | kennelliitto.fi |
| 76. | alko.fi |
| 77. | tekniikanmaailma.fi |
| 78. | kotiliesi.fi |
| 79. | thl.fi |
| 80. | ess.fi |
| 81. | duunitori.fi |
| 82. | valio.fi |
| 83. | tokmanni.fi |
| 84. | anna.fi |
| 85. | mehilainen.fi |
| 86. | satakunnankansa.fi |
| 87. | meillakotona.fi |
| 88. | matkahuolto.fi |
| 89. | tui.fi |
| 90. | stat.fi |
| 91. | netrauta.fi |
| 92. | hobbyhall.fi |
| 93. | aurinkomatkat.fi |
| 94. | io-tech.fi |
| 95. | netvisor.fi |
| 96. | xxl.fi |
| 97. | enfo.fi |
| 98. | k-rauta.fi |
| 99. | finavia.fi |
| 100. | stara.fi |