Haaga-Helia
ammattikorkeakoulu Oy

EU:n yleinen tietosuoja-asetus ja digitalisaatio 2020

Ella Malinen

Opinnäytetyö
Johdon assistenttityön ja kielten
koulutusohjelma
2020

Tiivistelmä

Haaga-Helia ammattikorkeakoulu Oy

Tekijä
Ella Malinen

Koulutusohjelma
Johdon assistenttityön ja kielten koulutusohjelma

Raportin/Opinnäytetyön nimi
EU:n yleinen tietosuoja-asetus ja digitalisaatio 2020

Sivu- ja liitesivumäärä
37 + 6

Tässä opinnäytetyössä on tutkittu Euroopan unionissa vuonna 2018 voimaan astunutta uutta tietosuoja-asetusta ja sen vaikutuksia organisaatioihin yleisellä käytännön tasolla noin kaksi vuotta lain voimaan astumisen jälkeen. Myös Suomen kansallista lainsäädäntöä uudistettiin, ja täten voimaan astui uusi tietosuojalaki vuonna 2019.

Datan määrä kasvaa jatkuvasti digitalisaation ja globalisaation myötä. Tämä on yrityksille sekä kilpailuvaltti, että mahdollinen uhka, jos tietosuojakäytänteistä ei pidetä huolta. Opinnäytetyössä kerrotaan, mitä kaikkea täytyy ottaa huomioon kun henkilötietoja käsitellään.

Opinnäytetyön alussa on kerrottu EU:n tietosuoja-asetuksen historiaa ja lain pääpiirteitä, sekä perusteltu miksi lakia tuli uudistaa. Tämän jälkeen on selitetty keskeistä terminologiaa, jota tietosuojatyön ymmärtäminen ja tekeminen vaatii.

Opinnäytetyön jälkiosa keskittyy dataan ja sitä hyödyntävän toimialan hallitseviin toimijoihin. Tässä yhteydessä on esitelty hyötyjä ja ongelmakohtia. Opinnäytetyön lopuksi kerrotaan yhteensä neljästä vuoden 2018 jälkeen tapahtuneesta tietosuojaloukkaustapauksesta globaalilla ja Suomen tasolla.

Asiasanat
Tietosuoja, digitalisaatio, globalisaatio

Sisällys

1 Johdanto 1
1.1 Näkökulma vuonna 2020 2
2 Tietosuoja 3
2.1 Ihmisoikeussopimukset ja EU:n perusoikeuskirja 3
2.2 EU:n yleisen tietosuoja-asetuksen tavoitteet 4
2.3 Osoitusvelvollisuus 4
2.4 Sisäänrakennettu ja oletusarvoinen tietosuoja 5
2.5 Linkittyminen organisaation strategiaan 5
3 Terminologiaa 7
3.1 Henkilötieto 7
3.2 Toimijat 7
3.2.1 Rekisterinpitäjä 7
3.2.2 Henkilötietojen käsittelijä 8
3.2.3 Tietosuojavastaava 9
3.2.4 Tietosuojavaltuutetun toimisto 9
3.2.5 Euroopan tietosuojaneuvosto 10
3.2.6 Euroopan tietosuojavaltuutettu 11
3.3 Käytänteet 12
3.3.1 Käsittely 12
3.3.2 Profilointi 12
3.3.3 Rekisteri 13
3.3.4 Pseudonymisointi 13
4 Rekisteröidyn yksityisyydensuoja 14
4.1 Rekisteröidyn oikeudet 14
4.2 Automaattinen päätöksenteko 14
4.3 Automaattinen päätöksenteko markkinoinnissa 15
4.4 Rekisteröityjen informointi 16
4.5 Riskit ja erityiset henkilötietoryhmät 17
5 Digitaalistrategia 18
5.1 Digitaaliset sisämarkkinat 18
5.2 Tietojen siirtäminen EU:n ulkopuolelle 19
5.3 Brexit 19
6 Tietosuoja ja tietoturva 21
6.1 Tietojohtaminen 21
6.2 Tietoturva mahdollistaa tietosuojan 21
6.3 Keinoäly 22
7 Dataa kerätään mobiilissa 24

7.1 Big Data ... 24
7.2 Suomalaisten internetin käyttö 2019 ... 24
7.3 Mitä tietoa kerätään? ... 25
7.4 Käyttäjätunnukset helpottavat profilointia ... 25
7.5 Kohdennettu mainonta ... 26
7.6 Datan keräämisen uhkat ... 26
7.6.1 Syrjintä ... 26
7.6.2 Tietojen joutuminen vääriin käsiin ... 27
7.7 Sijaintitiedot ... 27
8 Googlen ja Facebookin valta-asema ... 28
8.1 Googlen sijainnin seuranta ... 28
8.2 Googlen laitteet ... 29
8.3 Project Atlas ... 29
8.4 Cambridge Analytica -skandaali ... 30
8.5 Lobbaaminen ... 30
9 Tietosuojaloukkauksia ... 32
9.1 Case British Airways ... 32
9.2 Case Google ... 33
9.3 Case POP Pankki ... 33
9.4 Case Finnkino ... 34
10 Lopuksi ... 36
10.1 Opinnäytetyöprosessi ... 36
Lähteet ... 38

1 Johdanto

Euroopan unionin yleistä tietosuoja-asetusta (*General Data Protection Regulation*) (679/2016/EU) alettiin soveltaa kaikissa EU-maissa 25.5.2018 alkaen ja se korvasi tietosuojadirektiivin (46/1995/EY), joka annettiin vuonna 1995. Asetukset eivät edellytä kansallisilta hallituksilta uutta lainsäädäntöä kuten direktiivit, vaan ne ovat heti velvoittavia ja sovellettavissa. Suomessa kansallista lainsäädäntöä kuitenkin uudistettiin ja henkilötietojen käsittelyä koskeva uusi tietosuojalaki tuli Suomessa voimaan 1.1.2019. Suomen tietosuojalaki säätää tietyissä kysymyksissä poikkeuksia, sekä antaa täsmennyksiä EU:n tietosuoja-asetukseen. (Oikeusministeriö 2018.) Suomen tietosuojalaki kumosi vuonna 1999 säädetyn henkilötietolain, sekä vuonna 1994 säädetyin lain tietosuojalautakunnasta ja tietosuojavaltuutetusta (Tietosuojalaki 1050/2018). Tämä laki ei muodosta itsenäistä ja kattavaa kokonaisuutta, vaan sitä tulee soveltaa rinnakkain EU:n tietosuoja-asetuksen kanssa (Taskinen 2018).

Tässä opinnäytetyössä on tutkittu Euroopan unionissa vuonna 2018 voimaan astunutta uutta tietosuoja-asetusta ja sen vaikutuksia organisaatioihin yleisellä käytännön tasolla noin kaksi vuotta lain voimaan astumisen jälkeen. Opinnäytetyössä on lähdetty selvittämään, mitä uusi lainsäädäntö konkreettisesti muuttaa. Teknologiaa ja digitalisaatiota on tutkittu opinnäytetyössä arkielämän näkökulmasta ja johdon assistenttityön koulutuksen pohjalta, enkä esimerkiksi tietojenkäsittelyn tradenomin, jolloin työ voisi olla paljon teknisempi ja selvittää esimerkiksi miten big dataa jalostetaan ja järjestelmiä henkilötietojen käsittelyyn luodaan. Opinnäytetyö on laadittu kirjallisuuskatsauksena, jossa perehdyttiin lakitekstien lisäksi tietosuoja-asetuksesta ja digitalisaatiosta suomeksi julkaistuun tuoreeseen kirjallisuuteen. Työtä on laadittu lisäksi tutkimalla artikkeleja, sekä kahta laajempaa raporttia, joissa on esitetty datan keräämisen todellista mittakaavaa ja pohdittu sen eettisyyttä.

Datan määrä kasvaa jatkuvasti digitalisaation ja globalisaation myötä, ja tämä on yrityksille sekä kilpailuvaltti, että mahdollinen uhka, jos tietosuojakäytänteistä ei pidetä huolta. Opinnäytetyössä kerrotaan, mitä seikkoja täytyy ottaa huomioon, kun henkilötietoja käsitellään, eikä niinkään miten yritysten tulisi tällä hetkellä laatia tietosuojakäytänteitään. Nämä käytänteet on jo laadittu kahden vuoden siirtymäajan aikana, kun EU:n tietosuoja-asetuksen määrättiin astuvan voimaan.

Lopputulosta voi hyödyntää henkilö, joka tutustuu Euroopan unionin tietosuoja-asetukseen ja haluaa selkokielisen opasteen siitä, mitä kaikkea arkipäivän työssä tulee ottaa

huomioon ja millä perusteilla organisaatioiden tietosuojakäytänteet muodostuvat. Opinnäytetyö voi herätellä ihmisiä siihen, että oman datan jakaminen datayhtiöjäteille ei ole lopulta yhdentekevää.

1.1 Näkökulma vuonna 2020

Tietosuojaa uudistettiin, koska henkilötietojen suojaa koskevaa sääntelyä tuli uudistaa ja nykyaikaistaa, sillä teknologisen kehityksen ja globalisoitumisen myötä henkilötiedoiksi luettavaa tietoa kerätään huomattavasti enemmän kuin aiemmin. Korkeatasoisella tietosuojalla voidaan myös parantaa luottamusta verkkopalveluihin ja tietosuojaosaamisella auttaa hyödyntämään digitaalitalouden ja digitalisaation luomia mahdollisuuksia. (Andreasson, Riikonen & Ylipartanen 2019, 11.)

Aihe on kiinnostava ja ajankohtainen vuonna 2020, koska yritysten uudet asetuksen mukaisiksi säädetyt tietosuojakäytännöt ovat olleet nyt käytössä miltei kaksi vuotta ja eritasoisia tietoturvaloukkauksia on alkanut ilmenemään. Muutamia näitä tapauksia käsitellään opinnäytetyön lopussa. Capgemini-konsulttiyrityksen vuonna 2019 julkaistun raportin mukaan vain yksi kolmesta yrityksestä täyttää EU:n tietosuoja-asetuksen vaatimukset kansainvälisellä tasolla (Jian ym. 2019, 3).

Digitalisaatio aiheuttaa huolen myös eettisyydestä. Mobiililaitteiden saadessa suurinta jalansijaa verkkoselaamisessa ihmisillä on jatkuvasti sijaintia seuraava laite ja kymmenittäin erilaisia applikaatioita puhelimessaan, jotka keräävät kaikenlaista henkilökohtaista dataa ja voivat myydä sitä eteenpäin. Yritysten on toisaalta pakko hyödyntää digitalisaatiota strategiassaan tai muuten niiden kilpailukyky vaarantuu. Yhä useampien tehtävien hoitaminen vaatii henkilötietojen käsittelyä; nykyään ei ole käytännössä yhtään organisaatiota, jossa ei kerättäisi tai muuten käsiteltäisi henkilötietoja. Rekisterien koot kasvavat ja tietoa haluttaisiin käyttää moniin käyttötarkoituksiin digitalisaation huumassa. Ihmiset ovat puolestaan aikaisempaa valveutuneempia ja näin ollen halutaan pysyä kartalla siitä, mille tahoille henkilötietoja luovutetaan, miksi niitä kerätään ja mihin niitä tallennetaan. Toisaalta moni voi myös sivuuttaa nämä kysymykset, koska ei uskota esimerkiksi, että ei-julkisuuden asemassa olevan henkilön tiedoilla tekisi juuri mitään. Henkilötietojen käyttäminen, kun pyritään vaikuttamaan ihmisten ja joukkojen käyttäytymiseen, on kuitenkin laaja käsite ja yhtenä uhkakuvana onkin, että tietoa voitaisiin käyttää esimerkiksi erilaisten ryhmien eriarvoistamiseen.

2 Tietosuoja

Euroopan unionin tietosuojalainsäädäntö uudistui, kun Euroopan parlamentin ja neuvoston asetus yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta (679/2016/EU) astui voimaan 24. toukokuuta 2016. Tätä seurasi kahden vuoden siirtymäaika, jonka aikana organisaatioilla oli velvollisuus sopeuttaa toimintansa uuden tietosuoja-asetuksen vaatimuksen mukaisiksi. Lakia alettiin soveltaa kansallisesti 25. toukokuuta 2018.

Asetukset ovat säädöksiä, joita sovelletaan automaattisesti ja yhtäläisesti kaikissa EU-maissa heti niiden tultua voimaan. Niitä ei tarvitse erikseen saattaa osaksi kansallista lainsäädäntöä ja ne sitovat kaikkia EU-maita koko laajuudessaan. Euroopan unionissa asetus on säädöksistä (asetukset, direktiivit, päätökset ja suositukset) vahvin. (Euroopan Unioni 2019.) Asetus perusluonteeltaan estää jäsenvaltioita säätämästä asetustekstiä vahvempaa henkilötietojen suojaa. EU:n yleinen tietosuoja-asetus on kuitenkin siinä mielessä poikkeuksellinen asetus, että se jättää joissakin asioissa jäsenvaltioille direktiivinomaista kansallista liikkumavaraa (Andreasson ym. 2019, 36-38).

Tietosuoja on tietosuojan yleislain ja erityislakien henkilötietojen käsittelyä koskevien oikeuksien ja velvollisuuksien huomioon ottamista rekisterinpitäjän operatiivisessa toiminnassa, sekä luonnollisten henkilöiden yksityisyydensuojan ja oikeusturvan varmistamista. Tietosuoja ei ole tiedon varsinaista suojaamista, vaan hyvät käytännöt henkilötietojen käsittelyssä turvaavat tiedon kohteen yksityiselämää, etuja, oikeuksia ja vapauksia. Yksityiselämän suoja on perustuslaillinen oikeus (Suomen perustuslaki 731/1999). Tietosuojalainsäädäntö osoittaa rekisterinpitäjälle ne rajat, joilla on oikeus käsitellä muun muassa tiedon kohdetta koskevia arkaluontoisia henkilötietoja.

2.1 Ihmisoikeussopimukset ja EU:n perusoikeuskirja

EU:n tietosuoja-asetuksen taustalla ovat kansainväliset ihmisoikeussopimukset ja EU:n perusoikeuskirja (2000/C 364/01). Perusoikeuskirjan yksityisyyden suojaa koskevan 7 artiklan mukaan jokaisella on oikeus siihen, että hänen yksityis- ja perhe-elämäänsä, kotiaan ja viestejään kunnioitetaan ja artiklan 8 mukaan jokaisella on oikeus henkilötietojensa suojaan. Tällä perusteella EU:n tietosuoja-asetuksessa määrätään, että tietojen käsittelyn on oltava asianmukaista ja tapahduttava tiettyä tarkoitusta varten. Henkilötietojen käsittelyyn on oltava asianomaisen suostumus tai peruste tulee olla säädetty laissa. EU:n uusi tietosuoja-asetus sisältää säännökset muun muassa henkilötietojen käsittelyä koskevista periaatteista, käsittelyn lainmukaisuudesta sekä arkaluonteisten tietojen käsittelystä. Jo-

kaisella on oikeus tutustua niihin tietoihin, jotka hänestä on kerätty ja vaatia niiden oikaisua. EU:n perusoikeuskirjassa tunnustettuja perusoikeuksia voidaan sen 52 artiklan mukaan rajoittaa ainoastaan lailla. Tällöinkin oikeuksien olennaista sisältöä tulee noudattaa ja rajoitusten on oltava hyväksyttäviä ja välttämättömiä niillä tavoiteltavaan päämäärään nähden. Rajoitusten tulee kunnioittaa henkilötietojen käsittelyn kohteena olevan henkilön ja sivullisten oikeuksia ja vapauksia, sekä vastattava EU:n tunnustamia tavoitteita. Tätä kutsutaan suhteellisuusperiaatteeksi. (Andreasson ym. 2019, 28.)

2.2 EU:n yleisen tietosuoja-asetuksen tavoitteet

EU:n yleinen tietosuoja-asetus korvasi Euroopan parlamentin ja neuvoston direktiivin yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta (95/46/EY). Tietosuoja-asetus luo EU:lle ajanmukaisen, vahvan, yhtenäisen ja kattavan tietosuojakehyksen. Tietosuoja-asetuksen myötä päivitettiin ja nykyaikaistettiin henkilötietodirektiivin periaatteet sekä yhtenäistettiin jäsenmaiden erilaisia tietosuojaa koskevia käytänteitä. Tietosuoja-asetuksen tavoitteena on vahvistaa rekisteröityjen itsemääräämisoikeutta ja lujittaa Euroopan sisämarkkinaulottuvuutta esimerkiksi parantamalla luottamusta online-palveluihin. Tärkeää on myös huomioida tietosuojan globaali ulottuvuus ja tehostaa tietosuojasääntöjen täytäntöönpanon valvontaa. (Andreasson ym. 2019, 27.)

2.3 Osoitusvelvollisuus

EU:n yleinen tietosuoja-asetus perustuu pitkälti riskipohjaiseen ajatteluun. Tämä edellyttää riskilähtöistä tietosuojan suunnittelua ja kykyä todistaa tehdyt toimenpiteet. (Andreasson ym. 2019, 30.) Yksi EU:n tietosuoja-asetuksen ominaispiirteitä onkin osoitusvelvollisuus (*accountability*). Se tarkoittaa, että EU:n tietosuoja-asetuksen velvoitteiden toteutuminen käytännössä on pystyttävä osoittamaan oma-aloitteisesti muunmuassa dokumentein.

Rekisterinpitäjälle on määrätty osoitusvelvollisuus henkilötietojen käsittelyn asianmukaisuuden ja lainmukaisuuden varmistamiseksi. Lakia täytyy sekä noudattaa, mutta myös aktiivisesti ja oma-aloitteisesti eri tavoin, kuten dokumentein, sertifioinnein tai tietotilinpäätöksin osoittaa, että organisaatioon kohdistuvat tietosuojavaatimukset on otettu mukaan sen henkilötietojen käsittelyprosesseihin ja käytäntöihin. Osoitusvelvollisuuden tavoitteena on säästää kustannuksia sekä lisätä luotettavuutta ja tehokkuutta. Tietosuojavelvoitteiden noudattamatta jättäminen ja osoitusvelvollisuuden toteuttamatta jättäminen voi johtaa ankariin sanktioihin, kuten valvontaviranomaisen määräämiin hallinnollisiin sakkoihin. (Andreasson ym. 2019, 25.)

2.4 Sisäänrakennettu ja oletusarvoinen tietosuoja

Sisäänrakennetuksi tietosuojaksi (*data protection by design*) kutsutaan sitä, kun organisaatioita kannustetaan panemaan täytäntöön teknisiä ja organisatorisia toimenpiteitä käsittelytoimintojen suunnittelun alkuvaiheessa, jotta yksityisyys- ja tietosuojaperiaatteita suojataan alusta saakka. Tätä voidaan toteuttaa esimerkiksi tietojen pseudonymisoinnilla. (Euroopan komissio a.) Sisäänrakennettu tietosuoja on osa huolellisen suunnittelun periaatetta. EU:n tietosuoja-asetus korostaa henkilötietojen käsittelyn etukäteissuunnittelun ja huolellisuuden merkitystä. (Andreasson ym. 2019, 23.)

Yritysten ja organisaatioiden on oletusarvoisesti varmistettava, että henkilötiedot käsitellään korkea yksityisyydensuoja taaten. Tällöin käsitellään vain välttämättömiä tietoja, tiedon säilytysaika on lyhyt ja tietoihin on rajoitettu pääsy. Tähän perustuen on myös pidettävä myös huoli, että henkilötiedot eivät ole oletusarvoisesti rajoittamattomien henkilöiden käytettävissä. (Euroopan komissio.) Oletusarvoinen tietosuoja (*data protection by default*) vahvistaa sisäänrakennetun tietosuojan periaatetta ohjaamalla käsittelemään henkilötietoja vain siinä määrin, kuin on tarpeen kussakin yksittäistapauksessa. (Andreasson ym. 2019, 23-24.)

Näitä periaatteita noudatetaan, kun määritetään ja kuvataan käsittelyt ja prosessit, jotka vastaavat asetuksen vaatimuksia. Kaikessa tietojen käsittelyssä tulee varmistaa, että käsitellään vain käsittelyn tarkoituksen kannalta tarpeellisia henkilötietoja määrän, laajuuden, säilytysajan ja saatavilla olon suhteen. Lisäksi organisaatioiden on itse toteutettava tekniset ja hallinnolliset toimenpiteet tietosuojaperiaatteiden täytäntöönpanoa varten. Suojatoimenpiteitä ovat esimerkiksi henkilöstön koulutus, ohjeistus, salassapitosopimukset, omavalvonta ja sertifikaattien käyttöön ottaminen. (Andreasson ym. 2019, 30.)

2.5 Linkittyminen organisaation strategiaan

Digitaalinen murros on jo koskenut ja muuttanut monia toimialoja pysyvästikin. Näin ollen uusia teknisiä ratkaisuja hyödyntäviä toimijoita tulee markkinoille jatkuvasti. Uuden digiajan strategian luominen yritykselle on välttämätöntä, jotta organisaatio pysyy kilpailukykyisenä. Käytännön haasteina keskeisenä on digitalisaatioon liittyvän keskustelun ja käytännön toiminnan sirpaleisuus. Huonoimmassa tapauksessa kokonaiskuvaa ja -vastuuta ei ole organisaatiossa kellään, vaan yksiköt käsittelevät digitaalista murrosta omasta näkökulmastaan. Teknologia tukee strategian toteuttamista, mutta teknologia ei ole itsessään strategia. Uusia teknologioita hyödyntäviä kilpailijoita voi tulla globalisaation ansiosta mistä päin maailmaa tahansa ja perinteisiä toimialarajoja rikotaan. Näistä hyvinä esimerkkeinä toimii Amazon, Uber ja Airbnb. (Hämäläinen, Maula & Suominen 2016, 229-230.)

Tietosuojasta on tulossa näin ollen organisaatioissa strategisen toiminnan keskeinen osa-alue ja se koskettaa organisaation koko toimintaa. Tietosuojasta hyötyvät niin asiakkaat (eli rekisteröidyt), työntekijät kuin koko organisaatio. Tietosuoja on organisaatiolle parhaimmillaan tuottavuuden lisäämisen mahdollistava tekijä, kunhan työntekijöiden riittävä osaaminen ja oikeusturva on varmistettu, sekä asiakkaan yksityisyyden suoja on oikein mitoitettu. Organisaatiossa tulisikin olla resursoituna tietosuojatyön tekeminen, tietosuojavastaava tai tietosuojaryhmä. Tietosuojatyön laiminlyöminen ilmenee operatiivisen toiminnan seurauksina, kuten luottamuksen menettämisenä, imago-ongelmina, selvityskustannuksina, taloudellisina menetyksinä, tuottavuuden ja tehokkuuden laskuna, työntekijöiden työviihtyvyyden huonontumisena, rikossyytteinä, vahingonkorvauksina sekä valvontaviranomaisen hallinnollisina huomautuksina tai sakkoina. Kouluttamattoman työntekijän osaaminen voi olla puutteellista ja se voi vaarantaa hänen sekä asiakkaiden oikeusturvaa ja yksityisyyden suojaa. (Andreasson ym. 2019, 19-23.)

3 Terminologiaa

Suomen tietosuojalain rakenne seuraa EU:n yleisen tietosuoja-asetuksen rakennetta. Sääntelykokonaisuus muodostuu monimutkaiseksi, koska EU:n asetuskin on paikoin vaikeaselkoinen. Unionin oikeudesta johtuen asetuksen käsitteitä ei voi tulkita kansallisella lailla, joten terminologiassa on pitäydytty. (Andreasson ym. 2019, 38.) Tietosuoja-asetuksen ytimessä on henkilötieto ja tiedon keräyksen kohteena on rekisteröity.

3.1 Henkilötieto

Tietosuoja-asetuksessa henkilötiedolla tarkoitetaan tunnistettavaan tai tunnistettavissa olevaan rekisteröityyn liittyvää tietoa. Henkilötietoja voi olla tallennettuna esimerkiksi sähköisissä tiedostoissa, tietokannoissa, paperilla, kortistossa, mapeissa tai ääni- ja kuvatallenteella. (Tietosuojavaltuutetun toimisto a.)

Henkilötiedot on jaoteltu suoriin ja epäsuoriin tunnisteisiin. Suora tunnistetieto tarkoittaa tietoa, joka itsessään riittää henkilön tunnistamiseen, vaikka mitään muuta ei olisi kerrottu. Suorasta tunnistetiedosta esimerkkinä voidaan käyttää esimerkiksi koko nimeä tai henkilötunnusta. Epäsuorat tunnisteet puolestaan on jaettu vahvoihin epäsuoriin tunnisteisiin ja epäsuoriin tunnisteisiin. Vahva epäsuora tunniste ei viittaa suoraan henkilöön, mutta sen avulla voidaan helposti selvittää, kenestä henkilöstä on kyse, esimerkiksi auton rekisterinumerosta tai opiskelijatunnuksesta. Epäsuora tunniste ei yksin paljasta henkilöllisyyttä, mutta saattaa muihin tietoihin yhdistettynä mahdollistaa henkilön tunnistamisen ja siksi epäsuorat tunnisteet ovat näin ollen henkilötietoja. Tavallisia epäsuoria tunnisteita ovat esimerkiksi sukupuoli, ikä, koulutus ja kansallisuus. (Järvelä 2017.)

Mitä tunnistettavammassa muodossa tieto on, mitä yksilöitävämpään käyttötarkoitukseen ja mitä pidempiaikaisempaan käyttöön tietoja kerätään, sitä suurempi tarve on määrätä tiedon käsittelylle velvoitteita ja suojakeinoja. Tietyissä korkean riskin käsittelytilanteissa, kun käsitellään esimerkiksi suurta määrää arkaluonteista tietoa, tulee tehdä erityinen riskiarvio suunniteltujen tietojen käsittelytoimien vaikutuksista henkilötietojen suojalle. (Andreasson ym. 2019, 29.)

3.2 Toimijat

3.2.1 Rekisterinpitäjä

Rekisterinpitäjä on luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Rekisterinpitäjän käyttöä varten siis perustetaan henkilörekisteri ja rekisterin-

pitäjä määrää sen käytöstä. Jos henkilötietojen käsittelyn tarkoitukset ja keinot on määritelty unionin tai jäsenvaltioiden lainsäädännössä, rekisterinpitäjä tai tämän nimitystä koskevat erityiset kriteerit voidaan vahvistaa unionin oikeuden tai jäsenvaltion lainsäädännön mukaisesti. (Andreasson ym. 2019, 83-84.) Rekisterinpitäjän velvollisuus on ilmoittaa tietoturvaloukkauksista valvontaviranomaiselle ja rekisteröidylle. Rekisterinpitäjällä on myös velvollisuus antaa rekisteröidylle ilmaiseksi tiettyjä tietoja hänen henkilötietojensa käsittelystä. (Andreasson ym. 2019, 32.)

3.2.2 Henkilötietojen käsittelijä

Henkilötietojen käsittelijä on luonnollinen henkilö tai oikeushenkilö, viranomainen virasto tai muu elin joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Henkilötietoja voi myös käsitellä kolmas osapuoli. Tällä tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta toimielintä kuin rekisteröity, rekisterinpitäjä, henkilötietojen käsittelijä tai henkilöä jolla on oikeus käsitellä henkilötietoja suoraan rekisterinpitäjän tai henkilötietojen käsittelijän välittömän vastuun alaisena. (Tietosuojavaltuutetun toimisto b.) Henkilötietojen käsittelijällä ei siis tarkoiteta rekisterinpitäjän alaisuudessa toimivia työntekijöitä, jotka käsittelevät henkilötietoja osana työtehtäviään. (Tietosuojavaltuutetun toimisto c.)

Molempien osapuolten, rekisterinpitäjän ja henkilötietojen käsittelijän vastuulla on varmistaa käsittelyn ja suojattavien henkilötietojen asianmukainen turvallisuustaso. Rekisterinpitäjän, sekä henkilötietojen käsittelijän on ylläpidettävä selostetta kaikista vastuullaan olevista tietojenkäsittelytoimista. Henkilötietojen käsittelijän velvollisuus on ilmoittaa tietoturvaloukkauksista rekisterinpitäjälle ja annettava takeet siitä, että tietojen käsittely täyttää tietosuoja-asetuksen vaatimukset. Näin toimitaan kun noudatetaan käytännesääntöjä tai sertifiointimekanismeja. (Andreasson ym. 2019, 32.)

Jos henkilötietojen käsittelyä tekee muu taho, kuten pilvipalveluntarjoaja, tämä alihankkija vastaa jatkossa suoraan sanktioiden uhalla asetuksen vaatimusten noudattamisesta. Asetus edellyttää näissä tilanteissa kirjallisen sopimuksen tekemistä tietyin sisällöllisin vaatimuksin, joka voi tarkoittaa erimerkiksi osapuolen roolien ja vastuiden kirjaamista. Ulkoistustilanteet on tunnistettava ja huolehdittava, että sopimukset ja käsittelyohjeistukset on laadittu asianmukaisesti ja vastuukysymykset on otettu huomioon. Tietosuoja-asetuksessa henkilötietojen käsittelijän roolia ja velvoitteita on terävöitetty kumottuun henkilötietolakiin nähden. (Andreasson ym. 2019, 32.)

3.2.3 Tietosuojavastaava

Tietosuojavastaava on riippumaton organisaation sisäinen asiantuntija, joka seuraa henkilötietojen käsittelyä ja auttaa tietosuojasäännösten noudattamisessa. Tietosuojavastaava ei määrittele henkilötietojen käsittelyn tarkoituksia ja keinoja, vaan tämä kuuluu rekisterinpitäjälle. Organisaation tietosuojavastaavan yhteystiedot tulee ilmoittaa tietosuojavaltuutetun toimistolle. (Tietosuojavaltuutetun toimisto d.)

EU:n yleisessä tietosuoja-asetuksessa tietosuojavastaavan nimittämispakkoa julkisella ja yksityisellä sektorilla laajennettiin ja samalla tietosuojavastaavan asemaa parannettiin ja tehtäviä määriteltiin lainsäädännön tasolla tarkemmin. (Andreasson ym. 2019, 24.) Organisaatioon on nimettävä tietosuojavastaava aina kun on kyse julkisen sektorin toimijasta, joka ei ole tuomioistun ja silloin kun organisaation ydintehtävät muodostuvat laajamittaisesta henkilötietojen käsittelytoimista, joka edellyttää laajaa rekisteröityjen säännöllistä ja järjestelmällistä seurantaa. Tietosuojavastaava tulee nimittää myös silloin, jos organisaation yhdintehtävät kohdistuvat tietosuoja-asetuksen 9 artiklassa nimettyihin erityisiin henkilötietoryhmiin tai rikostuomioita tai rikkomuksia koskeviin tietoihin.

Tietosuojavastaava voi olla organisaation henkilöstön jäsen tai hoitaa tehtäviään palvelusopimuksen perusteella. Konserni/useampi viranomainen tai julkishallinnon elin voi tietyin edellytyksin nimittää vain yhden tietosuojavastaavan. Huomioon otetaan ammattipätevyys ja erityisesti asiantuntemus tietosuojalainsäädännöstä ja alan käytänteistä. Tietosuojavastaavaksi nimitettävän on oltava riippumaton eikä saa ottaa ohjeita vastaan hoitaessaan tehtäviä. Tietosuojavastaava kannattaa nimittää, vaikka tietosuoja-asetus ei nimenomaisesti sitä velvoittaisi. Vaikka laki ei velvoita, on kuitenkin syytä määritellä henkilö jonka tehtävänä on tietosuojaa koskevien asioiden huomioiminen organisation toiminnassa. Hän voi toimia yhteyshenkilönä rekisteröidyn oikeuksiin ja viranomaisvalvontaan liittyvissä kysymyksissä. Organisaation johto ei voi toimia tietosuojavastaavana, koska tässä syntyy eturistiriitatilanne jos johto valvoo omia päätöksiään. (Andreasson ym. 2019, 91.)

3.2.4 Tietosuojavaltuutetun toimisto

Tietosuojaviranomainen on riippumaton julkinen viranomainen, joka valvoo tietosuojalainsäädännön soveltamista ja jolla on valtuudet ryhtyä tutkinta- ja korjaustoimiin. Tietosuojaviranomainen tarjoaa asiantuntija-apua tietosuoja-asioissa ja käsittelee yleisen tietosuoja-asetuksen ja olennaisten kansallisten lakien rikkomista koskevia valituksia. (Euroopan komissio b.)

Jokaisessa EU-maassa on yksi tietosuojaviranomainen ja Suomessa se on Tietosuojavaltuutetun toimisto. Tietosuojavaltuutetun toimisto on perustettu vuonna 1987 ja tietosuojavaltuutettuna on toiminut Reijo Aarnio vuodesta 1997 lähtien. Tietosuojavaltuutetun nimittää valtioneuvosto. Tietosuojavaltuutetun toimisto turvaa ihmisten oikeuksia ja vapauksia henkilötietojen käsittelyssä. Se on asiantuntijaorganisaatio, jossa työskentelee noin 40 henkilöä. Tietosuojavaltuutetun toimisto tekee yhteistyötä muiden EU:n tietosuojaviranomaisten kanssa. Toimisto osallistuu myös Euroopan tietosuojaneuvoston toimintaan ja päätöksentekoon, sekä vie asioita tarvittaessa Euroopan tietosuojaneuvoston arvioitavaksi. Tietosuojavaltuutetun toimisto on itsenäinen ja riippumaton viranomainen. (Tietosuojavaltuutetun toimisto e.)

Tietosuojavaltuutetun toimiston tehtäviä on valvoa henkilötietojen käsittelyn lainmukaisuutta ja ihmisten tietosuojaoikeuksien toteutumista. Yksi tietosuojavaltuutetun toimiston tehtävistä on myös edistää tietoisuutta henkilötietojen käsittelyyn liittyvistä riskeistä, säännöistä, suojatoimista, velvollisuuksista ja oikeuksista. Toimisto tekee myös selvityksiä ja tarkastuksia, määrää seuraamuksia ja antaa lausuntoja henkilötietojen käsittelyä koskevista rikoksista. (Tietosuojavaltuutetun toimisto e.)

Tietosuojaoikeudet auttavat hallitsemaan omia tietoja. Jos oikeuksiaan haluaa käyttää, tulee ensin olla yhteydessä henkilötietoja käsittelevään yritykseen tai organisaatioon, eli rekisterinpitäjään. Jos rekisterinpitäjä kieltäytyy perusteetta, voi olla yhteydessä tietosuojavaltuutettuun. Joissain tapauksissa tietosuojavaltuutettu voi asettaa määräyksiä rekisterinpitäjälle. Tietosuojavaltuutetulle voi myös ilmoittaa, jos epäilee, että henkilötietoja käytetään jossain organisaatiossa tietosuojasäännösten vastaisesti. Tietosuojasäännösten vastaista käyttöä on esimerkiksi, jos henkilötietojen käsittelylle ole lainmukaista perustetta, tai jos tietoja käsitellään liian laajasti käsittelyn tarkoitukseen nähden. (Tietosuojavaltuutetun toimisto f.)

3.2.5 Euroopan tietosuojaneuvosto

Euroopan tietosuojaneuvoston (*European Data Protection Board*) tavoitteena on varmistaa yleisen tietosuoja-asetuksen ja poliisi- ja rikosoikeusviranomaisia koskean tietosuojadirektiivin yhdenmukainen soveltaminen Euroopan unionissa. Neuvosto voi antaa yleisiä ohjeita EU:n tietosuojalainsäädännön käsitteiden selventämiseksi, jotta sen sidosryhmät saavat yhdenmukaisen tulkinnan oikeuksistaan ja velvoitteistaan. Tietosuojaneuvostolla on valtuus tehdä kansallisia valvontaviranomaisia sitovia päätöksiä lain yhdenmukaisen soveltamisen varmistamiseksi. (Euroopan tietosuojaneuvosto.)

Euroopan tietosuojaneuvosto tarjoaa lainsäädäntöä selventäviä yleisiä ohjeita, antaa Euroopan komissiolle neuvoja henkilötietojen suojeluun ja Euroopan unionin uuteen ehdotettuun lainsäädäntöön liittyen, antaa yhdenmukaisuutta koskevia suuntaviivoja rajat ylittävissä tietosuojatapauksissa ja edistää yhteistyötä ja tehokasta tietojen ja parhaiden käytäntöjen vaihtoa kansallisten valvontaviranomaisten välillä. (Euroopan tietosuojaneuvosto.)

Euroopan tietosuojaneuvosto on riippumaton EU:n elin, jolla on oikeushenkilöllisyys ja myötävaikuttaa tietosuojasääntöjen yhdenmukaiseen soveltamiseen kaikkialla EU:ssa ja edistää valvontaviranomaisten välistä yhteistyötä. Tietosuojaneuvoston muodostavat valvontaviranomaisten päälliköt ja Euroopan tietosuojavaltuutettu tai heidän edustajansa. Tietosuojaneuvosto ei anna yksittäisiin pyyntöihin vastauksia vaan se tarjoaa yleistä neuvontaa. (Euroopan tietosuojaneuvosto.)

EDPB koostuu kansallisten tietosuojaviranomaisten ja Euroopan tietosuojavaltuutetun (*European Data Protection Supervisor*) edustajista. Myös ETA:n ja EFTA-valtioiden valvontaviranomaiset ovat jäseniä yleiseen tietosuoja-asetukseen liittyvien asioiden osalta ilman äänestysoikeutta tai mahdollisuutta tulla valituksi puheenjohtajaksi. Tietosuojaneuvosto on perustettu yleisellä tietosuoja-asetuksella ja sen toimipaikka on Brysselissä. Euroopan komissiolla ja yleiseen tietosuoja-asetukseen liittyvien asioiden osalta EFTAn valvontaviranomaisella on oikeus osallistua tietosuojaneuvoston toimintaan ja kokouksiin ilman äänestysoikeutta. (Euroopan tietosuojaneuvosto.)

Yleisesti on arvioitu, että EU:n yleinen tietosuoja-asetus vahvistaa valvontaviranomaisten roolia. Jokaisella jäsenvaltiolla oltava yksi tai useampi asetuksen soveltamista valvova riippumaton kansallinen viranomainen. EDPB valvoo asetuksen soveltamista unionin tasolla. Henkilötietojen käsittelyn tapahtuessa useammassa kuin yhdessä jäsenvaltossa rekisterinpitäjän tai henkilötietojen käsittelijän yleensä päätoimipaikan valvontaviranomainen toimii yhteyspisteenä asiassa ja tekee tarvittavaa yhteistyötä muiden jäsenmaiden valvontaviranomaisten kanssa. (Andreasson ym. 2019, 41.)

3.2.6 Euroopan tietosuojavaltuutettu

Euroopan tietosuojavaltuutettu valvoo, että EU:n hallinnossa käsitellään henkilötietoja yksityisyyttä suojaavien sääntöjen mukaisesti. Se neuvoo EU:n toimielimiä henkilötietojen käsittelyyn, sekä toimintapolitiikkoihin ja lainsäädäntöön liittyvissä kysymyksissä. EDPS käsittelee myös valituksia ja tekee tutkimuksia, tekee yhteistyötä EU-maiden kansallisten viranomaisten kanssa taatakseen tietosuojan johdonmukaisuuden. Yksi sen tehtävistä on

seurata uutta teknologiaa, jolla voi olla vaikutusta tietosuojaan. Euroopan tietosuojavaltuutettu nimetään viiden vuoden toimikaudeksi. Toiminta jakautuu kahteen kokonaisuuteen: Tietosuojan noudattamisen arviointiin EU:n toimielimissä ja muissa elimissä sekä EU:n lainsäätäjän neuvontaan tietosuojaan liittyvissä kysymyksissä eri politiikan aloilla ja uutta lainsäädäntöä koskevissa ehdotuksissa. (Euroopan unioni 2020.)

Jos henkilöllä on syytä uskoa, että EU:n toimielin tai muu elin on rikkonut hänen oikeuttaan yksityisyyteen, tulee ensin olla yhteydessä tietojen käsittelystä vastanneen virkamiehen puoleen. Tämän jälkeen tulee olla yhteydessä sen elimen tietosuojavaltuutettuun, jossa rikkomus tapahtui. Jos tämä ei onnistu, voi tällöin tehdä kantelun Euroopan tietosuojavaltuutetulle. (Euroopan unioni 2020.)

3.3 Käytänteet

3.3.1 Käsittely

Käsittely on toimintoa tai toiminnot, jotka kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti. Käsittelyä on tietojen kerääminen, tallentaminen, järjestäminen, säilyttäminen, muokkaaminen, tiedon haku ja käyttö. Myös tietojen luovuttaminen siirtämällä, levittämällä tai asettamalla saataville on sen käsittelyä, kuten myös tiedon yhdistäminen, rajoittaminen tai sen poistaminen. (OpiTietosuojaa.fi 2020.)

3.3.2 Profilointi

Profilointi on mitä tahansa henkilötietojen automaattista käsittelyä, jossa henkiötietoja käyttämällä arvioidaan luonnollisen henkilön tiettyjä henkilökohtaisia ominaisuuksia, erityisesti analysoidaan tai ennakoidaan piirteitä jota liittyvät esimerkiksi kyseisen luonnollisen henkilön työsuoritukseen, taloudelliseen tilanteeseen tai kiinnostuksen kohteisiin. Profilointi on yksittäistä henkilöä tai ihmisryhmää koskevan tiedon keräämistä ja heidän piirteidensä tai käyttäytymismallien arvioimista johonkin tiettyyn kategoriaan tai ryhmään sijoittamisen tarkoituksessa. Tarkoituksena voi olla analysoida ja ennakoida esimerkiksi kykyä suoriutua jostain tehtävästä, mielenkiinnon kohteita tai todennäköistä käyttäytymistä. Yksinkertainen ikään, sukupuoleen tai pituuteen perustuva henkilöiden luokittelu ei välttämättä ole profilointia. Yritys voi luokitella asiakkaitaan iän ja sukupuolen mukaan tilastollisia tarkoituksia varten. Tarkoituksena on saada kokonaiskuva asiakkaista tekemättä ennakointia. Tällöin ei ole yksilön henkilökohtaisten ominaisuuksien arviointi, jolloin ei ole kyse profiloinnista. Jos tarkoituksena olisia henkilökohtaisten ominaisuuksien arviointi, luokittelu saatettaisiin määritellä profiloinniksi. (Tietosuojavaltuutetun toimisto g.)

3.3.3 Rekisteri

Rekisteri on mitä tahansa jäsenneltyä henkilötietoa sisältävä tietojoukko, josta tiedot saa tietyin perustein. Joukko voi olla keskitetty, hajautettu, toiminnallisin tai maantieteellisin perustein jaettu. (Tietosuojavaltuutetun toimisto h.)

3.3.4 Pseudonymisointi

Pseudonyymi data on tietoa, joka ei ole sellaisenaan yhdistettävissä yksittäiseen henkilöön. Pseudonymisoiminen on yksi uusista EU:n yleisen tietosuoja-asetuksen määritelmistä ja siksi käsite tulee ymmärtää. Se tarkoittaa henkilötietojen käsittelemistä siten, että henkilötietoja ei voida enää yhdistää tiettyyn rekisteröityyn käyttämättä lisätietoa. Lisätieto tulee tässä tapauksessa olla erillään, jotta yhdistelyä tunnistettuun, tai tunnistettavissa olevaan luonnolliseen henkilöön ei tapahdu. Esimerkiksi evästetiedoista ei sellaisenaan voi usein tunnistaa tiettyä henkilöä, mutta tilanne muuttuu, jos evästeeseen yhdistetään kirjautumistietoja tai IP-osoitteita. (Tarhonen 2017.) Pseudonymisoidut tiedot lasketaan henkilötiedoiksi, joten niiden käsittelyyn tulee soveltaa tietosuojasäännöksiä. Pseudonymisointi on tavallista tutkimustoiminnassa ja tilastoinnissa. (Tietosuojavaltuutetun toimisto i.)

Pseudonymisoinnissa tiedon suora tunnistettavuus muutetaan, esimerkiksi korvaamalla tiettyjä tietoja satunnaisella tunnisteella. Anonymisointi puolestaan tekee tiedosta sellaista, ettei sitä voi missään tilanteessa enää yhdistää tiettyyn luonnolliseen henkilöön. (Tarhonen 2017.) Anonymisoituihin tietoihin ei enää sovelleta tietosuojasäännöksiä, koska niitä ei katsota henkilötiedoiksi (Tietosuojavaltuutetun toimisto i).

4 Rekisteröidyn yksityisyydensuoja

EU:n tietosuoja-asetuksen mukaan henkilötiedot on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten. Käsittely vaatii asetuksessa asetetun käsittelyperusteen. Vuonna 2018 voimaan astuneessa EU:n tietosuoja-asetuksessa tietojen käsittelyperusteet on määritelty huomattavasti tarkemmin, kuin sen kumoamassa henkilötietodirektiivissä. Esimerkiksi suostumukselle on annettu kumottua lakia takempia kriteereitä ja on huomioitava, että rekisterinpitäjää koskeva osoitusvelvollisuus koskee myös suostumuksen olemassaoloa. (Andreasson ym. 2019, 34.)

4.1 Rekisteröidyn oikeudet

Henkilöllä on oikeus tietää mitä henkilötietoja organisaatioilla on hänestä hallussaan ja mihin näitä henkilötietoja käytetään. Oikeuksiin kuuluu myös pyytää virheellisten, epätarkkojen ja puutteellisten henkilötietojen korjaamista tai poistamista. (Tietosuojavaltuutetun toimisto j.) Kerätty data pitää olla esitettävissä kohtuullisen nopeasti ja olla poistettavissa kokonaan, jos yritys haluaa välttyä rangaistusuhalta. Henkilötietojen käsittelyä saa myös vastustaa ja pyytää niiden käsittelyn rajoittamista. Henkilöllä on myös oikeus vaatia, että häntä koskevat päätökset tekee ihminen, eikä päätöksenteko ole täten automaattista (Tietosuojavaltuutetun toimisto k).

Henkilöllä on myös oikeus siirtää tietojaan toiselle rekisterinpitäjälle. Esimerkiksi joskus palveluntarjoajaa vaihtaessa voi olla etua siitä, että henkilöstä kerrytetty tieto siirtyy uuden organisaation haltuun. Tiedonsiirtämisen edellytyksenä on muun muassa se, että tietoja on käsitelty automaattisen tietojenkäsittelyn kautta. Tiedon siirtäminen ei myöskään tarkoita, että alkuperäinen rekisterinpitäjä poistaa kerätyn tiedon, vaikkakin henkilöllä on edelleen oikeus pyytää tietojen poistamista. (Tietosuojavaltuutetun toimisto l.)

4.2 Automaattinen päätöksenteko

Päätöksenteko on automaattista, kun on kyse vain automaattiseen henkilötietojen käsittelyn perusteella tehdyistä päätöksistä ja näillä päätöksillä on oikeusvaikutuksia tai ne muuten vaikuttavat rekisteröityyn merkittävästi. Päätöksiä voidaan tehdä automaattisesti ilman profilointia ja profilointia voidaan myös tehdä ilman automaattista päätöksentekoa. Samaan henkilötietojen käsittelytoimintoon voi myös sisältyä molempia, automaattista päätöksentekoa sekä profilointia. Myös päätökset, jotka eivät perustu automaattiseen henkilötietojen käsittelyyn, voivat sisältää profilointia; esimerkiksi jos pankki käsittelee lainanhakijan luottoluokitustietoa lainapäätöstä tehdessään ja luonnollinen henkilö osallistuu merkityksellisellä tavalla päätöksetekoprosessiin ennen lopullisen lainapäätöksen antamista.

Automaattinen päätöksenteko voi perustua muun muassa rekisteröidyltä itseltään saatuun tietoon kyselylomakkeen muodossa, havainnointuun tietoon, kuten puhelimen sijaintitietoihin tai pääteltyyn tietoon esimerkiksi valmiista profiilista, kuten luottoluokitustieto. (Tietosuojavaltuutetun toimisto g.)

Automaattisesta päätöksenteosta on kyse silloin, kun luonnollinen henkilö ei osallistu päätöksentekoon, kun automatisoidun prosessin seurauksena syntyy rekisteröityä koskeva suositus. Päätös on vain automaattiseen käsittelyyn perustuva jos kyseessä on rutiininomainen, automaattisesti luotujen profiilien soveltaminen henkilöihin ilman tosiasiallista lopputulokseen vaikuttamisen mahdollisuutta. Jotta luonnollisen henkilön voidaan katsoa osallistuvan päätöksentekoon, on hänen pystyttävä vaikuttamaan tehtävän päätöksen lopputulokseen. (Tietosuojavaltuutetun toimisto g.)

Rekisteröidyllä on oikeus olla joutumatta sellaisen päätöksen kohteeksi, joka perustuu pelkästään automaattiseen käsittelyyn, kuten profilointiin ja jolla on häntä koskevia oikeusvaikutuksia tai jotka vaikuttaa häneen vastaavalla tavalla merkittävästi. Tässä on kuitenkin poikkeuksia, kuten jos päätös on välttämätön rekisteröidyn ja rekisterinpitäjän välisen sopimuksen tekemistä tai täytäntöönpanoa varten tai se on hyväksytty rekisterinpitäjään sovellettavassa unionin oikeudessa tai jäsenvaltion lainsäädännössä tai jos se perustuu rekisteröidyn suostumukseen. Rekisterinpitäjän on tässä tilanteessa aina huolehdittava suojatoimenpiteistä; rekisteröidylle kerrotaan tietojen käsittelystä, tarjotaan yksinkertaisia tapoja vaatia ihmisen osallistumista tietojen käsittelemiseen ja mahdollisuus esittää oma kantansa tai riitauttaa päätös. Käsiteltävät tiedot sekä algoritmit tulee tarkistaa säännöllisesti, jotta voidaan varmistaa päätöksentekoprosessin toimivuus. Asiaa käsittelevän henkilön on pystyttävä vaikuttamaan tehtävän päätöksen lopputulokseen. Arviossa on otettava huomioon kaikki relevantti tieto ja lisäselvityksen toimittamiseen on annettava mahdollisuus rekisteröidylle. Rekisteröidyllä on myös oikeus saada selvitys kyseisen arvioinnin jälkeen tehdystä päätöksestä. (Tietosuojavaltuutetun toimisto g.)

4.3 Automaattinen päätöksenteko markkinoinnissa

Markkinointi perustuu kasvavassa määrin automatisoituihin työkaluihin ja voi sisältää usein pelkästään automaattista henkilötietojen käsittelyä. Jos markkinointi perustuu ainoastaan automaattiseen henkilötietojen käsittelyyn, rekisterinpitäjän on arvoitava soveltuuko automaattista päätöksentekoa koskeva sääntely omaan toimintaan. Yleensä kohdennetulla profilointiin perustuvalla markkinoinnilla ei ole oikeusvaikutuksia vastaavia merkittäviä vaikutuksia yksilöihin. Silloin se ei ole automaattista päätöksentekoa. Esimerkkinä tästä on verkkokaupan markkinointi, joka perustuu demografiseen profiiliin ja jonka kohderyhmä voisi esimerkiksi olla 20-vuotiaat pääkaupunkiseudulla asuvat naiset.

On myös mahdollista, että kohdistettuun profilointiin perustuvalla markkinoinnilla on vastaavia merkittäviä vaikutuksia yksilöihin. Tällöin arvioinnin kohteena on esimerkiksi profilointimenetelmän tunkeilevuus, kuten tapa jolla yksilöä seurataan eri verkkosivujen, laitteiden ja palveluiden välityksellä. Sellainen markkinointi, joka vaikuttaa normaalisti vain vähäisesti markkinoinnin kohteisiin, saattaa vaikuttaa merkittävällä tavalla henkilöryhmiin, kuten vähemmistöihin. Esimerkiksi korkeakorkoisten lainojen säännöllinen kohdennettu markkinointi henkilölle, joka on taloudellisessa ahdingossa, voi johtaa henkilön lisävelkaantumiseen. Myös lapsiin kohdennettavan markkinoinnin on oltava tarkasti säädeltyä. Tietosuoja-asetuksen mukaan erityisesti lasten henkilötietoja on pyrittävä suojaamaan kun on kyse lasten henkilötietojen käyttämisestä markkinointitarkoituksiin, henkilöprofiilien luomisesta tai lasten henkilötietojen keräämisestä kun lapsi käyttää hänelle tarkoitettuja palveluita. (Tietosuojavaltuutetun toimisto g.)

4.4 Rekisteröityjen informointi

Rekisteröidyllä on oikeus saada tietoa henkilötietojensa keräämisestä ja käsittelystä. Rekisterinpitäjän on toteutettava lainmukaiset toimenpiteet toimittaakseen rekisteröidylle kaikki käsittelyä koskevat tiedot tiiviisti esitetyssä sekä helposti ymmärrettävässä ja saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä. Rekisteröityä tulee informoida siitä, kuka on rekisterinpitäjä, tarkoituksista joihin tietoja käsitellään, tietojen säilytysajat, mihin tietoja luovutetaan ja kuinka rekisteröity voi käyttää oikeuksiaan. (Andreasson ym. 2019, 165-166.)

Informoinnin sisältö ja ajankohta liittyy siihen, mistä tiedot saatiin. Jos tiedot kerätään rekisteröidyltä itseltään, käsittelyä koskeva informaatio annetaan tietojen keräämisen aikaan. Jos tiedot saadaan muualta kuin rekisteröidyltä, informoidaan rekisteröityä kohtuullisessa ajassa, eli viimeistään kuukauden kuluttua tietojen saamisesta. (Andreasson ym. 2019, 166.)

Joissain tapauksissa henkilötietojen käsittelystä ei tarvitse ilmoittaa. Tällaisia tapauksia on esimerkiksi jos tiedot on saatu muualta kuin rekisteröidyltä ja jos tietojen hankinnasta tai luovutuksesta säädetään nimenomaiseti rekisterinpitäjään sovellettavassa lainsäädännössä, jossa vahvistetaan asianmukaiset toimenpiteet rekisteröidyn oikeutettujen etujen suojaamiseksi. Suomessa informointi tämänkaltaisissa tapauksissa tapahtuu usein organisaatioden internetsivujen kautta. (Andreasson ym. 2019, 166.)

4.5 Riskit ja erityiset henkilötietoryhmät

EU:n tietosuoja-asetuksessa riskeillä tarkoitetaan henkilötietojen käsittelystä rekisteröidylle mahdollisesti aiheutuvia fyysisiä, aineellisia tai aineettomia vahinkoja silloin esimerkiksi kun käsittely voi johtaa syrjintään, identiteettivarkauteen tai petokseen, taloudellisiin menetyksiin, sosiaaliseen vahinkoon, pseudonymisoinnin kumoutumiseen tai arkaluonteisten tietojen paljastumiseen sivulliselle.

Riski voi olla korkeampi silloin kun käsitellään erityisiin henkilötietoryhmiin kuuluvia tietoja tai heikossa asemassa olevien, kuten lasten tietoja. Riski kasvaa myös kun käsitellään suuria määriä henkilötietoja, käsittely koskee suurta rekisteröityjen määrää ja jos arvioidaan henkilökohtaisia ominaisuuksia, kuten jos ollaan tehty henkilöprofilointa varten suoritettu analyysi. Samaan joukkoon lukeutuvia tietoja myös ovat geneettisen tai terveyteen liittyvän tiedon käsittely. Rekisterinpitäjä ja henkilötietojen käsittelijä velvoitetaan ryhtymään toimiin, jotka vastaavat henkilötietojen käsittelyyn kulloinkin kohdistuvaa riskiä. (Andreasson ym. 2019, 29.)

5 Digitaalistrategia

Digitaalisen murroksen taustalla ovat tietotekniikan ja teknologian kehittyminen, sekä niiden käyttömahdollisuudet uusilla elämänalueilla. Digitalisoimisella tarkoitetaan sitä, kun joku aiemmin fyysisesti tehty asia muutetaan digitaalisesti tehtäväksi. Digitalisaatiolla puolestaan tarkoitetaan sitä, kun toimintaympäristö muuttuu ja on kyse innovaatioista, asiakaslähtöisyydestä ja digitaalitekniikan uudenlaisesta käytöstä. Lyhyesti, strategia tarkoittaa suunnitelmaa, joka määrittää organisaation suunnan ja liiketoiminnan laajuuden pidemmällä aikajänteellä. (Hämäläinen ym. 2016; 21, 65.) Kun toimintaympäristö muuttuu, siihen tulee adaptoitua.

Tieto- ja viestintätekniikka on lisännyt tuottavuutta ja talouskasvua EU:ssa 1995 vuodesta lähtien. Vuoteen 2020 mennessä eri tekniikoiden lähentyminen on hämärtänyt televiestinnän, lähetystoiminnan ja tietotekniikan välisiä rajoja. Euroopan komissio laittoi alulle digitaaliset sisämarkkinat vuonna 2015 ja antoi keskeiset lainsäädäntöehdotukset, jotka koskivat sähköisen kaupankäynnin vauhdittamista, tekijänoikeuksia, sähköisen viestinnän tietosuojaa, digitaalisten oikeuksien yhdenmukaistamista, yhdenmukaisia alv-sääntöjä ja kyberturvallisuutta. (Maciejewski & Gouardères 2019, 1.)

EU:n neuvosto antoi 7.6.2019 päätelmät pitkälle digitalisoidun Euroopan tulevaisuudesta vuoden 2020 jälkeen. Nämä päätelmät toimivat pohjana kehitettäessä EU:n tulevaa digitaalipolitiikkaa. Päätelmissä todettiin, että on tärkeää tukea innovointia ja edistää eurooppalaisia digiteknologioita kunnioittaen tekoälyssä eettisiä periaatteita ja arvoja, vahvistaa Euroopan kyberturvallisuusvalmiuksia, parantaa digitaitoja ja kehittää gigabittiyhteiskuntaa, johon kuuluu myös 5G. Näissä päätelmissä korostetaan myös, että alalla työskentelevien naisten lukumäärää tulisi kasvattaa ja varmistaa, että heikommassa asemassa olevat ryhmät hyötyvät digitalisaatiosta, eivätkä jää sen ulkopuolelle. (EU:n neuvosto 2019.)

5.1 Digitaaliset sisämarkkinat

Digitaalisten sisämarkkinoiden kehittämisessä on kyse kansallisten esteiden poistamisesta verkossa tapahtuvilta liiketoimilta. Kiinteistä käyttöjärjestelmistä siirrytään mobiilialustoille. Pilvipalveluiden, rajattoman mobiilidatan siirron kehittämiselle, yksityisyyden ja henkilötietojen suoja ja verkkoturvallisuus edellyttää lainsäädännön kehittämistä. Euroopan parlamentin lainsäädäntötoimet digitaalisten sisämarkkinoiden luomisessa lisäävät Euroopan kasvuun vuosittain 177 miljardia euroa. (Maciejewski & Ratcliff 2019, 1.)

5.2 Tietojen siirtäminen EU:n ulkopuolelle

EU:n yleistä tietosuoja-asetusta sovelletaan Euroopan talousalueella, johon kuuluvat EU-maiden lisäksi Islanti, Liechtenstein ja Norja. Keskeinen tavoite on taata henkilötietojen vapaa liikkuvuus Euroopan talousalueella. Siksi henkilötietoja saa siirtää Euroopan talousalueeseen kuuluvaan maahan samoilla perusteilla kuin Suomen sisällä. (Tietosuojavaltuutetun toimisto m.)

Kun henkilötietoja siirretään Euroopan unionin ja Euroopan talousalueen ulkopuolelle, tietosuoja-asetuksen takaama henkilötietojen suojan taso heikkenee. Tämä aiheuttaa riskejä rekisteröidylle, joiden tietoja siirretään. Siksi tietosuoja-asetuksessa määritellään edellytyksiä niille perusteille, joilla henkilötietoja voidaan siirtää ETA:n ulkopuolelle kolmansiin maihin tai kansainvälisille järjestöille. Tällöin sovelletaan tietosuoja-asetuksen viidennen luvun säännöksiä. (Tietosuojavaltuutetun toimisto m.)

EU:n yleisessä tietosuoja-asetuksessa määritetään perusteet, joiden nojalla henkilötietojen siirtäminen EU:n ulkopuolelle on sallittua. Tietoja saa siirtää, jos komissio on tehnyt päätöksen, että kyseinen kolmas maa varmistaa riittävän tietosuojan tason. Jos päätöstä ei ole tehty, henkilötietojen siirto on EU-alueen ulkopuolelle sallittua vain, jos rekisterinpitäjä tai henkilötietojen käsittelijä ovat toteuttaneet asianmukaiset suojatoimet ja jos rekisteröityjen saatavilla on täytäntöönpanokelpoisia oikeuksia ja tehokkaita oikeussuojakeinoja. Näitä suojakeinoja ovat esimerkiksi komission hyväksymät vakiolausekkeet, asetuksen mukaiset yritystä koskevat sitovat säännöt, jotka valvontaviranomainen on vahvistanut tai vakiolausekkeet, jotka tietosuojaviranomainen ja komissio ovat hyväksyneet. (Tietosuojavaltuutetun toimisto m.) Henkilötietoja voi siirtää suoraan vastaavuuspäätöksen perusteella, eikä esimerkiksi erillistä lupaa tietosuojavaltuutetulta tarvita. Tietosuojalainsäädäntöä on noudatettava näissäkin tilanteissa kokonaisuudessaan. Komissio tarkastelee päätöksiä uudelleen vähintään 4 vuoden välein. (Tietosuojavaltuutetun toimisto n.)

5.3 Brexit

Britannian EU-ero tuli voimaan 1.2.2020. Siirtymäkausi kestää vuoden 2020 loppuun, johon saakka jatketaan EU:n nykysäännöillä ja neuvotellaan tulevasta suhteesta. Siirtymäkauden aikana Britannialla on kaikki jäsenvaltion oikeudet ja velvollisuudet, mutta se ei osallistu enää EU:n päätöksentekoon tai EU:n elinten toimintaan. Henkilötietojen siirrot Britanniaan voivat jatkua samoilla edellytyksillä kuin ennen siirtymäkautta. Se tarkoittaa, että henkilötietoja voidaan siirtää Britanniaan samoilla perusteilla kuin Suomen sisällä vuoden 2020 loppuun asti. (Tietosuojavaltuutetun toimisto o.)

On mahdollista, että Euroopan komissio tekee siirtymäkauden aikana Britanniaa koskevan tietosuojan riittävää tasoa koskevan päätöksen, jonka perusteella tietoja siirrettäisiin. Tämä vaatii kuitenkin valmistelua ja kolmannen maan oikeusjärjestelmän laajan arvioinnin. (Tietosuojavaltuutetun toimisto o.)

6 Tietosuoja ja tietoturva

Digiturvallisuuden merkitys liiketoiminnassa kasvaa entisestään, kun esimerkiksi liiketoiminnan arvosta yhä suurempi osuus muodostuu tietojenkäsittelyä hyödyntämällä. Tietoturvaa on tietosuojan näkökulmasta kaikki tekniset ja hallinnolliset toimenpiteet, joilla tiedon turvaamiseen pyritään. Toimenpiteillä pyritään säilyttämään ja suojaamaan tiedon laatu, eheys, sekä luottamuksellisuus teknisin ja hallinnollisin keinoin. Käytännön toimenpiteitä on varmistaa tietojärjestelmien ja verkkojen keskeytymätön toiminta sekä estää valtuudeton käyttö ja tahallinen tai tahaton tiedon tuhoutuminen tai sen vääristyminen. (Andreasson ym. 2019, 21.) Vaikka työssään ei käsittelisi mitään salassa pidettävää tietoa, tulee tietoturvallisuus silti huomioida. Vaikka itsellään ei olisi suoraan pääsyä tietoihin, voidaan käyttäjää tai hänen käytössä olevia laitteita käyttää tietoihin käsiksi pääsyyn. (Järvinen & Rousku 2017.)

6.1 Tietojohtaminen

Tietojohtamisen pääpaino tulisi olla ennalta ehkäisevässä toiminnassa, koska tietoturva- ja tietosuoja-asioissa vahingon ennaltaehkäisy on huomattavasti halvempaa kuin sen jälkikäteinen korjaaminen. Analytiikka ja big data on joko mahdollisuus tai riski. Asiakkaiden käyttäytymisen ennustaminen voi olla parhaimmillaan avain menestykseen. Organisaatiossa tulee lakien ja asetusten tuntemuksen lisäksi osata hyödyntää dataa kaupallisesti. Optimaalisessa tapauksessa organisaatiossa tunnetaan menetelmät, ymmärretään kehitystoimien taustalla liiketoiminnan tavoitteet ja tiedostetaan ympäristön asettamat realiteetit. Samoin tiedetään millaisia yksityisyyttä suojaavia menetelmiä ratkaisun toteutuksessa on mahdollista soveltaa tai miten henkilötietojen käytöstä kannattaa viestiä eri kohderyhmille. Digitaaliseen turvallisuuteen tulee panostaa, eikä se voi olla tekemisen jälkiajatus, vaan kaikkialla läsnä sisäänrakennettuna valmiiksi kaikkiin rakenteisiin, palveluihin ja järjestelmiin. (Andreasson ym. 2019, 186.)

6.2 Tietoturva mahdollistaa tietosuojan

Organisaatioiden viisi suurinta uhkaa tietoturvallisuuden näkökulmasta ovat päivitysten laiminlyönti, kiristyshaittaohjelmat, huijausviestit ja tietojenkalastelu, ulkoistusten ja laitehankintojen hallinta, sekä hyökkäyksillä uhkaaminen ja niillä kiristäminen. (Andreasson ym. 2019, 150.) Riskit jakautuvat siis tietoaineistoon liittyviin uhkiin, kuten käyttäjätunnusvarkauksiin, sekä teknisiin uhkiin, kuten sovellushaavoittuvuuksiin. Tietoturvaongelmia syntyy herkästi perinteisten uhkien ja uusien toimintamallien ja palveluiden yhdistelmänä. (Valtiovarainministeriö 2010, 13.)

On yrityksen vastuulla pitää tietoturva kunnossa. Henkilötiedot tule suojata modernien tietoturvaratkaisujen avulla. Esimerkiksi, jos yrityksen henkilörekisteriin tapahtuu tietomurto, on se yrityksen vastuulla jos järjestelmä on alun perin hyväksynyt tietojen salaamiseen hyvin heikon salasanan ja tämä on murrettu. (Tivi 2016.) Myös kalasteluviestien uhkasta tulee kouluttaa työntekijöitä säännöllisesti. Työntekijöille täytyy selkeyttää sitä, mihin palveluihin organisaation jäsenet voivat syöttää tunnuksia ja salasanoja, sekä neuvoa siitä, miten vaikkapa URL-osoitteen oikeellisuuden voi tarkistaa. (Tietosuojavaltuutetun toimisto 2019a.)

Tietovuodot voivat pahimillaan aiheuttaa imagotappion, muiden vahinkojen korvaamista sekä muita taloudellisia seuraamuksia. EU:n yleisen tietosuoja-asetuksen yhtenä tavoitteena on tietosuojasääntöjen täytäntöönpanon valvonnan tehostaminen. Tietosuoja-asetus patistaakin siis rekisterinpitäjiä ja yrityksiä tarkistamaan tietosuojakäytäntöjensä lainmukaisuus, varmistaa tietoturvansa riittävyys ja varautua ongelmatilanteisiin. Tietosuoja-asetuksen tarkoituksena on ohjata yhteisöt ja yritykset ottamaan tietosuoja-asiat kokonaisvaltaisesti huomioon toimintansa suunnittelussa ja prosessiensa dokumentoinnissa. Apukeino mahdollistaa jatkuvan prosessin, jossa riskit tunnetaan niin hyvin kuin mahdollista etukäteen ja niihin osataan varautua. Tietosuojasta huolehtiminen on kilpailuetu ja se nopeuttaa tietojärjestelmien hankinnoissa tarvittavien vaatimusmäärittelyiden laadintaa. (Andreasson ym. 2019, 57-65.)

Käytännön riskejä tietoturvatyössä on käyttöoikeuksien ja käsittelyvaltuuksien hallinnan puutteet, jolloin käyttöoikeuksia järjestelmiin on voimassa vaikka ei pitäisi. Tätä voidaan ehkäistä tunnistautumisella ja käyttöoikeuksien säännöllisellä päivittämisellä. Yhtenä riskinä on myös henkilöstön koulutuksen puute, joka voi vaarantaa salassapitovelvollisuuden ja altistaa henkilön hairahtumaan esimerkiksi huijausviesteihin. Sosiaalinen hakkerointi on keino urkkia salassapidettäviä tietoja, kuten liikesalaisuuksia. Tätä voidaan estää esimerkiksi hyvin suojatulla turvapostilla ja kouluttamalla henkilöstö siihen, että kiireessäkin on sallittua selvittää ajan kanssa tarpeen mukaan tietojen pyytäjän henkilöllisyys ja oikeudet tietoihin. Kaikista konkreettisin esimerkki tietoturvatyöstä on jätteen käsittelyprosessin suunnitteleminen. Esimerkiksi salassa pidettävät paperit ja elektroniikkaromu tulee hävittää oikeaoppisesti ja hävityspalvelun voi tilata siihen erikoistuneelta yritykseltä. (Andreasson ym. 2019, 64-65.)

6.3 Keinoäly

Merkittävät viisi muutostekijää teknologian kehittymisessä ovat olleet päätelaitteet, tietoliikenne, tapa tuottaa palveluita, sosiaalinen media ja datan analysoiminen. Uudenlaiset palvelut, sensorit ja kerättävä tieto tulevat ohjaamaan tulevaisuudessa kaikkea toimintaamme

yhä enemmän proaktiiviseen suuntaan, jolloin tarpeet voidaan ennakoida tai jopa välttää kokonaan. Toistaiseksi esimerkiksi terveydenhuolto pohjautuu enimmäkseen reaktiiviseen toimintaan, kun jotain on jo tapahtunut. Tämänlainen toiminnan muovautuminen tapahtuu yhä enenevästi itseoppivien keinoälyjärjestelmien ansiosta. Perinteinen tietokoneohjelma on koodattu tekemään asiat aina samalla tavalla, mutta nykyinen keinoäly voi kehittyä ja oppia uusia toimintamalleja itsenäisesti. Tulevaisuudessa nämä järjestelmät voivat verkostoitua yhä enemmän keskenään ja olemaan entistä suorituskykyisempiä. Mitä enemmän tietoa kerätään, sitä enemmän sitä myös yhdistellään. Tässä tietoturva ja -suoja kohtaavat; tietoja ei saa päästä käyttämään ne tahot, joilla ei ole siihen oikeutta. Keinoälyjärjestelmien osalta tämä edellyttää tarkkaa normistoa ja lainsäädännön mallintamista niille. Jos keinoälyjärjstelmältä kysytään jotain, jota kysyvällä ei ole oikeus saada tietoonsa, järjestelmä ei saa luovuttaa tätä tietoa. (Järvinen & Rousku 2017.)

7 Dataa kerätään mobiilissa

Norjan kuluttajanviraston raportissa ”Out of Control” (2020) seurattiin kymmentä eri Android-pohjaista puhelinsovellusta ja selvisi, että ne luovuttavat dataa ainakin 135:lle kolmannelle osapuolelle, jotka ovat mukana mainostuksen ja käyttäytymisen profiloinnin kehittämisessä. Tämä on ongelmallista EU:n tietosuoja-asetuksen näkökulmasta. Tutkimuksen lopputulemana oli se, että 20 kuukautta asetuksen voimaantulon jälkeen käyttäjiä seurataan yhä kokonaisvaltaisesti. Mobiiliapplikaation käyttäjällä ei voi olla mitään arviota paljon hänen tietojaan loppujen lopuksi jaetaan kolmansille osapuolille, eikä näin ollen voi estää omien tietojensa liikkumista. Tietosuojavaltuutetut painostavat mainostajia ja julkaisijoita EU:n tietosuoja-asetuksella, jotta heidän olisi pakko keksiä uudet digitaalisen mainostamisen metodit kunnioittaakseen perusoikeuksia. (Forbrukerrådet 2020, 5-7.)

7.1 Big Data

Digitalisaatio on mahdollistanut suurten tietomäärien keräämisen. Asiakas kohdataan monikanavaisesti ja tuotanto- ja toimitusprosessit tuottavat suuria määriä tietoa. Yleisimmin Big Dataan liitetään kolme määrettä: Määrä (*volume*) tarkoittaa, ettei data ole käytettävissä määränsä takia yleisesti käytössä olevilla laitteilla ja ohjelmistoilla järkevässä ajassa. Datan ominaisuutta kuvaa myös nopeus (*velocity*), koska dataa kertyy usein automaattisesti kerättynä monista lähteistä kasaantuvasti ja se muuttuu nopeasti. Datalla ei ole välttämättä rakennetta, jolloin sitä on vaikea analysoida sellaisenaan. Tätä kutsutaan monimuotoisuudeksi (*variety*). (Sovelto 2020.)

Datan määrän kasvua ei voi pysäyttää. Vuonna 2020 määrän arvioidaan kasvavan entisestään. Datan määrän jatkuva kasvaminen luo uusia työpaikkoja sen käsittelemiseksi. Laitteet autoista leivänpaahtimiin on yhdistetty verkkoon. Datan analysointi tarjoaa myös kilpailuvaltin yrityksille. Kansainvälinen ICT-alan tutkimus- ja konsultointiyritys Gartner ennustaa, että suuret yritykset, jotka eivät investoi kattavasti datan analysoimiseen 2020 kevääseen mennessä, eivät välttämättä enää ole pystyssä vuonna 2021. (Foote 2020.)

7.2 Suomalaisten internetin käyttö 2019

Vuonna 2019 suomalaisista 79 % 16-89-vuotiaiden otannasta käytti internetiä useasti päivässä. Alle 45-vuotiaista lähes kaikki. Internetiä käytti useasti päivässä 65-74-vuotiaista 57 % ja 75-89-vuotiaista 23 %. Ylipäätään internetin käyttäjien osuus koko 16-89-vuotiaasta väestöstä oli 90 prosenttia. Nämä luvut sisältävät internetin yksityiskäytön, sekä töissä ja opiskelussa käytön. (Tilastokeskus 2019.) Suomalaiset käyttävät internetiä eniten matkapuhelimillaan, joka on edelleen kasvava trendi. Yhdysvalloissa tehdyn tutkimuksen

mukaan vuosina 1980-2000 syntyneistä joka viides ei käytä internetiä enää lainkaan tietokoneella. (Ilmarinen & Koskela 2015.)

Tilastokeskuksen mukaan internetiä käytetään asioiden hoitamiseen, medioiden seuraamiseen ja viestintään. Yleisintä asioinnista on verkkopankin käyttö. Vuonna 2019 oli verkkopankkia viimeisen kolmen kuukauden aikana käyttänyt 85 prosenttia 16-89-vuotiaista. Internetistä palveluita ja tavaroita oli ostanut viimeisen kolmen kuukauden aikana joka toinen suomalainen. (Tilastokeskus 2019.)

7.3 Mitä tietoa kerätään?

Tietoa kerätään kun kolmannen osapuolen sovellus (*software*) on syötetty sisälle verkkosivuihin ja applikaatioihin. Sovellukset keräävät tietoa käyttäjän yhteystiedoista, preferenseistä, aktiivisuudesta sosiaalisen median alustoilla, sekä myös päivittäistä tavoista käyttää laitetta. Näistä voidaan muodostaa profiileja, joihin on koottu tietoa ekonomisesta tilasta, elämäntyylistä, selaustavoista, puhelimen tilasta (käyttöjärjestelmä ja akun taso), terveystiedoista, sekä esimerkiksi askelmittarista. Tietoa kerätään aina kun selataan internetiä, käytetään puhelinta, siirretään rahaa tai liikutaan missä tahansa. Monet yhtiöt, kuten Facebook perustelevat tiedon keräämistä sillä, että sitä käytetään heidän palveluidensa muokkaamiseksi paremmaksi ja käyttäjäystävällisemmäksi. (Forbrukerrådet 2020; 21-22, 50-51.) Ongelmaksi muodostuu, jos kuluttaja ei saa tarpeeksi tietoa, tai voi valita sitä, saako häntä seurata ja profiloida. EU:n uusi tietosuoja-asetus vaatii laajan suostumuksen henkilötietojen käytön sallimiseen. Jos haluaa varmistua, ettei tietoja todella kerätä, saattaa ainoa keino usein olla, ettei lataa applikaatiota ollenkaan. (Forbrukerrådet 2020, 8.)

7.4 Käyttäjätunnukset helpottavat profilointia

Käyttäjän pitää usein kirjautua Applen palveluun, Googleen tai Amazoniin, jotta voi ottaa laitteensa kaikki ominaisuudet kokonaisvaltaisesti käyttöönsä. Tämä linkittää laitteen käyttäjään ja näin tehtyään yritysten on helpompi profiloida henkilön käyttäytymistä. Esimerkiksi, jos haluaa tallentaa koti- ja työosoitteensa Google Mapsiin, käyttäjän täytyy laittaa päälle Googlen WEB- ja APP-seuranta, joka antaa Googlelle luvan käyttää sijaintia, hakuhistoriaa ja app-aktiviteettia. Tämä tarkoittaa, että käyttäjälle voidaan tällöin näyttää kohdistettua mainontaa. (Cyphers 2019.)

Erilaisia profiileja muodostetaan myös yhdistelemällä tietoja, ilman erillistä käyttäjätunnuksen luomista. Esimerkiksi Adobe käyttää ID-synkronointia yhdistämään useita yksilöllisiä tunnisteita (*identifier, ID*) samaan henkilöön. ID:n täsmätessä toiseen palveluun yhdistet-

tyyn tunnettuun ID:seen, ne synkronoidaan keskenään. Esimerkiksi, jos toisella sivulla vierailija on ID123, toisella alustalla vierailija tunnetaan ID321. Adobe yhdistää tällöin keskenään nämä ID:t synkronointiprosessissa. Tämä lisää kokonaisdataa yhdestä kävijästä. (Forbrukerrådet 2019, 27.)

7.5 Kohdennettu mainonta

Mainontateknologian tavanomainen kaava on seuraavanlainen: asiakkaan käyttäytymistä seurataan, tästä kerätty data pilkotaan, kategorisoidaan ja käsitellään, ja lopuksi segmentoitu data lähetetään mainospalvelimelle, joka näyttää käyttäjälle sopivia mainoksia ja muuta sisältöä. Käyttäjän reaktiota mainoksiin seurataan, ja mainoskampanja mukautuu puolestaan tästä saatuun dataan.

Kohdennetun mainonnan estämiseen on esimerkiksi älylaitteiden asetusvalikoissa oma valintapainikkeensa. Tietosuoja-asetukseen nojaten datan suojaus tulisi olla aina valmiiksi asetettu sellaiseksi, ettei sitä oletusarvoisesti kerättäisi, vaan käyttäjä antaisi luvan itse. Älylaitteissa valintapainike on poikkeuksetta oletusasetettuna niin, että laite kerää dataa. (Forbrukerrådet 2019, 31-34.)

7.6 Datan keräämisen uhkat

Yritykset perustelevat datan keräämisen hyötyjä sillä, että näin saadaan luotua kuluttajille parempia palveluita. Tiedon olemassa oleminen ylipätään, profilointi ja automaattinen päätöksenteko voivat kuitenkin aiheuttaa myös ongelmia. Dataa kerätään kaikkialta mistä sitä saadaan irti; seurataan yhteystietoja, preferenssejä, tykkäyksiä ja päivittäisiä tapoja käyttää laitteita. Tätä tietoa käytetään palveluiden muokkaamiseksi paremmaksi ja käyttäjäystävällisemmäksi, mutta sitä voidaan käyttää myös epäeettisesti ja haitallisesti.

7.6.1 Syrjintä

Dataa voidaan käyttää negatiivisesti yksilöitä ja henkilöryhmiä kohtaan. Henkilöltä voidaan datan perusteella evätä tietyt palvelut kokonaan, tai hän voi saada kalliimmat hinnat tietylle palvelulle tai tuotteelle kerätyn datan perusteella. Datan pohjalta voidaan olla myös näyttämättä tiettyjä tarjouksia tai viestejä. Pahimmillaan tiettyjen sivustojen näyttäminen tai poisjättäminen henkilön internethauista voi estää keräämästä puolueetonta tietoa internetistä. Vaarallisimmillaan syrjinnän kohteeksi joutuu rodun, seksuaalinen suuntautumisen ja uskonnon perusteella. Alustojen algoritmit saattavat itse vahingossa luoda tämänlaisia estoja. Algoritmi voi konkreettisesti estää näkemästä esimerkiksi työ- tai asuntotarjouksia. Yhtenä esimerkkinä tiedon keräämisen erikoisistakin lähteistä, Intiassa lainahakemuksen

myöntäminen, tai myöntämättä jättäminen päätettiin puhelimeen asennettavan musiikkiapplikaation avulla kerätyn tiedon kautta. Käyttäjä ei tiennyt tästä, joten ei voinut protestoida tai suojella mitenkään itseään. (Forbrukerrådet 2019, 49.)

7.6.2 Tietojen joutuminen vääriin käsiin

Digitalisaation myötä yksityiskohtaista tietoa on mahdollista kerätä niin paljon yhdestä henkilöstä, että näiden tietojen joutuessa vääriin käsiin muodostuu realistisiksi uhkakuviksi identiteettivarkaus ja tiedolla kiristys. Mitä suuremmalla määrällä eri tahoja on pääsy tietoihin, sitä suurempi on riski ja todennäköisyys, että jotain haitallista tapahtuu.

7.7 Sijaintitiedot

Sijaintitietoja kerätään älylaitteista ja datan keräämiselle on monia keinoja. Sijaintitietoja saadaan GPS-vastaanottimesta, wi-fi-yhteyspisteistä, bluetoothin käytöstä ja matkapuhelinverkon tukiasemien avulla. Kun esimerkiksi tukiasemaa käytetään datan keräämiseen, ei puhelimen gps-paikannuksen tarvitse olla edes asetettuna aktiiviseksi. EU:n tietosuoja-asetuksen mukaan tiedon keräämiselle täytyy olla aina perusteet. On kyseenalaista, miksi kuvanmuokkaukseen tai kuukautiskiertoon liittyvät sovellukset vaatisivat käyttäjän jakamaan niille sijaintitietojaan, koska tieto ei liity mitenkään näiden sovellusten toimivuuteen. Seuranhakusovelluksissa puolestaan käyttäjät löytävät toisensa sijaintinsa perusteella, jolloin sijaintitiedon kerääminen on perusteltua. (Forbrukerrådet 2019, 83.)

Suhteellisen harmittomilta kuulostavista sijaintitiedoista voidaan päätellä yksityiskohtaisiakin tapahtumia yksilön elämässä. Tiedoista voidaan selvittää käynnit esimerkiksi sairaalassa tai yökerhossa. Tämän perusteella voitaisiin myös melko vaivattomasti tehdä mustavalkoisia päätelmiä esimerkiksi henkilön uskonnollisesta näkemyksestä kirkossa käynnin perusteella, seksuaalisesta suuntautumisesta homobaarissa käymisen perusteella, tai vaikka poliittisesta näkemyksestä tutkimalla sitä, käykö henkilö mielenosoituksissa. (Forbrukerrådet 2019, 82.)

8 Googlen ja Facebookin valta-asema

Amnesty vetoaa, että Googlen ja Facebookin bisnesmalli ja datan kerääminen on uhka ihmisoikeuksille. Google ja Facebook kontrolloi suurinta osaa palveluista internetissä. Googlen ja Facebookin suurin osa voitoista tulee mainostamisesta (yli 80 %), sekä Google ja Facebook yhdistettynä muodostavat yli 60 % online-mainosten tuloista maailmanlaajuisesti. Facebook hallitsee sosiaalista mediaa ja pikaviestimiä omistamalla muun muassa Instagramin ja WhatsAppin. Internethauista 90 % tehdään Googlen omistamalla hakukoneella. Sana ”googlata” on jopa vakiintunut nykykielessä tarkoittamaan tiedon hakemista internetistä. Google omistaa myös YouTuben, joka on puolestaan sekä toisiksi suurin hakukone maailmassa, että maailman laajin videoalusta. Lisäksi Google Chrome on käytetyin selain maailmassa. Google-pohjainen Android on maailman suosituin puhelinkäyttöjärjestelmä ja näin ollen yli 2.5 miljardia Android-laitetta on aktiivisena kuukausittain. (Amnesty International 2019, 11.)

Google otti viimeisen askeleensa Amnestyn mukaan ”tarkkailupohjaiseen” palveluunsa, kun se vaihtoi yksityisyydensuojasopimuksensa hyväksymään yhdistämään dataa sen mainosverkoston DoubleClickin kautta omaan dataansa kaikilta muilta alustoilta. Tämä tarkoittaa, että se voi kohdentaa rekisteröidylle suoraan mainontaa, joka pohjautuu todella tarkkaan yksityistietoon. Facebook otti saman askeleen jo vuonna 2014 kun se alkoi kerätä selausdataa kohdennettua mainontaa varten. (Amnesty International 2019, 41.)

8.1 Googlen sijainnin seuranta

Google kerää käyttäjän sijaintihistoriaa kun sijaintitietojen tallentaminen on kytketty päälle sekä Google-tilin asetuksissa, että laitteessa, ja käyttäjä on kirjautunut Google-tililleen. Sijaintihistorian keräämistä perustellaan sillä, että se parantaa käyttökokemusta Googlen tuotteissa ja palveluissa. Käyttäjä saa personoituja karttoja ja käyntikohteisiinsa liittyviä suosituksia, sekä esimerkiksi reaaliaikaista tietoa työmatkan liikenteen tilanteesta. Googlen sijaintihistoria on oletusarvoisesti pois käytöstä ja käyttäjä voi hallita pitkälti sen käyttöä. (Google 2020.) Tämä vastaa EU:n tietosuoja-asetuksen määräystä.

Australian kilpailu- ja kuluttajaviraston (ACCC) mukaan Google toimi kyseenalaisesti vuoden 2017 tammikuusta lähtien. Sen mukaan Google johti kuluttajaa harhaan kun se keräsi hyvin arkaluontoista ja yksityistä käyttäjädataa informoimatta tästä käyttäjää selkeästi. Googlella on kaksi sijaintidataa keräävää ominaisuutta; sijaintihistoria, sekä verkko- ja sovellusaktiivisuus. Molemmat toiminnot tulee olla kytkettynä pois päältä, jotta sijaintidataa ei kerätä. ACCC:n mukaan käyttäjä saattoi helposti luulla, että sijaintihistoriaominaisuuden pois kytkeminen riitti tietojen keräämisen estämiseksi. (ACCC 2019.)

Verkko- ja sovellustoiminta kerää tietoa puolestaan käyttäjän tekemistä hauista ja toiminnasta Google-palveluissa. Jos asetus on kytketty päälle, käyttäjä saa yrityksen mukaan esimerkiksi hyödyllisempiä sovellus- ja sisältösuosituksia. Kun asetus on päällä, toiminto kerää sijaintidataa sovellusten kautta. Tällöin esimerkiksi käyttäessään Googlen karttasovellusta määränpäähän mentäessä, Google tallentaa sovelluksen kautta käyttäjän sijaintidatan, vaikka laitteen sijaintihistorian tallennus olisi kytketty pois päältä. (ACCC 2019.)

Google tarjoaa nykyisin palvelun, että se poistaa kaiken historian ja aktiviteetin 3-18 kuukauden välein lokistaan. Käyttäjä saa itse valita haluamansa aikarajan tietojensa tuhoamiseen. Käyttäjän pitää kuitenkin käydä itse aktivoimassa palvelu. (Bader 2019.)

8.2 Googlen laitteet

Vuoden 2019 alussa Googlen Smart Home -malliston laitteessa oli mikrofoni, josta yhtiö ei ollut ilmoittanut yleisölle. Laitteen mikrofoniominaisuus paljastui, kun Google kertoi, että ääniaputoiminnot tulevat päivityksen mukana laitteeseen. Mikrofonia ei oltu koskaan aiemmin listattu laitteen ominaisuuksiin. Googlen mukaan kertomatta jättäminen oli vahinko, eikä tietoa oltu tahallisesti salattu. Google kertoi, että mikrofonia ei aktivoitu kuin vasta kunnes käyttäjä nimenomaisesti laittoi ominaisuuden päälle. Mikrofonia perusteltiin laitteen tarjoamana kotiin ja asumiseen liittyvänä turvatoimintona. Todellisuudessa mikrofoni oli ollut näissä kodin älylaitteissa sisäänrakennettuna vuodesta 2017 saakka. (Ng & Wollerton 2019.)

8.3 Project Atlas

Project Atlas (tai Facebook research) oli sovellus, jonka käyttämisestä maksettiin palkkioita nuorille henkilöille siitä, että se mahdollisti heidän päivittäisen puhelimen käyttönsä seuraamisen. Sovelluksen takana oli Facebook, joka toisin sanoen maksoi teineille että he ”ilmiantoivat” kaiken itsestään. Sovellusta markkinoitiin Instagramissa ja Snapchatissa näytettävien mainosten avulla. Näiden sosiaalisen medioiden alustojen perusteella sillä ei ollut laajaa liittyvyyttä niinkään itse Facebookiin. Sovellusta alettiin markkinoida vuonna 2016. Kun sovelluksen latasi, Facebook sai haltuunsa kaiken mitä puhelimella tehtiin, sisältäen yksityisviestit sosiaalisen median alustoilla, puhelimeen tallennetut videot ja kuvat, sähköpostit, selainhaut, internetin selaustilastot ja jatkuvasti lokaatiodataa. Sovellus oli tarkoitettu 13–35 vuotiaille, mutta Instagramissa ja Snapchatissa näytetyt mainokset oli kohdistettu pääosin nuoremman ääripään joukolle; 13–17-vuotiaille. Rekisteröintisivu ei maininnut sanaakaan Facebookista. Lapset saivat 20 dollaria kuukaudessa, jos sovellusta

käytettiin säännöllisesti, sekä 20 dollaria palkkiona uusien käyttäjien rekrytoinnista. Palkkioita ei maksettu rahana, vaan erilaisina lahjakortteina. Nuoren käyttäjäryhmän datan kerääminen on ollut Facebookin tähtäimessä, koska tämä ryhmä käyttää kilpailijoiden sovelluksia kuten TikTokia ja Snapchatia, joita Facebook ei omista. Tällä kyseenomaisella sovelluksella kerätty informaatio on voinut vaikuttaa siihen, että Facebook kopioi kilpailijaltaan Snapchatilta omistamaansa Instagramiin menestyksekkään *Stories*-ominaisuuden. (Constine 2019.)

8.4 Cambridge Analytica -skandaali

Cambridge Analytica oli datayhtiö, joka toimi Yhdysvaltain presidentin Donald Trumpin vaalikampanjassa vuonna 2014. Yhtiö kehitti sovelluksen nimeltä ”This is Your Digital Life”. Sovelluksessa Facebook-käyttäjä suoritti persoonallisuustestin ja hänelle kerrottiin, että tiedot menevät akateemiseen tarkoitukseen. Sovellus keräsi tietoa myös käyttäjän Facebook-kavereista, jolloin tietoa kerättiin suurelta verkostolta. Näitä tietoja käytettiin hyväksi, kun tehtiin ennustuksia ja haluttiin vaikuttaa äänestäjiin muun muassa Yhdysvaltain presidentinvaaleissa 2016. (Cadwalladr & Graham-Harrison 2018.)

Cambridge Analytica oli käyttänyt jopa 87 miljoonaa Facebook-profiilia luvatta muun muassa Trumpin kampanjan edistämiseksi. The Guardian julkaisi vuonna 2015 Cambridge Analyticasta jutun. Sen mukaan yritys hyödynsi Facebook-tiedoista koottuja ”psykologisia profiileja” Yhdysvaltain republikaanien presidenttiehdokkaan kampanjassa. Facebook ymmärsi Cambridge Analytican rikkoneen käyttäjäehtojaan, mutta ei kertonut tästä julkisesti. Facebook edellytti datayhtiötä tuhoamaan keräämänsä miljoonat profiilitiedot. Se ei kuitenkaan varmistanut, että toimenpiteisiin ryhdyttiin, joten tietoja hyödynnettiin vielä tämän jälkeen. (Rigatelli 2019.)

Vuonna 2018 väärinkäytökset nousivat mediaan ja Cambridge Analytican toimitusjohtaja irtisanottiin, koko yrityksen toiminta lopetetiin ja Facebookin toimitusjohtaja Mark Zuckerberg pyysi anteeksi ja häntä kuultiin Yhdysvaltain kongressissa, sekä EU-parlamentissa. Facebookin tuli selvittää paljonko käyttäjädataa oli levinnyt kolmansille osapuolille. Vuoteen 2019 mennessä mahdollisia väärinkäytöksiä oli löytynyt noin 10 000 sovelluksesta. Facebook sai kesällä 2019 yli viiden miljardin dollarin sakot käyttäjien yksityisyydensuojan loukkaamisesta. (Rigatelli 2019.)

8.5 Lobbaaminen

Facebook ja Google eivät tukeneet EU:n tietosuoja-asetusta. Vuonna 2016 Facebook katsoi, että toimiala ei olisi tarvinnut kehittyäkseen lakimuutosta ja sen tuomaa painostusta.

Facebookin perusteluina oli, että tiukempi laki saattaisi tukahduttaa toimialaa. (Kayali 2019.)

Lobbaaminen on normaali käytäntö kun tehdään lakeja, mutta tässä tapauksessa Facebookin ja EU:n filosofisen näkemyksen välissä oli suuret eettiset eroavaisuudet. Facebookin ja Euroopan komission väliset jännitteet alkoivat vuonna 2016, kun laadittiin ohjesääntöjä internetissä tapahtuvan vihapuheen ehkäisemiseksi. Facebook olisi toivonut voivansa toimia omien käyttöehtojensa näkökulmasta, eikä olla Euroopan unionin lain velvoittama tässä suhteessa. Facebook ja Euroopan komissio päätyivät asian suhteen kompromissiin 2016 toukokuussa, jolloin päätettiin, että toimenpiteissä vihapuhetta vastaan otettaisiin huomioon yhteisön ohjesäännöt sekä kansallinen laki. Facebookin mukaan heidän ohjeidensa painottaminen asiassa lain ohitse mahdollistaisi nopeampiin toimenpiteisiin. Euroopan komissio on tehnyt lakialoitteen siitä, että terrorismiin liittyvä propaganda tulee poistaa alustoilta tunnin sisällä kun se on raportoitu epäsopivaksi sisällöksi, koska tässä asiassa ei voida luottaa ainoastaan yritysten itsesäätelyyn. (Kayali 2019.)

E-Privacyyn liittyvä sääntely esiteltiin Euroopan komission toimesta vuonna 2017. Vaatimus tästä sääntelystä on noussut Euroopan komission mukaan Euroopan kansalaisilta, sillä he kokevat, että esimerkiksi sähköpostien ja pikaviestimien yksityisyyden ja suojauksen tulee olla taattu. (Kayali 2019.) E-Privacy -asetus tulee täydentämään EU:n tietosuoja-asetusta ja se muuttaa evästeiden käyttöä, sähköistä suoramarkkinointia ja mainosten kohdentamista. Se toisi viestintäpalvelimet kuten WhatsAppin, Facebook Messengerin ja Skypen samalle linjalle perinteisten teleoperaattorien kanssa ja näiden kaikkien palvelinten yksityisyydensuojaus tulisi taata samalla tavalla. (Koulutus.fi 2019.) E-Privacy aiheutti vastalauseiden syntymistä muun muassa Facebookilta, Googlelta, Eurooppalaisilta mediayhtiöiltä, tietoliikenneyhtiöiltä ja mainostajilta. (Kayali 2019.)

9 Tietosuojaloukkauksia

Tässä luvussa käsitellään tapauksia globaalilla ja Suomen tasolla, joita ilmennyt Euroopan unionin tietosuoja-asetuksen astuttua voimaan vuonna 2018. Keskuskauppakamarin juridiikkakatsauksen mukaan Euroopan unionin alueella annettiin tietosuoja-asetusrikkeisiin liittyen yli 100 sakkoa vuonna 2019. (Keskuskauppakamari 2019.)

Elämme informaatioyhteiskunnassa, jossa henkilötietoja kerätään ja välitetään huomattavasti suuremmassa mittakaavassa kuin aiemmin. Vahinko voi olla fyysistä, aineellista, aineetonta, taloudellista tai sosiaalista. Henkilötietoihin kohdistuvasta tietoturvaloukkauksesta tehdään ilmoitus tietosuojavaltuutetulle ja tietyin edellytyksin rekisteröidylle yksilölle. (Andreasson ym. 2019, 171-172.)

Kun organisaation vastuulla olevien tietojen salassapito, saatavuus tai eheys vaarantuvat, on kyse tietoturvaloukkauksesta. Tietoturvaloukkaus on tapahtuma, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, luovutetaan luvattomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta. Loukkauksesta voi seurata esimerkiksi identiteettivarkaus, petos, maineen vahingoittuminen, salassapitovelvollisuuden alaisten tietojen paljastuminen sivullisille, merkittävä taloudellinen vahinko tai sosiaalinen vahinko. (Andreasson ym. 2019, 171-172.)

9.1 Case Google

Ranskan tietosuojaviranomainen CNIL antoi vuonna 2019 Googlelle 50 miljoonan euron sakot Euroopan unionin tietosuoja-asetuksen rikkomisesta. Kyseessä oli ensimmäinen usean miljoonan euron sakko tietosuoja-asetukseen liittyen. (Laitila 2019.)

Sakkoa perusteltiin sillä, että Google ei ollut kertonut asiakkailleen riittävän selvästi mitä se tekee asiakkaidensa tiedoilla, miten kauan tietoa säilytetään ja mitä kaikkea tietoa yhtiö käyttää mainosten kohdentamiseen. Riittävän selvästi tarkoittaa tässä tapauksessa, että tieto on saatavilla, mutta Ranskan viranomaisten mukaan liian hankalasti löydettävissä ja puutteellista. EU:n tietosuoja-asetus vaatii tietojen esittämisen rekisteröidylle selkeästi ja kielellä, jota hänen on mahdollista ymmärtää. (Laitila 2019.)

Toinen peruste sakolle oli Googlen epämääräinen ja puutteellinen tapa pyytää käyttäjältä lupa tietojen käyttämiseen mainosten kohdentamisessa. Googlen käyttöehdoissa mainosten kohdentamisesta ei tuoda riittävän selvästi esille tietojen käytön laajuutta Googlen kaikissa eri palveluissa, kuten Youtubessa, hakukoneessa, kartoissa tai sovelluskaupassa.

Tämän vuoksi käyttäjältä saatua suostumusta tietojensa käyttöön ei voida pitää yksiselitteisenä tai selkeänä kuten EU:n yleinen tietoturva-asetus vaatii. (Laitila 2019.)

Ranskan tietosuojaviranomainen CNIL sai valituksen Googlesta ranskalaisilta digitaalisia oikeuksia ajavilta ryhmiltä. Pelkkä ilmoitus lainmukaisuudesta ei heidän mukaansa riitä, vaan EU:n tietosuoja-asetuksessa painotetaan juurikin osoitusvelvollisuutta. Nämä ryhmät ovat myös tehneet vastaavia valituksia Instagramin, Whatsappin ja Facebookin toiminnasta, joiden käsittelyt ovat vielä kesken. (Laitila 2019.)

9.2 Case British Airways

Iso-Britannialainen lentoyhtiö British Airways sai Iso-Britannian tietosuojaviranomaiselta ICOlta vuonna 2019 yli 204 miljoonan euron sakot toimimisesta EU:n tietosuoja-asetuksen vastaisesti. Summa vastasi 1,5 prosenttia British Airwaysin maailmanlaajuisesta liikevaihdosta vuonna 2017. Vertailukohteena Facebook sai aiemmin mainitun Cambridge Analytica -skandaalin johdosta maksimirangaistuksena miltei 600 000 euron sakot, kun EU:n uusi tietosuoja-asetus ei ollut vielä voimassa. EU:n uuden tietosuoja-asetuksen nojalla suurin sakotettava summa on neljä prosenttia yhtiön vuotuisesta liikevaihdosta. (BBC 2019; Konttinen 2019.)

Vuonna 2018 noin 500 000:n British Airwaysin asiakkaan tiedot päätyivät vääriin käsiin tietomurrossa, kun käyttäjä harhautettiin lentoyhtiön nimissä väärennetylle sivustolle. ICO perustelee sakkoa sillä, että British Airwaysn turvajärjestelmät eivät olleet riittävän kattavat. Hakkeri sai varastettua asiakkaiden nimet, sähköpostiosoitteet ja täydet luottokorttitiedot, sekä niiden turvaluvut. British Airways teki tapauksen tutkinnassa yhteistyötä ICOn kanssa parantaakseen turvajärjestelmiään. British Airways oli yhteydessä asiakkaisiinsa kesällä vuonna 2018 ja kertoi, että osoitteita ja sähköpostiosoitteita oli vuotanut. He informoivat myöhemmin, että luottokorttitiedot olivat myös altistuneet datavuodolle. (BBC 2019; Konttinen 2019.)

9.3 Case POP Pankki

Apulaistietosuojavaltuutettu antoi POP Pankille vuoden 2020 alussa huomautuksen, joka liittyi keväällä 2019 tapahtuneeseen tietoturvaloukkaukseen. Huomautukseen johti se, että pankki antoi verkkosivuillaan ja Facebook-sivuillaan puutteellista tietoa siitä, oliko se informoinut kaikkia tietoturvaloukkauksen kohteeksi joutuneita asiakkaitaan henkilökohtaisesti vai ei. (Tietosuojavaltuutetun toimisto 2020.)

Tietoturvaloukkauksessa oli kyse POP Pankin käyttämistä sähköisistä lomakkeista, joiden sisältämiin tietoihin oli liian laaja pääsy ulkopuolisella verkkopalveluita ylläpitävällä osapuolella. Kun tietoturvaloukkaus tuli ilmi, pankki muutti lomakkeitaan niin, etteivät niiden sisältämät henkilötiedot tallennu tietokantaan. POP Pankki varmisti, että aiemmin lomakkeille tallennetut tiedot ovat jatkossa vain pankin hallussa. (Tietosuojavaltuutetun toimisto 2020.)

Tietoturvaloukkauksen jälkeen POP Pankki otti yhteyttä osaan tietoturvaloukkauksen kohteeksi joutuneista henkilöistä. Pankilla ei ollut käytössä kaikkien tietoturvaloukkauksen kohteeksi joutuneiden riittävän kattavia yhteystietoja, joten se julkaisi julkisen tiedonannon loukkauksesta verkkosivuillaan ja yrityksen Facebook-sivuilla. Tiedonannoista saattoi saada käsityksen, että kaikkiin tietoturvaloukkauksen kohteeksi joutuneista oli oltu yhteydessä henkilökohtaisesti, vaikka näin ei ollut. Apulaistietosuojavaltuutetun mukaan pankin kanssa asioineet saattoivat perustellusti uskoa ja ymmärtää, että tietoturvaloukkaus ei koskenut heitä, jos siitä ei ollut saanut henkilökohtaista ilmoitusta. (Tietosuojavaltuutetun toimisto 2020.)

9.4 Case Finnkino

Apulaistietosuojavaltuutettu määräsi vuonna 2019 Finnkino Oy:n muuttamaan tietosuojakäytäntöjään. Finnkino oli toiminut suhteessa EU:n tietosuoja-asetukseen virheellisesti ja nämä toimintatavat koskivat asiakkaiden tietosuojaoikeuksien toteutumista ja sähköistä suoramarkkinointia. Tietosuojavaltuutetun toimistossa oli käsiteltävänä 40 Finnkinoa koskevaa asiaa. (Tietosuojavaltuutetun toimisto 2019b.)

Apulaistietosuojavaltuutettu antoi Finnkinolle huomautuksen pakotetusta suostumuksesta sähköiseen suoramarkkinointiin. Kun asiakas halusi ostaa Finnkinon e-sarjalippuja tai varata lippuja verkossa, hänen täytyi liittyä Finnkino Lab -asiakasohjelmaan ja suostua vastaanottamaan suoramarkkinointia. Asiakasohjelmaan ei voinut liittyä rastittamatta ruutua, joka ilmaisi suostumuksen suoramarkkinointiin. Tämä toimintatapa ei täytä EU:n tietosuoja-asetuksen vaatimuksia vapaaehtoisesta suostumuksesta henkilötietojen käsittelyn perusteena. Näin ollen Finnkino ei myöskään toteuttanut rekisteröidyn oikeutta vastustaa henkilötietojen käsittelyä. Tietosuojalainsäädännön perusteella rekisteröity voi milloin tahansa vastustaa henkilötietojensa käsittelyä suoramarkkinointia varten. Rekisteröidyn täytyy voida vastustaa tietojensa käsittelyä jo silloin, kun hänen henkilötietojaan kerätään. Se ei riitä käytännöksi, että asiakas voi myöhemmin pyytää yritystä lopettamaan sähköisen suoramarkkinoinnin. (Tietosuojavaltuutetun toimisto 2019b.)

Apulaistietosuojavaltuutettu antoi myös huomautuksen rekisteröidyn tunnistamiseen liittyvistä toimintatavoista, jotka aiheuttivat asiakkaalle kohtuutonta vaivaa. Finnkino vaati asiakasta lähettämään kuvan passista tai henkilökortin molemmista puolista tunnistamista varten. Lisäksi Finnkino vaati tunnistamiseen valokuvaa henkilön kasvoista henkilöllisyystodistuksen vieressä. Tässä tapauksessa Finnkino on vaatinut enemmän tietoa tunnistamista varten, kuin mitä sillä on alun perin ollut. (Tietosuojavaltuutetun toimisto 2019b.)

Finnkino sai myös huomautuksen siitä, että se ei kertonut puheluiden nauhoittamisesta asiakkaalleen. Tätä käytäntöä Finnkino kuitenkin muutti jo ennen apulaistietosuojavaltuutetun huomautusta. (Tietosuojavaltuutetun toimisto 2019b.)

Koska oikeustila on ollut yleisen tietosuoja-asetuksen soveltamisen alettua epäselvä, apulaistietosuojavaltuutettu katsoi, etteivät Finnkinon aiemmat käytänteet edellyttäneet huomautusta raskaampaa seuraamusta. Päätökseen vaikutti myös se, että Finnkino alkoi oma-aloitteisesti toimenpiteisiin EU:n tietosuoja-asetuksen noudattamiseksi saamansa palautteen perusteella. (Tietosuojavaltuutetun toimisto 2019b.)

10 Lopuksi

EU:n tietoturva-asetuksen noudattaminen on tänä päivänä kaikkien organisaation työntekijöiden vastuulla. Johdon assistentin näkökulmasta työn siirtyessä yhä enemmän laitteille ja verkkoon, tulee työssä noudattaa erityistä huolellisuutta käsitellessä kaikkea tietoa ja kiinnittää huomiota erilaisiin tietopyyntöihin. Johdon assistentti työskentelee usein viestin välittäjänä ja ”liimana” työpaikan eri prosessien ja yksiköiden välissä. Tästä johtuen johdon assistentilla saattaa olla pääsy useisiin tietokantoihin työn sujuvoittaviseksi, joten tiedon käsittelyssä tulee noudattaa erityistä huolellisuutta.

Päätoimisia tietosuojavastaavia on vielä hyvin harvassa organisaatiossa. Tietosuojavastaavan työtä tehdään siis oman muun varsinaisen työn ohessa ja tämä asettaa tietyt haasteet tietosuojatyön tekemiselle. Kun tietosuojatyön tekemisessä huolehditaan yhteistyöstä ja verkostoista, alkaa hiljalleen syntyä yhdenmukaisia tulkintoja, maan tapoja ja käytännesääntöjä. Nämä tulevat helpottamaan tietosuojatyötä tulevaisuudessa. (Andreasson ym. 2019, 199-201.)

Tietosuoja-asetusta tutkiessa ei voi olla miettimättä henkilötietodatan keräämiseen liittyviä eettisiä piirteitä. Tietoa voidaan tahallisesti tai algoritmien puutteellisuuden vuoksi käyttää epäeettisesti esimerkiksi syrjintään tai ostopäätösten manipuloimiseen. Digitalisaatio menee eteenpäin nopeasti jatkuvaa vauhtiaan ja tästä syystä ensinnäkin organisaatioiden on hyödynnettävä ilmiötä, mutta yksilön on myös pysyttävä kaiken perässä osatakseen pitää huolen omista oikeuksistaan.

Opinnäytetyön perusteella Euroopan unionin tietosuoja-asetus on jo onnistunut muovaamaan konkreettisia rajoja ja toimintatapoja sille, miten tavallisen kansalaisen henkilötietoja lopulta saa hyödyntää organisaatioiden toiminnassa. Lisäksi asetus on tuonut rekisteröidylle näkyvästi lisää oikeuksia, joiden laiminlyömiseen reagoidaan asian vaatimalla mittakaavalla. Rekisteröidyn tiedot tulee suojata organisaatiossa paremmin jo tietoturvasta lähtien kun järjestelmiä luodaan, sekä suoja automaattisesti paranee, kun ylimääräiset välikädet tietojen käsittelyssä poistetaan.

10.1 Opinnäytetyöprosessi

Koska opinnäytetyöllä ei ollut varsinaista toimeksiantajaa ja työn lähtökohtana oli hankkia tietoa tutkimuksen alla olevaan kysymykseen lähinnä omasta itsestä kumpuavasta motivaatiosta, toi se työn tekemiselle omat hyvät ja huonot puolensa. Päädyin opinnäytetyön teemaan syventävien juridiikan ja big data -kurssien perusteella ja aihe varmistui syksyllä 2019. Koska organisaatioiden henkilötietojen käsittelyyn liittyvät muutokset oli jo tehty lain

voimaan astumisen myötä, täytyi kysymyksen asettelu suunnata tulevaisuuteen. Digitalisaation teema on hyvin laaja ja tieto myös vanhenee suhteellisen nopeasti. Tämän takia rajasin työtä siten, että tietosuojalainsäädännön osuus on esitelty yleisellä tasolla ja dataa, sekä henkilötietoja käsittelevässä osuudessa tarkastellaan lähempää kahta datayhtiöjättiä, jotka ovat näkyvästi koko ilmiön keskellä ja niiden toiminta myös koskettaa todennäköisesti suurinta osaa tämän opinnäytetyön lukijoista.

Opinnäytetyön kirjoittaminen alkoi kevätlukukaudella 2020. Suurin osa työstä oli valmistunut ennen kuin koulut suljettiin pandemian takia, mutta uuteen työrutiiniin tuli asennoitua ja luoda lopulle työlle kokonaan uusi aikataulutus. Koin, että ohjaustapaamisista oli erityisen paljon hyötyä; ne antoivat vertaistukea ja interaktio ylipäätään motivoi pysymään aikataulussa.

Työtä oli aiheen puolesta mieluisaa tehdä ja lopputulos on loogisesti etenevä dokumentaatio. Jos opinnäytetyön olisi tehnyt vuosikin myöhemmin, se olisi varmaan jo erilainen, koska digitalisaation maailmassa asiat etenevät niin hurjaa tahtia. Kamppailu on sen välillä on kovaa, miten henkilötietoja voidaan hyödyntää mahdollisimman eettisesti ja milloin tietojen käsittely on kyseenalaista. Toisaalta on helppo ymmärtää organisaatioiden näkökulmaa, kun uusia innovaatioita kehitetään ja datan avulla saatava hyöty halutaan maksimoida. Opinnäytetyössä esitellyissä neljässä tietosuojaloukkaustapauksessa huomaa, että koska uusi tietosuojalainsäädäntö on niin tuore ja suhteellisen abstrakti, täytyisi pienimmätkin yksityiskohdat ottaa huomioon, tai muuten niistä opitaan vasta kantapään kautta.

Lähteet

ACCC. 2019. Google allegedly misled consumers on collection and use of location data. Luettavissa: https://www.accc.gov.au/media-release/google-allegedly-misled-consumers-on-collection-and-use-of-location-data. Luettu: 16.4.2020.

Amnesty International. 2019. SURVEILLANCE GIANTS: HOW THE BUSINESS MODEL OF GOOGLE AND FACEBOOK THREATENS HUMAN RIGHTS. Luettavissa: https://www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF. Luettu: 16.4.2020.

Andreasson, A.; Riikonen, J. & Ylipartanen, A. 2019. Osaava tietosuojavastaava. Tietosanoma Oy. Helsinki.

Bader, D. 2019. How to automatically delete your Google Location and Web & App Activity. Androidcentral. Luettavissa: https://www.androidcentral.com/how-automatically-delete-your-google-location-and-web-app-activity. Luettu: 16.4.2020.

BBC. 2019. British Airways faces record £183m fine for data breach. Luettavissa: https://www.bbc.com/news/business-48905907. Luettu: 17.4.2020.

Cadwallad, C. & Graham-Harrison, E. 2018. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian. Luettavissa: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Luettu: 17.4.2020

Constine, J. 2019. Facebook pays teens to install VPN that spies on them. TechCrunch. Luettavissa: https://techcrunch.com/2019/01/29/facebook-project-atlas/. Luettu: 16.4.2020.

Cyphers, B. 2019. Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance. Electronic frontier foundation. Luettavissa: https://www.eff.org/wp/behind-the-one-way-mirror. Luettu: 16.4.2020.

EU:n neuvosto. 2019. Digitaalipolitiikka vuoden 2020 jälkeen – neuvostolta päätelmät. Luettavissa: https://www.consilium.europa.eu/fi/press/press-releases/2019/06/07/post-2020-digital-policy-council-adopts-conclusions/. Luettu: 15.4.2020.

Euroopan unionin perusoikeuskirja 2000/C 364/01.

Euroopan komissio a. Mitä tarkoittaa 'sisäänrakennettu' ja 'oletusarvoinen' tietosuoja? Luettavissa: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_fi. Luettu: 15.4.2020.

Euroopan komissio b. Mitä ovat tietosuojaviranomaiset?. Luettavissa: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_fi. Luettu: 15.4.2020.

Euroopan tietosuojaneuvosto. Tietoa Euroopan tietosuojaneuvostosta. Luettavissa: https://edpb.europa.eu/about-edpb/about-edpb_fi. Luettu: 15.4.2020.

Euroopan unioni. 2019. Asetukset, direktiivit ja muut säädökset. Luettavissa: https://europa.eu/european-union/eu-law/legal-acts_fi. Luettu: 15.4.2020.

Euroopan unioni. 2020. Euroopan tietosuojavaltuutettu. Luettavissa: https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor_fi. Luettu: 15.4.2020.

Foote, K. 2020. Big Data Trends in 2020. Luettavissa: https://www.dataversity.net/big-data-trends-in-2020/. Luettu: Luettu: 16.4.2020.

Forbrukerrådet. 2020. Out of control. How consumers are exploited by the online advertising industry. Luettavissa: https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf. Luettu: 17.4.2020.

Google. 2020. Sijaintihistorian ylläpito. Luettavissa: https://support.google.com/accounts/answer/3118687?hl=fi. Luettu: 16.4.2020.

Hämäläinen, V.; Maula, H. & Suominen, K. 2016. Digiajan strategia. Talentum Media Oy. Helsinki.

Ilmarinen, V. & Koskela, K. 2015. Digitalisaatio: Yritysjohdon käsikirja. Talentum Oyj.

Jian, Z.; Jones, S.; Tolido, R.; Hunt, G.; Budor, I.; Bartoli, E.; van der Linden, P.; Buvat, J.; Theisler, J.; Wortmann, A.; Cherian, S. & Khemka, Y. 2019. Championing data protection

and privacy – a source of competitive advantage in the digital century. Capgemini. Luettavissa: https://www.capgemini.com/wp-content/uploads/2019/09/Report_Championing-Data-Protection-and-Privacy.pdf. Luettu: 15.4.2020.

Järvelä, K. 2017. Näin anonymisoit kvalitatiivisen tutkimusaineistosi. Tietoarkistoblogi. Luettavissa: https://tietoarkistoblogi.blogspot.com/2017/04/kvalitatiivisissa-tutkimusaineistoissa.html. Luettu: 15.4.2020.

Kayali, L. 2019. Inside Facebook's fight against European regulation. Politico. Luettavissa: https://www.politico.eu/article/inside-story-facebook-fight-against-european-regulation/. Luettu: 17.4.2020.

Keskuskauppakamari. 2019. Suuri määrä tietosuojasakkoja EU-alueella – Keskuskauppakamari kehottaa yrityksiä kiinnittämään huomiota tietosuojakäytäntöihin. Luettavissa: https://kauppakamari.fi/2019/12/30/suuri-maara-tietosuojasakkoja-eu-alueella-keskuskauppakamari-kehottaa-yrityksia-kiinnittamaan-huomiota-tietosuojakaytantoihin/. Luettu: 17.4.2020.

Konttinen, E. 2019. Hakkeri vei satojen tuhansien asiakkaiden tiedot – lentoyhtiö sai yli 200 miljoonan sakot. Tivi. Luettavissa: https://www.tivi.fi/uutiset/hakkeri-vei-satojen-tuhansien-asiakkaiden-tiedot-lentoyhtio-sai-yli-200-miljoonan-sakot/0df98217-0905-4150-97b3-57b26fd485f5. Luettu: 17.4.2020.

Koulutus.fi. 2019. ePrivacy – mikä se on? Luettavissa: https://www.koulutus.fi/artikkelit/e-privacy-mika-se-on-15301. Luettu: 17.4.2020.

Laitila, T. 2019. Ranska läimäisi ensimmäisen kymmenien miljoonien gdpr-sakon – kyseenalainen kunnia osui Googlelle. Tivi. Luettavissa: https://www.tivi.fi/uutiset/ranska-laimaisi-ensimmaisen-kymmenien-miljoonien-gdpr-sakon-kyseenalainen-kunnia-osui-googlelle/c3250dca-3a1c-3b27-8008-313efdcb57c0. Luettu: 17.4.2020.

Maciejewski, M. & Gouardères, F. 2019. Euroopan digitaalistrategia. Luettavissa: https://www.europarl.europa.eu/ftu/pdf/fi/FTU_2.4.3.pdf. Luettu: 15.4.2020.

Maciejewski, M. & Ratcliff, C. 2019. Digitaaliset sisämarkkinat. Luettavissa: https://www.europarl.europa.eu/ftu/pdf/fi/FTU_2.1.7.pdf. Luettu: 15.4.2020.

Ng, A. & Wollerton, M. 2019.

Google calls Nest's hidden microphone an 'error'. Cnet. Luettavissa: https://www.cnet.com/news/google-calls-nests-hidden-microphone-an-error/. Luettu: 16.4.2020.

Oikeusministeriö. 2018. Uusi tietosuojalaki voimaan vuoden 2019 alusta. Luettavissa: https://oikeusministerio.fi/artikkeli/-/asset_publisher/uusi-tietosuojalaki-voimaan-vuoden-2019-alusta. Luettu: 15.4.2020.

OpiTietosuojaa.fi. 2020. Henkilötietojen käsittely ja rekisterinpito. Luettavissa: https://opi-tietosuojaa.fi/fi/aloitus/rekisterinpito/12-automaattisesti-generoitu-otsikosta. Luettu: 15.4.2020.

Rigatelli, S. 2019. Cambridge Analytica -skandaalin paljastanut toimittaja taistelee internetjättien piilovaikuttamista vastaan – "Facebook pitäisi kieltää vaaleissa". Yle. Luettavissa: https://yle.fi/uutiset/3-10996034. Luettu: 16.4.2020.

Suomen perustuslaki 11.6.1999/731.

Sovelto. 2020. Avain syvempään asiakasymmärrykseen. Luettavissa: https://www.sovelto.fi/ratkaisut/ict-ja-uudet-teknologiat/big-data/. Luettu: 17.4.2020.

Tarhonen L. 2017. Henkilötietojen pseudonymisointi – ai siis mikä? Luettavissa: https://www.iab.fi/iablogi/henkilotietojen-pseudonymisointi-ai-siis-mika.html. Luettu: 17.4.2020.

Taskinen, L. 2018. Tietosuojalain hallituksen esitystä on odotettu kuin kuuta nousevaa – ja nyt se on saatavilla. Tietosuojauutiset.fi. Luettavissa: https://tietosuojauutiset.fi/2018/03/02/tietosuojalain-hallituksen-esitysta-on-odotettu-kuin-kuuta-nousevaa-ja-nyt-se-on-saatavilla/. Luettu: 15.4.2020.

Tietosuojalaki 5.12.2018/1050.

Tietosuojavaltuutetun toimisto 2019a. Tietosuojavaltuutetun toimistolle on ilmoitettu jo 2700 henkilötietojen tietoturvaloukkausta. Luettavissa: https://tietosuoja.fi/artikkeli/-/asset_publisher/tietosuojavaltuutetun-toimistolle-on-ilmoitettu-jo-2700-henkilotietojen-tietoturvaloukkausta. Luettu: 16.4.2020.

Tietosuojavaltuutetun toimisto 2019b. Apulaistietosuojavaltuutettu antoi Finnkinolle huomautuksen ja määräyksen muuttaa henkilötietojen käsittelyn toimintatapoja. Luettavissa: https://tietosuoja.fi/artikkeli/-/asset_publisher/apulaistietosuojavaltuutettu-antoi-finnkinolle-huomautuksen-ja-maarayksen-muuttaa-henkilotietojen-kasittelyn-toimintatapoja. Luettu: 17.4.2020.

Tietosuojavaltuutetun toimisto 2020. POP Pankille huomautus puutteellisesta tiedotuksesta tietoturvaloukkauksen kohteeksi joutuneille. Luettavissa: https://tietosuoja.fi/artikkeli/-/asset_publisher/pop-pankille-huomautus-puutteellisesta-tiedotuksesta-tietoturvaloukkauksen-kohteeksi-joutuneille. Luettu: 17.4.2020.

Tietosuojavaltuutetun toimisto a. Tietosuoja. Luettavissa: https://tietosuoja.fi/tietosuoja. Luettu: 15.4.2020.

Tietosuojavaltuutetun toimisto b. Rekisterinpitäjän seloste käsittelytoimista. Luettavissa: https://tietosuoja.fi/rekisterinpitajan-seloste-kasittelytoimista. Luettu: 15.4.2020.

Tietosuojavaltuutetun toimisto c. Henkilötietojen käsittelijät. Luettavissa: https://tietosuoja.fi/henkilotietojen-kasittelijat. Luettu: 15.4.2020.

Tietosuojavaltuutetun toimisto d. Tietosuojavastaavat. Luettavissa: https://tietosuoja.fi/tietosuojavastaavat. Luettu: 15.4.2020.

Tietosuojavaltuutetun toimisto e. Tietosuojavaltuutetun toimisto. Luettavissa: https://tietosuoja.fi/tietosuojavaltuutetun-toimisto. Luettu: 15.4.2020.

Tietosuojavaltuutetun toimisto f. Ilmoitus tietosuojavaltuutetulle. Luettavissa: https://tietosuoja.fi/ilmoitus-tietosuojavaltuutetulle. Luettu: 15.4.2020.

Tietosuojavaltuutetun toimisto g. Automaattinen päätöksenteko ja profilointi. Luettavissa: https://tietosuoja.fi/automaattinen-paatoksenteko-profilointi. Luettu: 15.4.2020.

Tietosuojavaltuutetun toimisto h. Usein kysyttyä yhdistystoiminnasta. Luettavissa: https://tietosuoja.fi/usein-kysyttya-yhdistystoiminta. Luettu: 15.4.2020.

Tietosuojavaltuutetun toimisto i. Pseudonymisoidut ja anonymisoidut tiedot. Luettavissa: https://tietosuoja.fi/pseudonymisointi-anonymisointi. Luettu: 15.4.2020.

Tietosuojavaltuutetun toimisto j. Tunne oikeutesi. Luettavissa: https://tietosuoja.fi/tunne-oikeutesi. Luettu: 17.4.2020.

Tietosuojavaltuutetun toimisto k. Oletko joutunut automaattisen päätöksenteon kohteeksi? Luettavissa: https://tietosuoja.fi/oletko-joutunut-automaattisen-paatoksenteon-kohteeksi. Luettu: 17.4.2020.

Tietosuojavaltuutetun toimisto l. Kun haluat siirtää tietosi toiselle rekisterinpitäjälle. Luettavissa: https://tietosuoja.fi/kun-haluat-siirtaa-tietosi. Luettu: 17.4.2020.

Tietosuojavaltuutetun toimisto m. Henkilötietojen siirrot Euroopan talousalueen ulkopuolelle. Luettavissa: https://tietosuoja.fi/henkilotietojen-siirrot-etan-ulkopuolelle. Luettu: 15.4.2020.

Tietosuojavaltuutetun toimisto n. Siirto tietosuojan riittävyyttä koskevan päätöksen perusteella. Luettavissa: https://tietosuoja.fi/siirto-tietosuojan-riittavyytta-koskevan-paatoksen-perusteella. Luettu: 15.4.2020.

Tietosuojavaltuutetun toimisto o. Brexit ja henkilötietojen siirrot Isoon-Britanniaan Luettavissa: https://tietosuoja.fi/brexit. Luettu: 15.4.2020.

Tilastokeskus. 2019. Suomalaisten internetin käyttö 2019. Luettavissa: https://www.stat.fi/til/sutivi/2019/sutivi_2019_2019-11-07_kat_001_fi.html. Luettu: 16.4.2020.

Tivi. 2016. Tällainen on tietosuoja-asetus – jopa 20 miljoonan sakot uhkaavat rikkojia. Luettavissa: https://www.tivi.fi/Kaikki_uutiset/tallainen-on-tietosuoja-asetus-jopa-20-miljoonan-sakot-uhkaavat-rikkojia-6606546. Luettu: 16.4.2020.

Järvinen, P. & Rousku, K. 2017. Työpaikan tietoturvaopas – tunnista uhat, hallitse riskit. Alma Talent Oy.

Valtiovarainministeriö. 2010. Sosiaalisen median tietoturvaohje. Luettavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=8b44c0bf-cff3-4e6c-a587-eea58a9e3ad7&groupId=10229. Luettu: 7.5.2020.

Yleinen tietosuoja-asetus 679/2016/EU.