VRIJE
UNIVERSITEIT
BRUSSEL

Proef ingediend met het oog op het behalen van de graad van
Master of Science in de Communicatiewetenschappen

Digitale berusting in een tijd van privacy onzekerheid

Femke Laura TINKL
0555887
Academiejaar 2019-2020

Promotor: Jo Pierson
Jury: Karl Verstrynge
Sociale Wetenschappen & Solvay Business School

VRIJE UNIVERSITEIT BRUSSEL

VERKLARING VAN AUTHENTICITEIT

De ondertekende verklaring van authenticiteit is een integrale component van het geschreven werk (Bachelorproef of Masterproef) dat wordt ingediend door de student.

Met mijn handtekening verklaar ik dat:

- ik de enige auteur ben van het ingesloten geschreven werk[1];
- ik dit werk in eigen woorden heb geschreven;
- ik geen plagiaat heb gepleegd zoals gedefinieerd in artikel 118 van het Onderwijs- en Examenreglement van de VUB; waarbij de meest voorkomende vormen van plagiaat zijn (niet-limitatieve lijst):
  - aard 1: tekst overnemen van andere auteurs, weliswaar met bronvermelding maar zonder gebruik van aanhalingstekens waar het om een letterlijke overname gaat;
  - aard 2: tekstfragmenten overnemen van andere auteurs, al dan niet letterlijk, zonder bronvermelding;
  - aard 3: verwijzen naar primair bronmateriaal waar de tekst en bronvermelding al dan niet letterlijk wordt overgenomen uit niet-vermelde secundaire bronnen;
  - aard 4: tekstfragmenten overnemen van andere auteurs, al dan niet met bronvermelding, met geringe en/of misleidende tekstaanpassingen.
- ik in de tekst en in de referentielijst volledig heb gerefereerd naar alle internetbronnen, gepubliceerde of ongepubliceerde teksten die ik heb gebruikt of waaruit ik heb geciteerd;
- ik duidelijk alle tekst heb aangeduid die letterlijk is geciteerd;
- ik alle methoden, data en procedures waarheidsgetrouw heb gedocumenteerd;
- ik geen data heb gemanipuleerd;
- ik alle personen en organisaties heb vermeld die dit werk hebben gefaciliteerd, dus alle ingediende werk ter evaluatie is mijn eigen werk dat zonder hulp werd uitgevoerd tenzij uitdrukkelijk anders vermeld;
- dit werk noch een deel van dit werk werd ingediend aan een andere instelling, universiteit of programma;
- ik op de hoogte ben dat dit werk zal gescreend worden op plagiaat;
- ik alle origineel onderzoeksmateriaal onmiddellijk zal indienen op het Decanaat wanneer hierom wordt gevraagd;
- ik op de hoogte ben dat het mijn verantwoordelijkheid is om na te gaan dat ik word opgeroepen voor een hoorzitting en tijdens de periode van hoorzittingen beschikbaar te zijn;
- ik kennis genomen heb van artikel 118 van het Onderwijs- en Examenreglement van de VUB omtrent onregelmatigheden en dat ik op de hoogte ben van de disciplinaire sancties;
- de afgedrukte kopie die ik indiende identiek is aan de digitale kopie die ik oplaadde op Turnitin.

Tekst

Student familienaam, voornaam: Tinkl Femke **Datum:** 7 juni 2020

Handtekening: Tinkl Femke

[1] Voor groepswerken zijn de namen van alle auteurs verplicht. Hun handtekeningen staan collectief borg voor de volledige inhoud van het geschreven werk.

VRIJE
UNIVERSITEIT
BRUSSEL

AFGIFTE- / ONTVANGSTBEWIJS MASTERPROEF

Persoonsgegevens:
Naam + voornaam: TINKL Femke Laura
Rolnummer: 0555887
Opleiding: Communicatiewetenschappen

Titel van de masterproef zoals op het voorblad van het ingediende werk:
Digitale berusting in een tijd van privacy onzekerheid

Engelse vertaling van de titel (verplicht):
Digital resignation in the age of privacy uncertainty

Naam: **Handtekening:**

Vak voorbehouden voor medewerker faculteitssecretariaat:

De student heeft zijn/haar Masterproef ingeleverd op

Datum van afgifte: .....

Naam ontvanger: .....

Abstract

In deze masterproef wordt er een onderzoek gevoerd naar het topic privacy. De hoofdonderzoeksvraag die daarbij gesteld werd, is:

> Welke factoren dragen bij aan de digitale berusting van Belgische privacy geletterden en niet-privacy geletterden en hoe kan dat bestreden worden?

Om een antwoord te kunnen formuleren op deze onderzoeksvraag werd er gebruik gemaakt van kwalitatieve interviews. Respondenten werden daarbij bevraagd naar hun online gedrag en naar hoe zij online omgaan met hun eigen privacy. Elk van de respondenten werd voorafgaand aan het interview onderworpen aan een test waarbij nagegaan werd in hoeverre zij privacy geletterd en/of digitaal berust zijn.

Uit de resultaten van de tests en van de interviews kunnen er verschillende conclusies worden getrokken. Er zijn namelijk verschillende factoren die bijdragen aan een gevoel van digitale berusting. Een eerste grote cluster aan factoren centreert zich rond de strategieën van bedrijven. Zo zijn privacyverklaringen onduidelijk en te academisch, blijkt er onvoldoende transparant te worden gecommuniceerd en sturen bedrijven gebruikers vooral aan op het minder beschermen van de privacy. Natuurlijk spelen niet alleen bedrijven een rol. Ook wetgevingen blijken niet aan de wensen te voldoen en zijn vandaag niet effectief genoeg. Er zijn daarnaast echter nog andere elementen. Zo is het een gewoonte geworden om zaken die gebeuren met onze privacy te accepteren, kunnen we niet meer zonder digitale media, is er geen overzicht meer, hebben we geen zin of geen tijd en zijn we onwetend of hebben we een vals gevoel aan vertrouwen.

Een belangrijk aspect dat naar boven kwam in dit onderzoek, is dat er geen strak onderscheid gemaakt kan worden tussen personen met een hoger of lager niveau van privacy geletterdheid. Er zijn absoluut een aantal verschillen, maar sommige lagere privacy geletterden vertonen op bepaalde vlakken kenmerken van hogere privacy geletterden en omgekeerd. Nuance is key!

Hoe pakken we dit nu aan? Sensibilisering, opleidingen en het aanpakken van privacyverklaringen en transparantie zijn absoluut noodzakelijk.

Aantal woorden excl. titelbladen, abstract, inhoudstafel, bijlagen en quotes uit de interviews:
22 182

Voorwoord

In deze masterproef staan de onderwerpen privacy en digitale berusting centraal. Deze topics werden gekozen naar aanleiding van een vraag die ik mezelf stelde, namelijk waarom probeer ik mijn privacy niet beter te beschermen terwijl ik dat eigenlijk wel zou willen. Daarbij was het mijn doel als onderzoeker om te weten te komen wat er aan de basis ligt van dat gedrag. Mijn opleiding Communicatiewetenschappen met afstudeerrichting Media, Strategische Communicatie en Marketing, die ik volg aan de Vrije Universiteit Brussel, gaf me de kans om dat fenomeen te onderzoeken.

Deze masterproef is (ten dele) tot stand gekomen in de periode dat het hoger onderwijs onderhevig was aan een lockdown en beschermende maatregelen ter voorkoming van de verspreiding van het COVID-19 virus. Het proces van opmaak, de verzameling van gegevens, de onderzoeksmethode en/of andere wetenschappelijke werkzaamheden die ermee gepaard gaan, zijn niet altijd op gebruikelijke wijze kunnen verlopen. De lezer dient met deze context rekening te houden bij het lezen van deze masterproef, en eventueel ook indien sommige conclusies zouden worden overgenomen.

Voor er echter gestart kan worden met het uit de doeken doen van het volledige onderzoek, wil ik allereerst alle personen bedanken die bijgedragen hebben aan het tot stand komen van deze masterproef. Op de eerste plaats komt mijn promotor professor dokter Jo Pierson. Hij begeleidde me in dit proces waarbij hij me hielp met het op punt stellen van mijn onderzoek en ervoor zorgde dat ik bleef focussen op het doel van deze thesis. Bij deze dus hartelijk bedankt professor dokter Jo Pierson!

Natuurlijk wil ik ook de personen bedanken die deel hebben genomen aan de interviews. Zonder hen zou er geen onderzoek zijn geweest en zouden er geen resultaten kunnen worden voorgelegd.

Mijn vrienden en familie verdienen het ook absoluut om hier vermeld te worden. Zij zorgden voor de nodige steun en motivatie. Tot slot wil ik nog iemand in het bijzonder bedanken, namelijk mijn vader. Hij gaf me de kracht om deze masterproef tot een goed einde te brengen.

Veel leesplezier gewenst!
Femke Tinkl

Inhoudsopgave

Lijst met tabellen en afbeeldingen

Tabellen

Lijst met afbeeldingen

Lijst met bijlagen

Interne bijlagen

Aparte bijlagen:

- Transcripties interviews
- Ruwe data test digitale berusting en privacy geletterdheid
- Codeboek

DEEL 1

LITERATUURSTUDIE

1. Inleiding

Het internet en sociale media lijken niet meer weg te slaan uit het dagelijkse leven van mensen (Chen, 2018, p. 1393; Coskun & Karayagız Muslu, 2019, p. 1004; Sarikakis & Winter, 2017, p. 1). Zo blijkt uit de Vlaamse Digimeter van Imec dat Vlamingen 33% van hun smartphonetijd spenderen aan sociale media (Vandendriessche & De Marez, 2019). 79% van de Vlamingen maakt zelfs dagelijks gebruik van een Facebookapp. Veel jongeren lijken namelijk bang te zijn iets te missen, wat tegenwoordig 'FOMO' of 'fear of missing out' wordt genoemd (Coskun & Karayagız Muslu, 2019, p. 1005). Dat wordt tevens aangetoond door cijfers van de Vlaamse Digimeter. 63% van de Vlamingen geeft aan bang te zijn om bepaalde events of bepaald nieuws te mislopen als men geen gebruik maakt van sociale media (Vandendriessche & De Marez, 2019). Maar wat vooral onrustwekkend is in deze ontwikkeling, is het feit dat het concept privacy steeds meer in de vergetelheid raakt. Socialemediaplatformen zoals Facebook en Instagram pikken de sporen op die mensen online achterlaten en gebruiken deze data om hun succesvol business model te voeden (Chen, 2018, p. 1393; Gimpel, Kleindienst, & Waldmann, 2018, p. 475). Een business model waar gebruikers geen gebruikers meer zijn, maar eerder het product dat verkocht wordt. Niet alleen de wetenschappelijke wereld debatteert hierover, ook de maatschappij onderkent het probleem. Zo trad in 2018 de GDPR (De Algemene Verordening Gegevensbescherming) in werking om de gegevens van de Europese burgers te beschermen (The Economist, 2019). Vandaag wordt het thema ook nog steeds besproken omwille van Covid-19. Men zou namelijk persoonlijke data willen gebruiken om na te gaan wie het virus heeft en waar deze personen geweest zijn om zo mogelijke andere besmette personen op te sporen (The Economist, 2020). De komst van de GDPR zorgde voor meer bescherming van de privacy, maar natuurlijk kan de overheid ons niet beschermen tegen alle pogingen die instanties ondernemen om onze data te verzamelen (Vlemings, 2018). Als we niet willen dat er met onze privacy wordt gespeeld, moeten we zelf actie ondernemen, maar doen we dat ook?

Wat in de wetenschap nu als hot topic naar voren komt, is de zogenaamde privacy paradox (Draper & Turow, 2019, p. 1824; Gimpel et al., 2018, p. 475; Kezer, Sevi, Cemalcilar, & Baruh, 2016). Gebruikers van het internet en socialenetwerksites zijn er zich wel van bewust dat hun privacy wordt geschonden en ze willen daar iets aan doen, maar hun bezorgdheid wordt niet omgezet in acties (Draper & Turow, 2019, p. 1825; Kezer et al., 2016). Mensen lijken een soort van hopeloosheid met zich mee te dragen waarbij ze het gevoel hebben dat wat ze ook doen, hun privacy toch niet beschermd kan worden. Dat gevoel wordt in de wetenschappelijke literatuur benoemd als de digitale berusting (Draper & Turow, 2019, p. 1825).

Een vraag die nu gesteld dient te worden, is waarom mensen zich op deze manier voelen. Het onderzoek van Draper en Turow (2019, p. 1830) geeft aan dat de bedrijven achter socialemediaplatformen mee aan de basis van de digitale berusting zouden liggen. Een voorbeeld daarvan is het beleid dat bedrijven omtrent privacy opstellen (Draper & Turow, 2019, p. 1831). Dat beleid is vaak te omslachtig, te uitgebreid en te ingewikkeld om te lezen voor de gebruiker. Als gebruikers het al willen lezen, begrijpen ze er vaak niet veel van (Draper & Turow, 2019, p. 1831).

Wat het onderzoek van Draper en Turow (2019, p. 1834) daarnaast ook stelt, is dat er wel degelijk nog extra onderzoek nodig is naar dit fenomeen. Zo duiden de onderzoekers al aan dat bedrijven mogelijk bijdragen aan het gevoel van digitale berusting, maar dat kan natuurlijk niet de enige oorzaak zijn. Het doel van deze masterproef is dus het achterhalen van de mogelijke aanleidingen van digitale berusting bij mensen. Om dat te weten te komen, is het zeker belangrijk om verder literatuuronderzoek uit te voeren. Tevens zullen kwalitatieve interviews aangewend worden om na te gaan wat een gevoel van digitale berusting voedt. Daarbij zal een onderscheid gemaakt worden tussen personen met een hogere of lagere privacy geletterdheid. In de wetenschappelijke wereld is er namelijk op dit moment nog geen consensus over het helpen van een hogere privacy geletterdheid bij het overwinnen van een gevoel van digitale berusting (Bartsch & Dienlin, 2016; Baruh, Secinti, & Cemalcilar, 2017; Draper & Turow, 2019; Kezer et al., 2016). Sommige onderzoekers stellen namelijk dat privacy geletterdheid mensen kan helpen om over die digitale berusting te komen (Bartsch & Dienlin, 2016, p. 153; Baruh et al., 2017, p. 26). Anderen zoals Kezer et al. (2016) lijken echter totaal niet overtuigd en geven zelfs aan dat leren over privacy mensen absoluut niet aanzet om hun privacy beter af te schermen. Ook het onderzoek van Turow, Hennessy en Draper (2015, p. 3) duidt aan dat mensen, die meer weten over hoe data door marketeers wordt verwerkt, niet per se minder data gaan delen. De vraag die daarbij dan gesteld moet worden is of privacy geletterdheid de digitale berusting net voedt of ondermijnt. Ook vanuit beleidsperspectief is deze vraag relevant. Als privacy geletterdheid een oorzaak en geen oplossing is, wat zou dan wel het probleem kunnen oplossen?

Naar aanleiding van de onderzochte wetenschappelijke literatuur werden de volgende onderzoeksvragen opgesteld:

> Welke factoren dragen bij aan de digitale berusting van Belgische privacy geletterden en niet-privacy geletterden en hoe kan dit bestreden worden?

- Wat is privacy, digitale berusting en privacy geletterdheid?
- Dragen bedrijven bij aan een gevoel van digitale berusting en welke andere factoren spelen nog een rol?
- Welke verschillen zijn er in de factoren die een rol spelen bij de digitale berusting van privacy geletterden en niet-privacy geletterden?
- Wat kan een oplossing vormen voor digitale berusting?

Elk van deze deelvragen zal binnen dit onderzoek besproken worden. Allereerst zal er wetenschappelijke literatuur worden gebruikt om de termen privacy, digitale berusting en privacy geletterdheid te ontleden. Daarbij zal ook worden nagegaan hoe digitale berusting en privacy geletterdheid kan worden getest bij de respondenten. Nadien zal een empirisch onderzoek aantonen welke factoren er in de digitale berusting meespelen en hoe privacy geletterdheid daar precies een rol in vervult.

2. Het digitale tijdperk

Verandering is als het ware een constante geworden in de samenleving (Deuze, 2011, p. 137). De digitalisering en andere technologische ontwikkelingen zoals the internet of things, artificiële intelligentie en digitale platformen sturen ons naar een nieuw revolutie, namelijk de vierde industriële revolutie (Schwab, 2017). Volgens Deuze (2011, p. 138) is media dan ook gewoon niet meer weg te slaan uit het dagdagelijkse leven en leiden we een 'medialife' waarbij media een vitaal onderdeel geworden is van ons leven.

Het inzicht in het belang van bijvoorbeeld digitale platformen en data kwam eigenlijk pas naar voren bij de komst van Web 2.0 (Gerlitz & Helmond, 2013, p. 1350). Bij Web 1.0 was men vooral gefocust op het bieden van informatie. Dat tijdperk werd dan ook gekenmerkt door de 'hit en link economy'. Bij de 'hit economy' werd geanalyseerd hoeveel mensen een bepaalde website bezochten terwijl bij de 'link economy' websites vooral beoordeeld werden op basis van hoeveel andere (belangrijke) websites naar hen verwezen (Gerlitz & Helmond, 2013, p. 1350).

Dat veranderde echter door de komst van Web 2.0. Bij Web 2.0 werd er niet meer gefocust op het aanbieden van informatie, maar op connectiviteit. Mensen worden wereldwijd met elkaar verbonden via digitale platformen (Gerlitz & Helmond, 2013, p. 1351). De Vlaamse Digimeter toont aan dat 79% van de Vlamingen dagelijks gebruik maakt van een Facebookapp (Vandendriessche & De Marez, 2019). Daarbij zouden Facebook zelf, WhatsApp en Messenger de populairste zijn. Daarnaast zou zelfs 57% dagelijks vier verschillende sociale netwerken raadplegen (Vandendriessche & De Marez, 2019).

Maar wat zijn socialemediaplatformen nu eigenlijk? Socialemediaplatformen worden door Van Dijck, Poell en De Waal (2018) in hun boek 'The Platform Society' gedefinieerd als sociaal-technologische infrastructuren die de communicatie en interactie tussen gebruikers niet alleen mogelijk maken maar ook sturen. Dat proces wordt mogelijk gemaakt door het feit dat er data van gebruikers verzameld en verwerkt wordt.

Deze definitie brengt drie verschillende implicaties met zich mee. Een eerste handelt over het feit dat Web 2.0 mensen via digitale platformen aanzet om hun creativiteit de vrije loop te laten om zo online content te creëren en online gemeenschappen te vormen (Van Dijck & Nieborg, 2009, pp. 856-857). Gebruikersparticipatie is als het ware de basis geworden van Web 2.0.

Wat deze definitie echter ook aanduidt, is dat platformen gebruikersactiviteiten sturen aan de hand van platformmechanismen, economische modellen en gebruikersactiviteiten (van Dijck, Poell, & De Waal, 2018). Een voorbeeld daarvan is het feit dat platformmechanismen ervoor zorgen dat we bijvoorbeeld op Facebook te zien krijgen wat onze vrienden doen. Dat wordt het intensificatieproces genoemd. Vrienden met online content zien omgaan, zet ons aan om met diezelfde content te interageren (Van Dijck, Poell, & De Waal, 2018).

Een laatste aspect dat in de bovenstaande definitie wordt beschreven, handelt tevens over de keerzijde van de medaille. Web 2.0 was namelijk ook het startschot voor het analyseren van data. Deze data wordt onder andere massaal verkregen door de aanwezigheid van mensen op het internet en het gebruik van sociale media (Solove, 2015, p. 71; Turow et al., 2015, p. 7).

Ook al is het gebruik van sociale media gratis, toch betalen we een prijs voor wat we online doen (Solove, 2015, p. 71; Turow et al., 2015, p. 7). Alles wat we online doen, wordt namelijk gevolgd en deze data wordt vervolgens opgeslagen en gedeeld (Solove, 2015, p. 71; Turow et al., 2015, p. 7). We zijn als het ware terechtgekomen in een tijdperk van 'surveillance capitalism' (Zuboff, 2019). Daarbij gaat het, volgens Zuboff (2019), niet enkel meer over het targeten van personen met persoonlijke reclame. De data die over personen wordt verzameld, wordt namelijk ook gebruikt in financiën, verzekeringen en retail.

Gebruikers van het internet en socialemediakanalen worden op verscheidene manieren gevolgd (Solove, 2015, p. 71; Turow et al., 2015, p. 7). Vanaf het moment dat we eender welke website bezoeken wordt er data over ons bijgehouden, zoals onze locatie, wat we precies bekijken op een website, welke vragen we stellen, de connecties die we online maken, welke computer we gebruiken of welk IP-adres we hebben, enzovoort. Ook wanneer we verbinding maken met bepaalde wifi-netwerken in bijvoorbeeld een koffiebar worden we gevolgd in de dingen die we online doen (Turow et al., 2015, p. 7). Het gaat zelfs verder dan dat. Sinds de komst van socialenetwerksites en mediagiganten zoals Facebook en Google is de dataverzameling geïntensiveerd (Gerlitz & Helmond, 2013).

Wat Facebook en andere socialemediaplatformen eigenlijk doen, is gebruikers doorheen het web volgen via 'social plug-ins' en 'cookies' (Gerlitz & Helmond, 2013, p. 1353). Dat valt onder wat men de 'like economy' noemt, waarbij de 'like buttons' van Facebook via cookies de activiteiten van gebruikers online blijven volgen. Dat wil dus zeggen dat zelfs het gedrag van gebruikers op andere websites door Facebook wordt gevolgd (Gerlitz & Helmond, 2013, p. 1353). Al deze data wordt dan vervolgens gekoppeld aan een specifiek online profiel, wat er voor zorgt dat men weet wie wanneer welke website heeft bezocht. Aan de hand daarvan wordt een soort van online identiteit gevormd die alle digitale informatie van een individu bevat (Mudialba, Nair, & Ma, 2017, p. 475). Volgens Gerlitz en Helmond (2013, p. 1353) zou Facebook door middel van deze tools zelfs de data van niet-gebruikers van sociale media volgen en opslaan.

Natuurlijk is het ook belangrijk om in acht te nemen dat het tracken van onze informatie niet enkel een punt is dat bij de socialemediabedrijven ligt (Solove, 2015, p. 72). Gebruikers delen vaak ook zelf spontaan persoonlijke en intieme informatie met anderen zoals foto's, blogposts, vriendschappen enzovoort. We zijn dan ook als het ware afhankelijk geworden van sociale media. We hebben platformen nodig om deel te kunnen nemen aan het dagdagelijkse sociale leven (Zuboff, 2019).

Data van mensen wordt zelfs niet alleen via online activiteiten getrackt, ook offline kunnen we niet meer onder de radar blijven (Solove, 2015, pp. 71-72). Camera's die in het straatbeeld opduiken, zijn namelijk allang geen uitzondering meer. Door het feit dat mensen online en zelfs offline constant gevolgd worden, maakt dat er grote vraagtekens geplaatst worden bij hoe de privacy van de bevolking nog kan worden gegarandeerd (Kezer et al., 2016; Solove, 2015, p. 71).

Want hoe kunnen dergelijke bedrijven de privacy van hun gebruikers garanderen als er massaal informatie wordt verzameld en verspreid? Daarnaast doen er zich ook vaak data-inbreuken voor waarbij de gegevens van miljoenen mensen gestolen worden (Wright & Xie, 2019, p. 124).

3. Het concept privacy ontleedt

3.1. De verwachting van privacy

Privacy is een term die over de eeuwen heen enorm veel definities toegekend heeft gekregen (Chen, 2018, p. 1394; Solove, 2015, pp. 73-78; Zureik et al., in Hoepman & van Lieshout, 2012, p. 75). Een aantal van deze definities zullen in hoofdstuk 3.2 worden besproken. Voor er echter specifieke definiëringen bijgehaald kunnen worden, dient privacy eerst vanuit een breder kader te worden bekeken, namelijk vanuit het kader van verwachte en gewenste privacy.

Een eerste perspectief gaat over het belang van verwachte privacy. Zo zien Wright en Xie (2019) het belang in om het concept te bekijken vanuit welke privacy er door de samenleving verwacht wordt, omdat zo de normen gesteld worden die door een samenleving worden gehanteerd. Solove (2015, pp. 73-78) geeft echter aan dat enkel het hanteren van de verwachting niet voldoende is om de privacy van de bevolking te beschermen. Hij merkt namelijk op dat er een groot verschil is tussen wat mensen verwachten en wat ze precies wensen. In het boek van Solove 'The Digital Person' (2004, p. 225) wordt het voorbeeld gegeven van de postverdeling in koloniaal Amerika. Toen verwachtte men dat de privacy van de post werd geschonden, maar men wenste wel meer confidentialiteit waardoor de wetten verstrengd werden. Er was dus een duidelijk verschil tussen wat men verwachtte en wat men wenste (Solove, 2004, p. 225). In de huidige samenleving kan dat verschil ook opgemerkt worden. Men verwacht niet dat Facebook en andere socialemediaplatformen onze privacy bewaren, maar dat wil niet zeggen dat we dat niet wensen. Wetten en regels veranderen dus niet omwille van de privacy die we verwachten, maar omwille van de privacy die we wensen (Solove, 2015; Solove, 2004). Wanneer er op het einde van deze masterproef mogelijke oplossingen voor digitale berusting worden meegegeven, zal dat ook gebeuren vanuit de gewenste privacy en niet vanuit de verwachte privacy.

Solove geeft in het boek 'Understanding Privacy' (2008) aan dat men privacy dan vooral moet bekijken vanuit specifieke problemen. Het zijn namelijk deze problemen die een gevoel van noodzakelijkheid naar privacy opwekken. Vier specifieke privacyproblemen worden omschreven (Solove, 2008):

- Dataverzameling;
- Dataverwerking;
- Dataverspreiding;
- Data-invasie.

Elk van de hierboven opgesomde privacyproblemen omvat verschillende mogelijke schadelijke activiteiten (Solove, 2008). Elk van deze schadelijke activiteiten zullen hieronder kort besproken worden.

Bedrijven kunnen twee soorten manieren aanwenden om de data van gebruikers te verzamelen, namelijk observatie of ondervraging (Solove, 2008). Onder de dataverwerking worden aggregatie, identificatie, onveiligheid, secundair gebruik en uitsluiting verstaan. Elk van deze activiteiten omvat een andere manier van dataverwerking. Bij het aggregeren van data worden verschillende stukken informatie vanuit verschillende databases bij elkaar gebracht. Vaak is data ook niet anoniem (Solove, 2008). Omdat de zaken die we online doen gelinkt zijn aan een persoonlijk profiel, wordt de data die over ons verzameld wordt ook gekoppeld aan dat profiel en dus onze eigen persoon. Dat proces wordt identificatie genoemd. Een derde manier van dataverwerking is het secundair gebruik van data. Data kan vaak voor meer doeleinden gebruikt worden dan initieel werd gedacht (Solove, 2008). Een voorbeeld daarvan is hoe data over elektrische auto's werd hergebruikt om een netwerk van oplaadpunten te installeren (Mayer-Schönberger & Cukier, 2013, p. 102). Wat vaak ook het geval is, is dat gebruikers geen weet hebben van alle data die over hen wordt verzameld en hoe daarmee wordt omgegaan. Het proces van uitsluiting handelt daarover.

Het voorlaatste dataprobleem, dataverspreiding, handelt zowel over het welwillend delen van informatie als data-inbreuken waarbij informatie zonder toestemming wordt verspreid (Solove, 2008). Schenden van vertrouwelijkheid, het onthullen van data, de blootstelling van data, de vervorming van data, het verhogen van de toegang tot data en de toe-eigening van data worden onder de noemer data-inbreuken geplaatst. Als laatste werd er door Solove (2008) ook nog gesproken over data-invasie, waarbij indringing in iemands data of rust en inmenging in iemands beslissingen twee belangrijke activiteiten vormen.

3.2. De dimensies van privacy

Zoals al werd aangehaald, blijkt dat privacy geen term is die met één specifieke definitie uit te leggen valt (Chen, 2018, p. 1394; Solove, 2015, pp. 73-78; Zureik et al., in Hoepman & van Lieshout, 2012, p. 75). Het concept evolueerde namelijk door de jaren heen. Een voorbeeld daarvan is hoe privacy werd gepercipieerd in het oude Rome. Daar was het bijvoorbeeld helemaal niet vreemd om het lichaam niet als privé te beschouwen terwijl dat nu niet meer denkbaar is. Privacy is dus iets dat niet vaststaat en dat verandert naargelang de samenleving en de tijdsgeest (Solove, 2015, pp. 73-78).

In de literatuur worden er dan ook verschillende beschrijvingen of dimensies toegekend aan het concept privacy. Zo halen bijvoorbeeld Chen (2018, p. 1394) en Solove (2015, pp. 73-78) elk verschillende dimensies aan waaronder controle over de eigen informatie, het recht om niet geïdentificeerd te worden, het recht om u als persoon af te zonderen van de samenleving, data security en geheimhouding.

De meest volledige omschrijving van privacy, werd echter gevonden in het werk van Zureik et al. (in Hoepman & van Lieshout, 2012, p. 75). In dat onderzoek beschrijft men onder andere de verschillende dimensies die hierboven worden besproken, maar er worden er nog een aantal aan toegevoegd:

1. Het recht om alleen gelaten te worden;
2. Gelimiteerde toegang tot de eigen persoon;
3. Geheimhouding;
4. De controle over de eigen persoonlijke informatie;
5. Individualiteit;
6. Intimiteit.

Elk van deze bovenstaande dimensies handelt over een ander aspect van privacy. Volgens Zureik et al. (in Hoepman & van Lieshout, 2012, p. 75) heeft 'het recht om alleen gelaten te worden' betrekking op het feit dat iemand contact met andere personen mag bannen indien dat gewenst is. Daarnaast handelt 'gelimiteerde toegang tot de eigen persoon' over het feit dat je bijvoorbeeld het recht hebt om een ander van je eigendom te weigeren (Zureik et al., in Hoepman & van Lieshout, 2012, p. 75). De dimensie geheimhouding gaat onder andere over de informatie die een persoon zelf niet wilt delen, maar het gaat zelfs verder dan dat (Solove, 2015, pp. 72-73; Zureik et al., in Hoepman & van Lieshout, 2012, p. 75). Volgens Solove (2015, pp. 72-73) valt ook de informatie die anderen over een persoon hebben daaronder. Denk daarbij maar aan de geheimhouding waar een dokter zich aan moet houden.

Bij de 'controle over de eigen persoonlijke informatie' heeft een persoon het recht om bijvoorbeeld informatie op te vragen of te laten verwijderen indien die door derden werd verzameld (Zureik et al., in Hoepman & van Lieshout, 2012, p. 75). Dataverzamelaars mogen namelijk niet zomaar doen wat ze willen met de data die ze verzameld hebben. De laatste twee dimensies van privacy, individualiteit en intimiteit, handelen dan weer respectievelijk over het zoeken naar de eigen persoonlijkheid en het kunnen weigeren van een ander persoon in de persoonlijke levenssfeer (Zureik et al., Hoepman & van Lieshout, 2012, p. 75).

Wat bij de communicatietechnologie een zeer belangrijke dimensie vormt, is het hebben van controle over de eigen persoonlijke communicatie (Solove, 2015, p. 73; Zureik et al., in Hoepman & van Lieshout, 2012, p. 75). Het is namelijk zeer belangrijk dat mensen weten welke informatie wordt gevolgd en bijgehouden en welke informatie wordt gedeeld (Solove, 2015, p. 73; Zureik et al., in Hoepman & van Lieshout, 2012, p. 75). Enkel door dat te weten kunnen mensen ook controle hebben over hun eigen informatie. Dat schiet volgens Solove (2015, p. 73) echter nog te kort. Als je bedenkt dat sommige mensen geweigerd worden voor bepaalde leningen of dat ze op een lijst van mogelijke terroristische activiteiten terechtkomen op basis van data, blijkt toch dat dit aspect nog altijd niet op punt staat en dat er nog geen volledige controle is over de data die verzameld wordt (Solove, 2015, p. 73).

Deze laatste dimensie 'de controle over de eigen informatie' vormt in dit onderzoek dan ook de focus. Tijdens het kwalitatieve onderzoek zal er vooral gevraagd worden naar het gedrag van personen op digitale media. Er wordt dus bekeken in hoeverre respondenten trachten controle te krijgen over hun eigen informatie en waarom ze dit wel of niet doen.

3.3. Privacy management

Omdat er gefocust zal worden op de controle die iemand uitoefent over zijn eigen persoonlijke informatie, zal ook het concept privacy management worden overlopen. Controle uitoefenen over iemands eigen persoonlijke informatie en de manier waarop dat gebeurt, wordt in het Communication Privacy Management model van Petronio (in Kezer et al., 2016) namelijk benoemd als privacy management. Binnen privacy management zijn er twee verschillende processen, namelijk het onthullen van informatie en het beschermen van iemands privacy (Petronio, in Chen, 2018, pp. 1394-1395). Het gaat dus over de handelingen of strategieën die een gebruiker toepast om oftewel informatie te delen met anderen of om deze informatie net af te schermen.

Wat nu blijkt uit het onderzoek van Petronio (in Chen, 2018, pp. 1394-1395) is dat deze twee processen niet altijd afzonderlijk van elkaar bekeken kunnen worden. We zijn niet altijd enkel onze privacy aan het afschermen of net volop informatie aan het delen met anderen. Denk maar aan de manier waarop Facebook werkt. Facebook zorgt ervoor dat gebruikers een netwerk van vrienden kunnen opbouwen om zo content met hen te kunnen delen. Maar het feit dat ze informatie delen met hun netwerk wil niet zeggen dat het proces van het beschermen van privacy niet tegelijk optreedt. De gebruiker kan namelijk ingesteld hebben dat enkel de personen binnen zijn/haar netwerk de gedeelde info kan bekijken. Volgens Petronio (in Chen, 2018, pp. 1394-1395) kiest de gebruiker er in dat proces dus voor om zowel zijn/haar privacy te beschermen tegen de buitenwereld, als om persoonlijke informatie te delen met een beperkte groep.

Het feit dat we tegenwoordig massaal online aanwezig zijn en interageren met eigen content en content van anderen zorgt ervoor dat we constant met deze twee processen in aanraking komen.

3.4. Het belang van privacy

Waarom is privacy nu net zo belangrijk? Er komt namelijk vaak naar voren dat privacy enkel voor individuen is die iets te verbergen hebben (Zureik et al., in Hoepman & van Lieshout, 2012, pp. 75-76). Deze veronderstelling is echter niet juist. Het is niet omdat een persoon zaken voor zichzelf wil houden dat dat betekent dat die persoon schadelijke informatie te verbergen heeft. Sommige zaken willen mensen namelijk gewoon niet delen met anderen (Zureik et al., in Hoepman & van Lieshout, 2012, pp. 75-76). Zo zou de privacy van vandaag zelfs belangrijk zijn voor de toekomst. De informatie die er vandaag is en nu geen probleem vormt, kan in de toekomst misschien wel storingen veroorzaken.

Zo kan data die over ons wordt verzameld, al dan niet online, leiden tot gevolgen waar we zelf niet altijd aan denken (Danna & Gandy, 2002; Zureik et al., in Hoepman & van Lieshout, 2012, pp. 75-76). De data die we online achterlaten, worden namelijk geanalyseerd om gebruikers te segmenteren en op te delen in profielen. Aan de hand van dat soort profielen bekijken bedrijven dan in welk soort producten of diensten personen geïnteresseerd zouden zijn. Daardoor is het mogelijk dat we bepaalde diensten geweigerd worden op basis van deze data. Een aantal voorbeelden daarvan worden gegeven door Danna en Gandy (2002) in hun onderzoek 'All that glitters is not gold'. Zo gebeurt dit soort praktijken onder andere in de banksector. Personen die volgens de opgemaakte profielen op lange termijn een hoge klantwaarde zouden hebben, kunnen bijvoorbeeld meer voordelen (betere tarieven of leningen) krijgen dan klanten die dat niet zijn (Danna & Gandy, 2002, p. 375).

Een ander voorbeeld van het belang van privacy, is wat er gebeurd is met Cambridge Analytica bij de presidentsverkiezingen in 2016 (Draper & Turow, 2019, pp. 1824-1825). De data van gebruikers van Facebook werden massaal gebruikt om de uitslag van deze verkiezingen te beïnvloeden. Het feit dat onze data in handen is van socialemediaplatformen en andere databedrijven heeft dus meer gevolgen dan dat we denken.

Natuurlijk is het volledig bannen van dataverzameling geen oplossing (Zureik et al., in Hoepman & van Lieshout, 2012, p. 75). Soms is het noodzakelijk om data over individuen te verzamelen om zo de samenleving te kunnen helpen, maar een belangrijke nuance die daarbij dan gemaakt moet worden, is dus dat er transparantie dient te zijn. Er moet duidelijk gecommuniceerd worden over hoe en waarom data wordt verzameld (Zureik et al., in Hoepman & van Lieshout, 2012, p. 75).

4. De privacy paradox

4.1. Wat is de privacy paradox?

Zoals hierboven wordt beschreven, is privacy een zeer ingewikkeld concept (Chen, 2018; Solove, 2015; Zureik et al., in Hoepman & van Lieshout, 2012). Dat is niet alleen te merken aan de definiëring, maar ook aan de manier waarop gebruikers van sociale media omgaan met hun eigen privacy. Zo zouden mensen namelijk aangeven dat ze privacy en het beschermen van hun persoonlijke gegevens belangrijk vinden, maar zouden ze geen actie ondernemen om dat ook effectief te doen (Draper & Turow, 2019; Gerber, Gerber, & Volkamer, 2018; Gimpel et al., 2018; Kezer et al., 2016). Het gaat zelfs verder dan dat. Gebruikers delen zonder nadenken zelf persoonlijke gegevens/data op sociale netwerken zoals wie hun vrienden zijn of waar ze op vakantie gaan (Gerber et al., 2018, p. 227). In deze bevinding schuilt dus een tegenstelling, want wat uit de voorgaande hoofdstukken nu naar voor komt, is dat de privacy van gebruikers toch in het gedrang komt door het feit dat er ongelofelijk veel data wordt verzameld, gedeeld en dat soms zonder het medeweten van de gebruiker. Deze tegenstelling wordt in de wetenschappelijke literatuur benoemd als de privacy paradox (Draper & Turow, 2019, p. 1825; Gerber et al., 2018, p. 227; Gimpel et al., 2018, p. 475; Kezer et al., 2016). Dit concept is echter niet nieuw. Het werd in 2006 geïntroduceerd door Barnes.

Dat concept is niet enkel iets dat in de theorie wordt bestudeerd. Het komt in de praktijk ook wel degelijk voor. Cijfers tonen dat namelijk aan. Zo werd er een studie gevoerd waarbij er aan gebruikers van digitale media gevraagd werd of ze zich zorgen maakten over hun eigen privacy (Symantec, 2015). Zo zou 57% van de Europeanen zich zorgen maken over de verzameling van data (Symantec, 2015). Wat dan net zo opmerkelijk is, is dat hun bezorgdheid niet wordt omgezet in daden. 59% van de respondenten in deze studie geeft aan dat ze de voorwaarden bij een aankoop maar met een half oog lezen. Verschillende respondenten (14%) zouden de voorwaarden zelfs volledig niet te lezen (Symantec, 2015).

Wat er gebeurd is tijdens de presidentsverkiezingen van 2016 met Cambridge Analytica duidt ook op het bestaan van de privacy paradox. Bij het uitkomen van dit schandaal was het duidelijk dat de privacy van de gebruikers geschonden was en dat het zelfs tegen hen gebruikt werd (Draper & Turow, 2019, p. 1825). Gebruikers sloten hun account op Facebook echter niet massaal af. Er waren wel een aantal gevallen die de rug keerden naar het socialemediaplatform, maar dat woog niet op tegen het aantal gebruikers die bleven (Draper & Turow, 2019, p. 1825).

4.2. De oorzaken van de privacy paradox

In de literatuur worden een aantal oorzaken opgesomd voor deze privacy paradox. De eerste oorzaak wordt omschreven als de 'gratification theory'. De 'gratification theory' gaat volgens Draper en Turow (2019, p. 1825), Gerber et al. (2018, p. 229) en Kezer et al. (2016) namelijk over het feit dat mensen een soort van risico-analyse maken over het delen van hun eigen informatie. Ze maken als het ware een balans op van de voor- en nadelen en als blijkt dat de voordelen opwegen tegen de nadelen, kan er beslist worden om toch de desbetreffende persoonlijke data te delen. De tweede reden handelt over het feit dat mensen niet voldoende geïnformeerd zouden zijn over onder andere het misbruik van de privacy en de (technische) mogelijkheden om daar iets aan te veranderen (Draper & Turow, 2019, p. 1825; Gerber et al., 2018, p. 230). Daarnaast wordt 'bounded rationality' als derde reden opgegeven voor de privacy paradox (Gerber et al., 2018, pp. 229-230). Waar men bij de 'gratification theory' kan werken op basis van rationele informatie om een beslissing te nemen, beschikt niet iedereen altijd over deze rationele informatie. Ze moeten dan als het ware een beslissing nemen op basis van beperkte gegevens. Dat wekt de illusie van een rationele beslissing op (Gerber et al., 2018, pp. 229-230).

Een vierde reden die wordt aangebracht door Gerber et al. (2018, p. 230), is de invloed van de omgeving. Zo oefenen niet enkel de ouders invloed uit op de manier waarop jongeren hun data delen, ook andere sociale kringen zoals vrienden spelen een rol. Daarnaast hebben mensen vaak de illusie dat ze enige initiële controle hebben over hun data (Gerber et al., 2018, p. 230). Zo hebben ze bijvoorbeeld controle over de privacy settings. Ze staan er echter niet bij stil dat er nadien nog verschillende bewerkingen (data mining, het delen van data met derde partijen) met deze data gebeuren door de beheerders van sociale media of andere digitale platformen. Hun initiële gevoel van controle is dus eigenlijk ongegrond (Gerber et al., 2018, p. 230).

Het 'risk and trust model' is ook een manier om de privacy paradox te verklaren. Daarbij zou vertrouwen meer invloed hebben op de eigenlijke beslissingen terwijl een risicogevoel eerder de intentie van het nemen van een beslissing beïnvloed. Concreet wil dit zeggen dat een risicogevoel niet meteen aanzet tot het nemen van een beslissing op vlak van privacy (Gerber et al., 2018, p. 230). Waar ook over gesproken wordt als mogelijke oorzaak, is het feit dat wanneer individuën spreken over het nemen van een beslissing, de uiteindelijk beslissing toch anders kan zijn (Gerber et al., 2018, p. 230)

Een laatste punt, dat naar voren komt als oorzaak van de privacy paradox, is de manier waarop de onderzoeken worden gevoerd. Gerber et al. (2018, p. 231) duidt aan dat de manier waarop onderzoekers hun methodologisch kader opstellen ook een oorzaak kan zijn voor niet vinden van een positief verband tussen het ongerust zijn over privacy en privacybeschermend gedrag.

5. De digitale berusting

5.1. De digitale berusting: wat en waarom?

Hierboven werden verschillende mogelijke oorzaken gegeven voor de privacy paradox. Nu blijkt echter dat er nog een andere reden aan de basis zou kunnen liggen van dat fenomeen (Draper & Turow, 2019; Kezer et al., 2016; Turow et al., 2015). Volgens Turow et al. (2015, p. 3) hebben marketeers een fout idee van de reden waarom mensen data vrijgeven. Mensen zouden namelijk geen risicoanalyse maken waarbij ze de voor- en nadelen van het onthullen van informatie nagaan. Marketeers grijpen die risicoanalyse aan als excuus om hun dataverzameling, dataverwerking en dataverspreiding te kunnen verderzetten. Als mensen data vrijgeven voor hun eigen gewin en daarin een weloverwogen beslissing zouden nemen, zijn er namelijk geen bezwaren voor marketeers om de data te verzamelen. Door de veronderstelling van een 'sterke' consument naar voren te brengen, houden ze ook beleidsmakers op afstand (Turow et al., 2015, p. 3). Het probleem is echter dat mensen vaak onvoldoende informatie hebben om een dergelijke risicoanalyse te maken of dat ze de foute veronderstelling hebben dat de overheid of de privacyverklaringen van bedrijven hen voldoende beschermt tegen de ongewilde verwerking en verspreiding van data (Turow et al., 2015, pp. 4-5). Een logische verklaring lijkt nu dat mensen hun data onvoldoende beschermen, omdat ze niet voldoende kennis hebben over deze thematiek. Volgens Turow et al. (2015, pp. 8-9) ligt echter ook dat niet aan de basis van de privacy paradox. De onderzoeken van Draper en Turow (2019), Kezer et al. (2016) en Turow et al. (2015) geven dan ook aan dat er een andere oorzaak zou zijn.

Gebruikers van het internet of sociale media zouden er namelijk vanuit gaan dat het beschermen van data nutteloos is, omdat ze denken dat hun persoonlijke gegevens en hun doen en laten op het internet toch worden bijgehouden. Het gaat er dus over dat mensen het gevoel hebben dat elke actie, die ze daartegen proberen uit te voeren, nutteloos zal zijn. (Draper & Turow, 2019; Kezer et al., 2016; Turow et al., 2015). Zelfs als gebruikers wel hun privacy proberen te beschermen door bijvoorbeeld hun privacyinstellingen te versterken of cookies te verwijderen, hebben ze nog het idee dat dat niets zal uithalen. Het gaat zelfs verder dan dat. Gebruikers van het internet zijn er zelfs van overtuigd dat het niet alleen niets uithaalt als ze hun privacy proberen te beschermen, maar dat ze ook nog eens negatieve effecten zullen ervaren (Turow et al., 2015, p. 9). Zo is het mogelijk dat ze onder andere minder aantrekkelijke promoties ontvangen, geen toegang krijgen tot bepaalde websites of diensten, content te zien krijgen die minder relevant is, enzovoort als ze meer privacybeschermend gedrag vertonen (Turow et al., 2015, p. 9).

Het fenomeen dat hierboven besproken wordt, wordt in de literatuur bestempeld als de digitale berusting. Iets dat dus zou voortkomen uit een gevoel van hopeloosheid over de situatie (Draper & Turow, 2019; Kezer et al., 2016; Turow et al., 2015).

In het onderzoek van Turow et al. (2015) wordt ook aangetoond dat deze digitale berusting niet alleen in de theorie een plaats heeft, maar dat het in de praktijk ook duidelijk bestaat. Zo geeft hun onderzoek aan dat 58% van de bevraagde Amerikanen digitaal berust zou zijn.

Dat uit zich dan vooral in het feit dat mensen hun data eerder gaan delen omdat ze digitaal berust zijn dan dat ze dat doen omdat ze bekeken wat de kosten en baten waren van het delen van hun data (Turow et al., 2015, p. 15).

In het onderzoek van Draper en Turow (2019, pp. 1827-1829) trachtten ze om voor dit fenomeen een theoretisch framework op te stellen op basis van twee perspectieven. Een eerste standpunt dat wordt ingenomen, is dat geen actie ondernemen tegen het ongewenst verzamelen van data niet aanzien moet worden als iets irrationeel. Als een persoon oog in oog staat met een ongewenste situatie waar men niets aan kan veranderen, moet dat zelfs aanschouwd worden als een logische reactie en niet als een gebrek aan interesse in de situatie (Draper & Turow, 2019, pp. 1827-1829). De situatie wel proberen veranderen, zou tot niets leiden of de situatie misschien zelfs verergeren.

Een tweede perspectief, dat besproken wordt in het framework van de digitale berusting, is het feit dat bedrijven het fenomeen liever versterken dan verminderen (Draper & Turow, 2019, pp. 1827-1829). Bedrijven willen namelijk liever niet dat gebruikers moeilijk doen over net datgene wat hun business model voedt. Een gevoel van hopeloosheid zorgt er namelijk ook voor dat er op vlak van beleid minder snel zaken veranderen, wat tevens voordelig is voor bedrijven (Draper & Turow, 2019, pp. 1827-1829).

Maar de grote vraag die daarbij nu gesteld moet worden, is wat er aan de basis ligt van deze digitale berusting. Een eerste bevinding in het onderzoek van Draper en Turow (2019, pp. 1830-1833) is dat het gedrag van bedrijven een oorzaak kan vormen. Dat zal in het volgende onderdeel worden besproken.

5.2. De rol van bedrijven in de digitale berusting

Volgens Draper en Turow (2019, pp. 1830-1833) zouden bedrijven een rol spelen in de digitale berusting. Zoals hierboven wordt vermeld, juichen ze de digitale berusting liever toe dan dat ze er iets tegen doen, omdat dat er net voor zorgt dat politieke acties op vlak van beleid of sanctionering uitblijven. Wat daarbij een rol speelt, is dat bedrijven binnen hun privacybeleid en transparantie-initiatieven een aantal misleidende tactieken toepassen die dat gevoel van digitale berusting alleen maar vergroten. Afleiden, het gebruik van jargon, geruststellen en verkeerd benamen zijn een aantal van deze tactieken (Draper & Turow, 2019, p. 1830).

Omtrent het privacybeleid zijn er twee zaken die bij kunnen dragen aan de digitale berusting. Het eerste is dat personen ervan uitgaan dat het bestaan van een privacybeleid hun privacy automatisch beter beschermd (Draper & Turow, 2019, p. 1831; Turow et al., 2015, p. 8). Er is hier dus een soort van misplaatst vertrouwen dat gebruikers hebben in de bedrijven die beschikken over een privacybeleid. Gebruikers hebben dus een verkeerd beeld over wat een privacybeleid is en over wat het inhoudt. Volgens Draper en Turow (2019, p. 1831) en Turow et al. (2015, p. 8) ligt dat aan het label 'privacybeleid' zelf. Deze benaming zou misleidend werken voor consumenten of gebruikers. In het bestaan van een 'privacybeleid' schuilen dus de misleidende tactieken geruststellen en verkeerd benamen.

Daarnaast vormt de manier waarop zo'n privacybeleid wordt geschreven ook een probleem. Een privacybeleid bevat jargon en moeilijke woorden die gebruikers vaak niet begrijpen. Vaak is zo'n beleid ook nog eens langdradig waardoor mensen zelfs de moeite niet willen nemen om het te beginnen lezen (Al-Saqer & Seliaman, 2016, p. 143; Draper & Turow, 2019, p. 1831). Gebruikers gaan omwille van deze redenen dan ook gewoon akkoord met een beleid zonder te weten wat erin staat.

Een tweede aspect zou handelen over de transparantie-initiatieven van bedrijven (Draper & Turow, 2019, pp. 1832-1833). Ondernemingen proberen hun transparante houding in de kijker te zetten. Zo willen ze consumenten een soort van controle geven over hun eigen data. Google en Facebook zijn bijvoorbeeld twee bedrijven die deze strategie toepassen. Gebruikers kunnen namelijk alle data die de twee bedrijven over hen hebben opvragen (Draper & Turow, 2019, pp. 1832-1833). Wat gebruikers te zien krijgen, is echter helemaal geen waarheidsgetrouw beeld van de data die het bedrijf heeft of van de strategieën die ze aanwenden om de data te verwerken en/of te verspreiden. Hier worden dus opnieuw een aantal van de hierboven opgesomde misleidende tactieken gebruikt, namelijk afleiden en geruststellen. Ze proberen gebruikers een vals gevoel van controle te geven door middel van zogenaamde transparantie (Draper & Turow, 2019, pp. 1832-1833).

Een laatste punt dat door Draper en Turow (2019, pp. 1832-1833) wordt aangehaald, is dat bedrijven consumenten of gebruikers ook ontmoedigen om een einde te maken aan het gebruik van de diensten van het bedrijf. Dat doen ze voornamelijk door consumenten en gebruikers er op te wijzen welke voordelen hun producten/diensten met zich meebrengen (Draper & Turow, 2019, pp. 1832-1833). Voorbeelden daarvan zijn Facebook of Instagram. Heel veel personen zijn aanwezig op deze socialemediaplatformen en het is makkelijk om in contact te blijven met vrienden en familie. Stoppen met deze platformen, maakt dat een stuk moeilijker.

Privacyverklaringen en transparantie-initiatieven zouden dus bijdragen aan de digitale berusting (Draper & Turow, 2019, pp. 1830-1833).

5.3. Digitale berusting testen

Om te kunnen achterhalen waarom personen zich nu precies digitaal berust voelen, moet er natuurlijk eerst nagegaan worden of ze zich ook daadwerkelijk zo voelen. Het onderzoek van Turow et al. (2015) biedt daarbij een manier om te bepalen of mensen zich nu digitaal berust voelen of niet.

Om na te gaan of personen digitaal berust waren, werden er twee stellingen voorgesteld, namelijk (Turow et al., 2015, p. 14):

- Ik wil controle kunnen uitoefenen over wat marketeers online over mij te weten kunnen komen.
- Ik heb geaccepteerd dat ik weinig controle kan uitoefenen over wat marketeers online over mij te weten kunnen komen.

Deze twee vragen werden gesteld aan de hand van een schaal waarbij respondenten konden kiezen uit de volgende antwoordmogelijkheden: helemaal mee eens, mee eens, niet mee eens, helemaal niet mee eens, geen van beide, weet ik niet (Turow et al., 2015, p. 14). Respondenten werden als digitaal berust bestempeld als ze met beide stellingen akkoord gingen. Tijdens het onderzoek in deze masterproef zal gebruik gemaakt worden van deze twee stellingen om na te gaan wie digitaal berust is en wie niet. Informatie over hoe de test precies gebruikt werd in dit onderzoek, kan u terugvinden in 'Deel 2: kwalitatief onderzoek'.

6. Privacy geletterdheid

6.1. De definiëring van privacy geletterdheid

Zoals hierboven al werd aangehaald, wordt er tegenwoordig ongelofelijk veel data over gebruikers en consumenten verzameld (Solove, 2015, p. 71; Turow et al., 2015, p. 7). Sinds de komst van het internet en sociale media zit het verzamelen, verwerken en verspreiden van data namelijk in de lift.

Maar in een tijd waar onlinemediabedrijven meer weten over gebruikers dan hun beste vrienden, mogen personen er niet op rekenen dat hun privacy voor hen zal worden beschermd. Ze moeten zelf ook actie ondernemen om ervoor te zorgen dat informatie die ze als privé beschouwen ook privé blijft (Wissinger, 2017, p. 379). Wat daarbij echter noodzakelijk is, is kennis over wat privacy precies is. Volgens Wissinger (2017, p. 379) kan een basiskennis over privacy en de manier waarop data wordt verzameld gebruikers helpen om een doordachte beslissing te nemen over het wel of niet delen van persoonlijke informatie.

Net zoals privacy is privacy geletterdheid geen concept waar consensus over gevonden wordt in de wetenschappelijke wereld (Bartsch & Dienlin, 2016, p. 148; Wissinger, 2017, pp. 379-380). Wissinger (2017, pp. 379-380) beschrijft in zijn onderzoek twee verschillende definities om het concept privacy geletterdheid te beschrijven. De onderzoeker haalt als eerste een definitie aan van Langenderfer en Miyazaki (2009): "the understanding that consumers have of the information landscape with which they interact and their responsibilities within that landscape" (p. 383). Een tweede beschrijving die wordt aangehaald door Wissinger (2017, pp. 379-380) zijn de woorden van Givens (2015) "one's level of understanding and awareness of how information is tracked and used in online environments and how that information can retain or lose its private nature" (p. 53). Wissinger (2017) haalt deze twee definities aan, omdat in zijn onderzoek privacy geletterdheid vooral neigt naar kritisch denken. Waarbij het vooral belangrijk is dat personen in het digitale tijdperk een bepaald proces doorgaan als het gaat over het delen van data. Het begrijpen, herkennen en realiseren van de manier waarop data wordt verzameld en verwerkt en wat dat kan betekenen voor een bepaald persoon zijn de eerste drie stappen in dat proces. Daarna moet deze persoon evalueren of het delen van zijn/haar info de juiste beslissing is en daarna volgt dan de beslissing (Wissinger, 2017, pp. 380-381).

De definities die Wissinger (2017) aanhaalt, focussen vooral op het kritisch denken over privacy en het delen van informatie, maar wat ontbreekt is een focus op kennis over hoe een persoon dat het beste kan doen. Een kritische ingesteldheid over het delen van informatie is een eerste stap, maar gebruikers van het internet moeten natuurlijk ook beschikken over een aantal skills om hun privacy te beschermen. Trepte et al. (2015) geven daarbij een aanvulling op de definities die hierboven werden beschreven:

> Online privacy literacy may be defined as a combination of factual or declarative ('knowing that') and procedural ('knowing how') knowledge about online privacy. In terms of declarative knowledge, online privacy literacy refers to the users' knowledge about technical aspects of online data protection, and about laws and directives as well as institutional practices. In terms of procedural knowledge, online privacy literacy refers to the users' ability to apply strategies for individual privacy regulation and data protection. (Trepte et al., 2015, p. 339)

In de bovenstaande definitie wordt privacy geletterdheid niet alleen bekeken vanuit het perspectief van kritisch denken. Er wordt ook aandacht besteed aan de 'knowing how', iets dat ontbreekt in de definities van Wissinger (2017). Het is namelijk belangrijk om als gebruiker van het internet ook kennis te hebben over wat privacyverklaringen inhouden en om te beschikken over de nodige skills om de eigen privacy te beschermen (Trepte et al., 2015). Zowel kritisch denken als kennis hebben over hoe dingen gebeuren, is belangrijk.

Het moet wel duidelijk zijn dat privacy geletterdheid iets anders is dan digitale geletterdheid (Wissinger, 2017, pp. 379-380). Een onderscheid dat in onderzoek vaak over het hoofd wordt gezien. Digitale geletterdheid zou namelijk een andere focus hebben dan privacy geletterdheid. Bij privacy geletterdheid is het belangrijk dat gebruikers inzien dat het delen van informatie zowel positieve als negatieve implicaties met zich meebrengt en dat de gebruikers zelf verantwoordelijk zijn om daarin een weloverwogen beslissing te nemen (Wissinger, 2017, pp. 379-380). Digitale geletterdheid handelt niet over de risico's die het delen van informatie met zich mee kunnen brengen. Daar gaat het over het feit dat gebruikers in staat zijn om online content en informatie te creëren en ermee te interageren door middel van onder andere kennis over communicatietechnologieën (Wissinger, 2017, pp. 379-380).

6.2. Versterkt of verzwakt privacy geletterdheid digitale berusting?

Een belangrijke vraag die nu gesteld moet worden, is of privacy geletterdheid bijdraagt aan digitale berusting of niet. In de wetenschappelijke wereld is daar op dit moment nog geen eenduidigheid over te vinden (Bartsch & Dienlin, 2016; Baruh et al., 2017; Draper & Turow, 2019; Kezer et al., 2016; Turow et al., 2015).

Aan de ene kant zijn er een aantal onderzoekers die via empirisch onderzoek aantoonden dat privacy geletterdheid wel degelijk leidt tot meer privacybeschermend gedrag. Zo zou het onderzoek van Bartsch en Dienlin (2016, p. 152) aantonen dat privacy geletterdheid mensen aanzet om bepaalde acties te ondernemen zoals het afschermen van iemands socialemediaprofiel. Dat kan onder andere door een profiel enkel beschikbaar te maken voor een beperkt aantal contacten. Ook zou privacy geletterdheid gebruikers van het internet een veiliger gevoel geven op vlak van privacy (Bartsch & Dienlin, 2016, p. 152).

Een tweede studie, die aangeeft dat privacy geletterdheid mensen aanzet om meer controle over hun privacy te nemen, is het onderzoek van Baruh et al. (2017). Daarin wordt vermeld dat hoe meer mensen online aanwezig zijn, hoe meer privacy geletterd ze zullen worden en hoe meer ze gaan proberen om hun online privacy te beschermen. Deze studies geven wel aan dat er nog extra onderzoek nodig is om de relatie tussen privacy geletterdheid en privacybeschermend gedrag te testen (Baruh et al., 2017).

Er zijn echter ook drie onderzoeken die aantonen dat privacy geletterdheid net niet bijdraagt aan privacybeschermend gedrag, namelijk die van Draper en Turow (2019), Kezer et al. (2016) en Turow et al. (2015, pp. 17-18). Zo wordt er aangetoond dat mensen, die meer info krijgen over de risico's van het delen van informatie, een hoger gevoel van digitale berusting hebben en bijgevolg dus minder privacybeschermend gedrag vertonen (Draper & Turow, 2019, p. 1834).

Omdat er net geen consensus is over de rol van privacy geletterdheid in digitale berusting, zal er in dit onderzoek een onderscheid gemaakt worden tussen privacy geletterden en niet-privacy geletterden. Er zal nagegaan worden welke verschillen er zijn in de factoren die digitale berusting beïnvloeden.

6.3. Privacy geletterdheid testen

In de probleemstelling werd al gesteld dat er tijdens het empirisch onderzoek een onderscheid zal gemaakt worden tussen respondenten die wel en niet privacy geletterd zijn. Om dat te weten te komen, dient er een test te worden uitgevoerd.

Doorheen het wetenschappelijke veld werden er verschillende manieren gebruikt om respondenten op privacy geletterdheid te testen. Een eerste onderzoek is dat van Bartsch en Dienlin (2016). Daarin wordt privacy geletterdheid beoordeeld op basis van zes vragen. Respondenten dienen daarbij te antwoorden op basis van een vijfpuntenschaal. De onderstaande vragen werden letterlijk vertaald (Bartsch & Dienlin, 2016, p. 153):

- Ik weet hoe ik mijn account moet deactiveren of verwijderen.
- Ik weet hoe ik de toegang tot de informatie op mijn profiel (hobby's, interesses) kan beperken. Ik weet hoe ik mijn profiel op Google ontoegankelijk moet maken.
- Ik weet hoe ik de controle over mijn gegevens kan bewaren als mijn naam getagd wordt op foto's.
- Ik weet hoe ik de toegang tot mijn posts kan beperken.
- Ik weet hoe ik de toegang tot mijn contactinformatie (vb.: naam, adres) kan beperken.

In het onderzoek van Bartsch en Dienlin (2016) is het niet zozeer een test die respondenten moeten uitvoeren. Het gaat meer over hoe zij hun eigen kunnen percipiëren. Daardoor is een dergelijke test ook niet altijd betrouwbaar, omdat mensen hun eigen kennis soms overschatten (Bartsch & Dienlin, 2016, p. 153).

Een tweede test die in de literatuur wordt aangehaald, is de OPLIS-test (Masur, Teutsch, & Trepte, 2017). OPLIS staat voor 'The online privacy literacy scale'. Deze test baseert zich op de definitie van Trepte et al. (2015), die vermeld wordt in hoofdstuk 6.1, waarbij zowel kennis over privacy en het delen van informatie als kennis over hoe privacy te beschermen van belang is. Bij deze test worden mensen bevraagd over hun kennis op vier verschillende punten (Masur et al., 2017):

- Institutionele praktijken;
- Technische aspecten van databescherming;
- Databeschermingswetgeving;
- Strategieën voor databescherming.

Bij elk van deze vier punten dienen respondenten vijf vragen te beantwoorden. De test bestaat in totaal uit 20 vragen. Deze test bevraagd respondenten dus naar de verschillende aspecten van privacy en beoordeelt personen op basis van hun feitelijke kennis en niet op basis van de perceptie van de eigen kennis (Masur et al., 2017). Omwille van deze reden zal de OPLIS-test gebruikt worden in dit onderzoek, omdat het betrouwbaardere resultaten kan opleveren. Informatie over hoe de test precies gebruikt werd in dit onderzoek, kan u terugvinden in 'Deel 2: kwalitatief onderzoek'.

7. Conclusie literatuurstudie

De literatuurstudie die gevoerd werd, heeft verschillende belangrijke inzichten met zich meegebracht. Het belangrijkste inzicht dat daarbij naar boven kwam, is welke kennis er nog ontbreekt binnen de wetenschappelijke literatuur. Digitale berusting zou een relatief nieuw fenomeen zijn waarbij er nog geen duidelijkheid is over waarom personen dit soort gevoelens ontwikkelen. Dat vormt dan ook de focus van dit onderzoek en vanuit deze bevinding werd de hoofdonderzoeksvraag opgesteld.

Daarnaast diende de literatuurstudie ook om de belangrijkste concepten te kunnen definiëren. Privacy, digitale berusting en privacy geletterdheid werden dan ook uitgebreid besproken. Er werd gekozen om het concept privacy vanuit één specifieke te dimensie te benaderen. Zo werd er gekozen voor de dimensie 'controle over de eigen informatie' (Zureik et al., in Hoepman & van Lieshout, 2012, p. 75). Deze dimensie heeft namelijk vooral betrekking op privacy binnen het online gebeuren.

Ook de termen digitale berusting en privacy geletterdheid dienden te worden verduidelijkt. Het was daarbij belangrijk om geschikte testen te vinden om bij respondenten te kunnen bepalen of ze digitaal berust zijn en op welk niveau ze zitten op vlak van privacy geletterdheid. De literatuur duidde voor de digitale berusting op het onderzoek van Turow et al. (2015). Aan de hand van twee stellingen zullen respondenten op digitale berusting getest worden. Voor het meten van de privacy geletterdheid kwam de OPLIS-test naar boven, waarbij men op vijf verschillende aspecten van privacy bevraagd zal worden (Masur et al., 2017).

DEEL 2

KWALITATIEF ONDERZOEK

8. Onderzoekdesign

8.1. Inleiding

Dit onderzoek zal zich vooral focussen op wat de gevoelens van digitale berusting precies voedt. Daarbij is het belangrijk om explorerend kwalitatief onderzoek te voeren zodat duidelijk wordt hoe die digitale berusting bij mensen aangewakkerd wordt. Er zal dus op zoek gegaan worden naar het diepere waarom.

Om dat te achterhalen zullen de deelnemers van dit onderzoek via kwalitatieve interviews bevraagd worden over hun gevoelens van digitale berusting en de oorzaken ervan. Daarbij wordt er een onderscheid gemaakt tussen mensen die privacy geletterd zijn en mensen die niet privacy geletterd zijn. Dat onderscheid wordt gemaakt op basis van de controverse die er op dit moment in de wetenschappelijke wereld bestaat omtrent dit topic. Sommigen geloven dat het een oplossing vormt, anderen net totaal niet (Bartsch & Dienlin, 2016; Baruh et al., 2017; Draper & Turow, 2019; Kezer et al., 2016; Turow et al., 2015). Het onderzoek in deze masterproef zal dus via een vergelijking moeten aantonen hoe privacy geletterdheid daar precies in past.

Om een antwoord te kunnen formuleren op de hoofdonderzoeksvraag werd het empirisch onderzoek opgesplitst in twee grote delen. Het eerste deel bestaat uit een test die de geselecteerde respondenten dienden in te vullen. Deze test moest de noodzakelijke criteria vastleggen, namelijk de digitale berusting en de privacy geletterdheid.

Een test alleen is natuurlijk niet voldoende. Na deze test werden de respondenten gevraagd om deel te nemen aan een kwalitatief interview waar dieper ingegaan zou worden op hoe de respondenten omgaan met hun online privacy en nog belangrijker waarom dat ze bepaalde dingen net wel of niet doen.

8.2. De respondenten

In tegenstelling tot een kwantitatief onderzoek is het bij kwalitatieve studies niet noodzakelijk om honderden respondenten te ondervragen. Bij dit onderzoek hebben dan ook 20 personen de test ingevuld en deelgenomen aan een interview. Er werd dan ook verder gezocht naar respondenten tot er een verzadiging optrad in de antwoorden die werden gegeven. Zo konden alle mogelijke resultaten verzameld worden.

Om de zoektocht naar respondenten te starten, werd er een bericht op Facebook gepost met een oproep aan mijn netwerk om deel te nemen aan het onderzoek. Er kwam heel wat reactie op waardoor er kon gestart kon worden met het bevragen van de eerste respondenten. Na een week werd de oproep herhaald om opnieuw nieuwe respondenten aan te trekken. Er werd daarbij de techniek van purposeful sampling gehanteerd.

In de berichten werd er namelijk specifiek aangehaald dat er gezocht werd naar personen die het gevoel hadden dat hun privacy online niet meer te beschermen valt, ook al zou men dat wel willen. Er werd op Facebook dus vooral gezocht naar personen die voldeden aan de criteria van digitale berusting. In bijlage één kan u de berichten terugvinden die verspreid werden op Facebook.

Naast de oproep op Facebook werden er ook respondenten via het sneeuwbaleffect gevonden. De respondenten gaven zelf aan dat ze een aantal contacten hadden die graag zouden deelnemen aan het onderzoek en die het concept privacy belangrijk vonden.

8.3. Informed consent

Er werd aan de respondenten ook gevraagd om een document te ondertekenen waarin staat dat ze akkoord gaan met de manier waarop de verzamelde resultaten zullen worden verwerkt. Dat werd gedaan aan de hand van een informatie- en toestemmingsformulier of een informed consent. Daarin werd uit de doeken gedaan wat er precies zal gebeuren met de gegevens die verzameld worden in dit onderzoek.

Daarnaast werd ook uitgebreid vermeld dat alle gegevens anoniem zullen worden verwerkt en dat er op geen enkele manier naar hun originele naam zal worden verwezen in het onderzoek. Deze informed consent kan u terugvinden in bijlage vijf.

8.4. Voorbereidende test

Een eerste stap, die er dus gezet diende te worden in dit onderzoek, is het invullen van een voorafgaande test. Deze test bestaat uit twee onderdelen namelijk een lijst met vragen omtrent de privacy geletterdheid en een aantal vragen omtrent de digitale berusting.

De test werd opgesteld via het programma Google Forms. De respondenten kregen een link opgestuurd om de test online te kunnen invullen. Er werd daarbij ook een korte introductie meegegeven over het doel van het onderzoek en de bedoeling van de test. In dat bericht was het vooral belangrijk om respondenten te waarschuwen om geen gebruik te maken van het internet om de vragen op te lossen. Dat zou namelijk de resultaten kunnen bedoezelen. De volledige test en de introductie die daarbij hoorde, kan u terugvinden in bijlage drie.

Digitale berusting

Een eerste punt dat zeker diende onderzocht te worden, was of de respondenten al dan niet digitaal berust waren. Uit de literatuurstudie bleek dat er twee stellingen zijn die het aanwezig zijn van digitale berusting kunnen bevestigen of uitsluiten (Turow et al., 2015, p. 14). Deze twee stellingen werden dan ook aan de respondenten voorgelegd in de voorbereidende test die ze dienden in te vullen. In het onderzoek van Turow et al. (2015, p. 14) werden beide stellingen random tussen de andere vragen van hun enquête geplaatst. Zo was het voor de respondenten niet duidelijk welke richting de onderzoekers uitwilden.

Dat zal in dit onderzoek ook gebeuren. De twee stellingen zullen random tussen de vragen omtrent privacy geletterdheid worden geplaatst.

In de originele test van Turow et al. (2015, p. 14) werden de respondenten verschillende antwoordmogelijkheden voorgelegd, namelijk helemaal mee eens, mee eens, niet mee eens, helemaal niet mee eens, geen van beide, weet ik niet. Er werd bij het interpreteren van de resultaten echter geen onderscheid gemaakt tussen personen die 'helemaal mee eens' of 'mee eens' hadden geantwoord. Hetzelfde gold voor 'helemaal niet mee eens' of 'niet mee eens'. Vanaf dat een persoon 'mee eens' antwoordde op beide stellingen werd de respondent beoordeeld als digitaal berust (Turow et al., 2015, p. 14). Om deze reden zullen er in dit onderzoek maar twee antwoordmogelijkheden worden gebruikt, namelijk of een persoon het eens is met de stelling of niet.

Wat echter ook belangrijk op te merken is, is dat een respondent niet zal worden uitgesloten indien hij/zij niet digitaal berust blijkt te zijn. Het kan namelijk ook interessante resultaten opleveren indien het antwoord op één van beide of beide stellingen 'nee' is. Tijdens het interview kan dan nagegaan worden waarom de respondent precies 'nee' antwoordde op beide of één van beide stellingen.

Privacy geletterdheid

In deze test werd naast de digitale berusting ook de privacy geletterdheid getest. In het literatuuronderzoek werden daarvoor een aantal tests uit de doeken gedaan, maar de test, die het meeste aansluit bij dit onderzoek, is de OPLIS-test. Deze test bestaat uit 20 vragen die een respondent op verschillende aspecten van privacy ondervraagt (Masur et al., 2017). De originele OPLIS-test staat in bijlage twee. De OPLIS-test is echter ontwikkeld door Duitse onderzoekers en is dan ook gericht op de Duitse bevolking. Omwille van die redenen werden er een aantal aanpassingen aangebracht aan de originele test zodat deze ook in dit onderzoek gebruikt kon worden.

Wat vooral aangepast diende te worden, waren de beleidsvragen. Zo komen er in de test een aantal vragen aan bod die van toepassing zijn op de Duitse wetgeving nog voordat de GDPR in werking trad. Dat zal voor dit onderzoek dan ook worden aangepast waarbij de vragen toegespitst zullen worden op de GDPR, de huidige Europese wetgeving omtrent privacy. Er werden in totaal vier vragen veranderd. Alle aanpassingen gebeurden aan de hand van de GDPR (Verordening (EU) 2016/679, 2018).

Een eerste vraag die aangepast werd, handelde over het Duitse recht om opgeslagen informatie te mogen inkijken. Dat recht geldt ook onder de GDPR (art. 15 Verordening (EU) 2016/679, 2018), waardoor de vraag maar licht werd aangepast. De 'Duitse wetgeving' werd vervangen door de 'GDPR'. De tweede vraag waar een verandering aan werd aangebracht, was een vraag over de Europese privacywetgeving die voor de GDPR van kracht was, namelijk de databeschermingsrichtlijn. Er werd namelijk gevraagd hoe deze wetgeving diende te worden geïmplementeerd in de lidstaten. Omdat die wetgeving dus verouderd is, werd de vraag aangepast en werd er gevraagd hoe de GDPR gehanteerd dient te worden door de lidstaten. Het antwoord op deze vraag is dat de GDPR verbindend is in al haar onderdelen voor elke lidstaat van de EU (Verordening (EU) 2016/679, 2018).

In de originele OPLIS-test werd er ook een vraag gesteld over de term 'informatieve zelfbeschikking', wat deel uitmaakte van de Duitse wetgeving voordat de GDPR van kracht werd (Masur et al., 2017). De GDPR bespreekt deze term niet (Verordening (EU) 2016/679, 2018). Deze vraag werd dan ook aangepast en er werd bevraagd wat 'het recht om vergeten te worden' precies betekent. 'Het recht om vergeten te worden' wordt namelijk wel besproken in de GDPR (art. 17 Verordening (EU) 2016/679, 2018). Het antwoord op deze vraag is dat het een recht is van iedere EU-burger. De laatste vraag waar iets aan werd veranderd, is een vraag die bevroeg of de Duitse wetgeving voorzag dat de algemene voorwaarden van sociale media allemaal aan dezelfde standaarden moesten voldoen. Dat was opnieuw een vraag die zich toespitste op de Duitse wetgeving. De vraag werd dan ook aangepast en er werd bevraagd of privacyverklaringen volgens de Europese privacywetgeving, de GDPR, aan bepaalde voorwaarden moest voldoen. Het antwoord op deze aangepaste vraag is 'ja' (art. 12 Verordening (EU) 2016/679, 2018).

Een tweede aspect dat gewijzigd moest worden, was de manier waarop de resultaten van de test werden beoordeeld. Wanneer het resultaat van de test van een bepaalde deelnemer bekend was, werd dat resultaat in het werk van Masur et al. (2017) vergeleken met de gemiddeldes van de Duitse bevolking. Het resultaat van de test werd dus vergeleken met een aantal normtabellen om na te gaan hoeveel procent van de Duitse bevolking beter of slechter scoorde op de test. Omdat er in dit onderzoek gewerkt zal worden met Vlaamse respondenten zal er geen gebruik gemaakt worden van de normtabellen die in het onderzoek van Masur et al. (2017) werden gebruikt. In dit onderzoek zullen respondenten worden beoordeeld op basis van het behalen van een 10 op 20.

8.5. Kwalitatieve diepte-interviews met topiclijst

Topiclijst

Na het uitvoeren van de test, werd er aan de respondenten gevraagd om deel te nemen aan een interview waar een resem aan topics omtrent privacy zou worden besproken. Hieronder kan u een lijst vinden van de besproken topics:

- Digitale mediagebruik;
- Gedrag op sociale media;
- Dagelijkse routine;
- Privacyinstellingen;
- Cookies;
- Formulieren of registraties;
- Privacybeleid;
- Transparantie;
- Privacyinbreuken;
- Privacy in de media;
- Wetgevingen – GDPR.

Deze topiclijst was bij de start van de interviews een beetje korter. De thema's gedrag op sociale media, dagelijkse routine, privacy in de media en wetgevingen werden pas na het uitvoeren van de eerste drie interviews toegevoegd. Dat werd gedaan om ervoor te zorgen dat er nog diepgaander op het topic privacy kon worden ingegaan. De andere 17 respondenten werden dus bevraagd op alle bovenstaande topics. Het is wel mogelijk dat deze extra topics terloops toch aan bod kwamen bij de drie respondenten.

Bij elk van de bovenstaande topics werden er verschillende vragen gesteld om na te gaan hoe de respondenten bepaalde handelingen in het dagelijkse leven uitvoeren en hoe ze tegenover het topic staan. De eerste drie topics, digitale mediagebruik, gedrag op sociale media en dagelijkse routine dienden vooral om na te gaan hoe vaak personen gebruik maken van digitale media en welke sites zij bezoeken. Het zijn als het ware een soort van inleidende topics om stapsgewijs over te gaan naar de concepten omtrent privacy.

Daarnaast werden de topics privacyinstellingen, cookies en formulieren bevraagd om te bekijken hoe de respondenten op internet omgaan met hun eigen privacy. Gaan zij net heel streng om met hun privacy of net niet? Door dat te bevragen kon ook nagegaan worden waarom bepaalde handelingen wel of niet gesteld worden en kan vastgesteld worden hoe zij staan t.o.v. hun eigen online privacy.

De topics transparantie en privacybeleid stroomden voort uit wat er tot nu toe al bekend is in de literatuur. Volgens de literatuur sporen een aantal strategieën van bedrijven digitale berusting net aan (Draper & Turow, 2019, pp. 1830-1833). Om dat te onderzoeken werden deze twee topics toegevoegd aan het onderzoek en werd de houding van de respondenten t.o.v. deze twee topics bevraagd.

De respondenten werd ook een vraag voorgeschoteld omtrent privacyinbreuken, dat om na te gaan of zij al geconfronteerd werden met een inbreuk op hun privacy in het verleden.

De laatste twee topics die besproken werden, zijn privacy in de media en de wetgeving omtrent privacy. Dat was vooral om na te gaan of de respondent enige kennis heeft over het topic en om te bekijken wat de respondenten vinden van de huidige wetgeving en of deze dient aangepast te worden. Vanuit de bevraging van deze topics kunnen namelijk een aantal aanbevelingen voortvloeien naar beleidsmakers toe. Volgens het onderzoek van Turow et al. (2015, p. 3) zouden bedrijven beleidsmakers namelijk misleiden omtrent de drijfveren van mensen om data te delen. Beleidsmakers worden dus verkeerd geïnformeerd wat een onevenwicht veroorzaakt in het beleidsdomein. Dit onderzoek wil op deze kwestie inspelen en een aantal aanbevelingen meegeven voor een krachtiger beleid omtrent privacy.

Aan de hand van alle bovenvermelde topics werd er achterhaald waarom respondenten zich wel of niet digitaal berust voelen en wat daar eventueel aan gedaan kan worden. De volledige topiclijst met alle bijhorende vragen kan u terugvinden in bijlage drie.

Visuele elementen

Tijdens de interviews was het oorspronkelijk de bedoeling om een aantal visuele elementen te tonen aan respondenten om zo diepgaandere antwoorden te bekomen.

De visuele elementen toonden telkens een handeling die online verricht moest worden, zoals het accepteren van cookies, het invullen van registraties of het instellen van privacyinstellingen. Er werden in totaal vijf visuele elementen gebruikt. Deze visuele elementen kan u terugvinden in bijlage vier. Door de coronacrisis werden de visuele elementen echter maar aan drie respondenten getoond. Hieronder volgt meer uitleg.

Het uitvoeren van de interviews

Het was oorspronkelijk de bedoeling om het interview face to face met de respondenten te houden en om tijdens de interviews een aantal visuele elementen te tonen. Het empirisch onderzoek was echter net voor de opkomst van de coronacrisis gestart waardoor er maar drie respondenten face to face konden worden gesproken en waardoor de visuele elementen maar aan drie respondenten konden worden getoond. De resterende interviews werden online gehouden via de hulpmiddelen Skype, WhatsApp en Messenger. Natuurlijk brengt dit een aantal belemmeringen met zich mee zoals problemen met de verbinding en het niet deftig kunnen tonen van de visuele elementen. Het was namelijk storend om het online interview te onderbreken om een visueel element te tonen.

8.6. De verwerking en analyse van de interviews

Na het afnemen van de interviews, dienden ze correct te worden geanalyseerd om te kunnen nagaan wat het resultaat van het onderzoek nu precies was. De interviews werden stuk voor stuk getranscribeerd. Deze transcripties kan u niet terugvinden in dit document. Deze staan namelijk in een aparte bijlage. De namen van de originele respondenten werden daarbij vervangen door pseudoniemen. De namen die u zal terugvinden in deze masterproef zijn dus fictief en hebben geen enkel verband met de respondenten.

Nadien werd elk interview ook geanalyseerd aan de hand van het programma MAXQDA. Daarbij werd er een codeboom opgesteld aan de hand van de literatuur en de topics in het interview. Deze codeboom kan u terugvinden in bijlage zes. Elk interview werd dus onderworpen aan een analyse aan de hand van deze codeboom. Daardoor konden de verschillende gecodeerde antwoorden makkelijk en gestructureerd met elkaar vergeleken worden.

Er werd bij de analyses in MAXQDA ook een onderscheid gemaakt tussen de niveaus van privacy geletterdheid. Dat niveau werd bepaald aan de hand van de test.

9. Resultaten

9.1. Beoordeling van de testen

In dit onderzoek werden de respondenten onderworpen aan een test waar twee aspecten werden bekeken, namelijk het niveau van privacy geletterdheid en het al dan niet digitaal berust zijn. Na het uitvoeren van de tests en de interviews blijkt echter dat de tests naar de toekomst toe nog voor verbetering vatbaar zijn.

De OPLIS-test die werd opgesteld door Masur et al. (2017) bevraagt privacy geletterdheid op vijf verschillende domeinen, namelijk institutionele praktijken, technische aspecten van databescherming, databeschermingswetgeving en strategieën voor databescherming. Wat echter is gebleken uit de ingevulde tests is dat van de 20 respondenten geen enkele respondent lager scoorde dan 10/20 (zie tabel 1 op p. 32). Er kunnen verschillende verklaringen zijn voor dat verschijnsel. Een eerste verklaring zou zijn dat elk van de uitgekozen respondenten een matige tot goede kennis van privacy had. Verschillende respondenten gaven echter aan weinig tot geen kennis te hebben van het concept privacy. Toch scoorden zij tussen de 10 en 13 op 20 op de test. Het is natuurlijk altijd mogelijk dat zij een onderschatting maakten van hun eigen kunnen, maar het is ook mogelijk dat zij door middel van eliminatie of gokken een aantal vragen juist beantwoordden. Tijdens het interview bleek dan ook dat een aantal respondenten die 10/20 scoorden geen kennis hadden van de manier waarop mediabedrijven gegevens kunnen gebruiken voor bepaalde doeleinden. Er waren daarentegen ook een aantal respondenten met 10/20 die bij bepaalde topics een hogere kennis bleken te hebben. Het is dus mogelijk dat de test geen volledig representatief beeld geeft van het niveau van privacy geletterdheid.

Een punt van verbetering zou dus zijn om de test uit te breiden of aan te passen. Een mogelijkheid zou zijn om de test uit te breiden met open vragen zodat men zich niet beperkt tot meerkeuzevragen. Eventueel een gis-correctie toepassen op de test zou er ook eventueel voor kunnen zorgen dat gokgedrag wordt afgestraft.

Een tweede punt aspect gaat over de manier waarop digitale berusting wordt vastgelegd. De digitale berusting werd vastgelegd aan de hand van twee stellingen, namelijk (Turow et al., 2015, p. 14):

- Ik wil controle kunnen uitoefenen over wat marketeers online over mij te weten kunnen komen.
- Ik heb geaccepteerd dat ik weinig controle kan uitoefenen over wat marketeers online over mij te weten kunnen komen.

In het onderzoek bleek dat alle respondenten op de eerste stelling ‘ja’ antwoordden. De tweede stelling werd echter een aantal keer met ‘nee’ beantwoord. Wanneer er op één van de twee stellingen ‘nee’ wordt geantwoord, wordt die persoon als niet-digitaal berust beschouwd.

Wat echter bleek uit de interviews is dat personen, die 'nee' antwoordden op de tweede stelling, deze vaak verkeerd interpreteerden.

> *"Ik weet dat dat oncontroleerbaar is. 'Ik heb geaccepteerd' is iets persoonlijk. In de ideale wereld zou dit allemaal niet gebeuren. Dit is niet ethisch verantwoord, maar naast dat is het wel zo werkbaar dus ik heb daar geen controle over. Accepteren, nee."*
> (Thomas, persoonlijke communicatie, 5 april 2020)

> "*Het is ook een heel brede vraag als je het woord accepteren gaat ontleden."*
> (Julian, persoonlijke communicatie, 31 maart 2020)

Een aantal respondenten gaven aan dat ze beseften dat ze geen controle kunnen uitoefenen over hun data, maar ze hebben dat op zich niet geaccepteerd. Ze vinden dergelijke praktijken eigenlijk nog altijd onacceptabel en onethisch. Ze hebben er zich bij neergelegd dat ze daar niets tegen kunnen doen, maar ze hebben niet geaccepteerd dat het oké is dat dit soort praktijken plaats vinden.

Wat dus opgemerkt kan worden, is dat de manier die Turow et al. (2015) in hun onderzoek gebruikten om digitale berusting vast te stellen geen 100% betrouwbare gegevens oplevert. Er zijn namelijk personen die volgens de test niet-digitaal berust zijn, maar tijdens interview dan toch tekenen van digitale berusting vertonen. De test meet dus als het ware niet wat het dient te meten waardoor er geen 100% waterdichte validiteit is.

Het zou dus noodzakelijk zijn om de tweede stelling op een andere manier te formuleren. Het woord 'accepteren' is vooral het struikelblok. Ze zouden bijvoorbeeld een iets neutralere formulering kunnen gebruiken zoals:

- Ik realiseer me dat ik weinig controle kan uitoefenen over wat marketeers online over mij te weten kunnen komen.

Daarbij omzeilt men het woord 'accepteren' en zal men geen problemen ondervinden bij personen die beseffen dat er geen privacy meer is, maar dat wel niet accepteren of niet fijn vinden.

9.2. Een overzicht van de respondenten

In totaal vulden 20 respondenten de test in en werden elk van deze 20 respondenten onderworpen aan een diepte-interview. Hieronder kan u van elke respondent het resultaat op de aangepaste OPLIS-test terugvinden en wordt aangegeven of de respondent in kwestie digitaal berust is of niet (zie tabel 1). Zoals besproken werd in het onderzoeksdesign werden de originele namen van de respondenten niet gebruikt. De namen die u in de tabel terugvindt, zijn dan ook fictief.

Zoals hierboven al werd aangehaald, zijn de testen echter niet 100% representatief voor de werkelijkheid. Er zitten een aantal tekortkomingen in de testen. Er werd dus op basis van het interview bekeken of een respondent een eerder hogere of lagere score verdiende op vlak van privacy geletterdheid. Na het interview werd er tevens nagegaan of het resultaat van de test omtrent digitale berusting de werkelijkheid representeerde. Er werd dus ook hier een nieuwe waarde toegekend wanneer daar aanleiding toe was.

RESPONDENT	**SCORE OP DE OPLIS-TEST**		**DIGITAAL BERUST OF NIET?**	
	Volgens de test	**Volgens het interview**	**Volgens de test**	**Volgens het interview**
Elke	13/20	Zelfde score	Ja	Ja
Emma	15/20	Zelfde score	Ja	Ja
Tessa	17/20	Zelfde score	Nee	Ja
Laura	15/20	Zelfde score	Ja	Ja
Veronique	16/20	Zelfde score	Ja	Ja
Amelie	15/20	Zelfde score	Ja	Ja
Thibeau	15/20	Zelfde score	Ja	Ja
Daan	10/20	Lagere score	Ja	Ja/Nee
Daniël	10/20	Lagere score	Ja	Ja
Ralf	19/20	Zelfde score	Nee	Ja
Hannah	12/20	Lagere score	Ja	Ja/Nee
Rosa	13/20	Hogere score	Ja	Ja
Lana	15/20	Zelfde score	Nee	Ja
Samantha	12/20	Hogere score	Ja	Ja
Julian	17/20	Zelfde score	Nee	Ja/Nee
Dimitri	16/20	Zelfde score	Ja	Ja
Emily	14/20	Zelfde score	Nee	Ja
Thomas	15/20	Hogere score	Nee	Ja
Alice	11/20	Hogere score	Ja	Ja
Camille	11/20	Lagere score	Ja	Ja

Tabel 1: Gegevens respondenten

Uit de tabel blijkt dat iedere respondent op z'n minst een bepaalde vorm van vorm van digitale berusting vertoont terwijl de test dit niet altijd aantoonde. Sommige respondenten zoals onder andere Julian of Hannah gaven aan dat ze bijvoorbeeld ook proberen de voordelen in te zien van het verzamelen van gegevens of dat ze er zich gewoon niet mee bezig houden. Daarnaast zeggen ze wel dat ze beseffen dat er gegevens worden verzameld en dat ze dat op zich niet altijd oké vinden, maar dat ze er eigenlijk niets aan kunnen doen. Ze vertonen dus tekenen van digitale berusting, maar er spelen wel nog andere factoren mee. Omdat zij dus bij de nieuwe waarde ook deels als digitaal berust worden beschouwd, zullen hun antwoorden tevens opgenomen worden in de resultaten.

Zoals tabel 1 aangeeft, heeft geen enkele respondent onder de 10/20 gescoord op de OPLIS-test. Bij de start van dit onderzoek werd vermeld dat respondenten zouden worden opgedeeld in klassen op basis van een 10 op 20. Door de bekomen resultaten is dat echter niet mogelijk en zullen er andere niveaus worden gehanteerd bij het analyseren van de interviews:

Lagere privacy geletterdheid	**Gemiddelde privacy geletterdheid**	**Hogere privacy geletterdheid**
10 – 13 op 20	14 – 15 op 20	16 – 20 op 20

Tabel 2: Niveau van privacy geletterdheid

Er kan uit de tabel ook afgeleid worden dat sommige respondenten na de interviews een eerder hogere of lagere privacy geletterdheid zouden hebben dan uit de test naar boven kwam. Omdat er echter gewerkt wordt met klassen om de resultaten van respondenten te analyseren, zal dat geen invloed hebben op hoe de resultaten worden onderzocht. Iemand die op basis van de OPLIS-test in de categorie lagere privacy geletterdheid past, zal ook in deze categorie blijven. Het zou namelijk te veel giswerk zijn om iemand een exacte score van privacy geletterdheid toe te kennen op basis van het interview. Er zal in de resultaten wel vermeld worden waarom er gedacht wordt dat sommige een hogere of lagere score verdienen.

9.3. Resultaten uit de interviews

Digitale mediagebruik

Frequentie van het digitale mediagebruik

Bij elk interview werden er allereerst een aantal inleidende vragen gesteld omtrent het digitale mediagebruik van de respondenten. Er werd dan ook nagegaan hoe vaak een persoon gebruik maakt van digitale media. In het interview werd zowel sociale media als ander gebruik van het internet via de gsm, de computer, de tablet of andere technologieën bestempeld als digitale media. Zowel hoge, gemiddelde als lagere privacy geletterden maken dagelijks gebruik van dergelijke technologieën. Geen enkele respondent sprak dat gegeven tegen. Het ging daarbij vaak zelfs over een gebruik van meerdere keren of zelfs meerdere uren per dag.

Er kan dus besloten worden dat digitale media in 2020 absoluut een weg gevonden heeft naar onze dagdagelijkse gewoonten.

> *"Ja, sowieso wel dagelijks. Hoeveel keer op een dag? Dat hangt ervan af waar ik mee bezig ben op een dag, maar ik zou gemiddeld zoiets zeggen tegen de 10 keer op een dag dat ik op mijn gsm kijk."* (Emma, persoonlijke communicatie, 10 maart 2020)

> *"Als ik daar heel eerlijk in ben, is dat eigenlijk wel om het uur, denk ik (lacht)."*
> *(Emily, persoonlijke communicatie, 2 april 2020)*

Gebruik van sociale media

Uit de interviews bleek dat het grootste deel van de respondenten toch gebruik maakt van sociale media tijdens de vrije tijd. Om daar een aantal op te plakken: 15 respondenten gaven aan regelmatig gebruik te maken van sociale media, 2 respondenten gebruiken sociale media maar af en toe en nog eens drie respondenten gebruiken het nooit.

Een eerste algemene bevinding bij het gebruik van sociale media is dat er enkel binnen de groepen met hogere en middelmatige privacy geletterdheid personen voorkomen die geen gebruik maken van sociale media. Zij halen daarvoor twee belangrijke redenen aan, namelijk privacy en een gebrek aan nut.

Bij de groep met een lagere privacy geletterdheid komen er geen personen voor die geen gebruik maken van sociale media. Er is wel iemand die er in mindere mate gebruik van maakt, maar privacy wordt daarvoor niet als reden aangehaald. Wat ook opgemerkt kan worden bij personen met een lagere privacy geletterdheid is dat er verschillende malen aangegeven wordt dat men sociale media gebruikt om te kunnen bekijken wat andere personen uit hun netwerk precies doen.

<u>Frequent gebruik van sociale media</u>

De eerste en meest voorkomende reden om sociale media te gebruiken is om in contact te blijven met andere personen uit het eigen netwerk. Communicatie is dus een belangrijke drijfveer.

> *"Ik ben daar eigenlijk vooral op, omdat ik in contact wil blijven met mijn dichte vrienden en soms ook een keer met een verre vriend ofzo, maar dat is dan meer echt sturen"*
> (Lana, persoonlijke communicatie, 2 april 2020)

De tweede meest voorkomende reden om sociale media te gebruiken is om te kijken naar wat andere personen of groepen uit het netwerk zoal doen in hun leven. Er wordt zelfs aangehaald dat men zich soms als een spion gedraagt, wat natuurlijk wel als metafoor dient. Deze reden wordt wel alleen maar aangehaald in de groep van respondenten met een lagere privacy geletterdheid.

> *"Maar ik ben wel vooral actief om te zien wat andere mensen doen. Een soort spion."*
> *(*Daniël, persoonlijke communicatie, 23 maart 2020):

> *"Bijvoorbeeld bij Instagram vind ik het ook gewoon leuk om in mensen hun dagelijks leven te kunnen kijken (lacht). En dan Facebook is gewoon meer het up-to-date blijven van gebeurtenissen." (*Samantha, persoonlijke communicatie, 30 maart 2020)

Om verder te gaan op de voorgaande quotes is het wel opvallend dat er maar één persoon aangeeft sociale media te gebruiken om anderen een beeld te geven van haar eigen leven. Deze persoon, Rosa, bevindt zich ook in de groep met een lagere privacy geletterdheid.

> *"Terwijl Instagram is iets dat ik vaker bekijk, omdat ik er zelf ook meer op post. Selfies, wat ben ik aan het doen, stories, enzovoort. Dus eigenlijk meer een beeld op mijn dagelijks leven."* (Rosa, persoonlijke communicatie, 28 maart 2020)

Een andere reden is het feit dat het aanmaken van een socialemediaprofiel ook afhangt van peer pressure. Het aanwezig zijn van vrienden of familie op een bepaald socialemediakanaal, geeft aanleiding om er zelf ook gebruik van te maken. Beïnvloeding speelt dus een rol. Emma verwoordt dit bijvoorbeeld op een nog specifiekere manier. Het zou volgens haar nu eenmaal deel van het dagelijkse leven geworden zijn.

> *"En Instagram dat is gekomen een paar jaar geleden, omdat iedereen dat ook begon te krijgen. Dat ik ook zei: ik zal dat ook aanmaken." (*Lana, persoonlijke communicatie, 2 april 2020)

> *"Because of life (lacht)." (*Emma, persoonlijke communicatie, 10 maart 2020)

Niet alleen de druk van anderen zou een rol spelen, maar ook de manier waarop bedrijven zaken weergeven is van belang. Soms hebben bezoekers van websites geen toegang tot bepaalde content als ze geen bepaald socialemediaprofiel aanmaken. Dat zou een strategie van bedrijven kunnen zijn om ervoor te zorgen dat er meer accounts worden aangemaakt om zo meer gegevens te bekomen.

> *"Als je zo ergens in een artikel Tweets ziet en je wilt die lezen of die filmpjes bekijken, heb je een Twitteraccount nodig om dat te kunnen doen."*
> *(*Rosa, persoonlijke communicatie, 28 maart 2020)

Als voorlaatste reden komt verslaving naar voor. Sociale media zou een bepaalde verslavingsfactor hebben waardoor men toch telkens teruggezogen wordt en men er toch gebruik van wilt maken.

> *"Maar om de een of andere manier is dat toch zo wel een verslaving. En dat dat u toch altijd zo terugtrekt. Ik weet niet hoe dat ik dat moet uitleggen."*
> (Elke, persoonlijke communicatie, 7 maart 2020)

De laatste twee redenen die voorkwamen tijdens de interviews is het feit dat 1. sociale media ook gebruikt wordt voor schoolverbanden en 2. daarnaast ook bepaalde onderwerpen bevat die in de lijn van iemands interesses kunnen liggen.

> "*Vooral voor de groepen van schoolverbanden dan ook en groepswerken en die zaken."*
> (Laura, persoonlijke communicatie, 14 maart 2020)

"Maar aangezien er ook heel veel op jouw Facebook verschijnt naar reclame toe en dingen die jou interesseren dan blijf je wel langer hangen op Facebook."
(Emily, persoonlijke communicatie, 2 april 2020)

Weinig tot geen gebruik van sociale media

De respondenten die geen of heel weinig gebruik maken van sociale media geven allemaal vergelijkbare redenen aan daarvoor. Een eerste en voornaamste reden is het gebrek aan privacy. De respondenten halen aan dat er op sociale media informatie over de gebruiker wordt verzameld en dat ze daar niet altijd controle over hebben.

"En het feit dat je gewoon geen privacy meer hebt. Dat is uiteraard voor een deel afhankelijk van hoe je er zelf voor een deel mee omgaat, maar nee, het staat mij niet aan."
(Ralf, persoonlijke communicatie, 23 maart 2020)

Daarnaast blijkt een gebrek aan interesse in het gebruik van sociale media ook een rol te spelen. Ze zien het nut van sociale media niet in of hebben liever persoonlijke contacten met andere personen. Thomas geeft bijvoorbeeld aan dat hij sociale media als een soort voyeurisme ziet.

"Waarom niet? Sociale media als ik het goed voorheb, is dat eigenlijk bedoeld om ook heel veel sharing te doen. Voor mij is dat een vorm van voyeurisme. Ik vind dat eigenlijk niet interessant wat mensen allemaal delen. (…) Dat hangt er een beetje vanaf wie dat je volgt. Afhankelijk van de, hoe moet ik het zeggen, topics die mensen allemaal niet delen. Het kan mij niet veel interesseren. Het is gewoon banaal, niet interessant en narcistisch. Dus daarom dat ik sociale media zoveel als mogelijk probeer te vermijden, omdat het eigenlijk geen belangrijke inhoudelijke bijdrage levert aan wat ik interessant vind."
(Thomas, persoonlijke communicatie, 5 april 2020)

"Het was wel leuk om contacten te blijven houden met mensen, maar ik ging nog naar school dus het sociaal contact had ik wel in levende lijven. En ik dacht dat is voor mij wel genoeg en uiteindelijk heb ik toch wel besloten om die Facebook te verwijderen. Ik had daar niet echt een toegevoegde waarde aan." (Dimitri, persoonlijke communicatie, 1 april 2020)

Houdt het topic privacy de respondenten bezig?

Dit onderzoek wil vooral onderzoeken waarom bepaalde gebruikers van digitale media zich digitaal berust voelen. Het wil echter niet zeggen dat wanneer een persoon digitaal berust is dat hij/zij zich niet bezig houdt met het topic. Binnen de respondenten kan men drie groepen onderscheiden. Allereerst heb je de grootste groep waarbij respondenten zich niet echt zorgen maken over het feit dat hun privacy onder druk staat. Ongeveer de helft van de respondenten behoort tot deze groep. Daarnaast heb je de groep die zich wel bekommert om zijn/haar privacy en toch reflecteren over het topic. Vijf respondenten behoren tot deze groep. Zij zullen niet per se altijd actie ondernemen, maar ze houden het aspect privacy wel in hun achterhoofd. Daarnaast onderkennen ze ook dat eventuele acties niet altijd vruchten afwerpen. De laatste groep, met ook vijf respondenten, bevinden zich ergens tussenin en zijn noch echt bezorgd, noch onverschillig. Wat wel opvalt, is dat vooral personen met een gemiddelde en hogere privacy geletterdheid zich zorgen maken en nadenken over hun eigen privacy. Dat wil echter niet zeggen dat er zich niemand binnen de groep met lagere privacy geletterdheid mee bezig houdt. De groep is gewoon minder vertegenwoordigd.

Bij de eerste groep waar men zich geen zorgen maakt, is er dus een soort van onverschilligheid omtrent het thema. Alice en Thomas verwoorden dit zeer duidelijk:

> "*Dat is nu eenmaal zo, denk ik. Ik lig daar niet van wakker.*"
> (Alice, persoonlijke communicatie, 7 april 2020)

> "*Dat houdt mij nu niet zo hard bezig. Aangezien dat privacy compleet overroepen is.*"
> (Thomas, persoonlijke communicatie, 5 april 2020)

Daarnaast zijn er dus ook respondenten die reflecteren over het topic privacy.

> "*Ja, awel ja. Ik vind dat wel een beetje eng eigenlijk als ik daarover nadenk. Ik hoor veel mensen zo zeggen dat maakt toch niet uit. Ik heb niets te verbergen. Het is niet dat ik wel iets te verbergen heb. Het is gewoon, ik vind dat gewoon geen leuk gegeven dat iedereen zomaar dingen weet.*" (Lana, persoonlijke communicatie, 2 april 2020)

Daarnaast verwoordt Ralf goed het algemene gevoel bij de groep die er zich ergens tussenin bevindt, qua bezorgdheid omtrent hun eigen privacy.

> "*Tussen de twee. Ik leg mij daar niet bij neer. Lig ik daar wakker van? Niet letterlijk.*"
> (Ralf, persoonlijke communicatie, 23 maart 2020)

Wat hier ook wel naar boven komt, is dat confrontatie een belangrijk aspect vormt. Men zal vaak privacy pas in acht nemen als men er echt mee geconfronteerd wordt.

> "*Ik merk het eigenlijk pas op als ik ermee geconfronteerd word.*"
> (Amelie, persoonlijke communicatie, 18 maart 2020)

Gedrag op digitale media

Cookies

Bij het gedrag t.a.v. cookies blijkt dat een merendeel van de respondenten cookies aanvaardt. Van de 20 respondenten waren er slechts vier die cookies niet aanvaarden. Daarbij kon er ook geen verschil worden opgemerkt tussen hoge, gemiddelde en lage privacy geletterden. In elke groep waren er telkens maar één of twee personen die wel verder keken en probeerden om op z'n minst te zoeken naar de minimale cookies. Omwille van die reden zal er hieronder vooral een overzicht gegeven worden van de verschillende verklaringen en wordt er geen onderscheid gemaakt tussen hoge of lagere privacy geletterdheid.

Verklaringen voor het aanvaarden van cookies

Eén van de meest opgegeven redenen voor het aanvaarden van cookies, is het feit dat de websites bezoekers vaak geen keuze geven. Men zou gewoon niet verder kunnen surfen naar een bepaalde website. Websites zouden bezoekers dus dwingen om hun data mee te geven in ruil voor de diensten van de website.

> *"Ja, meestal is dat zo … kan je niet echt naar een site kijken zonder die te aanvaarden. Dus dan heb je ook weer niet echt een keuze."* (Tessa, persoonlijke communicatie, 10 maart 2020)

Cookies worden volgens de verschillende respondenten vaak ook omslachtig weergegeven waardoor men geen zin heeft om die dan te lezen. Volgens Emma is een volledig werkende website belangrijker dan cookies aanvaarden.

> *"Waarom? Omdat ik heel vaak geen goesting heb om dat te lezen en een voor een te gaan aanschuiven of afschuiven of ja of nee te selecteren. Ook weer omdat het heel omslachtig omschreven is op websites. Waardoor ik ook wel zoiets heb van ja soit laat mij alles aanvaarden. Dan weet ik dat ik een werkende website heb. Ja, daarvoor vooral."*
> (Emma, persoonlijke communicatie, 10 maart 2020)

Emma geeft aan dat websites ook vooral willen dat gebruikers cookies aanvaarden. Ze zouden er namelijk op inspelen dat personen bepaalde informatie snel willen, want als men geen tijd heeft om cookies te lezen of na te kijken, zullen ze waarschijnlijk vaker gewoon worden aanvaard.

> *"Daar spelen ze wel echt op in van die willen nu die informatie."*
> (Emma, persoonlijke communicatie, 10 maart 2020)

Emma haalt daarnaast ook aan dat het moeilijk is om een overzicht te bewaren over alle sites die cookies verzamelen, over wat ze verzamelen en over wat de uiteindelijke gevolgen van die gegevensverzameling zijn. Er zou dus ten eerste geen duidelijk overzicht zijn over door wie en hoe gegevens verzameld worden, maar daarnaast zouden zaken te onduidelijk worden geformuleerd waardoor men niet echt een idee heeft wat een cookie, in dit geval, betekent.

"Ja, ik vind dat ook heel moeilijk om daar overzicht op te krijgen, want heel vaak accepteer je er eentje en dan accepteer je weer niet. Maar vaak is dat niet te volgen van waar juist die impact dan voorkomt of niet. Ik vind dat heel onoverzichtelijk en het is ook niet altijd even duidelijk wat een cookie juist doet, vind ik." (Emma, persoonlijke communicatie, 10 maart 2020)

Verschillende respondenten hebben tevens het idee dat hun informatie toch verzameld zal worden wat ze ook proberen. Een gevoel dat het weigeren niet helpt, zet hen dan ook aan om ze toch accepteren.

"Ja, ze gaan toch altijd alles van u kunnen vinden"
(Daniël, persoonlijke communicatie, 23 maart 2020)

Ook zou het aanvaarden van cookies gewoon normaal zijn geworden in ons dagelijkse leven. Het maakt er gewoon deel van uit. Het is iets eigen aan het internet.

"Het is een gewoonte geworden. Het is iets dat mensen hebben aanvaard, omdat dat nu eenmaal deel is van het internet denk ik ja." (Alice, persoonlijke communicatie, 7 april 2020)

Kennis blijkt tevens een rol te spelen. Emily geeft namelijk aan dat ze nog niet zo lang weet wat een cookie exact betekent. Ze had dus als het ware een fout beeld van wat een cookie precies doet. Het feit ze dat nu wel weet heeft echter geen impact op het accepteren van cookies of niet. Ze gaat er naar eigen zeggen wel bewuster mee om door haar browsergeschiedenis te wissen.

"En ook als ik eerlijk moet toegeven, ik weet ook nog niet zo heel, heel lang wat cookies zijn."
(Emily, persoonlijke communicatie, 2 april 2020)

Een aspect dat nog niet aan bod kwam, is het feit dat respondenten eigenlijk verlost willen zijn van de meldingen die ze krijgen omtrent cookies en dergelijke. Dat wordt maar aangehaald door twee respondenten die elk een lager niveau van privacy geletterdheid hebben. Het impliceert wel dat personen geen verdere tijd willen steken in het beschermen van de eigen privacy.

"En waarom omdat ik er gewoon vanaf wil zijn van die melding. Echt waar."
(Elke, persoonlijke communicatie, 7 maart 2020)

Daarnaast geeft Elke ook aan dat de pop-ups met cookies vaak een andere lay-out hanteren naargelang de optie die ze vertonen. De optie 'accepteren' staat vaak in het groot, terwijl de optie 'meer informatie' veel saaier wordt weergegeven. Dat zou impliceren dat websites proberen om mensen in een bepaalde richting te duwen. Elke is wel de enige persoon die dat aanhaalt.

"Met die cookies geven ze je inderdaad de keuze van: meer info dat je kan doorlezen en aanpassen of gewoon 'ik accepteer cookies', maar de lay-out is ook wel anders (er wordt terug verwezen naar het visuele element). Hier is het in het groot en wit en dat valt op en bij de informatie-instelling is het zo saai. " (Elke, persoonlijke communicatie, 7 maart 2020)

Er is eigenlijk maar één iemand die de voordelen van cookies inziet. Julian beseft langs de ene kant wel dat er gegevens over hem verzameld worden en hij vindt dat op zich niet aangenaam, maar langs de andere kant ziet hij het voordeel in van het bestaan van cookies. Cookies zorgen ervoor dat bepaalde instellingen onthouden worden, wat het gebruiksgemak verhoogt. Julian is dus wel digitaal berust, maar dat is niet de enige factor die meespeelt. De 'gratification theory' komt hier dus aan bod.

> *"Meestal accepteer ik die direct, omdat die vaak in mijn voordeel zijn. Bijvoorbeeld welke taal gebruik je? De volgende keer dat je naar de website gaat, kan je direct die taal zien."*
> *(*Julian, persoonlijk communicatie, 31 maart 2020)

Daarnaast geeft Julian aan dat cookies op dit moment nog geen bedreiging vormen voor de persoonlijke gegevens. Het feit dat Julian op dit moment nog geen negatieve gevolgen ondervindt, zorgt ervoor dat hij geen extra actie onderneemt en cookies accepteert.

- *Interviewer: "Oké, dus cookies zie jij niet echt als een gevaar, laten we het zo maar omschrijven, voor jouw gegevens?"*
- *Julian: - Korte pauze - Nee, nog niet nee"*
  (Julian, persoonlijke communicatie, 31 maart 2020)

<u>Redenen voor het niet aanvaarden van cookies</u>

Veronique is één van de respondenten die aangaf dat ze cookies toch zo veel mogelijk probeert te minimaliseren. Zij is dus één van de weinige in dit onderzoek die cookies niet direct accepteert. Zij geeft daarbij aan dat ze dat vooral doet uit onwetendheid van wat er allemaal gebeurt met de gegevens. Dat het onduidelijk is welke gegevens er allemaal aan wie worden doorgestuurd. Ook worden de eigen gegevens als niet belangrijk genoeg bestempeld, waardoor men denkt dat ze niet interessant zullen zijn voor bedrijven.

> *"Nee, ja uit schrik voor mijn gegevens. Allee ja uit schrik is wat overdreven. Of misschien uit onwetendheid van niet weten wat er allemaal met uw gegevens zou kunnen gebeuren of aan wie dat ze dat allemaal gaan doorgeven. Niet dat ik dan denk dat dat zo veel gegevens zijn of zo belangrijke gegevens of dat die naar ik weet niet waar gaan gestuurd worden, maar toch …"*
> *(Veronique, persoonlijke communicatie, 16 maart 2020)*

Dimitri is ook een persoon die cookies probeert te vermijden. Hij geeft namelijk aan dat hij geen meerwaarde ziet in het accepteren van cookies. Dimitri gelooft wel niet dat het vermijden van cookies veel uithaalt. Volgens hem zullen websites nog altijd gegevens verzamelen en bewaren, waaronder bijvoorbeeld het IP-adres.

> *"Ja, toch ja. Ik weet zij hebben sowieso informatie van uw pc of van uw IP-adres of wat dan ook, maar ja toch doe ik het. Toch doe ik het. Als ze vragen om die cookies te bewaren, doe ik het niet. Want ja, ik heb zoiets van ik heb daar geen meerwaarde aan. Ik heb heel snel internet en ik heb toch wel geduld. Als een pagina niet snel genoeg laadt, wacht ik een beetje of wat dan ook."* (Dimitri, persoonlijke communicatie, 1 april 2020)

Wat ook voorkomt, is dat personen die aangeven cookies te weigeren dat niet altijd doen. Lana is bijvoorbeeld een persoon die cookies eerder niet aanvaardt dan wel, maar wat ook blijkt, is dat nut toch wel een rol speelt. Moest een website een groot nut met zich meebrengen, zou ze de cookies toch aanvaarden ook al doet ze dat normaal niet. Nut blijkt dus een belangrijke drijfveer.

> "*Maar moest het wel op bepaalde andere sites zijn waar ik wel echt iets wil lezen dan zou ik het wel accepteren, denk ik."* (Lana, persoonlijke communicatie, 2 april 2020)

Het privacybeleid

Opnieuw kan vastgesteld worden dat van de 20 respondenten er slechts enkelen een privacybeleid lezen. Grofweg las maar ¼ een gedeelte of een volledig privacybeleid. De andere respondenten gaven vrij duidelijk aan het niet te lezen. Wat daarbij opvalt, is dat zowel personen die een privacybeleid lazen als diegene die dat niet deden, aangaven dat deze zeker niet optimaal is en dat er verschillende verbeterpunten zijn.

Bij het aspect privacyverklaringen is er een gelijkenis tussen respondenten met een hogere en lagere privacy geletterdheid terug te vinden. De meest voorkomende reactie op een privacybeleid, is het feit dat een privacybeleid vaak te lang en te academisch is. Dat aspect werd door elke respondent, ongeacht het niveau van privacy geletterdheid, aangehaald. Men heeft dus kritiek op de manier waarop een privacybeleid wordt opgesteld. Het is een te moeilijke tekst waarbij het te lang duurt om het te lezen.

> *"Hoe het geschreven werd? Ik vond dat heel academisch. Ik denk dat jongere gebruikers daar heel weinig aan gaan hebben. En tegelijk oudere gebruikers ook niet door al die nieuwe technologische termen die daarin staan. (…) Ik zeg het, daar zit al een eerste laag van vaagheid."* (Laura, persoonlijke communicatie, 14 maart 2020*)*

> *"Omdat dat ook allemaal heel veel tijd neemt. Ja en tijd is vandaag gewoon iets heel kostbaar. Alles moet snel gaan."* (Emily, persoonlijke communicatie, 2 april 2020)

Naast deze gelijkenis is er ook een verschil op te merken. Zo blijken personen met een hogere of meer gemiddelde privacy geletterdheid op te merken dat bedrijven een privacybeleid vaak expres op een bepaalde manier opstellen om ervoor te zorgen dat gebruikers hem niet lezen. Thomas en Ralf verwoorden dit zeer goed. Wat wel opvalt, is dat dit enkel wordt gezegd door personen met een hogere privacy geletterdheid.

> *"Die zijn ook zo ellenlang opgemaakt om geen gaten natuurlijk te hebben in hun juridische gegevens, maar waarschijnlijk ook voor een deel om mensen af te schrikken om dat te lezen. Want als je leest, begin je je af te vragen waarom je in godsnaam akkoord zou drukken."*
> (Ralf, persoonlijke communicatie, 23 maart 2020)

> *"Dat is enerzijds een heel slimme zet van de makers van zo'n document. Het lekker lang maken, liefst archaïsch taalgebruik zodat de grootste hoop van de mensen het niet eens begrijpen als ze het lezen"* (Thomas, persoonlijke communicatie, 5 april 2020)

Er komen naast de grootste verschillen en gelijkenissen tussen hogere en lagere privacy geletterden nog een aantal andere aspecten aan bod. Deze kan u hieronder terugvinden.

Wat werd er nog gezegd over privacyverklaringen?

Allereerst werden er een aantal zaken aangehaald die hetzelfde zijn als bij de cookies. Zo heb je vaak geen keuze en moet je die privacyverklaringen en cookies aanvaarden. Tessa spreekt daarover. Daarnaast vermeldt bijvoorbeeld Thomas ook dat het gewoon opnieuw een gewoonte is geworden en dat het een deel vormt van ons dagelijkse leven.

> *"Ja, je kan het niet meer gebruiken als je het niet aanvaardt. Dus je hebt op zich geen keuze. Dus je kan wel een andere aanbieder zoeken ofzo, maar ja zeker bij Google ofzo. Ja, je vindt niet zo gemakkelijk een substituut daarvoor."*
> (Tessa, persoonlijke communicatie, 10 maart 2020)

> *"Zolang dat je het zo snel mogelijk weg klikt … Dat zijn gewoon ambetante … allee dat is al een gewoonte he door akkoord te gaan."* (Thomas, persoonlijke communicatie, 5 april 2020)

Er wordt ook aangehaald dat een vorm van luidheid meespeelt. Dat zou betekenen dat mensen gewoon geen zin hebben om zich met dergelijke zaken bezig te houden. Ook spreekt Elke van het feit dat 90% van de gebruikers dit niet lezen. Dat kan ook aanduiden dat dat een reden is waarom Elke ze zelf niet leest, omdat anderen dat net ook niet doen. Een derde reden die door Elke aangehaald wordt, is het feit dat ze niet 100% zeker is dat eventuele maatregelen om je privacy te beschermen zouden helpen. De digitale berusting is dus prominent.

> *"Misschien is het ook weer een vorm van luiheid, omdat ik ook maar die cookies accepteer. Maar ja ik vraag mij dan af wie zou dat dan wel doen. Want toch 90% dat dat toch niet doet. Ook al kan dat wel een grote invloed hebben op wat dat ze sturen en wat dat ze bijhouden enzovoort. Ook al weet je natuurlijk niet 100% zeker van is dat ook echt wel zo."*
> (Elke, persoonlijke communicatie, 7 maart 2020)

Wat hier door Daan wordt aangehaald, is dat er heel veel updates worden gegeven van een privacybeleid. Dat zou dus een reden zijn waarom gebruikers deze niet lezen. Het zouden namelijk telkens updates zijn waar meer een paar woorden of punten aan veranderd zijn, waardoor de gebruiker van de website het nut er niet van inziet om het privacybeleid opnieuw te lezen. Het feit dat bedrijven updates sturen kan dus een bepaald gedrag in de hand werken, namelijk het niet lezen van een privacybeleid en bijgevolg het minder goed beschermen van iemands privacy.

> *"Ik kan dat een beetje vergelijken met een persoon die je ook kent, namelijk professor B. Een zin of een woord of een komma die verplaatst wordt of die verwijderd wordt dan krijgen we die mail over dat privacybeleid toch terug. Dan is dat aangepast. Dus dan moeten we heel dat beleid opnieuw aflezen en goedkeuren."* (Daan, persoonlijke communicatie, 20 maart 2020)

Een laatste puntje dat tevens naar boven komt, is het feit dat bedrijven privacyverklaringen enkel maken om zichzelf toe te dekken. Het zou dus niet in het voordeel zijn van de gebruiker dat een privacybeleid wordt opgesteld, maar eerder in het voordeel van bedrijven. Dat kan ook het gedrag van gebruikers sturen. Als ze toch het gevoel hebben dat een dergelijk beleid niet in hun eigen belang is dan zullen ze dit bijgevolg ook niet lezen en zullen ze er daardoor misschien ook minder in slagen om hun eigen privacy te beschermen.

> *"Dat dat meer is om hun eigen in te dekken. (…) Ja, ik denk dat het meer in hun voordeel is dan in de gebruiker zijn voordeel."* (Samantha, persoonlijke communicatie, 30 maart 2020)

Beschermt een privacybeleid gebruikers?

Volgens de literatuur zouden personen een verkeerd beeld hebben van wat een privacybeleid in een bedrijf precies inhoudt. Men zou namelijk denken dat het puur bestaan van een privacybeleid ook automatisch leidt tot het beter beschermen van de privacy van de gebruikers. Dat is echter niet correct (Draper & Turow, 2019, p. 1831; Turow et al., 2015, p. 8). In de interviews werd dan ook gevraagd of men denkt dat een privacybeleid gegevens beter beschermt.

Wat opgemerkt kan worden bij de antwoorden uit de interviews, is dat er in elke groep wel iemand aangeeft dat een privacybeleid niet altijd de privacy van gebruikers beschermt of dat ze toch aanhalen dat bedrijven niet altijd de bedoeling hebben om de gegevens van gebruikers te beschermen. Er is dus zeker nuance nodig wanneer er naar resultaten gekeken wordt.

In de groep met een hogere privacy geletterdheid is er niemand die voluit 'ja' antwoordde op de vraag of een privacybeleid de privacy intrinsiek beter beschermt. Er zijn er wel een aantal die twijfelen. Bij de respondenten met een gemiddelde privacy geletterdheid geeft de overgrote meerderheid aan te twijfelen of een privacybeleid echt iets zou uithalen. Het is dus niet zo dat iedereen met een hogere of meer gemiddelde privacy geletterdheid 100% weet dat een privacybeleid niet beter beschermd. Bij de lagere privacy geletterden gaven vier respondenten aan te geloven dat een privacybeleid de privacy beter beschermd. De andere vier twijfelen of melden dat ze niet geloven in een betere bescherming. Er is dus enige nuance geboden, omdat niet iedereen binnen de groep met lagere privacy geletterdheid dezelfde mening heeft. Nuance is belangrijk!

<u>Hoge privacy geletterdheid</u>

Binnen deze groep van privacy geletterden blijkt dat er toch een aantal respondenten zijn die weten dat een privacybeleid geen garantie biedt op een betere bescherming van de privacy. Personen met een hoge privacy geletterdheid kunnen dus blijk geven van een hoge kennis omtrent een privacybeleid binnen een bedrijf.

> *"Wel, wat ik daaraan versta, is dat een bedrijf die krijgt uw persoonlijke gegevens en die gaat dat op een manier gebruiken. Die gaat uw ook een document laten ondertekenen, een privacyverklaring. Waarbij dat ze gaan verklaren: wij gebruiken die gegevens bijvoorbeeld voor economische doeleinden of voor marketingdoeleinden. Die worden dan verstuurd naar derde partijen en dat is eigenlijk ja in grotendeels wat een bedrijf doet met u persoonlijke informatie."*
> (Dimitri, persoonlijke communicatie, 1 april 2020)

> *"De privacywetgeving zal bijdragen tot het beschermen van mijn privacy, maar niet het privacybeleid van Facebook zelf. Want zij hebben geen nut van mij privacy te gunnen."*
> (Ralf, persoonlijke communicatie, 23 maart 2020)

Personen die volgens de test een hoge privacy geletterdheid hebben geven echter ook soms aan dat ze niet weten of een privacybeleid nu helpt of niet. Ze denken dat het misschien wel zou kunnen bijdragen, maar eigenlijk geven ze aan het niet te weten. Ze twijfelen dus eerder en zeggen niet volmondig 'ja'. Niet iedereen binnen de groep van hogere privacy geletterdheid heeft dus dezelfde kennis over bepaalde aspecten.

> *"- Korte pauze - Ik veronderstel van wel, maar dat weet ik niet precies. Ik veronderstel dat die privacybeleiden mijn privacy willen beschermen, maar dat weet ik niet precies. Daar ben ik onwetend in."* (Julian, persoonlijke communicatie, 31 maart 2020)

Gemiddelde privacy geletterdheid

Binnen de groep gemiddelde privacy geletterden zijn er personen die er volledig van overtuigd zijn dat een privacybeleid niet leidt tot een betere bescherming van de privacy en dat gegevens ook gewoon doorverkocht mogen worden.

> *"Ah ja dat ze gewoon jouw gegevens gaan gebruiken en dat ze dat ook gewoon mogen doorverkopen. Een lijst met e-mailadressen voor zoveel euro aan dat bedrijf en dan gaat die lijst door naar het volgende bedrijf. Dat is gewoon die massadata dat ik ook zij he."*
> (Emily, persoonlijke communicatie, 2 april 2020)

Er zijn ook respondenten in de groep met een gemiddelde privacy geletterdheid die aangeven dat het zou moeten bijdragen, maar toch twijfelen. Zo geeft bijvoorbeeld Amelie aan dat een privacybeleid er toch voor moet zorgen dat gegevens beter beschermd worden, maar dat er misschien achterpoortjes worden gebruikt om toch gegevens te kunnen verwerken. Zij twijfelt dus aan de effectiviteit van een privacybeleid. Ook Thomas twijfelt. Hij geeft aan dat men volgens de GDPR niet zomaar data mag delen, maar dat het toch niet altijd zeker zal zijn dat een bedrijf dat zal doen. Dus dat er geen 100% zekerheid is dat iemands data zal beschermd worden, omdat het eigenlijk niet te controleren valt.

> *"Dat ze gevoelige data niet zomaar kan veropenbaren. Cv's kunnen niet zomaar gestored worden zonder consent van de medewerkers. Bepaalde persoonlijke data kan niet zomaar in het openbaar vrijgegeven worden. Zelfs niet naar collega's toe bijvoorbeeld. Plus ook het recht om niet langer gekend te zijn bij dat … Dat men mij niet kan linken als persoon aan die documenten die daar zijn. Dat is het privacybeleid dat ze zouden moeten voeren. GDPR-gewijs. (…) Dus privacybeleid. Het is niet 100% zeker. Je kan een bedrijf vragen om alle data die ze over jou hebben te vernietigen. Dat is jou volste recht. Ik kan u zelfs vragen om een bewijs te leveren, maar ja dat is niet waterdicht he. Je zou al een externe partij moeten aanstellen om effectief te bewijzen dat de data effectief verwijderd is. Ik geloof daar niet echt in."*
> (Thomas, persoonlijke communicatie, 5 april 2020)

"Dus eigenlijk denk ik dat daar instaat dat de gegevens niet zomaar worden doorverkocht ofzo. Ja en vertrouwelijk worden behandeld. Maar ja onder bepaalde voorwaarden misschien en dat er misschien een voorwaarde bijstaat die wij gemakkelijk kunnen schenden allee."
(Amelie, persoonlijke communicatie, 18 maart 2020)

Er is daarnaast toch een persoon binnen deze groep die wel aangeeft te geloven dat een privacybeleid zou bijdragen. Ze geeft alleen aan niet te weten wat er nu precies instaat.

"Vooral de Europese Unie die de zaak heeft opgespannen, denk ik dat dat sowieso wel moet bijdragen, maar het is gewoon van wat staat er dan nu in? Maar ja, sorry dat is even geleden dus ik weet niet goed meer wat er juist instond."
(Laura, persoonlijke communicatie, 14 maart 2020)

<u>Lage privacy geletterdheid</u>

Binnen de groep van respondenten met een lagere privacy geletterdheid zijn er wel vier respondenten die aangeven dat ze toch geloven dat privacyverklaringen de gegevens, die je online achterlaat, op een bepaalde manier zal beschermen. Het feit dat er personen zijn die dit geloven, komt overeen met wat de wetenschappelijk literatuur daarover schrijft (Draper & Turow, 2019, p. 1381; Turow et al., 2015, p. 8).

"Dat ze uw gegevens niet gaan doorverkopen denk ik. Ja - korte pauze -. Als je dan op een site komt en je moet een privacybeleid tekenen, ik duid dat dan altijd gewoon aan. Ik heb dat nog nooit gelezen. Hoe erg dat dat ook klinkt." (Hannah, persoonlijke communicatie, 26 maart 2020)

- *Interviewer: "Kan ik daaruit afleiden dat jij het gevoel hebt dat een privacybeleid jouw privacy beter beschermd inderdaad of zie ik dat fout?"*
- *Daan: "- korte pauze - Nee, je ziet dat juist "*
  (Daan, persoonlijke communicatie, 20 maart 2020)

Hieronder wordt duidelijk dat niet iedereen met een lagere privacy geletterdheid het gevoel heeft dat een privacybeleid beter beschermt. Alice geeft bijvoorbeeld aan dat het fijn is als respondent dat je toch controle hebt over je privacy door middel van een privacybeleid. Alice zegt er wel direct bij dat het eigenlijk gaat om een vals gevoel van veiligheid en dat als je goed nadenkt, moet weten dat je uw informatie deelt met de wereld. Dat zou dus impliceren dat ze eigenlijk niet gelooft dat een privacybeleid gegevens volledig beschermt. Daarnaast wordt door de respondent aangehaald dat bedrijven een privacybeleid ter beschikking stellen om op een goed blaadje te komen bij gebruikers. Dat geeft aan dat de respondent het gevoel heeft dat bedrijven dit gewoon doen om hun gebruikers te misleiden.

"Nee, dat weet ik niet. Ik ben daar niet zo in thuis. Ik denk dat het gewoon fijn is voor de gebruiker om te weten dat jij nog altijd de controle hebt over uw gegevens en informatie. Ja dat is zo … dat denk ik een beetje. Maar in hoeverre dat je controle … Ik bedoel Facebook heeft ook alles over u. Die weet alles wat je doet. Ik weet niet in hoeverre dat WhatsApp zogezegd vergrendeld is en dat Facebook daar niet aankan. Dat geloof ik niet. - Korte pauze - Ja. Dat is allemaal zowat een vals gevoel van privacy. Uiteindelijk als je uw gezond verstand gebruikt dan weet je ook wel dat je alles … allee dat je uw informatie deelt met de wereld."
(Alice, persoonlijke communicatie, 7 april 2020)

Beoordeling van de transparantie van bedrijven

Er werd aan de respondenten gevraagd wat ze vonden van de transparantie van de bedrijven. Daarbij kan eigenlijk opgemerkt worden dat bijna alle respondenten het eens zijn over het feit dat zaken verbeterd dienen te worden. Dus zowel respondenten met een hoge als gemiddelde als lagere privacy geletterdheid geven aan dat bedrijven op vlak van transparantie eigenlijk niet zo goed scoren.

Er is wel één respondent die aangeeft dat mensen eigenlijk al bewust gemaakt worden van wat er gebeurt met hun gegevens, maar dat het probleem eigenlijk ligt bij het feit dat personen die zaken niet lezen. Dat deels omdat dergelijke teksten vaak lang zijn, maar ook omdat het personen niet kan schelen.

> *"Dat zijn de kleine lettertjes. I consent. De cookies. I accept. Al die zaken die jij eigenlijk wegklikt met ik ga akkoord. Dat zijn de bewustmakers. Alleen niemand leest die shit. Haha. Niemand leest dat. (…) Je kan van mensen niet verlangen om vijf pagina's te lezen rond wat er gebeurt in een user agreement en ook van de consumer … die kleine lettertjes in feite. Who cares? (…) En langs de andere kant is het ook gewoon onverschilligheid. Zolang dat ik kan surfen op mijn Instagram en op mijn gsm, enzovoort. Ik denk dat men daar niet echt bewust mee bezig is. En als men zich tracht bewust te maken over de gevaren dan vrees ik dat je bij heel veel mensen weinig gaat bereiken."* (Thomas, persoonlijke communicatie, 5 april 2020)

Omdat alle andere respondenten ongeacht het niveau van privacy geletterdheid het eens zijn met het feit dat er verbetering noodzakelijk is, zal er hieronder gewoon een algemeen overzicht worden gegeven van wat er misloopt bij de transparantie.

<u>Wat de andere respondenten zeiden over de transparantie</u>

In het begin van dit deel over transparantie gaf respondent Thomas aan dat gebruikers van digitale media bewust gemaakt worden van wat er met hun gegevens gebeurt. Er zijn echter ook personen die eigenlijk een andere mening hebben. Zij geven aan dat mensen hier toch nog meer over geïnformeerd moeten worden met als doel om meer bewustzijn te creëren. Niet iedereen is het dus eens met Thomas.

- *Interviewer: "Dus vind je dat de bedrijven daarin een betere rol in kunnen spelen? Dat zij dat beter moeten communiceren naar gebruikers toe?"*
- *Emily: "Ja, absoluut. Absoluut. Maar dat is ook het punt van in het begin. Ik denk dat de mensen gewoon totaal niet bewust zijn van wat het juist allemaal inhoud als je aan het surfen bent. Ja."*
  (Emily, persoonlijke communicatie, 2 april 2020)

Wat als het voornaamste probleem wordt aangehaald, is dat men niet zou communiceren over wat men met de gegevens van gebruikers doet. Ook specifiëren aan wie gegevens worden doorgegeven, moet duidelijk worden vermeld en mag niet vaag gehouden worden. Dat is dus zeker een punt dat volgens de respondenten moet gecommuniceerd worden. Op dit moment vinden ze dat ze daar te weinig informatie over krijgen. Tessa en Samantha brengen dit onder woorden.

Daarnaast wordt net zoals bij de cookies en privacyverklaringen aangehaald dat zaken vaak te juridisch worden weergegeven waardoor er geen transparantie mogelijk is. Gebruikers van websites snappen het daardoor gewoon niet altijd. Vooral personen die niet zo thuis zijn in het digitale tijdperk.

> *"Het is moeilijk te vinden. Informatie over wat ze ermee doen en als je het vindt, is het moeilijk te lezen meestal. Dus ja, ook op Facebook is dat niet zo … Je vindt dat niet meteen, die informatie. En dan ook is dat ook zo'n juridische tekst zoals ook al die formulieren eigenlijk. Ja, dus ik vind dat eigenlijk helemaal niet transparant en eigenlijk ook niet toegankelijk voor mensen die niet zo veel … allee die niet zo media savy zijn."*
> (Tessa, persoonlijke communicatie, 10 maart 2020)

> "*Ja, want soms kan je ook zo aanklikken bij zo allee bij sites of via mail ofzo van 'Ik wil niet dat deze informatie aan derden wordt meegedeeld' ofzo, maar derden wie zijn dat dan. Dat is allemaal vaag he."* (Samantha, persoonlijke communicatie, 30 maart 2020)

Het feit dat er geen overzicht is, is ook iets dat al werd vermeld bij de cookies. Emma herhaalt dit nog eens bij het aspect transparantie. Men zou namelijk van mening zijn dat zaken door bedrijven vaak anders geïmplementeerd worden, waardoor het zeer moeilijk is om zaken bij te houden. Als iedereen iets anders doet, is er gewoon geen overzicht meer.

> *"Ja, ik heb daar wel over gelezen, maar ik heb zo de indruk dat dat toch bij ieder bedrijf anders is hoe ze dat juist implementeren dus ik vind dat moeilijk om daar juist overzicht over te houden. Ja, ik weet niet, daar wordt meer rond gedaan en er zijn bepaalde wetten en ik weet ook wel wat dat die zijn, maar ik heb niet de indruk dat dat door ieder bedrijf even nauw wordt gevolgd."*
> (Emma, persoonlijke communicatie, 10 maart 2020)

Het aspect specificiteit komt ook naar boven. Het gaat dan over hoe men zaken kan aanpassen in bijvoorbeeld de privacyinstellingen. Alles zou veel te algemeen worden weergegeven, zonder echt specifiek zaken uit te leggen. Gebruikers van bepaalde sites of van bepaalde socialemediakanalen zouden dus beter begeleid moeten worden in hoe ze hun privacy kunnen beschermen.

> "Pfff goh - korte pauze - Ik denk dat bedrijven daar wel redelijk goed over communiceren, maar dat die hun communicatie redelijk algemeen is. Gewoon kijk onder dat icoontje, daar kan je je privacyinstellingen aanpassen, maar niet specifiek genoeg, denk ik."
> (Veronique, persoonlijke communicatie, 16 maart 2020)

Er is ook één persoon die absoluut niet gelooft dat bedrijven ooit eerlijk zullen vertellen wat zij precies met gegevens doen. Wat er ook verteld wordt in een beleid omtrent privacy, zal door deze respondent dus nooit vertrouwd worden. Bedrijven zouden er namelijk geen baat bij hebben om compleet eerlijk te zijn over wat zij precies doen, omdat ze dan met concurrenten hun praktijken en methodes zouden delen. Iets dat ze natuurlijk niet zouden willen.

> *"Maar daar geloof ik niets van die mannen. Nee. Geen letter. Ja, dat zijn soorten waarheden allemaal. Maar die gaan niet zeggen wat dat die juist doen en wat dat die van plan zijn. Als zo'n bedrijf als Facebook moesten zeggen van kijk dat doen en dat doen we. En die zouden daar echt oprecht eerlijk in zijn. Die zouden hun concurrenten daar gewoon de pap in de mond geven om het ook te doen." (Thibeau, persoonlijke communicatie, 19 maart 2020)*

Als laatste komt aan bod dat bedrijven niet alle mogelijke processen die gegevens ondergaan zouden neerschrijven en dat ze de regels die dan wel neergeschreven staan ook niet 100% zouden volgen. Er wordt hier dus ook getwijfeld aan de integriteit en ethiek van de bedrijven.

> *"Ze gaan 95% of 90% volgens mij wel altijd neerschrijven. Gewoon om juridische redenen enzovoort. Maar ik stel mij de ethische vraag van hoeveel bedrijven hun algemene voorwaarden 100% echt gaan volgen en of ze daar voor de profit van het bedrijf of voor de winst of voor de groei van het bedrijf niet soms andere onethische zaken gaan doen met gegevens."*
> (Rosa, persoonlijke communicatie, 28 maart 2020)

Beoordeling van de huidige wetgevingen en handelen van overheden

De respondenten werden ook bevraagd naar de huidige wetgeving omtrent privacy, namelijk de GDPR of de Algemene Verordening Gegevensbescherming.

In elk niveau van privacy geletterdheid haalden respondenten aan dat er op vlak van wetgevingen verbetering nodig is naar de toekomst toe. Er is echter wel een klein verschil op te merken tussen personen met een hogere en lagere privacy geletterdheid. Zo wordt er enkel in de groep met een lage privacy geletterdheid door twee respondenten vermeld dat men de GDPR voldoende doeltreffend vindt op dit moment. Het is wel niet zo dat iedereen binnen de groep met een lagere privacy geletterdheid dezelfde mening deelt. Nuance is hier opnieuw zeer belangrijk.

> *"Ah zo. Ja, misschien wel. Het feit dat het er nu is betekent ook dat bedrijven niet zomaar alles kunnen doen. Dus als je nu toch niet uw toestemming zou geven en dan verder zegt en ja dan moet ik het niet zien. Dan kan je daar ook voor kiezen. En niet zomaar dat het automatisch is oké en surf maar. We zien alles. Dus er is wel een grens gekomen."*
> (Samantha, persoonlijke communicatie, 30 maart 2020)

- *Interviewer: "Vind jij – die is nu sinds een aantal jaren in actie getreden – vind jij dat die doeltreffend is? Vind jij dat die goed werkt?"*
- *Daan: "- Korte pauze - Tot nu toe wel."*
  (Daan, persoonlijke communicatie, 20 maart 2020)

Wat hierboven vermeld werd, is het enige dat als verschil tussen de niveaus van privacy geletterdheid kan opgemerkt worden. Alle andere respondenten gaven aan dat de GDPR een goede start is, maar dat er nog verschillende verbeterpunten zijn. Het feit dat respondenten aanhalen dat de huidige wetgeving niet altijd doeltreffend is, kan één van de oorzaken zijn van de digitale berusting.

<u>Wat de andere respondenten te melden hadden over wetgevingen</u>

Als eerste wordt er gemeld dat de GDPR eigenlijk alleen minimumvereisten bevat die geen garantie bieden op de bescherming van privacy. Daarnaast zouden databedrijven zoals Facebook en Google nog altijd gegevens kunnen verzamelen via de Verenigde Staten. De GDPR wordt dus op dat vlak al niet als voldoende doeltreffend aanschouwd.

"Allee wat ik nu heb gezien is dat websites een stuk wel transparanter zijn, maar dat ze ook wel het minimum doen. Dus dat is echt het strikte minimum eigenlijk. Het is een stuk transparanter, maar het kan nog beter eigenlijk. Het zou in principe veel duidelijker kunnen. Dus ik weet echt niet of die GDPR wel 100% die privacy omstandigheid gaat kunnen veranderen eigenlijk. Dat heeft wel een effect, want ja met die boetes en al. Maar ja, voor de grote toppers zoals Google en Facebook. (…) Facebook heeft ook al een loophole gevonden in het systeem. Die GDPR is een Europese wetgeving. Dus ik denk dat Facebook toch wel een deel is overgestapt naar de US wetgeving voor een stuk van miljarden gebruikers om toch aan die GDPR te kunnen ontsnappen eigenlijk. Dus ik denk toch niet dat de GDPR 100% doeltreffend is, nee."
(Dimitri, persoonlijke communicatie, 1 april 2020)

Een tweede beoordeling geeft aan dat, net zoals een privacybeleid, de GDPR niet altijd even helder is en dat het niet altijd duidelijk is welke gegevens wel en welke gegevens niet doorgegeven mogen worden. De GDPR op zich zou dus veel duidelijker mogen worden weergegeven.

"Ja, het zal het wel beter beschermen als we spreken over Europese websites natuurlijk en er zal wel meer juridischer, als ik het zo mag zeggen, mee omgegaan worden. Omdat er natuurlijk op bestraft kan worden, maar daarnaast is het nog altijd een redelijk omslachtige wetgeving met meer achterpoortjes. Veel dingen die niet gespecifieerd zijn. (…) Betere veiligheid, maar is dat voldoende, nee." (Rosa, persoonlijke communicatie, 28 maart 2020)

Wat in de lijn ligt met het feit dat zaken vaak onoverzichtelijk worden weergegeven, is het feit dat de teksten niet opgemaakt zijn voor de gewone burger. Zij zouden namelijk niet begrijpen wat er wordt vermeld, omdat de GDPR onduidelijk is en omdat er vooral vakjargon en moeilijke woorden worden gebruikt.

"En ik ben dat een keer beginnen lezen en dat was ook echt omg, allemaal zo veel blabla. Niet verwoord in gewone, simpele mensenwoorden."
(Amelie, persoonlijke communicatie, 18 maart 2020)

Wetgevingen zouden volgens Julian eigenlijk ook achter de feiten aanhollen. Volgens Julian zouden de mensen met de meeste kennis niet tewerkgesteld zijn bij de overheid, maar bij de technologische bedrijven zelf. Dat zorgt ervoor dat de technologie die ontwikkeld wordt eigenlijk altijd een paar stappen voor is op de wetgeving. De GDPR zou dus al een goede start zijn, maar de wetgeving zou eigenlijk altijd te laat komen en er zullen altijd zaken zijn waar wetgevingen de burgers niet tegen zullen kunnen beschermen.

"En zoals gezegd, de slimste mensen zitten in de ondernemingen, in de techbedrijven en niet in de politiek. Ik denk dat het altijd zo'n beetje achter de feiten aanhollen gaat zijn. Er zijn al verschillende processen geweest. De GDPR is gekomen enzovoort enzoverder, maar techbedrijven staan altijd drie stappen verder, omdat ze veel meer ressources hebben, veel meer macht, toegang tot informatie, toegang tot AI enzovoort enzoverder."
(Julian, persoonlijke communicatie, 31 maart 2020)

Hieronder wordt door Thibeau aangegeven dat wetgevingen toch geen verschil zouden uitmaken. De bedrijven zouden dat, volgens bepaalde respondenten, makkelijk kunnen omzeilen. Daarnaast wordt er een soort van straffeloosheid geïmpliceerd. Men geeft aan dat wanneer zou worden ontdekt dat bedrijven zich niet aan de regels houden, ze daarvoor niet gestraft worden. Deze bedrijven zorgen daarnaast ook voor werkgelegenheid. Nog een aspect dat zou aangeven dat overheden eigenlijk niets zouden kunnen doen. Dergelijke zaken kunnen natuurlijk ook een gevoel van digitale berusting voeden. Als men denkt dat zelfs de overheid geen zaken kan ondernemen om dergelijke praktijken te stoppen, hoe zou één gebruiker dat dan moeten doen? Er is dus een gevoel van straffeloosheid waarbij procedures zeer lang aanslepen en boetes niet het gewenste effect hebben.

> *"Ze maken daar allerlei regels over, maar ik ben ervan overtuigd dat zij dat toch langs alle kanten kunnen omzeilen. Alles valt te onderhalen. (…) Wat gaat de overheid tegen die mannen zeggen? We gaan u in de gevangenis gooien of je mag hier niet meer verder doen? Dat ze goed zot zijn. Die mannen die geven hier werk aan mensen en dat brengt geld in het laatje. Daar kan je niets tegen ondernemen ze." (Thibeau, persoonlijke communicatie, 19 maart 2020)*

> *"- Korte pauze - Het is niet dat bedrijven zo groot zijn geworden dat regelgeving hen niets meer doet, maar ten eerste er is al een gebrek aan regelgeving daarrond, want anders zou die procedure nooit zo lang kunnen aanslepen. En anderzijds zijn het echt multibedrijven. Bijvoorbeeld LinkedIn heeft ooit 11 miljoen denk ik gehad, omdat ze dark patterns hadden ingevoerd in hun procedure. Voor bedrijven zoals LinkedIn en Facebook … oké die betalen dat. Dat is misschien even een dip, maar die zijn zeker dat ze daar terug uit gaan komen en soms is dat zelfs niets voor hun. Dus ik vraag mij af van moet er niet strenger opgetreden worden."* (Rosa, persoonlijke communicatie, 28 maart 2020)

Algemene houding/mening t.o.v. de eigen privacy

Zoals de voorgaande resultaten uit de interviews al beschreven, werden respondenten bevraagd naar hun gedrag t.a.v. specifieke privacy gerelateerde handelingen op digitale media. Daarnaast werd echter ook bekeken wat de algemene houding of mening van de respondent is t.a.v. privacy. Hoe belangrijk vinden zij hun persoonlijke privacy en hoe evalueren zij hun online privacy? Door ook een algemeen beeld te bevragen, kunnen er opnieuw een aantal onderliggende redenen voor digitale berusting ontdekt worden.

Uit de interviews bleek dat respondenten heel veel verschillende aspecten meegaven. Daarbij werd er vaak telkens een nieuw aspect belicht. Er kon dus maar een klein verschil worden opgemerkt tussen de personen met een hogere, meer gemiddelde of lagere privacy geletterdheid. Iets wat namelijk opvalt, is dat enkel personen met een lagere privacy geletterdheid aangeven dat ze toch een bepaald vertrouwen hebben in bedrijven. Dat ze het vertrouwen hebben dat bedrijven hun geen kwaad kunnen doen. Ze geven echter wel tegelijkertijd aan te weten dat bedrijven van alles en nog wat over hen kunnen verzamelen. Dat fenomeen komt voor bij drie respondenten.

> *"Ja, dat is ook nog iets dat ik volledig vertrouw, als jij mij nu zegt heel de informatie dat je geeft dat is te vertrouwen en je geeft dat niet aan niemand door. Dan heb ik zoiets van als jij mij zegt dat zo gebeurt, dan hoop ik dat dat zo is."* (Daniël, persoonlijke communicatie, 23 maart 2020)

Daarnaast blijkt ook dat een beperkt aantal personen binnen de groep met een lagere privacy geletterdheid niet de juiste kennis hebben om een situatie te beoordelen. Zo komt naar boven dat bijvoorbeeld respondent Daan zich eerder zorgen maakt om hackers en niet zozeer gelooft dat technologiebedrijven iets fout kunnen doen met gegevens. Dit komt echter wel maar beperkt voor. Andere respondenten met een lager niveau van privacy geletterdheid weten wel dat technologiebedrijven ook een rol spelen. Het niveau van privacy geletterdheid van Daan zou dus misschien nog iets lager liggen dan dat de test aangaf. Daan vertoont dus wel tekenen van digitale berusting, maar er spelen ook andere factoren. Bij de respondenten met een hogere privacy geletterdheid komt dit niet voor.

- *Interviewer: "Dus als ik het zo mag samenvatten denk je niet dat de bedrijven zelf een probleem vormen, maar vooral wel dat de externe hackers je gegevens kunnen stelen en dat zij eigenlijk het probleem zijn daarin?"*
- *Daan: "Voilà, ook al doen firma's alles over onze bescherming te voldoen."*
  (Daan, persoonlijke communicatie, 20 maart 2020)

Daarnaast kon er tussen de drie niveaus van privacy geletterdheid geen belangrijk verschil gevonden worden. Daarom zullen hieronder vooral de voornaamste meningen/houdingen t.o.v. het concept privacy worden weergegeven.

Welke andere meningen komen nog naar boven?

Een eerste punt dat naar boven komt, is dat iemand digitale media volledig zou moeten bannen om de eigen privacy te kunnen beschermen. Wat daarbij echter het probleem vormt, is dat een dergelijke maatregel eigenlijk zeer moeilijk te implementeren valt, omdat we leven in een tijdperk waar digitale media een zeer belangrijke rol speelt. Men heeft digitale media dus nodig, ook al betekent dit dat men de eigen privacy niet kan beschermen. Lana bespreekt hier echter ook dat de bedrijven achter de digitale en sociale media zouden weten dat we niet zonder kunnen. Dat zou een ongelijke onderhandelingspositie impliceren waarbij digitale mediabedrijven de bovenhand hebben, omdat de gebruikers eigenlijk niet meer zonder digitale media zouden kunnen.

> *"Ik zou het er niet voor over hebben om het echt volledig uit mijn leven te bannen, omdat het echt wel handige functies heeft. En dat weten ze ook. (…) Goh, ik probeer eraan te werken, maar ik denk dat je nooit genoeg kan doen. Ik zeg het door gewoon al actief te zijn op bepaalde sites of bepaalde sociale media toon je al iets aan."*
> (Lana, persoonlijke communicatie, 2 april 2020)

Elke gaat zelfs nog een stap verder dan bijvoorbeeld Lana. Zij haalt namelijk aan dat als men het internet nu zou bannen er zelfs nog altijd online gegevens zouden circuleren over iemand. Men zou eigenlijk nooit aanwezig mogen zijn op het internet moest men dit willen vermijden. Dat kan opnieuw een reden vormen voor de digitale berusting. Het feit dat zaken toch onomkeerbaar zijn en dat men eigenlijk al te ver heen is zogezegd, kan ervoor zorgen dat gebruikers van digitale media het opgeven.

> *"Dat je daar zelf ook niet veel tegen kunt doen of je moet eigenlijk al van het internet verdwijnen. Of als je opgroeit eigenlijk, want wij hebben nu al zoveel op het internet gezeten. Dus je kunt dat gewoon niet meer ongedaan maken."*
> *(Elke persoonlijke communicatie, 7 maart 2020)*

Daarnaast speelt onwetendheid ook een belangrijke rol binnen de digitale berusting. Veronique haalt aan dat ze haar privacy wel wil beschermen, maar dat ze eigenlijk niet weet of dat wel lukt. Het feit dat er niet geweten is welke informatie er circuleert, speelt daarbij ook een rol. Het is echter niet hetzelfde soort onwetendheid als bijvoorbeeld Daan aangaf in het begin van dit hoofdstuk. Daar ging het vooral over het feit dat men niet wist dat ook technologische bedrijven waar we dagdagelijks mee in aanraking komen onze gegevens gebruiken.

> *"Ja, dat ik dat eigenlijk niet weet, maar dat dan weer die onwetendheid die zowat speelt. Ik wil wel dat ik mijn gegevens voldoende bescherm, maar ik weet het niet."*
> (Veronique, persoonlijke communicatie, 16 maart 2020)

Wat ook aan bod kwam tijdens de interviews, is dat het beschermen van iemands privacy niet altijd in de eigen handen ligt. Het is mogelijk dat persoonlijke informatie zoals je telefoonnummer in handen komt van personen uit je netwerk op sociale media. Daaruit kan voortkomen dat deze personen jouw telefoonnummer bijvoorbeeld bijhouden of delen, wat kan leiden tot ongewilde privacyinbreuken.

> *"Nee, dat denk ik niet. Bijvoorbeeld ik zit in vrij veel WhatsAppgroepen. Zo van werk of van toen ik op Erasmus was daar hadden we zo'n Erasmusgroep. En je hebt daar ook niet echt … Ja, dat waren groepen met 250 mensen in ofzo, dus dan hadden ook wel mensen uw nummer waarvan dat je het niet wou. Dus nee er zijn nog altijd inbreuken mogelijk, denk ik."*
> *(*Tessa, persoonlijke communicatie, 10 maart 2020)

'Het ondergaan in de massa' zijn de woorden die Tessa gebruikt om te verwoorden dat er nog een andere reden is voor het niet altijd beschermen van de privacy. Er zijn online namelijk een massa aan gegevens te vinden en men is ervan overtuigd dat de eigen gegevens daardoor niet significant lijken. Dat geeft dan een gevoel van veiligheid.

> *"Dus het is meer zo het ondergaan in de massa. Haha. Dat mij zo'n beetje een gevoel van veiligheid geeft." (*Tessa, persoonlijke communicatie, 10 maart 2020)

Sommige respondenten zijn er eigenlijk van overtuigd dat privacy alleen maar in beperkte mate mogelijk is naar andere gebruikers toe. Het is mogelijk om te bepalen wat andere gebruikers van digitale media of sociale media over iemand te zien krijgen online. Het zou minder mogelijk zijn om je gegevens af te schermen voor de bedrijven achter de sites of sociale media. Zij gebruiken die gegevens namelijk in hun voordeel.

> *"Quasi niet, nee. Nee, privacy in die zin van dat een andere gebruiker misschien niet altijd even gemakkelijk gaat terugvinden wie dat je bent op fora. Daar geloof ik nog wel in voor een groot deel. Het hangt er uiteindelijk vanaf wie dat je tegenover u hebt. Hoeveel dat hij kan met een pc. (…) Dus naar andere gebruikers toe zal dat op zich meestal wel meevallen. Naar grote bedrijven toe die informatie dan ook gebruiken om er hun voordeel mee te halen, vind ik dat minder leuk."* (Ralf, persoonlijke communicatie, 23 maart 2020)

Er was ook een persoon binnen de interviews die aanhaalde dat hij het niet fijn vindt dat er gegevens over hem worden verzameld. Hij vindt dat op zich dus niet zo aangenaam, maar hij verwijst naar het feit dat een dergelijk iets hem niet lichamelijk zal schaden. Dat kan opnieuw een mogelijke reden zijn voor de digitale berusting. Personen zien het namelijk niet direct als een bedreiging dat hun gegevens online verzameld worden.

"Ik denk mijn privacy dat die gedeeld zou worden en dat er heel veel data van mij zou worden verzameld. Ik vind dat op zich niet zo aangenaam, maar ik ga daar niet van sterven ofzo. De waarde die ik krijg in tegenstelling dat ik in contact kan blijven met mensen over heel de planeet. Dat ik constant dingen kan opzoeken, is voor mij eigenlijk ook heel, heel veel waard. Op zich stoort mij dat niet zoveel op deze moment." (Julian, persoonlijke communicatie, 31 maart 2020)

Wel bekijkt Julian de toekomst met een bepaald scepticisme. Volgens Julian zouden er wel bepaalde technologische ontwikkelingen kunnen plaatsvinden waarbij bijvoorbeeld personen een digitaal paspoort krijgen waar alle mogelijke informatie over die persoon opstaat. Dat zou ervoor kunnen zorgen dat personen geen toegang verleend worden tot bepaalde diensten. De mogelijke toekomstige technologische vooruitgang beangstigt sommige respondenten dus.

"Ja, hoe dat de technologie vooruitgaat en meer informatie … Mijn vraag is waar gaat dat eindigen. Op den duur denk ik dat we een digitaal paspoort gaan krijgen waar alles opstaat wat we doen, naar welke winkels dat we gaan. Nu bijvoorbeeld met het coronavirus gaan we misschien een paspoort krijgen van zijn we gevaccineerd al dan niet. Bijvoorbeeld die dat geen vaccinatie hebben, gaan we dan nog bepaalde dingen kunnen doen al dan niet. Gaan we dan nog welkom zijn overal? Van zo'n dingen ben ik wel een klein beetje achterdochtig. Voor de toekomst dan." (Julian, persoonlijke communicatie, 31 maart 2020)

Een laatste reden, die Julian aanhaalt, over waarom personen niet overgaan tot bepaalde privacybeschermende handelingen, zou zelfvertrouwen kunnen zijn. Julian is er bijvoorbeeld van overtuigd dat hij zich goed kan verdedigen tegen persoonlijke reclame. Dit duidt aan dat er bij Julian naast digitale berusting ook andere factoren spelen.

"Ik heb meer vertrouwen in mezelf dat ik niet zo kwetsbaar ben voor makkelijke advertising. Ik denk dat 80% van de dingen die dat graag doen, uw informatie hebben of die data dat die dat doen om uw heel specifiek te advertisen. Ik denk dat ik wel vrij, ik ga niet zeggen immuun ben, maar dat ik mij wel vrij goed kan verdedigen tegen die advertisement gefocust op mijn eigen consumptiegedrag." (Julian, persoonlijke communicatie, 31 maart 2020)

Thomas beschrijft hier dat privacy eigenlijk iets is dat niet meer bestaat. Daarbij komt er een nieuwe reden voor digitale berusting naar boven, namelijk het feit dat het online zijn en het delen van gegevens een gewoonte is geworden. Thomas argumenteert dat de sociale media en de manier waarop databedrijven werken stilletjes aan gegroeid is. Dat de technologische samenleving waarin we nu leven het nieuwe normaal is geworden. Om de woorden van Thomas te gebruiken: "point of no return". Volgens Thomas kunnen we niet meer terug en moeten we gewoon accepteren dat dit het nieuwe normaal is. Ook Rosa bespreekt dat fenomeen. Zij spreekt van een cultuurswitch.

"Maar wij zijn al zo ver, zoals ik zei de point of no return. Wij zijn al zo ver dat dit een gangbare praktijk is. Het is een gewoonte geworden. Het is iets dat geïntegreerd is in het systeem. Wij zijn daar zo langzaamaan ingerold. Het is niet de big bang geweest waarin dat wij in een keer bam en nu staat al uw data online. Nee, die gegevens zijn gegroeid. Die manier van werken, is gegroeid. Die data verzamelen dat is allemaal gegroeid. En wij zijn daar stilletjes in meegerold. Wij hebben netjes de Facebooks van deze wereld geïntegreerd."
(Thomas, persoonlijke communicatie, 5 april 2020)

"Ja en dat is misschien ook ergens een cultuurswitch die heeft plaatsgevonden in onze samenleving" (Rosa, persoonlijke communicatie, 28 maart 2020)

Er werden al verschillende mogelijke redenen voor de digitale berusting naar boven gebracht. Thibeau voegt er hier nog eentje aan toe. Hij is er allereerst al van overtuigd dat privacy niet meer bestaat. Daarnaast geeft hij toe dat het gewoon gemakkelijker is om overal mee akkoord te gaan i.p.v. bijvoorbeeld bepaalde instellingen in te stellen of om een privacybeleid te moeten analyseren.

"Ik ben wel op mijn privacy gesteld, maar ik vind dat het gemakkelijker is om te zeggen ja bekijk het maar he. In plaats van al die dingen te lezen."
(Thibeau, persoonlijke communicatie, 19 maart 2020)

Emily vertelde daarentegen dat instellingen die je gemaakt hebt ook vaak een rol kunnen spelen. Daarbij vermeldt ze dat door het feit dat je gebruik maakt van verschillende apparaten met verschillende accounts bepaalde instellingen misschien niet volledig gesynchroniseerd zijn. Het is dus mogelijk dat je denkt dat je goed beschermd bent, maar dat je dat eigenlijk niet bent.

- *Interviewer: "Oké, naargelang al die voorbeelden dat je geeft, heb je dan het gevoel dat privacy online te beschermen valt?"*
- *Emily: "Goh nee, want er komen ook bij Google zo vaak nieuwe dingen bij, zoals Googlefoto's ik wist zelfs niet eens dat dat bestond. En door dat je dat gebruikt op jouw computer en op jouw gsm en op nog een andere computer en inlogt via een computer van de school, ik zeg maar iets. Ja, worden die instellingen heel vaak aangepast of veranderd of door een oudere computer is dat nog niet helemaal gesynchroniseerd. Of zo'n zaken. Ik denk dat dat er ook vaak mee te maken heeft waardoor dat er dingen zoals dat mislopen."*
  (Emily, persoonlijke communicatie, 2 april 2020)

'Je moet op te veel zaken letten'. Dat is de boodschap van Samantha en Rosa. Door het feit dat er zoveel zaken zijn waar men rekening mee moet houden, zou het niet mogelijk zijn om alles onder controle te kunnen houden. Er zijn te veel bedrijven en te veel instellingen waardoor je gewoon geen overzicht hebt. Dit vormt opnieuw een onderliggende reden voor digitale berusting.

"Dat zijn zo veel bedrijven. Ik probeer wel van iedere keer zo als ik een spammail krijg mij uit te schrijven of zo dat ze mij niet meer moeten lastigvallen, maar dat blijft altijd maar komen. Van alle kanten. Dus het zijn er zo veel dat je er eigenlijk toch niet volledig grip kunt op hebben." (Samantha, persoonlijke communicatie, 30 maart 2020)

"Iets wat mij aan Facebook heel erg stoort, is gewoon het feit dat je op zoveel dingen moet klikken om uw instellingen volledig af te sluiten. Want je moet eigenlijk al klikken op uw persoonlijke instellingen. Dan moet je al klikken op uw naam of op u e-mailadres en dan nog eens afschermen en dan afschermen voor wie en dan nog eens op bevestigen. Dus je moet gewoon heel veel stappen nemen op alles af te schermen en dan denk ik wel dat je soms eens een bepaald aantal dingen kan vergeten. Of mogelijk kunt overslaan of minsinterpreteren zo ja." (Rosa, persoonlijke communicatie, 28 maart 2020)

Iets wat nog niet werd aangehaald, is dat bedrijven personen een vals gevoel van veiligheid willen geven zodat ze nog altijd gebruik zullen maken van hun diensten. Bedrijven zouden dus willen bijdragen aan het feit dat gebruikers hun privacy niet beschermen. Bedrijven wenden gegevens van personen namelijk aan om winst te maken.

"Ik denk dat ik nog altijd ja zou antwoorden. Je hebt daar geen controle over. Ik denk dat ze vooral een vals gevoel van controle willen geven zodat je hun platform nog zou gebruiken en hun website nog zou bezoeken. Maar het is vooral een vals gevoel en dat ik toch denk dat iedereen die uw gegevens heeft die ook gebruikt en dat is gewoon zo. Denk ik. Ik denk niet dat je daar iets aan kan veranderen." (Alice, persoonlijke communicatie, 7 april 2020)

Daarnaast wordt privacy door Alice zelfs ondergeschikt bevonden aan het gebruiksgemak van platformen. Privacy is als het ware ondergeschikt aan een goede gebruikerservaring.

"Ah gewoon wat dat je zei. Dat dat ondergeschikt is aan de efficiënte van die platformen. Sociale media." (Alice, persoonlijke communicatie, 7 april 2020)

Een voorlaatste aspect dat wordt aangehaald, is dat één gebruiker eigenlijk maar één gebruiker is. Wat kan je als gebruiker doen tegen de grote bedrijven? Dat is een vraag die Emma en Thibeau zich stellen. Het feit dat je ook niets kan beginnen tegen de grote bedrijven kan ook een gevoel van digitale berusting in de hand werken. Want als er dan iets verkeerd zou lopen, hebben Emma en Thibeau het gevoel dat daar toch niets aan gedaan kan worden.

"Ja, omdat via Facebook kunnen die toch heel gemakkelijk dingen van mij te weten komen. Ik kan wel van alles ondernemen, maar ik ben maar één enkeling t.o.v. de grote bedrijven, dus als ze dat willen weten, vinden ze dat wel." (Emma, persoonlijke communicatie, 10 maart 2020)

"Wij kunnen de Googles niet meer beheersen en de Facebooken. Dat is onmogelijk. Je kan die niet aan banden leggen. Die zijn te machtig. Dat kan je niet meer. Die gaan ons aan banden leggen." (Thibeau, persoonlijke communicatie, 19 maart 2020)

Na deze hele resem aan manieren om naar privacy te kijken, zijn we bij het laatste aspect gekomen. Daarbij wordt aangegeven dat bedrijven iemand zouden blijven lastigvallen met meldingen omtrent privacy. Het zou dus gewoon makkelijker zijn om bepaalde zaken te aanvaarden om ervoor te zorgen dat je je er niet meer mee moet bezighouden.

> *"Ik denk als je dat niet van de eerste keer accepteert dat ze constant gaan overvallen wat je ook doet. Doe het vanaf het begin dan ben je er vanaf en dan weten ze van uw interesse, wat dat je koopt of wat dat je wilt kopen."* (Daan, persoonlijke communicatie, 20 maart 2020)

Mogelijke manieren om zaken te verbeteren

Er werd aan de respondenten ook gevraagd of zij eventueel verbeterpunten zien in hoe zaken omtrent privacy vandaag geregeld worden en hoe zij deze verbeterpunten zouden aanpakken. De respondenten zijn wel digitaal berust en verwachten dus dat hun privacy niet beschermd zal worden (Draper & Turow, 2019; Kezer et al., 2016; Turow et al., 2015), maar vanuit hun gewenste privacy kwamen er toch een aantal suggesties naar boven zoals educatie naar de bevolking toe en transparantie vanuit de bedrijven zelf.

Educatie/sensibilisering

Een eerste punt dat dus naar boven kwam, was het feit dat educatie of sensibilisering een aspect is dat op dit moment nog onderbelicht is. Zowel educatie/sensibilisering via de televisie, scholen en de overheid werd voorgesteld.

Er zijn echter twee personen die het nut van opleidingen of bewustmaking in twijfel trekken. Zo geeft respondent Thomas allereerst aan dat gebruikers van digitale media eigenlijk nu al bewust gemaakt worden van dergelijke zaken, maar dat niemand gewoon de moeite doet om het te lezen. Onverschilligheid zou daarin een belangrijke rol spelen. De gebruikers zouden het volgens Thomas belangrijker vinden om van bepaalde diensten gebruik te kunnen maken. Bewustmakingscampagnes bijvoorbeeld zouden het gewenste effect, mensen aanzetten om hun privacy beter te beschermen, niet bereiken. Dat wordt aangetoond door de quote op p. 50.

Een tweede respondent Julian twijfelt ook eerder. Hij vermeldt dat er op dit moment misschien andere belangrijkere dingen dienen te worden geëduceerd.

> *"Maar educatie kan iets zijn, ja. Moet dat gebeuren? Geen idee. Maar ik denk dat er veel andere dingen zijn de belangrijker zijn en die moeten geëduceerd worden die nu niet geëduceerd worden. Maar dat zou wel een mogelijke oplossing zijn."*
> (Julian, persoonlijke communicatie, 31 maart 2020)

De andere respondenten delen deze mening echter niet. Zij geven een aantal suggesties om binnen opleidingen en sensibilisering zaken te verbeteren.

Via televisie

De eerste suggesties handelen over het sensibiliseren van personen via de televisie, waaronder reportages. Voor kinderen kan men daarnaast gebruik maken van het kindernieuwsprogramma Karrewiet. Ook gewone soaps zouden een rol kunnen spelen volgens respondent Samantha. Volgens haar zou dat ervoor zorgen dat personen op een onbewuste manier tips kunnen opvangen die ze dan zouden kunnen toepassen in het echte leven. Daarnaast wordt wel aangehaald door een andere respondent dat het gebruik van televisie wel gepaard moet gaan met een expert om ervoor te zorgen dat er juiste informatie wordt meegegeven.

Sociale media zou ook eventueel zelf verplicht moeten worden. Zodat zij nog meer informatie en sensibilisering zouden verschaffen aan de gebruikers van het platform, maar dat het dan wel op een simpele manier moet gebeuren.

> *"Wel, ik denk wel dat televisie toch wel iets meer zou kunnen zeggen over privacy. Maar televisie is toch wel een beetje sensatiegericht ook wel. In zo'n gevallen denk ik toch wel als je mensen wil informeren over privacy, moet je er een expert over laten spreken. Dus ofwel op televisie of in de krant ofzo, maar ja de uitleg zelf moet dan ook niet even omslachtig zijn als het privacybeleid zelf.* (Dimitri, persoonlijke communicatie, 1 april 2020)

> *"Bijvoorbeeld ook op Karrewiet voor kinderen vind ik ook wel dat dat soms wel een keer kan aangehaald worden. (…) Nu bijvoorbeeld in Familie ofzo vind ik dat ze dat daar wel in kunnen verwerken als er iemand daar zo problemen mee heeft en dat er zo zogezegd dan iemand komt uitleggen daaraan van ah maar je kan dat zo en zo. En dat je zo onbewust tips meekrijgt he."*
> (Samantha, persoonlijke communicatie, 30 maart 2020)

> *"- Korte pauze - Hmmm, reportages ofzo. Ja of via de sociale media zelf verplichten. Zoiets"*
> (Camille, persoonlijke communicatie, 8 april 2020)

Via scholen of andere educatieve instellingen

Een eerste manier om via educatieve instellingen mensen bewust te maken van het gegeven privacy is via de instelling Mediawijs. Mediawijs is namelijk een instantie die voor meer kennis over media bij de bevolking moet zorgen (Mediawijs, s.d.). Zij zouden volgens Alice deze taak op zich moeten nemen.

> *"Meer voorlichting he vanuit wat is het Mediawijs? Ja, maar het kan ook zijn dat die mensen dat helemaal niet erg vinden dat ze zo openbaar gesteld worden. Ik weet het niet, maar meer voorlichting ja." (Alice, persoonlijke communicatie, 7 april 2020)*

Naast de instelling Mediawijs zouden er volgens de respondenten ook via de scholen gewerkt moeten worden aan opleidingen over privacy. Een bemerking die respondent Rosa daarbij geeft, is dat er wel goed nagedacht moet worden over waar dat dan precies in zal passen qua vakken. Men moet er namelijk voor zorgen dat er in alle middelbare opleidingsniveaus, ASO, TSO, BSO en BUSO, een dergelijke opleiding wordt voorzien. Daarnaast is het niet alleen belangrijk om aan te tonen hoe dat bepaalde dingen worden gedaan, maar ook waarom ze gedaan moeten worden. Alleen door de 'waarom' mee te geven zouden jongeren volgens Rosa tot actie overgaan.

> *"Ik was zoiets aan het denken aan vakken zoals ja hoe noemt dat tegenwoordig? Maatschappijleer of zoiets. Maar dan mis je alweer die groep van TSO en BUSO. Dus je moet echt op zoek gaan naar een vak dat iedereen krijgt en dat zit je al direct bij Nederlands. En dan was de vraag hoe ga je dat daar integreren? Maar ja ik vind dat ze dat wel daar echt moeten integreren. En niet alleen in het middelbaar. Ik vind dat dat meermaals mag terugkomen, want oké je kan daar dan misschien een week of twee over leren, maar dan kan je dat misschien terug vergeten. Als je dat bijvoorbeeld al van jongs af aan leert van oké, zoals in het lager dat ik zei, van maak zo een account aan, maar leer mij ook ineens om dat af te schermen. En laat dan in het middelbaar nog eens terugkomen, maar laat dat dan in het middelbaar dan nog eens terugkomen met waarom dat ze dat moeten. Wat zijn de gevaren daarvan?"*
> (Silke, persoonlijke communicatie, 28 maart 2020)

<u>Via de overheid</u>

Ook de overheid heeft een verantwoordelijkheid volgens de respondenten. Zij zouden hun burgers moeten beschermen en moeten inlichten over het gegeven privacy. Sensibiliseringscampagnes zouden dus vanuit de overheid cruciaal zijn om mensen informatie te verschaffen.

> "*Ik vind dat er vanuit de regering wel degelijk sensibiliseringscampagnes zouden mogen gedaan worden."* (Ralf, persoonlijke communicatie, 23 maart 2020)

<u>Andere mogelijkheden</u>

Een laatste deel dat werd aangehaald omtrent het sensibiliseren, is dat jongeren daarbij voor de oudere generatie een rol moeten spelen. De jongere generatie zou inderdaad bereikt worden als men werkt met opleidingen, maar wat met de oudere generatie. Daarbij zouden jongeren kunnen bijspringen om de ouderen in hun familie te leren om bewust met digitale media om te gaan.

> *"Ik denk dat ouderen sowieso hun kinderen en kleinkinderen gaan raadplegen om te helpen opzetten van die digitale media en dan vind ik het ook wel de taak van die kinderen om te zien dat die privacyinstellingen in orde staan."* (Rosa, persoonlijke communicatie, 28 maart 2020)

Transparantie/ Duidelijkheid

Qua duidelijkheid werd er in de voorgaande hoofdstukken al verschillende malen aangehaald dat een privacybeleid vaak omslachtig, lang en juridisch zijn. Dat zou namelijk één van de redenen zijn waarom mensen deze niet lezen. De respondenten haalden als mogelijke oplossing aan om de manier waarop de informatie gepresenteerd wordt, aan te passen.

Eerst en vooral opnieuw moeten zaken korter weergegeven worden. Dat is iets dat door Elke wordt aangehaald. Een privacybeleid in drie puntjes weergeven zou al veel verbeteren. Daarnaast zouden personen verplicht gemaakt moeten worden om een privacybeleid te lezen. Op dit moment kan je niet verder surfen indien je niet akkoord gaat, maar dat zegt nog niets over het wel of niet gelezen hebben van dat beleid. Respondent Elke geeft daarbij aan dat, indien een dergelijke technologie bestaat, bedrijven zouden moeten registreren wanneer personen een privacybeleid hebben gelezen. Enkel dan zouden ze mogen verder surfen.

> *"Ik denk het wel ja. Nog maar in drie regels. Het is meestal gewoon in één oogopslag, zeker op het internet, dat je ziet het interesseert mij of het interesseert mij niet. Ik denk het wel, ja. En dan kan je nog klikken op meer info daarnaast. En ik dacht even aan misschien dat ze zo'n venster kunnen maken, als je het echt hebt gelezen, ik weet niet of ze dat dan kunnen registreren, dat je dan pas verder kunt naar de website. Dat ze het een soort van verplicht maken."* (Elke, persoonlijke communicatie, 7 maart 2020)

Een andere respondent had een ander idee om de structuur van privacyverklaringen te optimaliseren. Bedrijven zouden gebruik kunnen maken van een filmpje waar ze dan op een 'toffere' manier zaken omtrent privacy zouden kunnen tonen en uitleggen. Daarbij zou het zeker ook met een andere structuur en met andere kleuren moeten worden weergegeven.

> *"Dus ja, ik snap dat wel dat is moeilijk om mee te geven, maar ja misschien op een toffere manier met een filmpje of weet ik veel wat. Een beetje wat verduidelijking geven ofzo. Want zo een lange tekst die er dan weer opkomt dat leest toch weer niemand. (…) Ja, ik denk dat wel. En ook met zo wat meer kleuren en wat meer structuur zo. Wat speelser dat aanpakken."*
> (Samantha, persoonlijke communicatie, 30 maart 2020)

Wat ook al werd aangegeven door de respondenten als tekortkoming, was het aspect overzichtelijkheid. Dat wil zeggen dat respondenten aangaven dat ze geen overzicht kunnen houden over wie over welke gegevens beschikt. Daarbij zou het dus bijvoorbeeld een optie moeten zijn om in één oogopslag te kunnen zien welke informatie door welke bedrijven worden bijgehouden.

De respondenten geven echter direct ook aan dat dergelijke systemen zelf een aantal problemen met zich meebrengen. Zo moet verzekerd kunnen worden dat jij alleen jouw eigen gegevens kan inkijken bij zo'n systeem. Daarnaast zou het ook opgezet moeten worden vanuit een breder overheidskader. Dat wil zeggen dat een regering van één enkel land niet het verschil zal kunnen maken en dat er dus vanuit Europa gewerkt moet worden.

"Ja, absoluut. Het zou fantastisch zijn om een soort van bod (Engelse term) te hebben waarin ik een e-mailadres kan ingegeven of een naam kan ingeven en kijken waar het allemaal hits heeft. In welke omgeving. (…) Aan de andere kant als ik mezelf kan opzoeken, kan iemand anders mij ook opzoeken. Dat brengt opnieuw een gevaar met zich mee."
(Thomas, persoonlijke communicatie, 5 april 2020)

"Ja het zou goed zijn moest daar een systeem van bestaan waar dat ik in één opslag kan zien waar ik ingeschreven sta. Dat ik dat zo zelf kan verwijderen, maar ik denk dat dat onbegonnen werk is en dat dat dan echt vanuit Europa moet komen of toch iets algemeen."
(Amelie, persoonlijke communicatie, 18 maart 2020)

Een andere mogelijkheid die aangehaald wordt om de transparantie en duidelijkheid van bedrijven te verhogen, zou het werken met een 'frequentky asked questions' pagina zijn waar alle informatie duidelijk en makkelijk op te vinden is. Ook hier wordt echter aangehaald dat het zeker in verstaanbaar Nederlands moet worden vermeld.

"Ja, wat ik heel fijn zou vinden, is als je in een menu de optie had zoals je vaak zo van die 'frequently asked questions' ofzo hebt. Dat je daar ook van zo van die officiële documenten hebt en dat dan ook gewoon een beknopt document is wat dan ook in verstaanbaar Nederlands, om het zo te zeggen, wat er met die data gebeurt."
(Tessa, persoonlijke communicatie, 10 maart 2020)

Als laatste kwam uit een interview naar voren dat constante updates niet aangenaam zijn en dat gebruikers van digitale media daardoor een privacybeleid eerder skippen. Het jaarlijks ter beschikking stellen van een beleid zou dus voldoende zijn en mensen meer reden geven om het te lezen.

"Ik zou het doen als ze dat bijvoorbeeld jaarlijks zouden doen en niet constant."
(Daan, persoonlijke communicatie, 20 maart 2020)

Wetgevingen

Uit de voorgaande resultaten werd ook al duidelijk dat de huidige wetgeving aan verbetering vatbaar is. Er wordt echter getwijfeld aan de mogelijkheid daarvan. Wetgevingen zouden dus eigenlijk niet echt een extra oplossing kunnen vormen. Vooral omdat we in een wereld zitten met heel veel verschillende culturen en landen, waarbij er geen algemeen kader is voor het vormen van een mondiale wetgeving.

> *"Maar daarnaast stel ik me dan weer de vraag we zitten op Europees niveau. Kunnen er op nationaal niveau, op mondiaal niveau nog andere maatregelen genomen worden? Persoonlijk vind ik wel dat er op mondiaal niveau maatregelen moeten genomen worden, maar dan is de vraag wie gaat dat maken. Er is ook geen gerechtshof op mondiaal niveau. Dan kan je zitten bij de Verenigde Naties, want die zitten met veiligheid enzovoort, maar mondiaal: ja ik zou dat willen. Ja, dat lijkt mij nodig, maar nee dat is niet haalbaar."*
> (Rosa, persoonlijke communicatie, 28 maart 2020)

10. Discussie resultaten

Uit het empirisch onderzoek konden er verschillende resultaten worden afgeleid. Een eerste aspect dat besproken dient te worden, zijn de tests die gebruikt werden om digitale berusting en privacy geletterdheid vast te stellen. De stellingen uit het onderzoek van Turow et al. (2015), die gebruikt werden om digitale berusting te testen, werden door de respondenten namelijk niet altijd op de juiste manier geïnterpreteerd waardoor sommige personen zouden bestempeld worden als niet-digitaal berust terwijl dat wel zo is. Een aanpassing aan één van de twee stellingen is dus noodzakelijk. Daarbij zou het woord 'accepteren' aangepast kunnen worden naar het woord 'realiseren', wat een volledig andere connotatie heeft. 'Accepteren' kan namelijk ook impliceren dat je het eens bent met wat er gebeurt, wat bij vele digitaal beruste respondenten niet het geval is.

Naast de test omtrent digitale berusting zou de test omtrent privacy geletterdheid ook geen volledig waarheidsgetrouw beeld geven. Zo geven sommige respondenten een eerder hogere of lagere privacy geletterde indruk tijdens het interview dan dat de test aangaf. Een aanpassing van de test kan dan ook nuttig zijn. Het stellen van open vragen of het toepassen van giscorrectie kan ervoor zorgen dat er toch een correct beeld van de werkelijkheid wordt weergegeven.

Wat uit dit onderzoek ook bleek, is dat digitale media alomtegenwoordig is. De respondenten in dit onderzoek zijn dan ook massaal aanwezig op het internet en maken er dagelijks gebruik van. Daarvan zijn de meeste aanwezig op sociale media waarvoor verschillende redenen werden opgegeven zoals het in contact blijven met vrienden en familie, bijhouden wat anderen doen, geen keuze hebben, de verslavende factor enzovoort.

Wat betreft de resultaten omtrent de redenen voor de digitale berusting zijn er heel wat resultaten verzameld. Een eerste bevinding is dat respondenten met een hogere privacy geletterdheid vaker reflecteren over het topic privacy. Het is niet zo dat ze hun privacy veel meer beschermen, maar ze denken toch na over het delen van hun gegevens. Dat betekent wel niet dat ze meteen geloven dat privacybeschermend gedrag iets uithaalt. Ze reflecteren over het topic, maar zijn wel nog altijd digitaal berust. Het reflecteren over het topic privacy kwam minder voor bij de groep met een lagere privacy geletterdheid. Dat wil wel niet zeggen dat niemand dit deed. Het aantal was gewoon minder.

Dat brengt ons naar de volgende belangrijke bevinding. Een specifiek onderscheid tussen personen met een hogere en lagere privacy geletterdheid kan niet gemaakt worden. Het is geen rechtlijnige scheidingslijn. Op sommige vlakken verschillen personen met een hogere privacy geletterdheid met personen met een lagere privacy geletterdheid, maar op andere vlakken vertonen ze gelijkenissen. Ook is het soms zo dat een persoon uit de groep met een lagere privacy geletterdheid dezelfde motieven aangeeft als iemand uit de groep met een hogere privacy geletterdheid. Nuance is dus geboden. Het zwart-wit bekijken van deze situatie zou dan ook verkeerd zijn.

Er zal om die reden vooral een overzicht gegeven worden van alle mogelijke oorzaken van digitale berusting. Wanneer er een belangrijke gelijkenis of een belangrijk verschil naar boven kwam, zal dit daarbij vermeld worden.

Wat blijkt uit de literatuur, is dat er verschillende redenen zijn waarom personen zich digitaal berust voelen. Bedrijven zouden allereerst bijdragen aan dat gevoel door onder andere privacyverklaringen. Een privacybeleid zou een misleidend aspect met zich meedragen, namelijk dat ze personen een vals gevoel van veiligheid geven (Draper & Turow, 2019, p. 1831; Turow et al., 2015, p. 8). Dit empirisch onderzoek bevestigt dat. Er zijn inderdaad personen in dit onderzoek die aangeven dat ze denken dat het bestaan van een privacybeleid hen beter beschermt. Het is wel zo dat dit vooral voorkomt bij personen met een lagere privacy geletterdheid. Respondenten met een hogere privacy geletterdheid waren meer geneigd om aan te geven dat ze twijfelen aan de effectiviteit van een privacybeleid. Het is natuurlijk wel niet zo dat niemand binnen het lagere niveau van privacy geletterdheid aangaf in een privacybeleid te geloven, maar het komt wel vooral in deze groep voor.

Wat dit onderzoek nog bevestigt, is dat privacyverklaringen volgens de respondenten vaak te lang, omslachtig en juridisch worden omschreven. Dat aspect is ook iets dat door Draper en Turow (2019, p. 1831) wordt gezegd. Door het feit dat een privacybeleid vaak te lang is, gaan mensen die dingen niet lezen en wordt er bijgedragen aan een gevoel van digitale berusting. Het onderzoek dat in deze thesis gevoerd werd, gaat daar wel nog dieper op in en er kwam daarbij ook naar boven dat personen enerzijds te lui waren om een privacybeleid te lezen en dat ze er anderzijds gewoon geen tijd voor hebben, omdat zaken in dit leven nu eenmaal snel moeten gaan. Een andere opvallende bevinding daarbij is dat respondenten aangeven dat het een gewoonte is geworden. De manier waarop databedrijven werken en het feit dat wij als gebruiker op akkoord klikken, zou gewoon horen bij het dagelijkse leven. Het is het 'nieuwe normaal' geworden.

Er kwam omtrent privacyverklaringen nog een laatste aspect naar boven en dat gaat over het feit dat bedrijven dergelijke zaken expres lang en moeilijk maken of gebruikers blijven lastiggevallen met meldingen om ervoor te zorgen dat ze akkoord gaan. Bedrijven zouden namelijk vooral gegevens willen verzamelen en niet geïnteresseerd zijn in het beschermen van de privacy van gebruikers. Er worden dus vragen gesteld bij de ethiek van de technologiebedrijven. De onderzoeken van Draper en Turow (2019) en Turow et al. (2015) worden dus opnieuw bevestigd. Het is wel zo dat deze bevinding enkel naar boven kwam bij respondenten met een hogere of meer gemiddelde privacy geletterdheid. Respondenten met een lagere privacy geletterdheid gaven dit bijvoorbeeld niet aan.

Wat Draper en Turow (2019) ook vermeld hadden in hun onderzoek, is dat transparantie zou meespelen en dat blijkt inderdaad zo te zijn. Bijna alle respondenten, ongeacht hun niveau van privacy geletterdheid, vermeldden dat transparantie absoluut verbeterd dient te worden. Daarbij werd aangehaald dat 1. het te lang maken van een privacybeleid niet bijdraagt aan transparantie, 2. dat er absoluut geen overzicht is in wie welke gegevens verzamelt waardoor men niet weet waar te beginnen en 3. dat ze niet voldoende info geven over hoe verzamelde gegevens worden verwerkt.

Die onwetendheid is ook een reden voor het niet deftig kunnen beschermen van privacy en bijgevolg de digitale berusting. Als je niet weet waar je gegevens zitten, hoe kan je er dan voor zorgen dat ze beschermd worden?

In deze masterproef worden de bevindingen van Draper en Turow (2019) dus bevestigd. Het is duidelijk: bedrijven dragen wel degelijk bij aan een gevoel van digitale berusting.

Naast het feit dat bedrijven zouden bijdragen aan een gevoel van digitale berusting, kwamen er ook nog een aantal andere factoren naar boven drijven. Een eerste is daarbij het feit dat de Europese wetgeving omtrent privacy eigenlijk nog niet voldoende doeltreffend is. Niet effectief genoeg, straffeloosheid en onduidelijkheid zijn een aantal termen waarmee de GDPR wordt omschreven. Wat zou één enkele gebruiker kunnen doen als zelfs een wetgeving al niet voldoende helpt? Dat is het algemene beeld dat respondenten schetsen. De bedrijven zouden gewoon te veel macht hebben. Het is wel zo dat er enkel binnen de groep met een lagere privacy geletterdheid vermeld werd dat de GDPR misschien toch effectief is. Dat werd echter maar door twee respondenten aangehaald en telt zeker niet voor alle respondenten met dit niveau van privacy geletterdheid.

Wat ook verschillende malen aan bod kwam, is dat het puur aanwezig zijn op digitale media er eigenlijk al voor zorgt dat je gegevens over jezelf blootlegt. Het dilemma daarbij is dat het online gaan en gebruik maken van bijvoorbeeld sociale media deel is geworden van het leven. We kunnen er gewoon niet vanaf stappen, omdat we het nodig hebben in alledaagse omstandigheden. We zouden nu ook al zo lang online zijn dat zaken gewoon niet meer ongedaan gemaakt kunnen worden.

Nu het feit dat we massaal aanwezig zijn op digitale media zorgt ook voor een extra aspect, namelijk 'het ondergaan in de massa' om de woorden van respondent Tessa (persoonlijke communicatie, 10 maart 2020) te quoten. Respondenten stellen zich de vraag waarom hun gegevens nu zo belangrijk zouden zijn en ondernemen omwille van die reden geen actie om ze bijvoorbeeld te verwijderen. Pas als men met privacyinbreuken geconfronteerd wordt, blijkt men zich echt zorgen te maken. 'Out of sight, out of mind' is een spreekwoord dat hier wel lijkt te passen. Als mensen niet met de neus op de feiten worden gedrukt, gebeurt er op vlak van privacy vaak weinig.

Wat respondenten ook verschillende malen vertelden, was dat er ook gewoon geen overzicht te houden is. Er zijn te veel bedrijven en te veel opties, waardoor gebruikers van digitale media gewoon het gevoel hebben dat er geen beginnen aan is.

Als laatste komt nog een ander aspect van die onwetendheid naar boven. Sommige personen weten gewoon niet dat databedrijven hun gegevens verwerken en denken dat het alleen de hackers zijn die jouw gegevens proberen te gebruiken. Dit soort onwetendheid heeft iets minder betrekking op de digitale berusting, maar het speelt wel een rol. Dat soort onwetendheid komt alleen maar voor bij personen met een lagere privacy geletterdheid. Dat is natuurlijk niet bij iedereen zo, maar het komt wel alleen maar bij deze groep voor.

Nu is een belangrijke vraag: hoe zou dit fenomeen opgelost kunnen worden? Er werden verschillende mogelijkheden gegeven. Zo is educatie en sensibilisering een belangrijk aspect. Mensen bewust maken zorgt ervoor dat ze alle nodige informatie hebben en dat ze zelf een beslissing kunnen nemen over hoe ze met hun eigen data zullen omgaan. Het zal misschien niet leiden tot meer privacybeschermend gedrag, maar zo kunnen gebruikers in ieder geval zelf een beslissing nemen. Daarnaast wordt ook verschillende malen aangehaald dat de transparantie vanuit bedrijven moet verbeterd worden en dat dat eventueel zou kunnen aan de hand van filmpjes over privacyverklaringen en makkelijk te raadplegen tools om de eigen gegevens te bekijken. Geen constante updates geven, is ook echt een must zodat het nuttiger lijkt om een beleid te lezen.

11. Conclusie

Het doel van deze masterproef was om na te gaan welke factoren er bijdragen aan de digitale berusting en of privacy geletterdheid daar een rol bij speelt. De hoofdonderzoeksvraag luidde dan ook als volgt:

> Welke factoren dragen bij aan de digitale berusting van Belgische privacy geletterden en niet-privacy geletterden en hoe kan dit bestreden worden?

Digitale berusting is een relatief nieuw fenomeen waarbij een gevoel van hopeloosheid omtrent het beschermen van privacy naar boven komt (Draper & Turow, 2019; Kezer et al. 2016; Turow et al., 2015). Dat gevoel zou gebruikers van digitale media dan ook aanzetten om hun privacy minder te beschermen, omdat ze denken dat het toch niets zal uithalen. Om nu de grote 'waarom'-vraag te achterhalen, werd er in deze thesis een empirisch onderzoek gevoerd met kwalitatieve interviews. De respondenten werden allereerst aan een test onderworpen om te bepalen of ze al dan niet digitaal berust waren en hoe hoog hun niveau van privacy geletterdheid was.

Nu is het moment aangekomen om ons te buigen over de factoren die aan de basis liggen van de digitale berusting. Allereerst werd het zeer duidelijk dat bedrijven absoluut een rol spelen bij het gevoel van digitale berusting. Dat doen ze allereerst door een foute connotatie te geven aan het woord 'privacybeleid', maar daarnaast zorgen ze er ook nog voor dat dat privacybeleid vaak lang en omslachtig is waardoor gebruikers van digitale media geen zin of geen tijd hebben om zoiets te lezen. De transparantie laat tevens de wensen over. Te vaag of te weinig informatie zijn woorden die tijdens de interviews heel regelmatig werden herhaald. Onwetendheid over wat er nu met gegevens gebeurt, speelt dan ook een rol. Het zou echter geen toeval zijn dat dit gebeurt. Bedrijven willen namelijk niet dat gebruikers hun privacy beschermen, omdat ze zo meer gegevens kunnen gebruiken. Het is dus ook zo dat bedrijven expres op dit soort gedrag zouden aansturen.

Maar het probleem ligt natuurlijk niet alleen bij de bedrijven. Er zijn ook andere elementen die meespelen zoals het feit dat er een vals gevoel van vertrouwen circuleert, dat er geen overzicht is, dat wetgevingen niet effectief genoeg zijn, dat we niet met onze neus op de feiten worden gedrukt, dat we onze gegevens niet belangrijk genoeg achten, dat cookies of privacyverklaringen accepteren een gewoonte is geworden of dat we eigenlijk van het internet moet wegblijven terwijl we gewoon niet meer zonder kunnen. Om de woorden van respondent Thomas (persoonlijke communicatie, 5 april 2020) te quoten we zijn 'the point of no return' voorbij.

Natuurlijk is het aan ons als gebruiker om toch iets te ondernemen en daarvoor zouden initiatieven zoals opleidingen, sensibilisering en meer transparantie absoluut een meerwaarde zijn. Want pas als je weet wat er gebeurt, hoe iets gebeurt en hoe je het kan veranderen, kan je een weloverwogen beslissing nemen waar je zelf volledig achterstaat.

Om nu het laatste aspect van de hoofdonderzoeksvraag te beantwoorden, zijn we aangekomen bij de verschillen tussen hoge en lage privacy geletterdheid. Er werden een aantal verschillen vastgesteld, maar een verschil in niveau bepaalt absoluut niet alles. Sommige personen met een lager niveau van privacy geletterdheid hebben op bepaalde vlakken dezelfde kennis als personen met een hogere privacy geletterdheid. Soms is dat ook niet zo. Het is inderdaad zo dat er meer personen met een hogere privacy geletterdheid weten dat een privacybeleid niet altijd bedoeld is om gebruikers te beschermen. Ook weten voornamelijk hogere privacy geletterden dat bedrijven expres aansturen op het niet beschermen van privacy, maar dat wil absoluut niet zeggen dat er niemand binnen de groep met lagere privacy geletterdheid dat weet. Het zijn er gewoon minder. Wat vooral de boodschap is, is dat het noodzakelijk is om met een genuanceerde blik naar de resultaten te kijken, want niet alles is zomaar zwart-wit. Het is aan ons om het grijs te creëren.

12. Beperkingen en verder onderzoek

Dit onderzoek is een kwalitatief onderzoek. Bij een kwalitatief onderzoek kunnen er veel en verschillende resultaten bekomen worden, maar schuilt nuance natuurlijk om de hoek. Er dient dus opgepast te worden met eenduidige conclusies, omdat nu net die nuance belangrijk is. Daarnaast mogen deze resultaten ook niet gebruikt worden om conclusies te trekken over een volledige populatie. Er werd namelijk geen steekproef getrokken die representatief is voor de volledige bevolking.

Daarnaast dient ook zeker nog vermeld te worden dat het coronavirus ervoor zorgde dat interviews niet face to face konden doorgaan, waardoor misschien af en toe wat diepgang verloren ging.

Naar verder onderzoek toe kan er zeker verder gewerkt worden aan de tests voor digitale berusting en privacy geletterdheid. Bijgaand onderzoek zou namelijk kunnen aantonen of de voorgestelde verbeteringen in de praktijk werkzaam zijn. Als laatste kunnen toekomstige wetenschappelijke werken ook verder bouwen om het concept digitale berusting verder te ontleden om zo tot nog meer oplossingen te komen.

13. Bronnen

Al-Saqer, N. S., & Seliaman, M. E. (2016). The Impact of Privacy Concerns and Perceived Vulnerability to Risks on Users Privacy Protection Behaviors on SNS: A Structural Equation Model. *International Journal of Advanced Computer Science and Applications, 7*(5), 142-147.

Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior*, *56*, 147–154.

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online Privacy Concerns and Privacy Management: A Meta-Analytical Review: Privacy Concerns Meta-Analysis. *Journal of Communication*, *67*(1), 26–53.

Chen, H. T. (2018). Revisiting the Privacy Paradox on Social Media with an Extended Privacy Calculus Model: The Effect of Privacy Concerns, Privacy Self-Efficacy, and Social Capital on Privacy Management. *American Behavioral Scientist*, *62*(10), 1392–1412.

Coskun, S., & Karayagız Muslu, G. (2019). Investigation of Problematic Mobile Phones Use and Fear of Missing Out (FoMO) Level in Adolescents. *Community Mental Health Journal*, *55*(6), 1004–1014.

Danna, A., & Gandy, O. H. (2002). All That Glitters is Not Gold: Digging Beneath the Surface of Data Mining. J*ournal of Business Ethics, 40*(4), 373–386.

Deuze, M. (2011). Media life*. Media, culture & society, 33*(1), 137-148.

Draper, N. A., & Turow, J. (2019). The corporate cultivation of digital resignation. *New Media & Society*, *21*(8), 1824–1839.

Facebook. (s.d.-a). *Privacyinstellingen en -functies* [webpagina]. Geraadpleegd op 14 februari, 2020 via https://www.facebook.com/settings?tab=privacy

Facebook. (s.d.-b). *Je Facebook-gegevens* [webpagina]. Geraadpleegd op 14 februari, 2020 via https://www.facebook.com/settings?tab=your_facebook_information

Flair. (s.d.-a). *Wij maken gebruik van cookies* [webpagina]. Geraadpleegd op 14 februari 2020, via https://www.flair.be/nl/

Flair. (s.d.-b). *Cookie-instellingen [*webgpagina]. Geraadpleegd op 14 februari 2020, via https://www.flair.be/nl/

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, *77*, 226–261.

Gerlitz, C., & Helmond, A. (2013). The like economy: Social buttons and the data-intensive web. *New Media & Society*, *15*(8), 1348–1365.

Gimpel, H., Kleindienst, D., & Waldmann, D. (2018). The disclosure of private data: Measuring the privacy paradox in digital services. *Electronic Markets*, *28*(4), 475–490.

Givens, C. L. (2015). *Information privacy fundamentals for librarians and information professionals.* New York, De Verenigde Staten: Rowman and Littlefield.

Hoepman, J. H., & van Lieshout, M. (2012). Privacy. In E. R. Leukfeldt, & W. P. Stol (Reds.), *Cyber Safety: An Introduction* (pp. 75-87). Den Haag, Nederland: Eleven International Publishing.

Kezer, M., Sevi, B., Cemalcilar, Z., & Baruh, L. (2016). Age differences in privacy attitudes, literacy and privacy management on Facebook. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *10*(1).

Langenderfer, J., & Miyazaki, A. D. (2009). Privacy in the information economy. *Journal of Consumer Affairs, 43*(3), 380-388.

Masur, P. K., Teutsch, D. & Trepte, S. (2017). Entwicklung und Validierung der Online Privatheits-Kompetenzskala (OPLIS) [Development and validation of the Online Privacy Literacy Scale (OPLIS)]. *Diagnostica, 63*, 256-268.

Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think*. Boston, De Verenigde Stagen: Houghton Mifflin Harcourt.

Mediawijs. (s.d.). *Over ons* [webpagina]. Geraadpleegd op 22 mei, 2020 via https://mediawijs.be/over-ons

Mudialba, P. J., Nair, S., & Ma, J. (2017). Finger printing on the web. *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*, 475–477. Geraadpleegd op 19 december, 2019 via https://ieeexplore.ieee.org/document/8249089

Resengo (s.d). *Login – Inschrijven* [webpagina]. Geraadpleegd op 14 februari, 2020 via https://www.resengo.com/Code/Login_Simple.asp?CID

Sarikakis, K., & Winter, L. (2017). Social Media Users' Legal Consciousness About Privacy. *Social Media + Society*, *3*(1), 1-14.

Schwab, K. (2017). *The fourth industrial revolution*. New York, De Verenigde Staten: Crown Business.

Solove, D. J. (2004). *The digital person: Technology and privacy in the information age*. New York, De Verenigde Staten: New York University Press.

Solove, D. J. (2008*). Understanding Privacy*. Cambridge, De Verenigde Staten: Harvard University Press.

Solove, D. J. (2015). The meaning and value of privacy. In B. Roessler, & D. Mokrosinska (Reds.), *Social Dimensions of privacy: Interdisciplinary perspectives* (pp. 71-81). Cambridge, Verenigd Koninkrijk: Cambridge University Press.

Symantec. (2015). *State of privacy report 2015*. Geraadpleegd op 15 november, 2019 via https://www.yumpu.com/en/document/read/54981523/state-of-privacy-report-2015

The Economist. (2019, 18 december). Companies should take California's new data-privacy law seriously. Geraadpleegd op 31 mei, 2020 via https://www.economist.com/business/2019/12/18/companies-should-take-californias-new-data-privacy-law-seriously

The Economist. (2020, 23 april). Privacy in a pandemic. Geraadpleegd op 31 mei, 2020 via https://www.economist.com/europe/2020/04/23/privacy-in-a-pandemic

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., et al. (2015). Do people know about privacy and data protection strategies? Towards the "online privacy literacy scale" (OPLIS). In S. Gutwirth, R. Leenes, & P. de Hert (Reds.), *Reforming European data protection law* (pp. 333-365). Heidelberg, Duitsland: Springer.

Turow, J., Hennessy, M., & Draper, N. (2015). The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them Up to Exploitation. *The Annenberg School for Communication*, 1-24. Geraadpleegd op 3 november, 2019 via https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_0.pdf

Vandendriessche, K., & De Marez, L. (2019). *Imec.Digimeter.* Geraadpleegd op 31 mei, 2020 via https://www.scribbr.nl/apa-voorbeelden/rapport-jaarverslag-online/

Van Dijck, J., & Nieborg, D. (2009). Wikinomics and its discontents: a critical analysis of Web 2.0 business manifestos. *New media & society, 11*(5), 855-874.

Van Dijck, J., Poell, T., & De Waal, M. (2018). *The platform society: Public values in a connective world*. New York, De Verenigde Staten: Oxford University Press.

Verordening (EU) 2016/679. (2018, 25 mei). Geraadpleegd op 24 februari, 2020 via https://eurlex.europa.eu/legalcontent/NL/TXT/?qid=1528874672298&uri=CELEX%3A32016R0679

Vlemings, J. (2018, 25 mei). Meer privacy met GDPR vanaf vandaag? Wat er nu écht voor u verandert. *HLN*. Geraadpleegd op 3 november, 2019 via https://www.hln.be/ihln/internet/meer-privacy-met-gdpr-vanaf-vandaag-wat-er-nu-echt-voor-u-verandert~a2870fa6/

Wissinger, C. (2017). Privacy Literacy: From Theory to Practice. *Communications in Information Literacy*, *11*(2), 378-389.

Wright, S. A., & Xie, G. X. (2019). Perceived Privacy Violation: Exploring the Malleability of Privacy Expectations. *Journal of Business Ethics*, *156*(1), 123–140.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. New York, De Verenigde Stagen: Public Affairs.

DEEL 3

BIJLAGEN

Bijlage 1: Facebookberichten met oproep aan respondenten

Eerste bericht werd verstuurd op 24 februari 2020

Hallo iedereen,

Ik zit in mijn laatste jaar Communicatiewetenschappen en voor mijn masterproef onderzoek ik het concept privacy en welke invloed het gebrek daaraan heeft op ons. Om dat te kunnen onderzoeken, ben ik op zoek naar personen die wel controle over hun privacy willen uitoefenen, maar het gevoel hebben dat wat ze ook doen hun privacy toch niet beschermd kan worden. Je hoeft daarvoor geen specifieke kennis van het concept te hebben, maar mensen met voorkennis zijn ook zeker welkom.

Ben jij iemand die je privacy wilt beschermen, maar het gevoel hebt dat je dat niet lukt? Stuur me dan zeker een persoonlijk berichtje.

Alvast ongelofelijk bedankt!

Groetjes
Femke Tinkl

Tweede bericht werd verstuurd op 3 maart 2020

Ben jij iemand die je online privacy wilt beschermen, maar het gevoel hebt dat je dat niet lukt? Stuur me dan zeker een persoonlijk berichtje. Ik ben voor mijn masterproef namelijk op zoek naar deelnemers voor mijn onderzoek.

Groetjes
Femke Tinkl

Bijlage 2: Originele OPLIS-test

Hieronder kan u alle 20 vragen van de originele OPLIS-test terugvinden. De bron van deze test is de volgende:

Masur, P. K., Teutsch, D. & Trepte, S. (2017). Entwicklung und Validierung der Online Privatheits-Kompetenzskala (OPLIS) [Development and validation of the Online Privacy Literacy Scale (OPLIS)]. *Diagnostica, 63*, 256-268.

Label	Item	Answer options
Knowledge about institutional practices		
PRA_01	The National Security Agency (NSA) accesses only public user data, which are visible for anyone.	True/**false**/don't know
PRA_02	Social network site operators (e.g. Facebook) also collect and process information about non-users of the social network site.	**True**/false/don't know
PRA_03	User data that are collected by social network site operators (e.g. Facebook) are deleted after five years	True/**false**/don't know
PRA_04	Companies combine users' data traces collected from different websites to create user profiles	**True**/false/don't know
PRA_05	E-mails are commonly passed over several computers before they reach the actual receiver.	**True**/false/don't know

Tabel 3: OPLIS-test vragen omtrent institutionele praktijken (Masur et al., 2017).

Label	Item	Answer options
Knowledge about technical aspects of data protection		
TEC_01	What does the term „browsing history" stand for?	In the browsing history… **A. ...the URLs of visited websites are stored.** B. ...cookies from visited websites are stored. C. ...potentially infected websites are stored separately. D. ...different information about the user are stored, depending on the browser type
TEC_02	What is a „cookie"?	**A. A text file that enables websites to recognize a user when revisiting.** B. A program to disable data collection from online operators. C. A computer virus that can be transferred after connecting to a website. D. A browser plugin that ensures safe online surfing.
TEC_03	What does the term „cache" mean?	**A. A buffer memory that accelerates surfing on the Internet.** B. A program that specifically collects information about an Internet user and passes them on to third parties. C. A program, that copies data on an external hard drive to protect against data theft. D. A browser plugin that encrypts data transfer when surfing online.
TEC_04	What is a „trojan"?	A trojan is a computer program, that… **A. ...is disguised as a useful application, but fulfills another function in the background** B. ...protects a computer from viruses and other malware C. ... was developed for fun and has no specific function. D. ... caused damage as computer virus in the 90ies but doesn't exist anymore
TEC_05	What is a „firewall"?	**A. A fallback system that will protect the computer from unwanted web attacks.** B. An outdated protection program against computer viruses C. A browser plugin that ensures safe online surfing. D. A new technical development that prevents data loss in case of a short circuit.

Tabel 4: OPLIS-test vragen over de technische asp. van databescherming (Masur et al., 2017).

Label	Item	Answer options
Knowledge about data protection law		
GES_01	Forwarding anonymous user data for the purpose of market research is legal in the European Union.	**True**/false/don't know
GES_02	The EU-Directive on data protection...	**A. ... has to be implemented into national data protection acts by every member state.** B. ... does not exist yet. C. … functions as a transnational EU-data protection act. D. ... solely serves as a non-committal guideline for the data protection acts of the member states.
GES_03	In Germany the same standard GTC applies for all SNS. Any deviations have to be indicated	True/**false**/don't know
GES_04	According to German law, users of online applications that collect and process personal data have the right to inspect which information about them is stored.	**True**/false/don't know
GES_05	Informational self-determination is…	**A. …a fundamental right of German citizens.** B. ... a philosophical term. C. ... the central claim of data processors. D. ...the central task of the German Federal Data Protection Commissioner...

Tabel 5: OPLIS-test vragen over de privacywetgeving (Masur et al., 2017).

Label	Item	Answer options
Knowledge about data protection strategies		
STR_01	Tracking of one's own internet is made more difficult if one deletes browser information (e.g. cookies, cache, browser history) regularly.	**True**/false/don't know
STR_02	Surfing in the private browsing mode can prevent the reconstruction of your surfing behavior, because no browser information is stored.	**True**/false/don't know
STR_03	Using false names or pseudonyms can make it difficult to identify someone on the Internet.	**True**/false/don't know
STR_04	Even though It-experts can crack difficult passwords, it is more sensible to use a combination of letters, numbers and signs as passwords than words, names or simple combinations of numbers.	**True**/false/don't know
STR_05	In order to prevent the access to personal data, one should use various passwords and user names for different online applications and change them frequently.	**True**/false/don't know

Tabel 6: OPLIS-test vragen over strategieën om data te beschermen (Masur et al., 2017).

Bijlage 3: Gegevensverzameling

Test om privacy geletterdheid en digitale berusting vast te leggen

Introductietekst

Beste deelnemer,

Mijn naam is Femke Tinkl en ik ben een masterstudente Communicatiewetenschappen aan de VUB. Allereerst wil ik u hartelijk bedanken voor uw deelname aan dit onderzoek. Naar aanleiding van mijn masterproef onderzoek ik namelijk het concept privacy waarbij het doel is om te bekijken hoe internetgebruikers omgaan met hun privacy.

Vooraleer er van start kan gegaan worden met het diepte-interview, zou ik u willen vragen om de volgende test in te vullen. De vragenlijst zal ongeveer 15 tot 20 minuten in beslag nemen. Bij elke vraag dient er maar 1 antwoord te worden aangeduid. Het is belangrijk dat u bij het invullen van deze vragenlijst geen beroep doet op het internet of andere hulpmiddelen. De uitkomst van de test geeft mij namelijk inzicht over uw kennis van het onderwerp.

U mag er ook op vertrouwen dat er betrouwbaar omgegaan zal worden met de resultaten van dit onderzoek en dat uw gegevens anoniem zullen worden verwerkt.

Nog eens hartelijk bedankt voor uw deelname aan dit onderzoek.

Met vriendelijke groeten
Femke Tinkl

Vragenlijst die het onderzoek voorafging

Algemene gegevens:

Naam	
Geboortedatum	
Woonplaats	
Beroep/opleiding	

Onderwerpgerelateerde vragen:

1. E-mails passeren vaak eerst meerdere computers voordat ze de eigenlijke ontvanger bereiken.
    a. Waar
    b. Onwaar
    c. Geen idee

2. Wat is een "cookie"?
    a. Een programma dat het verzamelen van gegevens door online applicaties uitschakelt.
    b. Een tekstbestand dat websites in staat stelt om een gebruiker te herkennen wanneer deze een bepaalde website opnieuw bezoekt.
    c. Een computervirus dat kan worden overgedragen nadat er verbinding wordt gemaakt met een website.
    d. Een browser plugin die ervoor zorgt dat men veilig online kan surfen.

3. Het doorsturen van anonieme gebruikersgegevens voor marktonderzoek is legaal in de Europese Unie.
    a. Waar
    b. Onwaar
    c. Geen idee

4. Het gebruik van valse namen of pseudoniemen maakt het voor anderen moeilijker om iemand online te identificeren.
    a. Waar
    b. Onwaar
    c. Geen idee

5. De GDPR (De algemene verordening gegevensbescherming) ...
    a. ... is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke EU-lidstaat.
    b. ... bestaat nog niet.
    c. ... is een Amerikaanse wetgeving.
    d. … dient uitsluitend als vrijblijvende richtlijn voor de EU-lidstaten.

6. Om de toegang tot persoonlijke gegevens te voorkomen, moet men verschillende wachtwoorden en gebruikersnamen voor verschillende onlinetoepassingen gebruiken en deze regelmatig wijzigen.
    a. Waar
    b. Onwaar
    c. Geen idee

7. Socialenetwerksites zoals Facebook verzamelen en verwerken ook informatie over niet-gebruikers van de socialenetwerksite.
    a. Waar
    b. Onwaar
    c. Geen idee

8. De National Security Agency (NSA) heeft enkel toegang tot openbare gebruikersgegevens, die voor iedereen zichtbaar zijn.
    a. Waar
    b. Onwaar
    c. Geen idee

9. Wat is een "trojan"? Een trojan is een computerprogramma, dat...
    a. ...een computer beschermt tegen virussen en andere malware.
    b. ... werd ontwikkeld voor de lol en geen specifieke functie heeft.
    c. ... in de jaren '90 als computervirus schade veroorzaakte, maar niet meer bestaat.
    d. ...vermomd is als een nuttige toepassing, maar op de achtergrond eigenlijk een andere functie vervult.

10. Volgens de GDPR, hebben gebruikers van online applicaties (die persoonlijke gegevens verzamelen en verwerken) het recht om te controleren welke informatie over hen is opgeslagen.
    a. Waar
    b. Onwaar
    c. Geen idee

11. Ik wil controle kunnen uitoefenen over wat marketeers online over mij te weten kunnen komen.
    a. Ja
    b. Nee

12. Waar staat de term 'browsegeschiedenis' voor? In de browsegeschiedenis...
    a. ... worden cookies van bezochte websites opgeslagen.
    b. ... worden mogelijk geïnfecteerde websites apart opgeslagen.
    c. ... worden de URL's van bezochte websites opgeslagen.
    d. ... wordt, afhankelijk van het type browser, verschillende informatie over de gebruiker opgeslagen.

13. Het "recht om vergeten te worden" is ...?
    a. ... een recht van elke burger van de Europese Unie.
    b. ... een filosofische term.
    c. ... de centrale claim van dataverwerkers.
    d. ... de centrale taak van de Gegevensbeschermingsautoriteit.

14. Het tracken van iemands internetgebruik wordt belemmerd als men regelmatig browserinformatie (bijv. cookies, cache, browsergeschiedenis) verwijdert.
    a. Waar
    b. Onwaar
    c. Geen idee

15. In Europa dienen privacyverklaringen van bedrijven aan bepaalde voorwaarden te voldoen die vastgelegd zijn in de GDPR.
    a. Waar
    b. Onwaar
    c. Geen idee

16. Privébrowsen zorgt ervoor dat men iemands surfgedrag moeilijker kan tracken, omdat er geen browserinformatie wordt opgeslagen.
    a. Waar
    b. Onwaar
    c. Geen idee

17. Wat betekent de term "cache"?
    a. Een programma dat specifiek informatie over een internetgebruiker verzamelt en doorgeeft aan derden.
    b. Een buffergeheugen dat het surfen op het internet versnelt.
    c. Een programma, dat gegevens op een externe harde schijf kopieert om ze te beschermen tegen gegevensdiefstal.
    d. Een browser plugin die de overdracht van data bij het online surfen versleutelt.

18. Gebruikersgegevens die door socialenetwerksites (zoals Facebook) worden verzameld, worden na vijf jaar verwijderd.
    a. Waar
    b. Onwaar
    c. Geen idee

19. Hoewel IT-experts moeilijke wachtwoorden kunnen kraken, is het beter om een combinatie van letters, cijfers en tekens als wachtwoord te gebruiken dan woorden, namen of eenvoudige combinaties van cijfers.
    a. Waar
    b. Onwaar
    c. Geen idee

20. Wat is een "firewall"?
    a. Een fallback-systeem dat de computer zal beschermen tegen ongewenste webaanvallen.
    b. Een verouderd beveiligingsprogramma tegen computervirussen.
    c. Een browser plugin die ervoor zorgt dat men veilig online kan surfen.
    d. Een nieuwe technische ontwikkeling die dataverlies bij kortsluiting voorkomt.

21. Ik heb geaccepteerd dat ik weinig controle kan uitoefenen over wat marketeers online over mij te weten kunnen komen.
    a. Ja
    b. Nee

22. Bedrijven combineren de data, die gebruikers achterlaten op verschillende websites, om een gebruikersprofiel op te stellen.
    a. Waar
    b. Onwaar
    c. Geen idee

Belangrijke opmerking:
De vragen die hierboven werden opgesteld, zijn gebaseerd op de onderzoeken van:

- Masur, P. K., Teutsch, D. & Trepte, S. (2017). Entwicklung und Validierung der Online Privatheits-Kompetenzskala (OPLIS) [Development and validation of the Online Privacy Literacy Scale (OPLIS)]. *Diagnostica, 63*, 256-268.
- Turow, J., Hennessy, M., & Draper, N. (2015). The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them Up to Exploitation. Geraadpleegd op 3 november, 2019 via https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_0.pdf

Diepte-interview

Topiclijst met per topic een aantal mogelijke vragen

Topic	Mogelijke vragen
Digitale mediagebruik	○ Hoe vaak maak je ongeveer gebruik van online media (dagelijks, wekelijks, …)? ○ Welke soort sites bezoek je het vaakst? ○ Maak je ook gebruik van sociale media? ➔ Zo ja, dewelke?
Gedrag op sociale media	○ Deel jij regelmatig zaken op sociale media? ➔ Waarom net vaak of weinig? ○ Welke informatie deel jij zoal op sociale media? ➔ Waarom bepaalde informatie wel of niet?
Digitale Routine	Beschrijf eens een dag uit jouw leven van 's morgens tot 's avonds waarbij je telkens vermeldt hoe digitale media daarin past.
Privacyinstellingen	○ Bekijk jij regelmatig de privacyinstellingen van de sociale media waarop je actief bent? ▪ Waarom wel/niet? ○ Vind je de privacyinstellingen makkelijk in gebruik? ▪ Waarom wel/niet? ○ Denk je dat wanneer je de *privacy settings* op een bepaalde manier instelt, je onlinebedrijven kan tegenhouden om ongewild gegevens te verzamelen en te verwerken? ▪ Waarom wel/niet?

Cookies	○ Vermijd je websites die cookies gebruiken? ▪ Waarom wel/niet? ○ Wanneer een website vraagt om cookies te aanvaarden, doe je dit dan meteen of bekijk je eerst over welke cookies het gaat? ○ Denk je dat online bedrijven je gegevens niet meer opslaan als je cookies weigert?
Formulieren	○ Weiger je soms om persoonlijke gegevens online te delen als daarom gevraagd wordt door websites? (Aanmelden voor wedstrijden, intellectuele eigendom, bepaalde producten of diensten) ▪ Waarom wel/niet? ○ Heb je het gevoel dat je bepaalde voordelen misloopt als je je persoonlijke gegevens niet deelt?
Privacybeleid	○ Wat betekent het volgens jou als een bedrijf een privacybeleid heeft? ○ Lees je het privacybeleid van websites waar je op surft eerst? ▪ Waarom wel/niet? ○ Denk je dat bedrijven met een privacybeleid je privacy beter beschermen? ▪ Waarom wel/niet?
Transparantie	Online bedrijven dienen nu transparant te zijn in hoe ze gegevens van leden verzamelen en verwerken. ○ Heb je het gevoel dat je weet hoe bedrijven jouw gegevens verzamelen, verwerken en delen? ▪ Wat denk jij dat bedrijven over jou weten? ▪ Wat denk jij dat bedrijven precies met jouw gegevens doen? ○ Heb je ooit al de gegevens, die bepaalde socialemediaplatformen hebben verzameld over jou, opgevraagd? ▪ Waarom wel/niet? ○ Heb je jezelf ooit al eens opgezocht op Google om na te gaan welke info ze precies over jou hebben? ➔ Waarom wel/niet?

	○ Vind je dat online bedrijven voldoende transparant zijn? ▪ Waarom wel/niet? ▪ Wat vind je dat er op vlak van transparantie bij bedrijven nog verbeterd kan worden?
Privacyinbreuken	○ Heb je al een aantal momenten gehad waarop je online privacy werd geschonden? ▪ Zo ja, kan je een aantal voorbeelden geven? ○ Vond je het belangrijk om deze privacyinbreuken te melden of op te lossen? ○ Denk je dat je iets had kunnen doen om die privacyinbreuken tegen te gaan? ▪ Zo ja/nee waarom? ○ Denk je dat je nu voldoende maatregelen hebt genomen om mogelijke toekomstige privacyinbreuken tegen te gaan? (Privacyinstellingen, het uitzetten van cookies, …)?
Privacy in de media	Tegenwoordig komen er vaak berichten in de media over datalekken of privacyinbreuken bij bedrijven zoals Facebook (Cambridge Analytica). ○ Wat denk jij daar precies van? ○ Maak je je daar zorgen over? ▪ Zo ja/nee, waarom?
GDPR	Een aantal jaren terug, kwam de GDPR tot leven. ○ Weet jij precies wat de belangrijkste punten van de GDPR zijn? ○ Vind je dat de GDPR doeltreffend is? ➔ Waarom wel/niet?
Privacycontrole (Afsluitende vraag)	Heb je nu als gebruiker van het internet het gevoel dat je controle kan uitoefenen over je eigen privacy? ▪ Deze laatste vraag dient als richtlijn. Naargelang de antwoorden van de respondenten, wordt deze vraag aangepast.

Bijlage 4: Visuele elementen voor het interview

Visueel element omtrent privacyinstellingen

Afbeelding 1: Privacysettings Facebook (Facebook, s.d.-a).

Visueel element omtrent het opvragen van de eigen informatie

Afbeelding 2: Instellingen 'Je Facebook-gegevens (Facebook, s.d.-b).

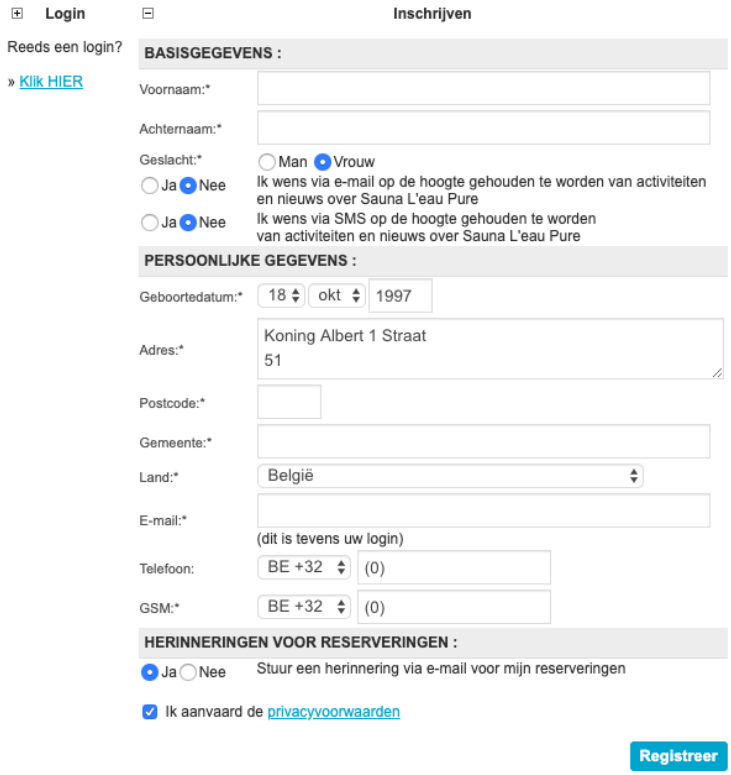
Visueel element omtrent de notificatie van cookies

Afbeelding 3: Cookienotificatie Roularta (Flair, s.d.-a).

Visueel element omtrent de instellingen van cookies

Afbeelding 4: Cookie-instellingen Roularta (Flair, s.d.-b).

Visueel element omtrent het invullen van gegevens in registraties



Afbeelding 5: Voorbeeld formulieren of registraties (Resengo, s.d.).

Bijlage 5: Informed consent formulier

TOESTEMMINGSFORMULIER (informed consent)

Betreft: Masterproef onderzoek naar privacy

Onderzoeker: Femke Tinkl

Verklaring deelnemer:

Ik begrijp dat:

- ik vrijwillig aan het onderzoek deelneem en dat ik mijn deelname aan het onderzoek op elk moment kan stopzetten zonder daarvoor een bepaalde reden te moeten opgeven.
- er gegevens over mij verzameld zullen worden tijdens het onderzoek.
- de gegevens, die over mij verzameld worden, met de nodige vertrouwelijkheid zullen worden behandeld en volledig zullen worden geanonimiseerd.

Ik verklaar dat:

- de onderzoeker mij voldoende heeft geïnformeerd over de verschillende aspecten van het onderzoek (de aard, het doel, de methode en de eventuele voor- en nadelen).
- er mij voldoende tijd werd gegeven om over mijn deelname aan het onderzoek na te denken.
- de onderzoeker me de kans heeft gegeven om mogelijke vragen over het onderzoek te stellen en me op deze vragen een helder antwoord heeft verschaft.
- mijn deelname aan het onderzoek volledig vrijwillig is en dat de onderzoeker de toestemming heeft om het interview op te nemen.
- de informatie en gegevens, die ik tijdens mijn deelname aan het onderzoek verschaf, in alle anonimiteit verwerkt mogen worden in een rapport, een presentatie, een artikel of een andere publicatie.

Naam, voornaam:

Handtekening Datum: __/__/__

……

Verklaring onderzoeker: Als onderzoeker binnen deze masterproef verklaar ik dat ik voldoende informatie heb verschaft over de verschillende aspecten van het onderzoek (aard, doel en methode) en dat ik eventuele bijkomende vragen naar waarheid zal beantwoorden.

Naam, voornaam:

Handtekening Datum: __/__/__

……

Bijlage 6: Codeboom

Gebruik van digitale media

- Dagelijkse routine
- Verhouding sociale media en anderen
- Hoeveelheid van het gebruik
- Gebruik van sociale media
- Gebruik van andere sites
- Gebruik van digitale media

Gedrag bij het gebruik van digitale media

- Eigen informatie opvragen of bekijken
- Het bannen van digitale media?
- Beoordeling van eigen gedrag
- Mening over het gedrag van de algemene bevolking
- Het delen van persoonlijke informatie
    - Reden voor het delen of niet delen van informatie
    - Delen van gegevens via registraties
    - Delen van gegevens op sociale media
- Gedrag t.a.v. privacyinstellingen
    - Reden van het gedrag t.a.v. privacyinstellingen
- Gedrag t.a.v. cookies
    - Reden van het gedrag t.a.v. cookies
- Gedrag t.a.v. privacybeleiden
    - Reden van het gedrag t.a.v. privacybeleiden

Evaluatie v/d strategiën van bedrijven

- Beoordeling van sociale media als kanaal
- Evaluatie van huidige wetgevingen (GDPR)
- Evaluatie handelen overheden
- Evaluatie v/d strategieën van bedrijven
    - Transparantie
    - Privacyinstellingen
    - Privacybeleiden
    - Het opvragen/verzamelen van gegevens
    - Het gebruik van gegevens
        - Persoonlijke reclame
    - Cookies

Houding/mening t.o.v. eigen privacy

- Reden van deze houding

Privacyinbreuken

- Aanpak om het te vermijden

Kennis van het online privacygegeven

- Bron van de kennis
- Kennis over cookies
- Kennis over privacyinstellingen
- Kennis over privacybeleiden
- Kennis over verhalen in de media over privacy
- Kennis over wetgevingen
- Kennis over het verzamelen en gebruik van gegevens
- Kennis over digitale media
    - Kennis over sociale media

Mogelijke verbeteringen/oplossingen

- Sensibilisering/opleidingen
- Transparantie
- Wetgevingen