

Opinnäytetyö (AMK)

Liiketalous

Mediatuotanto

2023

Jari Pöllänen

DIGITAALINEN MARKKINOINTI EVÄSTEETTÖMÄSSÄ MAAILMASSA



OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Liiketalous | Mediatuotanto

2023 | 52 sivua

Jari Pöllänen

Digitaalinen markkinointi evästeettömässä maailmassa

Opinnäytetyöni käsittelee digitaalista markkinointia ja sen muuttumista yksityisyydensuojaa kunnioittavaan suuntaan. Yksityisyys on tärkeä tekijä käyttäjän luottamuksessa verkkopalveluihin, yrityksiin ja niiden tuotteisiin. Evästeiden käyttö on vähentymässä yksityisyydensuojan myötä. Evästeiden käytön väheneminen eri selaimissa on yksi keskeinen tekninen muutos digitaalisessa markkinoinnissa, vaikka evästeet ovat silti tärkeässä roolissa yritysten käyttämien digitaalisten markkinointikanavien ja työkalujen toiminnassa. Opinnäytetyössäni esittelen olennaisimpia esimerkkejä siihen, kuinka yritykset ottavat käyttöön uusia menetelmiä tietojen keräämiseen ja niiden käsittelyyn yksityisyydensuoja huomioiden. Lisäksi tutkin vaihtoehtoja siihen, kuinka yritykset voivat varautua digitaalisen markkinoinnin muuttumiseen evästeiden poistuessa ja käyn läpi esimerkkejä siitä, minkälaisia muutoksia suuret teknologiajätit ovat tehneet yksityisyydensuojan parantamiseksi.

Asiasanat:

Digitaalinen markkinointi, evästeet, yksityisyydensuoja, zero-party data

BACHELOR'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business | Media Management

2023 | 51 pages

Jari Pöllänen

DIGITAL MARKETING IN A COOKIELESS WORLD

My thesis focuses on digital marketing and its transformation towards respecting privacy. Privacy is an important factor in user trust towards online services, companies, and their products. The reduction of cookie usage in various web browsers is a key technical change in digital marketing, but cookies still play an important role in the operation of digital marketing channels and tools used by companies. In my thesis, I present some examples of how companies are adopting new methods for data collection and processing while taking privacy into account. Additionally, I explore alternatives for how companies can prepare for the changes in digital marketing as cookies are phased out and provide examples of the types of changes that major technology giants have made to enhance privacy.

Keywords:

Digital marketing, cookies, protection of privacy, zero-party data

Sisältö

Sanasto	6
1 Johdanto	10
2 Katsaus digitaaliseen markkinointiin	12
2.1 Digimarkkinoinnin tärkeimmät osa-alueet ja työkalut	13
2.2 M-RACE viitekehys	15
2.3 Digimarkkinoijan ensisijaiset työkalut ja käsitteet	17
2.4 Datan hyödyntäminen digimarkkinoinnissa	19
2.4.1 Datan tilastollinen mallintaminen	21
2.4.2 Segmentointi ja profilointi	22
3 Asiakaskokemus ja käyttäjätiedon kerääminen	25
3.1 Digitaalisen markkinoinnin muuttuminen	25
3.2 Henkilötiedon pseudonymisointi ja anonymisointi	26
3.3 Henkilötiedot ja epäsuorat tunnistimet	27
3.4 Yksityisyydensuoja ja rekisteröidyn oikeudet	27
3.5 Datan kerääminen ja käyttötarkoitussidonnaisuus	29
3.6 Muuttava lainsäädäntö: DSA ja DMA	30
4 Evästeiden maailma	33
4.1 Erilaisia evästeitä	33
4.2 Evästeiden poistuminen ja poistaminen	34
4.3 Googlen tekemät muutokset	35
4.4 Yrityksen mahdollisuudet evästeiden kadotessa	37
4.5 Kirjautunut käyttö	38
5 Tulevaisuus ja muutokset	40
5.1 Google PrivacySandBox	41
5.2 Google Topics	42
5.3 Apple ja iOS	43
6 Pohdintaa	46

Lähteet

49

Kuvat

Kuva 1. MRACE-viitekehys (Suomen Digimarkkinointi Oy, 2022).	16
Kuva 2. DMP esimerkki (SmartyAds, 2021).	19
Kuva 3. Esimerkki tilastollisesta mallintamisesta (Medium, 2022).	22
Kuva 4. Asiakkaiden segmentointi mahdollisuuksia (Hubspot, 2022).	23
Kuva 5. Chromen markkinaosuus (Oberlo, 2023).	35

Sanasto

AFFILIATE-markkinointi

digitaalisen markkinoinnin muoto, jossa yritys maksaa provisiota toiselle yritykselle tai yksittäiselle henkilölle näiden tuomasta liikenteestä, myynnistä tai muista tavoitteista. Affiliate-markkinointi perustuu yleensä linkkien jakamiseen ja niiden avulla tapahtuvaan liikenteen ohjaamiseen.

CDP

(Customer Data Platform) on asiakastietojen hallintajärjestelmä, joka kerää, yhdistää ja hallinnoi asiakastietoja eri tietolähteistä, kuten verkkosivuilta, CRM-järjestelmistä, sosiaalisesta mediasta ja muista sovelluksista. CDP mahdollistaa yrityksille asiakasprofiilien luomisen ja personoidun viestinnän tuottamisen asiakkaille. CDP:llä on merkittävä rooli asiakaskokemuksen parantamisessa ja yritysten liiketoiminnan kehittämisessä

DMP

(Data Management Platform) on ohjelmistopohjainen työkalu, joka kerää, tallentaa, käsittelee ja analysoidaan dataa eri lähteistä, kuten verkkosivustoista, mobiilisovelluksista ja mainonnan kampanjoista. DMP:n avulla yritykset voivat hallita ja hyödyntää dataa tehokkaammin markkinointistrategioissaan ja kohdentaa mainontaa tarkemmin halutuille kohderyhmille.

GDPR

on lyhenne sanoista General Data Protection Regulation, ja se on EU:n yleinen tietosuoja-asetus. GDPR tuli voimaan toukokuussa 2018, ja sen tarkoituksena on antaa yksilöille entistä paremman hallinnan omista henkilötiedoistaan ja niiden käytöstä. GDPR:n myötä yritykset ovat velvoitettuja noudattamaan tiukempia tietosuoja- ja tietoturvamääräyksiä, ja yksilöillä on oikeus pyytää tietoa, korjata tietoaan, ja pyytää tietojensa poistamista yritysten rekistereistä.

DATABROKER

on yritys tai organisaatio, joka kerää, ylläpitää ja myy tietoja kuluttajista, yrityksistä ja muista organisaatioista. Nämä tiedot voivat sisältää esimerkiksi

henkilökohtaisia tietoja, kuten nimi, osoite, sähköpostiosoite ja puhelinnumero, sekä muita tietoja, kuten ostohistoriaa, käyttäytymistä verkossa ja muita demografisia tietoja. Databrokerit toimivat usein markkinointi- ja mainostoimistojen sekä muiden yritysten kumppaneina, jotka käyttävät näitä tietoja kohdentaakseen markkinointia ja mainontaa tarkasti oikeille kohderyhmille.

LINERIAALINEN REGRESSIO

on matemaattinen menetelmä, jota käytetään tarkastelemaan kahden muuttujan välistä lineaarista suhdetta. Se pyrkii löytämään suoran, joka parhaiten sovittaa havainnot käytettävissä olevaan dataan. Lineaarisen regressiomallin avulla voidaan ennustaa yhden muuttujan arvo toisen muuttujan perusteella. Se on yleinen menetelmä esimerkiksi taloustieteessä, jossa sitä käytetään esimerkiksi hintojen ja kulutuksen välisten suhteiden tutkimiseen.

KLUSTEROINTI

tarkoittaa datan jakamista ryhmiin tai klustereihin, jotka ovat samanlaisia keskenään mutta erilaisia muiden klustereiden kanssa. Klusterointia käytetään yleisesti datan analysoinnissa ja datan kaivuussa sekä koneoppimisessa ja tilastollisessa mallintamisessa. Klusteroinnin avulla voidaan löytää tiettyjä kaavoja tai säännönmukaisuuksia, jotka auttavat ymmärtämään dataa paremmin ja tekemään sen perusteella parempia päätöksiä.

KONTEKSTUAALINEN KOHDENTAMINEN

tarkoittaa esimerkiksi mainosten näyttämistä käyttäjille tietyn kontekstin perusteella. Tämä tarkoittaa esimerkiksi sitä, että mainoksia näytetään verkkosivuilla käyttäjille, joiden selaimen hakusanat, sivuston aihe tai sisältö vastaavat mainoksen aihepiiriä. Kontekstuaalinen kohdentaminen pyrkii löytämään mainokselle sopivan ympäristön ja oikean kohdeyleisön, mikä lisää mainoksen tehokkuutta ja vähentää turhia näyttökertoja.

MRACE – VIITEKEHYS

on Suomen Digimarkkinoinnin (SDM) kehittämä malli, joka korostaa mittaamista digitaalisessa markkinoinnissa ja sen soveltamista eri osa-alueille.

PRIVACY BY DESIGN (PbD)

tarkoittaa tietosuojan huomioimista jo tuotekehitysvaiheessa ja sen integroimista osaksi tuotteen suunnittelua ja toteutusta. PbD:n tavoitteena on taata käyttäjän yksityisyyden suojaaminen ja tietoturvan korkea taso jo tuotteen käyttöönotosta lähtien. PbD:ssä huomioidaan esimerkiksi henkilötietojen käsittely, tietoturva, läpinäkyvyys ja käyttäjän hallintamahdollisuudet.

PHISHING

tarkoittaa tietojenkalastelua, joka on yleinen huijausmenetelmä internetissä. Se yleensä tapahtuu siten, että huijarit lähettävät sähköpostiviestejä tai luovat väärennettyjä verkkosivustoja, jotka näyttävät luotettavilta ja pyytävät käyttäjiä antamaan henkilökohtaisia tietojaan, kuten salasanoja tai luottokorttitietoja. Tämän jälkeen huijarit käyttävät näitä tietoja varastaakseen rahaa tai henkilökohtaisia tietoja uhreiltaan.

PRIVACY RELAY

on Applen lanseeraama palvelu, joka välittää sähköposteja tai muita viestejä yksityisesti ja anonymisti. Se toimii estämällä viestien vastaanottajan tiedot lähettäjältä ja välittäjältä, mikä auttaa suojaamaan yksityisyyttä ja estämään roskapostia. Privacy Relay-palvelut ovat yleensä käytettävissä maksua vastaan ja ne ovat suosittuja erityisesti silloin, kun käyttäjät haluavat suojella henkilökohtaisia tietojaan tai välttää ei-toivottua viestintää.

SANDBOXING

tarkoittaa tietokoneohjelmien tai -järjestelmien suojaamista eristämällä ne muusta tietokoneen toiminnasta. Tällöin ohjelmat toimivat erillisessä ympäristössä, johon niillä ei ole pääsyä tai vaikutusta muuhun järjestelmään. Sandboxingin avulla voidaan estää haittaohjelmien leviäminen ja vahingollisten

ohjelmien toiminnan aiheuttamat vahingot voidaan minimoida. Lisäksi se auttaa suojaamaan käyttäjän henkilökohtaisia tietoja ja estämään luvattoman käytön.

1 Johdanto

Opinnäytetyöni aiheena on digitaalisen markkinoinnin muuttuminen yksityisyydensuojaa kunnioittavaan suuntaan. Digitaalinen markkinointi on jatkuvassa kasvussa ja se on tullut yhä tärkeämmäksi yrityksille niiden tavoitellessa asiakkaitaan digitaalisessa ympäristössä. Samalla kun digitaalinen markkinointi on kehittynyt, on syntynyt myös aiheellinen huoli käyttäjien yksityisyydensuojasta. Yksityisyys on yksi tärkeimmistä tekijöistä, joka vaikuttaa käyttäjän luottamukseen yrityksiin, heidän palveluihinsa ja tuotteisiin. Läpinäkyvyydestä on tullut tärkeä osa palveluiden kehitystä, markkinointia ja arvolupausta. Yritysten täytyy olla tarkkoja siitä, kuinka he lunastavat arvolupauksensa ja ansaitsevat asiakkaan luottamuksen kilpailun ja markkinan kiristyessä. Käyttäjien tietoisuus omasta datasta, sen käyttötarkoituksista ja mahdollisista väärinkäytöksistä ovat tärkeitä huomioita kuluttajakäyttäytymisessä digitaalisessa ympäristössä.

Esittelen opinnäytetyössäni myös erilaisia teknisiä ratkaisuja ja muutoksia, joita lähiaikoina yksityisyydensuojan näkökulmasta on tapahtunut ja on tapahtumassa tulevaisuudessa. Yksi keskeinen tekninen muutos digitaalisessa markkinoinnissa on ollut evästeiden käytön väheneminen. Evästeet ovat pieniä tiedostoja, joita verkkosivustot tallentavat käyttäjän tietokoneelle tai mobiililaitteelle. Näin yritykset saavat liiketoimintakriittistä dataa käyttöönsä. Evästeiden avulla yritykset voivat tehokkaammin mitata ja analysoida markkinointikampanjojensa toimivuutta, verkkosivuston kävijöitä sekä tuotteidensa tai palvelujensa kehittämistä. Evästeiden avulla yritys voi myös tehdä digitaalisesta markkinoinnista kuluttajille luonnollisempaa personoinnin, kohdentamisen ja suosittelun avulla. Evästeiden keräämä data on kuitenkin herättänyt huolta yksityisyydensuojasta, sillä ne voivat myös tallentaa arkaluontoisia ja henkilökohtaisia tietoja, kuten esimerkiksi sijaintitietoa, selaushistoriaa ja hakukyselyitä. Evästeet ovat kuitenkin tärkeässä osassa digitaalisten markkinointikanavien ja niiden työkalujen toiminnassa, joita yritykset käyttävät digimarkkinoinnin mittaamiseen ja analysointiin.

Tähän opinnäytetyöhön olen tehnyt selkeät rajaukset käsiteltävistä aiheista. Suurin osa tämän opinnäytetyön tietoperustasta ja käsiteltävistä aiheista rakentuu yli 10 vuoden työkokemukseeni digitaalisesta markkinoinnista ja media-alasta. Koska digimarkkinointi ja teknologia kehittyvät nopeasti, olen kerännyt myös ajankohtaista tietoa alan suurimmilta ja luotettavimmilta medioilta tätä opinnäytetyötä varten. Tässä opinnäytetyössä käyn läpi vain murto-osan työkaluista ja ydinaiheista liittyen digitaaliseen markkinointiin, evästemuutoksiin ja yksityisyydensuojaan. Digitaalinen markkinointi on hyvinkin laaja käsite, jonka vuoksi tarkka raja on tärkeää. Opinnäytetyön eri vaiheissa korostuu useasti luottamus yrityksen ja asiakkaan välillä sekä tietosuojalain määrittelemät lainsäädännöt datan ja henkilötietojen keräämisestä.

Tässä opinnäytetyössä kerron esimerkkejä siihen, kuinka yritykset ottavat käyttöön uusia menetelmiä tietojen keräämiseen ja niiden käsittelyyn yksityisyydensuoja huomioiden. Opinnäytetyössä tutkin myös vaihtoehtoja siihen, kuinka yritykset voivat varautua digitaalisen markkinoinnin muuttumiseen evästeiden poistuessa. Esittelen myös esimerkkejä siitä, minkälaisia muutoksia suuret teknologiajätit ovat tehneet yksityisyydensuojan parantamiseksi.

Tämän opinnäytetyöni tavoitteena on tarjota tiivis katsaus digitaalisen markkinointiin sekä toimia pienempien yritysten oppaana siinä, kuinka varautua evästeiden poistumiseen ja toteuttaa tehokasta digitaalista markkinointia myös tulevaisuudessa. Pyrkimyksenäni on tarjota käytännöllisiä esimerkkejä ja ratkaisumalleja, jotka auttavat yrityksiä menestymään alati muuttuvassa digitaalisessa ympäristössä.

2 Katsaus digitaaliseen markkinointiin

Digitaalinen markkinointi on markkinointistrategia, joka käyttää digitaalista teknologiaa ja alustoja edistääkseen yrityksen liiketoimintaa myymällä ja markkinoimalla tuotteita tai palveluita. Tämä strategia on tärkeä osa nykyaikaista markkinointia, sillä yhä useammat kuluttajat käyttävät päivittäin internetiä ja muita digitaalisia alustoja, kuten sosiaalista mediaa ja muita mobiilisovelluksia. Koronapandemian aikaan digitaalisten palveluiden, medioiden ja sovelluksien käyttö kasvoi merkittävästi. Esimerkiksi sosiaalisen median käyttö kasvoi yli 13 prosenttia vuoden sisällä ja tällä hetkellä yli 70 prosenttia 16–89-vuotiaista suomalaisista käyttää erilaisia sosiaalisen median alustoja. (Tilastokeskus 2021.)

Yrityksen digitaalinen markkinointi kattaa monia erilaisia alueita, kuten hakukoneoptimoinnin (SEO), sosiaalisen median markkinoinnin, sähköpostimarkkinoinnin, sisältömarkkinoinnin ja mobiilimarkkinoinnin. Näiden strategioiden avulla yritykset voivat tavoittaa kohdeyleisönsä tehokkaasti ja saada heidät sitoutumaan yrityksen brändiin ja tuotteisiin. (Lahtinen, N. & Pulkka, K. & Karjaluoto, H. & Mero, J. 2022, 133–147)

Digitaalinen markkinointi tarjoaa monia etuja perinteiseen markkinointiin verrattuna. Yksi merkittävimmistä eduista on kohdennetun markkinoinnin mahdollisuus. Tämän avulla yritykset voivat tarkasti kohdistaa mainoksiaan tietyille kohderyhmille, jotka ovat todennäköisesti kiinnostuneita heidän tuotteistaan tai palveluistaan. Tämä terävöittää ja optimoi markkinointibudjettia, vähentää hukkakontakteja ja lisää mainonnan tehokkuutta.

Digitaalinen markkinointi on myös tehokkaammin mitattavissa verrattuna esimerkiksi printti-, TV- tai radiomainontaan. Markkinoijat voivat seurata kampanjoidensa tuloksia reaaliajassa ja tehdä muutoksia tarvittaessa nopeasti. Tämä mahdollistaa kampanjoiden optimoinnin ja parantaa samalla tuloksia.

Lisäksi digitaalinen markkinointi on kustannustehokkaampaa kuin perinteinen markkinointi. Esimerkiksi sosiaalisen median mainonta on yleensä halvempaa kuin televisiomainonta ja sen avulla yritykset voivat tavoittaa huomattavasti

suuremman yleisön. Digitaalinen markkinointi myös kehittyy jatkuvasti, mikä antaa yrityksille mahdollisuuden pysyä ajan tasalla uusimmista trendeistä ja mainontakeinoista. Yrityksen valmiudet ja resurssit ovat tässä tapauksessa tärkeässä roolissa, jotta näiden trendien ja mahdollisuuksien ajankohtaisuus on hyödynnettävissä tehokkaasti. (Lahtinen, N. & Pulkka, K. & Karjaluoto, H. & Mero, J. 2022, 14–22.)

2.1 Digimarkkinoinnin tärkeimmät osa-alueet ja työkalut

Seuraavaksi esittelen digitaalisen markkinoinnin tärkeimmät osa-alueet ja pohdin näiden merkitystä yrityksen näkökulmasta. Lisäksi käyn läpi digimarkkinoijan tärkeimmät työkalut digitaalisessa ympäristössä ja analysoinnin niiden toimintaa. Evästeet ja niihin liittyvät teknilliset muutokset ovat tärkeässä osassa näitä osa-alueita.

Hakukoneoptimointi (SEO – Search Engine Optimization) on jatkuva käynnissä oleva prosessi, jonka avulla yritykset pyrkivät parantamaan verkkosivujensa näkyvyyttä hakukoneiden, kuten Googlen ja Bingin, hakutuloksissa. SEO:n avulla yritykset pyrkivät saamaan korkeamman sijoituksen hakutuloksissa, mikä lisää verkkosivujen näkyvyyttä ja houkuttelee enemmän kävijöitä. SEO on tärkeä osa digitaalista markkinointia, sillä se auttaa yrityksiä löytämään uusia asiakkaita ja lisäämään verkkosivujen liikennettä. (Suomen Digimarkkinointi Oy, 2023a.)

Hakukonemainonta (SEM, Search Engine Marketing) on digitaalisen markkinoinnin muoto, joka keskittyy mainostamaan yrityksen tuotteita tai palveluita eri hakukoneissa. SEMiin kuuluu usein hakukonemainonnan (PPC) kampanjoiden luominen, joissa yritys voi maksaa mainostilasta hakutulossivulla tietyillä avainsanoilla, jotka liittyvät heidän tuotteisiinsa tai palveluihinsa. Tavoitteena on houkutella käyttäjiä napsauttamaan mainosta ja vierailemaan yrityksen verkkosivuilla. (Suomen Digimarkkinointi Oy, 2023a.)

Sosiaalinen media on tällä hetkellä yksi tärkeimmistä digitaalisen markkinoinnin kanavista. Sosiaalisessa median avulla yritykset voivat tavoittaa suuren yleisön ja luoda vahvan suhteen potentiaalsiin asiakkaisiin. Sosiaalisen media kanavista tärkeimmät ovat Facebook, Instagram ja TikTok, Twitter ja LinkedIn. Näiden kanavien avulla yritykset voivat jakaa sisältöä, mainostaa tuotteitaan ja palveluitaan sekä kommunikoida asiakkaiden kanssa.

Sähköpostimarkkinointi on yksi vanhimmista digitaalisen markkinoinnin kanavista, mutta se on edelleen tehokas tapa tavoittaa asiakkaita ja pitää heidät ajan tasalla yrityksen uutisista ja tarjouksista. Sähköpostimarkkinoinnin avulla yritykset voivat lähettää henkilökohtaisia ja personoituja viestejä potentiaalisille asiakkailleen, joka lisää asiakassitoutumista ja auttaa kasvattamaan myyntiä.

Markkinoinnin automaatio on monitahoinen käsite, joka kattaa laajan valikoiman teknologioita, prosesseja ja käytäntöjä, joiden tavoitteena on automatisoida markkinoinnin toimintoja ja parantaa markkinointitoimenpiteiden tehokkuutta. Tällaisia toimintoja voivat olla esimerkiksi sähköpostikampanjoiden luonti, sosiaalisen median julkaisujen aikataulut, asiakastiedon hallinta ja analysointi sekä verkkosivuston personointi ja optimointi. Lisäksi erilaiset ilmoitukset esimerkiksi sovelluksissa ovat tärkeitä. Markkinoinnin automaatio perustuu usein asiakasprofiilien luomiseen ja analysointiin, jolloin voidaan kohdentaa oikeanlaisia viestejä oikeille asiakkaille oikeaan aikaan. Rekisteröitynyt ja tunnistettu käyttäjä on tärkeässä roolissa markkinoinnin automaation optimaalisessa toteutumisessa. (Marketo,2021.)

Sisältömarkkinointi on prosessi, jossa yritykset luovat ja jakavat arvokasta sisältöä, joka houkuttelee ja sitouttaa asiakkaita. Sisältömarkkinointi voi olla blogipostauksia, artikkeleita, videoita tai infografiikoita. Sisältömarkkinoinnin materiaaleja jaetaan yleensä sosiaalisessa mediassa tietoisuuden ja kiinnostuksen herättämiseksi. (Suomen Digimarkkinointi Oy, 2023b.)

Natiivimainonta on yksi digitaalisen markkinoinnin muodoista, jossa mainos näyttää samalta kuin ympäröivä sisältö. Se on usein merkitty mainokseksi, mutta sen ulkoasu on suunniteltu mahdollisimman huomaamattomaksi ja luonnolliseksi.

Natiivimainonta on tehokas tapa markkinoida tuotteita ja palveluita digitaalisesti, sillä se lisää mainoksen huomiota ja sitoutumista asiakkaisiin, koska mainos sovitetaan ympäröivän sisällön ulkoasuun. Mainoksen visuaalinen ilme ja tyyli ovat samanlaisia kuin sivustolla jo oleva sisältö. Tämä antaa myös mainostajille mahdollisuuden välittää markkinointiviestinsä asiakkaille tavalla, joka on vähemmän häiritsevää kuin perinteiset mainokset.

Natiivimainonta voi kuitenkin johtaa ongelmiin, jos sitä ei ole merkitty selkeästi mainokseksi. Tämä voi johtaa kuluttajien luottamuksen menetykseen mainostajaa kohtaan, ja jopa mainostajan mainehaittaan. Lisäksi mainonnan eettiset kysymykset voivat nousta esiin, jos mainokset eivät ole läpinäkyviä tai sisältö on harhaanjohtavaa.

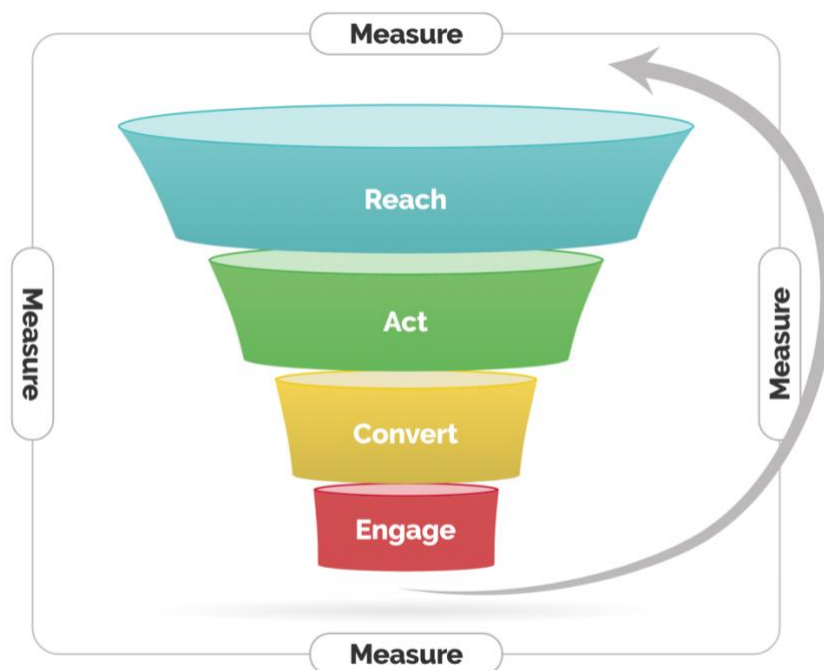
Natiivimainonnan menestyksen avain onkin luottamuksen rakentaminen asiakkaiden ja mainostajan välille. Tämä tapahtuu selkeän merkinnän ja läpinäkyvyyden avulla. Kun kuluttajat tietävät, että he katsovat mainosta, he ovat todennäköisemmin avoimia sille, ja se voi johtaa parempiin tuloksiin mainostajalle. (IAB Finland, 2015.)

2.2 M-RACE viitekehys

MRACE-viitekehys on yksi tunnetuimmista digitaalisen markkinoinnin malleista, jonka avulla yritykset voivat suunnitella ja toteuttaa tehokkaita digitaalisia markkinointikampanjoita. MRACE-malli eroaa aiemmasta globaalista RACE-mallista siinä, että siinä on lisäksi oma mittaamiseen keskittyvä osa-alueensa, M eli Measure. Jatkuvasti muuttuvassa toimintaympäristössä testaaminen ja kehittäminen ovat tärkeää, jotta yritys pystyy saavuttamaan halutun tuloskehityksen ja mukautumaan asiakaskäyttäytymisen ja teknologian muutoksiin.

Alla olevassa kuvassa (ks. kuva 1) tuodaan esille, kuinka MRACE-malli koostuu neljästä vaiheesta, joita ovat Reach, Act, Convert ja Engage. Reach-vaiheessa keskitytään tavoitettavuuteen ja pyritään lisäämään yrityksen brändin tunnettuutta ja houkuttelevuutta potentiaalisten asiakkaiden keskuudessa. Act-vaiheessa puolestaan keskitytään liidien eli potentiaalisten asiakkaiden hankkimiseen ja vuorovaikutukseen heidän kanssaan. Convert-vaiheessa tavoitteena on muuttaa liidit myyntivalmiiksi liideiksi tai saada asiakkaalta tarjouspyyntö. Viimeisessä Engage-vaiheessa keskitytään asiakkaiden sitouttamiseen ja pitkäaikaisten asiakassuhteiden luomiseen. (Suomen Digimarkkinointi Oy, 2023c.)

MRACE-viitekehys tarjoaa yrityksille selkeän ja yksityiskohtaisen suunnitelman, jonka avulla voidaan kehittää tehokkaita digitaalisia markkinointikampanjoita. Tämä malli auttaa yrityksiä keskittymään tärkeisiin markkinointitoimenpiteisiin ja varmistamaan, että ne ovat kohdennettuja ja tuloksellisia.



Kuva 1. MRACE-viitekehys (Suomen Digimarkkinointi Oy, 2022).

2.3 Digimarkkinoijan ensisijaiset työkalut ja käsitteet

Web-analytiikka ja markkinoinnin mittaaminen ovat tärkeitä osia digitaalisessa markkinoinnissa, koska ne mahdollistavat markkinoijille reaaliaikaisen näkymän kampanjoiden suorituskykyyn ja auttavat heitä tekemään parempia päätöksiä markkinoinnin strategioiden suhteen. Markkinointijärjestelmät ovat tärkeitä työkaluja yrityksille, joiden tavoitteena on saavuttaa asiakas- ja markkinointitavoitteet tehokkaasti. (Digital Marketing Institute, 2022.)

Tätä opinnäytetyötä varten on valittu vain tärkeimmät työkalut, jotka ovat relevantteja digimarkkinoinnin mittaamisesta kiinnostuneille käyttäjille.

Google Analytics on yksi suosituimmista ja tärkeimmistä web-analytiikan järjestelmistä, joka tarjoaa kattavan analytiikan sivuston liikenteestä ja käyttäjistä. Sallittujen evästeiden avulla tämä data on yrityksen käytettävissä. Järjestelmässä on erilaisia ominaisuuksia, kuten kävijätiedot, liikenteen lähteet, kävijäpolkuanalytiikka ja konversio seuranta. Google Analytics auttaa markkinoijia ymmärtämään paremmin sivustonsa käyttäjiä ja optimoimaan verkkosivuston suorituskykyä.

Hotjar on monipuolinen työkalu, joka tarjoaa web-analytiikan lisäksi käyttäjäpalautetta ja käyttäjäkokemuksen arviointia. Hotjar sisältää ominaisuuksia, kuten käyttäjäpolkuanalytiikka, käyttäjäkyselyt ja käyttäjätestaus, jotka auttavat markkinoijia ymmärtämään tehokkaammin, kuinka asiakkaat käyttävät palvelua ja mitä he siellä tekevät.

SEMrush on markkinoinnin mittarointityökalu, joka tarjoaa tietoa kilpailijoista, hakukoneoptimoinnista (SEO) ja hakusanamainonnasta (SEM). SEMrush sisältää ominaisuuksia, kuten avainsana-analyysi, backlink-analyysi ja kilpailijan analysointi, jotka auttavat markkinoijia kehittämään parempia SEO- ja SEM-strategioita.

Hootsuite on sosiaalisen median markkinointityökalu, joka auttaa markkinoijia hallitsemaan ja mittaamaan sosiaalisen median kampanjoita. Hootsuitessa on ominaisuuksia, kuten kampanjoiden ajoitus, viestintätyökalut ja raportointi,

jotka mahdollistavat tehokkaan sosiaalisen median markkinoinnin. Hootsuite integroituu useisiin eri sosiaalisen median alustoihin, kuten Facebookiin, Instagramiin, Twitteriin ja LinkedIniin, mikä helpottaa kampanjoiden hallintaa yhdestä paikasta käsin.

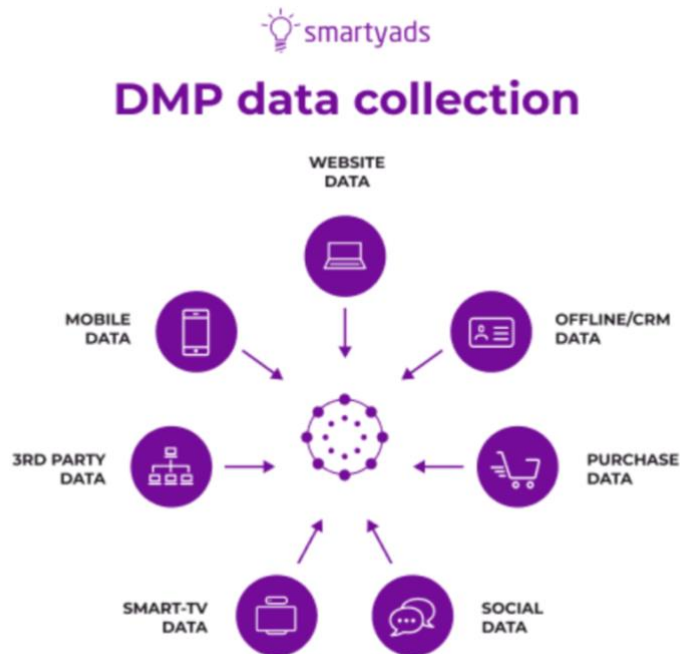
Hootsuiten avulla markkinoijat voivat ajoittaa kampanjoitaan sopivaan aikaan, jolloin tavoitettavuus on korkeimmillaan, sekä hallita useita sosiaalisen median tilejä samanaikaisesti. Hootsuite tarjoaa myös viestintätyökaluja, jotka mahdollistavat vuorovaikutuksen asiakkaiden kanssa sosiaalisessa mediassa, kuten nopean vastaamisen yksityisviesteihin ja kommentteihin.

DMP (Data Management Platform) on teknologia-alusta, joka mahdollistaa markkinoinnin ja mainonnan kohdentamisen. Alla olevassa kuvassa (ks. kuva 2) tuodaan selkeästi esille, kuinka DMP:n avulla yritykset voivat kerätä, tallentaa, analysoida ja aktivoida dataa eri lähteistä, kuten sosiaalisesta mediasta, verkkosivuilta ja mobiilisovelluksista. DMP auttaa yrityksiä ymmärtämään asiakkaidensa käyttäytymistä ja mieltymyksiä sekä kehittämään henkilökohtaisempia ja tehokkaampia markkinointistrategioita. (SmartyAds, 2021.)

CDP (Customer Data Platform) on alusta, joka keskittyy asiakastietojen keräämiseen, hallintaan ja analysointiin. CDP mahdollistaa asiakastietojen yhdistämisen eri lähteistä, kuten verkkosivuilta, asiakaspalvelujärjestelmistä ja myyntikanavista. CDP auttaa yrityksiä ymmärtämään asiakkaidensa tarpeita ja mieltymyksiä, mikä puolestaan mahdollistaa henkilökohtaisemman ja kohdennetumman markkinoinnin. (Salesforce, 2023.)

DMP ja CDP ovat molemmat tärkeitä työkaluja yrityksille, jotka haluavat hyödyntää asiakasdataa tehokkaasti. Vaikka molemmat teknologia-alustat ovat keskittyneet tietojen hallintaan ja analysointiin, niiden käyttötarkoitukset eroavat toisistaan. DMP keskittyy markkinoinnin ja mainonnan kohdentamiseen, kun taas CDP keskittyy asiakastiedon ymmärtämiseen ja asiakaskokemuksen parantamiseen. Molempien teknologia-alustojen avulla yritykset voivat kuitenkin

luoda tehokkaampia ja henkilökohtaisempia markkinointistrategioita, jotka perustuvat parempaan asiakasymmärrykseen ja tietoon.



Kuva 2. DMP esimerkki (SmartyAds, 2021).

2.4 Datan hyödyntäminen digimarkkinoinnissa

Digitaalisen markkinoinnin optimointi ja konversio ovat kaksi tärkeää käsitettä digitaalisen markkinoinnin alalla. Markkinoinnin optimoinnilla tarkoitetaan prosessia, jossa pyritään parantamaan digitaalisen markkinoinnin tehokkuutta ja saavutettuja tuloksia. Konversio puolestaan tarkoittaa verkkosivuston vierailijan tai potentiaalisen asiakkaan muuttamista todelliseksi maksavaksi asiakkaaksi eli konvertoinniksi. (SEMrush, 2022.)

Digitaalisen markkinoinnin kokonaisvaltaiseen optimointiin liittyy useita eri tekijöitä, kuten sivuston käyttökokemus (UX), hakukoneoptimointi (SEO), sisällöntuotanto ja mainonnan kohdentaminen. Tavoitteena on parantaa verkkosivuston näkyvyyttä ja houkuttelevuutta, jotta käyttäjät viipyisivät sivustolla

pidempään ja todennäköisemmin muuttuisivat maksaviksi asiakkaiksi. (SEMrush, 2022.)

Konversio-optimoinnissa keskitytään puolestaan sivuston käyttäjien käyttäytymisen ja toiminnan analysointiin. Tavoitteena on lisätä konversioita, eli muuttaa sivuston vierailijat mahdollisimman suureksi määräksi asiakkaita. Konversio-optimoinnin avulla voidaan parantaa esimerkiksi verkkokaupan ostoskorin käyttöä, sivustolla vietettyä aikaa ja sivuston käyttöä eri laitteilla.

Näiden kahden käsitteen yhdistäminen auttaa yrityksiä löytämään oikeat kohderyhmät ja optimoimaan verkkosivustonsa ja kampanjansa paremmin. Tärkeää on huomioida, että optimointi on jatkuvaa prosessia ja vaatii jatkuvaa seuranta ja analyysiä, jotta saavutetaan parhaat tulokset. (HubSpot, 2022a.)

Personointi ja kohdentaminen

Digitaalisen markkinoinnin muuttuminen ja kehittyminen on antanut markkinoijille mahdollisuuden personoida ja kohdentaa viestintäänsä yksilöllisesti. Tämä on johtanut kohdennetumpaan markkinointiin, joka on osoittautunut tehokkaammaksi kuin massamarkkinointi televisiossa tai radiossa. Personointi tarkoittaa yksilöllisten tarpeiden ja mieltymysten huomioimista markkinointiviestinnässä. Tämä voi sisältää henkilökohtaisten suositusten, algoritmipohjaisten suositusten tai yksilöllisten tarjousten tarjoamista asiakkaille.

Kohdentaminen tarkoittaa markkinointiviestinnän kohdistamista tiettyihin yleisöihin, jotka ovat todennäköisimmin kiinnostuneita tuotteista tai palveluista. Kohdennus perustuu usein asiakkaan demografisiin tai käyttäytymistietoihin, jotka ovat saatu asiakkaan toiminnasta digitaalisissa kanavissa. Tämä kohdennus mahdollistaa markkinoijien tavoittaa vain potentiaaliset asiakkaat, jolloin markkinointiviestinnän tehokkuus kasvaa.

Personoidun ja kohdennetun markkinointiviestinnän avulla markkinoijat voivat tarjota asiakkaille tarkoituksenmukaisempaa sisältöä, joka on juuri heille tärkeää. Tämä lisää asiakasuskollisuutta ja parantaa asiakaskokemusta, joka puolestaan

johtaa pidempään asiakassuhteeseen ja lisääntyneeseen myyntiin, koska mainonta on henkilökohtaisempaa ja yksilöidymppää. (Berger, B. 2022)

2.4.1 Datan tilastollinen mallintaminen

Kaikista käyttäjistä ja sivustokävijöistä yritykset eivät voi automaattisesti tietää kaikkea, jolloin tärkeäksi työkaluksi muodostuu tilastollinen mallintaminen. Siinä käytetään tilastotieteellisiä menetelmiä markkinointikampanjan optimointiin ja tehokkuuden parantamiseen. Tilastollinen mallintaminen perustuu tilastollisten mallien kehittämiseen ja soveltamiseen erilaisiin markkinointitietoihin, kuten käyttäjädataan ja kuluttajatietoihin.

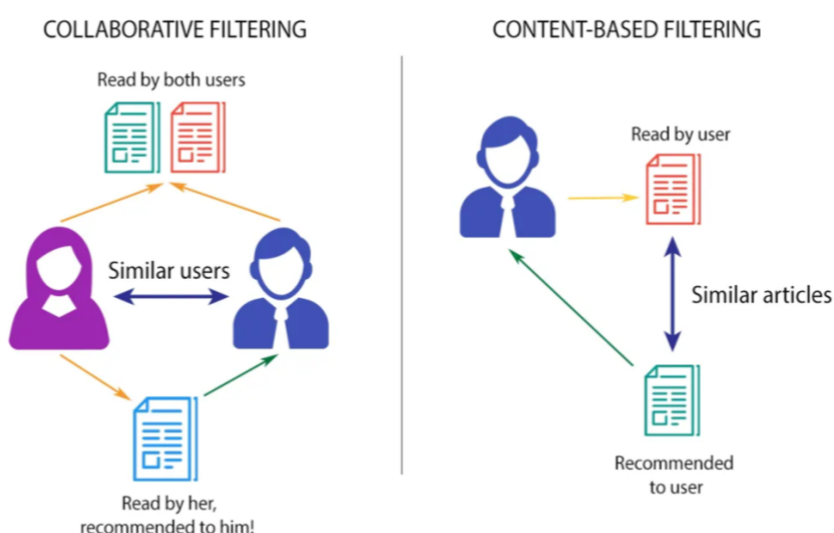
Tilastollinen mallintaminen auttaa markkinoijia ymmärtämään paremmin asiakkaiden käyttäytymistä ja tarpeita, mikä mahdollistaa datan jalostamisen kohdennetun markkinoinnin ja personoinnin avuksi. Esimerkiksi kuluttajadatasta voidaan kehittää ennustemalleja, jotka ennakoivat tulevaa kuluttajakäyttäytymistä ja auttavat markkinoijia tarjoamaan oikeanlaisia tuotteita ja palveluita oikeaan aikaan. Yksi tehokas digimarkkinoinnin keino on myös suosittelu, johon myös erilaiset mallinnuskeinot perustuvat. Suosittelemalla käyttäjille voidaan suositella samankaltaisen persoonien avulla kerätyn datan avulla vastaavanlaisia tuotteita, sisältöjä tai palveluita, joista muut samankaltaiset ihmiset ovat kiinnostuneita (ks. kuva 3).

Tilastollinen mallintaminen voidaan toteuttaa erilaisilla tilastollisilla menetelmillä, kuten lineaarisella regressiolla, logistisella regressiolla ja klasteroimalla. Nämä menetelmät auttavat tunnistamaan merkittäviä muuttujia, jotka vaikuttavat markkinoinnin tehokkuuteen, ja kehittämään ennustemalleja, jotka auttavat optimoimaan markkinointikampanjaa. (Madonna, F. 2022.)

Tilastollisen mallintamisen käyttö digitaalisessa markkinoinnissa on kasvanut viime vuosina merkittävästi, sillä markkinoijat ovat ymmärtäneet sen hyödyt tehokkuuden parantamisessa. Tilastollisen mallintamisen avulla markkinoijat voivat ymmärtää asiakkaiden käyttäytymistä ja tarpeita paremmin, mikä auttaa

heitä tarjoamaan räätälöityä markkinointia ja parantamaan asiakastytyvyyttä.

Lopuksi on tärkeää huomata, että tilastollisen mallintamisen käyttö edellyttää hyvää ymmärrystä tilastotieteestä ja sen soveltamisesta markkinointiin. Lisäksi on tärkeää huolehtia asiakastietojen yksityisyydestä ja tietoturvasta sekä varmistaa, että tilastollisia malleja käytetään vastuullisesti ja eettisesti.



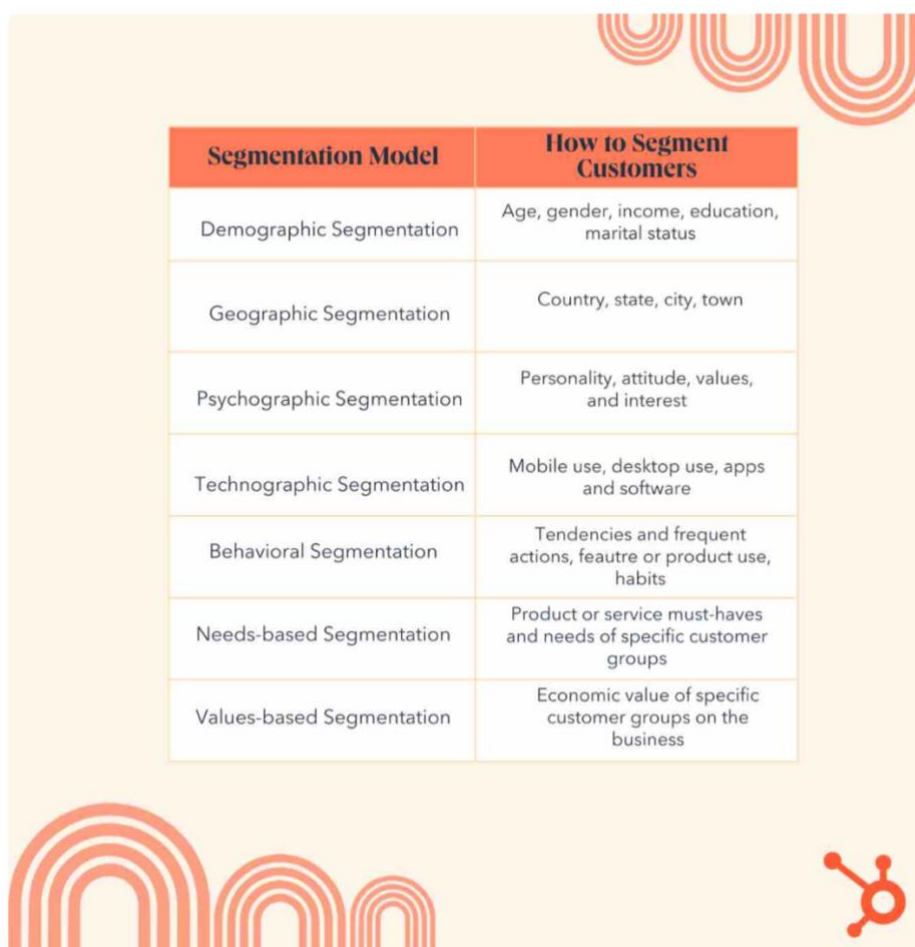
Kuva 3. Esimerkki tilastollisesta mallintamisesta (Medium, 2022).

2.4.2 Segmentointi ja profilointi

Segmentointi ja profilointi ovat tärkeitä käsitteitä markkinoinnin alalla, joilla ja niillä pyritään ymmärtämään asiakasryhmiä ja tavoittamaan ne tehokkaammin. Segmentointi tarkoittaa asiakkaiden jakamista eri ryhmiin yhteisten piirteiden, kuten demografisten tai käyttäytymiseen liittyvien tekijöiden perusteella (ks. kuva 4). Profilointi taas tarkoittaa yksittäisten asiakkaiden tunnistamista ja yksilöllisten tarpeiden ja mieltymysten huomioimista markkinoinnissa. (HubSpot, 2022b.)

Segmentoinnin avulla markkinoijat voivat tunnistaa ja ymmärtää erilaisia asiakasryhmiä ja jakaa ne tarkoituksenmukaisiin segmentteihin. Tämä auttaa markkinoijia tarjoamaan kohdennetumpaa ja tehokkaampaa markkinointia, joka vastaa paremmin kunkin asiakasryhmän tarpeita ja mieltymyksiä. Segmentoinnin avulla markkinoijat voivat myös löytää uusia asiakassegmenttejä, jotka saattavat olla kiinnostuneita heidän tuotteistaan tai palveluistaan. (HubSpot, 2022b.)

Profilointi taas keskittyy yksittäisten asiakkaiden yksilöllisiin tarpeisiin ja mieltymyksiin. Profiloinnin avulla markkinoijat voivat kerätä ja analysoida tietoja asiakkaista, kuten heidän ostohistoriastaan, verkkokäyttäytymisestään ja sosiaalisen median toiminnastaan. Näiden tietojen avulla markkinoijat voivat rakentaa yksilöllisiä profileja asiakkaista ja tarjota heille juuri heidän tarpeisiinsa ja mieltymyksiinsä sopivaa markkinointia. (HubSpot, 2022b.)



Segmentation Model	How to Segment Customers
Demographic Segmentation	Age, gender, income, education, marital status
Geographic Segmentation	Country, state, city, town
Psychographic Segmentation	Personality, attitude, values, and interest
Technographic Segmentation	Mobile use, desktop use, apps and software
Behavioral Segmentation	Tendencies and frequent actions, feature or product use, habits
Needs-based Segmentation	Product or service must-haves and needs of specific customer groups
Values-based Segmentation	Economic value of specific customer groups on the business

Kuva 4. Asiakkaiden segmentointi mahdollisuuksia (HubSpot, 2022.)

Segmentointi ja profilointi ovat tärkeitä tekijöitä markkinointistrategian suunnittelussa. Kun markkinoijat ymmärtävät asiakasryhmät ja yksilölliset tarpeet, he voivat tarjota heille kohdennettua ja yksilöllistä markkinointia, joka on merkityksellistä ja tehokasta. Tämä voi johtaa pidempään ja vakinaiseen asiakassuhteeseen myynnin vahvistuessa. (HubSpot, 2022b.)

Lisäksi on hyvä muistaa, että segmentointi ja profilointi eivät ole itsetarkoitus markkinoinnissa. On tärkeää, että markkinoijat ymmärtävät vastuunsa asiakastietojen käsittelyssä ja pyrkivät käyttämään niitä aina vastuullisesti. Segmentointi ja profilointi voivat herättää myös eettisiä kysymyksiä. Markkinoijien on varmistettava, että he noudattavat tietosuojalakeja ja kunnioittavat asiakkaiden yksityisyyttä kerätessään ja käyttäessään tietoja asiakkaista. Lisäksi markkinoijien on varmistettava, että he eivät käytä segmentointia tai profilointia epäoikeudenmukaisella tai syrjivällä tavalla, kuten esimerkiksi syrjimällä tiettyjä asiakasryhmiä. Lisäksi markkinoijien on oltava avoimia ja läpinäkyviä siitä, miten he keräävät ja käyttävät asiakkaiden tietoja. (HubSpot, 2022b.)

3 Asiakaskokemus ja käyttäjätiedon kerääminen

Kuten aiemmin on todettu, digitaalinen markkinointi on hyvin kustannustehokas ja hyvin tunnettu kanava tavoittaa asiakkaita ja luoda heidän kanssaan pitkäaikaisia suhteita. Tämä tarkoittaa myös sitä, että datan kerääminen on keskeinen osa markkinointia, sillä se mahdollistaa tarkemman ja personoidumman markkinoinnin. Samalla kun datan kerääminen on tärkeää, on myös tärkeää ymmärtää sen merkitys asiakaskokemuksen ja luottamuksen kannalta. Ne vaikuttavat asiakkaan ostopäätökseen ja asiakassuhteen jatkumiseen. Kun yritys kerää tietoa asiakkaistaan, asiakkaat luottavat siihen, että heidän tietonsa käsitellään turvallisesti ja vastuullisesti. Siksi yritysten on varmistettava, että asiakkaan henkilötietoja käsitellään tietoturvallisesti ja että niitä käytetään vain markkinointitarkoituksiin. Yritysten on myös varmistettava, että asiakkailla on mahdollisuus hallita tietojensa käyttöä ja että he voivat milloin tahansa pyytää tietojensa poistamista. (Forbes, 2021.)

3.1 Digitaalisen markkinoinnin muuttuminen

Euroopan unionin yleinen tietosuojalaki (GDPR) astui voimaan toukokuussa 2018 ja se muutti merkittävästi digitaalisen markkinoinnin toimintaympäristöä. GDPR:n tarkoituksena on suojella yksityisyyttä ja henkilötietoja sekä varmistaa, että yritykset käsittelevät henkilötietoja vastuullisesti.

GDPR edellyttää yrityksiltä, että ne keräävät henkilötietoja laillisesti, käyttävät niitä vain niihin tarkoituksiin, joihin henkilö on antanut luvan, ja varmistavat, että henkilötietojen säilytys ja käsittely on turvallista. Lisäksi GDPR antaa yksilöille oikeuden tarkistaa, mitä tietoja heistä on tallennettu ja pyytää niiden poistamista, jos ne ovat vanhentuneita tai tarpeettomia.

GDPR:n vaikutukset digitaaliseen markkinointiin ovat moninaiset. Se on esimerkiksi rajoittanut evästeiden käyttöä, joka on ollut perinteinen tapa kerätä käyttäjätietoa digitaalisessa markkinoinnissa. GDPR:n myötä evästeiden käyttö

edellyttää käyttäjän suostumusta, mikä on vähentänyt evästeiden tehokkuutta yrityksen näkökulmasta.

GDPR on myös lisännyt yritysten vastuuta henkilötietojen turvallisesta käsittelystä ja varmistanut, että yritykset ovat vastuussa henkilötietojen käytöstä. Tämä on lisännyt kuluttajien luottamusta yrityksiin, jotka ovat vastuullisia ja huolehtivat henkilötietojen turvallisuudesta. Samalla GDPR on rajoittanut epäeettistä käyttöä henkilötiedoilla ja edistänyt kuluttajien yksityisyyden suojaa. (EU:n yleinen tietosuoja-asetus (EU) 2016/679.)

Kokemukseni mukaan GDPR:n vaikutukset ovat johtaneet uusiin digitaalisen markkinoinnin toimintatapoihin ja teknologioihin, jotka ovat vastuullisia ja turvallisia henkilötietojen käsittelyssä läpinäkyvästi.

3.2 Henkilödatan pseudonymisointi ja anonymisointi

Pseudonymisointi on yksi tapa suojata henkilötietoja. Pseudonymisointi tarkoittaa henkilökohtaisten tietojen poistamista tai korvaamista yksilöllisellä tunnisteella, joka ei ole yhteydessä henkilöön. Tämä tarkoittaa, että henkilökohtaisia tietoja ei voida enää yhdistää yksilöihin, mikä parantaa yksityisyydensuojaa.

Anonymisointi on toinen tapa suojata henkilötietoja: Anonymisoinnissa henkilökohtaiset tiedot poistetaan kokonaan, jolloin niitä ei voida enää yhdistää yksilöihin. Anonymisointi on tehokkaampi tapa suojata henkilötietoja kuin pseudonymisointi, mutta se voi myös rajoittaa markkinointikampanjoiden tehokkuutta, koska se rajoittaa tietojen käyttöä kohdentamiseen.

Datan pseudonymisointi ja anonymisointi ovat tärkeitä henkilötietojen suojaamisen kannalta, mutta ne eivät aina ole riittäviä. On myös eettisesti ja vastuullisesti tärkeää, että henkilötietoja käsitellään ja käytetään vain siihen tarkoitukseen, johon ne on kerätty. (Tietosuojavaltuutetun toimisto, 2023a).

3.3 Henkilötiedot ja epäsuorat tunnisteet

Henkilötiedot ovat tietoja, jotka liittyvät joko tunnistettuun tai muulla tavalla tunnistettavissa olevaan henkilöön. Henkilötiedot voivat sisältää esimerkiksi henkilön nimen, osoitteen, sähköpostiosoitteen, puhelinnumeron, syntymäajan, henkilötunnuksen tai passinumeron.

Epäsuorat tunnisteet puolestaan ovat tietoja, joita ei voida suoraan yhdistää tiettyyn henkilöön, mutta jotka voivat silti johtaa henkilön tunnistamiseen. Esimerkiksi verkkosivuilla kävijän IP-osoite, selaimen käyttöjärjestelmä tai evästeiden tallentama data voivat olla epäsuoria tunnisteita. (Tietosuojavaltuutetun toimisto, 2023b)

Henkilötietojen ja epäsuorien tunnisteiden käyttöä säätelee GDPR. Tämä velvoittaa yrityksiä käsittelemään henkilötietoja huolellisesti ja turvaamaan niiden suojaamisen. Epäsuoria tunnisteita tulee myös käsitellä huolellisesti, sillä niiden avulla henkilö voi tulla tunnistetuksi ja heidän yksityisyydensuojaansa voidaan loukata.

GDPR edellyttää, että yrityksillä on laillinen peruste henkilötietojen käsittelylle ja että henkilöille kerrotaan selkeästi, mitä tietoja heistä kerätään ja miten niitä käytetään. Yrityksen kannattaa panostaa turvalliseen datan käsittelyyn ja omien datavarastojen rakentamiseen, sillä se tuo yritykselle useita etuja. Oma datavarasto mahdollistaa yrityksen kontrolloida omaa dataa ja sen käyttöä, mikä takaa datan laadun ja tietoturvan. (Tietosuojavaltuutetun toimisto, 2023b.)

3.4 Yksityisyydensuoja ja rekisteröidyn oikeudet

Tietosuoja-asetuksen (EU) 2016/679 artikla 12 käsittelee tarkemmin rekisteröidyn oikeuksia ja yksityisyydensuojaa. Nämä käsitteet liittyvät siihen, kuinka henkilötietoja käsitellään ja miten yksilön oikeudet huomioidaan tietojen käsittelyssä.

Yksityisyydensuoja tarkoittaa henkilöiden oikeutta suojata henkilökohtaisia tietojaan, kuten nimiä, osoitteita, syntymäaikoja, sosiaaliturvatunnuksia ja muita tunnistetietoja. Tietosuojalainsäädännön tarkoituksena on varmistaa, että henkilötietojen käsittely tapahtuu lainmukaisesti, oikeudenmukaisesti ja avoimesti. Tämä tarkoittaa muun muassa sitä, että rekisteröidyn henkilön tulee olla tietoinen siitä, että hänen tietojaan käsitellään, millaisia tietoja käsitellään, miksi niitä käsitellään ja kenelle niitä voidaan luovuttaa.

Rekisteröidyn oikeudet ovat keskeinen osa tietosuojalainsäädäntöä. Rekisteröidyllä tarkoitetaan henkilöä, jonka henkilötietoja käsitellään. Rekisteröidyllä on useita oikeuksia, joita hän voi käyttää tietojensa suojaamiseksi. Tärkeimpiä näistä oikeuksista ovat:

1. Tietojen käsittelyn läpinäkyvyys: Rekisteröidyllä on oikeus saada tietoa siitä, millaisia tietoja hänen henkilötiedoistaan käsitellään, kenelle tietoja luovutetaan ja mihin tarkoituksiin tietoja käytetään.
2. Oikeus saada tietoja: Rekisteröidyllä on oikeus saada mahdollinen pääsy omiin henkilötietoihinsa, joita käsitellään. Tämä tarkoittaa sitä, että rekisteröidyn tulee saada kopio tietojaan koskevista asiakirjoista.
3. Oikeus tietojen oikaisemiseen: Rekisteröidyllä on oikeus pyytää oikaisemaan tai täydentämään virheellisiä tai puutteellisia henkilötietojaan.
4. Oikeus tietojen poistamiseen: Rekisteröidyllä on oikeus pyytää poistamaan henkilötietonsa, jos niitä ei enää tarvita tietosuojasetuksessa määriteltyihin tarkoituksiin.
5. Oikeus vastustaa tietojen käsittelyä: Rekisteröidyllä on oikeus vastustaa tietojensa käsittelyä määrättyissä olosuhteissa, kuten esimerkiksi suoramarkkinoinnissa. Tämä tarkoittaa sitä, että jos rekisteröity vastustaa henkilötietojensa käsittelyä suoramarkkinointitarkoituksessa, yritys ei saa enää käsitellä hänen henkilötietojaan kyseiseen tarkoitukseen. Tämä oikeus

on tärkeä tapa varmistaa, että henkilötietojen käsittely tapahtuu rekisteröidyn suostumuksen mukaisesti ja että hänen yksityisyyttään kunnioitetaan.

Kaikkia näitä oikeuksia tulee kunnioittaa ja ne on sisällytettävä yrityksen tietosuojakäytäntöön. Rekisteröityjen oikeuksien kunnioittaminen on tärkeää paitsi tietosuojan ja yksityisyyden kannalta, myös yrityksen maineen ja luottamuksen rakentamisen näkökulmasta. Kun yritys kunnioittaa rekisteröidyn oikeuksia ja käsittelee henkilötietoja vastuullisesti, se luo pohjaa pitkäaikaiselle asiakassuhteelle ja positiiviselle brändikuvalle. Toisaalta, jos yritys ei kunnioita rekisteröityjen oikeuksia ja käsittelee henkilötietoja huolimattomasti tai laittomasti, se voi menettää asiakkaiden luottamuksen ja joutua vakaviin seuraamuksiin tietosuoja-asetusten rikkomisesta. (Tietosuojavaltuutetun toimisto, 2023c.)

3.5 Datan kerääminen ja käyttötarkoitussidonnaisuus

Datan kerääminen ja käyttötarkoitussidonnaisuus ovat keskeisiä käsitteitä tietosuojassa ja tietosuojalainsäädännössä. Datan kerääminen tarkoittaa henkilötietojen käsittelyä, joka sisältää kaikki henkilötietojen käsittelyn vaiheet, kuten keräämisen, tallentamisen, käyttämisen, siirtämisen ja poistamisen. Datan keräämisellä on useita käyttötarkoituksia, kuten markkinoinnissa, asiakaspalvelussa ja monissa muissa toiminnoissa läpi yrityksen. Tietosuoja perustuu perusperiaatteisiin, joihin kuuluu henkilötietojen käsittelyn tarkoituksenmukaisuus, asianmukaisuus, minimointi ja käyttötarkoitussidonnaisuus. Käyttötarkoitussidonnaisuus tarkoittaa, että henkilötietoja kerätään ja käytetään vain tiettyyn tarkoitukseen. Tämä tarkoittaa sitä, että henkilötietoja ei saa käyttää tai käsitellä muulla tavalla kuin alkuperäisessä tarkoituksessa, jolle ne on kerätty. (Tietosuojavaltuutetun toimisto, 2023d.)

Datan käyttötarkoitus on määritettävä jo ennen sen keräämistä, ja kerätyn datan käyttöön tarvitaan rekisteröidyn suostumus. Rekisteröidyllä on oikeus saada

tietoa siitä, miten hänen henkilötietojaan käytetään ja mihin tarkoituksiin niitä käytetään. Lisäksi rekisteröidyllä on oikeus vaatia henkilötietojensa poistamista, jos ne eivät enää palvele alkuperäistä käyttötarkoitusta. (Tietosuojavaltuutetun toimisto, 2023d.)

Datan keräämiseen liittyy myös henkilötietojen minimointiperiaate. Tämä tarkoittaa sitä, että kerättävät henkilötiedot ovat tarpeellisia ja suhteutettuja käyttötarkoitukseen. Henkilötietoja ei saa kerätä enempää kuin mitä on tarpeen tietyn tarkoituksen saavuttamiseksi. (Tietosuojavaltuutetun toimisto, 2023d.)

Yrityksen tulee esitellä selkeästi tietosuojalauseke ja palvelun käyttöehdot kerätessä käyttäjien tietoja. (Tietosuojavaltuutetun toimisto, 2023d.)

3.6 Muuttava lainsäädäntö: DSA ja DMA

DSA-direktiivi eli Digital Services Act (Regulation (EU) 2022/2065) on Euroopan unionin uusi lainsäädäntö, joka on suunniteltu sääntelemään digitaalisten palvelujen tarjoamista Euroopassa. DSA-direktiivi on suunniteltu vastaamaan nykyajan haasteisiin, joita digitaaliset palvelut ja niiden tarjoajat kohtaavat, kuten harhaanjohtava digitaalinen mainonta, vihapuhe ja disinformaatio.

Yksi tärkeimmistä asioista DSA-direktiivissä on sen soveltamisala. Direktiivi koskee kaikkia digitaalisia palveluntarjoajia, jotka tarjoavat palveluita Euroopassa, mukaan lukien sosiaalisen median alustat, hakukoneet, markkinapaikat, verkkokaupat ja pilvipalveluntarjoajat. Direktiivi asettaa tiukat velvoitteet palveluntarjoajille, jotka ovat suurempia ja joilla on suurempi vaikutusvalta, kuten käyttäjien oikeuksien turvaaminen ja vastuu haitallisen sisällön poistamisesta.

Toinen tärkeä asia DSA-direktiivissä on sen sääntelymekanismi. Direktiivi perustaa digitaalisten palvelujen valvontaelimen, jonka tehtävänä on valvoa palveluntarjoajia ja varmistaa, että ne noudattavat direktiivin vaatimuksia. Valvontaelimen rooli on myös koordinoida kansallisten viranomaisien toimintaa

ja tehdä yhteistyötä muiden Euroopan unionin toimielinten kanssa. (Digital Services Act, Regulation (EU) 2022/2065)

Kolmas tärkeä asia DSA-direktiivissä on sen vaikutus online-mainontaan. Direktiivi sisältää uusia vaatimuksia online-mainonnalle, kuten avoimuusvaatimuksen, joka vaatii mainostajia ilmoittamaan selkeästi mainokset. Direktiivi sisältää myös säännöksiä, jotka koskevat henkilötietojen suojaamista, mainonnan kohdentamista ja personointia. (Digital Services Act, Regulation (EU) 2022/2065)

Neljäs tärkeä asia DSA-direktiivissä on sen vaikutus digitaaliseen kilpailuun. Direktiivi sisältää uusia sääntöjä markkinoiden hallitsevien asemien väärinkäytön estämiseksi ja uusia velvoitteita suurille alustoille, kuten avoimen rajapinnan vaatimus. Tämän pitäisi mahdollistaa uusien palveluntarjoajien ja innovaatioiden syntyminen digitaalisilla markkinoilla. (Digital Services Act, Regulation (EU) 2022/2065)

DSA-direktiivi on tärkeä lainsäädäntö, jonka avulla pyritään varmistamaan, että yritykset noudattavat tietosuojasetuksia ja että kuluttajien yksityisyys on turvattu. Direktiivi asettaa tärkeitä vaatimuksia digitaalisten markkinointikampanjoiden suunnittelulle ja toteuttamiselle ja sen noudattamatta jättäminen voi johtaa rangaistuksiin. (Digital Services Act, Regulation (EU) 2022/2065)

Digitaalisen markkinoinnin alalla DMA-direktiivi (Digital Markets Act, Regulation (EU) 2022/1925) on yksi tärkeimmistä säädöksistä, joka säätelee suoramarkkinointia ja digitaalista mainontaa. Direktiivin tavoitteena on suojella yksityisyyttä ja henkilötietojen käyttöä markkinointitarkoituksissa.

DMA-direktiivi sisältää useita tärkeitä kohtia, joita markkinoijien tulee noudattaa. Yksi tärkeimmistä kohteista on asiakkaan suostumus markkinointiin. Markkinoijat eivät saa lähettää mainoksia tai muita markkinointiviestejä henkilöille, jotka eivät

ole antaneet suostumustaan tällaiseen viestintään. Suostumus tulee olla vapaaehtoinen, yksilöllinen, tietoinen ja yksiselitteinen. (Digital Markets Act, Regulation (EU) 2022/1925)

DMA-direktiivi edellyttää myös, että markkinointiviesteissä on oltava selkeästi esitetty tieto siitä, miten henkilötietoja käytetään ja kuka niitä käsittelee. Lisäksi viesteissä tulee olla selkeästi esitetty opt-out-mahdollisuus, jolla vastaanottaja voi kieltäytyä vastaanottamasta lisää markkinointiviestejä. Direktiivi edellyttää myös, että markkinointiviestien lähettäjän tulee olla selvästi tunnistettavissa. Tämä tarkoittaa esimerkiksi sitä, että sähköpostiviesteissä tulee olla lähettäjän yhteystiedot ja yrityksen nimi. (Digital Markets Act, Regulation (EU) 2022/1925)

DMA-direktiivi velvoittaa myös markkinoijia käsittelemään henkilötietoja huolellisesti ja suojattuna. Markkinoijien tulee ottaa käyttöön asianmukaiset tekniset ja organisatoriset turvatoimet henkilötietojen suojaamiseksi. Rekisteröidyllä on lisäksi oikeus saada tietoa häntä koskevista henkilötiedoista, joita yritys käsittelee. (Digital Markets Act, Regulation (EU) 2022/1925)

GDPR, DSA ja DMA-direktiivit ovat samankaltaisia lainsäädännöllisiä välineitä, jotka pyrkivät edistämään yksityisyyden suojaa ja tietoturvallisuutta digitaalisessa toimintaketjussa. Näiden direktiivien tärkeimpänä tavoitteena on luoda kokonaisvaltaista luottamusta digitaalisiin palveluihin varmistamalla henkilötietojen käsittelyn turvallisuus ja luotettavuus. (Digital Markets Act, Regulation (EU) 2022/1925)

4 Evästeiden maailma

Evästeet ovat pieniä tekstitiedostoja, jotka tallentuvat käyttäjän laitteelle selaimen kautta. Nämä ovat elinehto suurelle osalla erilaisista digitaalisen markkinoinnin työkaluista, joita käytetään verkkosivujen personointiin ja mainonnan kohdentamiseen. Evästeiden avulla saadaan kerättyä paljon erilaista dataa sivuston ja palveluiden käyttäjistä.

4.1 Erilaisia evästeitä

Evästeet voidaan jakaa kahteen päätyyppiin: 1. osapuolen evästeisiin ja 3. osapuolen evästeisiin. 1. osapuolen evästeet ovat peräisin verkkosivustolta, jolla käyttäjä vierailee. Ne tallennetaan käyttäjän tietokoneelle vain sen sivuston käyttöä varten. Esimerkiksi, kun käyttäjä kirjautuu sisään verkkokaupan sivustolle, verkkokauppa luo 1. osapuolen evästeen, jotta käyttäjän kirjautumistiedot voidaan tallentaa ja muistaa seuraavan kerran, kun käyttäjä vierailee sivustolla. (Kyberturvallisuuskeskus, 2023.)

3. osapuolen evästeet ovat peräisin eri verkkotunnukselta kuin se sivusto, jolla käyttäjä vierailee. Tällaiset evästeet luovat mainostajat tai mainosverkostot, joiden tarkoituksena on kerätä tietoa käyttäjien toiminnasta eri verkkosivustoilla. Esimerkiksi, jos käyttäjä vierailee verkkokaupassa ja ostaa tuotteen, 3. osapuolen evästeet voivat tallentaa tiedon ostosta ja käyttää sitä kohdistukseen käyttäjälle mainoksia kyseisestä tuotteesta muilla verkkosivustoilla. (Kyberturvallisuuskeskus, 2023.)

Databrokerit ovat yrityksiä, jotka keräävät tietoa lukuisista eri lähteistä, mukaan lukien 3. osapuolen evästeet, ja myyvät näitä tietoja edelleen muille yrityksille. Databrokerit voivat kerätä tietoa esimerkiksi käyttäjän verkkokäyttäytymisestä, demografisista tiedoista ja ostohistoriasta. Tämä tieto voi olla arvokasta yrityksille, jotka haluavat kohdentaa mainoksia mahdollisimman tarkasti ja tehokkaasti. Databrokerit voivat myös käyttää tätä tietoa esimerkiksi

markkinatutkimuksessa, ennusteiden ja mallinnuksien tekemisessä. (Grauer, Vice-blogi, 2018)

Tämä evästeiden avulla kerätyn datan kaupankäynti eri tahojen välillä on herättänyt keskustelua yksityisyydensuojasta ja tietoturvasta, sillä käyttäjät eivät välttämättä ole tietoisia siitä, että heidän tietojensa kerätään ja käytetään tällä tavalla.

4.2 Evästeiden poistuminen ja poistaminen

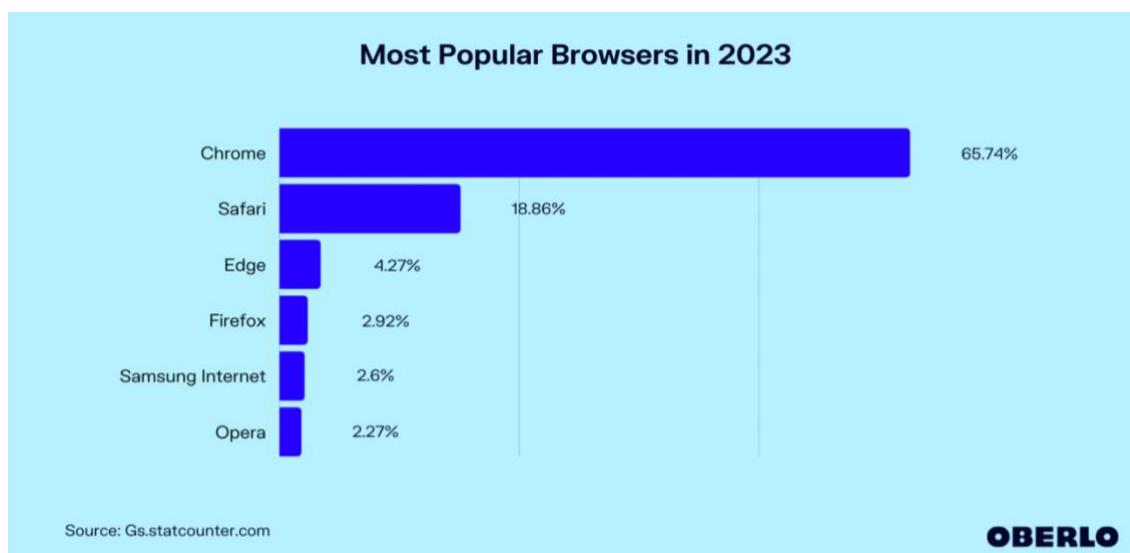
Evästeiden poistuminen voi tapahtua useasta eri syystä. Käyttäjä voi itse haluta poistaa evästeet, jotta hänen verkkokäyttämisen ei tallentuisi. Tämä voi johtua esimerkiksi yksityisyydensuojan tunteesta tai halusta välttää kohdennettua mainontaa. Evästeiden poistuminen voi myös johtua selaimen päivityksistä tai asetusten muutoksista.

Evästeiden poistuminen voi johtua myös suoraan laitevalmistajien tai palveluntarjoajien toteuttamista teknisistä muutoksista, jotka vaikuttavat verkkosivustojen käyttäjäkokemukseen sekä tietosuojaan. Juurisyy tähän kehitykseen on varmasti lainsäädännön kiristyminen ja yksityisyyden suojan entistä tärkeämpi korostaminen.

Digimarkkinoinnin kannalta evästeiden poistuminen edellä mainittujen toimenpiteiden johdosta vaikuttaa merkittävästi yritysten toimintaan, tuotekehitykseen ja palveluihin. Kun käyttäjät poistavat evästeet, markkinoijat menettävät tämän arvokkaan datan ja joutuvat käyttämään muita tapoja mainonnan kohdentamiseen ja sillä on selkeä vaikutus mainonnan tehokkuuteen. Kun käyttäjät eivät ole tunnistettavissa evästeiden kautta, mainokset voivat näkyä epäsovivassa ympäristössä tai väärille kohderyhmille. Tämä voi johtaa mainonnan heikentyneeseen tehokkuuteen ja hukattuihin mainosbudjetteihin. Tämä vaikuttaa myös markkinoinnin ja yksityisyyden suhteen tasapainoon.

4.3 Googlen tekemät muutokset

Vuonna 2020 Google ilmoitti, että se poistaa kolmannen osapuolen evästeet Chrome-selaimesta vuoden 2022 loppuun mennessä. Vaikka Safari ja Firefox ovat tehneet vastaavan päätöksen jo vuosia sitten, Google on lykännyt tätä päätöstä useaan otteeseen. Tämän opinnäytetyön kirjoitusvaiheessa Googlen viimeisin ilmoittama aikarajana on vuoden 2024 loppuun mennessä (Cookiebot, 2022.) Kuten alla olevan kuvan perusteella voidaan todeta (ks. kuva 5), Chromen markkinaosuuden olevan edelleen erittäin suuri. Tämä tarkoittaa, että evästeiden poistuminen tulee vaikuttamaan merkittävästi mainostajien ja mainosalustojen toimintaan tulevaisuudessa.



Kuva 5. Chromen markkinaosuus (Oberlo, 2023).

Sitä ennen Google on kuitenkin päättänyt lakkauttaa Google Universal Analyticsin ja velvoittaa yrityksiä siirtymään käyttämään uutta Google Analytics 4 työkalua heinäkuun 2023 loppuun mennessä. Se on suunniteltu uudelleen "Privacy by design" mallin mukaisesti ja käyttäjien yksityisyydensuoja huomioiden. (Google, 2020.)

Privacy by design ei ole täysin uusi käsite. Sitä on käsitelty jo 1970-luvulla. Sen viitekehys kehitettiin edelleen 1990-luvulla silloisen Ontarion tietosuoja- ja

informaatiokomissaarin, Ann Cavoukianin, toimesta. Privacy by design on suunnitteluperiaate, joka on kehitetty varmistamaan tietoturvan ja yksityisyyden huomioiminen tuotteen tai palvelun kaikissa vaiheissa. Tämä lähestymistapa korostaa henkilötietojen suojaamista suunnittelun alusta alkaen ja edellyttää tietoturvan ja yksityisyyden huomioimista läpikotaisin. (Carbide, 2023.)

Arvelen, että suurin syy Googlea ja sen toimintaa muokkaavana tekijänä on varmasti ollut maailmanlaajuisesti lainsäädännön kiristyminen ja yksityisyydensuojan vahvistuminen. Yksityisyydensuojan kehittymisen myötä valta ja oikeus käyttäjän henkilötietoihin on siirtynyt takaisin yksittäiselle käyttäjälle, mikä on johtanut siihen, että Google ei halua rikkoa yhtenäisiä määräyksiä, altistua oikeudellisille seuraamuksille ja suurille sanktioille.

Tämä muutos lainsäädännössä on vaikuttanut merkittävästi myös siihen, kuinka Yhdysvaltojen suuret teknologia- ja datajätit, joita vakiintuneesti kutsutaan yhteisellä nimellä GAFAM (Google, Apple, Facebook, Amazon ja Microsoft) käyttävät henkilötietoja. Yritykset joutuvat noudattamaan tiukempia yksityisyydensuojan standardeja ja varmistamaan, että toiminta on yhdenmukaista uusien lainsäädännöllisten vaatimusten kanssa.

Toisaalta Google on myös kertonut, että sen tavoitteena on tarjota mainostajille vaihtoehtoisia tapoja kohdentaa mainoksia ilman kolmannen osapuolen evästeitä. Yksi näistä tavoista on Google Topics, joka mahdollistaa kohdennetun mainonnan ilman henkilötietojen jakamista kolmannen osapuolen kanssa. Tämä on kohti kontekstuaalisempaa mainontaa, jossa mainoksia kohdennetaan yksityisyydensuoja huomioiden käyttäjien intressien ja kiinnostuksien perusteella.

Kaiken kaikkiaan voidaan todeta, että edistysaskeleet yksityisyyden suojan ja vastuullisuuden alalla ovat johtaneet positiiviseen kehitykseen kohti luottamuksellisempaa ja läpinäkyvämpää mainontaa, joka on hyödyllistä niin

yrittäjille kuin kuluttajillekin. Tämä muokkaa myös yleistä ajattelu- ja toimintamallia kohti aidompaa, luonnollisempaa ja luotettavampaa markkinointia.

4.4 Yrityksen mahdollisuudet evästeiden kadotessa

Yrityksen kannattaa panostaa omaan dataan ja omaan datavarastoon monista eri syistä. Yksi tärkeimmistä syistä on, että yritys voi suoraan käyttää omaa dataa asiakkaiden tuntemiseen ja parempien palveluiden tarjoamiseen. Oma data voi olla myös kilpailuetu, sillä se on yrityksen omassa hallinnassa eikä ole riippuvainen kolmansista osapuolista, kuten databroker -yrityksistä. Yritys on samalla myös varautunut tulevaisuuden lainsäädännöllisiin ja teknologisiin muutoksiin, johon yrityksiltä vaaditaan nopeaa reagoitua. (Bloomreach, 2022.)

Oman datavaraston rakentaminen voi kuitenkin olla haastavaa ja vaatii erilaisia resursseja. Yrityksen on varmistettava, että kerätty data on oikeaa ja tarpeellista liiketoiminnan kannalta. On myös tärkeää, että dataa kerätään asiakkaiden suostumuksella ja noudatetaan tietosuojalainsäädäntöä. Omaan dataan panostaminen voi auttaa yritystä myös kokonaisvaltaisessa datan laadun parantamisessa. Yritys voi itse päättää, millaista dataa kerätään, miten sitä käytetään ja milloin sitä hyödynnetään. Lisäksi yrityksen oma data voi olla helpommin yhdisteltävissä muihin datalähteisiin, mikä lisää sen arvoa ja käyttömahdollisuuksia. (Bloomreach, 2022.)

Zero-party data on käyttäjän itsensä antamaa tietoa, jota yritykset keräävät suoraan asiakkailtaan tai potentiaalisilta asiakkailtaan. Tämä eroaa perinteisestä kolmannen osapuolen keräämästä datasta, joka kerätään usein evästeiden avulla käyttäjän selatessa verkkosivuja. Zero-party datan kerääminen on yleistynyt GDPR:n ja muiden yksityisyydensuojaan liittyvien säädösten vuoksi, jotka ovat rajoittaneet kolmannen osapuolen datan keräämistä. Lisäksi käyttäjänsä itse antama tieto on moninkertaisesti arvokkaampaa ja laadukkaampaa kuin evästeiden kautta kerätty data. Tämä data perustuu silloin

henkilöltä suoraan kysytyyn tietoon, eikä evästeiden tai muiden lähteiden kautta arvattuun. (Bloomreach, 2022.)

Zero-party datan kerääminen tapahtuu suoraan käyttäjiltä, joilta pyydetään tiettyjä tietoja tiettyä käyttötarkoitusta varten. Tämä voi tapahtua esimerkiksi yrityksen nettisivulla, jossa käyttäjälle voidaan esittää tiettyjä kysymyksiä tai tarjota mahdollisuus liittyä uutiskirjeen tilaajaksi vastineeksi tietyn edun, kuten alennuskoodin tai ilmaisen oppaan saamisesta. Yritykset voivat myös hyödyntää zero-party dataa asiakasprofiilien rakentamisessa ja personoinnissa, joka auttaa tarjoamaan käyttäjille henkilökohtaisempia ja räätälöityjä kokemuksia. (Bloomreach, 2022.)

Zero-party datan avulla yritykset voivat kerätä tarkempaa ja laadukkaampaa tietoa asiakkaistaan, joka auttaa ymmärtämään paremmin heidän tarpeitaan ja käyttäytymistään. Tämä puolestaan auttaa yrityksiä kehittämään parempia tuotteita ja palveluita sekä parantamaan asiakaskokemusta. Lisäksi zero-party data voi auttaa yrityksiä luomaan vahvempia asiakassuhteita, kun käyttäjien antamaa tietoa käytetään henkilökohtaisempien, merkityksellisempien ja ajankohtaisten viestien ja tarjousten lähettämiseen. (Gartner, 2021.)

4.5 Kirjautunut käyttö

Evästeet olivat yksi keino tunnistaa sivuston vierailijat paremmin eri palveluissa. Niiden poistuessa yrityksille on tulevaisuudessa tärkeää myös tunnistaa sivustonsa käyttäjät ja vierailijat paremmin, koska se mahdollistaa asiakaskokemuksen parantamisen ja personoinnin. Pysyvin käyttäjäprofiilien avulla yritykset voivat kerätä dataa omaan varastoonsa ja rikastuttaa dataa haluamallaan tavalla. Kun yritykset tuntevat käyttäjänsä ja vierailijansa, he voivat tarjota paremmin kohdistettuja ja räätälöityjä palveluita ja tuotteita, mikä johtaa asiakastytyväisyyden kasvuun ja sitoutumiseen. Oma data voi auttaa yrityksiä kehittämään tuotteitaan ja palveluitaan paremmin vastaamaan asiakkaidensa tarpeisiin ja toiveisiin.

Tunnistaminen on myös tärkeää tietoturvan kannalta, sillä se auttaa yrityksiä tunnistamaan ja estämään haitallista toimintaa sivustoillaan, kuten huijausyritykset, petokset ja tietomurrot. Lopuksi, kun yritykset tunnistavat paremmin käyttäjänsä ja vierailijansa, he voivat myös parantaa markkinointikampanjoitaan ja mainontaa, mikä johtaa tehokkaampaan ja kustannustehokkaampaan markkinointiin. Tämä auttaa yrityksiä saavuttamaan paremman tuoton sijoitukselleen ja kasvattamaan liikevaihtoaan.

5 Tulevaisuus ja muutokset

GAFAM (Google, Amazon, Facebook, Apple, Microsoft) teknologiajätit ovat viime vuosina ryhtyneet tekemään merkittäviä parannuksia yksityisyyden suojaan liittyen. Yritykset ovat oivaltaneet, että yksityisyys on yksi tärkeimmistä aiheista, joka huolestuttaa heidän käyttäjiänsä ja että asiakastyytyväisyyden kannalta on tärkeää tarjota käyttäjilleen entistä parempia yksityisyydensuoja-asetuksia. Yksityisyydensuojasta ja sen kunnioittamisesta on tullut kilpailuetu yritykselle ja erottautumistekijä markkinoilla.

Yksi esimerkki parannuksista, joita teknologiajätit ovat tehneet, on henkilötietojen käytön rajoittaminen. Kuten aiemmin on todettu, Google on tuomassa muutokset Chrome-selaimensa vuoden 2024 aikana (Cookiebot, 2022.) Apple on lisännyt uusia yksityisyydensuojaominaisuuksia suoraan laitteidensa käyttöjärjestelmiin. Nämä parannukset antavat käyttäjille paremman mahdollisuuden hallita tietojen jakamista ja valita, mitkä yritykset voivat käyttää tietoja mainostamiseen.

Lisäksi yritykset ovat ryhtyneet kehittämään uusia yksityisyysominaisuuksia, jotka antavat käyttäjille entistä paremman hallinnan tietojensa käytöstä. Esimerkiksi Apple on kehittänyt uuden Privacy Report -ominaisuuden laitteillaan ja Safari-selaimessa, joka näyttää käyttäjille, mitkä verkkosivut yrittävät kerätä tietoja heidän selailustaan ja sovelluksien käytöstä. (Apple, 2022.)

Facebook taas on tuonut käyttöön Privacy Checkup -ominaisuuden, joka auttaa käyttäjiä tarkistamaan ja säätämään tietosuoja-asetuksiaan Facebook on yksi suurimmista sosiaalisen median alustoista, ja sen tietosuoja-asiat ovat olleet usein esillä julkisuudessa (BBC, 2020). Siksi on tärkeää, että Facebook tarjoaa käyttäjilleen Privacy Checkup -ominaisuuden, joka auttaa käyttäjiä tarkistamaan ja säätämään tietosuoja-asetuksiaan. Tämä antaa käyttäjille paremman mahdollisuuden hallita omia tietojaan ja suojella henkilökohtaista yksityisyyttään Facebookin käytön aikana. (Facebook, 2023.)

On tärkeää korostaa, että yksityisyyden suoja koskeva keskustelu on tärkeää ja hyvinkin ajankohtaista niin yrityksissä kuin medioissakin ja sitä koskeva kehitys on jatkuvaa. Vaikka suuret teknologiayritykset ovatkin tehneet paljon parannuksia, on markkina vasta muuttumassa ja tehtävää riittää jokaisessa yrityksessä, jossa käyttäjien tietosuoja ja yksityisyys tulee pitää korkealla prioriteetilla yritysten tietoturvallisuusstrategioissa.

5.1 Google PrivacySandBox

Google on suunnitellut käyttöjärjestelmän nimeltään PrivacySandBox, joka on tarkoitus integroida tulevaisuudessa kaikkiin Android-käyttöjärjestelmiin. PrivacySandBoxin tarkoituksena on lisätä tietoturvaa ja yksityisyydensuojaa käyttäjille, erityisesti niille, jotka käyttävät Android-sovelluksia. (Google, 2023.)

PrivacySandBox käyttää virtuaalista ympäristöä, jossa sovellukset suoritetaan eristettynä muusta järjestelmästä. Jokainen sovellus käynnistetään omaan suojaavaan virtuaalikoneeseen, joka estää sovellusta pääsemästä käyttäjän henkilökohtaisiin tietoihin. Tämä tarkoittaa sitä, että vaikka sovelluksessa olisi haitallinen koodi, se ei voi aiheuttaa vahinkoa käyttäjän laitteelle tai henkilökohtaisille tiedoille. (Google, 2023.)

Lisäksi PrivacySandBox tulee sisältämään muita tietoturvateknologioita, kuten salattua liikennettä, joka suojaaa käyttäjän tiedonsiirtoa sovellusten ja palveluiden välillä. Näin käyttäjän henkilökohtaiset tiedot pysyvät suojattuina ulkopuolisilta uhilta. (Google, 2023.)

Google on aikaisemmin käyttänyt vastaavia tietoturvateknologioita, kuten Chrome-selaimen käyttämää Sandboxing-tekniikkaa. Tämä tekniikka on ollut erittäin tehokas estämään haittaohjelmia, phishing-hyökkäyksiä ja muita verkkouhilta, jotka voivat vaarantaa käyttäjän tietoturvan. PrivacySandBox on jatkoa tälle kehitystyölle ja tarjoaa entistä paremman suojan käyttäjien henkilökohtaisille tiedoille. (CNET, 2020.)

Lopuksi PrivacySandBox on tärkeä askel kohti parempaa tietoturvaa ja yksityisyydensuojaa Android-käyttäjille. Se auttaa suojaamaan käyttäjän tietoja haitallisilta ohjelmilta, verkkohyökkäyksiltä ja muilta uhilta. Tämä tekee PrivacySandBoxista tärkeän tekijän Googlen tietoturvallisuusstrategiassa. (Google, 2023.)

5.2 Google Topics

Google Topics on Googlen kehittämä työkalu, joka käyttää tekoälyä ja koneoppimista tunnistukseen ja kategorisoidakseen verkon sisältöä eri aihealueiden alle. Evästeiden näkökulmasta Google Topics ei vaadi käyttäjiltä erillisiä evästeitä, sillä se käyttää tietoa, joka on jo olemassa Googlen palveluissa ja selaimissa, kuten hakukyselyistä, selaushistoriasta ja käyttäjän Googlen palveluihin tallentamista tiedoista. (Goel, V. 2022.)

Google lopetti Flocin, eli "*Federated Learning of Cohorts*" -teknologian, koska se herätti huolta käyttäjien yksityisyyden suojasta. Flocin avulla käyttäjät jaettiin "kohorteiksi" tiettyjen käyttäjäprofiilien perusteella, jotta mainokset voitiin kohdistaa tietyille käyttäjäryhmille. Tämä herätti huolta käyttäjien henkilökohtaisten tietojen keräämisestä ja käytöstä mainostajien toimesta. (Goel, V. 2022.)

Sen sijaan Google suosittelee käyttämään Privacy Sandbox -ratkaisua mainosten kohdistamiseen, joka käyttää yksityisyyttä kunnioittavia tekniikoita kuten anonymisointia ja rajoitettua datan jakamista. Privacy Sandbox -ratkaisu pyrkii suojaamaan käyttäjien yksityisyyttä samalla, kun se mahdollistaa mainostajille tehokkaan mainosten kohdistamisen. (Goel, V. 2022.)

Evästeiden jälkeen Google Topics käyttää tekoälyä ja koneoppimista tunnistukseen ja kategorisoidakseen verkon sisältöä eri aihealueiden alle. Tämä mahdollistaa käyttäjille helpomman tavan löytää kiinnostavaa sisältöä ja tutkia

sitä syvällisemmin. Samalla Privacy Sandbox -ratkaisun käyttö auttaa suojaamaan käyttäjien yksityisyyttä, kun mainoksia kohdistetaan käyttäjille. (Goel, V. 2022.)

Topics voi kuitenkin tarjota käyttäjille enemmän yksityisyydensuojaa kuin nykyiset mainosjärjestelmät. Tämä on siksi, että käyttäjän henkilökohtaisia tietoja ei kerätä ja käytetä mainosten kohdistamiseen, vaan käyttäjät ovat osa suurempia kohortteja, joiden selailutavat ovat samankaltaisia. (Goel, V. 2022.)

Kaiken kaikkiaan Topics on Googlen yritys löytää tasapaino yksityisyydensuojan ja mainosten kohdistamisen välillä. On kuitenkin tärkeää, että käyttäjien yksityisyydensuoja turvataan ja että mainostajat eivät saa liikaa valtaa käyttöönsä. (Goel, V. 2022.)

5.3 Apple ja iOS

Apple on yksi ensimmäisistä teknologiayrityksistä, joka on ottanut käyttöön erilaisia yksityisyyden parantamiseen tähtäviä toimia. Vuonna 2021 julkaistussa iOS 14.5-versiossaan Apple otti käyttöön uusia yksityisyyttä parantavia ominaisuuksia. (The Verge, 2021.)

Yksi merkittävimmistä parannuksista on App Tracking Transparency (ATT), joka vaatii sovelluskehittäjiä pyytämään käyttäjän lupaa ennen kuin he voivat seurata ja jakaa käyttäjän henkilökohtaisia tietoja kolmansille osapuolille. ATT:n avulla käyttäjät voivat itse valita, mihin sovelluksiin ja mihin tarkoituksiin he antavat suostumuksensa tietojensa jakamiseen. (Apple, 2021a.)

Toinen tärkeä uudistus Applelta on "*Kätke sähköpostiosoitteeni*" – ominaisuus. Tämä toiminto perustuu yksityisyyden suojaamiseen liittyvään teknologiaan, joka on nimeltään "*Private Relay*". Tämä teknologia on osa Applen uutta iCloud+ -palvelua, joka tarjoaa myös muita edistyksellisiä lisäominaisuuksia käyttäjien yksityisyyden suojaamiseen. (Apple, 2021b.)

Kätke sähköpostiosoitteeni -toiminto toimii siten, että kun käyttäjä antaa sähköpostiosoitteensa verkkosivustolle tai sovellukselle, toiminto luo väliaikaisen, yksityisen sähköpostiosoitteen. Tämä väliaikainen sähköpostiosoite välitetään sitten verkkosivustolle tai sovellukselle sen sijaan, että käyttäjän varsinaista sähköpostiosoitetta käytettäisiin. Tämä väliaikainen sähköpostiosoite suojaa käyttäjän yksityisyyttä, sillä verkkosivusto tai sovellus ei tiedä käyttäjän varsinaista sähköpostiosoitetta. Tällä hetkellä monet verkkosivustot ja sovellukset vaativat käyttäjän antamaan sähköpostiosoitteensa ennen sisällön katselua tai lataamista. Tämä voi johtaa käyttäjän henkilökohtaisten tietojen väärinkäyttöön tai roskapostin määrän kasvuun. (Apple, 2021b.)

Aiemman kokemukseni ja havaintojeni mukaan myös pelkästä sähköpostiosoitteesta on helposti pääteltävissä useitakin erilaisia yksilöiviä tietoja. Perinteisestä "etunimi.sukunimi@yritys.com" osoitteesta on helposti pääteltävissä henkilön sukupuoli ja yritys, jossa hän työskentelee. Mikäli kyseessä on henkilökohtainen sähköpostiosoite esimerkiksi "etunimi_75@gmail.com" on tästä helposti pääteltävissä henkilön sukupuolen lisäksi myös oletettu syntymävuosi. Kun nämä tiedot on anonymisoitu Applen tarjoaman palvelun avulla, niin datan hyödyntäminen mallinnuksessa ja jatkoanalysointi on haasteellisempaa.

Lisäksi Apple on parantanut yksityisyyttä suoraan myös Safari-selaimessaan, joka on saanut uusia ominaisuuksia, kuten aiemmin esitellyn Privacy Report -toiminnon. Lisäksi Safari selaimissa on myös "Kätke osoitteeni" -toiminto ja liikenteen salaussmahdollisuus. Kätke osoitteeni -toiminto piilottaa käyttäjän IP-osoitteen sivustolta, jotta käyttäjä voi selata verkkoa anonymisti ja suojalla yksityisyyttään esimerkiksi sijaintinsa välittymiseltä verkkosivuston käyttöön. IP-osoitteen on toki pystynyt aiemmin myös salaamaan VPN-sovelluksen avulla, mutta tämä on vaatinut aina erillisen sovelluksen asentamisen ja osaamisen asiasta. Siksi Apple on halunnut tehdä tästä helposti lähestyttävän ja kuluttajille mahdollisemman helpon tavan suojata yksityisyyttään eri palveluissa. Tämän

asetuksen saa päällä suoraan selaimessa ilman erillisiä asentamisia ja on käyttäjälle hyvin helppoa. (Apple, 2021b.)

Kaiken kaikkiaan Apple on tehnyt useita parannuksia yksityisyydensuojassa ja on edelläkävijä tällä alalla. Yksi merkittävimmistä keinoista, jolla Apple on suojannut käyttäjiensä yksityisyyttä lähtökohtaisesti alusta lähtien, on App Store -sovelluskaupan valvonta. Apple tarkistaa tarkasti kaikki sovellukset ennen niiden julkaisemista App Storessa. Tämän avulla Apple voi varmistaa, että sovellukset ovat turvallisia ja että ne noudattavat yhtiön tietosuojakäytäntöjä. Googlen Play-kauppa ei tee vastaavanlaisia tarkastuksia yhtä pieteetillä, joten Android-puhelimiin on mahdollista ladata suoraan haitallisia ja tietoja kerääviä sovelluksia suoraan. (*TechAdvisor, 2020.*)

Apple on osoittanut, että yksityisyys on tärkeä arvo yritykselle, ja se on pyrkinyt tarjoamaan käyttäjilleen mahdollisimman paljon hallintaa tietojensa käytöstä ja jakamisesta.

6 Pohdintaa

Tietojen kerääminen on edelleen elintärkeää yrityksille, koska oman datavaraston avulla yritys ei ole riippuvainen ulkopuolisesta mahdollista muutoksista. Datan keräämisessä tulee kuitenkin muistaa se, että se tehdään oikein ja huolellisesti. Yritysten on selkeästi kerrottava asiakkailleen, miksi tietoja kerätään, miten niitä käytetään ja miten ne voidaan poistaa tarvittaessa. Tämä on läpinäkyvyyden ja luottamuksen perusta asiakkaan ja yrityksen välillä. Asiakkaat ovat yleensä valmiita jakamaan henkilökohtaisia tietojaan, kunhan kerääminen tapahtuu luontevasti, oikeassa vaiheessa ja kun asiakas ymmärtää, miksi tietoja kysytään.

Kun lainsäädäntö kiristyy ja tekniset rajoitukset muuttuvat, yritysten kannattaa keskittyä zero-party-tietojen keräämiseen, joka tarkoittaa suoraan käyttäjiltä itse kerättyä dataa. Yrityksen ei tarvitse olla riippuvainen kolmannen osapuolen datasta, eikä arvailla asiakkaan segmenttiä tai mieltymyksiä. Yritykset voivat kerätä tietoja useassa eri vaiheessa asiakaspolkua, mutta tietojen keräämisen on oltava käyttötarkoitussidonnaista. Tietoja voidaan kerätä esimerkiksi rekisteröitymisen yhteydessä tai eri kohdissa verkkosivustoa palvelumuotoilun avulla. Myös asiakkaalle tuotettujen sisältöjen esimerkiksi arvontojen tai testien yhteydessä on luontevaa pyytää tarvittavia tai puuttuvia tietoja käyttäjistä. Datan keräämisen yhteydessä yrityksiä kannattaa läpinäkyvästi tuoda esille se, että mitä hyötyjä tietojen antamisesta on ja kuinka molemmat osapuolet siitä hyötyvät.

Yritysten kannattaisi panostaa omiin teknisiin ratkaisuihin, jotta datan kerääminen on ylipäättään mahdollista, sen hyödyntäminen tehokasta ja siihen on varattu tarpeeksi resursseja. Oikein kerätyn datan avulla ja sen hyödyntämisellä yritys voi kasvattaa tehokkaasti liikevaihtoaan, kehittää ja innovoida uusia palveluita, pitää asiakaskokemuksen ja tyytyväisyyden korkealla tasolla ja menestyä markkinoilla kilpailijoita paremmin.

Yritysten tietojenkäsittely- ja analysointikyky on nykyään kriittinen menestystekijä. Yritykset, jotka hyödyntävät tietoa tehokkaasti, voivat saavuttaa kilpailuetua muihin toimijoihin nähden. Datapohjaiset yritykset ovatkin osoittautuneet erittäin kilpailukykyisiksi ja pystyvät vastaamaan asiakkaiden muuttuviin tarpeisiin paremmin. Näin ollen, on tärkeää ymmärtää, että yrityksen datan hyödyntäminen ja sen pohjalta tehty päätöksenteko on välttämätöntä yrityksen menestyksen kannalta tulevaisuudessa.

Opinnäytetyöni on varmasti hyvinkin ajankohtainen usean pienemmän yrityksen digimarkkinoinnin näkökulmasta. Lainsäädännön kiristymisestä ja teknisten rajoitusten muuttumisesta on ollut puhetta jo useamman vuoden ajan. Kaikilla yrityksillä ei ole kuitenkaan ollut aikaa tai resursseja lähteä muuttamaan ja rakentamaan digistrategioita uudestaan. Muutos on vasta tapahtumassa pikkuhiljaa ja yrityksillä on mahdollisuus vielä reagoida markkinan muuttumiseen, ennen kuin se on liian myöhäistä. On hyvä kuitenkin nostaa asiaa esille useassa eri yhteydessä eri tahojen kanssa, kun pohditaan seuraavia markkinakampanjoita ja teknisiä uudistuksia yrityksen sisällä.

Opinnäytetyötäni varten olen käyttänyt tunnettuja ja luotettavia media- ja digimarkkinointi alan lähteitä, joiden uskon täydentävän opinnäytetyön tietopohjaa ja tukemaan omaa kokemustani ja näkemystäni alasta.

Reflektointina tulevaisuutta varten pohdin seuraavia teknillisiä ratkaisuja ja mahdollisuuksia siihen, kuinka suurten datamassojen avulla voitaisiin esimerkiksi ennaltaehkäistä erilaisia sairauksia, onnettomuuksia tai haitallisia toimintamalleja. Olisivatko ihmiset valmiita jakamaan tarkkoja terveystietojaan tai henkilökohtaisia mieltymyksiään, jos niillä pystyttäisiin tilastollisen mallinuksen avulla ennustaan erilaisia riskitekijöitä tai ongelmatilanteita, joilla halutaan suojalla käyttäjää? Yksityisyydensuoja on hyvä ja olen erittäin tyytyväinen siihen, että käyttäjillä on mahdollisuus itsellä vaikuttaa omaan datajälkeensä. Dataa tulee kuitenkin käyttää vastuullisesti ja läpinäkyvästi. Kuluttajan on kuitenkin hyvä

muistaa myös ne positiiviset asiat ja ne lukuisat mahdollisuudet, joita kerätyllä datalla on mahdollista tehdä.

Lähteet

Apple, 2021a. User Privacy and Data Use. Viitattu 14.3.2023
<https://developer.apple.com/app-store/user-privacy-and-data-use/>

Apple, 2021b. About iCloud Private Relay. Viitattu 14.3.2023
<https://support.apple.com/en-us/HT212614>

Apple, 2022c. About App Privacy Report. Viitattu 24.2.2023
<https://support.apple.com/en-us/HT212958>

BBC, 2020. Facebook sued over Cambridge Analytica data scandal Viitattu 20.3.2023 <https://www.bbc.com/news/technology-54722362>

Berger, B. 2022. WebDesignerDepot-blogi, The Complete Guide To Personalized Marketing. Luettu 14.3.2023
<https://www.webdesignerdepot.com/2022/06/the-complete-guide-to-personalized-marketing/>

Bloomreach, 2022. The Importance of Zero-party Data. Viitattu 1.2.2023
<https://www.bloomreach.com/en/blog/2021/importance-of-zero-party-data>

Carbide, 2023. The Seven Principles of Privacy By Design. Viitattu 20.3.2023
<https://carbidesecure.com/resources/the-seven-principles-of-privacy-by-design/>

CNET, 2020. Google Chrome's privacy changes will hit the web later this year. Luettu 18.3.2023 <https://www.cnet.com/tech/computing/google-chromes-privacy-changes-will-hit-the-web-later-this-year/>

Cookiebot, 2022. Google ending third-party cookies in Chrome. Viitattu 2.2.2023 <https://www.cookiebot.com/en/google-third-party-cookies/>

Digital Marketing Institute, 2022. What Tools Should You Be Using for Your Digital Marketing, Viitattu 10.3.2023
<https://digitalmarketinginstitute.com/blog/digital-marketing-tools>

Digital Markets Act, Regulation (EU) 2022/1925 Viitattu 1.3.2023

Digital Services Act, Regulation (EU) 2022/2065 Viitattu 1.3.2023

EU:n yleinen tietosuoja-asetus (EU) 2016/679

Facebook, 2023. Facebookin tietosuojatarkistus. Viitattu 20.3.2023

<https://www.facebook.com/help/443357099140264>

Forbes, 2021. Beyond compliance re-imagining privacy as customer experience. Viitattu 14.3.2023

<https://www.forbes.com/sites/forbestechcouncil/2021/06/03/beyond-compliance-re-imagining-privacy-as-customer-experience/>

Gartner, 2021. Marketers Are Under a Digital Ad Siege and Must Now Convince Customers to Share Data. Viitattu 20.2.2023

<https://www.gartner.com/en/marketing/insights/articles/marketers-are-under-a-digital-ad-siege-and-must-now-convince-customers-to-share-data>

Goel, V. 2022. Google: Get to know the new Topics API for Privacy Sandbox. Viitattu 3.3.2023 <https://blog.google/products/chrome/get-know-new-topics-api-privacy-sandbox/>

Google, 2020. Introducing the new Google Analytics. Viitattu 3.4.2023

https://blog.google/products/marketingplatform/analytics/new_google_analytics/

Google, 2023. The Privacy Sandbox. Viitattu 2.4.2023

<https://privacysandbox.com/>

Grauer, Y. 2018. Vice: What Are 'Data Brokers,' and Why Are They Scooping Up Information About You? Viitattu 7.2.2023

<https://www.vice.com/en/article/bjpx3w/what-are-data-brokers-and-how-to-stop-my-private-data-collection>

HubSpot, 2022a. Conversion Rate Optimization. Viitattu 12.3.2023

<https://blog.hubspot.com/marketing/conversion-rate-optimization-guide>

HubSpot, 2022b. Customer Segmentation: How to Effectively Segment Users & Clients. Viitattu 14.3.2023 <https://blog.hubspot.com/service/customer-segmentation>

IAB Finland, 2015. Natiivimainonnan opas. Luettu 14.1.2023

<https://www.iab.fi/media/natiivimainonnan-opas-iab-finland.pdf>

Kyberturvallisuuskeskus, 2023. Evästeet. Viitattu 6.2.2023

<https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/evasteet>

Lahtinen, N. & Pulkka, K. & Karjaluoto, H. & Mero, J. 2022. Digimarkkinointi: Luo strategia, vie se käytäntöön, myy enemmän. Helsinki: Alma Talent Oy

Madonna, F. 2022. How to use Statistical Modelling in Digital Marketing-blogi. Luettu 14.3.2023 <https://medium.com/@fabiano.madonna/how-to-use-statistical-modelling-in-digital-marketing-b28653365405>

Marketo, 2021. What is Marketing Automation? Viitattu 11.3.2023 <https://www.marketo.com/marketing-automation/what-is-marketing-automation/>

Salesforce, 2023. What Is a Customer Data Platform? Viitattu 11.3.2023 <https://www.salesforce.com/resources/articles/what-is-a-customer-data-platform/>

SEMrush, 2022. Marketing Basics. Viitattu 12.3.2023 <https://www.semrush.com/blog/category/marketing/marketing-basics/>

SmartyAds, 2021. Data Management Platforms: 4 Things They Do for Marketing Campaigns. Viitattu 10.3.2023 <https://smartyads.com/blog/programmatic-guide-to-data-management-platforms/>

Suomen Digimarkkinointi Oy, 2023a. Viitattu 3.2.2023. <https://www.digimarkkinointi.fi/blogi/sem-ja-seo-yhdessa>

Suomen Digimarkkinointi Oy, 2023b. Viitattu 3.2.2023. <https://www.digimarkkinointi.fi/blogi/sisaltostrategia-markkinoinnin-perusta>

Suomen Digimarkkinointi Oy, 2023c. Viitattu 3.3.2023 <https://www.digimarkkinointi.fi/blogi/myyntisuppilo>

TechAdvisor, 2020. Google Play is much worse than Apple's App Store for your privacy, Viitattu 14.3.2023 <https://www.techadvisor.com/article/739180/google-play-is-much-worse-than-apples-app-store-for-your-privacy.html>

The Verge, 2021. Why Apple's new privacy feature is such a big deal. Viitattu 14.3.2023 <https://www.theverge.com/2021/4/27/22405474/apple-app-tracking-transparency-ios-14-5-privacy-update-facebook-data/>

Tietosuoja-asetuksen (EU) 2016/679 artikla 12

Tietosuojavaltuutetun toimisto, 2023a. Pseudonymisoidut ja anonymisoidut tiedot. Viitattu 15.2.2023 <https://tietosuoja.fi/pseudonymisointi-anonymisointi>

Tietosuojavaltuutetun toimisto, 2023b. Mitä on henkilötieto? Viitattu 15.2.2023 <https://tietosuoja.fi/mika-on-henkilotieto>

Tietosuojavaltuutetun toimisto, 2023c. Rekisteröidyn oikeudet. Viitattu 15.2.2023 <https://tietosuoja.fi/rekisteroidyn-oikeudet>

Tietosuojavaltuutetun toimisto, 2023d. Käyttötarkoitussidonnaisuus. Viitattu 15.2.2023 <https://tietosuoja.fi/kayttotarkoitussidonnaisuus>

Tilastokeskus, 2021. Median merkitys on kasvanut pandemian aikana. Viitattu 2.2.2023. <https://tilastokeskus.fi/tietotrendit/artikkelit/2021/median-merkitys-on-kasvanut-pandemian-aikana-monet-ikaihmiset-ovat-ottaneet-melkoisen-digil>