OULUN AMMATTIKORKEAKOULU

Milja Hakunti

YKSITYISYYDEN VÄHENEMINEN INTERNETISSÄ

YKSITYISYYDEN VÄHENEMINEN INTERNETISSÄ

Milja Hakunti
Opinnäytetyö
Kevät 2022
Tietojenkäsittelyn tutkinto-ohjelma
Oulun ammattikorkeakoulu

TIIVISTELMÄ

Oulun ammattikorkeakoulu
Tietojenkäsittelyn tutkinto-ohjelma

Tekijä: Milja Hakunti
Opinnäytetyön nimi: Yksityisyyden väheneminen internetissä
Työn ohjaaja: Minna Kamula
Työn valmistumislukukausi ja -vuosi: Kevät 2022 Sivumäärä: 38

Työn aiheena on yksityisyys internetissä ja miksi tämä on hiljalleen vähentynyt teknologian edistymisen ja digitalisoitumisen myötä. Tutkimuksessa käydään läpi aiheen historiaa jota hyödynnetään myös taustatietona. Lähteisiin kuuluu myös tutkimuksia, näiden tuloksia, sekä uutisointia liittyen internetin ja IoT laitteiden eri palveluiden tietosuojakäytäntöihin ja näiden rikkomuksiin. Tutkimuksessa käydään myös läpi tietoturvarikosten aihetta ja kuinka nämä ovat muuttuneet internetin laajenemisen myötä.
Tutkimuksen tulokset osoittavat, että suurin tekijä yksityisyyden vähenemiselle on internetin nopea laajeneminen ja yritykset, jotka nousivat jäteiksi tämän mukana. Jättiyritykset ovat saaneet paljon vapautta sen myötä, kun näiden palveluita ja sovelluksia pidetään oletuksena ja helpoimpana käyttövaihtoehtona.
Työn viimeisissä osioissa läpikäydään siitä, miten käyttäjä voi paremmin turvata oman yksityisyytensä valitsemalla datan turvallisuuteen panostavia yrityksiä, lisäosia ja sovelluksia selatessaan internettiä.

Asiasanat: Yksityisyys, internet, tietoturva, kyberturvallisuus, tietomurto

ABSTRACT

Oulu University of Applied Sciences
Bachelor of Engineering, Information Technology

Author: Milja Hakunti
Title of thesis: Loss of privacy on the internet
Supervisor: Minna Kamula
Term and year when the thesis was submitted: Spring 2022
Number of pages: 38

The subject of the thesis is privacy on the internet and why this has slowly diminished with the advancements of technology and digitalization. In the research, history of the subject is looked into and used as a background source of information. The sources also include researches, their results and newsreporting regarding the privacy policies of the services of the internet and IoT devices. The research also dwells into the subject of cybercrimes and how these have developed with the expansion of the internet.

Results show, that the biggest factor for the loss of privacy is the fast expansion of the internet and companies, that became giants along with it. Giant techcorps have gained much freedom through the fact, that their services and applications have gained the default status and are considered the easiest option for use.

The final sections of the work go into how the user can better secure their privacy by choosing companies, extensions and applications that focus on keeping data secure as they browse the internet.

Keywords: Privacy, internet, information security, cyber security, data break-in

SISÄLLYS

1 JOHDANTO

Internetillä on suuri rooli nykyisessä arkipäivässä. Nykyisin on harvinaista löytää henkilö tai yritys, joka ei jossain muodossa hyödyntäisi tätä laajaa verkostoa. Sosiaalinen media, foorumit, uutisten julkaisupalstat ja monet muut tiedon sekä viihteen lähteet vain hakemisen päässä; jos et löydä mitään omaan haluun tai tarpeeseen olisit yksi harvoista.

Internetin alku oli kuitenkin hyvin erilainen. Yksi ensimmäisistä yhdistetyistä verkostoista, joka loi pohjaa nykyiselle internetille, ARPANET, oli vuonna 1966 suunniteltu nopeuttamaan tiedon jakamista ja estämään tutkintojen tarpeetonta toistamista yliopistoissa. Tieteellisen tarkoituksen lisäksi pian luotiin myös verkostot armeijalle sekä markkinoinnin organisaatioille. (Bilgil 2009.)

Nyt internet ei ole enää rajattu vain tieteelliseen tai muuten organisaationaaliseen käyttöön vaan on myös yksityishenkilön käytössä. Sosiaalinen media on suurempi kuin koskaan ja älylaitteista on myös tullut arkipäivää. IoT (Internet of Things) laitteita on aikaisempina vuosina ennustettu olevan jopa 46 miljardia vuonna 2021; 200% suurempi määrä kuin vuonna 2016 (G Nick 2021).

Internetin ja tämän myötä myös IoT:n ja sosiaalisen median nousut eivät kuitenkaan ole tapahtuneet ilman negatiivisia puoliaan. Vuonna 2021 Facebookissa tapahtuneessa tietovuodossa käyttäjien tietoja puhelinnumeroista henkilötietoihin päätyivät vääriin käsiin vuonna 2019 löydetyn ohjelmistoheikkouden takia (Holmes 2021). Tämänkaltaiset tietovuodot sekä sosiaalisten medioiden liiankin täydellisesti personalisoidut mainonnat yksityishenkilöä kohtaan ovat nostaneet huolia yksityisyydestä. Kuinka paljon tietoa käyttäjistä oikeasti kerätään ja mitä varten? Kuinka tähän hetkeen on päästy, missä henkilön tekemät julkaisut sosiaalisen median alustoilla analysoidaan selvittääkseen pienimmätkin yksityiskohdat tämän elämästä ja käytännöistä? Entä kuinka käy tapauksessa, kun vanhemmat laittavat päivityksiä lapsestaan alustoillensa ennen, kun tämä pystyy edes antamaan oman mielipiteensä tästä; kun lapsi täyttää 13 ja vihdoin pääsee käyttämään internettiä itse, tästä on jo olemassa profiili mihin häneen kohdistuvaa tietoa on kerätty.

Tässä opinnäytetyössä tutkitaan, miksi yksityisyys on internetissä vähentynyt ja mitä käyttäjä voi tehdä suojellakseen itseään. Tutkintaan kuuluu myös muun muassa identiteettirikosten ja muiden tietoturva rikkomien vaikutukset digitaalisessa ympäristössä.

2 INTERNET ENNEN

Miten internetin voisi konseptina tiivistää? Kyseessä on maailmanlaajuinen ”verkkojen verkko”, joka muodostuu monista toisiinsa kytketyistä verkostoista. Nykyään voidaan puhua miljardeista sivustoista; kaikki tämä internetin nousevan suosion takia jo vuosia sitten.

Alkuperäinen verkosto, joka loi pohjaa internetin syntymiselle, oli nimeltään ARPANET (Advanced Research Project Agency). Kyseessä oli Yhdysvaltojen luoma verkosto sotilashallinnon ja yliopistojen tarpeisiin. Tämä aluksi käsitteli vain neljää tietokonetta, mutta laajeni vähitellen, kunnes vuonna 1973 ensimmäiset kansainväliset yhteydet luotiin, kun Englanti sekä Norja ottivat verkoston käyttöönsä. (Ahonen & Kolari 1994, 23.)

NCP (Network Control Protocol) oli ARPANETin aikainen protokolla, jonka avulla tiedostoja pystyttiin vaihtamaan ja lähettämään tietokoneiden välillä. Tämä kuitenkin korvattiin vuonna 1983 TCP/IP (Transmission Content Protocol/Internet Protocol) protokollalla, joka on käytössä yhä tänä päivänä. (Techopedia 2012.)

Myös Suomessa internetin ahkerimpia käyttäjiä olivat alussa yliopisto- ja tiedemaailma. Vuonna 1984 luotu FUNET-verkon (Finnish University and Research Network) kautta tärkeimmät tutkimuslaitokset korkea- ja ammattikorkeakoulujen mukana pääsivät internet-yhteyksien piireihin. Vielä vuonna 1994 suuri osa suomalaisista käyttäjistä tulivatkin internettiin tämän verkoston kautta. Samalla vuosiluvulla myös internetin kaupallinen käyttö oli kiihtymässä Suomessa joka viikko ja ympäri maailmaa internetistä oli jo tullut jokapäiväinen työväline. (Ahonen & Kolari 1994, 8.)

2.1 Tiedonkeruu ennen internettiä

Nykyaikana löytääkseen tietoa käyttäjän täytyy vain avata lähin hakukoneella varustettu laite ja kirjoittaa mitä on etsimässä. Oikeita termejä ja avainsanoja käyttämällä voi löytää tarvittavansa vain parissa minuutissa. Ennen internettiä tiedon tarve kuitenkin yleisesti tarkoitti joko kirjastoon lähtemistä tai itse omistettujen kirjojen tutkimista. Edes kirjojen lainaaminen ei kuitenkaan ollut yhtä vaivatonta kuin nykypäivänä, kun kirjastoissa käytettiin korttijärjestelmää listaamaan saatavilla olevat kirjat sekä myös merkkaamaan lainaukset.

Monissa tapauksissa tietoa saatiin myös kokemuksen kautta töissä ja tämän jälkeen tietoa opetettiin muille ja käytettiin myös muuten töiden ulkopuolella. Esimerkkinä 1800-luvulla henkilö saattoi oppia budjetointia töissä ja tämän jälkeen auttoi kirkkoaan budjetin luomisen kanssa.

Myös armeijan kautta saatiin tietoa; armeijan ohjekirjat autojen, rekkojen ja lentokoneiden korjaamiseen antoivat myöhemmin veteraaneille kokemuksen omien kotikoneiden korjaamiseen samantyylisten ohjekirjojen avulla. (Cortada 2016.)

Kirkot olivat myös tärkeitä henkilö- ja sukutiedon kerääjiä. Vielä nykypäivänä sukututkija voi käydä kirkonherranvirastolla tutkimassa yli satavuotiaita kirkonkirjojen mikrofilmikortteja. (Suomen Evankelis-Luterilainen kirkko 2016.)

Yritysten kohdalla tietoa mahdollisista työntekijöistä saatiin työvoimavirastojen kautta. Aikakautena, kun töiden etsiminen sanomalehdestä oli yhä tyypillistä, yritykset ottivat yhteyttä työvoimavirastoihin. Näillä virastoilla oli tietoja monista mahdollisista kandidaateista, jotka täyttäisivät yrityksen vaatimukset. (Agency central 2013.)

2.2 Web 1.0, World Wide Web

Web 1.0 viittaa World Wide Web:in kehityksen ensimmäiseen vaiheeseen. Käyttäjämäärä oli internetin alussa paljon pienempi ja tämä näkyi sisällöntuotannon määrässä; sisällöntuottajia oli paljon vähemmän kuluttajiin verrattuna. Henkilökohtaiset sivustot olivat suosittuja, isännöitsijänä joko ISP:n serverit tai ilmainen isännöitsijä palvelu internetissä.

Yksi Web 1.0:n olennainen ominaisuus oli sivujen staattisuus. Tämä tarkoitti, että sivut olivat ilman interaktiivista toimintaa; kun käyttäjä kävi sivustolla, sivut eivät tallentaneet tietoa käytöstä tai muokkautuneet käytön perusteella. Julkaistuja artikkeleita ei tyypillisesti päivitetty. Web-isännöitsijät harvoin myöskään tukivat palvelinpuolisten komentojen tekemistä, jota esimerkiksi tarvittiin sähköposti lomakkeiden lähettämistä varten. Tämän seurauksena lomakkeiden sijasta painaessaan ”Lähetä” -painiketta, käyttäjän sähköpostiohjelma käynnistyisi ja käyttäjän tuli lähettää lomakkeensa sähköpostitse verkkosivuston antamaan sähköpostiosoitteeseen. (Websitebuilders 2017.)

2.3 Digitaalisen markkinoinnin alut

Se mitä ei yleensä Web 1.0:n kanssa huomioidaan on fakta, että mainostaminen netin surffaamisen yhteydessä oli alunperin kiellettyä. Yritykset pystyivät kyllä luomaan omat sivustona, mutta nämä olivat vain katalogeja, josta tuotteita tai palveluita pystyi selata. Harvalla oli sivu, jossa tilauksen voi tehdä; tyypillisempää oli vain antaa sähköpostiosoite, jonne tilauksen pystyi laittaa. (Chakraborty 2021.)

Internetin kasvun myötä tämän markkinointimahdollisuudet kuitenkin huomattiin. Vuonna 1993 ensimmäinen sivuvalikossa klikattava mainos julkaistiin, joka merkitsi alun markkinoinnin digitaaliselle aikakaudelle (Monnappa 2022). Ensimmäinen laaja-alaisempi selain Netscape sai alkunsa vuonna 1994 ja tämän kautta digitaalinen markkinointi lähti todella käyntiin. Sähköposti, kehittyneet hakukoneet, kuten Yahoo! ja Google, ja kaupallisten sivustojen, kuten Amazonin ja eBayn, luominen toivat uusia tapoja yrityksille tavoittaa käyttäjät. Sähköpostista tuli markkinointityökalu, hakukoneet tapa, jolla asiakkaat voivat löytää tuotteita. Tämän lisäksi käyttöön otettiin varhaisimmat SEO-tekniikat. (UWA Online, 2019.)

2.4 Tiedonkeruu aikaisessa internetissä

Aikaisessa internetissä tietoa ei sinänsä kerätty vaan internet itse oli tiedonlähde, jota käyttäjät hyödynsivät tiedon etsimisessä. (Monnappa 2022). Internettiä siis hyödynnettiin varastona tiedolle; tähän kuuluen myös viranomaisten tietojärjestelmiä. Tämän takia vuonna 1999 voimaan tuli julkisuuslaki. Kyseinen laki koski viranomaisten tietojärjestelmien julkisuutta. Viranomaisten tuli luoda seloste, josta ilmenee järjestelmän tarkoitus, tähän talletetut tiedot, tietojen julkisuus tai salassa pito sekä tämän perustelut. Tällä kansalaiset saivat mahdollisuuden valvoa julkisen vallan käyttöä, osallistua päätöksentekoon sekä valvoa oikeuksiensa ja etujensa toteutumista. (Tilastokeskus 2018; Krakau & Haapalehto 2020, 15,19.)

2.5 Ensimmäisiä tunnettuja tiedonkeruu rikoksia

Internet tiloissa laittomaan tiedonkeräämiseen liittyy vakoiluohjelmien (engl.spyware) käyttö. Vakoiluohjelma on tietokoneviruksiin kuuluvaa ohjelma, joka kirjaa käyttäjän laitteen käyttöä, tietoja ja lähettää datan hyökkääjälle. Henkilökohtainen tieto tyypillisesti kerätään käyttäjän online käytännöistä, mutta vakoiluohjelmakoodi voi olla myös mukautettu tiettyjen käyttötietojen keräämiseen. (Innes 2021.)

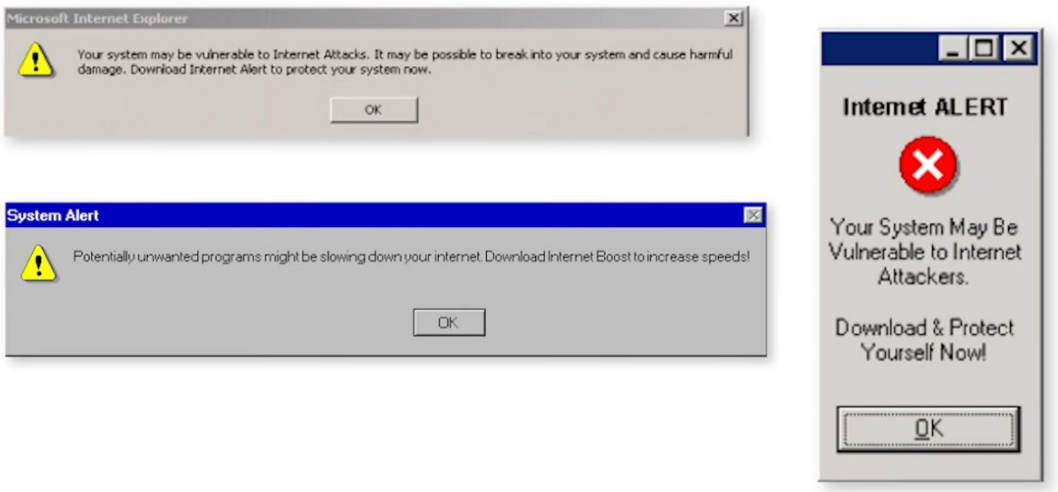
Termiä "spyware" käytettiin ensimmäistä kertaa lokakuussa vuonna 1995. Kyseessä oli Usenet julkaisu, joka käytti termiä pilkatakseen Microsoftin liiketoimintamallia. Vakoiluohjelmien ensimmäinen vaikutus käyttäjiin oli vuorostaan vuonna 1999, kun tuolloin suositun ilmaisohjelmapelin Elf Bowlingin havaittiin sisältävän seurantaohjelmistoja. Vakoiluohjelmien tekijöiden on tiedetty maksavan ilmaisohjelmien kehittäjille lisätäkseen ohjelmansa muuten harmittomaan ohjelmaan tai pakettiin. Joissain tapauksissa vakoiluohjelmien tekijät voivat myös itse lisätä vakoiluohjelmansa koodin ilmaissovelluksiin tai markkinoivat tekemäänsä harmitonta ohjelmaa, johon ovat käyttäjien tietämättä lisänneet myös seurantaohjelmistoja. Vakoiluohjelmat

voivat myös joutua käyttäjän laitteistoon laitteen haavoittuvuuden tai haitallisilla sivuilla käymisen takia. (Innes 2021; Malwarebytes 2022.)

Bonzi buddy

Yksi tunnettu aikainen tiedonkeruu rikos koskee virtuaaliassistentti ohjelmaa nimeltä Bonzi Buddy. Tämä otti mallia Microsoftin omasta "Microsoft agent" -ideasta. Vaikkakin Agentin jälkeen tullut Clippy oli pettymys ja parhaimmillaan ärsyke käyttäjille, Bonzi buddy onnistui valloittamaan yllättävän suuren demografian. Ohjelma pystyi moneen, joka ei enää nykypäivänä yllättäisi. Tämä pystyi ylläpitämään kalenteria, muistuttamaan käyttäjää kirjatuista tapahtumista, lukemaan sähköpostit ääneen käyttäjälle, hallita latauksia ja jopa selata internettiä- ja paljon muuta.

Bonzi buddy oli ilmainen ohjelma ja ystävä käyttäjälle; vitsien ja pienien faktojen kertomisen lisäksi, ollakseen ystävä tämän toki piti tuntea käyttäjä. Kun käyttäjä ensimmäistä kertaa aloitti ohjelman, tähän kuului rekisteröinti. Tätä varten oli pakollisia täytettäviä tietoja kuten nimi, ikä, zip/postinumero, maa ja sähköpostiosoite. Ei-pakollisina osioina olivat myös osoite, kaupunki ja maakunta. Itsenään näiden tietojen kysyminen ei näyttänyt vielä herättävän epäilyä käyttäjissä. Ohjelma vaikutti harmittomalta, kunnes käyttäjät alkoivat huomata omituisia Windows System alert -viestejä, kuten kuvassa 1.



Kuva 1: BonziBuddy - The Internet Spyware That Plagued Windows (Demonstration) (NationSquid 2021) Kuvakaappaus kohdasta 07:29

Tämä selveni vuonna 2002, kun ohjelman luonnut Bonzi software joutui oikeuteen, syytteenä mainosohjelmien sisällyttäminen assistenttiohjelmaan. Ohjelmisto avasi luvattoman takaoven,

jonka kautta syöttäisi käyttäjän koneeseen Windows alertin näköisiä varoitusviestejä, jotka väittivät koneen olevan haavoittuvainen ja suositteli lataamaan Bonzi softwaren muita ohjelmistoja suojaamaan konetta. Mainoksien lisäksi takaoven lisääminen jätti käyttäjien koneet alttiiksi muille haittaohjelmille kuten viruksille. Tämän lisäksi kävi ilmi, että takaovea käytettiin myös keräämään käyttäjätietoja ja lähettämään nämä takaisin Bonzi software tietokantaan. Käyttäjiä oli monista ikäluokista, mutta käydessään ilmi, että näihin kuului alle 13-vuotiaiden tietoja, Bonzi software joutui uudestaan oikeuteen COPPA (Children's Online Privacy Protection Act) lain perusteella. Tämän lainkäynnin jälkeen yritys joutui lopettamaan toimintansa ja Bonzi Buddyn sivut suljettiin vuonna 2008. (NationSquid 2021.)

3 INTERNET NYT JA YKSITYISYYDEN MUUTOS

Internet on läpikäynyt suuren ja nopean muutoksen vain muutamien vuosien sisällä. Kyseinen muutos on ollut kokoaikaista kehittämistyötä. Kaikki tämä parantamaan internetin tehokkuutta, turvallisuutta ja myös arvoa. Tämän myötä käyttäjätiedoista on tullut tärkeä tuote yrityksille.

3.1 Web 2.0

Internetin ja tämän teknologian edistymisen myötä kuulumme nyt Web 2.0 aikaan. Sivustot eivät ole enää staattisia ja täysin ilman interaktiivisuutta. Tämä ei tietenkään tarkoita, että Web 1.0 olisi täysin menneisyyttä, sillä käytämme yhä osaa vanhoista teknologioista ja käytänteistä. Tämän takia näitä Web versioita ei pysty erottamaan toisistaan.

Yksi olennainen muutos, joka tuli Web 2.0:n mukana ovat HTTP-evästeet. Evästeet ovat pieniä tekstitiedostoja, jotka ovat tallennettu käyttäjän koneelle. Näiden sisältämä informaatio on vierailtujen verkkosivujen palvelimien luettavissa. Yli 95% verkkosivuista käyttävät evästeitä ja suurin osa näistä sisältävät harmitonta tietoa. Tiedostot ovat apuna koneen tunnistamisessa; tämän tiedon avulla pystytään varmistamaan, että verkkosivut lataavat mahdollisimman nopeasti, sisäänkirjautumisen tiedot tai ostoskorin sisällöt pystytään muistamaan, tai mahdollistetaan verkkosivun mahdollisuus pitää kirjaa eri kävijöiden määrästä. Useimpien sivustojen hallussa olevaa dataa ei voida käyttää tunnistamaan käyttäjä. Ongelma kuitenkin piilee suurissa yrityksissä, kuten Googlessa, Amazonissa tai Facebookissa, joilla on valtava määrä henkilökohtaista käyttäjädataa. Kaiken tämän datan avulla yritysjätit pystyvät luomaan profiileja käyttäjistä, jotka he pystyvät mitä luultavemmin yhdistämään oikeaan henkilöön. Ongelmana ei ole siis itse teknologia, vaan yritykset, jotka hyväksikäyttävät sitä, tiesivät käyttäjät siitä tai ei. (Hill 2015.)

3.2 Mobiili- ja älylaitteiden nousu

Mobiili- ja älylaitteiden aikakauden aloittajaksi sanotaan olevan Apple, kun yritys julkaisi ensimmäisen iPhone älypuhelimen vuonna 2007 (Järvinen 2022). Puhelimien käyttö on tätä myötä paljon muuttunut; enää käyttäjät eivät säikähdä ja ala stressaamaan puhelinlaskun nousua, kun vahingossa avaa internetin kännykässään. Nykyään moni älypuhelin on aina liitettynä Wi-Fiin, kun internetin välityksellä toimivien ohjelmien käyttäminen on jopa halvempaa kuin mobiilidatan käyttö.

Tietokoneet ja puhelimet eivät kuitenkaan enää ole ainoita, jotka toimivat internetissä. Nyt puhumme älypuhelimista, kaiuttimista, kelloista tai jopa jääkaapeista tai muista kodinlaitteesta. Oman niin sanotun ”smart” kodin omistaminen voi kuulostaa houkuttelevalta; pelkällä painikkeen kosketuksella pystyy hallitsemaan kodinlaitteita, valaistusta ja jopa hälytysjärjestelmää. Moni kuitenkin unohtaa, että nämä luksukset tulevat omien riskiensä kanssa. IoT:n kasvaessa aina vaan useampi laite on internettiin yhdistettynä; ja tämän myötä rikollisilla on aina vaan enemmän eri lähtökohtia, joista voivat päästä käyttäjän verkostoon sisään ja tämän kautta tietoihin. Yksi huolestuttava jopa trendiksi noussut teko on hakkerien murtautuminen vauvojen itkuhälyttimiin.

Rikollisten lisäksi myös itse laitteet voivat olla riski yksityisyydelle, kun internetyhteys mahdollistaa käyttäjätietojen lähettämisen takaisin laitteiden kehittäjille. Yksi esimerkki tämänkaltaisista laitteista ovat älykaiuttimet, kuten Amazonin Alexa, Applen Siri ja Googlen oma Google Assistant. Älykaiuttimet kuuntelevat aina sen varalta, että käyttäjä sanoo aktivointisanan; äänentunnistusteknologia ei kuitenkaan ole täydellistä ja Northeastern Universityn tekemässä tutkimuksessa kävi ilmi, että Alexa ja muut älykaiuttimet voivat vahingossa päätyä kuuntelemaan käyttäjää jopa 19 kertaa päivässä. (Nita 2021.)

Alexan tapauksessa Amazon on rauhoitellut väkeä sanomalla, että tämänkaltaista dataa käytetään vain parantamaan palvelua. Alexan täytyy oppia ymmärtämään käyttäjänsä äänen jos haluaa olla hyödyksi. Tämän lisäksi käyttäjä voi aina laittaa kuuntelun pois päältä tai tyhjentää datahistorian. Kuitenkin vuonna 2019 Amazon totesi, että ei aina poista kaikkea tallennettua dataa, jonka saa äänivuorovaikutuksesta Alexa tai Echo laitteiden kautta, vaikka käyttäjä itse päättää poistaa datan. Syy tähän väitetään olevan, että datan poisto voisi vaikuttaa laitteen toimintaan tai estää Alexan tekemästä halutun toiminnon tai poistaminen on yksinkertaisesti vain pidempi prosessi. 2019 huhtikuussa Bloombergin tekemä raportti Amazonista kuitenkin huolestutti monia: monilla työntekijöillä -joista osa eivät välttämättä edes ole suoraan Amazonin työntekijöitä- on pääsy sekä Alexan ääni- että tekstitranskriptioihin, joita voitaisiin teoriassa käyttää kokoamaan tietoja käyttäjän henkilökohtaisesta elämästä. (Kelly & Statt 2019; Nita 2021.)

Mobiilisovellukset

Nykypäivän älypuhelimet ovat periaatteessa pieniä kannettavia tietokoneita. Nämä toimivat assistentteina jokapäiväisessä arjessa- ja käyttävät tämän tekemistä varten monia erilaisia toimintoja. Itse nämä toiminnot eivät tietenkään ole ongelma. Vaan se, kun näitä toimintoja hyväksikäytetään muuhun. Epäluotettavat sovellukset tyypillisesti kuuluvat tähän kategoriaan. Verkkosovelluskauppa Google Play on monia kertoja reportoinnut toimistaan poistamaan tämän kaltaisia sovelluksia. Sovelluksia, jotka ladatessaan voivat käyttäjän tietämättä käyttää puhelimen mikrofonia, kameraa ja jopa sijaintia. Kaikkea tätä vastaan koko ajan kehitetään uusia turvallisuusmekanismeja, mutta sovellusten laajan määrän ja monien oikeiden käytännöllisten toimintojen takia, oikea tasapaino on hankala löytää. (Temming 2018.)

Sovelluksen ei kuitenkaan tarvitse olla tehty haitalliseksi luodakseen turvallisuusriskejä. Yksi tapaus on Snapchat, jonka tietoturvakäytännöt ovat huolestuttaneet käyttäjiä. Yksi esimerkki näistä käytänteistä on enkryptoinnin puute viesteissä. Snapchat käyttää enkryptointia tämän pääsijaisiin 'snap' viesteihin (kuvia tai videoita), jotka myös poistetaan tietyn ajan kuluttua. Enkryptointia ei kuitenkaan käytetä esimerkiksi teksti- tai ryhmäviesteissä. Tämä enkryptoinnin puute ja turvallisuuden sekä yksityisyyden vähäinen priorisointi pitäisi saada käyttäjät harkitsemaan tarkemmin mitä kaikkea suostuvat jakamaan sovelluksessa. (Choosetoencrypt 2020.)

3.3 Sosiaalinen media

Sosiaalisuus on ollut osana verkkomedioita jo alusta asti keskustelualueiden muodossa, mutta ensimmäiset nykyaikaiset sosiaaliset mediat saivat alkunsa 2000-luvun alussa, kun internettiä käytti tarpeeksi laaja väestö. Aikainen blogi -palvelu, joka sisälsi paljon nykyaikaisia ominaisuuksia, on MySpace, joka avattiin vuonna 2003. Omat käyttäjäprofiilit, kaverit, kuvien, videoiden sekä omien tekstipäivitysten tekeminen ja jako oli uutta. Alusta nousi selväksi käyttäjien suosikiksi, ylittäen 65 miljoonaa käyttäjää vuonna 2006. Tämä suosio ei kuitenkaan jatkunut kauan, kun vuonna 2004 Mark Zuckerberg perusti Facebookin. Zuckerbergin Harvard opintojen aikana luodun sivuston alkuperäinen tavoite oli kerätä naispuolisten opiskelijoiden kuvia nettiin, mutta on nykyään melko erilainen. Sivuston alku oli toki myrskyinen, mutta jo vuonna 2007 tämä oli levinnyt suosiossaan myös Suomeen. (Järvinen 2022, 273-274.)

Vuosien aikana sanat Facebook ja ”yksityisyyden rikkominen” ovat monta kertaa mainittu yhdessä. Mikä alunperin on monille saattanut kuulostaa vain paranoidilta ajattelulta, on myöhemmin todistettu todelliseksi- ainakin melkein. Yhtenä esimerkkinä käyttäjien teorioista on se, että Facebook kuuntelee. Käyttäjät saattaisivat satunnaisesti puhua jostain ja myöhemmin käydessään Facebookissa huomaavat mainoksia tähän liittyen. Kyseessä ei sinänsä kuitenkaan ole suora kuuntelu. Jopa yli 95% Facebookin tuloista tulee mainoksista; yrityksen liiketoimintamalli keskittyy siksi paljon mainosten ja sisällön kohdentamiseen sopiville käyttäjille. Tätä varten he tarvitsevat paljon tietoa käyttäjästä; tiedon keräämistä ja profilointia varten Facebook siksi mahdollistaa käyttäjän onlinekäytäntöjen seuraamisen myös silloin, kun käyttäjä ei ole kirjautuneena sisään. Tähän Facebook käyttää kolmannen osapuolen evästeitä; monet muut yritykset ja sivustot myös tekevät yhteistyötä Facebookin kanssa parantamaan markkinointiaan Facebook Pixelin avulla. Seuraamalla käyttäjää selaimessa, Facebook kerää paljon tietoa ja voi näin kohdistaa, mikä aihe voisi heitä mahdollisesti kiinnostaa. Niin sanottu offline ja online tiedonkeräys pidetään erossa toisistaan, mutta lopputulos on silti samanlainen. Tieto menee markkinointiin. Tämän lisäksi itse Facebook sovelluksen sisällä ohjelma seuraa myös käyttäjän ystävien, ryhmien tai jopa tapahtumien kulkua ja yhdistää näitä tietoja myös käyttäjän profiiliin. (Nield, 2020; Dinita, 2021.) Nämä käytännöt, kuinka Facebook seuraa käyttäjiään -tai jopa heitä, joilla ei ole Facebook tiliä- ovat monien mielestä ahdistavia. Käyttäjien huolia ei myös helpota Facebookin historia monenlaisten skandaalien kanssa, johon kuuluu myös tietovuotoja, joissa miljoonien ihmisten tiedot päätyvät kaikkien nähtäväksi.

Facebook saattaa olla sosiaalisista medioista tunnetuin yksityisyyden rikkoja, mutta ei ole ainoa. Myös monet muut sosiaaliset mediat ja näiden alustat ovat syylistyneet yksityisyyden rikkomiseen. Instagram, joka on nykyään Facebookin omistama, on myös monta kertaa rikkonut lapsia koskevaa tietosuojalakia. Kiinalaisyritys ByteDance:n omistama TikTok on myös saanut paljon kritiikkiä tämän yksityisyyskäytännöistä. Sovelluksen käyttäjäehdoissa ja tietosuojakäytännöissä mainitaan kerätyn tiedon myynti eteenpäin kolmansille osapuolille siinä tapauksessa, että yritys tai osa tästä myydään. Ehdoissa on myös maininta tietojen antamisesta eteenpäin viranomaisille tai muille organisaatioille, jos pyyntö tai velvoite näiden antamisesta tulisi. Myös sovelluksen ehtojen ja käytäntöjen kirjaamisen ulkopuolella on esiintynyt paljon erilaista tietojen hyväksikäyttöä. Saksalainen tutkimus todisti, että sovellus asensi selainseuraajia käyttäjän laitteeseen ja yksityisen Reddit käyttäjän tekemässä sovelluksen purkamisessa kävi ilmi, että sovellus myös muun muassa selvittää mitä muita sovelluksia on ladattu, laitteen tietoja ja paljon muuta. Jotkut jopa väittävät, että TikTok sosiaalisena mediana on valhe ja sovelluksen oikea tarkoitus on tiedonkeruu. (Janssen 2022.)

Sosiaalisilla medioilla on ollut toistuvasti sama puolustus saadessaan syytteitä yksityisyyden rikkomisesta; se, että tämä mainitaan joko käyttäjäehdoissa tai tietosuojakäytännöissä. Mutta tietääkö käyttäjä tosissaan, mihin antaa luvan, kun antaa esimerkiksi sovellukselle luvan käyttää laitteensa kameraa? Jos sovelluksessa tehdään kuvaamista, niin toki luvan antaminen kameran käyttöön on itsestäänselvyys; mutta harva on tietoinen siitä, jos tämä sisältää myös luvan käyttää kameraa tai tallentaa puhetta käyttäjän tietämättä.

3.4 Selaimet ja hakukoneet

Internetin käytön lisääntyessä syntyi uusi markkina selaimille sekä hakukoneille. Markkinasta tuli nopeasti kilpailullinen, kun ensimmäiset selainsodat (engl. Browser wars) käytiin 1900-luvun lopulla Internet Explorerin ja Navigatorin välillä. Nämä selaimet eivät enää ole massakäytössä, mutta selainsotaa käydään yhä nykyaikaisten selainten välillä.

Internetin nykyisessä ympäristössä, Googlen kehittämä Chrome on selaimista käytetyin. Syitä tähän on selaimen modernimpi tila, verrattuna esimerkiksi Microsoft Edgeen ja Firefoxiin, jotka saivat alkunsa jo Web 1.0:n aikana Internet Explorerin ja Netscapen muodoissa. Tämän lisäksi Googlen aloittama Open source -projekti Chromium teki selaimesta suositun kehittäjien kanssa.

Yhdistettynä, Google suosituimpana hakukoneena ja Chrome suosituimpana selaimena, Google on varmistanut asemansa tärkeänä osana internettiä. Tämä suosio on kuitenkin myös huolenaihe. Jos muut selaimet ja hakukoneet eivät saa tarpeeksi tukea, ei voi olettaa, että näiden kehitystä jatketaan. Google ja Chrome eivät myös ole ilman haitallisia yksityisyyskäytäntöjään. Yhtenä esimerkkinä on vuonna 2021 Googlen aloittama tutkimus, jossa pieni osa käyttäjistä otettiin mukaan heidän tietämättä. Kyseisen tutkimuksen kohteena oli Googlen kehittämän uuden teknologian, FloC:n (Federated Learning of Cohorts) testaus. Teknologian tarkoitus oli luoda uusi tapa kohdentaa mainoksia käyttäjiin seuraamalla käyttäjien toimintaa internetissä; tämän perusteella käyttäjät ryhmiteltäisiin eri luokkiin ja näiden luokkien tiedot jaettaisiin kolmansien osapuolien ja muiden mainostajien kanssa internetissä. Jo se, että käyttäjiä otettiin testiin mukaan ilman heidän suostumustaan, on loukkaus käyttäjien luottamusta vastaan. (Cyphers 2021.)

Hiljainen uusien teknologien testaaminen käyttäjillä ei ole ainoa rikkomus, josta Google ja tämän monet palvelut ovat syyllisiä. Juha-Pekka Raesten kirjassa ”Maailman 50 vaarallisinta yhtiötä” (2020) Google on asetettu listan ensimmäiseksi myös syystä. Nykyiset teknologiajätit ovat niin valtavia, että näiden ympärille on hankala asettaa minkäänlaisia rajoitteita. Nämä yritykset

pystyvät helposti ostamaan pienempiä yrityksiä, joiden avulla vain kasvattavat omaa agendaansa. Google tunnetusti myös kerää paljon tietoa käyttäjistään. Googlen palveluita tulee valmiiksi ladattuna monissa laitteissa ja näiden eri toiminnot antavat eri dataa kuten Google Maps ja historia käyttäjän sijainneista, Gmail ja listatut eri tapahtumat ja näiden ajat, YouTube ja käyttäjän videohaut ja paljon muuta. Google on niin valtava, että kokonaisuudessaan on hyvin vähän dataa, jota tämä ei voi kerätä.

4 TIEDONKERUUN TARKOITUS JA VAIKUTUS

Tietoa kerätään moniin tarkoituksiin, mutta tavoite on tyypillisesti sama. Tiedonkeruun tarkoitus on ymmärtää ongelma, käyttäjien tarpeet tai esimerkiksi markkinoinnissa kohdeyleisö. Kerättyä tietoa käytetään tukena ongelmanratkaisussa, parantamaan nykyisiä palveluja ja tavoittamaan asiakkaat. Käyttäjädata on siksi yksi tärkeimmistä tuotteista mitä yritys voi kerätä.

Käyttäjädatan keräämisen lisääntyessä myös säännöt tähän liittyen ovat muuttuneet. Vuonna 2018 Euroopassa käyttöön otettu GDPR (General Data Protection Regulation) laki pyrki suojaamaan ja vahvistamaan käyttäjän roolia omien tietojensa käsittelyn kanssa. Käyttäjä pystyisi pyytää tarkistamaan tai korjaamaan omat tietonsa sekä pyytää, että omat tietonsa poistetaan yrityksen tiedoista perusteiden kanssa. Yritykseltä vaaditaan enemmän avoimuutta ilmoittamalla mitä tietoja kerätään ja mihin, sekä ilmoittamaan jos tietoturvarikkomus on tapahtunut. Yrityksellä täytyy myös olla perustellut syyt tietojen keräämiseen.

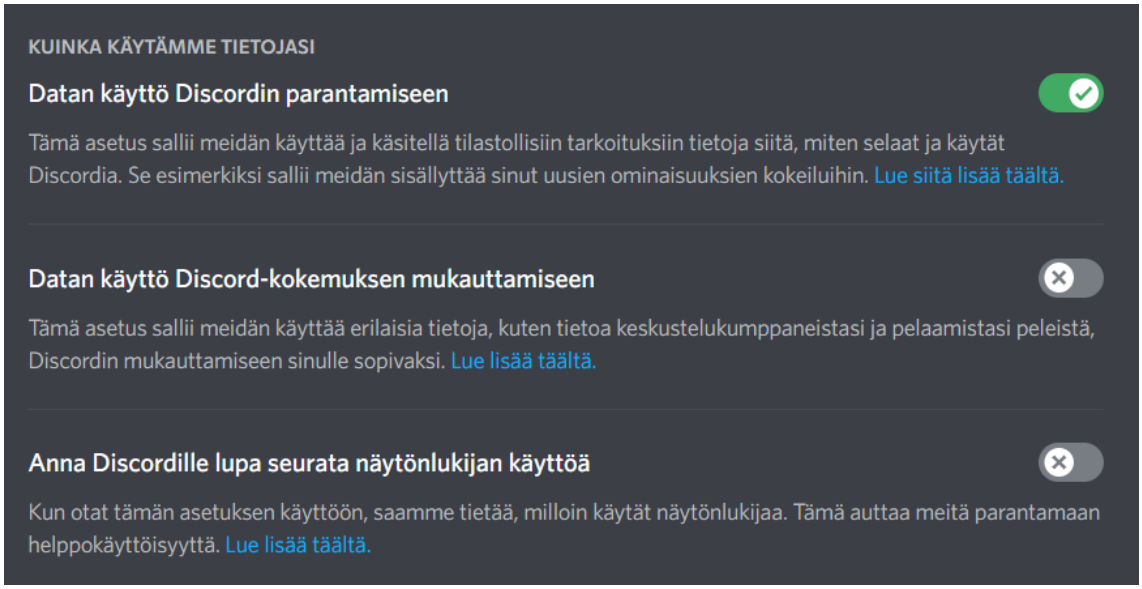
GDPR on onnistunut lisäämään tietoisuutta yksityisyyden tärkeydestä ja lisäämään painostusta tämän takaamiseen. Myös yritysten läpinäkyvyys tietomurtojen tapahtuessa on yleistynyt. Laki ei kuitenkaan ole täydellinen; lain astuessa voimaan tällä oli heikko tukijärjestelmä yrityksille, joka teki uusiin käytäntöihin siirtymisestä hankalan prosessin. Helppokäyttöisiä välineitä tai tapoja seurata, että yritykset todellisuudessa seurasivat näitä käytäntöjä ei myöskään ollut. Kaiken lisäksi käyttäjät saivat ekstra ärsykkeen toistuvista evästeiden hyväksymispyynnöistä. Yrityksillä ei myös ole mitään pakotetta tehdä tietosuojakäytäntötekstistä helppoa luettavaa, joka johtaa siihen, että monet käyttäjät päätyvät hyväksymään evästeet ilman, että edes lukevat mihin ovat suostumassa. (Lechner 2020.)

4.1 Tiedonkeruu kehittämistä varten

Sovellusten, eri laitteiden ja sivustojen kehittämiseen kuuluu monia eri osia ja tämän takia aikaisissa testeissä tarvitaan paljon tietoa käyttäjän kokemuksista ja käytöksestä. Kehittäminen kuitenkin tapahtuu myös tuotoksen julkaisun jälkeen; varsinkin verkkosivuilla ja sovelluksissa kehittäjät haluavat ymmärtää käyttäjän polun valmiin tuotteen kanssa. Tuotteen ensimmäisten versioiden testeissä on harvoin kuviteltu käyttäjämäärä, joten analysointi myös tuotteen julkaisun jälkeen on tärkeää. Tämän avulla voidaan selvittää, miten eri tavoin sivuilla käyttäydytään, miten käyttäjä navigoi UI:ta (User Interface) ja kuinka kauan tietyillä sivuilla pysytään. Tämän tiedon

avulla kehittäjät pystyvät parantamaan ohjelmaa; tämä tapahtuen joko muuttamalla navigointikäytäntöjä, lisäämällä uusia toimintoja tai tekemään tietyistä toiminnoista selvempiä. Keräämällä tietoa siitä miten käyttäjät päätyvät sivuille ja mitkä sivuista kiinnostavat eniten voidaan myös kehittää sivuja pitämään käyttäjät kauemman aikaa. Nettisivuilla datan keräämiseen on monia eri webanalytiikkatyökaluja, kuten Google Analytics, Kissmetrics ja Mixpanel. Jotkin työkalut keskittyvät tarkemmin käyttäjäkunnan selvittämiseen ja toiset käyttäytymiseen verkkosivuilla. Google Analytics on varsinkin monilla nettisivuilla käytetty analytiikkatyökalu. Tämän ohjelman tiedonkeruun voi kuitenkin onneksi estää sivuilla kieltämällä kolmansien osapuolien tiedonkeruun sivuilla.

Monet sovellukset myös sisältävät taustaprosesseja, jotka samalla tavalla keräävät käyttäjätietoa ja lähettävät tätä takaisin kehittäjille. Ohjelmat kuten Discord tai Firefox selain, antavat käyttäjälle vapauden valita haluavatko he lähettää dataa kehitystä varten. Kuten kuvassa 2 esitetään, Discordilla on useampi asetus liittyen tiedonkeräämiseen ja käyttöön.



Kuva 2: Kuvakaappaus Discordin tietojenkeruuasetuksista

Tiedonkeräämiseen kuuluu myös virheraportointi; tämä tarkoittaa virheraportteja, jotka kuvaavat laitteessa tai ohjelmassa tapahtuneita virheitä. Ehkä tunnetuin näistä on Windows 10:n ”blue screen”, joka ilmestyy ilmoittamaan käyttäjälle kriittisestä ongelmasta käyttöjärjestelmässä, jonka takia Windows joutuu käynnistämään itsensä uudelleen. Ennen uudelleenkäynnistystä Windows kerää tietoja tapahtuneesta virheestä ja tallentaa tämän event -tiedostoihin.

Tiedonkerääminen on tärkeä osa ohjelmien ja teknologian kehittämistä varten, mutta tämä ei tarkoita, ettei käyttäjien kannata kyseenalaistaa mikä tieto on oikeasti tarpeellista kehitystä varten

ja mikä ei. Vuonna 2016 Quidsup niminen Youtube-käyttäjä teki videon, jossa kävi läpi pieniä tilastotietoja Windows 10:n käytöstä, kun tämä oli saavuttanut 200 miljoonan aktiivisen käyttäjän määrän käyttöjärjestelmässä. Muiden tilastojen yhteydessä oli esimerkiksi maininta siitä, kuinka monta kuvaa käyttäjät olivat katsoneet Valokuvat -sovelluksessa ja kuinka kauan käyttäjillä oli ollut selain päällä. (Quidsup 2016.) Huolen aiheena ovat myös älylaitteet kuten Amazonin Alexa ja Google Assistant älykaiuttimet. Nämä keräävät tietoa palvelunkehittämistä varten, mutta osa tiedosta on todettu olevan arkaluontoista ja kerätty ilman käyttäjän tietämistä. Amazon ja Google ovat myös saaneet COPPA (Children's Online Privacy Protection Act) lain murtosyytöksiä; Amazon tämän lapsille suunnatun Echo version takia ja Google YouTuben tiedonkeräämiskäytännöistä. (Kelly & Statt 2019.)

4.2 Tiedonkeruu markkinointia varten

Tiedonkerääminen markkinointia varten tarkoittaa dataa, jota kerätään pystyäkseen kohdistamaan palveluiden ja tuotteiden mainoksia sopiville käyttäjille.

Internetin nousun ja Web 2.0:n tuoman sosiaalisen median myötä online markkinointi on muuttunut suuresti. Sosiaalisessa mediassa yritykset voivat selata käyttäjien itse jakamaa tietoa ja tämän myötä paremmin oppia minkälaisia ihmisiä heidän kohdeyleisöönsä kuuluu. Online markkinointiin kuuluu myös mainospalvelujen käyttö, esimerkiksi Google ads tai Facebookin Pixel. Google ads toimii huutokaupan tyylisellä tavalla, missä käyttäjä tekee tarjouksen avainsanoista. Kyseessä ei kuitenkaan ole vain korkeimman tarjouksen valitseminen, vaan Google ottaa myös huomioon mainoksen laadun. Yhdistämällä arvion mainoksen laadusta ja tarjouksen määrän, sivusto antaa mainoksella AdRankin. Tämä AdRank kertoo, kuinka useasti mainos näytetään paikoissa, missä avainsana on ajankohtainen. Se, miten Google selvittää mitkä sivustot tai käyttäjät ovat yhteensopivia avainsanojen kanssa on evästeiden avulla. (Akhtar 2020.)

Käyttäjädataa voi myös ostaa, mutta tämän laillisuus on hyvin kyseenalaista. Vuonna 2020 PCMag ja Motherboardin tekemä yhteistutkimus paljasti, että antivirusyritys Avast on käyttäjien tietämättä kerännyt tietoa heidän internetin käytöstä sekä Avastin antiviruksen ja selainlisäosan kautta. Tämän jälkeen tieto lähetettiin eteenpäin Jumpshot nimiselle tiedonmyyntiyritykselle, joka loi tiedosta erilaisia paketteja ja myi niitä eteenpäin yrityksille. Tietoihin kuului Google hakuja, tietoja etsityistä alueista ja näiden GPS koordinaateista Google Mapsissä, LinkedIn sivuja, YouTube videoita sekä aikuisviihdesivustoja. Näillä sivustoilla tietoihin saattoi jopa kuulua mitä termejä käyttäjä etsi ja mitä videoita hän katsoi. Kun tämä tieto ensimmäistä kertaa paljastettiin käyttäjille, Avast väitti, että kaikilta käyttäjiltä pyydettiin lupa tiedon keräämiseen. Motherboardin

tekemissä haastatteluissa kuitenkin käyttäjät sanoivat, etteivät tienneet tästä mitään tai kuinka tarkkaa tietoa oikeasti kerättiin. Vaikka kerättyyn tietoon ei kuulunut tietoja kuten käyttäjien nimiä, ekspertit silti väittävät, että osat tiedoista sisältävät niin yksityiskohtaisia selaustietoja, että joidenkin käyttäjien henkilöllisyys olisi selvitettävissä. New Yorkissa sijaitseva yritys nimeltä Omnicon oli yksi näistä asiakkaista ja sai pääsyn kaikkiin neljästätoista maasta kerättyihin tietoihin. Hakujen sijasta näihin tietoihin kuului "klikkaustietoja" (engl. Click feed) eli tieto siitä mitä osia sivuissa käyttäjät painoivat, missä ja missä järjestyksessä. Dokumenteissa Jumpshot mainitsee, että kaikki henkilökohtaistavat tiedot ovat poistettu, mutta tiedot kuitenkin vielä sisältävät käyttäjien päätellyn sukupuolen ja iän selauskäyttäytymisen perusteella sekä koko URL-merkkijonon. Omnicon ja moni muu yritys, kuten Google ja Loreal eivät vastanneet kommenttipyyntöön tilanteesta. (Cox, 2020.)

5 MIKSI YKSITYISYYDELLÄ ON VÄLIÄ?

Yksityisyys on oikeus päättää siitä, mitä kertoo, kenelle, kuinka ja missä. Suuren datan ja tiedon hyödyntämisen aikakaudella tämä yksityisyys on kuitenkin koko ajan vähenemässä. Vuonna 2021 Yhdysvalloissa kävi ilmi, että syyskuuhun mennessä tietomurtojen määrä oli jo ylittänyt aikaisemman vuoden numerot 17 prosentilla. Yksityisyys ei kuitenkaan ole vähentynyt pelkästään lisääntyvien tietomurtojen takia ja nämä tietomurrot eivät tapahdu sattumalla. Todellisuudessa monet aliarvioivat yksityisyyden tärkeyden internetissä ja näin eivät ymmärrä, kuinka paljon tietoa itsestään jakavat sekä sosiaalisessa mediassa että internettiä selaamalla. (Sushko 2021.)

Yksityisyydellä on suora yhteys tietoturvaan; liiallisen henkilökohtaisen tiedon jakamisen tai vuodon takia on altis monelle vaaralle kuten sosiaaliselle manipuloinnille (engl. Social engineering) tai jopa vaanimiselle (engl. Stalking). Tapoja häiriköidä toisia internetissä on monia ja nämä yleensä hyödyntävät tietoa, jota uhrista löydetään. Kuvassa 3 on esitetty näitä konsepteja sekä niiden määritelmiä.

Table 1. Definitions of digital harassment and abuse and related concepts.

Concept	Study	Definition
Cyber-aggression	Shapka and Maghsoudi (2017)	Aggression that occurs virtually via a digital/electronic medium such as a mobile phone or over the internet, including comments that are socially embarrassing, hurtful, mean or hate based.
Cyberbullying	Tokunaga (2010); Willard (2007)	Any behaviour performed through electronic or digital media by individuals or groups that repeatedly communicates hostile or aggressive messages intended to inflict harm or discomfort on others, including: flaming, harassment (repetitive, offensive messages), outing and trickery, exclusion, impersonation, cyberstalking (sending repetitive threatening communications), and non-consensual 'sexting' (distributing nude pictures of another individual without that person's consent).
Cyber-obsessional pursuit (COP)	Spitzberg and Hoobler (2002)	Unwanted pursuit of intimacy through the repeated invasion of a person's sense of physical or symbolic privacy conducted via digital or online means.
Cyberstalking	Dreßing et al. (2014); Reyns et al. (2012)	Repeated unwanted communication, unwanted contact, unwanted sexual advances, threats of violence/physical harm; and that cause a victim to feel fearful for their safety.
Digital harassment and abuse	Powell and Henry (2016)	Offensive comments and name-calling, social embarrassment, targeted harassment, technology-facilitated sexual violence and hate-based abuse.
Electronic aggression	Bennet et al. (2011)	Experiences include hostility, intrusiveness, humiliation and exclusion.
Image-based sexual abuse (IBSA)/ Image-based abuse (IBA)	Powell and Henry (2016, 2017)	Taking, distributing and/or threatening to distribute a nude or sexual image of a person without their consent.
Internet harassment	Ybarra and Mitchell (2004)	Overt, intentional acts of aggression towards another person online.
Online harassment	Finn (2004); Lindsay et al. (2016); Finkelhor et al. (2000)	Repeated messages that threaten, insult, or harass; threats or other offensive behaviour sent to the victim or posted online for others to see.
Technology-facilitated sexual violence (TFSV)	Powell and Henry (2014, 2017); Henry and Powell (2014, 2015, 2016)	Harmful sexually aggressive and harassing behaviours perpetrated with the aid or use of digital communication technologies, including: sexual aggression and/ or coercion; image-based sexual abuse (including 'revenge pornography' and 'sextortion'); online sexual harassment; and sexuality and/or gender-based harassment (including hate-speech).
Technology-facilitated stalking	Woodlock (2013, 2016)	Repeated, unwanted contact that results in a victim feeling fearful.
Virtual hate speech	Awan and Zempi (2017)	Material of a malicious nature that is posted with the intent to promote or justify intolerance, hostility and prejudice towards an individual or group of people.

Kuva 3: Digitaalisen häirinnän ja väärinkäytön sekä liittyvien konseptien määritelmiä (Powell, Scott & Henry 2018.)

5.1 Itse annettu tieto ja tämän uhat

Sosiaalisessa manipuloinnissa on kyse toisen käyttäjän manipuloinnista tai kiristämisestä saadakseen käyttäjä tekemään tai jakamaan jotain, mitä tämä ei omasta halustaan halua välttämättä tehdä. Manipulointia tehdään joko päästäkseen käsiksi tietoihin tai rahan takia. (Kortelainen 2020.)

Sosiaalinen manipulointi yleensä hyödyntää ihmisten halua auttaa tai yksinäisyyttä. Yksi esimerkki tästä ovat rakkausrikokset. Rikoksen voi jakaa kolmeen eri vaiheeseen. Ensimmäisenä huijari tapaa uhrinsa sosiaalisessa mediassa, chat- tai treffipalvelussa. Huijari ei heti pyydä rahaa, vaan pyrkii luomaan suhteen uhrinsa kanssa. Ennen toista vaihetta huijari on pyrkinyt osaksi uhrin elämää. Tässä on tyypillisesti hyväksikäytetty uhrin yksinäisyyttä; huijari kertoo uhrille asioita, joita tämä haluaa kuulla ja näin luo riippuvaisen rakkaussuhteen. Se mitä uhri haluaa kuulla, on opittu keskusteluiden kautta, kun uhri alkaa avautua huijarille omasta elämästään. Toisessa vaiheessa huijarille tai tämän perheelle on sattunut jokin yhtäkkinen tapaturma, mitä varten tämä tarvitsee rahaa ja nopeasti. Huijari saattaa hyvinkin vedota uhrin tunteisiin kuvaamalla yleensä traagisen tapahtuman johon uhri mahdollisesti samaistuu myös. Huijauksen kolmas vaihe on, kun huijari pyytää uhriltansa rahaa. Rahan saamisen kanssa on aina kiire ja selitykset tälle ovat moninaisia. (Kortelainen 2020.)

Vaaniminen on toinen ongelma, joka on lisääntynyt, kun ihmiset vapaasti kertovat kohdistavia tietoja itsestään muun muassa sosiaalisessa mediassa. Yksittäiset laajat tiedot, kuten missä maassa asuu ja mikä etu- tai lempinimi on ei vielä mitään erityistä riskiä luo. Paljon yksityiskohtaisempien tietojen jakaminen, kuten sukunimen, paikkakunnan, kaupungin, työpaikan tai koulun jakaminen jo luo mahdollisuutta ongelmille.

Jokaisen käyttäjän pitäisi myös harkita enemmän, ennen kuin jakaa kuvia sosiaalisessa mediassa. Jos some tili on avonainen eikä yksityinen, kuka tahansa saattaa päätyä katsomaan kuvia. Tämän lisäksi, jos kuvassa on selkeitä maamerkkejä, riskeeraa oman sijaintinsa paljastamisen. Oman sijainnin paljastaminen on riski varsinkin ”influencer” (suom. Vaikuttaja) -tyyppisille käyttäjille sekä julkkiksille, joilla on tuhansia faneja. Hyvin äärimmäinen esimerkki siitä, kuinka pitkälle hullaantunut fani voi mennä on 2019 tapahtunut rikos. Vaanijaksi muuttunut fani löysi japanilaisen pop-tähden sijainnin analysoimalla reflektiota tämän silmässä. Vaanija näin selvitti, millä juna-asemalla hän oli ja tämän jälkeen seurasi häntä kotiin asti, jossa pop-tähti joutui hyökkäyksen kohteeksi. (Peters 2019.)

Pelkästään suuret sosiaaliset figuurit eivät kuitenkaan ole häiriköinnin kohteina. Internetin alustoilla tapahtuu moninaista häiriköintiä ja tämä usein kohdistuu varsinkin vähemmistöihin.

Vuonna 2018 tehtiin tutkimus, jossa haastateltiin australialaisia ja brittiläisiä näiden kokemuksista digitaalisen häiriköinnin kanssa. Tutkimukseen kuului seksuaalista ja sukupuolista vähemmistöä, ja tulokset viittaavat paljon korkeampaan häiriköinti prosenttiin heidän kohdallaan. Myös rasismin ja esimerkiksi xenophobia (muukalaisviha) ovat yleisiä syitä häiriköinnille. Pahimmillaan tämä leviää myös internetin ulkopuolelle väkivallan tai muun harmin kuten kotiosoitteen julkaisun (engl.doxing) uhkauksilla. (Powell ym. 2018.)

5.2 Kerätyn tiedon uhat

Riippuen osapuolista, myös kerätyllä tiedolla on omat uhkansa. Tyypillinen verkkosivusto, joka käyttää evästeitä on tuskin harmillinen, vaan käyttää tietoa ehostamaan palveluaan. Vahingollisten tietovuotojen lisäksi on kuitenkin muita skenarioita, joissa kerätty tieto on mahdollinen uhka.

Yksi esimerkki uhkaavasta tiedonkeräämisestä on Kiinan valvontatavat. Maassa jokaista valvotaan. Jopa väliaikaisesti maahan tulevia henkilöitä tarkkaillaan lataamalla näiden puhelimeen sovellus, joka etsii esimerkiksi Quran tekstejä. Ihmisiä jopa kannustetaan seuraamaan naapuriensa toimintaa. Sen lisäksi, ettei ihmisillä tunnu olevan omaa yksityisyyttä, tilanne vain pahenee, kun kaikkea kerättyä tietoa käytetään kontrolloimaan ja uhkaamaan väestöä. Yksi esimerkki tästä on Kiinan vakoilu Xingjiang alueella; alueella asuu paljon eri muslimi vähemmistöistä väkeä. Raporttien mukaan auktoriteetti käyttää edistynyttä teknologiaa analysoimaan väkeä QR koodien, biometrien, tekoälyn, suuren datan ja jopa suoraan vakoilun avulla. (HRW, 2018; Khandelwal 2019.)

Kiina ei kuitenkaan ole ainoa, joka syylistyy ihmisten vakoiluun ja identifiointiin internetin avulla. Myös Amerikassa vuonna 2020 George Floydin murhan ja tämän jälkeisten protestien jälkeen paljastui, että poliisivoimat olivat kehittäneet työkalun, jonka avulla seuloivat sosiaalisen median läpi etsiessään tunnisteita protesteissa olleista henkilöistä. Tätä laaja-alaista työkalua käytettiin myös seuraamaan ihmisiä heidän puhelimiensa kautta ja lähettämään tämän tiedon takaisin viranomaisille; olivat nämä henkilöt rikosepäiltyjä tai ei. (Ryan-Mosley & Richards 2022.)

5.3 Tietovuotojen uhat

Tietovuoto on tapahtuma, kun hakkeri pääsee käsiksi käyttäjän, palvelun tai yrityksen tietoihin ja julkaisee nämä. Kyseessä voi olla esimerkiksi käyttäjätunnuksia ja salasanoja, tai mahdollisesti

arkaluontoisempaa tietoa kuten henkilötunnuksia, osoitteita tai maksukorttitietoja. (F-secure 2022.)

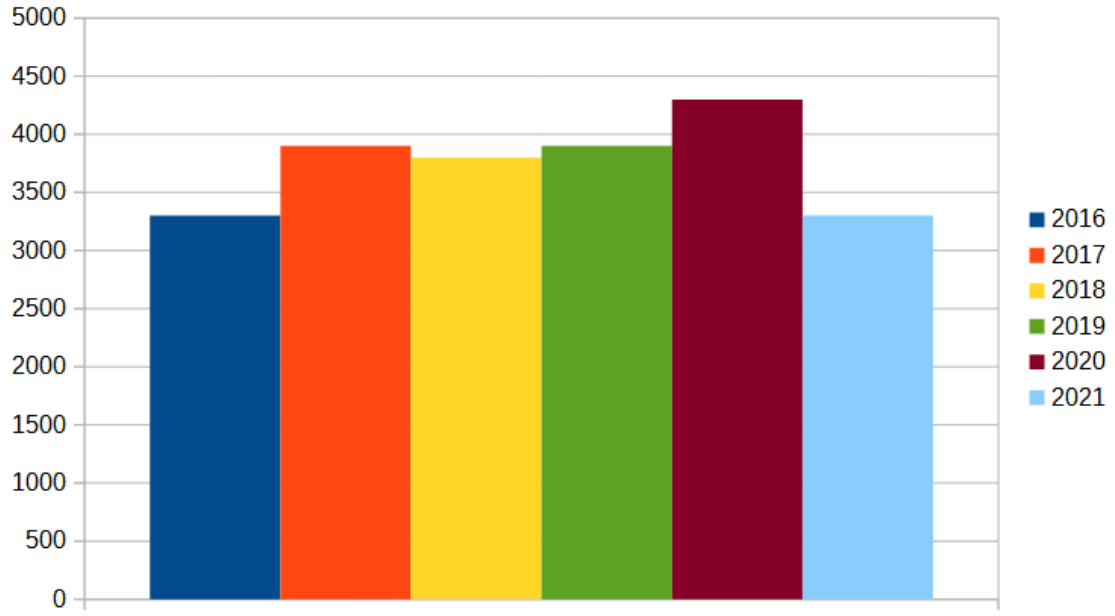
Varastetuilla henkilötiedoilla voi saada monenlaista harmia aikaiseksi. Toisen henkilötietojen käyttämisestä käytetään yleisesti termiä identiteettirikos, mutta itse tekoja on monenlaisia. Kaikkia rikoksia kuitenkin yhdistää harmin tai vahingon aiheuttaminen uhrille tekojen kautta. Toisen käyttäjätunnuksien käyttö, tiedonkalastelu, toisen nimellä kirjoitetut sähköpostit ja someviestit, kaikki nämä lasketaan identiteettivarkauksiksi. Ei siis ole ihme, että identiteettirikoksien numero on suuri ja tulkinnan mukaan jopa yleisin rikos Suomessa, varsinkin kun rikos on sinänsä vielä uusi Suomen rikoslaissa. Vuonna 2009 identiteettirikoksia ei ollut vielä kriminalisoitu Suomen rikoslaissa; muutos tähän tuli vasta vuonna 2015. (Järvinen 2022, 166; Yle 2009; Rikoslaki 368/2015, 9 a §.)

Tilauspetokset ovat identiteettirikoksia, joissa hyväksikäytetään muiden tietoja pettämään kauppakäynnissä. Tyypillisessä tilauspetoksessa uhrin varastettuja tietoja käytetään esimerkiksi avaamaan puhelinliittymiä, tekemään ostoksia osamaksulla, avaamaan pankkitilin uhrin nimin tai jopa nostamaan pikavippejä. Laskut tietenkin menevät uhrille- ja pahimmassa tapauksessa huijari on voinnut tehdä osoitteenmuutoksen, jolloin petoksen löytöön voi mennä jopa kuukausia. (Järvinen 2022, 169.)

Yksi esimerkki viimeaikaisesta tietovuodosta Suomessa on psykoterapiakeskus Vastaamon tietovuoto. Huonojen tietoturvakäytäntöjen takia hakkeri -tai useampi- oli pääsyt käsiksi terapiakeskuksen tietokantoihin. Vasta vuonna 2020 kun itse tietovuoto tapahtui tuli ilmi, että ulkoinen osapuoli oli pääsyt tietokantoihin jo vuosina 2019 ja 2018. Murrosta oli jo aikaa, jonka takia syyllisen löytäminen oli hankalaa. Tietomurron tapahtuessa tärkeintä olisi aina toimia nopeasti. Vastaamo ei kuitenkaan tehnyt mitään vuonna 2018 -oli syynä, että murto jäi huomaamatta tai ei- ja tämän takia potilaiden arkaluontoisia tietoja päätyi vääriin käsiin. Hakkeri ensin yritti kiristää itse terapiakeskusta, mutta kun tämä ei toiminut hän siirtyi nettiin. Täällä hän myi tietoja eteenpäin heille, jotka niistä maksoivat. Osat uhreista kävivät itse maksamassa, jotta heidän tietonsa poistettaisiin pysyvästi dokumentista. Jotkut ihmiset vuorostaan käyttivät tilaisuutta hyväkseen; nähdessään tilaisuuden kostoon, yksi anonyymi käyttäjä kommentoi näin: ”...Jos ei nyt vuodon vuoksi ajaudu itsemurhaan niin ehkäpä saan tehtyä sen elämästä yhtä helvettiä koko loppuelämän ajaksi.” Kommenteissa oli myös väkeä huolissaan läheisistään ja jotkut vuorostaan kokivat tämän hetkeksi kritisoida potilaita, kuinka ”joillakin on helvetin helppo elämä, kun pitää mennä kallonkutistajalle lähinnä itkemään”. Tietovuodossa ei siis pelkästään ollut uhka tietojen väärinkäytöstä esimerkiksi tilaus- tai identiteettirikokseen, vaan myös ihmisten terveys, sosiaalinen elämä, pelot ja omat henkiset kamppailut olivat paljastettuna muille. Ei ole

myöskään yllätys, että jotkut kommenteissa totesivat, etteivät tämän jälkeen haluaisi enää ikinä puhua ongelmistaan muille. (Järvinen 2022, 108-115.)

Identiteettirikokset voidaan vielä laskea melko uudeksi lisäykseksi rikoslaissa. Kriminalisointi on kuitenkin tuonut lisää tietoisuutta aiheelle, mikä myös näkyy rikosten raportoinnissa vuosien aikana, kuten tilastokeskuksen avulla tehdyssä kaaviossa esitetään. Vuoden 2020 ja 2021 välisen ajan muutoksen luultavasti selittää korona tilanne. Kuva 4 ei silti välttämättä esitä tilannetta todellisesti, sillä identiteettirikoksen kohteeksi joutumista monesti pidetään nolona ja ei välttämättä tämän takia ilmoiteta.



Kuva 4: Raportoitujen identiteettirikosten määrät (Lähde: Tilastokeskus)

6 MITEN OMAN YKSITYISYYDEN INTERNETISSÄ VOI TURVATA?

Omaan yksityisyyteen voi parhaiten vaikuttaa ymmärtämällä mihin voi laittaa luottamuksensa tietojensa kanssa ja mihin ei. Parantamaan käyttäjien ymmärrystä on tärkeää lisätä opetusta tietoturvasta, tähän liittyvistä laeista ja omien tietojen käytöstä. Myös yksityisyyttä painostavien organisaatioiden ja ohjelmien tukeminen auttaa luomaan turvallisempaa internettiä. Monissa lähteissä toistettu hyvä sanonta on vastaava: “Jos laite tai ohjelma on ilmainen voit olettaa, että yksityisyytesi ja tietosi käyttäjänä ovat hinta.”

6.1 Lisää opetusta tietoturvasta

Tärkeä aloituskohta yksityisyyden lisäämiselle on tietoturvan opettamisen lisäys. Puhe tietoturvasta kuitenkin harvoin tuodaan esille peruskäytön aikana- etenkin sosiaalisessa mediassa, missä käyttäjiä jopa kannustetaan jakamaan tietoa itsestään ja omasta elämästä ja kaikki käyttäjäehdot hyväksytään ilman lukemista. Vuonna 2018 Yhdysvalloissa tehty tutkimus paljasti, että kahdestatuhannesta käyttäjästä 91% hyväksyy käyttö- ja oikeudelliset ehdot ilman niiden lukemista, nuoremmassa käyttäjäkunnassa prosentin olevan vielä korkeampi 97%. Syitä tähän on tekstin pituus, käytetyn termistön monimutkaisuus ja myös tapauksia, missä päivitetyt ehdot hyväksytään, koska on jo palvelun aktiivinen käyttäjä. (Obar & Oeldorf-Hirsch 2018.)

Monilukutaito on aina vain tärkeämpi kyky ja tästä on hyvä opettaa kaikille ikäluokille. Lasten ja nuorten kanssa tietoturvasta opettaminen tukee myös vuorovaikutustaitoja. Miten käyttäytyä ja puhua internetissä, mitä internetissä on ja voiko kaikkeen uskoa, mitä voi kertoa tai jakaa itsestä sekä perusteita omien laitteiden ja tilien turvallisuudesta, kuten vahvan salasanan valitseminen. Tutustumalla erilaisiin ohjelmiin ja viestintäteknologisiin laitteisiin luo hyvät perusteet. Oppimista voi myös toteuttaa monessa eri muodossa kotona tai koulussa. Kyberturvallisuuskeskus tarjoaa lapsille suunnatun tietoturvaoppaan, joka opettaa tietoturvasta erilaisten tehtävien avulla. Tietoturvaopetus on myös otettu huomioon SOG (School of Gaming)in toiminnassa. Pelillistämällä tietoturvan aiheita lapset oppivat mieluisan toiminnan yhteydessä.

Internet on aina muuttuva, joten myös aikuisten on tärkeä opettaa itseään muuttuvassa ympäristössä. Lähteitä on monia, mutta on tärkeää myös olla tarkka näiden ohjeiden tai muiden kertomien tietojen varmuudesta. Spreadprivacy.com on Duck Duck Go, inc:in luoma blogi, johon on kerätty monia vinkkejä ja käytäntöjä, joiden avulla voi paremmin suojella omaa yksityisyyttään.

Tähän kuuluu vinkkejä laitteiden ja hakujen suojaamiseen sekä erilaisia tutkimuksia yksityisyyteen liittyen.

Seniorikäyttäjien keskuudessa on hyvin erilaisia kokemuksia internetin ja tämän palveluiden sekä sovelluksien käytöstä. Jotkut eivät välttämättä osaa käyttää laitteita ja toiset ovat käyttäneet tietokoneita esimerkiksi töissä. Riippuen käyttöhistoriasta on tärkeää opettaa senioreille laitteista monipuolisesti. Termistö kuten Wi-Fi, ISP, lataaminen ja evästeet voivat olla täysin tuntemattomia. Yle uutisten haastattelema Pohja Seppo toimii Mukanetti ry:llä, missä tarjotaan vertaistukea ja opetetaan laitteiden käyttämistä ja tämän myötä myös muita internetin käyttöön kuuluvia kykyjä ikäihmisille. Saman kaltaisia senioreiden tietotekniikkayhdistyksiä on Suomessa yhteensä neljä. Pohjan mukaan digitalisoituminen on tapahtunut liian nopeaa ja mennyt jopa ikäsyrjinnän puolelle. Kaikki palvelut ja jopa ajanvaraukset päästäkseen paikanpäälle tehdään internetin kautta, ja ikäihmiset unohdetaan, kun palveluita ja uusia laitteita suunnitellaan. Laitteiden näytöt ovat liian pieniä tai muuten hankalia silmille, sivustojen tekstit ja eri painikkeet ovat liian pieniä. Vähemmän harjoitettujen medialukutaitojen takia vanhempi käyttäjä ei välttämättä myöskään tunnista kalasteluviestiä tai väärää kirjautumissivua, joka mahdollisesti johtaa tietojen, tilin tai rahan varastamiseen. Lisäämällä tietoisuutta näistä vertaistukiryhmistä ja kannustamalla myös muita auttamaan, ikäihmisten medialukutaitoa ja turvallisia käytäntöjä netissä pystyttäisiin parantamaan. (Paajanen 2022.)

6.2 Open source sekä yksityisyyttä panostavat organisaatiot ja ohjelmat

Open source (suom. Avoin lähdekoodi) viittaa ohjelmaan, jonka lähdekoodi on julkisesti saatavilla. Tämä julkisuus vähentää ohjelmien salaisten haitallisuuksien riskin, sillä kaikki toiminnot ja koodin sisällöt ovat julkisesti luettavissa.

Firefox on avoimeen lähdekoodiin perustuva selain, joka panostaa yksityisyyteen. Selaimen luonut ohjelmistoyhteisö Mozilla on itse luonut lähdekoodin ja mainitsee manifestissään ylläpitävän aatetta, että käyttäjien turvallisuus ja yksityisyys internetissä ovat olennaisia ominaisuuksia, eikä niitä pidetä vapaaehtoisina (Mozilla 2009). Firefox selaimeen kuuluu myös automaattisesti tehostettu suojaus seuraimilta ja käyttäjä pystyy itse päättämään tämän vahvuudesta halutessaan.

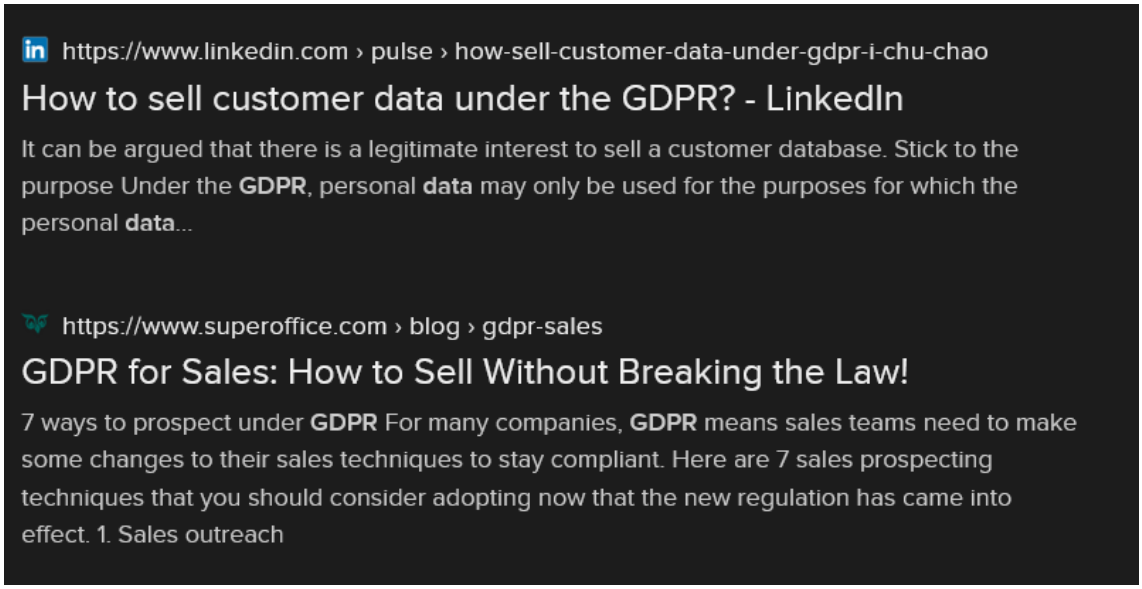
DuckDuckGo on 2008 perustettu yksityisyyteen panostava yritys, joka tarjoaa monia erilaisia palveluja. Näistä tunnetuin on yrityksen hakukone, joka lupaa, ettei koskaan tallenna käyttäjiensä selaustietoja. Hakukone käyttää vain tarvitut tiedot, eikä tallenna näitä. Yritys tarjoaa myös lisäosia ja sovelluksia selaimiin ja älypuhelimiin.

EFF (Electronic Frontier Foundation) on 1990-luvun aikana perustettu organisaatio, joka on alusta asti pitänyt teknologian saavutettavuutta tärkeänä. Organisaatio tarjoaa käyttäjille useita lisäosia selaimeen oman yksityisyyden tukemista varten ja toimii aktivistina ja opettajana monissa internettiin ja teknologiaan liittyvissä aiheissa. (EFF 2007.)

7 JOHTOPÄÄTÖKSET

Yksityisyyden väheneminen internetissä pohjautuu pariin päätekijään. Näistä suurin yhteinen tekijä on tiettyjen yritysten kasvaminen jäteiksi; kuten esimerkiksi Google, Facebook ja Microsoft. Yritysten laajuuden takia näiden sovellukset, ohjelmat ja palvelut ovat monien käyttäjien ja myös laitteiden ja yritysten oletuksena. Tämä luo eräänlaisen effektin, jonka myötä yhden henkilön on hankalempi vaihtaa toiseen ohjelmaan- esimerkkinä tästä vaihto Facebookin WhatsAppista toiseen chat-palveluun. Jos käyttäjä ei onnistu saaman muita mukaan ohjelmanvaihtoon tämä jäisi yksin, koska WhatsApp ei tue keskustelua eri chat-palveluiden välillä. Sama pätee myös työelämässä ja töissä käytettyihin ohjelmiin ja sovelluksiin. Tämän myötä syntyy myös ympäristö, missä pienemmät yritykset ja näiden palvelut tai sovellukset eivät ole läheskään yhtä tunnettuja. Vähäisen monetisaation takia pienemmät yritykset päätyvät hyödyntämään jättien palveluja, siten tukien näiden käytäntöjä.

Yritykset myös löytävät porsaanreikiä asetetuista säännöistä. GDPR pyrki antamaan käyttäjälle oman yksityisyytensä kontrolloinnin voiman; vaikka tämä onnistui joissan määrin, laki ei ollut täydellinen. Käy ilmi, että suuri osa väestä ei edes lue käyttöehtoja tämän pitkäjänteisyyden takia ja pitävät tätä ärsyttävänä ekstra askeleena aloittamisen edessä. Helppokäyttöisyys päihittää muun. Tämän myötä yritykset voivat vedota saanneen haluamansa luvan käyttäjältä sen lisäksi, että heillä on GDPR:n mukainen oikeutettu syy tiedon keräämiseen ja myyntiin, kuten kuva 5 esittää.



Kuva 5: Kuvakaappaus hakukoneesta: selling data GDPR compliant

Teknologian kehittyminen ja tiedonkeruu ei omina konsepteinaan ole paha asia. Se on, kun yritykset hyväksikäyttävät näitä myyntiä varten, ongelmat alkavat. Assistentit ja eri älylaitteet voivat olla monelle hyödyksi ja jopa tehdä elämästä helpompaa. Tarpeellinen tiedonkeruu tapahtuisi vain keräämällä tarvittava data palvelun suorittamista ja kehittämistä varten. Aivan liian usein dataa kuitenkin kerätään niin paljon, että sen mahdollisesti luotava linkki käyttäjän oikeaan identiteettiin on mahdoton perua (Cox 2020). Tiedonkeruulla on hieno raja, mikä identifioi käyttäjän ja mikä ei.

Digitalisoitumisen nopeus on toinen tekijä. Muutos digitaalisessa ympäristössä on tapahtunut niin nopeasti, että monella ei ole muuta vaihtoehtoa kuin vain mennä muiden perässä. Laitteet vanhenevat nopeammin kuin koskaan ennen ja oman käyttäjäkokemuksen modifioinnista ei enää puhuta yhtä paljon, vaan palvelut uskotaan täydellisesti räätälöidyksi alusta asti. Digitalisoituminen on yhdessä ääripäässä kasvattanut käyttäjiä hyväksymään kaikki termit mitä palvelu tarvitsee ja toisessa ääripäässä jättänyt väkeä ilman tukea uuden oppimiseen, joka luo ongelmia, kun kaikki palvelut siirtyvät internettiin.

Yksityisyys internetissä on vähäistä, kun jätit tuntuvat kontrolloivan jokaista aluetta. On kuitenkin olemassa organisaatioita ja yrityksiä, jotka haluavat tukea ja vahvistaa käyttäjien oikeutta yksityisyyteen.

8 POHDINTA

IoT ja teknologian kehittyminen on tehnyt monista käytännöistä helppoa. Jopa niin helppoa, että moni käyttäjä päätyy valitsemaan helppokäyttöisyyden yksityisyyden sijasta. On paljon nopeampaa ottaa laite tai ohjelma käyttöön perusasetuksilla, kuin lähteä tutkimaan ja muuttamaan asetuksia, joka hidastaa käyttöönottoa. Windows 10 ja muut Windows järjestelmät ovat monesti jo ladattuna tietokoneisiin mikä tekee tästä helpompaa, kuten esimerkiksi Linuxin käyttöönoton, joka riippuen versiosta voi tarvita enemmän tai vähemmän teknistä tietoa latausta ja asentamista varten. Älylaitteiden tai muiden ohjelmistojen kohdalla voi tapahtua myös niin sanottua pelottelua, jossa kerrotaan, että tiettyjen asetusten muuttaminen tai osien poistaminen voi vahingoittaa laitetta tai ohjelmaa, tai modifiointi voi viedä oikeudet takuuseen tai vastaavaa.

Tietokoneiden ja muiden laitteiden käytössä tuntuu tapahtuneen eräänlainen taaksepäin kääntyminen; ennen tietokoneet olivat vain harvojen IT-alan tietäjien käytössä. Tietokoneiden käytön lisääntyessä laitteista pyrittiin tekemään helppokäyttöisiä kaikille ja nyt olemme eräänlaisessa hybriditilassa. Koneet ovat helppo ottaa käyttöön, mutta oman kokemuksen, asetusten ja vastaavien muokkaamista enemmän, kuin pintatasolla taas ajatellaan olevan vain harvojen tietävien tehtävissä. Helppokäyttöisyyttä ja uusia hienoja ominaisuuksia kuten puheentunnistamista ja tekoäly-teknologioita heilutellaan käyttäjien silmien edessä samalla, kun yritykset pyrkivät piilottamaan mitä kaikkea näiden teknologioiden taustalla pyörii. Tietokoneissa on monia taustaprosesseja, jotka pyörivät, vaikka käyttäjä ei tee mitään. Käyttäjällä on pintatasoinen käsitys siitä, että näitä prosesseja tarvitaan koneen ja ohjelmien toimimista varten, mutta ei osaa erottaa mitkä näistä ovat vastaavia ja mitkä ovat ekstraa.

Katsoessani omaa kasvuani ja kiinnostustani tietoturva-alaan, vain yksi asia tulee mieleen: missä on digitalisoitumisen raja? Teknologiaa kehitetään koko ajan eräänlaisessa kisassa hakkeroiden tietämystä vastaan- kannattaako siis kaiken tiedon ja vuorovaikutuksen digitalisointia jatkaa ikuisuuteen? Internetin käytön laajuus on tehnyt siitä täydellisen potin rikollisille ja arkaluontoisten tietojen ja erilaisten transaktioiden läpikäyminen internetissä ja tämän laitteissa vaan lisää tätä.

”Yritykset keräävät niin paljon dataa, ei kukaan keskity minun tietoon yksinään” tai ”ei minun data tee mitään eroa” on ajatustapa johon törmäsin tutkinnan aikana. Yksinkertaisesti sanottuna: tämä ajattelutapa huolestuttaa minua kovasti. Tämä ”ihan sama” -ajattelu mitä luultavammin myös vaikutti siihen miten paljon dataa Googlen ja Facebookin kaltaiset yritykset ovat pystyneet kerätä.

Mainitsin tutkimuksessa lyhyesti, kuinka Windows 10:n taustasovelluksetkin keräävät dataa johonkin asteeseen asti. Tämä internetin ja laitteen yhdistyminen olisi myös kiinnostava tutkinnan aihe; onko laajasta internetistä erotettu kone ainoa täysin vapaa, ilman tiedonkeräilyä?

LÄHTEET

Agency central 2013. What did recruitment look like before the internet? Hakupäivä 11.2.2022. https://www.agencycentral.co.uk/articles/10-2013/what-did-the-world-of-recruitment-look-like-before-the-dawn-of-the-internet.htm

Ahonen, Paavo & Kolari, Jukka 1994. Internet OS/2 Warp -opas. Jyväskylä: Teknolit OY

Akhtar, Aazim 2020. Google Ads: What are they and how do they work (A simple guide). Monsterinsights. Hakupäivä 23.4.2022. https://www.monsterinsights.com/google-ads/

Bilgil, Youtube 2009. History of the Internet. Hakupäivä 17.12.2021. https://www.youtube.com/watch?v=9hIQjrMHTv4

Chakraborty, Kuntal 2021. What is web 1.0? - Definition from Techopedia. Techopedia. Hakupäivä 25.2.2022. https://www.techopedia.com/definition/27960/web-10

Choosetoencrypt 2020. Is Snapchat Privacy-Friendly? [Analysis] Hakupäivä 8.4.2022. https://choosetoencrypt.com/privacy/is-snapchat-privacy-friendly/

Cortada, James W 2016. How Americans found information before the internet. Hakupäivä 20.1.2022. https://blog.oup.com/2016/10/americans-information-google/

Cox, Josepth 2020. Leaked documents expose the secretive market for your web browsing data. Vice. Hakupäivä 21.4.2022. https://www.vice.com/en/article/qjdkq7/avast-antivirus-sells-user-browsing-data-investigation

Cyphers Bennett 2021. Google Is Testing Its Controversial New Ad Targeting Tech in Millions of Browsers. Here's What We Know. EFF. Hakupäivä 21.4.2022. https://www.eff.org/deeplinks/2021/03/google-testing-its-controversial-new-ad-targeting-tech-millions-browsers-heres

Dinita, Madalina 2021. Stop Facebook from tracking your Internet activity. Technipages. Hakupäivä 12.4.2022. https://www.technipages.com/stop-facebook-from-tracking-your-internet-activity

EFF 2007. About EFF. Hakupäivä 23.4.2022. https://www.eff.org/about

F-Secure 2022. Selvitä, ovatko henkilökohtaiset tietosi vuotaneet nettiin. Hakupäivä 24.3.2022. https://www.f-secure.com/fi/home/free-tools/identity-theft-checker

G Nick, Techjury 2021. How many IoT devices are there in 2021? Hakupäivä 15.12.2021. https://techjury.net/blog/how-many-iot-devices-are-there/

Hill, Simon 2015. Are cookies crumbling our privacy? We asked an expert to find out. Digitaltrends. Hakupäivä 26.3.2022. https://www.digitaltrends.com/computing/history-of-cookies-and-effect-on-privacy/

Holmes, Insider 2021. 533 million facebook users' phone numbers and personal data have been leaked online. Hakupäivä 16.12.2021. https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4?op=1&r=US&IR=T

HRW (Human Rights Watch), 2018. China: Massive crackdown in Muslim Region. Hakupäivä 24.3.2022. https://www.hrw.org/news/2018/09/09/china-massive-crackdown-muslim-region

Innes, Matthew 2021. What is Spyware? Security Gladiators. Hakupäivä 17.3.2022. https://securitygladiators.com/threat/spyware/

Janssen, David 2022. The privacy risks of TikTok- Why this invasive app is so dangerous. Vpnoverview. Hakupäivä 19.4.2022. https://vpnoverview.com/privacy/social-media/tiktok-privacy/

Järvinen, Petteri 2022. Digiajan tietosuoja. Helsinki: Tammi.

Kelly, Makena & Statt, Nick. Amazon confirms it holds on to Alexa data even if you delete audio files. Theverge. Hakupäivä 7.4.2022. https://www.theverge.com/2019/7/3/20681423/amazon-alexa-echo-chris-coons-data-transcripts-recording-privacy

Kortelainen, Hannu 2020. Rakkaushuijaus: Tästä se yleensä lähtee. Helsingin rikostutkinta. Poliisi. Hakupäivä 2.2.2022. https://poliisi.fi/blogi/-/blogs/rakkaushuijaus-tasta-se-yleensa-lahtee

Krakau, Tarja & Haapalehto, Saija 2020. Tietopyynnöt ja henkilötietojen luovuttaminen. Helsinki: Alma Talent Oy.

Lechner, Paul 2020. GDPR: Three ways the world has changed in the privacy law's first two years. Cpomagazine. Hakupäivä 19.4.2022. https://www.cpomagazine.com/data-protection/gdpr-three-ways-the-world-has-changed-in-the-privacy-laws-first-two-years/

Malwarebytes 2022. Spyware – What is it & how to remove it? Hakupäivä 17.3.2022. https://www.malwarebytes.com/spyware

Monnappa, Avantika 2022.. The history and evolution of digital marketing. Simplilearn. Hakupäivä 10.3.2022. https://www.simplilearn.com/history-and-evolution-of-digital-marketing-article

Mozilla 2009. The Mozilla Manifesto Addendum. Hakupäivä 23.4.2022. https://www.mozilla.org/en-US/about/manifesto/

NationSquid, Youtube 2021. BonziBuddy - The Internet Spyware That Plagued Windows (Demonstration). Hakupäivä 17.3.2022. https://www.youtube.com/watch?v=nCGD92DDsvc

Nield, David 2020. All the ways Facebook tracks you- And how to limit it. Wired. Hakupäivä 12.4.2022. https://www.wired.com/story/ways-facebook-tracks-you-limit-it/

Nita, Adrian 2021. Is Amazon's Alexa spying on you? MakeUseOf. Hakupäivä 7.4.2022. https://www.makeuseof.com/is-amazon-alexa-spying-on-you/

Obar, Jonathan A & Oeldorf-Hirsch Anne 2018. The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services. Hakupäivä 23.4.2022. https://ssrn.com/abstract=2757465

Paajanen Salla 2022. Seppo Pohja, 69, auttaa vapaaehtoisena muita senioreita kun salasanat on hukattu ja älypuhelin ei toimi: "Ihmiset hakevat apua itku kurkussa". Yle uutiset. Hakupäivä 23.4.2022. https://yle.fi/uutiset/3-12388362

Peters, Jay 2019. The reflections in a pop star's eyes told a selfie stalker exactly how to find her. Theverge. Hakupäivä 16.2.2022. https://www.theverge.com/2019/10/11/20910551/stalker-attacked-pop-idol-reflection-pupils-selfies-videos-photos-google-street-view-japan

Powell, Anastasia, Scott, J Adrian & Henry, Nicola 2018. Digital harassment and abuse: Experiences of sexuality and gender minority adults. Sagepub. Hakupäivä 17.2.2022. https://journals.sagepub.com/doi/full/10.1177/1477370818788006

Quidsup, Youtube 2016. Windows 10 spying is worse than I ever imagined. Hakupäivä 24.3.2022. https://www.youtube.com/watch?v=RVzc5wK2-pc

Rikoslaki 368/2015. Hakupäivä 31.3.2022. https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001?search%5Btype%5D=pika&search%5Bpika%5D=Identiteettivarkaus#a10.4.2015-368

Ryan-Mosley, Tate & Richards, Sam. The secret police: Cops built a shadowy surveillance machine in Minnesota after George Floyd's murder. Technologyreview. Hakupäivä 8.4.2022. https://www.technologyreview.com/2022/03/03/1046676/police-surveillance-minnesota-george-floyd/

Suomen Evankelis-Luterilainen kirkko 2016. Sukututkimus. Hakupäivä 20.1.2022. https://evl.fi/tietoa-kirkosta/kirkko-ja-yhteiskunta/sukututkimus

Sushko, Olga 2021. What is online privacy and why does it matter? Clario. Hakupäivä 28.1.2022. https://clario.co/blog/what-is-online-privacy/

Techopedia 2012. What is Network Control Protocol (NCP)? Hakupäivä 11.1.2022. https://www.techopedia.com/definition/27856/network-control-protocol-ncp

Temming, Maria 2018. Smartphones put your privacy at risk. Sciencenewsforstudents. 8.4.2022. https://www.sciencenewsforstudents.org/article/smartphones-put-your-privacy-risk

Tilastokeskus 2018. Julkisuuslaki. Hakupäivä 10.3.2022. https://www.tilastokeskus.fi/meta/lait/julkisuuslaki.html

UWA Online 2019. The Evolution and History of Digital Marketing. Hakupäivä 27.2.2022. https://online.uwa.edu/news/history-of-digital-marketing/

Websitebuilders 2017. What Is Web 1.0? A History Lesson About The Early Stages Of The World Wide Web. Hakupäivä 25.2.2022. https://websitebuilders.com/how-to/glossary/web1/

Yle uutiset 2009. Identiteettivarkaus on Suomessa toistaiseksi tuntematon rikos. Hakupäivä 31.3.2022. https://yle.fi/uutiset/3-5293044