Kolmansien osapuolien tietovuodot Suomen evankelis-luterilaisten seurakuntien verkkosivuilla

TURUN YLIOPISTO
Tietotekniikan laitos
TkK-tutkielma
Tietotekniikka
Kesäkuu 2025
Henna Lohi

TURUN YLIOPISTO
Tietotekniikan laitos

HENNA LOHI: Kolmansien osapuolien tietovuodot Suomen evankelis-luterilaisten seurakuntien verkkosivuilla

TkK-tutkielma, 25 s.
Tietotekniikka
Kesäkuu 2025

Verkkopalveluiden käytön yleistyessä käyttäjien yksityisyyden suoja on noussut merkittäväksi huolenaiheeksi. Erityisesti uskonnollisten yhteisöjen verkkosivustoilla vierailu voi paljastaa arkaluonteisia tietoja käyttäjästä, kuten hänen uskonnollisen vakaumuksensa. Tässä tutkielmassa selvitetään, millaisia tietovuotoja kolmansille osapuolille tapahtuu Suomen evankelis-luterilaisten seurakuntien verkkosivuilla, ja kuinka hyvin nämä verkkopalvelut noudattavat tietosuojalainsäädäntöä ja yksityisyyden suojan periaatteita.
Tutkimus yhdistää kirjallisuuskatsauksen ja empiirisen verkkoliikenteen analyysin. Aineistona käytettiin 31 seurakunta- ja hiippakuntasivustoa, joita analysoitiin verkkopyyntöjen, evästebannereiden ja tietosuojaselosteiden näkökulmista. Tarkastelun kohteena olivat erityisesti kolmansien osapuolien (kuten Googlen ja Metan) läsnäolo sekä tiedon mahdollinen vuotaminen ilman käyttäjän selkeää suostumusta.
Tulosten perusteella seurakuntien verkkosivustot tarjoavat keskimäärin hyvän yksityisyyden suojan tason, erityisesti niillä sivustoilla, jotka hyödyntävät kirkon Lukkari-julkaisualustaa ja yksityisyyttä tukevaa Matomo-analytiikkaa. Kuitenkin tietovuotoja esiintyi erityisesti Lukkari-järjestelmän ulkopuolisilla sivustoilla, ja evästesuostumukseen liittyi usein käyttöliittymäratkaisuja, jotka saattoivat ohjata käyttäjää antamaan suostumuksen ilman todellista harkintaa. Tutkimus osoittaa, että vaikka teknisiä parannuksia on tehty, tietosuojaselosteiden läpinäkyvyys ja suostumuksen selkeys vaativat edelleen kehittämistä. Erityisesti arkaluonteisia tietoja käsitteleville verkkosivuille suositellaan ulkopuolisia tietosuojatarkastuksia.

Asiasanat: yksityisyys, tietosuoja, evästeet, kolmannet osapuolet, verkkosivut, seurakunnat, Lukkari, GDPR

Sisällys

1 Johdanto

Digitaaliset palvelut ovat muodostuneet keskeiseksi osaksi myös uskonnollisten yhteisöjen toimintaa. Verkkosivujen avulla voidaan jakaa tietoa, järjestää tapahtumia ja rakentaa yhteisöllisyyttä niin nykyisten jäsenten kuin uusien kiinnostuneiden keskuudessa [1]–[4]. Internet mahdollistaa uskonnollisen viestinnän laajentamisen fyysisten rajojen ulkopuolelle, ja sen käyttöä pidetään monissa yhteisöissä sekä käytännöllisenä että teologisesti hyväksyttävänä osana nykyaikaista seurakuntatyötä.

Samalla kun verkkopalvelut tarjoavat hyötyjä uskonnolliselle viestinnälle, ne altistavat käyttäjät erilaisille tietosuojahaasteille. Erityisesti huomiota tulee kiinnittää siihen, mitä tietoja käyttäjistä välittyy kolmansille osapuolille, kuten mainosverkostoille tai analytiikkapalveluille, mahdollisesti ilman käyttäjän tietoista suostumusta. Tämä on erityisen merkityksellistä tilanteissa, joissa verkkosivun käyttö voi paljastaa arkaluonteisia tietoja, kuten henkilön uskonnollisen vakaumuksen [5], [6]. Euroopan unionin yleisen tietosuoja-asetuksen, GDPR (General Data Protection Regulation), mukaan uskonnollinen vakaumus kuuluu erityisiin henkilötietoryhmiin, joiden käsittely on lähtökohtaisesti kielletty ilman nimenomaista suostumusta [7]. Tästä syystä verkkosivujen suunnittelussa tulee noudattaa erityistä huolellisuutta, ja käyttäjän yksityisyyden suojan on oltava keskeinen osa teknistä ja sisällöllistä toteutusta.

Kolmansien osapuolien seuranta ja mahdolliset tietovuodot verkkosivuilta ovat olleet toistuvasti tietosuojatutkimuksen kohteena. Tutkimukset ovat osoittaneet, että verkkosivustot voivat välittää henkilötietoja, kuten IP-osoitteita, selainasetuksia ja vierailtuja sivu-

ja, analytiikkapalveluille, jotka hyödyntävät tietoa esimerkiksi kohdennettuun mainontaan tai muuhun profilointiin [8], [9]. Vaikka kolmansien osapuolien käyttö on sinänsä yleistä monilla verkkosivustoilla, sen vaikutukset korostuvat erityisesti julkisen sektorin tai luottamuksellisia palveluja tarjoavien tahojen kohdalla. Tähän liittyen esimerkiksi Suomen tietosuojavaltuutetun toimisto on korostanut, että viranomaispalveluiden käyttäjien ei tulisi joutua alttiiksi kaupalliselle seurannalle.

Tässä tutkielmassa tarkastellaan kolmansien osapuolien mahdollisesti aiheuttamia tietovuotoja Suomen evankelis-luterilaisten seurakuntien verkkosivuilla. Tutkielma peustuu kansainvälisessä ICSEA 2024 -konferenssissa julkaistuun artikkeliin *A Study of Third-Party Tracking on Religious Websites* [6], joka kuuluu osaksi Suomen Akatemian rahoittamaa IDA-hanketta (IDA – Intimacy in Data-Driven Culture). Tarkastelun kohteena oli yhteensä 31 verkkosivustoa eri puolilta Suomea. Näistä osa käytti kirkon omaa Lukkari-julkaisualustaa, kun taas osa toimi itsenäisesti. Verkkoliikennettä analysoitiin HTTP-lokitiedostojen (HAR) avulla, ja tutkimuksessa selvitettiin, mihin kolmansille osapuolille tietoja vuotaa ja millaisessa muodossa nämä vuodot tapahtuvat.

Tutkimuksessa hyödynnettiin tieteellisten julkaisujen ohella viranomaisten ohjeistuksia, kansallisia ja EU-tason säädöksiä, sekä kirkon omia verkkosivumateriaaleja. Hakusanoina käytettiin muun muassa ”third-party data leaks”, ”privacy policy” ja ”cookie consent”. Lähteiden valinnassa painotettiin ajankohtaisuutta ja asiayhteyteen sopivuutta. Tiedonhaku kohdistui erityisesti eurooppalaisiin ja kansallisiin tietosuojaviranomaisiin sekä keskeisiin yksityisyystutkimuksiin.

Tutkielmassa vastataan seuraaviin tutkimuskysymyksiin:

1. Minkälaista tietoa Suomen evankelis-luterilaisten seurakuntien verkkosivut välittävät kolmansille osapuolille?

2. Onko näissä tietovuodoissa havaittavissa yksityisyyden tai tietosuojan kannalta ongelmallisia piirteitä?

3. Kuinka hyvin verkkosivujen tietosuojakäytännöt vastaavat tietosuojalainsäädännön vaatimuksia ja läpinäkyvyyden periaatteita?

Tutkielman toisessa luvussa esitellään yksityisyyden suojan ja tietoturvan keskeiset käsitteet sekä perehdytään evästeisiin, suostumuskäytäntöihin ja tietosuojaselosteiden merkitykseen. Kolmannessa luvussa esitellään tutkimusympäristö ja -menetelmät sekä analysoidaan tutkimustulokset. Tutkielma päättyy johtopäätöksiin, joissa arvioidaan yksityisyyden suojan toteutumista kirkon verkkosivuilla ja esitetään kehitysehdotuksia verkkoviestinnän parantamiseksi.

2 Yksityisyys, tietosuoja ja kolmannet osapuolet

2.1 Yksityisyys

Meillä jokaisella on tietoa, jonka emme halua päätyvän ulkopuolisten tietoon tai käyttöön. Käytämme internetiä päivittäin ja huomaamatta jätämme jälkeemme henkilökohtaista tietoa. Esimerkiksi salasanat eri sivustoille ja pankkikortin tunnusluku ovat tietoja, joiden emme halua päätyvän vääriin käsiin. Kuitenkin tällaiset tiedot ovat aina alttiina väärinkäytölle.

Yksityisyys on käsite, joka tarkoittaa yksilön oikeutta päättää, mitä henkilötietoja hän itsestään luovuttaa ja kenelle [7]. Nykymaailmassa, jossa suuri osa vuorovaikutuksesta, kaupankäynnistä ja tiedonvaihdosta tapahtuu verkossa, yksityisyyden merkitys korostuu entisestään. Jokainen käyttäjän toimi, kuten verkkohaku, sosiaalisen median käyttö tai verkkokaupoissa asiointi, tuottaa dataa, jota voidaan käyttää yksilön profilointiin. Tämä tieto voi paljastaa paljon esimerkiksi käyttäjän kiinnostuksen kohteista, käyttäytymisestä ja sijainnista.

Yksityisyyden suoja on perusoikeus, joka on turvattu Suomen perustuslaissa. Lain 10 §:n mukaan jokaisella on oikeus yksityiselämään, kunniaan ja kotirauhaan, ja viestinnän salaisuus on loukkaamaton [10]. Tämä suoja kattaa myös henkilötiedot, joiden käsittelyä säädellään tarkemmin lailla.

Henkilötiedot tarkoittavat kaikkia tietoja, joiden avulla yksilö voidaan tunnistaa joko suoraan tai epäsuorasti. Näitä ovat esimerkiksi nimi, osoite, sähköposti ja puhelinnumero, mutta myös tekniset tiedot, kuten IP-osoite, voivat kuulua henkilötietoihin [11]. Näiden tietojen suojaaminen on olennaisen tärkeää, sillä niiden väärinkäyttö voi johtaa vakaviin seurauksiin, kuten identiteettivarkauksiin ja muuhun haitalliseen toimintaan.

Yksityisyydensuoja on keskeinen osa Euroopan ihmisoikeussopimusta, joka astui voimaan vuonna 1950. Sopimus takaa jokaiselle oikeuden henkilökohtaisen ja perhe-elämän kunnioitukseen. Euroopan unioni on vahvistanut tätä oikeutta omalla lainsäädännöllään, erityisesti teknologian ja internetin nopean kehityksen myötä. [12]

Vuonna 1995 hyväksyttiin Euroopan tietosuojadirektiivi, joka asetti vähimmäisvaatimukset henkilötietojen suojaamiselle. Direktiivin pohjalta jäsenvaltioiden tuli säätää omat tietosuojalakinsa. Samoihin aikoihin internetistä alkoi kehittyä laajamittainen tietojen keruualusta, esimerkiksi ensimmäinen bannerimainos julkaistiin vuonna 1994.

Vuonna 2006 Facebook avattiin yleisölle, ja tietosuojakysymykset nousivat yhä tärkeämmiksi. Vuonna 2011 Google joutui oikeuteen sähköpostien sisällön skannaamisesta, mikä herätti huolta yksityisyydensuojasta. Tämän seurauksena Euroopan tietosuojaviranomainen totesi, että tarvitaan kattavampi ja yhtenäisempi lähestymistapa tietosuojaan koko EU:n alueella.

Tämä johti uuden lainsäädännön laatimiseen: GDPR eli yleinen tietosuoja-asetus hyväksyttiin vuonna 2016. Asetusta on sovellettu kaikissa EU-maissa toukokuusta 2018 alkaen, ja sen tavoitteena on vahvistaa yksilöiden oikeuksia ja yhdenmukaistaa tietosuojalainsäädäntö EU:n alueella. [7]

2.2 Tietoturva

Internetin ja digitaalisten palveluiden laaja käyttö on tehnyt henkilökohtaisen tiedon suojaamisesta entistä haastavampaa. Verkkopalveluiden tietomurrot, identiteettivarkaudet ja erilaiset huijausyritykset ovat yleisiä uhkia, jotka voivat johtaa vakaviin seurauksiin, kuten

taloudellisiin menetyksiin ja maineen menetykseen. Tästä syystä tietoturva on keskeinen osa digitaalista arkea.

Tietoturva viittaa menetelmiin ja käytäntöihin tiedon ja järjestelmien turvaamiseksi. Tietoturva määritellään tiedon suojaamisena luvattomalta pääsyltä, käytöltä, julkaisemiselta, häirinnältä, muokkaamiselta tai tuhoamiselta. Yleisesti tietoturva jaetaan kolmeen pääperiaatteeseen: luottamuksellisuuteen, saatavuuteen ja eheyteen. Näihin kolmeen osa-alueeseen viitataan yleensä CIA-mallilla, jonka avulla näitä perusperiaatteita on mahdollista hahmottaa. [13]

Luottamuksellisuus (engl. confidentiality) tarkoittaa tiedon suojaamista siten, että vain valtuutetuilla henkilöillä on pääsy kyseiseen tietoon. Tämä varmistaa, etteivät arkaluonteiset tiedot, kuten henkilötiedot, päädy luvattomille tahoille väärinkäytettäväksi. Hyvin yksinkertainen esimerkki luottamuksellisuuden rikkomisesta on salasanan päätyminen ulkopuoliselle. Tällöin kyseinen henkilö pääsee halutessaan käsiksi henkilökohtaiseen tietoon ja pystyy myös käyttämään sitä väärin. [14]

Eheys (engl. integrity) tarkoittaa tiedon säilyttämistä tarkoitetussa muodossaan, siten ettei sitä pystytä muokkaamaan huomaamattomasti. Eheys suojaa tietoa sekä luvattomien että tahattomien muutosten varalta. Esimerkkinä tästä on tilanne, jossa tiedon osittaista poistamista tai muuttamista suorittaa taho, jolla ei ole oikeutta käsitellä kyseistä tietoa. Eheyden vaarantuminen voi myös tarkoittaa valtuutetun henkilön suorittamaa tiedon muokkausta, joka on epätoivottua tai virheellistä. Tiedon eheyttä voidaan varmistaa versionhallinnalla ja lokitiedostoilla. [14]

Saatavuus (engl. availability) tarkoittaa, että tieto ja tietojärjestelmät ovat käytettävissä tarvittaessa valtuutetuille käyttäjille, ja että ne toimivat oikein. Tämä varmistaa, että käyttäjät pääsevät käsiksi tarvitsemiinsa tietoihin aina, kun he niitä tarvitsevat. Saatavuuden varmistaminen on tärkeää, koska vaikeasti saatavilla oleva tieto on lähes hyödytöntä. Saatavuus voidaan turvata esimerkiksi varmuuskopioiden avulla. [14]

CIA-mallia voidaan myös täydentää Parkerin kuusikoksi [14]lisäämällä kolme uutta

käsitettä: autenttisuus, utiliteetti ja hallussapito. Tämä malli tarjoaa CIA-mallia kattavamman käsityksen tietoturvallisuuden osa-alueista.

Todennuksella (engl. authenticity) tarkoitetaan, että tieto voidaan todeta aidoksi ja sen voidaan varmistaa tulevan luotettavasta lähteestä. Esimerkki todennuksesta on verkkosivuston käyttäjätilin kirjautumisprosessi. Kun käyttäjä kirjautuu sivustolle käyttäjätunnuksen ja salasanan avulla, järjestelmä tarkistaa, että nämä tiedot vastaavat tallennettuja tietoja. Tietojen täsmätessä käyttäjä päästetään sivustolle. [14]

Käyttökelpoisuudella (engl. utility) tarkoitetaan tiedon käyttökelpoisuutta käyttäjälle. Tämä tarkoittaa, että tieto on esitetty sellaisessa muodossa, että se on hyödyllinen käyttäjälle. Esimerkkinä käyttökelpoisuudeesta toimii varastettu muistitikku. Jos muistitikulle tallennettu tieto on hyvin salattu, sen käyttökelpoisuus varkaalle on pieni. Toisaalta, jos tietoa ei ole salattu mitenkään, se on helposti käytettävässä muodossa. [14]

Hallinnalla (engl. possession) tarkoitetaan tiedon tallenusmedian fyysistä sijaintia ja hallintaa. Tämä tarkoittaa, että tiedon fyysistä olinpaikkaa voidaan turvata ja vartioida asiattomalta pääsyltä. Tässäkin esimerkissä toimii hyvin muistitikku. Kun muistitikku on valtuutetulla henkilöllä ja vain hän tietää tikun olinpaikan, on tieto suojattuna. [14]

Seuraavassa kuvassa on havainnollistettu Parkerin kuusikkoa ja sen osa-alueiden yhtenäisyyksiä:

Kuvaan on merkitty kuusikon osa-alueet eri väreillä havainnolistamaan niiden riippuvuutta toisistaan. Parkerin kuusikko täydentää CIA-mallia ottamalla huomioon myös inhimillisen puolen tietoturvassa.

Luottamuksellisuus ja hallussapito täydentävät toisiaan, minkä vuoksi ne on merkitty kaavioon samalla värillä. Voidaan ajatella, että jokainen rike luottamusta vastaan on myös rike hallussapitoa vastaan. Salasanan päätyminen vääriin käsiin rikkoo sekä luottamuksellisuutta että hallussapitoa. Toisaalta, hallusapidon rikkoutuminen ei suoraan tarkoita myös luottamuksellisuuden rikkoutumista. Muistitikku voidaan varastaa, mutta sen sisältämään tietoon ei välttämättä päästä vielä käsiksi.

Kuva 2.1: Parkerian Hexad -malli

Eheys ja todennus on myös merkitty kaavioon samalla värillä, sillä todennus on luotu täydentämään eheyttä. Siinä, missä eheys tarkastelee tiedon säilyttämistä halutussa muodossa, todennus tarkastelee tiedon lähteen luotettavuutta.

Saatavuus ja käyttökelpoisuus muistuttavat pitkälti toisiaan. Molemmissa tarkastelun kohteena on tiedon käyttöönoton tehokkuus. Käyttökelpoisuus on luotu täydentämään saatavuuden puutteita. Esimerkiksi tieto voi olla helposti saatavilla muistitikulla, mutta sen käyttöönotto voi olla vaikeaa. Tieto voi olla salattuna salasanan taakse tai se voi olla vaikeasti tulkittavassa muodossa (esimerkiksi vieraalla kielellä tai koodilla kirjoitettuna).

2.2.1 Kolmannet osapuolet

Kolmannet osapuolet ovat usein verkkosivuston ylläpitäjän kanssa yhteistyössä toimivia tahoja, kuten mainosverkostoja ja analytiikkapalveluita, joille annetaan pääsy samoihin tietoihin kuin ylläpitäjälle. Kolmansien osapuolten tuottama tieto tarjoaa sivuston ylläpitäjille merkittävää kilpailuetua, sillä se mahdollistaa paremmin kohdennettujen palveluiden ja mainosten tarjoamisen. [15]. Kolmansien osapuolien haitta ilmenee kuitenkin siinä, miten ne keräävät ja käyttävät henkilökohtaista dataa käyttäjästä. Tätä dataa käytetään

käyttäjän profilointiin ja sen avulla kohdennettuun mainontaan.

Profiloinnilla tarkoitetaan prosessia, jossa henkilötietoja käsitellään automaattisesti, jotta voidaan muodostaa arvioita yksilön ominaisuuksista. Tavoitteena voi olla esimerkiksi ennustaa henkilön käyttäytymistä, kiinnostuksen kohteita tai kykyä suoriutua tietyistä tehtävistä. Profilointi liittyy usein asioihin, kuten terveyteen, taloudelliseen tilanteeseen tai liikkumiseen, ja sen avulla yksilö pyritään sijoittamaan johonkin ryhmään tai kategoriaan. Kaikki luokittelu ei kuitenkaan ole profilointia. Jos esimerkiksi ihmisiä ryhmitellään iän tai sukupuolen perusteella pelkästään tilastollisiin tarkoituksiin ilman, että yksilöistä tehdään henkilökohtaisia johtopäätöksiä, ei kyse ole profiloinnista. [16]

Tällaine kerätty data voi olla hyvin henkilökohtaista ja arkaluontoista, kuten uskonto, seksuaalinen suuntautuminen, terveydentila tai taloudellinen tila. Tällaisen tiedon vuotaminen eteen päin kolmansilta osapuolilta voi altistaa käyttäjät epäedulliseen tai jopa vaaralliseen tilanteeseen. Tämän työn kannalta on keskeistä tarkastella käyttäjän dataa kerääviä kolmansia osapuolia, joita ovat esimerkiksi Google Analytics ja Meta.

2.2.2 Evästeet

Evästeet (engl. cookies) ovat tiedostoja, jotka tallennetaan käyttäjän tietokoneelle, kun verkkoselain kommunikoi palvelimen verkkosivuston kanssa. Nämä tiedostot sisältävät yleensä tietoa asiakkaan ja palvelimen välisestä toiminnasta, kuten käyttäjän istuntoon liittyviä tietoja, mieltymyksiä ja käyttöasetuksia. Oletuksena nykyaikaiset selaimet hyväksyvät evästeet, eli ne sallivat selaimen tallentaa nämä tiedostot käyttäjän tietokoneelle ja säilyttää niitä palvelimen määrittämän ajan.

Evästeitä käytetään verkkosivuilla moniin tarkoituksiin, kuten parantamaan käyttäjäkokemusta tallentamalla käyttäjän mieltymyksiä, ylläpitämään käyttäjän istuntoa, seuraamaan sivuston käyttöä analytiikkatarkoituksiin ja kohdentamaan mainoksia käyttäjän kiinnostuksen kohteiden perusteella. Evästeiden ongelma piilee siinä, ettei käyttäjä ole aina tietoinen siitä, että verkkosivu kerää tietoa hänestä. Kaikki verkkosivut eivät ilmoita

käyttävänsä evästeitä, jolloin käyttäjälle ei anneta mahdollisuutta kieltäytyä tai vaikuttaa hänestä kerättävän tiedon laatuun. Tämä voi johtaa siihen, että käyttäjät eivät ole tietoisia, kuinka paljon ja mitä tietoa heistä kerätään, ja mihin tarkoituksiin sitä käytetään. [17]

Monet verkkosivut sisältävät myös kolmansien osapuolien käyttämiä evästeitä, jotka keräävät tietoa käyttäjän toiminnasta verkkosivuilla. Nykyään useat verkkosivut myös vaativat kolmansien osapuolien evästeiden hyväksynnän ehtona sivun käyttämiseen. [17]

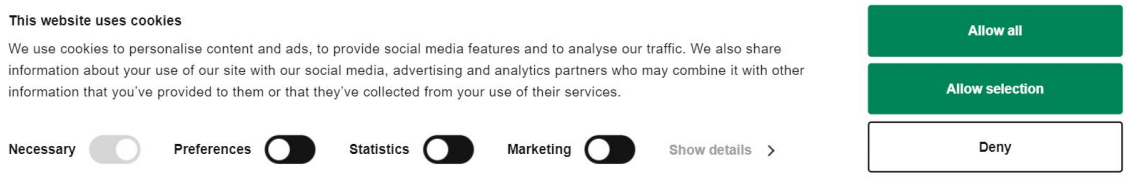
Evästeiden käyttöön liittyvät yksityisyysongelmat ovat johtaneet siihen, että monet maat ovat ottaneet käyttöön yksityisyyteen liittyvää lainsäädäntöä, kuten GDPR, joka edellyttää, että verkkosivustot hankkivat käyttäjien suostumuksen ennen evästeiden tallentamista ja antavat selkeää tietoa siitä, miten evästeitä käytetään. Tämä auttaa käyttäjiä hallitsemaan paremmin yksityisyyttään verkossa ja tekee evästeiden käytöstä läpinäkyvämpää. [18]

2.2.3 Pimeät käytännöt

Vaikka evästeiden läpinäkyvyyttä on pyritty parantamaan lainsäädännöllä, liittyy niihin silti vielä paljon yksityisyysongelmia. Lainsäädännön kiristymisen myötä kolmannet osapuolet ovat kehitelleet erilaisia taktiikoita käyttäjän ohjaamiseen siten, että kaikki sivustolla olevat evästeet saisivat käyttäjältä luvan toimia.

Tällaisia ohjaamisen huijaamisen ja harhaanjohtamisen keinoja kutsutaan pimeiksi käytännöiksi (eng. dark patterns). Pimeitä käytäntöjä käytetään verkkosivuilla ohjaamaan käyttäjäkokemusta käyttäjälle mahdollisesti haitallisella tavalla. Niiden tarkoituksena on saada käyttäjät tekemään tahattomia ja vastentahtoisia päätöksiä henkilötietojensa käsittelystä tietämättään. [19] Kuva 2.2 esittää Suomen evankelisluterilaisen kirkon (evl.fi) verkkosivujen evästeiden hyväksyntää.

Evästeiden hyväksyntä verkkosivuilla rakentuu usein useasta kerroksesta. Ensimmäinen kerros on tavallisesti verkkosivun alareunaan tai keskelle ilmestyvä ilmoitusbanneri, joka kertoo evästeiden käytöstä. Tässä vaiheessa käyttäjälle tulisi tarjota mahdollisuus hy-



Kuva 2.2: Suomen evankelis-luterilaisen kirkon verkkosivujen banneri

väksyä kaikki evästeet, hyväksyä ainoastaan välttämättömät evästeet tai kieltäytyä evästeistä kokonaan. Kun nämä vaihtoehdot ovat näkyvillä heti ensimmäisessä vaiheessa, voidaan seuraavaksi tarkastella käyttöliittymän visuaalisia ratkaisuja, erityisesti painikkeiden väritystä.

Yleinen käytäntö on käyttää visuaalisia keinoja ohjaamaan käyttäjää valitsemaan kaikkien evästeiden hyväksyminen. Esimerkiksi ”Hyväksy kaikki” -painike saatetaan korostaa kirkkaalla ja huomiota herättävällä värillä, kun taas ”Hylkää” tai ”Hyväksy vain välttämättömät” -painikkeet voivat olla hillitympiä ja sulautua taustaan. Tällainen suunnitteluratkaisu voi ohjata käyttäjää tekemään päätöksen, joka ei välttämättä vastaa hänen todellista tahtotilaansa tai tietoista harkintaansa.

Joissakin tapauksissa ensimmäinen kerros ei tarjoa lainkaan suoraa mahdollisuutta evästeistä kieltäytymiseen. Käyttäjälle esitetään tällöin vain vaihtoehdot hyväksyä evästeet tai siirtyä tarkempiin asetuksiin. Kieltäytyminen vaatii siis siirtymistä evästeiden hyväksynnän toiseen kerrokseen, jossa asetuksia voidaan muokata yksityiskohtaisemmin.

Toinen kerros sisältää tyypillisesti mahdollisuuden hallita eri evästekategorioita, usein valintaruutujen avulla. Näiden avulla käyttäjä voi erikseen sallia tai estää esimerkiksi tilastolliset, markkinointiin liittyvät tai personointia koskevat evästeet. Yksi yleinen dark pattern -menetelmä tässä vaiheessa on käyttää valmiiksi aktivoituja valintaruutuja, jolloin käyttäjän tulee itse aktiivisesti poistaa ei-toivotut evästeet käytöstä. Tällainen asettelu vaatii käyttäjältä enemmän aikaa ja vaivannäköä, ja voi johtaa siihen, että ei-toivottuja evästeitä jää käyttöön passiivisuuden tai epätietoisuuden seurauksena.

Kuvasta 2.2 huomataan, että ruudut ovat tässä tapauksessa jo ensimmäisessä kerrok-

sessa, eikä niitä ole valmiiksi aktivoitu. Tämä on esimerkki hyvistä käytänteistä, joita jokaisen sivuston pitäisi harjoittaa.

2.2.4 Tietosuojaseloste

Tietosuoja on yksilön perusoikeus, joka turvaa rekisteröidyn oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Sen keskeisenä tavoitteena on määrittää, milloin ja millä edellytyksillä henkilötietojen käsittely on sallittua. Henkilötietojen käsittelylle tulee aina olla lakiin perustuva oikeutus, ja toiminnan lainmukaisuutta valvoo riippumaton viranomainen. Näitä tietoja voidaan säilyttää eri muodoissa, kuten sähköisissä järjestelmissä, paperiasiakirjoissa tai audiovisuaalisissa tallenteissa. Henkilö, jota tiedot koskevat, on rekisteröity, kun taas rekisterinpitäjä määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Rekisterinpitäjän puolesta toimiva ulkopuolinen taho on henkilötietojen käsittelijä. Tietosuoja eroaa tietoturvasta siten, että tietoturva on väline tietosuojan toteuttamiseen. [11][20]

Tietosuojaseloste on keskeinen väline henkilötietojen käsittelyn läpinäkyvyyden varmistamisessa ja rekisteröidyn informointivelvollisuuden täyttämisessä. Se toimii dokumentoituna kuvauksena siitä, miten henkilötietoja kerätään, käytetään, säilytetään ja suojataan, ja on näin olennainen osa tietosuojalainsäädännön mukaista osoitusvelvollisuutta. [21] Tietosuojaselosteessa esitetään muun muassa rekisterinpitäjän ja mahdollisten henkilötietojen käsittelijöiden yhteystiedot, käsittelyn tarkoitukset, käsiteltävien tietojen tyypit, tietojen säilytysajat, vastaanottajat ja mahdolliset tiedonsiirrot EU:n tai ETA-alueen ulkopuolelle. Lisäksi selosteessa kuvataan rekisteröidyn oikeudet, kuten oikeus saada pääsy omiin tietoihinsa, oikaista virheellisiä tietoja tai vaatia tietojen poistamista. Tietosuojaselosteen julkinen saatavuus, esimerkiksi verkkosivustolla, tukee tietosuojan läpinäkyvyyttä ja vahvistaa yksilön mahdollisuuksia valvoa omien henkilötietojensa käsittelyä. [22][19]

3 Tietovuotojen analyysi seurakuntien verkkosivuilla

3.1 Tutkimusympäristö ja menetelmä

Tutkimuskohteeksi valittiin Suomen evankelis-luterilainen kirkko sen suuren jäsenmäärän ja erityisen valtiollisen aseman vuoksi. Evankelis-luterilainen kirkko on Suomen suurin kirkko, jolla on yli 3,5 miljoonaa jäsentä. [23] Tämä tarkoittaa, että noin 65,1 % Suomen väestöstä kuuluu tähän kirkkoon, mikä tekee siitä merkittävän osan suomalaista yhteiskuntaa. Evankelis-luterilaisella kirkolla on erityinen asema kansankirkkona (yhdessä Suomen Ortodoksisen kirkon kanssa) ja se pystyy myös verottamaan jäseniään.[24]

Suomessa on yhteensä 345 evankelis-luterilaista seurakuntaa, jotka sijaitsevat jokaisessa Suomen kunnassa [25]. Tämän lisäksi Suomi on jaettu alueellisesti yhdeksään hiippakuntaan, joiden alaisuuteen seurakunnat kuuluvat. Hiippakunnat toimivat alueellisina halllintoyksikköinä ja johtavat seurakuntien toimintaa piispojen johdolla. [26]

Suuren jäsenmääränsä ja satojen seurakuntien myötä evankelis-luterilaisen kirkon verkkosivuilla on myös paljon mahdollisia kävijöitä. Koska kyseessä on uskonnollisen yhteisön sivustot, niiden sisältöä voidaan pitää arkaluoontoisena ja henkilökohtaisena. Sivustot voivat sisältää tietoa uskonnollisista tapahtumista, kirkkoon liittymisestä sekä muista henkilökohtaisia uskonelämään liittyvistä asioita. Tämän vuoksi olisi erityisen tärkeää kiinnittää huomiota yksityisyyden suojaan näillä sivuilla.

Suuren määränsä vuoksi tutkimukseen ei voitu valita kaikkia kirkon seurakuntia, vaan tutkittavat verkkosivut valittiin seuraavien kriteerien mukaan:

- Jokaisesta hiippakunnasta valittiin satunnaisesti kaksi verkkosivua
- Kaikki yhdeksän hiippakuntaa valittiin
- Kaikki seurakunnat, jotka eivät käyttäneet kirkon omaa verkkosivupohjaa (Lukkari), valittiin mukaan tutkimukseen. Itsenäisinä verkkosivuina, niiden oletettiin sisältävän erilaisia kolmansia osapuolia ja tietovuotoja.
- Evankelis-luterilaisen kirkon pääsivusto (evl.fi) valittiin myös tutkittavaksi.

Kaiken kaikkiaan tutkimukseen valittiin 31 verkkosivua, joista 17 käytti samaa Lukkari-pohjaa.

Lukkari on Suomen evankelis-luterilaisen kirkon kehittämä verkkosivustojen julkaisualusta, jonka tavoitteena on luoda yhteinäiset verkkosivut kaikille Suomen evankelis-luterilaisille seurakunnille. Vuoden 2024 alussa 96 % seurakunnista oli julkaissut Lukkari-verkkosivunsa. [27]

Lukkari-alustaa käyttävillä sivustoilla oli yhtenäinen paneeli evästeiden hallinnoimiselle. Myös tietosuojaseloste oli jokaisella sivustolla sama ja se ohjasi käyttäjän kirkon pääsivustolle.

3.1.1 Verkkoliikenteen tallentaminen

Tämä tutkimus perustui lähtökohtaisesti verkkoliikenteen tallentamiseen ja tutkimiseen eri verkkosivuilla. Verkkoliikenteen tallentamiseen käytettiin Google Chromen kehittäjätyökaluja (engl. *Developer Tools*), jonka jälkeen tallennetut tulokset vietiin HAR-tiedostoihin (lyhenne *HTTP Archive*)[1].

[1]HAR-tiedostoformaattia käytetään verkkoliikenteen tallentamiseen ja analysointiin. Se sisältää mm. HTTP-pyynnöt, vastaukset, otsikkotiedot ja mahdollisesti pyyntöjen mukana kulkevaa hyötykuormaa. Formaatti soveltuu erinomaisesti verkkosivujen tietovuotojen tutkimukseen.

Tutkimus aloitettiin siirtymällä halutulle verkkosivustolle. Tämän jälkeen selaimen välimuisti tyhjennettiin, jotta aiemmin tallennettu tieto ei vaikuttaisi tutkimustuloksiin. Sivustolla hyväksyttiin kaikki evästeet, mikä oli tutkimuksen kannalta oleellista, sillä tarkastelun kohteena oli erityisesti kolmansien osapuolten keräämä tieto. Toisaalta tutkimusasetelma olisi voinut keskittyä myös siihen, mitä tietoa kolmansille osapuolille välittyy ilman käyttäjän nimenomaista suostumusta. On kuitenkin huomattava, että käyttäjä hyväksyy evästeet usein oletuksena tai automaattisesti, esimerkiksi värikkäästi korostetun ”Hyväksy kaikki” -painikkeen tai muiden pimeiden käytäntöjen vuoksi.

Seuraavaksi suoritettiin haku sivuston hakutoiminnolla, mikäli sellainen oli käytettävissä, ja navigoitiin muille verkkosivuston alasivuille. Erityistä huomiota kiinnitettiin sivuihin, joiden sisältö saattoi paljastaa käyttäjän uskonnon harjoittamiseen liittyvää tietoa. Näihin kuuluivat esimerkiksi tapahtumasivut, jotka käsittelivät jumalanpalveluksia, hartauksia tai kristillisiä perhejuhlia. Lisäksi tarkasteltiin sivuja, joilla käsiteltiin lahjoitusten tekemistä, sielunhoitoa tai sosiaalista tukea, kuten päihdeongelmista kärsiville suunnattua apua.

Verkkoliikenteen tallentamisen ensisijaisena tarkoituksena oli selvittää, vuotiko käyttäjää koskevaa arkaluonteista tietoa kolmansille osapuolille HTTP-pyyntöjen kautta. Tallennetuista tiedoista suodatettiin pois kaikki muut kuin kolmansille osapuolille (eli tutkittavan verkkosivuston ulkopuolisille domaineille) kohdistuvat HTTP-pyynnöt. Näiden suodatettujen pyyntöjen hyötykuormat analysoitiin manuaalisesti mahdollisten tietovuotojen tunnistamiseksi.

Erityisesti etsittiin kahta tietovuototyyppiä:

- **Hakutermit**: Käyttäjän kirjoittamat hakusanat voivat paljastaa yksityisiä ja henkilökohtaisia tietoja, kuten kiinnostuksen uskonnollisiin tapahtumiin tai palveluihin. Tällaiset hakutermit saattavat paljastaa henkilön uskonnollisen vakaumuksen tai hengelliset tarpeet.

- **Sivun URL-osoitteet**: Useilla seurakuntien verkkosivuilla yksittäiset tapahtumat tai

palvelut (esimerkiksi *jumalanpalvelus*, *apua ja tukea* tai *lahjoita*) sijaitsevat omilla alasivuillaan. Kun näiden sivujen URL-osoitteet vuotavat kolmansille osapuolille, ne voivat paljastaa, millaiseen uskonnolliseen toimintaan käyttäjä on kiinnostunut osallistumaan.

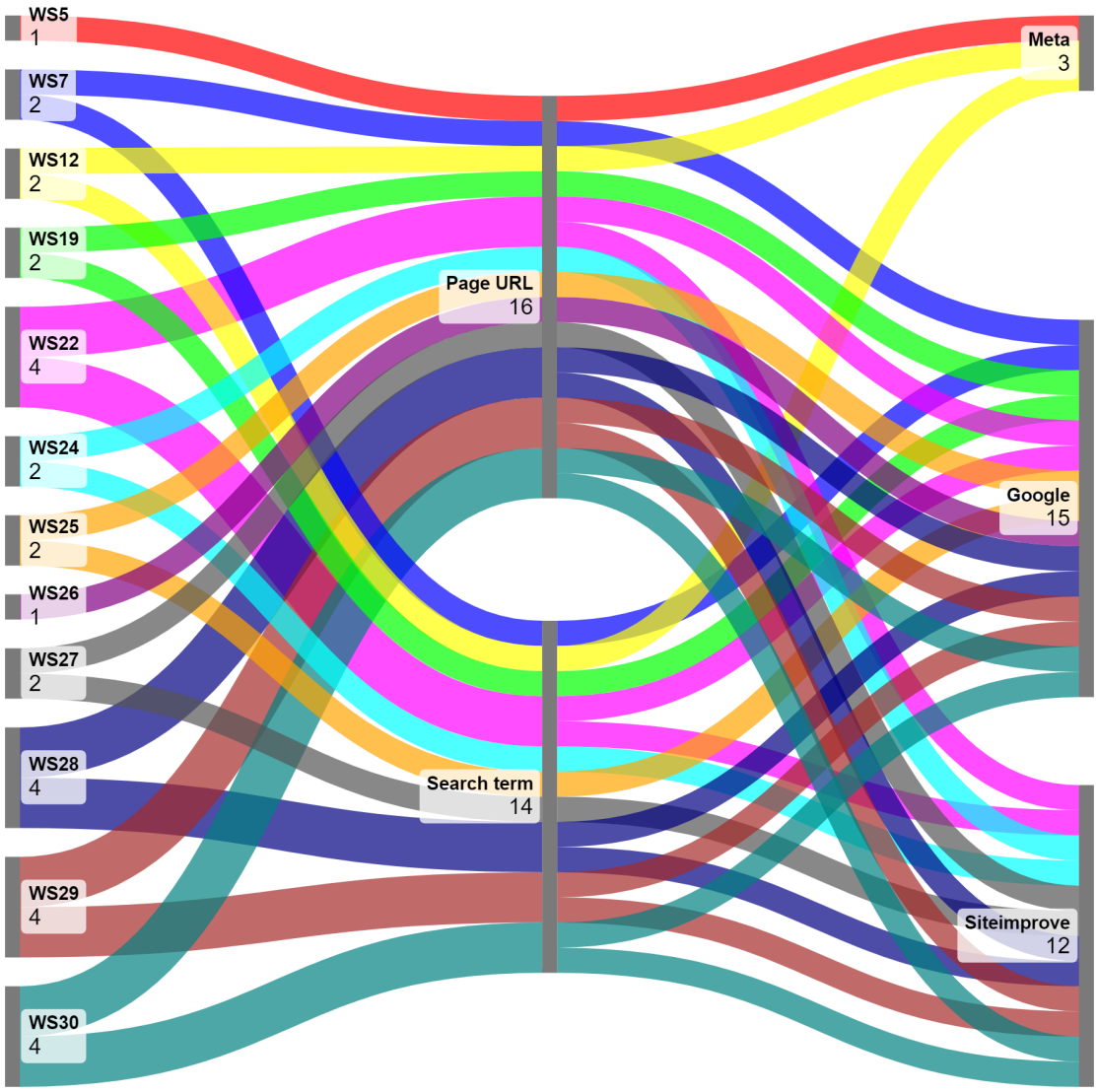
Nämä tietovuodot muodostavat erityisen yksityisyyshuolen, kun niitä tarkastellaan yhdessä yksilöivän teknisen tiedon, kuten IP-osoitteiden tai evästeiden kautta saatavien asiakastunnisteiden, kanssa. Kolmannet osapuolet, kuten Google tai Meta, voivat näin ollen yhdistää käyttäjän henkilöllisyyden ja uskonnolliset kiinnostuksenkohteet, mikä rikkoo yksityisyyden suojaa ja voi johtaa vakaviin seurauksiin käyttäjän tietoturvalle ja yksityisyydelle.

3.1.2 Verkkoliikenteen analysointi

Kuvassa 3.1 esitetään vakavimmat havaituista tietovuodoista: sivun URL-osoitteiden ja hakutermien vuotaminen 31 tutkitulla Suomen evankelis-luterilaisen kirkon verkkosivustolla. Vasemmalla puolella esitetään kunkin verkkosivuston kokonaisvuotomäärät (sekä URL-osoitteiden että hakutermien vuodot). Keskellä vuototiedot on jaettu kahteen kategoriaan: sivun URL-osoitteiden vuodot ja hakutermien vuodot. Oikealla näkyy, kuinka monta tietovuotoa kukin kolmas osapuoli vastaanotti.

Kuten kuvasta käy ilmi, sivun URL-osoitteita vuoti 16 kertaa ja hakutermejä 14 kertaa. Vuotaneiden tietojen vastaanottajina toimivat Google, Meta ja Siteimprove. Ei ole yllättävää, että Google Analytics vastasi 50 % kaikista URL- ja hakutermivuodoista, sillä sen on todettu olevan suurin yksittäinen syy verkkosivustojen seurantaan ja tietovuotoihin [28][5]. Tässä tutkimuksessa Meta oli kuitenkin vastaanottajana vain kolmessa tietovuodossa, kun taas huomattavasti pienempi analytiikkapalvelu Siteimprove keräsi 12 tietovuotoa. Tämä selittyy sillä, ettei verkkosivustoilla käytetty Metan varsinaista analytiikkatyökalua (Meta Pixel), vaan hyödynnettiin sosiaalisen median liitännäisiä.

Kaiken kaikkiaan vain 12/31 (38,7 %) tutkituista verkkosivustoista sisälsi tietovuotoja,



Kuva 3.1: Tietovuodot seurakuntien verkkosivuilla

mitä voidaan pitää hyvänä tuloksena, etenkin kun otetaan huomioon, että tutkimuksessa valittiin tarkoituksella mukaan useita verkkosivustoja, joiden epäiltiin todennäköisemmin vuotavan tietoja, eli sellaisia, jotka eivät käyttäneet kirkon Lukkari-alustaa.

Niillä verkkosivustoilla, joilla tietovuotoja havaittiin, oli keskimäärin 2,5 vuotoa per sivusto. Pienin määrä vuotoja yhdellä sivustolla oli 1 ja suurin 4.

3.1.3 Tietosuojaseloste ja pimeät käytännöt

Tutkimuksessa havaittiin, että neljällä verkkosivustolla ei nimetty kolmansia osapuolia tietosuojakäytännöissä tai evästebannereissa, vaikka verkkoliikenteen analyysi osoitti kolmansien osapuolien olevan läsnä. Sen sijaan 25 muulla verkkosivustolla, joilla kolmansia osapuolia oli mukana, nämä mainittiin joko tietosuojaselosteissa tai evästebannereissa, mikä katsottiin myönteiseksi tulokseksi.

Tutkimuksessa kuitenkin todettiin, ettei yhdelläkään käyttäjätietoja keränneellä sivustolla informoitu käyttäjiä riittävästi yksilöllisen tunnistamisen mahdollisuudesta. Myöskään sitä, että vierailtuja URL-osoitteita tai hakutermejä jaetaan kolmansille osapuolille, ei mainittu tietosuojaselosteissa tai evästeiden suostumusbannereissa, vaikka näin usein tapahtui. Kahdeksan sivuston havaittiin kuitenkin viittaavan epämääräisesti siihen, että käyttäjien sivuston käyttöä seurataan. Uskonnollisten vakaumusten vuotamisen mahdollisuutta ei mainittu kertaakaan.

Kaikkien seurakuntien tutkittujen verkkosivustojen tietosuojakäytännöt ja evästeiden suostumusbannerit todettiin keskenään identtisiksi. Samoin todettiin, että myös hiippakuntien verkkosivustoilla käytetyt tietosuojakäytännöt ja evästebannerit olivat yhtä lukuun ottamatta identtisiä. Toisin sanoen seurakunnissa käytettiin yhtä mallipohjaa ja hiippakunnissa toista. Tästä huolimatta havaittiin, että verkkosivustojen sisältämät kolmannet osapuolet vaihtelivat.

Monissa hiippakuntien tietosuojaselosteiden kohdissa tiedonkeruun mahdollisuus selostettiin teknisin termein, joiden katsottiin olevan vaikeasti ymmärrettäviä keskivertokäyttäjälle. Tämän ongelman on aiemmin tunnistanut myös muu tutkimus [29]. Lisäksi havaittiin, että tiedonkeruumenetelmien luokittelut olivat usein virheellisiä tai epäselviä.

Seurakuntien tietosuojaselosteiden todettiin linkittävän samaan verkkosivustoon, jota ylläpitää Suomen evankelis-luterilainen kirkko [30]. Sivustolla listattiin kaikki käytössä olevat kolmannet osapuolet, ja evästeiden käyttöä selitettiin lyhyesti yleiskielisesti. Tarkemmat tiedot evästeistä tarjottiin kuitenkin linkkien kautta, jotka johtivat analytiikkapal-

velujen omille verkkosivuille. Näiden verkkosivujen todettiin useimmiten olevan englanninkielisiä ja vaativan käyttäjältä lupaa tietojen keräämiseen, mitä pidettiin ongelmallisena. Käyttäjän nähtiin joutuvan siirtymään kolmannen osapuolen sivustolle ja tekemään päätös tietojen keräämisestä, vain saadakseen tietoa siitä, miten alkuperäisellä seurakunnan sivustolla käytetyt evästeet toimivat.

Tutkimuksessa todettiin, että 31 verkkosivustosta 5 ei pyytänyt lainkaan suostumusta evästeiden ja henkilötietojen keräämiseen, vaikka henkilötietoja kerättiin. Positiivisena havaintona todettiin, että muissa tutkituissa evästebannereissa esitettiin hylkäyspainike jo ensimmäisellä kerroksella, eikä valintaruutuja ollut esivalittuina.

Kuitenkin yhdeksällä verkkosivustolla havaittiin, että evästebannereissa korostettiin hyväksymispainiketta visuaalisesti kirkkailla väreillä ja kontrastilla, mikä nähtiin ongelmallisena. Lisäksi havaittiin, että hylkäyspainike oli aina merkitty muodossa ”Salli vain välttämättömät”, mitä pidettiin osittain harhaanjohtavana.

Valintaruutujen väreissä havaittiin myös poikkeama vakiintuneesta käytännöstä: annettu suostumus esitettiin vaaleanharmaana ja suostumuksen puute mustana. Tämä nähtiin harhaanjohtavana, sillä yleensä valitsemattomat ruudut esitetään vaaleampina ja valitut tummempina. Käytännössä värien käyttötapa oli näissä bannereissa käännetty tavanomaisesta käytännöstä poikkeavaksi.

3.2 Myönteiset huomiot

Tietosuojalinjausten noudattaminen. Toisin kuin monet muut julkisen sektorin toimijat, Suomen evankelis-luterilainen kirkko on ottanut vakavasti apulaistietosuojavaltuutetun näkemykset kolmansien osapuolten hyödyntämisestä verkkosivustoilla sekä seuranta- ja analytiikkateknologioiden käytön huolellisesta arvioinnista. Tämä osoittaa, että tietosuojaviranomaisten suosituksilla ja linjauksilla voi olla konkreettista vaikutusta yksityisyyden suojan toteutumiseen verkkopalveluissa. Esimerkiksi monet kunnat eivät ole noudattaneet näitä ohjeistuksia yhtä johdonmukaisesti. Vaikka tutkimuksesta saadut havainnot ovat so-

vellettavissa myös muihin uskonnollisiin yhteisöihin, on epätodennäköistä, että kaikki toimijat ovat yhtä tarkasti seuranneet yksityisyydensuojaa koskevia suosituksia. Sama ilmiö näkyy myös muilla sektoreilla, kuten terveydenhuollossa, jossa verkkopohjaisissa palveluissa ilmenee usein puutteita tietosuojan toteutuksessa.

Yhteinen alusta ja selkeät suositukset. Valtaosa verkkosivustoista käyttää samaa julkaisualustaa, Lukkaria, ja kirkko suosittelee vahvasti paikallisen analytiikkaratkaisun, Matomon, käyttöä Google Analyticsin sijaan. Matomo mahdollistaa sen, että kirkko voi hallita kerättyä dataa ilman, että käyttäjien henkilötietoja jaetaan kolmansille osapuolille [31], [32]. Vaikka yhteisen alustan käyttö voi joissain tapauksissa heikentää yksityisyyden suojaa esimerkiksi helpottamalla kolmansien osapuolten analytiikkaratkaisujen sisällyttämistä [33], se voi oikein toteutettuna myös vähentää tietovuotojen riskiä merkittävästi.

Google Analyticsista luopuminen. Hyödyntämällä yhteistä julkaisualustaa kirkko on järjestelmällisesti siirtynyt pois Google Analyticsin käytöstä. Tätä palvelua on pidetty yksityisyyden kannalta ongelmallisena ja jopa laittomana tietyissä olosuhteissa. On kuitenkin syytä täsmentää, että apulaistietosuojavaltuutettu ei ole ottanut kantaa Google Analyticsin laillisuuteen sinänsä, vaan on painottanut sen käyttöön liittyviä tietosuojariskejä julkisen sektorin verkkopalveluissa.

Siirtyminen pois kolmannen osapuolen analytiikasta. Suomen evankelis-luterilaisen kirkon esimerkki osoittaa, että myös aikaisemmin Google Analyticsilla kerätty analytiikkadata voidaan siirtää Matomo-järjestelmään. Siirtymä ei kuitenkaan ole täysin suoraviivainen tai nopea prosessi erityisesti silloin, kun vanhaa dataa on kertynyt paljon.

Pienen kolmansien osapuolien joukon käyttö. Kirkon verkkosivustot käyttivät vain hyvin rajoitettua määrää kolmannen osapuolen palveluita, ja tietoja vuoti ainoastaan kolmelle taholle (Google, Meta ja Siteimprove). Tämä mahdollistaa ulkopuolisten palveluiden tarkemman valvonnan ja parantaa käyttäjän yksityisyyden suojaa. Verrattuna muihin verkkosivustokategorioihin ja aikaisempiin tutkimuksiin, tämä voidaan nähdä erittäin myönteisenä tuloksena.

3.3 Ratkaistavat ongelmat

Yhteisen alustan puutteellinen käyttö ja suositusten laiminlyönti. Osa seurakuntien verkkosivustoista ei käyttänyt tarjolla olevaa Lukkari-alustaa, vaikka se on ollut käytettävissä jo noin kymmenen vuoden ajan. Lisäksi osa verkkosivustoista, joita ei ollut rakennettu tämän alustan avulla, käytti yhä Google Analyticsia, vaikka sen käyttöä on sekä kirkon että tietosuojaviranomaisten toimesta nimenomaisesti pidetty ei-toivottavana.

Riskialttiiden kolmansien osapuolien huomiotta jättäminen. Toinen keskeinen ongelma oli se, että joillakin sivustoilla tietosuojariskit sivuutettiin, vaikka käytössä oli yhteinen verkkosivualusta. Merkittävin esimerkki tästä oli tilanne, jossa kahden Lukkari-alustaa käyttäneen verkkosivuston kautta vuoti vierailtujen sivujen URL-osoitteita Metalle. Oli perusteltua rinnastaa Meta tietojen kerääjänä Googlen kaltaisiin toimijoihin, sillä aiemmat tutkimukset osoittivat, että Meta hyödynsi mahdollisesti arkaluonteisia henkilötietoja kaupallisiin tarkoituksiin, erityisesti mainonnassa [34]. Tästä näkökulmasta katsottuna apulaistietosuojavaltuutetun aiemmin esittämää kannanottoa olisi tullut soveltaa myös Metaan. Metan palveluiden käyttö ei siis ollut perusteltua sellaisilla verkkosivuilla, joilla käsiteltiin arkaluonteisia tietoja ja joilla tapahtui URL-osoitteiden vuotoa.

Epämääräiset tietosuojaselosteet. Kaikilla tutkituilla verkkosivustoilla käytettiin tietosuojaselosteita, jotka olivat yleisluonteisia ja monin paikoin epäselviä. Koska verkkosivustoilla käytetyt kolmannet osapuolet vaihtelevat, tulisi myös tietosuojaselosteiden kuvata tämä ja mainita selkeästi, mitä kolmannen osapuolen palveluita käytetään. Käyttäjällä tulisi olla mahdollisuus saada tietoa siitä, minkälaista henkilötietoa luovutetaan ja mille kolmansille osapuolille se jaetaan. Tietosuojaselosteissa tulisi myös mainita, että vierailtujen sivujen osoitteet ja aiheet voivat vuotaa kolmansille osapuolille, joista osa saattaa käsitellä tietoja Euroopan ulkopuolella.

Riittämätön suostumus. Kaikki verkkosivustot eivät pyytäneet suostumusta evästeiden ja henkilötietojen keräämiseen. Tämä rikkoo yleistä tietosuoja-asetusta (GDPR), kun sivusto käyttää evästeitä [35]. Uskonnollisiin vakaumuksiin liittyvien tietojen vuotaminen

on erityisen vakavaa silloin, kun suostumusta ei ole pyydetty. Vaikka yleinen suostumus tietojen keräämiseen olisikin pyydetty, uskonnollisiin vakaumuksiin liittyvää tietoa ei koskaan mainittu erikseen, ja on epätodennäköistä, että käyttäjä osaisi odottaa tällaista tietoa jaettavan kolmansille osapuolille.

3.4 Vaikutukset käyttäjille

Verkkosivustojen käyttäjiin kohdistuvat vaikutukset ovat erityisen merkittäviä silloin, kun kyse on uskonnolliseen vakaumukseen liittyvän tiedon vuotamisesta kolmansille osapuolille. Tällaiset tietovuodot voivat loukata käyttäjän yksityisyyttä ja luottamusta, erityisesti jos tiedot jaetaan ilman käyttäjän tietoista suostumusta tai ymmärrystä tapahtuneesta tiedonkäsittelystä.

Yksi keskeinen ongelma liittyy siihen, että yksilön uskonnollinen vakaumus voidaan päätellä epäsuorasti, esimerkiksi sen perusteella, mitä sivuja käyttäjä vierailee tai mitä hakutermejä hän käyttää seurakunnan verkkosivustolla. Kun nämä tiedot yhdistetään yksilöivään tekniseen tietoon, kuten IP-osoitteeseen tai evästeisiin perustuvaan tunnisteeseen, kolmannet osapuolet, kuten Google tai Meta, voivat yhdistää uskonnolliset kiinnostuksenkohteet suoraan tiettyyn henkilöön.

Tällä voi olla useita kielteisiä seurauksia. Käyttäjä saattaa kokea menettäneensä kontrollin henkilökohtaiseen tietoonsa ja tuntea ahdistusta siitä, että hänen uskonnolliset vakaumuksensa ovat joutuneet ulkopuolisten tietoon. Pahimmassa tapauksessa kerättyä tietoa voidaan käyttää esimerkiksi kohdennettuun mainontaan, vaikuttamisyrityksiin tai jopa poliittiseen profilointiin. Tämä ei ainoastaan herätä eettisiä kysymyksiä, vaan voi johtaa myös yksilön autonomian heikentymiseen.

Lisäksi tietyissä yhteiskunnissa tai yhteisöissä uskonnollinen vakaumus voi altistaa henkilön syrjinnälle, leimautumiselle tai muulle epäasialliselle kohtelulle. Erityisen huolestuttavia ovat tilanteet, joissa vuotaneet tiedot voivat joutua vihamielisten tai epäeettisten toimijoiden käsiin. Vaikka tällaiset skenaariot ovat harvinaisia esimerkiksi Suomessa,

niiden mahdollisuus on riittävä peruste varmistaa, että yksityisyyttä kunnioitetaan verkkoympäristössäkin.

On myös huomattava, että tietovuodot voivat vaikuttaa laajemminkin koko uskonnollisen yhteisön uskottavuuteen ja suhteeseen sen jäseniin. Mikäli kävijät menettävät luottamuksensa verkkopalveluihin, tämä voi vahingoittaa seurakunnan mainetta ja heikentää yhteisöllisyyden tunnetta. Luottamuksen säilyttäminen on keskeistä etenkin uskonnollisissa yhteisöissä, joissa yksityisyys ja luottamuksellisuus ovat usein syvällisesti sidoksissa hengelliseen elämään.

4 Johtopäätökset

Tämän tutkielman tavoitteena oli tarkastella, kuinka hyvin Suomen evankelis-luterilaisten seurakuntien verkkosivut turvaavat käyttäjiensä yksityisyyttä ja millaisia tietovuotoja kolmansille osapuolille mahdollisesti esiintyy. Tutkimustulosten perusteella voidaan todeta, että kokonaisuudessaan seurakuntien verkkosivustot tarjoavat varsin hyvän yksityisyydensuojan tason. Tämä liittyy erityisesti siihen, että suuri osa seurakunnista hyödyntää kirkon omaa Lukkari-julkaisujärjestelmää. Yhtenäinen alusta on auttanut edistämään hyvien tietosuojakäytäntöjen leviämistä ja vähentänyt yksittäisten sivustojen välillä esiintyvää vaihtelua.

Tutkimuksessa ilmeni kuitenkin merkittäviä poikkeamia, erityisesti sivustoilla, jotka eivät olleet Lukkari-alustan piirissä. Nämä sivustot osoittautuivat alttiimmiksi tietovuodoille, ja niillä havaittiin useammin kolmansien osapuolien, kuten Googlen ja Metan, analytiikka- ja seurantasovelluksia. Näiden palveluiden käyttö voi johtaa siihen, että käyttäjän uskonnollinen vakaumus paljastuu epäsuorasti esimerkiksi haettujen termien tai vierailtujen alasivujen kautta. Vaikka tällaisia vuotoja havaittiin vain osassa sivustoista, ne herättävät perusteltuja huolia erityisesti siitä näkökulmasta, että uskonnollinen vakaumus on luonteeltaan arkaluonteista henkilötietoa, jonka käsittely edellyttää erityistä huolellisuutta ja käyttäjän nimenomaista suostumusta.

Tutkimus toi esiin myös puutteita tietosuojaselosteiden ja evästebannereiden selkeydessä. Vaikka suurin osa sivustoista tarjosi muodollisesti hyväksyttävän suostumusmekanismin, moni toteutus sisälsi elementtejä, joita voidaan pitää käyttäjän päätöksentekoa

ohjaavina tai harhaanjohtavina pimeinä käytäntöinä. Esimerkiksi evästebannereiden visuaaliset painotukset, epätasapainoiset valintavaihtoehdot ja hämmentävät värikoodaukset saattoivat ohjata käyttäjää antamaan suostumuksen ymmärtämättä sen todellista laajuutta. Lisäksi tietosuojaselosteista puuttuivat usein tiedot siitä, millaisia henkilötietoja jaetaan kolmansille osapuolille ja missä laajuudessa näitä toimijoita on mukana.

Yhteenvetona voidaan todeta, että vaikka kirkko on ottanut merkittäviä askeleita yksityisyyden suojaamiseksi verkkoviestinnässään, työ ei ole vielä valmis. Erityisesti niillä verkkosivustoilla, jotka käsittelevät mahdollisesti arkaluonteisia tietoja, olisi perusteltua teettää riippumattomia tietosuojatarkastuksia. Lisäksi olisi tärkeää yhdenmukaistaa tietosuojaselosteiden sisältö ja varmistaa, että käyttäjille tarjotaan aidosti ymmärrettäviä ja tasapainoisia vaihtoehtoja evästesuostumuksen hallintaan. Käyttäjän mahdollisuus tietoon perustuvaan valintaan ja hänen oikeutensa yksityisyyteen tulee asettaa kaiken teknisen ja sisällöllisen suunnittelun keskiöön.

Lähdeluettelo

[1] O. Golan ja N. Stadler, ”Building the Sacred Community Online: The Dual Use of the Internet by Chabad”, *Media, Culture & Society*, vol. 38, nro 1, s. 71–88, 2016.

[2] P. H. Cheong, P. Fischer-Nielsen, S. Gelfgren ja C. Ess, ”Digital Religion, Social Media and Culture: Perspectives, Practices and Futures”, *Religion, Media and Digital Culture*, vol. 4, nro 1, s. 1–28, 2009.

[3] T. Hutchings, ”Contemporary Religious Community and the Online Church”, *Information, Communication & Society*, vol. 14, nro 8, s. 1118–1135, 2011.

[4] A. Vitullo, ”Multisite Churches: Creating Community from the Offline to the Online”, *Social Compass*, vol. 66, nro 1, s. 95–112, 2019.

[5] N. Samarasinghe, P. Kapoor, M. Mannan ja A. Youssef, ”No salvation from trackers: Privacy analysis of religious websites and mobile apps”, teoksessa *International Workshop on Data Privacy Management*, Springer, 2022, s. 151–166.

[6] H. Lohi, S. Rauti, P. Puhtila, T. Heino ja S. Rajapaksha, ”ICSEA 2024: The Nineteenth International Conference on Software Engineering Advances”, teoksessa *Proceedings of the International Conference on Software Engineering Advances (ICSEA 2024)*, S. Vasilache ja R. Kočí, toim., vol. 9, IARIA, 2024, s. 19–25.

[7] GDPR.eu, *What is GDPR, the EU's new data protection law?*, Accessed: 2025-04-21. url: `https://gdpr.eu/what-is-gdpr/`.

[8] T. Wambach ja K. Bräunlich, ”Data Privacy and Tracking: The Role of Third-Party Trackers in Website Traffic Analysis”, *Journal of Cyber Policy*, vol. 1, nro 2, s. 235–250, 2016.

[9] P. M. Schwartz, ”Information Privacy in the Cloud”, *University of Miami Law Review*, vol. 64, s. 471–493, 2011.

[10] Suomen perustuslaki, *10 § Yksityiselämän suoja*, https://www.finlex.fi/fi/laki/ajantasa/1999/19990731#L2P10, Viitattu 21.4.2025, 1999. url: https://www.finlex.fi/fi/laki/ajantasa/1999/19990731%5C#L2P10.

[11] Tietosuojavaltuutetun toimisto. ”Mikä on henkilötieto?” Viitattu 21.4.2025. (2025), url: https://tietosuoja.fi/mika-on-henkilotieto.

[12] Euroopan neuvosto, *Euroopan ihmisoikeussopimus – Artikla 8: Oikeus nauttia yksityis- ja perhe-elämän kunnioitusta*, https://www.echr.coe.int/documents/d/echr/convention_fin, Sopimus tehty 4.11.1950, voimaan 3.9.1953. Viitattu 21.4.2025, 1950.

[13] Jyväskylän yliopisto. ”Mitä on tietoturva?” Viitattu 21.4.2025. (2025), url: https://www.jyu.fi/fi/yliopistopalvelut/digipalvelut/palvelut/tietoturva/mita-on-tietoturva.

[14] G. Pender-Bey, ”The parkerian hexad”, *Information Security Program at Lewis University*, 2019.

[15] J. R. Mayer ja J. C. Mitchell, ”Third-party web tracking: Policy and technology”, teoksessa *2012 IEEE symposium on security and privacy*, IEEE, 2012, s. 413–427.

[16] Tietosuojavaltuutetun toimisto. ”Automaattinen päätöksenteko ja profilointi”. Viitattu 21.4.2025. (2025), url: https://tietosuoja.fi/automaattinen-paatoksenteko-profilointi.

[17] I. D. Mitchell, ”Third-party tracking cookies and data privacy”, 2012.

[18] Euroopan unioni. ”Verkkoyksityisyys: evästeet ja tietosuoja”. Viitattu 21.4.2025. (2025), url: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/online-privacy/index_fi.htm.

[19] Tietosuojavaltuutetun toimisto. ”Euroopan tietosuojaneuvostolta ohjeistusta valvontaviranomaisten yhteistyöstä ja sosiaalisen median käyttöliittymiä koskeva ohje”. Viitattu 21.4.2025. (2023), url: https://tietosuoja.fi/-/euroopan-tietosuojaneuvostolta-ohjeistusta-valvontaviranomaisten-yhteistyosta-ja-sosiaalisen-median-kayttoliittymia-koskeva-ohje.

[20] Tietosuojavaltuutetun toimisto. ”Tietosuoja”. Viitattu 21.4.2025. (2025), url: https://tietosuoja.fi/tietosuoja.

[21] Tietosuojavaltuutetun toimisto. ”Henkilötietojen käsittely”. Viitattu 21.4.2025. (2025), url: https://tietosuoja.fi/henkilotietojen-kasittely.

[22] Tietosuojavaltuutetun toimisto. ”Henkilötietojen siirrot Euroopan talousalueen ulkopuolelle”. Viitattu 21.4.2025. (2025), url: https://tietosuoja.fi/henkilotietojen-siirrot-etan-ulkopuolelle.

[23] Suomen evankelis-luterilainen kirkko. ”Perustietoa kirkosta”. Viitattu 21.4.2025. (2025), url: https://evl.fi/tietoa-meista/perustietoa-kirkosta/.

[24] Suomen evankelis-luterilainen kirkko. ”Kansankirkko”. Viitattu 21.4.2025. (2025), url: https://evl.fi/sanasto/kansankirkko/.

[25] Suomen evankelis-luterilainen kirkko. ”Seurakunnat”. Viitattu 21.4.2025. (2025), url: https://evl.fi/seurakunnat/.

[26] Suomen evankelis-luterilainen kirkko. ”Hiippakunta”. Viitattu 21.4.2025. (2025), url: https://evl.fi/sanasto/hiippakunta/.

[27] Suomen evankelis-luterilainen kirkko. ”Julkaistut – Lukkari”. Viitattu 21.4.2025. (2025), url: `https://lukkariohje.evlut.fi/tietoa-lukkarista/julkaistut`.

[28] T. Heino, S. Rauti, R. Carlsson ja V. Leppänen, ”Study of Third-Party Analytics Services on University Websites”, teoksessa *International Conference on Hybrid Intelligent Systems*, Springer, 2022, s. 1284–1292.

[29] C. D. Asay, ”Consumer information privacy and the problems (s) of third-party disclosures”, *Nw. J. Tech. & Intell. Prop.*, vol. 11, s. 321, 2012.

[30] Evangelical Lutheran Church of Finland. ”Evästeiden käyttö verkkosivuilla”. Viitattu: 21.4.2025. (2024).

[31] J. Gamalielsson, B. Lundell, S. Butler et al., ”Towards open government through open source software for web analytics: The case of Matomo”, *JeDEM-eJournal of eDemocracy and Open Government*, vol. 13, nro 2, s. 133–153, 2021.

[32] D. Quintel ja R. Wilson, ”Analytics and privacy”, *Information Technology and Libraries*, vol. 39, nro 3, 2020.

[33] S. Rauti, R. Carlsson, S. Mickelsson et al., ”Analyzing third-party data leaks on online pharmacy websites”, *Health and Technology*, s. 1–18, 2024.

[34] J. G. Cabañas, Á. Cuevas ja R. Cuevas, ”Unveiling and quantifying facebook exploitation of sensitive personal data for advertising purposes”, teoksessa *27th USENIX security symposium (USENIX security 18)*, 2018, s. 479–495.

[35] T. Wei, C. Cao ja Y. Shi, ”Personal Information Protection Behaviors of Consumers in Different Country Context and User Interface Designs”, teoksessa *International Conference on Human-Computer Interaction*, Springer, 2022, s. 82–98.