FACULTEIT ECONOMIE EN BEDRIJFSKUNDE

WELKE PARTIJEN ZIJN IN STAAT OM PRIVACY TE WAARBORGEN IN HET METAVERSUM?

Word count: 21.748

Matthias Calmeyn
Stamnummer: 01507917

Promotor: Prof. Marleen Easton

Masterproef voorgedragen tot het bekomen van de graad van:
Master of Science in de Handelswetenschappen
Afstudeerrichting:
Master Management en Informatica

Academiejaar: 2021-2022

UNIVERSITEIT GENT

VERTROUWLIJKHEIDSCLAUSULE

TOESTEMMING

Ondergetekende verklaart dat de inhoud van deze masterproef mag geraadpleegd en/ of gereproduceerd worden, mits bronvermelding.

Naam student: Matthias Calmeyn

WOORD VOORAF

Het schrijven van deze tweede masterproef was niet altijd even gemakkelijk, daarom bedank ik graag de mensen die mij steunden in het nemen van deze laatste horde als student. Eerst en vooral wil ik mijn promotor Prof. Dr. Marleen Easton bedanken, die mij de kans gaf om dit onderzoek uit te voeren en op wie ik kon rekenen om vragen te stellen. Zelf aanschouw ik een masterproef als een bewijsstuk van zelfstandig werken waarbij kritisch denken en doorzettingsvermogen de grote uitdagingen vormen. De manier waarop mevrouw Easton met haar studenten omgaat en het vertrouwen dat hierbij komt kijken, ligt volledig in lijn met mijn visie rond een optimale aanpak van een samenwerking.

Verder wil ik mijn dankbaarheid betuigen aan mijn vrienden en familie voor de steun die ze mij gaven. In het bijzonder bedank ik graag Alix De Wilde en Zoë Geboes voor hun hulp bij het nakijken van dit werk. Tenslotte wil ik graag WeGroup bedanken die mij de kans gaf om deze masterproef af te ronden. Bij WeGroup werkte ik als studentondernemer tijdens het schrijven van deze masterproef. Door de tijd die kroop in het maken van dit werkstuk, nam ik vroeger dan gepland afscheid. Het begrip hiervoor was hartverwarmend.

Het inlezen en nadenken over het metaversum en privacy heeft mij tot nieuwe inzichten doen komen, wat absoluut zorgt voor een verbreding van mijn persoonlijk wereldbeeld. Zelf ben ik meer bewust geworden omtrent het ‘digitale spoor’ dat elke internetgebruiker, onbewust, achterlaat. Idealiter verhoogt deze masterproef het bewustzijn rond digitale privacy of zet het aan tot vervolgonderzoek. In ieder geval moet deze masterproef doen aanzetten tot denken.

Matthias Calmeyn, 2022

ABSTRACT

Deze thesis onderzoekt welke partijen in staat zijn privacy te waarborgen binnen het metaversum en tracht te verklaren waarom dit zo moeilijk is. Het metaversum is een virtuele wereld waarin gebruikers met elkaar tegelijk in verbinding staan en vrij kunnen interageren met virtuele objecten. Het grote verschil met de huidige sociale media is dat het metaversum gebruik maakt van draagbare sensoren en technologieën die de bezoekers willen onderdompelen in een virtuele realiteit door middel van immersie. Door de extra sensoren en de immersieve technologieën, geven eindgebruikers onbewust meer gevoelige informatie vrij waardoor hun privacy in het gedrang komt. Om te onderzoeken welke partijen deze privacy kunnen waarborgen, werd een systematisch literatuuronderzoek gevoerd, waarbij empirisch bewijsmateriaal werd verzameld door het analyseren van een vooraf gespecificeerde selectie van bestaande literatuur. Het is volgens de literatuur niet ondenkbaar dat een grote hoeveelheid van gevoelige data leidt tot een schending van de persoonlijke levenssfeer van de metaverse-gebruikers. Dit komt doordat de huidige bedrijfsmodellen van sociale internetplatformen voornamelijk gebouwd zijn rond het verzamelen en gebruiken van deze gegevens. Op basis van het literatuuronderzoek blijkt dat dit probleem moeilijk te reguleren valt vanwege een tekort aan bewustzijn van de consument. Onbewuste internetgebruikers blijken namelijk bereid om hun persoonlijke levenssfeer op te geven als onderdeel van het gehanteerde bedrijfsmodel. Hoewel overheden vandaag de dag waken over de persoonsgegevens van hun burgers, blijken deze publieke instanties onvoldoende in staat om digitale privacy te waarborgen. Bestaande onderzoeken suggereren, dat een overheid op vlak van technologische innovaties vaak te traag is of niet bereid is om in te grijpen. Bijkomend zijn overheden niet in staat om aan dezelfde snelheid te handelen als de Big Techreuzen. Ondanks dat deze Techbedrijven onderhevig zijn aan de wetten die hun eindgebruikers beschermen, blijven deze in staat om niet adequate wetten te omzeilen. De bedrijven die het metaversum uitbaten, hebben er baat bij om aan zelfregulatie te doen. Om ervoor te zorgen dat deze zelfregulering adequaat en transparant gebeurt, is er nood aan een grote druk van de bevolking en aan een globale instantie met soevereiniteit die meer concrete regels opstelt. Vandaag de dag is het moeilijk om privacy te laten waarborgen door één alleenstaande partij. Er is meer nood aan een wisselwerking tussen burgers, publieke instanties en bedrijven.

INHOUDSTABEL

AFKORTINGENLIJST

AI: Artificiële Intelligentie

AR: *Augmented reality*

EER: Europese Economische Ruimte

EU: Europese Unie

EVRM: Europees Verdrag voor de Rechten van de Mens

IT: Informatie Technologie

MR: *Mixed reality*

NFT: *Non-Fungible Token*

SLR: *Systematic Literature Review*

VR: *Virtual reality*

WWW: Wereldwijde web

XR: *Extended reality*

1 Introductie

De laatste decennia heeft de commercialisering van het internet en de exponentiële stijging van informatietechnologieën een grote impact gehad op het dagelijkse leven. Enerzijds heeft deze revolutie het belang van data aanzienlijk doen toenemen, anderzijds bracht het een fundamentele verandering in de sociale structuur van onze samenleving teweeg (Easton, 2019). Eén van deze technologische veranderingen met een grote maatschappelijke impact was de opkomst van sociale media. Hierdoor kwamen private bedrijven plots aan de bron te zitten van een grote hoeveelheid persoonsgegevens, vaak Big data genoemd. De populariteit van deze sociale netwerkplatforms is de laatste jaren aanzienlijk gegroeid in gebruik en in aantallen. Jain et al. (2021) verklaren deze trend doordat deze platformen zodanig ontwikkeld zijn opdat ze heel gemakkelijk in gebruik zijn. Hierdoor werden gebruikers van verschillende leeftijden naar deze platformen gelokt en gaven ze onbewust de essentiële voeding voor de big-datarevolutie. De sterke verbondenheid van ons dagelijks leven met het internet en de mogelijkheden om enorme hoeveelheden informatie te verwerken, vormen naast nieuwe technologische mogelijkheden, ook een bedreiging voor de veiligheid en privacy (Easton, 2019; van Schaik et al., 2018).

De digitalisering en de rol van het internet in ons dagelijkse leven heeft ook een impact op het sociale net van onze samenleving in zijn geheel. Dit komt mede doordat mensen steeds meer gebruik maken van online sociale netwerken (van Schaik et al., 2018). Sociaal netwerken zelf, is het uitbreiden van iemands contact met andere individuen, meestal via sociale mediasites zoals Facebook, Twitter, Instagram, LinkedIn en nog veel meer (Jain et al., 2021). Facebook is echter veel meer dan een netwerk waar gebruikers gemakkelijk met elkaar kunnen communiceren. In de loop der jaren is Facebook uitgegroeid tot een platform, speciaal ontworpen voor het genereren en delen van informatie met andere internetgebruikers. Vandaag de dag wordt Facebook in het algemeen erkend als het meest gebruikte sociaal medium voor het verspreiden van informatie onder de gebruikers (Akgül & Uymaz, 2022). Facebook wordt, naast het delen van inhoud, ook gebruikt als een persoonlijk communicatiemiddel (Brandtzaeg et al., 2010). Hierdoor komt er steeds meer informatie, in verschillende vormen, in de handen van sociale netwerken (Jain et al., 2021). Aanhangers van Big data zijn ervan overtuigd dat het combineren van deze grote hoeveelheden aan data, zal leiden tot betere beslissingen (Casanovas et al., 2017). Tegenstanders zijn dan weer bang dat deze gegevens misbruikt worden, wat de privacy van de eindgebruikers in gevaar brengt (Jain et al., 2021).

In oktober 2021 kondigde Facebook aan hun naam te wijzigen naar ‘Meta’. Meta verwijst naar de metaversum plannen die CEO Mark Zuckerberg ambieert. Volgens Almarzouqi et al. (2022) wijst deze recente aankondiging op een mogelijke toename van technologische innovatie die de wereld aanzienlijk zal veranderen. De naamswijziging van Facebook wekte alvast veel aandacht op voor het concept van het metaversum. Deze aandacht leidde tot de instroom van andere internetgiganten, wat op zijn beurt zorgde voor de versnelde ontwikkeling van de industrie en de intrede van kapitaal (Liu et al., 2022). Als gevolg stimuleerde deze kapitaalsinjectie de internationale beurzen tot een hogere waardering voor het metaversum waardoor het voormalige Facebook, volgens Liu et al. (2022), slaagde in zijn opzet. Met het metaversum verwijst Meta naar een virtuele wereld waarin de fysieke wereld en de cyberwereld met elkaar versmelten aan de hand van *virtual reality* (VR) en *augmented reality* (AR) (Legrand, 2021). Het verschil tussen deze realiteiten is dat *VR* zich volledig afspeelt in de cyberwereld, daar waar AR de fysieke wereld verrijkt met grafische elementen. Volgens Zuckerberg zal het samengaan van VR en AR binnen een online-omgeving, de volgende fase van het internet inluiden (Legrand, 2021). Het metaversum gaat bijgevolg nog een stap verder dan de traditionele sociale netwerken. Het wordt voorgesteld als de volgende, krachtigere versie van het internet. De belofte is dat gebruikers meer dan ooit ondergedompeld zullen worden in een reeks virtuele werelden die onderling met elkaar verbonden zijn (Van der Haegen et al., 2022).

Het begrip metaversum is echter niet nieuw. De term werd reeds in 1992 gebruikt door Neil Stephenson in zijn cyberpunk roman genaamd *Snow Crash* (Almarzouqi et al., 2022). Stephenson beschreef destijds het metaversum als een ruimte binnen een 3D-virtuele realiteit die toegankelijk is via persoonlijke VR-brillen (Almarzouqi et al., 2022). Jaren later, in 2009, werden Metaverses door Antonio Chavez-Aguayo omschreven als geanimeerde, *multi-user*, driedimensionale (3D) immersieve omgevingen met geluid die in real time met elkaar in verbinding staan. Ball (2022) voegt hieraan toe, dat het metaversum uiteindelijk zal dienen als toegangspoort tot de meeste online-ervaringen, en ook een groot deel van de fysieke wereld zal ondersteunen.

Onderzoeksbureau Gartner voorspelt dat 25 procent van de mensen, tegen 2026, minstens één uur per dag zullen doorbrengen in het metaversum (Gartner, 2022). Het ziet er naar uit dat wanneer het metaversum zijn verwachtingen zou inlossen, de eindgebruikers een nieuwe golf van informatie zouden afstaan aan de bedrijven achter het metaversum. Dit is iets dat volgens Jain et al. (2021) de verzamelwoede van deze technologiereuzen alleen maar zou aanwakkeren. Een inbreuk op de persoonlijke levenssfeer is een probleem waar rekening mee moet worden gehouden bij sociale activiteiten in het metaversum (Kye et al., 2021). De reden hiervoor ligt bij het feit dat er bij interacties in een metaversum allerlei

informatie wordt gegenereerd die in real time wordt verzameld en verwerkt (Kye et al., 2021). Bijgevolg is het mogelijk dat informatie wordt verzameld, die bij fysieke interacties niet kan worden opgeslagen. Volgens Rosenberg (2022) is het niet de technologie van het metaversum dat een risico vormt voor de samenleving, maar de technische infrastructuur die nodig is om deze virtuele wereld mogelijk te maken. Doordat slechts een bepaald aantal spelers in staat zijn om het metaversum te bouwen, komt er veel macht bij een beperkt aantal bedrijven te liggen. Rosenberg (2022) stelt dat deze bedrijven hierdoor de mogelijkheden krijgen om verschillende aspecten van ons leven te observeren, analyseren en bemiddelen (Rosenberg, 2022). Dit kan gaan over welke producten, diensten en informatie we te zien krijgen online, tot welke mensen we leren kennen, bevriend mee geraken en met wie we connecteren (Rosenberg, 2022). Aangezien de constructie van het metaversum en de gehele virtuele wereld evenwel nog in de kinderschoenen staat, dient zij reeds te worden onderworpen aan het toezicht van de bevoegde internationale instanties (Liu et al., 2022). Echter is het niet duidelijk wie er bevoegd is om deze virtuele wereld te leiden (Van der Haegen et al., 2022).

Aangezien metaverses mondiale platformen zijn, zorgen deze voor een vervaging van nationale grenzen. Hetgeen hand in hand gaat met de geleidelijke vervaging van nationale grenzen en de uitholling van de soevereiniteit van natiestaten (Meltzer, 2015). Almarzouqi et al. (2022) en Shen et al. (2021) verklaren dit doordat globale platformen zorgen voor een stijging van internationale activiteiten tussen landen en voor een stijging van communicatie tussen burgers onderling. De drempels om elkaar te ontmoeten is namelijk lager door deze soort van internettoepassingen. Door deze vervaging van grenzen, is het niet ondenkbaar dat er verwarring kan zijn over wie er de verantwoordelijkheid draagt over dit soort virtuele werelden. Zeker wanneer er wordt gekeken naar hoe Europa vandaag de dag er maar niet in slaagt om de technologiereuzen zoals Facebook of Amazon in bedwang te houden (Van Haver & Serrure, 2022). Momenteel is er geen duidelijke strategie in de wetgeving rond dataverzameling (Bremmer, 2022). Volgens Bremmer (2022) zal geen enkele overheid in de nabije toekomst de gigantische winsten en de enorme invloed van de technologiereuzen bestrijden. Volgens Rosenberg (2022) staan we, als maatschappij, aan de vooravond van een nieuwe grote technologische overgang. De wereld zit in een shift waarbij de huidige sociale media platformen verschuiven naar immersieve media, zoals het metaversum van morgen (Rosenberg, 2022). Echter, omdat deze digitale wereld nog in de vroege ontwikkelingsfase verkeert, en de ontwikkelingsregels nog niet perfect zijn, is het noodzakelijk om de uitdagingen aan te gaan op vlak van toezicht (Liu et al., 2022).

Het doel van dit onderzoek is om een analyse te maken van de relaties tussen het sociale aspect van het metaversum en de beginselen van privacy en de regulering hiervan. Door het

systematisch analyseren van de bestaande literatuur, tracht dit onderzoek een antwoord te bieden op de onderzoeksvraag:

Welke partijen zijn in staat om privacy te waarborgen binnen het metaversum?

Het onderzoek probeert de huidige problemen binnen dit gebied te verduidelijken, waardoor de voornaamste risico's van metaverses op de persoonlijke levenssfeer van de eindgebruiker, in kaart worden gebracht.

2 Methodologie

Dit onderzoek kadert zich binnen het onderzoeksdomein rond de impact van technologische ontwikkelingen op de veiligheid van een gemeenschap. Om tot een actueel en maatschappelijk relevant onderwerp te komen, werd gestart met een verkennend onderzoek naar de technologieën waar grote verwachtingen rond heersen. Hierbij kwam aan het licht dat het er veel aandacht wordt gespendeerd aan het metaversum en dat er tegelijkertijd zorgen bestaan rond de rol die het zal spelen op vlak van digitale privacy (Van der Haegen et al., 2022).

Dit onderzoek tracht de bestaande literatuur te analyseren met als doel het metaversum te beschrijven en de maatschappelijke relevantie ervan te kaderen. Binnen het onderzoeksdomein werd de volgende onderzoeksvraag opgesteld: '*Welke partijen zijn in staat om privacy te waarborgen binnen het metaversum?*'. Om deze onderzoeksvraag te beantwoorden, werd gekozen voor een systematisch literatuuronderzoek of *Systematic Literature Review* (SLR). Een SLR kan kortweg worden omschreven als een studie rond de reeds bestaande studies. Deze vorm van literatuuronderzoek tracht empirisch bewijsmateriaal te verzamelen dat voldoet aan vooraf gespecificeerde geschiktheidscriteria om een specifieke onderzoeksvraag te beantwoorden (Liberati et al., 2009). Deze manier van literatuuranalyse, dient om de validiteit van het onderzoek te kunnen waarborgen. Hoewel het volgens De Pelsmacker en Van Kenhove (2014) nagenoeg onmogelijk is om in wetenschappelijk onderzoek alle regels te volgen, is het toch nuttig om deze regels naar voor te schuiven als norm, een ideaal waarmee elke onderzoeksprocedure moet worden vergeleken. Mede door het volgen van een logisch wetenschappelijk kader, behoudt wetenschappelijk onderzoek zijn drie belangrijke kenmerken: theorievorming en modelbouw, validiteit en betrouwbaarheid (De Pelsmacker & Van Kenhove, 2014).

Na het opstellen van de maatschappelijk relevante onderzoeksvraag, worden vijf fases doorlopen om het onderzoek zo zorgvuldig mogelijk uit te voeren.

1. Onderzoeksvragen identificeren
2. Relevante studies zoeken
3. Selecteren van studies
4. In kaart brengen van gegevens
5. Verzamelen, samenvatten en rapporteren van resultaten

In de eerste fase worden trefwoorden en synoniemen geformuleerd die de basis vormen om in de volgende fases relevante studies op te zoeken via de wetenschappelijke databank *Web of Science.* Aangezien het gaat over een Engelstalige databank, zijn de zoektermen in het Engels geformuleerd. Volgende zoektermen zijn gebruikt om de huidige literatuur op te sporen: *'Metaverse', 'Privacy' en 'Regulation'*.
Hiernaast worden volgende synoniemen gebruikt om het aantal zoekresultaten uit te breiden: *virtual world, digital society, digital privacy, security, governance, E-governance, security provision.*

De *search string* ziet er als het volgt uit:

(Metaverse OR virtual world OR digital society) AND (Privacy OR Digital privacy) AND (Regulation OR Security OR Governance OR E-governance OR security provision)

De tweede fase draait erom de juiste publicaties te vinden en bij te houden. Hierbij worden criteria opgesteld die de zoekresultaten verder verfijnen met als doel het minimaliseren van bias, om zo betrouwbare bevindingen op te leveren waaruit conclusies kunnen worden getrokken en beslissingen kunnen worden genomen (Liberati et al., 2009). Er wordt in dit onderzoek voornamelijk gekeken naar de publicaties die zowel met het metaversum als met één van de andere eerder opgesomde zoektermen te maken hebben. Bijkomend worden de onderzoeken die niet publiek toegankelijk zijn, via de database, eruit gefilterd. Het opzoeken en filteren van de publicaties leverde 55 verschillende secundaire bronnen op. De Pelsmacker en Van Kenhove (2014) beschrijven dit soort bronnen als bestaande gegevens die door de eigen onderneming of door anderen zijn samengesteld, maar niet in de eerste plaats om een welomschreven probleem te helpen oplossen. Het is bijgevolg niet zo dat deze resultaten allemaal de gekozen probleemstelling kunnen beantwoorden. Echter zal het bundelen en correct interpreteren van deze informatie wel kunnen helpen een antwoord te formuleren op de gekozen onderzoeksvraag (De Pelsmacker & Van Kenhove, 2014). Het is dus belangrijk om in een volgende fase de studies te bestuderen die nauw aansluiten bij de essentie van het eigen onderzoek.

In de derde fase worden de relevante studies geselecteerd op basis van de abstract met als doel het genereren van betrouwbare en valide informatie die in lijn ligt met de gekozen onderzoeksvraag. Binnen dit onderzoek worden 39 verschillende publicaties overgehouden rond het metaversum, privacy en regulering. De onderzoeken die deze selectie niet haalden weken te ver af van de essentie, bespraken slechts één soort metaversum, waren verouderd of waren simpelweg niet beschikbaar. Ondanks het feit dat er wordt gekozen om enkel te zoeken op publicaties die publiek toegankelijk waren via de databank, bleken de 55 bronnen

uit fase twee niet allemaal raadpleegbaar. Hierdoor werd naast de Web of Science ook gebruik gemaakt van de databank *Researchgate*, waar enkele van de gekozen artikels publiek beschikbaar waren.

Voor de vierde stap is het belangrijk om de gegevens in kaart te brengen. Zoals voor elk onderzoek geldt, moeten systematische reviews volledig en transparant worden gerapporteerd om de lezers in staat te stellen de sterke en zwakke punten van het onderzoek te beoordelen (Liberati et al., 2009). Hiervoor wordt gebruik gemaakt van een Excel bestand waar de gekozen literatuur wordt verzameld en de inhoudelijke argumenten worden opgesomd. Dit bestand vormt de basis van het SLR en kan geraadpleegd worden in bijlage 1.

Tot slot worden de gegevens met elkaar vergeleken en gebundeld tot een literatuurstudie die het onderwerp zoveel mogelijk tracht te duiden. In deze vijfde en laatste stap worden conclusies getrokken uit de verzamelde studies die al dan niet een antwoord kunnen bieden op de vooropgestelde onderzoeksvraag. Het is volgens De Pelsmacker en Van Kenhove (2014) echter niet altijd mogelijk deze te beantwoorden wanneer een mogelijke probleemstelling nog in zijn kinderschoenen staat en er bijgevolg minder publicaties rond zijn. Hierbij kan de literatuurstudie dienen als basis voor vervolgonderzoek. Het onderzoek is hierdoor niet per se onbetrouwbaar, maar eerder exploratief. In exploratief of verkennend onderzoek wordt het terrein afgetast, waarbij wordt nagegaan welke cruciale aspecten van het onderwerp voor ander onderzoek in aanmerking komen (De Pelsmacker & Van Kenhove, 2014).

3 Het metaversum

3.1 Definitie metaversum

Wanneer er in 2022 aan Zuckerberg wordt gevraagd wat hij bedoelt met het metaversum, zal hij het hebben over de opvolger van het mobiele internet. Een metaversum stelt, volgens de CEO van Meta, eindgebruikers in staat om echt samen te zijn in een gedeelde omgeving (Legrand, 2021). Het grote verschil ten opzichte van de huidige sociale media, is dat deze virtuele wereld niet meer zal beperkt worden door de mogelijkheden van een traditioneel beeldscherm. Hierdoor speelt het metaversum meer in op de totale beleving van de eindgebruiker. Het metaversum verwijst naar een virtuele realiteit die naast de werkelijkheid bestaat (Kye et al., 2021). Het zijn meerdere virtuele werelden waarop gebruikers tegelijk met elkaar in verbinding staan en vrij kunnen interageren met virtuele objecten (Shen et al., 2021). Deze virtuele werelden vormen volgens Antonio Chavez-Aguayo (2009) een metafoor voor het echte universum, waaruit de term 'metaverse' voortvloeit. Het komt van de samentrekking tussen de volgende Engelse woorden: '*metaphors'* en '*universes'*. Deze term verwijst naar een gedigitaliseerde aarde die als nieuwe wereld tot uitdrukking komt via digitale media zoals smartphones en het internet (Kye et al., 2021). Metaverses worden, volgens Shen et al. (2021) ondersteund door technologieën die de gebruikers ervan trachten onder te dompelen in een virtuele realiteit met behulp van waargenomen immersie. Als eerste stap van de creatie van het metaversum stelde Meta, hun metaversum *'Horizon Worlds'* voor. Dit is een virtuele wereld of beter een metaversum, toegankelijk voor iedereen met een VR-bril, waarin men zich via een avatar kan voortbewegen (Verrycken, 2022).

Binnen een metaversum worden de gebruikers digitaal voorgesteld door een avatar (Antonio Chavez-Aguayo, 2009). De letterlijke betekenis van een avatar is een alter ego dat naar de aarde is afgedaald (Park & Kim, 2022). Binnen de context van het metaversum gaat het echter om de gebruiker die afdaalt naar de digitale wereld (Park & Kim, 2022). Het is via een avatar dat de gebruikers van het metaversum kunnen deelnemen aan sociale, economische en culturele activiteiten binnen de metaversumwereld (Kye et al., 2021). De avatar wordt, in het metaversum, geïdentificeerd met iemands ware identiteit (Kye et al., 2021). Dit alter ego vormt als het ware een eigen digitale persoonlijkheid waarvan men zelf kan kiezen hoe het eruit zal zien. Idealiter zou deze avatar volgens Park & Kim (2022), geleidelijk veranderen tot ideale vorm die het ego weerspiegelt. De avatar hoeft er bijgevolg niet steeds hetzelfde uit te zien. Deze kan in een digitale wereld, naar believen van de gebruiker, van huidskleur, geslacht of gedaante veranderen (Antonio Chavez-Aguayo, 2009; Park & Kim, 2022). Men hoeft bijgevolg geen bivakmuts te dragen om een anoniem bestaan te leiden binnen het metaversum. Op vlak van onderling contact tussen gebruikers onderling, hoeft er niet per se

een link te zijn met de fysieke eindgebruiker. Dit is een belangrijk aspect wat implicaties heeft op vlak van gebruikersinteractie, anonimiteit en privacy.

Binnen de literatuur wordt vaak gesproken over het metaversum als deel van meerdere metaverses (Corballis & Soar, 2022; Dhelim et al., 2022; Kye et al., 2021; Romansky & Noninska, 2020). Dit komt doordat er op dit moment, in tegenstelling tot het werkelijke universum, meerdere metaverses zijn (Dhelim et al., 2022). Dhelim et al. (2022) schatten de kans hoog in dat er meerdere gefragmenteerde metaversums zullen komen in plaats van één gedistribueerd universeel metaversum. Het is mede door technologische verschillen en het geïsoleerde karakter van de huidige metaverses, dat het uiterst moeilijk is om deze onafhankelijke metaverses onderling te verbinden tot een universeel metaversum (Dhelim et al., 2022). Van der Haegen et al. (2022) geloven wel dat deze verschillende metaversums ooit met elkaar in verbinding zullen staan. Het feit dat er op dit moment meerdere metaverses zijn, lijkt op het eerste zicht een banaal verschil maar dit heeft implicaties op de regelgeving (zie infra, ‘6.1.5’).

3.2 Transitie van het internet

Het metaversum krijgt soms de naam Web 3.0, als zogenaamde opvolger van het mobiele internet (Van der Haegen et al., 2022). Deze vaak geclaimde term, wijst op een grote verandering van het Web door revolutionaire technologie. Omwille van de recente economische en technologische veranderingen die de wereld de laatste decennia heeft gekend, zijn de principes die het internet beheersen onderhevig aan grote veranderingen als gevolg van nieuw gebruik, nieuwe behoeften en nieuwe trends (Benhaddi, 2017). Sinds het Web 1.0 heeft het internet een enorme transitie gemaakt, naar wat men noemt het Web 3.0. Vroeger was het internet een eenzijdig communicatiekanaal met eerst enkel tekst. Dit was de reden waardoor het Web 1.0 ook het “alleen lezen web” wordt genoemd (Ankerson, 2015). Later kwamen hier respectievelijk eerst foto’s en daarna video’s bij (Ankerson, 2015).

De mogelijkheid van eindgebruikers om zelf content te creëren luidde het Web 2.0 tijdperk in. Ozcinar et al. (2020) definiëren het Web 2.0 als een meer gepersonaliseerde, communicatieve vorm van het zogenaamde *Wereldwijde Web* (WWW). Hierbij staan participatie, verbinding, samenwerking, het delen van informatie en het delen van ideeën tussen gebruikers centraal. De transitie van Web 1.0 naar Web 2.0, vormde het internet om tot een tweezijdig communicatiemiddel. Aangezien Web 2.0 verder gaat dan zijn oudere versies, wordt dit ook wel het "lees-schrijf-web" genoemd. Hierbij stelt de raadpleegbare inhoud het grote publiek in staat om actief bij te dragen aan het WWW en de inhoud ervan vorm te geven (Ozcinar et al., 2020). Door de transitie ontstonden er nieuwe interfaces die

eindgebruikers met weinig technische kennis in staat stelden om op een eenvoudige manier te interageren met zowel de inhoud en de structuur van webpagina's als met de andere eindgebruikers (Benhaddi, 2017). Deze revolutie zorgde voor een ongeziene toestroom van persoonlijke data (Jain et al., 2021). Volgens Ankerson (2015) werden toonaangevende bedrijven tijden de Web 2.0 transitie aangezien deze het delen van door gebruikers gegenereerde inhoud hebben vergemakkelijkt.

Tot slot wordt er tegenwoordig gesproken van een nieuwe revolutie binnen het internet namelijk de transitie van Web 2.0 naar Web 3.0. Echter is dit een revolutie van het internet zonder dat er concreet gezegd kan worden wat deze inhoudt. Dit komt doordat iedereen zijn eigen technologie naar voren schuift als revolutionair en innovatief, waardoor de term Web 3.0 tot op vandaag meerdere betekenissen heeft. Thakuria & Baruah (2022) zien in deze internetrevolutie de overgang van het "lees-schrijf-web" naar het "semantische web". Het semantische web begrijpt de stukken informatie die het opslaat en is in staat om er logische verbindingen tussen te maken aan de hand van artificiële intelligentie (AI) (Thakuria & Baruah, 2022). Het is door de grote impact van AI, dat Thakuria & Baruah (2022) dit zien als de derde generatie van het internet. Volgens Benhaddi (2017) gaat de term Web 3.0 over het faciliteren van een wereld waarin mensen en computers samenwerken. Dey et al. (2022) sluiten zich hierbij aan en voegen toe dat dit zal steunen op veel technologieën tegelijk zoals: *blockchain*, artificiële intelligentie (AI), *cloud computing*, *edge computing*, enzovoort. Het is begrijpelijk dat ook op het metaversum de term Web 3.0 wordt geplakt. Dit voornamelijk om een hype te creëren die nodig is om aan te tonen dat men bezig is met het creëren van *the next big thing*. Hoewel het nog niet heel duidelijk is wat het Web 3.0 precies inhoudt, kan er wel al worden gesteld dat het internet niet stilstaat. Het internet blijft op korte tijd evolueren waardoor het alvast meer is dan een "lees-schrijf-web". Deze snelle evoluties, als gevolg van technologische innovaties, zorgen ervoor dat het ontwerpen van adequate regels een grote uitdaging vormt voor de bevoegde instanties (Renwick & Gleasure, 2021).

3.3 Benodigdheden voor het metaversum

Om verbinding te maken met een metaversum zijn er enkele vereisten. Eerst en vooral is er een toestel nodig dat kan connecteren met het metaversum. Vandaag kan dit via allerlei verschillende apparaten zoals smartphones, laptops of spelconsoles. Verder is er, net zoals bij traditionele netwerkplatformen, een goede internetverbinding vereist. Hoewel het internet door de jaren heen duidelijk evolueerde, bleef een monitor of beeldscherm een conditio sine qua non om content op het internet te kunnen waarnemen. Tot nu. Daar waar de gebruiker vroeger een toeschouwer was van het internet, zal deze in een immersieve omgeving eerder een actief deelnemer worden. Voor sommige van deze immersieve toepassingen is het

gebruik van een virtualrealitybril of een controller echter wel vereist (Van der Haegen et al., 2022). De digitale ervaring kan worden versterkt door het gebruik van een VR-bril of haptische sensoren (bv. handschoenen waarbij drukpunten worden gesimuleerd). Via een VR-bril komt de gebruiker in een andere wereld terecht (visueel), dit is essentieel wanneer het metaversum de belofte van totale immersie wilt waarmaken. Het doel van Zuckerberg is om dit decennium een miljard mensen te bereiken en honderden miljarden dollars aan digitale handel te realiseren (Legrand, 2021). Hierbij moeten de extra benodigde toestellen voor de gebruikers en de tools voor ontwikkelaars zo goedkoop mogelijk zijn (Legrand, 2021).

3.4 Mogelijkheden van het metaversum

Het metaversum draait om de virtuele ervaring van de eindgebruiker. Het grootste verschil van deze ervaring, vergeleken met traditionele sociale media, ligt bij de transitie van een 2D- naar een 3D-omgeving (Dhelim et al., 2022). De ervaring wordt voornamelijk gecreëerd door verschillende technologische innovaties zoals AR, VR en MR (Dhelim et al., 2022). Shen et al. (2021) beschrijven *Augmented Reality* als een *realtime* weergave van een door de computer gegenereerde inhoud over een scène in de echte wereld. *Virtual Reality* beschrijven Shen et al. (2021) als een computer-gesimuleerde, interactieve en immersieve virtuele omgeving waarbij gebruik wordt gemaakt van verschillende immersiemethoden, die de gebruiker isoleren van de omringende fysieke omgeving. Tot slot spreken Shen et al. (2021) over een *Mixed Reality* of gemengde werkelijkheid, dit is het dynamisch naast elkaar bestaan van virtuele en reële inhoud in dezelfde ruimte. Het metaversum zou grotendeels bestaan uit deze gemengde werkelijkheid (Dhelim et al., 2022). Een werkelijkheid die bovendien steeds meer realistischer zal worden, aangezien deze onderhevig is aan steeds betere grafische computereffecten (Antonio Chavez-Aguayo, 2009).

Uit voorgaande onderzoeken is gebleken dat virtuele ervaringen ook als echt kunnen ervaren worden, zowel de psychologische als de sociologische aspecten (de Graaf, 2016; Shen et al., 2021). Dit komt volgens de Graaf enerzijds doordat de emoties die worden ervaren tijdens virtuele belevingen echte emoties zijn (2016). Zo kan men oprecht plezier hebben, gefrustreerd of opgewonden zijn en zelfs gevoelens zoals verliefdheid ontwikkelen (de Graaf, 2016). Het psychologisch bedotten van de geest wordt immers mogelijk gemaakt door de immersieve technologieën (Shen et al., 2021). Immersieve technologieën trachten de geest onder te dompelen door de visuele, auditieve, haptische en bewegingswerkelijkheid te simuleren (Shen et al., 2021). Het is een combinatie van computersoftware en -hardware die de vijf zintuigen van de mens in een gesimuleerde omgeving proberen te prikkelen (Shen et al., 2021). Volgens Rosenberg (2022) hebben immersieve technologieën zoals VR en MR het potentieel om het leven magisch te maken.

Volgens de Graaf steunen de gevoelens op het concept van *suspended disbelief*. Suspended disbelief verwijst naar situaties waarin personen weten dat iets 'niet echt' is, maar omdat er gevoelens zijn van plezier en genot weigeren toe te geven aan het zogenaamde 'gevoel van ongeloof' (de Graaf, 2016). De immersieve technologieën waar het metaversum op steunt zijn speciaal ontworpen om de zintuigen te misleiden en de grens tussen authentieke en 'namaak' ervaringen opzettelijk te doen vervagen. In het verlengde hiervan verwacht Rosenberg (2022) dat het misbruik van sociale media aanzienlijk zal worden versterkt.

Volgens Van der Haegen et al. (2022) zijn er ontelbaar veel mogelijke toepassingen met voordelen voor eindgebruikers binnen het metaversum. Het metaversum, waar in theorie alles mogelijk is, heeft veelbelovende toepassingen zoals virtueel onderwijs, virtuele werkplekken, virtuele concerten en gamen (Van der Haegen et al., 2022; Dhelim et al., 2022; Kye et al., 2021). De voordelen voor de eindgebruiker liggen in lijn met die van sociale media, met als grootste verschil de digitale ervaring. Doordat deze virtuele bijeenkomsten in *realtime* zijn, kan het metaversum het meest sociale platform worden. Sociale interactie met andere gebruikers is volgens de Graaf (2016) de grootste drijfveer voor het gebruik van het metaversum. In essentie komt het neer op het onderhouden van een digitaal sociaal netwerk, waarbij fysieke grenzen en drempels vervagen door het samenbrengen van verschillende mensen uit verschillende geografische regio's (Jain et al., 2021). Bijkomend helpen sociale platformen bij het vinden van groepen waarbij individuen zich kunnen aansluiten (Jain et al., 2021). Binnen deze groepen kunnen gebruikers met dezelfde gemeenschappelijke interesses en sympathieën elkaar ontmoeten en hun opvattingen delen. Verder heeft het metaversum ook de kracht om mensen met een lichamelijke handicap zich te laten bewegen zoals mensen zonder handicap (Zhao et al., 2021). Dit zou volgens Jain et al. (2021) bijdragen tot een open samenleving. Een open samenleving waar er volgens Park & Kim (2022) mogelijks minder sociale discriminatie zou heersen, mede doordat avatars naar believen van huidskleur en geslacht kunnen veranderen. Easton (2019) stelt evenzeer dat een verhoging van de mate waarop burgers onderling kunnen connecteren, een impact heeft op het sociale weefsel van de hele samenleving. Dit zal volgens Easton (2019) verdere vragen met zich meebrengen rond de essentie van een controleorgaan zoals de politie.

Naast de mogelijkheden en voordelen van het metaversum voor de eindgebruiker zijn er ook veel mogelijkheden voor bedrijven. Als de voorspellingen van Gartner uitkomen, en er in 2026 minstens één uur per dag in metaverses zal worden geleefd, vormt het metaversum een enorme commerciële kans voor bedrijven. Het platform dat de meeste gebruikers aantrekt, heeft de mogelijkheid om veel inkomsten te genereren. Logischerwijs gaat dit hand

in hand met het gekozen businessmodel (zie infra, ‘3.7’). Niettemin zijn er naast het ontwikkelen van het meest succesvolle metaversum, nog andere mogelijkheden voor bedrijven. Zo is NVIDIA bezig met het creëren van het NVIDIA omniverse-platform. Dit is een virtuele fabriek binnen een afgesloten metaversum met als doel echte producten te testen (Liu et al., 2022). De gegevens kunnen worden gesynchroniseerd met de echte fabriek, wat de productie minder kan belasten, de kosten kan drukken en de efficiëntie kan verhogen (Liu et al., 2022). Tot slot steeg sinds de coronapandemie de vraag naar virtuele toepassingen (Van der Haegen et al., 2022). Het is volgens Van der Haegen et al. (2022) slechts een kwestie van tijd vooraleer er via het metaversum zal worden vergaderd en samengewerkt worden. Dit met behulp van virtuele communicatieplatformen zoals Meta's ‘*Horizon Workrooms*’ of Microsofts ‘*Microsoft Mesh’*. Echter stellen Dhelim et al. (2022) dat om de mogelijkheden van een virtueel universum te benutten, de metaverse-toepassingen aan bepaalde eisen moeten voldoen, zoals een ultrahoge internetsnelheid, connectiviteit tussen toepassingen en veiligheids- en privacy kwesties. Technologische innovaties, zoals bijvoorbeeld het uitrollen van een 5G-netwerk, kunnen een oplossing bieden voor deze eerste uitdagingen (Rosenberg, 2022). Het oplossen van privacy kwesties is echter nog een ander vraagstuk.

3.5 Uitdagingen van het metaversum

3.5.1 Uitdagingen op sociaal vlak

De mogelijkheden van metaverses brengen naast voordelen ook enkele uitdagingen met zich mee. Zoals eerder aangehaald kunnen gebruikers in het metaversum deelnemen aan sociale activiteiten. Hierdoor zijn enkele sociale uitdagingen van sociale netwerksites ook van toepassing op de digitale wereld. Een voorbeeld van deze uitdagingen, is de asociale kant van sociale media. Volgens de Graaf (2016) is het bijna paradoxaal dat we Facebook een sociaal netwerk noemen, dit omdat het platform zijn gebruikers niet in staat stelt om elkaar te ontmoeten en als groep of gemeenschap met elkaar om te gaan. Jain et al. (2021) verklaren dat sociale media de band tussen gebruikers zeker heeft verbeterd, maar omgekeerd heeft het ook de sociale interactie in het echte leven verhinderd. Mensen vinden het gemakkelijker om de commentaren te volgen van mensen die ze kennen, in plaats van hen persoonlijk op te zoeken of te bellen (Jain et al., 2021). Reeds in 2011 wisten de beleidsmakers van metaverses al de sociale moeilijkheden die deze platformen zouden ondervinden. De belangrijkste sociale problemen waren toen al: sociale isolatie, zich eenzaam voelen, passiviteit, gebrek aan vrienden en een adequaat persoonlijk sociaal netwerk (de Graaf, 2016).

De digitalisering bracht volgens Easton (2019) een fundamentele wijziging teweeg bij de relaties tussen individuen en organisaties. Dat relaties tussen mensen onderling kunnen wijzigen door technologie, wordt bevestigd door Kye et al. (2021). Hierdoor lijkt het aannemelijk dat de opkomst van een technologie zoals het metaversum, in staat is om deze fundamentele wijzigingen verdere door te trekken. Door het toepassen van immersieve technologieën zou de geest van de gebruikers namelijk worden ondergedompeld, waardoor de ervaringen binnen de digitale wereld als echt worden ervaren (zie supra, ‘3.3’). Dhelim et al. (2022) waarschuwen dat gebruikers problemen kunnen ondervinden om de realiteit te scheiden van het virtuele universum. Naarmate het onderscheid tussen de virtuele en de echte wereld vervaagt, kunnen gebruikers verward geraken over hun persoonlijke identiteit (Kye et al., 2021). Dit gevaar bestaat wanneer de bezoekers te hard opgaan in hun relaties binnen de virtuele realiteit of voldaan zijn met enkel deze virtuele relaties. Uit het onderzoek van Kye et al. (2021) blijkt dat wanneer de behoefte aan intimiteit reeds werd voldaan in de virtuele wereld, intieme relaties in de ‘echte wereld’ verwaarloosd worden. Nochtans kan het belang van een sociaal netwerk niet genoeg worden benadrukt. Er is volgens de Graaf (2016) bewijs dat eenzame, geïsoleerde mensen meer gezondheidsproblemen hebben dan actieve personen. Het kunnen onderhouden van relaties is bijgevolg geen keuze maar eerder een must. De Graaf (2016) stelt dat er grote uitdagingen liggen rond het versterken van deze sociale netwerken, in het bijzonder met alle bevolkingsgroepen in het achterhoofd.

Deze problemen omtrent sociale exclusie zijn bijgevolg belangrijk om mee te nemen bij de ontwikkeling van het volgende sociale platform zoals het metaversum.

3.5.2 Uitdagingen rond leeftijdsgroepen

De Graaf (2016) ziet virtuele sociale netwerken niet als sociaal, aanzien ze minder worden gebruikt door oudere leeftijdsgroepen. Zo stelde onderzoeksbureau Omnicore in 2022 vast dat de groep 65-plussers, de kleinst vertegenwoordigde groep op was Facebook. Deze vertegenwoordigen slechts 4,8% van de totale populatie op Facebook (Omnicore, 2022). Huidige bevindingen over internetgebruik en gebruik van sociale media, geven aan dat ouderen minder frequente gebruikers zijn ten opzichte van de jongere generatie (Blieszner et al., 2019). Dit valt volgens de Graaf deels te verklaren door het feit dat leeftijd een bepalend kenmerk is geworden op vlak van online aanwezigheid (2016). Terwijl leeftijd volgens Almarzouqi et al. (2022) op zijn beurt een impact heeft op de waargenomen compatibiliteit van de technologie. Almarzouqi et al. (2022) beschrijven de waargenomen compatibiliteit als het niveau waarop gebruikers vinden dat technologie aansluit bij hun levensstandaard, noden en behoeften. Het is de mate waarin een technologische innovatie aansluit bij de voorkeuren van de bezoeker, waardoor het invloed heeft op de adoptie van de technologie (Almarzouqi et al., 2022). Het probleem is niet de leeftijd van de oudere persoon maar eerder de manier waarop IT-oplossingen worden ontworpen en gepresenteerd. In het geval van adoptie van de metaverse door ouderen, is het dus belangrijk te onderzoeken hoe deze technologie compatibel kan worden gemaakt met deze leeftijdsgroep. Een mismatch tussen deze bevolkingsgroep en het metaversum kan leiden tot het verlies aan mogelijkheden om relaties te onderhouden (Yu et al., 2018).

Naast de technologische moeilijkheden is er nog een reden die een belemmering vormt voor ouderen om toe te treden tot de huidige sociale netwerken. Zoals eerder gezegd zijn dit soort sociale-netwerken geen ontmoetingsplaatsen, maar eerder een plaats waar contacten worden onderhouden met reeds bestaande kennissen. Helaas is een inherente trieste eigenschap van ouder worden, het verliezen van vrienden en de vermindering in mogelijkheden om nieuwe te maken (Blieszner et al., 2019). Aanvullend onderzoek toont aan dat oudere Facebookgebruikers kleinere aantallen online vrienden hebben, maar een groter aandeel daadwerkelijke vrienden hebben dan jongere Facebookgebruikers (Blieszner et al., 2019; Yu et al., 2018).

3.5.3 Uitdagingen rond gebruikersveiligheid

Op vlak van gebruikersveiligheid zijn er ook uitdagingen voor het metaversum. De reeds gevestigde sociale mediakanalen hebben nog steeds moeite om een veilige online

omgeving aan te bieden en hun gebruikers te beschermen tegen online bedreigingen, seksuele intimidatie, cyberpesten en identiteitsdiefstal (Dhelim et al., 2022). Online intimidatie is een gekend fenomeen binnen grote groepen mensen. Het metaversum zal een grote groep mensen bij elkaar brengen, aangezien de virtuele ontmoetingsplaatsen binnen het metaversum worden ontwikkeld met de gedachte om mensen gemakkelijk in contact te brengen (zie supra, '3.4'). Hierdoor is het enerzijds gemakkelijker om vrienden te maken via sociale netwerkplatformen, anderzijds vereenvoudigd dit ook de mogelijkheid tot intimidatie (Jain et al., 2021). De grote mate van vrijheid en de anonimiteit die dit soort platformen bieden, is hierbij een voordeel voor mensen met slechte intenties. Dit komt volgens Kye et al. (2021) doordat de mogelijkheid tot anonimiteit binnen het metaversum, ervoor zorgt dat het schuldgevoel van mensen over misdaden verminderd. Volgens Jain et al. (2021) is dit een constant probleem geweest voor bezoekers van sociale media. Onder een digitale alias, zoals een vals profiel of een virtuele avatar, is het gemakkelijk om anoniem te blijven. Vroeger werd iemand alleen *face-to-face* gepest, vandaag de dag kan echter iedereen anoniem iemand online pesten (Jain et al., 2021). Een nadeel van het metaversum ten opzichte van de conventionele sociale mediakanalen is dat de interactiviteit van de virtuele 3D-wereld, online intimidatie verergerd. Deze intimidatie kan zich volgens Zhao et al. (2021) voordoen in de vorm van kwaadaardig avatar-gedrag zoals pesterijen (Zhao et al., 2021). Dit is volgens Dhelim et al. (2022) te wijten doordat potentiële daders via het metaversum toegang krijgen tot meer gevoelige informatie die ze vandaag de dag niet kunnen krijgen via traditionele sociale netwerken. Bovendien kunnen er zich volgens Zhao et al. (2021) onvermijdelijk scenario's voordoen waardoor sommige mensen zich ongepast voelen, louter door culturele verschillen.

Digitale interactie is één van de extra toegevoegde waardes van een 3D-metaversum ten opzichte van een 2D-sociaal medium zoals Facebook of Twitter. Hierdoor zijn er ook mogelijke problemen die kunnen optreden die niet, of slechts in mindere mate, kunnen voorvallen binnen de conventionele platformen. Eén van deze bedreigingen valt onder de noemer van cyber-seksueel geweld. Cyber-seksueel geweld verwijst naar een vorm van schadelijk seksueel agressief gedrag dat wordt gepleegd met behulp van digitale technologieën (Cripps & Stermac, 2018). Volgens Cripps & Stermac (2018) is dit een ruim begrip dat kan bestaan uit niet-vrijwillige pornografie en andere op beelden gebaseerde seksuele uitbuiting, online seksuele aanranding of intimidatie, cyberstalking en online op gender gebaseerde haatzaaiende taal. Hoewel dit volgens Dhelim et al. (2022) een probleem is dat altijd heeft bestaan op sociale netwerken zou het metaversum hier een extra dimensie aan toevoegen. Voornamelijk op vlak van digitale seksuele aanranding. Door de immersieve technologieën waarop het metaversum steunt die de geest trachten onder te dompelen, komen deze emoties harder binnen bij de gebruiker (Shen et al., 2021).

Gebruikers van het metaversum die seksuele intimidatie ervaren in het virtuele universum, kunnen last krijgen van psychologische effecten als gevolg van dergelijke virtuele intimidatie (Dhelim et al., 2022). Cripps & Stermac (2018) stellen dat de gevolgen van online slachtofferschap een zware en langdurige impact kunnen hebben op het verdere emotionele welzijn van de getroffene. Deze gevolgen zijn onder andere: depressie, angst, posttraumatische stress symptomen, drugsmisbruik, vijandigheid, angst, pijn, schaamte en afwijzing (Cripps & Stermac, 2018). Hierdoor vormt digitale seksuele intimidatie één van de meest ernstige bedreigingen voor het metaversum met een mogelijks grote impact op de fysieke maatschappij (Cripps & Stermac, 2018; Dhelim et al., 2022).

3.5.4 Uitdagingen rond beveiliging

Volgens Van der Haegen et al. (2022) zijn de risico's rond veiligheid die het metaversum met zich meebrengt, vergelijkbaar met die van het huidige internet. Naast de beveiliging van het platform zelf zijn er risico's verbonden aan samenwerkingen met derde partijen. Van het metaversum wordt verwacht dat het, net zoals sociale media platformen, zal zorgen voor een stijging van persoonsgegevens (zie infra, 4. Big data'). Hierdoor kan het een geweldig reclamemedium worden voor marketeers (Jain et al., 2021). Wanneer deze derden de veiligheidskwesties van het platform niet serieus nemen stelt het platform zich volgens Jain et al. (2021) kwetsbaar op voor verschillende bedreigingen. Gekende bedreigingen voor sociale media zijn misdaden zoals het onderscheppen van gegevens, het bespioneren van de persoonlijke levenssfeer, inbreuken op het auteursrecht en informatiefraude (Jain et al., 2021). Bovendien riskeren deze platformen hun vertrouwelijke gegevens in gevaar te brengen, wat kan leiden tot vertrouwensbreuk met de eindgebruikers (Jain et al., 2021).

3.5.5 Uitdagingen rond gezondheid

Zoals eerder aangehaald heersen er problemen rond de sociale exclusie. Hoewel dit een sociaal aspect is, stelt de Graaf dat het kan zorgen voor psychische gezondheidsproblemen (2016). Dit kan zijn doordat eindgebruikers zich niet op de juiste manier kunnen aanpassen aan de virtuele realiteit (Kye et al., 2021), of doordat de technische toetredingsdrempels van nieuwe technologieën te ingewikkeld zijn voor bepaalde groepen (Blieszner et al., 2019). Deze foute manier van omgaan met deze technologie kan leiden tot eenzaamheid. Mensen hebben voornamelijk last van eenzaamheid wanneer ze zich niet langer in staat voelen deel te nemen aan de sociale omgeving (de Graaf, 2016). Wanneer deze eenzaten in de problemen komen, kunnen zij volgens de Graaf (2016) alleen nog maar terugvallen op de overheid. Overheden kunnen hun bijstaan door het faciliteren van professionele psychische zorgverlening.

Vandaag de dag is er geweten dat overmatig gebruik van technologie zoals het internet of online gamen kan leiden tot verslaving (Dhelim et al., 2022). Jain et al. (2021) voegen hieraan toe dat uit de huidige beschikbare gegevens blijkt dat sociale netwerken zelfs verslavender zijn dan sigaretten en alcohol. Volgens Dhelim et al. (2022) zou het metaversum hierop geen uitzondering vormen. Het risico op internetverslaving zou vanwege de immersieve ervaring zelfs met 44 procent kunnen verhogen in vergelijking met traditionele toegangsapparaten zoals de smartphone of laptop (Dhelim et al., 2022; Ning et al., 2018). Het is triest te beseffen dat het verslavende aspect van deze media bewust zit ingebakken in de strategie. Klokkenluider Frances Haugen kwam hiermee in 2021 naar buiten. De voormalige productmanager bij Facebook claimde dat het sociale netwerk doelbewust zijn algoritmes ontwikkeld zodat mensen langer op het platform zouden spenderen (Verrycken, 2021). Hierdoor werkt het de verslavingsgevoeligheid van de eindgebruikers in de hand. Omwille van het verslavende karakter voelen mensen zich vaak leeg en depressief wanneer ze een hele dag hun sociale media-account niet checken (Jain et al., 2021). Dat het vaak de polariserende berichten zijn die de eindgebruikers het langst op facebook weten te houden, speelt ook niet in de kaart van deze sociale platformen. Volgens Haugen onderhoudt Facebook hierdoor dagelijks haat en verdeeldheid (Verrycken, 2021). Haugen versterkte haar claims door het lekken van interne documenten waaruit bleek dat Facebook kennis heeft over de reële schade die het kan aanrichten bij gebruikers én dat dit bedrijf er weinig aan doet om dit te verhelpen (Verrycken, 2022). Volgens Verrycken (2022) is het omwille van deze problemen van sociale media platformen, dat Haugen sceptisch is ten opzichte van het metaversum.

Naast het mentale aspect zijn er ook bedreigingen voor de fysieke gezondheid. Zo is het niet ondenkbaar dat men in de toekomst veel tijd zou gaan spenderen in het metaversum. Vanwege de haast eindeloze mogelijkheden van het metaversum (zie supra, ‘3.4’). Lange uren doorbrengen met VR-helmen of -brillen, die zich op enkele centimeters van de ogen van gebruikers bevinden, zal volgens Dhelim et al. (2022) ernstige oogproblemen veroorzaken. Naast de gekende impact van intensieve lichtinval op onze ogen, werd aangetoond dat dat kinderen die 20 minuten lang een VR-bril gebruikten, hier op korte termijn reeds last van hadden (Dhelim et al., 2022; Yamada-Rice et al., 2017). Deze hadden moeite met het onderscheiden van de afstanden van objecten in de werkelijkheid als gevolg van de digitale beelden (Dhelim et al., 2022; Yamada-Rice et al., 2017).

3.5.6 Uitdaging rond ecologische voetafdruk

Veel avatars samenbrengen op éénzelfde virtuele plek vergt veel grafische rekenkracht van verschillende processoren. Hierdoor zou de virtuele wereld een ongelofelijke ecologische

voetafdruk achterlaten op de echte planeet (Van Der Haegen et al., (2022). Dit komt doordat het opslaan van al deze gegevens van het metaversum gebeurt in gigantische energieverslindende datacenters (Van Der Haegen et al., (2022).

Samenvattend kan worden gesteld dat het metaversum nog veel uitdagingen heeft op vlak van sociale aspecten zoals verbondenheid, gebruikersveiligheid, beveiliging, gezondheid en ecologie. Daarbovenop dienen er volgens Van der Haegen et al. (2022) nog moeilijke beslissingen te worden genomen met betrekking tot ethische kwesties en interacties tussen het metaversum en de echte wereld. Wanneer alle metaversums met elkaar verbonden zullen worden, zullen de vragen rijzen over wie er de regels zal bepalen en wie er de orde zal handhaven (Van Der Haegen et al., (2022). Kye et al. (2021) verwachten dat naarmate virtuele werelden populairder zullen worden, de mate van vrijheidsgevoel zal toenemen binnen het metaversum. De vrees bestaat dat er nieuwe misdrijven zullen opduiken die wreder en geraffineerder zijn dan in de echte wereld (Kye et al., 2021). De mogelijkheid van nieuwe misdaden, waarvan men deze vandaag de dag niet kan inbeelden, creëert een noodzaak van een flexibel en snel aanpasbaar regelgevend orgaan. Aangezien er enorm veel uitdagingen zijn voor het metaversum, werd binnen dit onderzoek gekozen om zich vooral te richten op de problemen omtrent de privacy. Dit onderwerp vormt een eigen hoofdstuk, waar het uitvoerig zal worden besproken (zie infra, ‘5 Privacy’). Desondanks kan het maatschappelijk belang van bovenstaande problemen niet genoeg worden benadrukt. Vervolgonderzoek omtrent de regulering hiervan, dringt zich op.

3.6 De blockchain

Het metaversum zal naar de verwachtingen van Renwick & Gleasure (2021) en Rosenberg (2022) een eigen economie hebben waarbij digitale munten een grote rol zullen spelen. Deze munten zijn niet nieuw en zijn tegenwoordig erg populair bij speculanten die het zien als een vorm van belegging (Corballis & Soar, 2022). Het meest gekende voorbeeld hiervan is Bitcoin, een munt gebaseerd op de blockchain technologie die in dit hoofdstuk zal worden uitgelegd. De blockchaintechnologie heeft volgens Dey et al. (2022) meer potentieel dan alleen maar het fundament te vormen voor digitale munten. Het zou mogelijks aan de basis kunnen liggen van een gedecentraliseerd internet waarbij bezittingen, zoals data, terug worden gegeven aan ieder individu (Dey et al., 2022) (zie infra, '6.1.5.1').

3.6.1.1 Bitcoin

Reeds in 2008 stelde een anonieme onderzoeker of groep onderzoekers, onder de naam Nakamoto, een systeem voor dat elektronische transacties mogelijk maakt dat, in tegenstelling tot de gangbare betalingssystemen, niet berust op vertrouwen. De paper "*Bitcoin: A Peer-to-Peer Electronic Cash System",* heeft tot op vandaag nog steeds een grote impact. De paper beschrijft de blockchain-technologie die vandaag de dag bekend is vanwege zijn rol in het mogelijk maken van digitale munten zoals Bitcoin (Renwick & Gleasure, 2021). Het is een alternatief voor de manier waarop betalingen traditioneel verlopen, namelijk het op vertrouwen gebaseerde model. Bij dit laatstgenoemde model verlopen transacties via een derde partij zoals de bank of een notaris. Dit systeem werkt goed genoeg voor de meeste transacties, maar lijdt desondanks onder de inherente zwakke punten, namelijk vertrouwen in deze tussenpersonen (Nakamoto, 2009). Het vertrouwen van de consumenten in de bank was op het moment dat deze paper werd gepubliceerd extreem laag mede door de huizencrisis die in 2007 zorgde voor een globale economische crisis (Demets, 2008). Volgens Nakamoto was er een hoge nood aan een elektronisch betalingssysteem dat gebaseerd is op cryptografisch bewijs in plaats van vertrouwen, waardoor twee bereidwillige partijen rechtstreeks met elkaar handel kunnen voeren (Nakamoto, 2009). Door de blockchain technologie is er geen tussenkomst van institutionele bemiddelaars vereist bij het overmaken van geld van de ene entiteit naar de andere (Dey et al., 2022). Volgens Van der Haegen et al. (2022) zal de hele digitale economie worden gedragen door digitale munten met een link naar de werkelijke economie. Een of meerdere digitale munten, zoals de Bitcoin, die hoogstwaarschijnlijk zijn gebaseerd op de blockchain.

3.6.1.2 Blockchain

De blockchain zelf kan het best worden omschreven als grote logboeken of registers van alle transacties tussen gebruikers, die als identieke kopieën worden bijgehouden op alle computers binnen een gedecentraliseerd, *peer-to-peer* netwerk (Renwick & Gleasure,

2021). Deze transacties worden opgeslagen in blokken code, die uniek zijn per transactie. Per transactie wordt deze code toegevoegd aan de logboeken waardoor er een ketting van blokken ontstaat, vandaar de naam *Blockchain*. De transacties worden telkens geverifieerd door individuele gebruikers die een “bewijs van werk” kunnen leveren, de zogenaamde *proof of work* (Nakamoto, 2009). Dit is een zeldzame cryptografische sleutel die alleen kan worden ontdekt door de toepassing van enorme rekenkracht (Renwick & Gleasure, 2021). De meest gangbare motivatie om deze moeilijke berekeningen te doen, is het verkrijgen van een deel van de valuta of digitale munt (Nakamoto, 2009). De transacties worden eerst uitgerekend, het *proof of work* concept, en dan opgeslagen als blok in alle logboeken. Wanneer zo een blok gewijzigd moet worden, zouden alle blokken die hierop volgen ook moeten worden aangepast (Nakamoto, 2009). Hierdoor is systeem extreem veilig en moeilijk te hacken. Volgens Nakamoto (2009) is het systeem veilig zolang de eerlijke bezitters van de virtuele logboeken meer CPU-kracht controleren dan een samenwerkende groep aanvallende knooppunten. De logboeken zijn openbare registers van transacties die zichtbaar zijn voor iedereen binnen het peer-to-peer netwerk. Deze registers hebben het potentieel om volledige gegevensreservoirs te creëren, wat op het eerste zicht niet privacy vriendelijk lijkt (Renwick & Gleasure, 2021). Echter verminderen ze de behoefte aan een gecentraliseerd toezicht en bestuur, waardoor nieuwe mogelijkheden ontstaan op vlak van anonimiteit tussen verschillende digitale en fysieke systemen (Renwick & Gleasure, 2021). Doordat controle van buitenaf niet meer nodig is, kan de privacy toch worden gehandhaafd door de informatiestroom op een andere plaats te onderbreken (Nakamoto, 2009). De publieke sleutels die personen aan een ID linken, werden reeds in 2009 door Nakamoto anoniem gehouden. Het publiek kan zien dat iemand een bedrag naar iemand anders stuurt, maar zonder de informatie die de transactie met iemand in verband brengt (Nakamoto, 2009).

3.7 Bedrijfsmodel metaversum

Zoals eerder aangehaald zijn er reeds meerdere initiatieven aan de gang rond het construeren van het metaversum. Deze platformontwikkelaars zijn uiteraard geen liefdadigheidsinstellingen en voor overheden of publieke initiatieven zijn de technologische toetredingsdrempels te hoog (Renwick & Gleasure, 2021). De uitbaters van het metaversum zullen commerciële entiteiten zijn met nood aan rendabele bedrijfsmodellen die aanzienlijke inkomsten genereren om de belangen van hun werknemers en aandeelhouders te ondersteunen (Rosenberg, 2022). Het metaversum is een platform dat naast de vereiste van enorm veel rekenkracht en opslagcapaciteit, ook het resultaat is van hoogtechnologische ontwikkeling (Van der Haegen et al., 2022). Zowel het voorzien van deze IT-infrastructuur als het bijeenbrengen van kennis, vereisen grote investeringen die zich naar verloop van tijd dienen terug te betalen (Renwick & Gleasure, 2021). De rendabiliteit van dit project hangt bijgevolg dus af van het gekozen bedrijfsmodel. Sociale netwerken zoals Facebook of zoekmachines zoals Google hanteren een bedrijfsmodel dat neerkomt op de exploitatie van privé-informatie (Jain et al., 2021). Consumentengegevens vormen de basis waarop bedrijven hun bedrijfsmodellen bouwen om te kunnen concurreren in alle sectoren die online vertegenwoordigd zijn (Bleier et al., 2020). Volgens Rosenberg (2022) verzette het publiek zich tegen het betalen van abonnementen voor toegang tot sociale platformen, waardoor de industrie koos voor gratis toegang tot hun producten en diensten in ruil voor het exporteren van data. Het aanmaken van een account op sociale netwerksites is hierdoor gratis, het geld wordt voornamelijk verdiend met de advertenties die de platformontwikkelaars op hun websites tonen (Jain et al., 2021). Bedrijven die dergelijke gegevens kunnen verzamelen, zijn een belangrijk onderdeel van de digitale economie geworden (Binns, et al., 2018).

Met Big data kunnen bedrijven gerichte aanbiedingen doen aan consumenten op basis van diens interesses (Tucker, 2012). Deze aanbiedingen zijn er in drie vormen: gerichte advertenties, aanpassing van producten en op maat gemaakte prijzen (Montes, Sand-Zantman, & Valletti, 2015). Op deze manier verzamelen deze sociale netwerksites een enorme hoeveelheid persoonlijke gegevens van de gebruiker, die aan honderden bedrijven kunnen worden verkocht zonder de expliciete toestemming van de gebruikers (Jain et al., 2021). De persoonlijke gegevens en de hieraan verbonden privacy van de gebruiker, zijn bijgevolg in gevaar (zie infra, ‘5.5’). Een mogelijke manier om dergelijke gegevenslekken tegen te gaan, is door de bezoekers te informeren over de gegevens die worden gedeeld (Jain et al., 2021).

Het wijdverspreide gebruik van persoonlijke gegevens in marketing heeft een grote markt gecreëerd voor persoonlijke informatie van consumenten. Deze industrie is naar schatting

156 miljard Amerikaanse dollars per jaar waard (Pasquale, 2014). Sommige van deze bedrijven zijn grote gegevensverzamelaars, terwijl andere zich bezighouden met het louter sorteren van consumenten (Pasquale, 2014). Het opslaan, verwerken of doorverkopen van Big data, is vandaag de dag het meest gangbare bedrijfsmodel binnen deze sector waar consumentengegevens de basis vormen waarmee bedrijven concurreren (Jain et al., 2021; Rosenberg, 2022; Tucker, 2012). Rosenberg (2022) verwacht dat deze manier om inkomsten te genereren zich ook zal voordoen bij de uitbaters van het metaversum, waar nota bene nog een heleboel extra data zullen worden verzameld en verkocht. Het verzamelen van deze data leidde enerzijds tot een hele hoop aan data en anderzijds tot vraagstukken omtrent de privacy van de eindgebruikers. Deze onderwerpen worden verder besproken in hoofdstuk 4 ‘Big data’ en hoofdstuk 5 ‘Privacy’.

4 Big data

Met de omvorming van het Web 1.0 naar het Web 2.0 werd het internet een tweezijdig communicatiekanaal. Dit impliceerde dat ook de eindgebruikers inhoud begonnen te delen, waardoor er plots een enorme groei kwam in data (zie supra, '3.2'). Verder zorgden de vooruitgang op het gebied van telecommunicatie en computertechnologie, voor een algemene kostenverlaging binnen de sector (Kshetri, 2014). Eén van deze innovaties was het digitaliseringsproces die de kosten voor het verzamelen, analyseren en opslaan van gegevens aanzienlijk heeft verlaagd (Bleier et al., 2020). De combinatie van beide oorzaken heeft volgens Ksherti (2014) en Bleier et al. (2020) geleid tot een exponentiële groei van beschikbare gegevens. Onder het motto: "hoe meer gegevens, hoe beter", ontstond zo een cultuur waarin bedrijven de data van hun eindgebruikers begonnen op te slaan (Romansky & Noninska, 2020). Het opslaan van deze gegevens en het verwerken hiervan tot bruikbare informatie, valt onder de noemer van Big data. De term Big data deed reeds in de vroege jaren negentig zijn intrede. Het is een overkoepelend begrip dat wordt gebruikt om de belangrijkste vorderingen, kansen en risico's binnen de datawetenschappen te benoemen (Casanovas et al., 2017).

Big data zijn verzamelde eenheden van informatie met een hoog volume, een hoge omloopsnelheid en/of een grote variëteit die kosteneffectieve en innovatieve vormen van informatieverwerking vereisen die een beter inzicht, een betere besluitvorming en procesautomatisering mogelijk maken. Romansky & Noninska (2020) zien Big data als een verzameling van opgeslagen informatie in zeer grote hoeveelheden, afkomstig van verschillende bronnen op verschillende plaatsen, voor verdere verwerking voor ongeacht welk doel. Het éénzijdig definiëren van Big data hoeft echter niet, aangezien de verbeterde analytische mogelijkheden de drijvende kracht vormen achter Big data (Casanovas et al., 2017). Hierdoor blijft het een actueel begrip waarvan de definitie jaarlijks wordt bijgewerkt. De snelheid waarmee big data worden verzameld en opgeslagen, blijft jaar na jaar stijgen (Amaizu et al., 2022). Een jaarlijkse stijgende trend waarvan niet meteen wordt verwacht dat deze zal stoppen (Amaizu et al., 2022). Hoewel er in het verleden niets met deze soort data kon worden gedaan, hebben technologische veranderingen het vandaag de dag mogelijk gemaakt om deze data bij te houden, te ontleden en er conclusies uit te trekken (Casanovas et al., 2017). Binnen het kader van deze masterscriptie is de nieuwe databron het metaversum. Het metaversum zal naar de verwachtingen van Amaizu et al. (2022) veel gegevens vanuit de echte wereld genereren, door middel van draagbare sensoren en andere slimme apparaten. Volgens Liu et al. (2022) zullen bedrijven proberen om hun reeds verzamelde persoonsgegevens te integreren in het toekomstige metaversum, met als doel

deze gegevens aan elkaar te koppelen. Dit kan de eerste stap vormen in het bouwen van een brug tussen de fysieke en de digitale wereld, waardoor het begrip Big data opnieuw ruimer wordt (Liu et al., 2022).

Vandaag de dag is Big data kapitaal geworden, waarbij ondernemingen het inzetten om hun processen en klantrelaties aanzienlijk te verbeteren (Gruschka et al., 2018). Meglena Kuneva, voormalig EU-commissaris, stelde reeds in 2009 dat Big data de nieuwe olie is van het internet. De waarde van informatie steeg sindsdien zienderogen terwijl de gebruikers, wiens informatie verzameld werd, dit niet altijd door hadden (Bleier et al., 2020). Dit is zo gegroeid aangezien internetgebruikers hier zelf voor gekozen hebben. Zij kozen volgens Rosenberg (2022) en Tucker (2012) massaal voor gratis diensten die worden aangeboden in ruil voor de aanvaarding van reclame.

Big data stellen organisaties in staat hun efficiëntie te verhogen door de bedrijfsvoering te verbeteren, innovatie en aanpassingsvermogen te vergemakkelijken en de toewijzing van middelen te optimaliseren (Kshetri, 2014). Echter brengt het bijhouden van deze Big data ook risico's en bedreigingen met zich mee. Zo kan deze data worden gestolen door mensen met slechte intenties (Jain et al., 2021). Bovendien kunnen deze hackers ook de vertrouwelijke informatie over hun doelwitten stelen van de partijen waaraan de data worden verkocht (Jain et al., 2021). Het maakt dus niet uit hoe veilig het dataplatform is, dit aangezien aanvalstechnieken meestal gericht zijn op de zwakste schakels (Dhelim et al., 2022; Ning et al., 2018). Volgens Ksherti (2014) is de grootse angst rond Big data gefocust op de mogelijke openbaring van gevoelige informatie, wat een duidelijke inbreuk vormt op de persoonlijke levenssfeer. Deze zorgen worden niet opgelost met de verwachtingen rond de metaverse, integendeel. Zorgen over privacy zijn volgens Renwick & Gleasure (2021) gebruikelijk bij opkomst van nieuwe technologieën, aangezien de meest recente digitale systemen vaak persoonlijke of gevoelige informatie integreren en uitwisselen.

5 Privacy

5.1 Omkadering privacy

Eerder werd geschetst hoe het verzamelen van *Big data* zonder legaal kader kan zorgen voor een inbreuk op de privacy (zie supra, '4. Big data'). Amaizu et al. (2022) stellen dat privacy een belangrijk aspect is van het leven en wijzen op de noodzaak aan privacy binnen het metaversum. Volgens Renwick & Gleasure (2021) is het moeilijk om privacy te reguleren aangezien het begrip niet eenvoudig te definiëren en nog moeilijker te meten valt. Een bijkomend nadeel is dat het ontbreken van een duidelijke definitie rond privacy voor een gebrek aan bewustzijn zorgt bij de gebruikers (Bleier et al., 2020; Romansky & Noninska, 2020). Omwille van dit maatschappelijke belang zal dit hoofdstuk het begrip privacy trachten te duiden.

Op het vlak van digitale privacy zijn er volgens Dienlin en Trepte (2014) meerdere aspecten om rekening mee te houden. Enerzijds gaat het over zeggenschap rond het verwerken en overdragen van persoonlijke informatie online, anderzijds gaat het over de autonomie op vlak van contact met anderen (Dienlin & Trepte, 2014). Verder speelt ook het aspect van de persoonlijke privacy, waarbij er controle kan worden behouden over gevoelige informatie (van Schaik et al., 2018). Ondanks dat privacy geen éénduidig begrip vormt, komt het telkens op hetzelfde neer namelijk: "*Het recht op privacy is ons recht om een domein om ons heen te houden dat alles omvat die deel van ons uitmaken, zoals ons lichaam, ons huis, onze bezittingen, onze gedachten, gevoelens, geheimen en identiteit*" (Romansky & Noninska, 2020). Privacy is een mensenrecht met internationale betekenis en het wordt erkend in verschillende internationale en regionale wetten (zie infra, '6.1.1') (Romansky & Noninska, 2020).

Thienpont & Herman (2009) beschrijven mensenrechten als rechten die iedere mens toekomen louter omdat hij of zij mens is (Thienpont & Herman, 2009). Ze gelden voor iedereen, los van afkomst, geloof, geslacht, huidskleur of overtuiging (Thienpont & Herman, 2009). Het zijn minimale voorwaarden waaraan voldaan moet zijn om op een vrije en menswaardige manier te kunnen leven (Thienpont & Herman, 2009). Mensenrechten zijn bedoeld om het individu te beschermen tegen mogelijk machtsmisbruik van de overheid (Thienpont & Herman, 2009). Juridisch gezien zijn er absolute en niet absolute mensenrechten (Gibens, 2021). Bij absolute rechten zijn er geen beperkingen toegestaan, waardoor overheden hierop geen uitzonderingen kunnen maken (Gibens, 2021). Dit is een belangrijk aspect op vlak van regulatie. Relatieve rechten kunnen wel, onder bepaalde voorwaarden, voor de uitoefening ervan aan beperkingen worden onderworpen (Gibens,

2021). Het recht op privacy is een relatief mensenrecht. Dit houdt in dat het recht op de bescherming van privégegevens vervalt wanneer er volgens de overheid gegronde redenen zijn om deze te beperken (De Raedt, 2016). Echter dienen deze redenen proportioneel te zijn, waardoor het begrip 'privacy' erg rekbaar wordt en afhangt van factoren zoals het type overheid. Men voelt aan dat proportionele redenen anders worden geïnterpreteerd in een democratisch verkozen overheid in België ten opzichte van een dictatoriaal regime als in Noord-Korea (Dobbelaere-Welvaert, 2020). Binnen de Belgische grondwet wordt ook gewag gemaakt van het recht op privacy, namelijk in artikel 22 (zie infra, '6.1.1').

Deze grondrechten en wetten zijn slechts deels gericht op de overheid, echter zijn er meerdere actoren die de bescherming van persoonsgegevens moeten waarborgen (zie infra). Volgens Romansky & Noninska (2020) dienen alle instanties rekening te houden met de bescherming van de privacy, wat rechtstreeks verband houdt met de persoonlijke levenssfeer van die personen. Hierbij gaat het over alle relaties tussen personen onderling en verhoudingen met de maatschappij, voorgesteld door overheidsinstellingen, bedrijven, openbare en particuliere organisaties en andere subjecten die persoonsgegevens verwerken (Romansky & Noninska, 2020). Bijgevolg horen ook de toekomstige uitbaters van het metaversum bij deze instanties. Reeds in 2009, vóór de Big datarevolutie, benadrukte Antonio Chavez-Aguayo het belang van privacy en anonimiteit binnen het metaversum. Ruim een decennia later heerst er nog steeds onduidelijkheid omtrent de bevoegde partijen die de privacy van deze gebruikers zullen waarborgen (Van der Haegen et al., 2022). Zeker aangezien het verhandelen van Big data, bij uitstek, het geliefkoosde bedrijfsmodel is binnen de industrie (zie supra, '3.7').

5.2 Big data en privacy

Het motto van *Big Tech* om zoveel mogelijk data te verzamelen, creëert volgens Romansky & Noninska (2020) negatieve gevolgen voor de privacy en is in strijd met het GDPR-beginsel van minimalisering van persoonsgegevens bij de verwerking (zie infra). Ondanks dat privacy een relatief mensenrecht is (zie surpa, '5.1'), blijft dit een erg actueel discussiepunt. Vermits de Big data revolutie door sommige wetenschappers wordt aanzien als een regelrechte invasie op de persoonlijke levenssfeer (Casanovas et al., 2017; Ksherti, 2014). Big data verschillen in hun soort data op vlak van hoeveelheid, omloopsnelheid en verscheidenheid van data. Bijkomend insinueert de definitie dat de data dienen verwerkt te worden, alvorens er kan gesproken worden over Big data. De hoeveelheid en verscheidenheid van verzamelde data vormen de grootste bedreigingen voor de privacy. Het volume aan verzamelde data heeft waanzinnige proporties aangenomen. Dit komt volgens Bleier & Eisenbeiss (2015) door de tactiek waarbij bedrijven zoveel mogelijk data verzamelen om

achteraf pas te analyseren welke ze effectief nodig hebben. Verder was er de introductie van het Web 2.0, die eindgebruikers toeliet om zelf informatie te uploaden (zie supra, '3.2'). Deze door gebruikers gegenereerde inhoud, doet vragen rijzen in verband met verantwoordelijkheid en aansprakelijkheid (OESO, 2011).

Coltman (2007) verklaart dat het vermogen om klanten te identificeren en marketing hierop aan te passen, veel bedrijven in staat heeft gesteld om hun concurrentievoordeel te behouden. Om reclame gepersonaliseerd en doelgericht te maken, werden enorme inspanningen geleverd op vlak van het monitoren van gebruikers op het platform (Rosenberg, 2022). Het monitoren van bezoekers leverde een hele hoop aan persoonlijke informatie op, waarrond de sociale media hun bedrijfsmodellen hebben gebouwd (Tucker, 2012) en waarvan verwacht wordt dat de aanbieders van het metaversum hetzelfde zullen doen (Renwick & Gleasure, 2021; Rosenberg, 2022). Volgens Tucker (2012) en Rosenberg (2022) koos het publiek om niet te betalen met geld waardoor er zonder het te beseffen, gekozen werd om als gebruiker zelf het product te zijn dat wordt verhandeld op deze platformen. Men gooide als het ware, zonder het al te goed te beseffen, de privacy te grabbel. Dit is belangrijk aangezien een mentaliteitswijziging van de consument ten aanzien van privacy nodig is om de potentiële problemen te verminderen (Rosenberg, 2022). Een hogere bereidheid om te betalen voor toegang tot het metaversum zou bijgevolg een oplossing kunnen zijn voor het privacyvraagstuk (Rosenberg, 2022). Volgens Renwick & Gleasure (2021) is dit echter niet zo vanzelfsprekend. Dit komt doordat de grens over wat aanvaardbaar voor consument, varieert op basis van persoonlijke percepties rond waarde en persoonlijke bereidheid om langetermijnkosten in te ruilen tegen kortetermijnwinsten (Renwick & Gleasure, 2021).

De mogelijkheid om platformen te betalen voor digitale diensten zoals het metaversum, in plaats van het afstaan van data, lijkt enerzijds een oplossing voor de privacy. Dit komt neer op het betalen voor toegang tot het metaversum in ruil voor privacy. Anderzijds kan dit leiden tot ongelijkheid doordat niet iedereen in staat is om hiervoor extra te betalen (Romansky & Noninska, 2020). In dit scenario wordt de welgestelde zijn privésfeer gerespecteerd, terwijl iemand met een lager inkomen zijn data moet afstaan (Dobbelaere-Welvaert, 2020). Indirect zou dit ertoe kunnen leiden dat deze mensen met een lager inkomen ertoe verplicht zijn hun data af te staan om deel uit te maken van het digitaal sociale netwerk. Hoewel eerder in de literatuur werd vastgesteld dat het niet deel uit maken van een sociaal netwerk, kan leiden tot sociale uitsluiting (de Graaf, 2016).

Zoals eerder beschreven zijn er meerdere uitdagingen voor het metaversum. Binnen het kader van privacy regulering, is de grootste bedreiging diep ingeworteld in het bedrijfsmodel

zelf. Hierbij wordt er winst gemaakt door Big data te verzamelen en door te verkopen (zie supra, '3.7'). Alles begint hierbij op de manier waarop de bedrijven deze data verzamelen door het monitoren van hun eindgebruikers. Belangrijk hierbij, op vlak van regulering, is dat dit vaak gebeurt zonder dat men het goed beseft (Jain et al., 2021). Hierdoor is het ook moeilijk om als consument bewust te zijn van de mogelijke gevaren van het systematisch verzamelen van informatie aan de hand van *tracking*.

5.3 Het monitoren van gebruikers

De voorbije twee decennia hebben technologiebedrijven er een sport van gemaakt om consumenten te monitoren en hen te categoriseren op basis van gebruikskarakteristieken op hun platformen (Rosenberg, 2022). Het is mede hierdoor en door de ontwikkelingen op vlak van Big data, dat bedrijven de mogelijkheden bezitten om reclame doelgericht te maken en ervoor te zorgen dat deze alleen wordt getoond aan bepaalde vooraf geselecteerde groepen mensen (Tucker, 2012). Technologische vooruitgang betekent in dit geval dat consumenteninformatie kan worden gebruikt om de eigenlijke inhoud van de getoonde reclame te personaliseren en af te stemmen op de interesses van de persoon die ze ziet (Tucker, 2012). Ondanks de vele mogelijke voordelen rond het monitoren van gebruikers, voor zowel de bedrijven als consumenten, hebben dergelijke praktijken de consumenten uitgebuit en diens privacy aangetast (Rosenberg, 2022). Hierdoor krijgen consumenten het benauwd wanneer zij te dicht door bedrijven worden gevolgd en zullen zich hierdoor tegen dergelijke reclame verzetten (Tucker, 2012).

Gegevens van eindgebruikers kunnen aan de hand van monitoring zowel actief als passief worden verzameld. Het verschil tussen beide zit hem bij de betrokkenheid van de personen wiens data verzameld worden. Bij een actieve verzameling geeft deze betrokkene zelf vrijwillig zijn data af. Bijvoorbeeld wanneer deze zijn adres ingeeft voor online shoppen of wanneer deze zelfstandig zijn gegevens ingeeft voor het registreren van een profiel. Bij passieve dataverzameling zal deze persoon minder betrokken zijn. De informatie zal dan verzameld worden via *cookies* en tal van andere passieve manieren waar de consument niet bewust van is. *Cookies* zijn de meest gebruikelijke methode voor het identificeren en volgen van online consumentenactiviteit. Dit aan de hand van kleine tekstbestanden op de harde schijf van een bezoeker die vervolgens worden aangeboden aan de website tijdens latere bezoeken van de betrokkene (Miyazaki, 2008). Hoewel de huidige regelgeving websites en applicaties verplicht hier transparant over te zijn, blijft dit echter een heikel punt op vlak van privacy (zie infra).

Tot slot, zorgde het monitoren van gebruikers ervoor dat sociale media werden omgevormd tot polariserende kanalen (Rosenberg, 2022). Het monitoren stelt derden namelijk in staat om aangepaste berichten te verspreiden die vakkundig gericht zijn op specifiek doelgroepen. Deze tactiek heeft als effect gehad dat bestaande vooroordelen binnen bevolkingsgroepen werden versterkt, politieke standpunten radicaliseerden en verkeerde informatie werd verspreid (Rosenberg, 2022). Samenvattend komt het erop neer dat sociale media in staat is om iemand zijn waargenomen werkelijkheid te beïnvloeden door te filteren in datgene wat men al dan niet te zien krijgt. Wanneer Big data zomaar worden verhandeld, heeft niemand nog privacy en wordt iedereen zomaar in groepen gedeeld. Aan de hand van deze data kunnen mensen op verschillende manier worden beïnvloed (Rosenberg, 2022), met de bovenstaande maatschappelijke problemen tot gevolg. Het grootste probleem hierbij is dat van het metaversum echter verwacht wordt dat deze negatieve aspecten, ten gevolge van het monitoren van gebruikers, alleen maar zullen verergeren (Rosenberg, 2021a). Dit komt doordat het metaversum de mogelijkheden heeft om nog meer data te verzamelen dan de huidige sociale platformen (Amaizu et al., 2022; Dhelim et al., 2022). De technologie zal namelijk niet alleen bijhouden waar bezoekers op klikken, maar ook waar ze naartoe gaan, wat ze doen, waar ze naar kijken en zelfs hoe lang hun blik blijft hangen (Rosenberg, 2022). Volgens Dobbelaere-Welvaert (2020), zijn de potentiële gevaren die hand in hand gaan met het afstaan van persoonsgegevens, niet te voorspellen. Het is dus niet onlogisch dat eindgebruikers hiervoor moeten worden beschermd.

5.4 Big data en het metaversum

Het metaversum bevat meer rijke gegevens over gebruikers dan de traditionele sociale media (Amaizu et al., 2022; Dhelim et al., 2022; Rosenberg, 2022). Mede doordat de Techreuzen hun eindgebruikers in *realtime* kunnen monitoren (zie supra, ‘5.3’). Volgens van Schaik et al. (2018) zal dit automatisch leiden tot een hogere kans op het schenden van de privacy. De data zullen worden opgeslagen wanneer de gebruikers bijvoorbeeld vertragen om producten of diensten te bekijken, of wanneer ze versnellen om locaties te passeren waarin ze niet geïnteresseerd zijn (Rosenberg, 2022). De maatschappelijke noodzaak om privacy binnen het metaversum te waarborgen, wordt echter duidelijk wanneer dit gaat over gevoelige informatie.

Het *realtime* verwerken van data uit een digitale wereld, zorgt volgens Kye et al. (2021) voor een inbreuk op de privacy bij sociale activiteiten in het metaversum. Zoals eerder beschreven zou een ervaring binnen het metaversum als echt worden aanschouwd, waardoor er ook wordt gesproken over het ervaren van echte emoties (zie supra, ‘3.4’). Binnen een digitale wereld zullen er veel interacties plaatsvinden tussen avatars onderling.

Volgens Zhao et al. (2021) mag ervan worden uitgegaan dat deze interacties niet allemaal bedoeld zijn om door anderen begrepen te worden. De nauwere band tussen gebruikers zorgt deels dat er gevoeligere informatie ontstaat binnen het metaversum, die door mensen met slechte intenties kan worden gestolen (Zhao et al., 2021). Het uitlekken van persoonlijke informatie van avatars, zou volgens Dhelim et al., (2022) kunnen leiden tot identiteitsdiefstal. Het is naast een duidelijke regulering omtrent het opslaan van deze Big data uit het metaversum, ook belangrijk dat dit soort platformen uiterst veilig worden ontworpen door de ontwikkelaars.

5.5 Gevaren Big data voor privacy

Jain et al. (2021) stellen dat er een gebrek aan bewustzijn rond privacy heerst. Nochtans zijn er veel mogelijke gevaren door het zomaar afstaan van data. Deze gegevens kunnen zeer alledaagse informatie bevatten over de gebruiker en zijn omgeving, maar ook gevoelige informatie die tegen elke prijs vertrouwelijk moet worden gehouden (Amaizu et al., 2022). Dit ligt niet in lijn met de manier waarop organisaties tegenwoordig geneigd zijn om gebruikersgegevens als een bron van waarde te zien, zelfs als dat ten koste gaat van de privacy (Renwick & Gleasure, 2021). Het indelen van gebruikers aan de hand van dit soort gegevens kan bedrijven helpen betere reclame en overtuigingspogingen te bedenken, die soms roofzuchtig kunnen zijn (Kshetri, 2014; Tucker, 2012). Zo is het mogelijk om niet-persoonlijke gegevens te gebruiken om voorspellingen te maken rond gevoelige aard zoals: seksuele geaardheid, etniciteit, religieuze en politieke opvattingen, persoonlijkheidskenmerken, intelligentie, mate van geluk, verslavend middelengebruik, scheiding van ouders, leeftijd, geslacht en financiële status (Kshetri, 2014). Wanneer een bezoeker van het platform aangeeft dat dit soort informatie niet publiek mag worden verhandeld, druist het doorverkopen hiervan in tegen de privacy van het subject (zie infra, ‘6.1.1’). Zeker wanneer de gebruiker deze gegevens nooit expliciet heeft meegedeeld aan de dataverzamelaars. Ksherti (2014) suggereert zelfs dat bedrijven de waarschijnlijkheid kunnen bepalen dat iemand aan een ernstige ziekte heeft geleden en deze informatie kunnen misbruiken om onnodige verzekeringspolissen op de markt te brengen. Het meest frappante van dit soort voorspellingen is volgens Ksherti (2014) dat ze gebeuren op grond van een algoritme dat getraind is om personen te categoriseren aan de hand van op het eerste zicht onschuldige data zoals *likes* op Facebook. Big data en het recht op een privéleven gaan in bovenstaand scenario dus niet goed samen. Hoewel mensen op het eerste zicht, gevoelige informatie niet prijs geven, kunnen deze algoritmes hier toch een voorspelling rond maken op basis van zogenaamde onschuldige data (Jain et al., 2021). Een onjuiste interpretatie van de verzamelde big data voor een persoon is mogelijk, wat problemen kan veroorzaken voor de relatie van de persoon binnen een organisatie, en in

zijn/haar familie (Romansky & Noninska, 2020). Volgens Romansky & Noninska kunnen onjuiste conclusies leiden tot bepaalde ethische afwijkingen of discriminatie. Hierdoor kunnen mensen worden ingedeeld in categorieën zonder dat ze dit beseffen, waardoor er nieuwe vormen van discriminatie kunnen plaats vinden (Kshetri, 2014). Naast het duidelijk schenden van de privacy, is het grote probleem hierbij dat internetgebruikers vandaag de dag geen idee heeft wat er gebeurt met onze data aangezien de macht bij de bedrijven zit (Legrand, 2021). Veel van deze bezorgdheden overstijgen specifieke technologieën. Het gaat over een toenemende verstrengeling van het analoge en het digitale leven en de noodzaak van bescherming tegen ongewenste privacy inbreuken door derden (Renwick & Gleasure, 2021).

6 Regulatie van Big data binnen het metaversum

Uit het hoofdstuk 3.5.3 omtrent de uitdagingen voor het metaversum, blijkt dat er met veel zaken rekening moet worden gehouden om van het metaversum een veilige omgeving te maken. Zo zijn er uitdagingen op vlak van de toegankelijkheid van het platform, de gebruikersveiligheid, beveiliging, mentale en fysieke gezondheid, het milieu en natuurlijk ook de privacy. Om potentiële problemen te voorkomen, moeten alle partijen die een invloed hebben op het metaversum, nadenken over een zinvolle en adequate regelgeving (Renwick & Gleasure, 2021). Bovendien moet dergelijke regelgeving snel worden overwogen, voordat de problemen diep in de infrastructuur en bedrijfsmodellen van het metaversum worden verankerd waardoor ze moeilijk ongedaan te maken zijn (Rosenberg, 2022). Dit onderzoek richt zich op de mogelijkheden om het gebruik van persoonsgegevens te reguleren binnen deze digitale werelden. Het bekijkt welke partijen invloed hebben op het metaversum en hoe deze de privacy van de eindgebruikers kunnen waarborgen. De overige opgesomde uitdagingen, gaan vaak niet alleen over regelgeving maar ook over de moderatie en de ontwikkeling van het platform. Deze aspecten werden geschetst met oog op het maatschappelijke belang en verdienen diepgaand vervolgonderzoek.

De Big data-industrie is uitgegroeid tot een branche die opereert binnen een grijze zone op vlak van regelgeving (Kshetri, 2014; Renwick & Gleasure, 2021; Romansky & Noninska, 2020). De bedrijven die Big data exploiteren, vinden dat het gebruik van persoonlijke gegevens, die via andere diensten verzameld zijn, de gebruikerservaring verhoogt (Tucker, 2012) (zie supra, ‘4. Big data’). Daartegenover vormt deze ongecontroleerde verzameling van gegevens, met het oog op het verbeteren van niet-direct gerelateerde services, een inbreuk op de privacy van de gebruiker (zie supra, ‘5. Privacy’). De ernst van deze kwestie wordt vergroot door het feit dat de huidige regelgeving de consument onvoldoende beschermt tegen het doorverkopen van hun persoonlijke informatie aan derden (Kshetri, 2014). Daarboven wordt verwacht dat door de opkomst van het metaversum er gigantische hoeveelheden aan persoonlijke data zullen bijkomen (Verrycken, 2022). Volgens Boone et al. (2021) zouden bedrijven in strikte zin alleen de minimale informatie mogen verzamelen die nodig is voor het leveren van diens specifieke service of product. Dit verschilt met de huidige strategieën om zoveel mogelijk gegevens te verzamelen om inzichten tussen services te krijgen (Boone et al., 2020). Een dergelijke strategie zou ook in overeenstemming zijn met het concept van gegevensminimalisatie van de GDPR (zie infra). Tot slot stellen Romansky & Noninska (2020) dat de Big data voor verschillende doeleinden worden verzameld, wat in strijd is met het GDPR-beginsel van gegevenscorrectheid (zie infra).

Volgens Rosenberg (2021b) is het belangrijk dat de mate waarop bedrijven hun klanten onbewust monitoren, wordt beperkt. Zoals eerder beschreven is het monitoren van gebruikers namelijk niet ongebruikelijk voor aanbieders van onlinediensten (zie supra, '5.3'). Deze bedrijven zouden klantengegevens niet langer mogen opslaan dan de korte tijd die nodig is om de gebruikservaring te optimaliseren (Rosenberg, 2021b; Tucker, 2012). Wanneer deze bedrijven de verzamelde data enkel intern gebruiken, zal de mate waarmee derden ons gedrag analyseren geleidelijk afnemen (Rosenberg, 2021b). Bovendien moeten deze bedrijven volgens Rosenberg (2021b) het publiek informeren over wat er wordt bijgehouden en hoe lang dat gebeurt. De voor de hand liggende oplossing voor deze privacy gerelateerde problemen, is de verwerking van Big data te reguleren. Echter bemoeilijken er volgens Renwick & Gleasure (2021) ten minste vier factoren de pogingen om doeltreffende wetgeving te ontwerpen (Renwick & Gleasure, 2021). Ten eerste is het niet eenvoudig om privacy te definiëren en te meten (Renwick & Gleasure, 2021; Dobbelaere-Welvaert, 2020). Ten tweede zijn veel mensen bereid privacy op te geven als onderdeel van een economische ruil voor producten en diensten (Renwick & Gleasure, 2021). Ten derde verschilt de behoefte van individuen om persoonlijke informatie te beschermen per land (Renwick & Gleasure, 2021). Tot slot is er nog de onduidelijkheid omtrent welke entiteiten regels moeten opleggen (Renwick & Gleasure, 2021).

De eerste factor, die luidt dat privacy moeilijk af te bakenen valt, ligt in lijn met de bevindingen van het hoofdstuk '5.1 Omkadering privacy'. In dit hoofdstuk wordt het begrip privacy besproken en voorzien van een definitie die neerkomt op: 'het recht op privéleven, zowel fysiek als digitaal'. Dat privacy subjectief is en bijgevolg verschilt van persoon tot persoon, wordt extra benadrukt in de tweede factor die de wetgeving rond Big data regulering bemoeilijkt. Deze stelt dat sommige mensen bereid zijn om digitale diensten te gebruiken in ruil voor het afstaan van data (Renwick & Gleasure, 2021). Deze stelling ligt in lijn met de bedenkingen uit het hoofdstuk '3.7 Bedrijfsmodel van het metaversum'. Het is met name moeilijk om Big data te bestrijden aangezien dit diepgeworteld zit in de manier waarop de aanbieder van het platform winst maakt. Zeker wanneer niet iedereen bewust is van de gevaren rond privacy, waardoor er verschillende percepties heersen rond de waarde van persoonlijke data (zie supra, '5.5'). Dit maakt het volgens Renwick & Gleasure (2021) moeilijk om te definiëren wat aanvaardbaar is als bedrijfsmodel. De derde en vierde factor gaan rond culturele verschillen die een impact hebben op de behoefte om persoonlijke informatie te beschermen, en rond de onduidelijkheid over welke actoren regels moeten opstellen (Renwick & Gleasure, 2021). Welke mogelijke partijen privacy kunnen waarborgen binnen een metaversum, wordt verder afgetoetst in een volgend hoofdstuk (zie infra, '6.1'). Het is niet onlogisch dat hierbij culturele verschillen heersen, aangezien privacy subjectief is en het metaversum een globaal platform is. Deze complexiteit bemoeilijkt de mogelijkheden

om het metaversum te laten reguleren door één bepaalde overheid. Easton (2019) sluit zich aan bij de stelling dat het vervagen van grenzen zorgt voor een uitdaging voor heel wat actoren binnen het veiligheidsdomein. Volgens haar is er hierdoor een groeiend bewustzijn op het terrein dat er moet samengewerkt worden om digitale veiligheid te waarborgen (Easton, 2019).

6.1 Welke partijen zijn in staat privacy in het metaversum te reguleren?

Binnen het metaversum zijn er meerdere actoren die invloed kunnen hebben op de spelregels. Zoals eerder aangegeven hoeft dit geen exclusieve taak te zijn voor publieke instanties. Zo zijn er naast de overheden nog andere spelers die toegang moeten verlenen alvorens men verbinding kan maken met het metaversum. Enerzijds dienen eindgebruikers toegang te hebben tot het internet (zie supra, '3.3'). Hierdoor spelen telecommunicatie operatoren mogelijks ook een rol binnen het metaversum. Verder zijn er uiteraard nog de bedrijven die de metaversums ontwikkelen, zoals het vaak aangehaalde Meta van Zuckerberg. Volgens Ksherti (2014) is er behoefte aan een Big data-beleid, op bedrijfsniveau, vanwege de onderontwikkelde regelgevende instellingen. Deze dienen bijvoorbeeld rekening te houden met de mate van gevoeligheid van informatie wat de privacy kan bedreigen (Kshetri, 2014). Tot slot is er nog de burgermaatschappij die een grote invloed kan hebben.

Om te kijken hoe metaverses gereguleerd kunnen worden op vlak van databescherming, is het belangrijk om te kijken naar welke rechten men vandaag de dag bezit op vlak van digitale vrijheid en bescherming van persoonlijke data. Aangezien er geen specifieke regelgeving is omtrent metaverses op zich, is het volgens Rosenberg (2022) nuttig om eerst de argumenten in overweging te nemen die zijn aangevoerd voor de regulering van internetdiensten zoals bijvoorbeeld sociale mediaplatformen. Dit komt doordat het metaversum wordt gezien als een evolutionaire uitbreiding van soortgelijke industrieën (Rosenberg, 2022). Hoewel het metaversum gebaseerd is op een verdere ontwikkeling en combinatie van bestaande technologieën zoals gametechnologie, AR en VR, is het bovenal een internettoepassing (Legrand, 2021; Rosenberg, 2022). Doordat het metaversum voortvloeit uit bestaande technologieën, is er reeds een basis voor regulering en wetgeving omtrent privacy en Big data (Rosenberg, 2022). Zoals eerder aangeven is het algemene doel van privacy regulering, de mate te beperken waarin bedrijven de persoonlijke informatie van consumenten kunnen traceren en gebruiken (Bleier et al., 2020) (zie supra, '5.3').

6.1.1 Publieke instanties

Het waarborgen van een passende bescherming rond elektronische persoonsgegevens over de grenzen heen, is een belangrijk aandachtspunt voor de regeringen (Meltzer, 2015). Binnen de Belgische grondwet staat in artikel 22 een stuk geschreven over privacy. Artikel 22 luidt: "Ieder heeft recht op eerbiediging van zijn privéleven en zijn gezinsleven, behoudens in de gevallen en onder de voorwaarden door de wet bepaald". Echter hinkelt het Belgische recht, zoals vaak, op vlak van technologische innovaties, wat achterop

(Dobbelaere-Welvaert, 2020). Zo staat er bijvoorbeeld niks over de digitale privacy in het Belgische recht. Dit komt omdat het recht op databescherming van de Europese consument vandaag de dag op Europees niveau wordt geregeld (Gruschka et al., 2018).

Het blijkt echter niet gemakkelijk om globale wetten op te stellen rond privacy. Eén van de uitdagingen rond de regulatie van een globaal platform zoals het metaversum, is dat het zorgt voor een geleidelijke vervaging van nationale grenzen en de uitholling van de soevereiniteit van natiestaten (Meltzer, 2015). Volgens Easton (2019) zijn digitale gemeenschappen minder afgelijnd en moeilijker geografisch te lokaliseren aangezien er zowel inzake probleemdefiniëring als bij het opzetten van partnerschappen grensoverschrijdend moet worden nagedacht. Daarnaast stelt Meltzer (2015) dat landen onderling de bescherming van de persoonlijke levenssfeer en de uitvoer van consumentengegevens op verschillende manieren aanpakken. Bijkomend zijn er volgens Renwick & Gleasure (2021) verschillen van land tot land tussen de houding waarop burgers staan ten opzichte van publieke instellingen die op zoek zijn naar persoonlijke informatie. Deze overheidsinstanties kunnen volgens Medzini (2021) privé-informatie gebruiken om de politieke en commerciële voorkeuren van individuen te traceren, onjuist te informeren en te beïnvloeden. Bovenstaande zaken vermoeilijken de inspanningen om globale regels op te stellen voor publieke toezichthouders (Renwick & Gleasure, 2021). Hierdoor lijkt het deels zinloos om deze digitale, grenzeloze wereld, louter te reguleren op basis van wetten gebaseerd op grenzen binnen de fysieke wereld. Het verenigen van meerdere Europese landen met als doel algemene wetten op te stellen over de spelregels van het Web, kan wel een stap in de goede richting zijn. Een bijkomstig voordeel van Europese wetten is dat deze naast de bezorgdheden rond privacy en Big data (zie supra, ‘5.5’), ook een impact hebben op bezorgdheden rond politieke actoren (Medzini, 2021).

Zoals eerder aangehaald, heeft artikel 8 in het EVRM[1] bettrekking op de bescherming van persoonsgegevens. Ondanks dat dit artikel gaat om een relatief grondrecht, kwam in het literaire onderzoek reeds naar voren dat Big data worden doorverkocht aan derden zonder de expliciete toestemming van de gebruikers (Jain et al., 2021). Dit is niet compatibel met de manier waarop privacy wordt omschreven binnen dit onderzoek. Het verkopen van Big data, zonder toestemming van de eindgebruiker, ligt niet in lijn met de relatieve rechten van de

[1] Artikel 8 (EVRM) – “*De bescherming van persoonsgegevens: Eenieder heeft recht op bescherming van zijn persoonsgegevens. Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Eenieder heeft recht van inzage in de over hem verzamelde gegevens en op rectificatie daarvan. Een onafhankelijke autoriteit ziet erop toe dat deze regels worden nageleefd.”* (FRA, s.d).

Europeaan, zoals beschreven in artikel 8 van het EVRM. Het monitoren van de eindgebruikers, wat reeds jaar en dag de modus operandi is van deze techreuzen, is bijgevolg illegaal zonder expliciete toestemming (Bleier et al., 2020). Verder zou een onafhankelijke autoriteit hierop moeten toezien. In het geval van private aangelegenheden is het niet ongebruikelijk dat een publieke instantie, zoals een overheidsinstelling, hierop toeziet (Romansky & Noninska, 2020). Ordehandhaving is namelijk traditioneel een publieke aangelegenheid (Nalla & Gurinskaya, 2020). In het derde deel van artikel 8 (EVRM), staat echter niet dat deze autoriteit de overheid is. Het is dus met name geen exclusieve overheidsbevoegdheid om de privacy te controleren.

Mengela Kuneva opperde reeds in 2009 voor de ontwikkeling van een instrument die de belangen van het bedrijfsleven en die van de consument met elkaar in evenwicht brengen. Hierbij bracht ze twee belangrijke principes naar voren, namelijk: de eerbiediging van het recht van gebruikers om hun publieke bekendheid te controleren, en de verplichting om hen te beschermen tegen misbruik en risicovolle praktijken die tegen hen gericht zijn (Kuneva, 2009). Deze principes vormen de fundamenten waaruit de huidige *General Data Protection Regularisation* (GDPR) ook gekend als de Algemene Verordening Gegevensbescherming (AGV), is voortgevloeid. De GDPR-wetgeving zijn wetten die sinds mei 2018 van kracht zijn binnen de Europese Unie (EU). Deze vertrekken vanuit het standpunt dat elke inwoner binnen de EU, het recht heeft dat diens data worden beschermd (European Commission, z.d). De wetten zijn van toepassing op alle organisaties binnen de EU, de Europese Economische Ruimte (EER) en ook voor organisaties uit andere landen die gegevens van Europese burgers verwerken (Gruschka et al., 2018). Hierdoor zijn de regels van toepassing op de meeste grote bedrijven wereldwijd (Gruschka et al., 2018). Deze regelgeving verhindert zelfs de uitvoer van gegevens naar landen buiten de EU met een minder strenge wetgeving inzake gegevensbescherming (Meltzer, 2015). De wetgeving is gebaseerd op een aantal principes waaraan alle bedrijven, overheidsdiensten, organisaties en instellingen die in Europa persoonsgegevens verwerken, gebruiken, registreren of bewaren, moeten voldoen (Vlaamse Overheid, z.d). Artikel 5 van de GDRP, omschrijft deze principes betreffende de verwerking van persoonsgegevens.

1. Persoonlijke data moeten:
    a. Rechtmatig, billijk en transparant ten aanzien van de betrokkene worden verwerkt.
    b. Voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verkregen en mag vervolgens niet worden verwerkt op een wijze die onverenigbaar is met deze doeleinden.

c. Nauwkeurig zijn en, waar nodig, worden bijgewerkt. Alle redelijke maatregelen moeten worden genomen om te zorgen dat persoonsgegevens die onjuist zijn, gewist of gecorrigeerd worden.
d. Niet langer worden bewaard in een vorm die het mogelijk maakt de betrokkenen te identificeren dan noodzakelijk is voor de verwezenlijking van de doeleinden waarvoor zij worden verwerkt. Persoonsgegevens mogen langer worden bewaard voor zover de data uitsluitend worden verwerkt voor archivering in het algemeen belang, voor wetenschappelijk of historisch onderzoek of voor statistische doeleinden.
e. Worden verwerkt op een wijze die een passende beveiliging van de persoonsgegevens waarborgt, met inbegrip van bescherming tegen ongeoorloofde of onwettige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. Waarbij passende technische of organisatorische maatregelen worden genomen.

De principes van de GDPR-wetgeving zijn samenvattend: "*transparantie*", "*gegevensminimalisatie*", "*nauwkeurigheid*", "*opslagbeperking*" en "*integriteit en veiligheid*". Deze principes representeren de minimale verwachtingen die de consument heeft ten opzichte van organisaties die hun data verzamelen. Het principe van transparantie zou een oplossing bieden rond de vragen omtrent privacy op vlak van passieve dataverzameling (zie supra, '5.3'). Dit principe zorgt er namelijk voor dat elke organisatie eerst toestemming moet vragen aan de betrokkene, om diens data te verzamelen. Hiermee tracht de GDPR-wetgeving een antwoord te bieden op de vragen omtrent *cookies* en privacy.

Het is echter de vraag of deze GDPR-wetgeving er effectief voor kan zorgen dat de privacy van de Europese consumenten gewaarborgd blijft. Zo zullen bedrijven nog steeds de juridische verantwoordelijkheid in de schoenen van de consumenten schuiven (Dobbelaere-Welvaert, 2020). Dit doen bedrijven vaak aan de hand van de zogenaamde *Terms of Agreement* (Buttarelli, 2019). Deze gebruikersovereenkomsten zijn over het algemeen bedoeld om een dienstverlener te beschermen tegen juridische geschillen (Buttarelli, 2019). Buttarelli, Europees *data protection supervisor,* kaart aan dat deze voorwaarden de GDPR-wetgeving omzeilen op vlak van het transparantie en billijkheid beginsel (2019). Op het eerste zicht lijken deze servicevoorwaarden transparant doordat ze open en bloot alles aankaarten. Echter bestaan deze soms uit meer dan 20.000 moeilijk te begrijpen woorden, waardoor de serviceverlener weet dat niemand deze grondig zal lezen (Dobbelaere-Welvaert, 2020). Op vlak van billijkheid zijn deze voorwaarden ook strijdig met de principes van de GDPR. Zo vormen ze geen overeenstemming tussen twee gelijke partijen, maar

worden deze opgesteld door de dienstverlener die niet openstaat voor enige vorm van onderhandelingen (Buttarelli, 2019). De dienstverlener blijft in het bezit van een machtspositie waardoor de consument eerder voor een voldongen feit staat dan voor een vrije keuze (Dobbelaere-Welvaert, 2020).

De GDPR-wetgeving zorgt er ook voor dat de data niet mag verwijzen naar de persoon van wie deze afkomstig is. Echter stellen Jain et al., (2021) dat hoe meer details er worden verstrekt, hoe gemakkelijker het is voor derden om deze informatie te gebruiken om identiteit te stelen of andere cybermisdrijven te plegen. Het metaversum zal bijgevolg dit probleem niet vergemakkelijken aangezien er wordt verwacht dat er hierdoor nog extra data in omloop zal komen (Amaizu et al., 2022). Het delen van informatie zou volgens Jain et al., (2021) moeten worden beperkt in plaats van worden uitgebreid. Hoewel de GDPR-wetgeving stelt dat enkel de data mag worden opslaan die nodig is voor gerechtvaardigde doeleinden, is dit niet altijd het geval. Zo is er bijvoorbeeld Uber, een Amerikaans bedrijf dat een online platform heeft ontwikkeld om consumenten en chauffeurs te verbinden. Het bedrijf Uber bezit zelf geen auto's maar levert wel een dienst via het internet. Om het servicelevel te verhogen, monitort Uber het gedrag van zijn consumenten. Hoewel het een Amerikaans bedrijf is, is Uber ook actief binnen het Europese continent en zijn de data van de Europese burgers bijgevolg onderhevig aan de Europese wetten. Echter zal de Europese consument, ondanks de GDPR-regelgeving, nog steeds de lange servicevoorwaarden van Uber moeten uitpluizen, alvorens deze kan achterhalen waarom het bedrijf toegang wil krijgen tot diens foto's. Dobbelaere-Welvaert (2020) stelt dat het gevolg van de GDPR-wetgeving, op vlak van passieve dataverzameling, zich vooral toont op vlak van omslachtigheid. In de plaats van onopgemerkt alle data op te slaan, vragen organisaties dit nu via pop-ups (2020). Applicaties zullen dus wel de toestemming vragen, maar het is absoluut niet duidelijk voor de consumenten welke data ze afstaan. Het is duidelijk dat datatransparantie meer is dan alleen wat moeilijk te interpreteren woorden in ellenlange voorwaarden van het overeenkomstdocument. Het vereist dat er iets mogelijk wordt gemaakt voor degenen die zich met die woorden bezighouden (Obar, 2022). Om de beoogde transparantie te realiseren, moeten volgens Obar (2022) de mogelijkheden voor controle van data verzameling worden herdacht, met het doel verantwoording af te leggen aan de bevoegde instanties.

Tot slot is het belangrijk te vermelden dat het volgens Ksherti (2014) en Renwick & Gleasure (2021) niet zeker is of de overheden het gebruik van privégegevens en Big data volledig willen reguleren. Enerzijds omdat ze zelf Big data gebruiken om de prestaties van de door overheidsinstanties geleverde diensten verbeteren (Kshetri, 2014). Zo helpen Big data wetshandhavers om middelen efficiënter in te zetten, sneller te reageren en de

aanwezigheid in criminaliteitsgevoelige gebieden te vergroten (Kshetri, 2014). Anderzijds is het ontwerpen van regelgeving een uitdaging wanneer technologieën nog in de kinderschoenen staan, omdat de aard en omvang van de risico's doorgaans onduidelijk zijn (Renwick & Gleasure, 2021). Zowel Buttarelli (2019), Gruschka et al. (2018) en Ksherti (2014) stellen dat overheden vaak niet kunnen opboksen tegen de snelheid waarmee technologieën zich ontwikkelen en aanpassen. Daarnaast willen overheden niet voortijdig handelen uit schrik de innovatie te belemmeren (Renwick & Gleasure, 2021). Volgens Meltzer (2015) is de belangrijkste uitdaging voor de toekomst het open karakter van het internet zoveel mogelijk te handhaven en tegelijkertijd de overheidsbemoeienis te beperken tot wat nodig is. De trend van de laatste decennia is dan ook om in de beginfase van technologieën overheidsregulering te vermijden (Renwick & Gleasure, 2021). Overheden hebben namelijk schrik om de innovatie in te perken en zo competitiviteit te verliezen ten opzichte van andere landen (Meltzer, 2015; Renwick & Gleasure, 2021). In plaats daarvan laten overheden meerdere partijen beslissen over: het gebruik van de technologie, de risico's en de aanvaardbare afwegingen tussen waarde, privacy en andere sociale kosten (Renwick & Gleasure, 2021). Deze terughoudendheid van overheden, heeft volgens Renwick & Gleasure (2021) de deur opengezet voor andere regelgevers. Echter is het niet duidelijk welke andere entiteiten, als die er al zijn, het recht of de middelen hebben om regelgeving op te leggen (Renwick & Gleasure, 2021; Rosenberg, 2022).

6.1.2 Internetoperatoren en telecommunicatie-infrastructuur aanbieders

Een internetverbinding is noodzakelijk om verbinding te maken met het metaversum. Het zijn de internetoperatoren die deze verbindingen mogelijk maken. Deze vaak private instanties regelen het internetverkeer tussen de zender en ontvanger. Aanbieders van internettoegang stellen tegen betaling de fysieke infrastructuur ter beschikking die nodig is voor toegang tot het internet. Deze operatoren kunnen daarbij persoonlijke informatie verzamelen, gebruiken, bekendmaken en bewaren (Obar, 2022). Hierdoor zijn operatoren een potentiële partij met invloed op het verzamelen van data binnen het metaversum. Hoewel eindconsumenten weten aan welke internetoperator zij elke maand betalen, beseffen deze volgens Obar (2022) niet dat elke digitale interactie tussen verzender en ontvanger via deze operatoren loopt. Deze operatoren zitten bijgevolg aan de bron van het dataverkeer. Hierdoor kan er zonder duidelijke regulatie een inbreuk gebeuren op de persoonlijke levenssfeer van de eindgebruiker. Zeker met de verwachtingen rond data uit het metaversum in het achterhoofd. Op dit moment verzamelen deze operatoren reeds veel data zoals: locatiebepaling, gegevens rond types apparaten, gegevens van beveiligingsapparatuur thuis en bewakingsgegevens van winkels (Obar, 2022). Obar (2022) verwacht zelfs dat operatoren boven op deze data nog diverse andere soorten gegevens

verzamelen, afhankelijk van het bedrijfsmodel van elke aanbieder. Hieruit kan worden afgeleid dat deze partijen een invloed kunnen hebben op de privacy. Het is volgens Meltzer (2015) belangrijk dat deze partijen opereren binnen een duidelijk wettelijk kader.

In tegenstelling tot het grensoverschrijdende concept van het digitale metaversum, zijn internetoperatoren wel entiteiten die binnen fysieke grenzen opereren. Aanbieders van internetdiensten moeten immers fysiek aanwezig zijn in hetzelfde rechtsgebied als hun gebruikers om hun diensten te kunnen aanbieden (Meltzer, 2015). Hierdoor is het voor een overheid gemakkelijk om deze tussenpersonen te reguleren en te controleren. Aangezien deze moeten investeren in middelen, apparatuur en personeel in het land waar zij actief zijn, hebben deze daarvoor toestemming van de staat nodig en moeten ze zich houden aan de nationale wetgeving (Meltzer, 2015). Op vlak van regelgeving hangen operatoren dus vast aan de eerder omschreven wetten die de publieke instanties zoals België of Europa opleggen. Echter zouden deze internetproviders, volgens Obar (2022), transparanter mogen zijn op vlak van hun privacy standaarden. Deze operatoren geven niet genoeg details over de soorten persoonlijke informatie die ze verzamelen (Obar, 2022). De afwezigheid van transparantie op vlak van datagebruik, is een eerder vermeld probleem dat ertoe leidt dat consumenten niet bewust zijn van de mogelijke gevaren ervan (Jain et al., 2021; Rosenberg, 2022).

6.1.3 De makers van het internet

Zoals eerder aangehaald is het internet zoals nu gekend, niet hetzelfde als toen het ontstond. Het internet is destijds ontstaan als een “alleen-lees-web”, gebouwd als gemeenschappelijke omgeving waar ideeën en kennisuitwisseling kon plaatsvinden zonder al te veel regels en beperkingen (zie supra, ‘3.2’). Echter groeide het internet uit tot een "lees-schrijf-web" waar iedereen een bijdrage kon leveren. Deze evolutie gebeurde niet door de oorspronkelijke technische gemeenschap, maar onder invloed van private bedrijven die het internet gebruikten om diensten te verkopen (Ankerson, 2015; Ozcinar et al., 2020). Het in de jaren zeventig ontworpen internet, ligt door deze Web 2.0 evolutie veraf van de manier waarop het internet vandaag de dag werkt. Ankerson (2015) ziet de manier waarop het Web 1.0 evolueerde naar Web 2.0 niet als een mislukking van de verbeelding of een technologische beperking, maar als een strategische en zwaarbevochten prestatie van deze bedrijven. Omwille van deze duidelijke scheidingslijn tussen Web 1.0 en Web 2.0, lijkt het onlogisch dat de moeilijkheden kunnen worden opgelost door de uitvinders van het internet.

Wanneer blijkt dat de evolutie van Web 2.0 naar Web 3.0 zou inhouden dat eindgebruikers de macht teruggrijpen rond hun data, zou dit wel in lijn liggen met de verwachtingen van de

makers van het internet (Benhaddi, 2017). Dit kan enkel gepaard gaan met een wijziging in het bewust zijn rond de gevaren van Big data en privacy (Jain et al., 2021). Bijkomend zouden de consumenten van internetdiensten moeten bereid zijn om te betalen voor het aanmaken van een account op een internetplatform, of zouden nieuwe bedrijfsmodellen moeten ontstaan (Rosenberg, 2022). Dit doet vermoeden dat de bedrijven die de macht grepen in de Web 2.0 revolutie de oplossing in handen hebben om de privacy te waarborgen.

6.1.4 De bedrijven achter het metaversum

In de voorgaande hoofdstukken werd omschreven hoe bedrijven persoonsgegevens gebruiken met oog op winstbejag in plaats van de privacy van hun klanten. De drang om winst na te streven, was niet de eerste intentie van de makers van het internet (Ankerson, 2015). Het grote verschil van deze bedrijven ten opzichte van de stichters van het internet, is dat techreuzen beursgenoteerd zijn. Hoewel het internet in eerste instantie niet bedoeld was als middel om data te verzamelen, is het dat wel geworden (zie supra, '3.2'). Bijkomend slagen de publieke instanties er niet in om adequaat deze bedrijven te reguleren en te bestraffen. Enerzijds doordat het opstellen van regels veel achterloopt ten opzichte van de snelheid waarmee nieuwe technologieën worden ontwikkeld. Anderzijds doordat overheden deze bedrijven niet al te veel wil beperken in het ontwikkelen van deze technologieën (zie supra, '6.1.1'). Zolang er geen bewustzijn gecreëerd wordt rond de gevaren van privacy, zal Big data blijven gebruikt worden met oog op het doorverkopen hiervan. Verwacht wordt dat dit in het metaversum niet anders zal zijn (Van Der Haegen, 2022).

De problemen rond Big data en privacy zijn enerzijds het gebruiken van algoritmes die mensen classificeren op basis van voorspellingen (zie supra, '5.5'). Anderzijds het gevaar dat deze gevoelige data in verkeerde handen valt (Jain et al., 2021). Zoals vermeld in hoofdstuk 6.1.1, worden deze problemen binnen Europa gereguleerd via de GDPR-wetgeving. Deze wet stelt dat bedrijven die data doorverkopen aan derden de consument expliciet op de hoogte moeten stellen. Wanneer de bedrijven hun verzamelde data met het oog op een verbetering van de internetdienst doorverkopen zonder dat de gebruiker dit weet, is dit in strijd met de GDPR-regelgeving vanwege de onverenigbaarheid met de doeleinden (zie supra, '6.1.1'). Echter leert de literatuur dat bedrijven deze wetten doelbewust trachten te omzeilen, bijvoorbeeld aan de hand van *pop-up* schermen die vragen de voorwaarden te accepteren (Buttarelli, 2019). Aangezien de consument zich niet bewust is van de gevaren, of geen zin heeft om de lange overeenkomstvoorwaarden te lezen, worden deze pop-ups vaak automatisch geaccepteerd (Dobbelaere-Welvaert, 2020). Hierdoor houden de bedrijven zich aan de GDPR-wetgeving zonder de consument zijn

privacy echt te beschermen, wat de grote tekortkoming is van deze trage wetten volgens Dobbelaere-Welvaert (2020). Medzini (2021) voegt hieraan toe dat deze praktijken niet ethisch zijn en dat deze digitale dienstverleners beter aan zelfregulering moeten doen naast de opgelegde overheidsregels.

Met zelfregulering bedoelt Medzini (2021) het proces waarbij individuele organisaties of volledige sectoren, regels en procedures ontwerpen en deze regels en procedures vervolgens zelf toepassen. Op het eerste zicht lijkt het raar dat bedrijven zichzelf gaan reguleren. Zeker als het gaat over een belangrijk aspect met het oog op winst maken. Echter waarschuwen Bleier et al. (2020) en Tucker (2012) dat privacy een belangrijk onderdeel kan worden van een bedrijfscultuur wanneer het bewustzijn er rond zou stijgen. Zeker wanneer consumenten actief kiezen voor internettoepassingen die geen gevoelige data opslaan en doorverkopen. Het is niet volgens Hofmann et al. (2017) niet onlogisch dat men kijkt naar zelfregulatie als oplossing om orde op zaken te krijgen op het internet. Hofmann et al. (2017) stellen dat regulatie zich kenmerkt door opzettelijke en doelgerichte interventies in een beleidsdomein, met het doel het gedrag van anderen te beïnvloeden. Regulering kan hierdoor meerdere vormen aannemen zoals: wetgeving, particuliere zelfregulering of regelingen met meerdere actoren; in alle gevallen echter verbindt het processen met expliciete doelstellingen en maatregelen (Hofmann et al., 2017). Volgens Medzini (2021) doet zelfregulering zich pas voor wanneer beleidsmakers het initiatief beginnen te nemen tot het opstellen van een wetgeving, bijvoorbeeld als er geen bestaande wetten zijn, of als regelgevers dreigen met uitvoerende besluiten. Wanneer de overheid meer concrete regels zou opstellen, of hier zelf nog maar mee zou dreigen, is het mogelijk dat de sector hierop anticipeert en zichzelf begint te reguleren (Medzini, 2021). Zelfregulatie door bedrijven die het metaversum uitbaten, is zeker een stap in de goede richting maar is echter niet voldoende. Zo toonde de bestaande literatuur aan dat de grote vrijheid van de gebruikers, het metaversum gevaarlijker maakt dan de bestaande onlinediensten en games (Kye et al., 2021). Hoewel deze vrijheid enerzijds een voordeel is van het metaversum op vlak van beleving, vormt dit ook een vraagstuk op vlak van privacybescherming. Volgens Kye et al. (2021) kunnen de beheerders van het metaversum niet alle handelingen van gebruikers voorspellen. Dit lijkt een positief aspect op vlak van privacy maar zorgt voor een vermindering in gebruikersveiligheid. Dit is volgens Dobbelare-Welvaert (2020) een vraagstuk waar ook de fysieke wereld mee worstelt. Enerzijds willen we meer privacy en anderzijds willen we meer camera's om criminelen af te schrikken of om mensen terug te vinden (Dobbelare-Welvaert, 2020).

De bedrijven die het metaversum zullen uitbaten, zijn verantwoordelijk voor de werking van het product. Net zoals bij de sociale media platformen van vandaag, zullen de metaverse

platformen van morgen zich actief moeten bezighouden met het modereren van inhoud die op hun platformen verschijnt (Rosenberg, 2021b). Hoe deze moderatie binnen dit soort platformen het best wordt gedaan, is interessant voor vervolgonderzoek. De regulering van virtuele werelden vergt volgens Antonio Chavez-Aguayo (2009) een andere manier van denken. Hierbij moeten nieuwe paradigma's gevormd worden die alle regels controleren, maar niet beperken om het interactieniveau hoog te houden en anarchie te voorkomen (Antonio Chavez-Aguayo, 2009). Op vlak van privacy is het belangrijk dat de uitbaters actief controleren of mensen geen slechte intenties hebben op het platform. Dit aangezien in het metaversum meer details worden gebruikt waardoor het gemakkelijker is voor derden om deze informatie te gebruiken om identiteit te stelen (Jain et al., 2021). Hiervoor moet men volgens Dhelim et al. (2022) multifactoriële identificatie voor de metaverse-gebruikers implementeren, om de veiligheid en privacy van de eindgebruikers en hun avatars te verzekeren. Gebruikersveiligheid, met het oog op privacy is dus een belangrijk aspect dat de uitbaters zelf zullen moeten waarborgen. De kans dat gebruikers van het platform gaan wegstappen doordat er geen veiligheidsgevoel heerst op het platform, lijkt groter dan dat het platform zal worden verlaten doordat de Big data onbewust wordt verkocht (Antonio Chavez-Aguayo, 2009; Dhelim et al., 2022; Jain et al., 2021). Dit kan worden verklaard doordat de emoties binnen het metaverse als echt worden ervaren (de Graaf, 2016). Door de immersieve technologieën zullen deze negatieve emoties onder volledig bewustzijn worden ervaren en onthouden (de Graaf, 2016). In tegenstelling tot de fysieke wereld zou anarchie in het metaversum betekenen dat er wordt overgestapt naar een ander metaversum (Antonio Chavez-Aguayo, 2009). Dit is een verschil met onze fysieke wereld waar er weinig alternatieven zijn voor zij die zich niet vinden in de maatschappelijke wetten. In het kader van winstbejag zou een lage gebruikersveiligheid in een metaversum geen goede zaak zijn voor het bedrijf erachter. Dit soort reputatieschade kan volgens Medzini (2021) een drijfveer vormen voor de sector om een striktere zelfregulatie toe te passen.

Naast het zich houden aan de bestaande privacywetten en de eventuele zelfregulatie, moeten bedrijven ook in staat zijn hun persoonlijk verzamelde data te beschermen. Aanvallen van hackers zouden volgens de GDPR-regelgeving moeten worden tegengehouden aangezien deze verplicht op een veilige manier moeten worden opgeslagen (zie supra, '6.1.1'). Onbevoegden zouden geen toegang mogen hebben tot de data. Het is dus ook belangrijk dat er een grondige analyse gebeurt over de derden aan wie de data wordt doorverkocht. Aangezien hackers zich altijd zullen richten op de zwakste schakel van de ketting (zie supra, '4. Big data'). Hoewel een bedrijf als bijvoorbeeld Meta veel ervaring heeft met het veilig opslaan van persoonlijke gegevens, is het gegeven dat het metaversum zich in *real time* afspeelt een groot verschil tussen het metaversum en de traditionele sociale media platformen (Verrycken, 2022). Door de tijdsafhankelijke aard van de

gegevensstromen binnen het metaversum, zijn de veiligheidsproblemen groter tijdens de piek van het gegevensverkeer (Ksherti, 2014). Het kan organisaties bijvoorbeeld ontbreken aan mogelijkheden om enorme hoeveelheden gegevens veilig op te slaan en de verzamelde gegevens te beheren tijdens deze pieken (Kshetri, 2014). Ook Haugen, de voormalige productmanager bij Facebook, stelt luidop de vraag hoe Meta zijn metaversum wil uitbaten als het vandaag al moeilijk heeft om de eenduidige platformen die het controleert veilig te houden (Verrycken, 2022). Vervolgonderzoek over de manier waarop het metaversum zal worden beveiligd, is derhalve interessant.

Volgens Jain et al. (2021) is het bijkomend belangrijk dat gebruikers zich op de hoogte stellen van de privacy- en veiligheidsinstellingen van de verschillende sociale media platforms die ze gebruiken. Echter is dit net zoals de *Terms of agreement* geen sinecure. Dit komt doordat de privacy-instellingen die digitale dienstverleners als standaard aanbieden, niet als zodanig moeten worden overgenomen (Jain et al., 2021). Hierdoor heeft elk platform zijn eigen privacy- en beveiligingsinstellingen, waarmee de gebruiker kan beperken wie en welke groepen de verschillende aspecten van het profiel van de gebruiker kunnen zien. (Jain et al., 2021). Standaardinstellingen, die op elk platform hetzelfde zijn, zouden een mogelijke oplossing kunnen bieden om deze opgave voor de eindgebruiker te vereenvoudigen en zo het bewustzijn verhogen. Het opleggen van deze standaarden zou kunnen door zelfregulatie binnen de sector of door de overheid (Medzini, 2021).

6.1.5 De burgergemeenschap

Als laatste maar zeker niet onbelangrijkste, vormen de eindgebruikers zelf een belangrijke partij op vlak van privacy binnen het metaversum. Hoewel deze groep net beschermd zou moeten worden, kan deze groep ook zelf een rol van betekenis spelen op vlak van regelgeving. Enerzijds kan deze groep een grote impact hebben op de noodzaak tot regelgeving, door het bewustzijn te vergroten rond privacy (zie supra, '5. Privacy'). Anderzijds zorgt het metaversum voor een verhoging van de connectiviteit tussen de burgers onderling (zie supra, '3.4'). Hierdoor zal de traditionele territoriale logica van de politie opnieuw worden uitgedaagd (Easton, 2019). Volgens Easton (2019) is het hierbij belangrijk dat er meer rekening wordt gehouden met de verwachtingen van de burgers, aangezien dit de kern moet zijn van de gemeenschapsgerichte politiezorg.

Dobbelaere-Welvaert (2020) stelt dat er een groeiend bewustzijn rond digitale privacy heerst, waardoor dit onderwerp jaar na jaar relevanter en belangrijker wordt. Dit lijkt te kloppen wanneer wordt gekeken naar een onderzoek uit 2011 dat in Europa werd uitgevoerd onder de naam 'Special Eurobarometer 359'. Hieruit kwam naar voren dat 74 procent van de Europeanen het als normaal aanschouwt dat persoonlijke informatie zomaar wordt verspreid (2011). De belangrijkste reden voor consumenten om hun data te delen was om toegang te verkrijgen tot een onlinedienst (Special Eurobarometer 359, 2011). Zowel voor gebruikers van sociale netwerken als voor online shoppers (Special Eurobarometer 359, 2011). Destijds gaf 70 procent van de bevraagde Europeanen aan, zich zorgen te maken dat de verzamelde data gebruikt worden voor andere doeleinden dan die waarvoor ze waren opgeslagen (Special Eurobarometer 359, 2011). Uit een meer recent onderzoek van Janrain in 2018, met meer dan duizend Amerikaanse consumenten, blijkt dat 91 procent van de deelnemers pleit voor meer controle over hun data (Dongleur, 2019; Sterling, 2018). Er wordt geopperd dat de overheid moet ingrijpen via wetten omtrent privacy, beveiliging en het bezitten van persoonlijke data. Het onderzoek wijst uit dat de meerderheid van de respondenten bereid is om persoonlijke gegevens uit te wisselen in ruil voor een vorm van waarde voor de eindgebruiker (Sterling, 2018). Hierbij speelt de inhoud van data een belangrijke rol (Sterling, 2018). Zo blijkt financiële informatie veel gevoeliger te zijn dan bijvoorbeeld medische voorgeschiedenis of privé conversaties (Sterling, 2018). Tot slot gaf 36 procent aan dat het niet toestaat dat een bedrijf hun persoonlijke gegevens zou gebruiken (Sterling, 2018). Een manier waarop privacy bewuste consumenten hun privacy kunnen beschermen, is door een vergoeding te betalen om uit de database van het bedrijf te verdwijnen (Montes et al., 2015). Deze 'privacy kost' kan worden geïnterpreteerd als de moeite die consumenten besteden om hun acties online te verbergen (Montes, Sand-Zantman, & Valletti, 2015).

Tot nog toe waren tussenpersonen nodig om zaken te controleren tussen burgers. Denk maar aan de rol van banken bij transacties, de rol van notarissen bij de verkoop van vastgoed, de rol van politie bij interventies of de rol van een rechter bij het bepalen van een strafmaat. Binnen de digitale wereld uit zich dit door de rol van banken voor digitale transacties, moderatie door de platformontwikkelaars, wetten aan de hand van gebruikersovereenkomsten door de platformontwikkelaars en het opsporen van misdaden door de overheid via de politie. Volgens aanhangers van een gedecentraliseerd internet zou de blockchaintechnologie helpen bij het wegwerken van sommige tussenpersonen (Dey et al., 2022) (zie supra, '3.6.1.2'). Hierdoor zou de Web 3.0 revolutie mogelijks de poorten kunnen openzetten tot een nieuwe manier van regelgeving en ordehandhaving. Het meest gekende voorbeeld hiervan is de digitale munt '*Bitcoin'* waarbij de noodzaak van een controlerend orgaan zoals de bank, wegvalt.

6.1.5.1 Toepassingen blockchain voor burgergemeenschap

De toepassing van blockchaintechnologie is niet alleen beperkt tot digitale munten zoals *Bitcoin* (Dey et al., 2022). De blockchain is reeds nuttig gebleken bij het toekennen van de herkomst van documenten, het traceren van eigendom, digitale activa, fysieke activa en stemrechten (Dey et al., 2022). Via de blockchaintechnologie kan worden aangetoond wie de eigenaar is van een digitaal voorwerp (Nakamoto, 2009). Door de noodzaak om een eigenaar aan te duiden van digitale goederen, zagen de *non-fungible tokens* of NFT's in 2014 het levenslicht (Liu et al., 2022). Een NFT is een virtueel niet-vervangbaar eigendomscertificaat (Van der Haegen et al., 2022). Het is een *token* dat wordt gekoppeld een aan digitaal goed, waar vaak een waarde aan wordt gehangen door middel van een digitale munt (Liu et al., 2022). Het komt erop neer dat elke NFT staat voor een voorwerp en een beschrijving van het voorwerp, zoals de eigenaar en de waarde. Deze staan opgeslagen in de blockchain waardoor het, net zoals de digitale munten, automatisch beveiligd is (Liu et al., 2022). Door gebruik te maken van NFT kunnen makers gemakkelijk het eigendom aantonen van onder andere 'foto's', 'video's' en 'kunstwerken', zodat intellectuele eigendomsrechten goed beschermd kunnen worden (Liu et al., 2022). Deze toepassing van de blockchain, maakt het dus mogelijk voor gebruikers om binnen een digitale wereld onderling te bepalen aan wie de zaken toebehoren. Dit wordt bereikt door de implementatie van code als wet: autonome regels die worden uitgevaardigd zonder dat menselijke interpretatie nodig is (Corballis & Soar, 2022). Deze technologie stelt de consumenten bijgevolg in staat om een volledig virtuele economie uit de bouwen waar virtuele goederen kunnen verhandeld worden zonder supervisie (Van der Haegen et al., 2022). Omdat geen enkele platform ontwikkelaar de enige eigenaar zal zijn van de

metaverse, verwacht ook Gartner dat deze een virtuele economie zal hebben die mogelijk wordt gemaakt door digitale valuta en niet-fungibele tokens (NFT's). Het metaversum zal volgens Gartner (2022) uiteindelijk zelfs een mogelijke invloed hebben op elk bedrijf waarmee consumenten dagelijks in aanraking komen.

6.1.5.2 Privacy toepassing blockchain voor de eindgebruikers

Het interessante aspect van de blockchain, op vlak van Big data en privacy, is dat het mogelijks gebruikt kan worden om de eindgebruiker terug eigenaar te laten worden van diens data. Volgens Renwick & Gleasure (2021) hebben de Blockchain-technologieën zich ontwikkeld van anti-establishment digitale munteenheden, die buiten de reguliere financiële systemen opereren, tot een revolutionaire technologische blauwdruk voor gedistribueerde computerarchitecturen. Het is een ontwerp van hoe men eigendom kan toekennen zonder nood aan een tussenpersoon. Het is vandaar niet onlogisch dat gekeken wordt hoe de principes van de blockchain kunnen worden doorgetrokken om consumenten terug de macht te geven over hun persoonlijke gegevens (Renwick & Gleasure, 2021). Hierbij zou de eindgebruiker, over metaverses heen, via de blockchain als eigenaar worden bestempeld van diens persoonlijke data. Bedrijven zouden deze data dan niet zomaar mogen doorverkopen nog raadplegen zonder toestemming van de eigenaar (Renwick & Gleasure, 2021). Deze visie is in sommige opzichten aanlokkelijk omdat het de gebruikers hun eigen individuele soevereiniteit belooft (Corballis & Soar, 2022).

Er zijn natuurlijk ook nadelen aan deze blockchaintechnologie. Onder het mom van volkssoevereiniteit en meer privacy wordt er vaak opgeroepen om meer gebruik te maken van de blockchain-technologieën (Corballis & Soar, 2022). Volgens Corballis en Soar (2022) is het belangrijk om uiterst sceptisch te staan tegenover de utopische beweringen rond de blockchain aangezien het eerst duidelijk moet zijn wiens belangen zo'n ideologisch project precies dient. Vandaag de dag wordt de blockchain al te vaak gepromoot om de eerste speculanten financieel te bevoordelen (Corballis & Soar, 2022). Bijkomend zien huidige toezichthouders het gebrek aan controle rond blockchain als een potentiële blinde vlek voor criminele activiteiten zoals het witwassen van geld en de financiering van terrorisme (Renwick & Gleasure, 2021). Tot slot bedreigt één zwakte in een technologie het hele systeem (zie supra, ‘4. Big data’). Aangezien het metaversum gebruik zou maken van vele technologieën zijn er dus meerdere mogelijkheden voor hackers om binnen te dringen (Dhelim et al., 2022). Dhelim et al. (2022) stellen dat publieke blockchain transacties van aankopen van digitale activa, kunnen worden geanalyseerd om de identiteit van de kopers en verkopers te raden. Het is dus mogelijk dat deze technologie niet onfeilbaar is wat een gouden kans geeft aan privacy indringers en hackers om slachtoffers te maken (Dhelim et al., 2022).

7 Discussie

7.1 Bevindingen van het onderzoek

Het metaversum kan de manier waarop sociale interactie via het internet verloopt, heruitvinden. Het gaat over een platform dat net zoals het internet in staat is om mensen van over de helen wereld te verbinden, waarbij het gevoel wordt gecreëerd dat de gebruikers 'echt' bij elkaar zijn. Het grote verschil met de huidige sociale media is dat deze virtuele wereld niet langer beperkt wordt door de mogelijkheden van een traditioneel scherm, maar gebruik maakt van draagbare sensoren en andere slimme apparaten (Shen et al., 2021). Bijkomend zal de gebruikservaring berusten op technologieën die de bezoekers van het metaversum willen onderdompelen in een virtuele realiteit door middel van waargenomen immersie. Door de extra sensoren en door de immersieve technologieën wordt verwacht dat de eindgebruikers onbewust meer gevoelige informatie zullen vrijgegeven (Rosenberg, 2022). Volgens de literatuur is het niet ondenkbaar dat deze nieuwe en mogelijks gevoeligere data leidt tot een schending van de persoonlijke levenssfeer, waardoor er vragen rijzen rond de regulatie van deze digitale platformen (Rosenberg, 2022). Om de onderzoeksvraag te beantwoorden, wordt gekeken welke partijen vandaag de dag trachten de digitale privacy te waarborgen.

Vandaag de dag zijn de huidige bedrijfsmodellen van sociale internetplatformen voornamelijk gebouwd rond het verzamelen en gebruiken van persoonlijke gegevens (Jain et al., 2021). Hierdoor is het mogelijk dat de grotere hoeveelheid van de soms gevoelige data uit het metaversum, zal worden gebruikt om hogere winsten te maken (Amaizu et al., 2022). De grootste angst hierbij is een mogelijke openbaring van gevoelige informatie of het misbruiken van deze informatie, wat een duidelijke inbreuk vormt op de privacy van de gebruikers van het metaversum (Rosenberg, 2022). Vanwege deze reden is het belangrijk dat de mate waarin bedrijven hun klanten in het metaversum monitoren, wordt beperkt.

Er is volgens dit onderzoek nood aan meer bewustzijn rond privacy en de gevaren van big data. Bij het afstaan van data maakt het namelijk niet uit wie of wat je bent, het draait om wat de algoritmes bepalen. Deze algoritmes zijn in staat om, na het verzamelen en analyseren van de data, gevoelige persoonlijke eigenschappen te voorspellen (Kshetri, 2014; Romansky & Noninska, 2020). Het is volgens dit onderzoek ethisch niet correct om mensen in te delen in groepen op basis van verzameld digitaal gedrag. Net zoals het niet strafbaar is om toevallig dezelfde dingen te *liken* op Facebook als iemand die een misdrijf

heeft gepleegd. Een gepaste regulering dringt zich op omtrent het verzamelen van dit soort gegevens, die in staat is om mee te gaan met de snelheid van technologische nieuwigheden. Om tot een gemeenschappelijke visie rond privacy en de regulering hiervan te komen, moeten volgens Renwick & Gleasure (2021) meerdere partijen onderhandelen over wat aanvaardbaar is.

Echter zijn er meerdere factoren die het bemoeilijken om deze dataverzameling te reguleren. Zo is privacy enerzijds een subjectief begrip dat moeilijk te definiëren noch te meten valt (Renwick & Gleasure, 2021). Anderzijds zijn veel mensen bereid hun persoonlijke levenssfeer op te geven als onderdeel van het gehanteerde bedrijfsmodel of verschilt de behoefte aan privacy door culturele verschillen (Renwick & Gleasure, 2021). Tot slot heerst er nog onduidelijkheid rond de bevoegde entiteiten die de dataverzameling moeten reguleren (Park & Kim, 2022; Renwick & Gleasure, 2021; Rosenberg, 2022; Shen et al., 2021). Mede hierdoor is het niet vanzelfsprekend dat publieke instanties alleen zullen waken over de digitale privacy van hun burgers.

Het waarborgen van een passende bescherming rond elektronische persoonsgegevens over de grenzen heen, wordt vandaag de dag geregeld door overheden (Hofmann et al., 2017). Dit gebeurt aan de hand van wetten die trachten de inwoners hun privacy te waarborgen. Zo worden de Belgische consumenten vandaag de dag voornamelijk beschermd door de Europese GDPR-wetgeving. Echter is het niet gemakkelijk om internationale wetten op te stellen rond privacy vanwege het mondiale karakter van het metaversum (Meltzer, 2015). Bijkomend verschilt de aanpak van landen onderling om privacy te reguleren, doordat er culturele verschillen heersen rond privacy en het belang ervan (Renwick & Gleasure, 2021). De laatste jaren gaan de technologische veranderingen veel te snel om dit als overheid te kunnen bijhouden, waardoor de wetten die hierop volgen te traag en niet adequaat genoeg zijn (Buttarelli, 2019; Gruschka et al., 2018; Kshetri, 2014). Bijkomend bracht de literatuur naar voren dat overheden vaak technologieën in de beginfase niet willen beperken uit schrik de ontwikkeling ervan af te remmen (Renwick & Gleasure, 2021). Hierdoor blijken overheden niet altijd de ideale toezichthouder op vlak van digitale privacy. Tot slot stelt Ksherti (2014) dat overheden ook zelf belanghebbende partijen zijn op vlak van Big data, aangezien overheden zelf data verzamelen om overheidsdiensten te verbeteren.

Internetoperatoren hangen vast aan de wetten die de publieke instanties zoals België of Europa opleggen (Meltzer, 2015). De macht van een overheid ten aanzien van deze operatoren is groot aangezien de operatoren zonder toestemming niet kunnen opereren binnen een grondgebied (Obar, 2022). Op vlak van dataverzameling is deze partij gebonden aan de wetten die het land of de regio oplegt. Desalniettemin zouden deze partijen

transparanter mogen zijn op vlak van hun privacy standaarden (Obar, 2022). Operatoren geven volgens dit onderzoek niet genoeg details over de data die ze bijhouden. Het ontbreken van transparantie leidt ertoe dat consumenten minder bewust zijn over vormen van privacyschending (Jain et al., 2021; Rosenberg, 2022).

Verder lijken de makers van het internet niet in staat privacy te waarborgen omwille van de duidelijke scheidingslijn tussen het oorspronkelijke Web 1.0 en het huidige Web 2.0 / Web 3.0 (Ankerson, 2015; Ozcinar et al., 2020).

De bedrijven die het metaversum uitbaten en het bedrijfsmodel dat deze hanteren, zullen volgens dit onderzoek grotendeels bepalen hoezeer de persoonlijke gegevens van hun eindgebruikers worden verzameld en bewaakt. Het onderzoek wijst uit dat de bedrijven enerzijds de Big data kunnen gebruiken om via algoritmes mensen te classificeren op basis van voorspellingen (Kshetri, 2014). Anderzijds heerst er het gevaar dat deze gevoelige data in verkeerde handen valt (Jain et al., 2021). Hoewel bedrijven onderhevig zijn aan de wetten die hun eindgebruikers beschermen, slagen deze er soms toch in om deze wetten te omzeilen. Dit valt op wanneer er wordt gekeken naar de GDPR-wet, die de belangrijkste wetgeving vormt rond datagebruik door private bedrijven. De GDPR-wet kan bijvoorbeeld worden omzeild door de juridische verantwoordelijkheid in de schoenen van de consumenten te schuiven (Dobbelaere-Welvaert, 2020). Deze theoretisch gezien legale praktijk gebeurt aan de hand van *pop-up* berichten die vragen om de voorwaarden te accepteren (Buttarelli, 2019). Het is volgens dit onderzoek dan ook duidelijk dat overheden niet in staat zijn om aan dezelfde snelheid te handelen als de Big Techreuzen (Buttarelli, 2019; Gruschka et al., 2018; Kshetri, 2014). Uit het onderzoeken van de literatuur blijkt dat deze bedrijven er baat bij hebben om aan zelfregulatie te doen (Medzini, 2021). Bedrijven of hele sectoren doen dit door zelf regels en procedures in te voeren en toe te passen (Medzini, 2021). Dit kan volgens Medzini (2021) onethische praktijken verhelpen en de reputatie van het bedrijf of de sector positief beïnvloeden.

Langs de andere kant komt in dit onderzoek naar voren dat er meerdere mogelijke problemen dreigen in het metaversum zoals bijvoorbeeld verbondenheid, gebruikersveiligheid en beveiliging (Blieszner et al., 2019; de Graaf, 2016; Dhelim et al., 2022; Jain et al., 2021; Kye et al., 2021). Hierdoor moeten bedrijven, die instaan voor de gebruikersveiligheid op hun platform, sommige handelingen van hun gebruikers kunnen controleren (Kye et al., 2021). Het is dus niet eenvoudig om privacy te waarborgen aangezien data een essentiële rol vervult op vlak van ordehandhaving in een digitale wereld (Kye et al., 2021). Volgens de GDPR-wetgeving moet in deze gevallen de data veilig worden opgeslagen en zou deze data enkel mogen gebruikt worden om de gebruikerservaring te

verhogen. Na het analyseren van de bestaande literatuur blijkt dat ook voor deze gevallen zelfregulatie een belangrijk aspect vormt, aangezien wetten zich vaak niet uitspreken over welke manier het veiligst is om data te bewaren en welke data mag worden bewaard (Jain et al., 2021; Medzini, 2021). Bedrijven vormen bijgevolg, naast de overheid, belangrijke partijen die privacy kunnen waarborgen binnen een digitale wereld. Volgens Medzini (2021) komen initiatieven rond zelfregulatie sneller tot stand wanneer publieke instanties meer concrete regels opstellen of dreigen dit te doen.

Hoewel de eindgebruikers op vlak van privacy de groep vormen waarvan de data moet worden beschermd met het oog op privacy, toont de literatuur aan dat deze actor meer is dan alleen het lijdend voorwerp. Volgens dit onderzoek is het belangrijk dat het bewustzijn rond digitale privacy wordt vergroot binnen de burgergemeenschap. Hierdoor wordt de druk vergroot op overheden om met maatregelen te komen voor de bedrijven die misbruik maken van ongeïnformeerde eindgebruikers (Medzini, 2021). Digitale privacy gaat namelijk over meer dan alleen de zoekgeschiedenis van gebruikers. Het waarborgen van een digitale persoonlijke levenssfeer gaat ook over het worden beschermd tegen algoritmes die op basis van patroonherkenning consumenten onbewust indelen in categorieën. Digitale discriminatie ten gevolge van gevoelige data die wordt geraden door algoritmes, is een mogelijk gevaar van Big data misbruik waar elke internetgebruiker zich tegen moet verzetten alvorens het te laat is (Kshetri, 2014). Hoewel dit soort algoritmes volgens de literatuur vandaag de dag theoretisch al mogelijk zijn, kan het metaversum met nieuwe additionele data hier een stroomversnelling aan geven (Rosenberg, 2022). Volgens de literatuur is het mede door het ontbreken van een bewustzijn rond privacy, dat de huidige bedrijfsmodellen van sociale media gebouwd zijn rond dataverzameling (Jain et al., 2021; Pasquale, 2014). Volgens Montes et al. (2015) zouden bedrijven de mogelijkheid moeten bieden, aan privacy bewuste consumenten, om een vergoeding te betalen met als doel de verzamelde gegevens te laten verdwijnen uit de database van een bedrijf. Verder suggereert de literatuur dat het niet eenvoudig is om als internetgebruiker te begrijpen hoe men zijn eigen digitale privacy kan waarborgen op verschillende internetplatformen (Jain et al., 2021). Dit komt doordat elk platform zijn eigen privacy- en beveiligingsinstellingen heeft. Om dit probleem te verhelpen, zouden overheden de platformuitbaters kunnen verplichten tot de invoering van standaardinstellingen die op vlak van privacy en beveiliging overal gelijk en eenvoudig te wijzigen zijn. Een internationale publiek orgaan, zou hiervoor de geschikte partij zijn om dit in te voeren. Tot slot hoeft het verhandelen van data op een transparante manier, met het oog op het verbeteren van externe diensten, niet altijd de privacy van een consument te schenden (Romansky & Noninska, 2020). Zo tonen de onderzoeken van Corballis & Soar (2022) en Renwick & Gleasure (2021) aan dat sommige consumenten wel degelijk hun data willen omruilen voor een gratis digitale dienstverlening. Om deze consumenten terug

eigenaar te maken van deze data, zijn er mogelijkheden om de blockchaintechnologie hiervoor te gebruiken (Renwick & Gleasure, 2021). De grootste troeven hierbij zijn dat deze technologie veilig is en tussenpersonen overbodig maakt. Echter is er nog niet voldoende bewijs dat de blockchain hiervoor het beste middel is. Toetsend vervolgonderzoek hieromtrent is aangewezen, alvorens hierover oordelen kunnen worden geveld.

7.2 Beperkingen van het onderzoek

De bevindingen van dit onderzoek helpen bij het zoeken naar een verklaring waarom privacy waarborgen binnen het metaversum zo moeilijk is. Echter biedt het geen oplossing over hoe dit probleem kan worden opgelost. De verklaring hiervoor kan liggen bij het feit dat het metaversum nog in opbouw is, waardoor het onderzoek naar regulatie binnen een metaversum in de beginfase zit. Hoewel er reeds veel literatuur bestaat rond de gevaren van privacy en Big data, zijn er maar een gering aantal onderzoeken naar de mogelijke impact van het metaversum hierop en de regulatie ervan. Volgens De Pelsmacker en Van Kenhove (2014) is het niet mogelijk om een conclusief onderzoek te voeren wanneer de onderzoeker niet in staat is een aantal concrete hypothesen te formuleren. Hierdoor is zo een onderzoek eerder exploratief, waarbij wordt nagegaan welke cruciale aspecten van het probleem in aanmerking komen voor vervolgonderzoek (De Pelsmacker & Van Kenhove, 2014). Deze cruciale problemen voor vervolgonderzoek rond het metaversum, werden toegevoegd aan de conclusie (zie infra, ‘7.3’).

Door de beperkte beschikbaarheid van publicaties rond privacy een regulatie van het metaversum, werden deze aangevuld met onderzoeken over Big data en de huidige manier van regulatie hiervan. Liberati et al. (2009) stellen dat dit soort aanvullingen binnen een SLR mogelijk zijn, maar dat deze kunnen zorgen voor een verlaagde transparantie en openheid van het onderzoek. Om hierop een antwoord te bieden, werden alle gebruikte bronnen met hun hoofdargumenten verzameld en als bijlage toegevoegd aan dit document (zie Bijlage 1).

Tot slot is privacy op zich een subjectief begrip (zie supra, ‘5. Privacy’). Hierdoor is het moeilijk om het begrip eenduidig te definiëren, laat staan het te meten (Renwick & Gleasure, 2021). Volgens Liberati et al. (2009) kunnen beoordelaars hierdoor oordelen dat het zinloos is om meerdere onderzoeken over een subjectief onderwerp als privacy te combineren. De beslissing om gegevens al dan niet te combineren is een methodologische component die niet per se juist of fout hoeft te zijn (Liberati et al., 2009). Aangezien de keuze subjectief is, moeten auteurs volgens Liberati et al. (2009) echter transparant zijn over hun beslissingen en deze voor de lezers beschrijven.

7.3 Conclusie

Deze thesis zoekt een antwoord op de vraag: ‘Welke partijen zijn in staat privacy te waarborgen binnen het metaversum?’. Dit onderzoek bekijkt aan de ene kan hoe het metaversum aan de hand van data de privacy kan schenden. Langs de andere kant kijkt het naar de rol die overheden, internetoperatoren, de makers van het internet, de ontwikkelaars van het metaversum en de eindgebruikers zelf kunnen spelen op vlak van de regulatie van datagebruik uit het metaversum. Hiervoor werd de huidige literatuur bestudeerd aan de hand van een systematische literatuuranalyse. Uit de bevindingen van het onderzoek komt naar voren dat het waarborgen van privacy in een digitale wereld moeilijk door één alleenstaande partij kan worden georganiseerd. Publieke instanties zijn over het algemeen traag in het stemmen en invoeren van wetten of hebben schrik om zo innovatie in de weg te staan en hierdoor competitiviteit ten opzichte van andere landen te verliezen. Bedrijven zien in het gebruiken van data een lucratieve opbrengst, en de consument ligt niet wakker van het feit dat hun data wordt gebruikt. Vanwege de verwachting dat het metaversum extra data in omloop zal brengen, zal het waarborgen van de eindgebruikers hun privacy mogelijks nog moeilijker zijn dan nu het geval is bij de sociale netwerken.

Op basis van de literatuur lijkt een stijging van het bewustzijn rond de gevaren van Big data door de eindgebruikers, een mogelijke eerste stap te kunnen zijn in de goede richting. Hierdoor zouden bedrijven die de privacy niet respecteren simpelweg worden genegeerd door de consumenten die makkelijk kunnen overstappen tussen de verschillende metaversums. Een bedrijf of een hele sector wordt namelijk in staat geacht zich sneller dan overheidsinstanties te kunnen aanpassen aan de nieuwste technologische updates. Hierdoor zou het verzamelen van Big data voornamelijk moeten gebeuren door een gekozen transparante koers van een bedrijf dat onderhevig is aan zelfregulatie. Om ervoor te zorgen dat deze zelfregulering adequaat en transparant gebeurt, is er uiteraard meer nodig dan een grotere druk van de bevolking. De overheid speelt ook een grote rol in het voorzien van een externe motivatie voor bedrijven om zichzelf te reguleren op vlak van een inkomstenbron zoals data. Er is nood aan een globale instantie met soevereiniteit die meer concrete regels opstelt, of hiermee dreigt. Bijkomend heeft een overheid ook de middelen om zijn bevolking te sensibiliseren rond de gevaren van Big data en de noodzaak van digitale privacy. In de toekomst wordt het belangrijk dat iedereen op de hoogte wordt gesteld over de gevaren van Big data waardoor deze bovenbeschreven wisselwerking in stand kan worden gehouden.

Tot slot benadrukt dit onderzoek dat het belangrijk is om verder te na te gaan hoe de eindgebruikers meer zeggenschap kunnen verwerven over hun data. Nieuwe innovaties zoals het gebruiken van de blockchaintechnologie om deze kwestie op te lossen, zijn

bijgevolg interessant voor vervolgonderzoek. Aanvullend zijn er mogelijks meerdere problemen waarmee het metaversum dreigt de kampen. Zo zijn er naast digitale privacy in het metaversum uitdagingen rond sociale aspecten zoals inclusiviteit, gebruikersveiligheid, beveiliging, gezondheid en ecologie; die zeker nog moeten worden onderzocht.

BIBLIOGRAFIE

Almarzouqi, A., Aburayya, A., & Salloum, S. A. (2022). Prediction of User's Intention to Use Metaverse System in Medical Education: A Hybrid SEM-ML Learning Approach. IEEE ACCESS, 10, 43421–43434. https://doi.org/10.1109/ACCESS.2022.3169285

Amaizu, G., Njoku, J., Lee, J. M., & Kim, D.-S. (2022). Security in Metaverse: A Closer Look.

Ankerson, M. S. (2015). Social Media and the ``Read-Only'' Web: Reconfiguring Social Logics and Historical Boundaries. SOCIAL MEDIA + SOCIETY, 1(2). https://doi.org/10.1177/2056305115621935

Antonio Chavez-Aguayo, M. (2009). Democratization of Creativity and Cultural Production in Virtual Worlds: A new Challenge for Regulation and Cultural Management. In M. Pivec (Ed.), PROCEEDINGS OF THE 3RD EUROPEAN CONFERENCE ON GAMES BASED LEARNING (pp. 103–109).

Benhaddi, M. (2017). Web of Goals: A Proposal for a New Highly Smart Web. In S. Hammoudi, M. Smialek, O. Camp, & J. Filipe (Eds.), ICEIS: PROCEEDINGS OF THE 19TH INTERNATIONAL CONFERENCE ON ENTERPRISE INFORMATION SYSTEMS - VOL 2 (pp. 687–694). https://doi.org/10.5220/0006250306870694

Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., Libert, T., & Shadbolt, N. (2018). Third Party Tracking in the Mobile Ecosystem. Reuters Institute for the Study of Journalism, (pp. 1-9). Department of Computer Science, University of Oxford.

Bleier, A., & Eisenbeiss, M. (2015). Personalized Online Advertising Effectiveness: The Interplay of What, When, and Where. Marketing Science.

Bleier, A., Goldfarb, A., & Tucker, C. (2020). Consumer privacy and the future of data-based innovation and marketing. International Journal of Research in Marketing, 37. https://doi.org/10.1016/j.ijresmar.2020.03.006

Blieszner, R., Ogletree, A., & Adams, R. (2019). Friendship in Later Life: A Research Agenda. Innovation in Aging, 3. https://doi.org/10.1093/geroni/igz005

Boone, W., Martinez, C. D., Pasiunaite, G., & Agbor, D. A. (2020). News Aggregation and Personalization in Google News: Privacy Impact Assessment. KU Leuven: Privacy and Big data (B-KUL-H00Y2A).

Bremmer, I. (2022). Zonder tegenmaatregelen zal technologie de politieke wereld verder verdelen in 2022. De Tijd. Geraadpleegd op 23 mei 2022, via: https://www.tijd.be/opinie/analyse/technologie-polariseert-de-wereld/10357877

Casanovas, P., De Koker, L., Mendelson, D., & Watts, D. (2017). Regulation of Big Data: Perspectives on strategy, policy, law and privacy. HEALTH AND TECHNOLOGY, 7(4), 335–349. https://doi.org/10.1007/s12553-017-0190-6

Coltman, T. (2007). Why build a customer relationship management capability? The Journal of Strategic Information Systems, pp. 301-320.

Corballis, T., & Soar, M. (2022). Utopia of abstraction: Digital organizations and the promise of sovereignty. BIG DATA \& SOCIETY, 9(1). https://doi.org/10.1177/20539517221084587

Cripps, J., & Stermac, L. (2018). Cyber-Sexual Violence and Negative Emotional States among Women in a Canadian University. INTERNATIONAL JOURNAL OF CYBER CRIMINOLOGY, 12(1), 171–186. https://doi.org/10.5281/zenodo.1467891

de Graaf, H. (2016). Social inclusion through Games and VR Use of games and virtual worlds to strengthen the personal `real life' social network of people who are challenged in that area. 2016 8TH INTERNATIONAL CONFERENCE ON GAMES AND VIRTUAL WORLDS FOR SERIOUS APPLICATIONS (VS-GAMES).

De Pelsmacker, P., & Van Kenhove, P. (2014). Marktonderzoek: methoden en toepassingen (4th ed.), Amsterdam, Nederland: Pearson Education Benelux.

De Raedt, S. (2016). Hoofdstuk 5 recht op privéleven . (pp. 1-31). Universiteit Gent.

Dey, S., Saha, S., Singh, A. K., & McDonald-Maier, K. (2022). SmartNoshWaste: Using Blockchain, Machine Learning, Cloud Computing and QR Code to Reduce Food Waste in Decentralized Web 3.0 Enabled Smart Cities. SMART CITIES, 5(1), 162–176. https://doi.org/10.3390/smartcities5010011

Dhelim, S., Kechadi, T., Chen, L., Aung, N., Ning, H., & Atzori, L. (2022). Edge-enabled Metaverse: The Convergence of Metaverse and Mobile Edge Computing. https://doi.org/10.36227/techrxiv.19606954

Dobbelaere-Welvaert, M. (2020). Ik weet wie je bent en wat je doet. Borgerhoff & Lamberigts.

Dongleur, W. (2019). De hoogste tijd om consumenten te belonen voor hun data. Geraadpleegd op 10 juni 2022, via Frankwatching: https://www.frankwatching.com/archive/2019/09/29/consumenten-belonen-voor-data/

Easton, M. (2019). Digitalisering brengt politie dichter bij de essentie van een gemeenschapsgerichte politiezorg. Cahier Politiestudies, 50(1), 59–66.

European Commission. (z.d). Data protection in the EU. Geraadpleegd op 10 juni 2022, via: European Commission: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

FRA. (z.d). European Union Agengy for Fundamental Rights. Artikel 8 De bescherming van persoonsgegevens. Geraadpleegd op 2 mei 2022, via: https://fra.europa.eu/nl/eu-charter/article/8-de-bescherming-van-persoonsgegevens#international-law

Gartner (2022). Gartner Predicts 25% of People Will Spend At Least One Hour Per Day in the Metaverse by 2026. Geraadpleegd op 28 april 2022, via: https://www.gartner.com/en/newsroom/press-releases/2022-02-07-gartner-predicts-25-percent-of-people-will-spend-at-least-one-hour-per-day-in-the-metaverse-by-2026

Gartner. (2014). IT Glossary. Retrieved from Gartner: https://www.gartner.com/en/information-technology/glossary/big-data

Gibens, S. (2021). Grondrechten inkijkcursus. In Recht en Sociaal werk.

Goldfarb, A., & Tucker, C. (2019). Digital marketing. Elsevier , pp. 259-290.

Gruschka, N., Mavroeidis, V., Vishi, K., & Jensen, M. (2018). Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR. In N. Abe, H. Liu, C. Pu, X. Hu, N. Ahmed, M. Qiao, Y. Song, D. Kossmann, B. Liu, K. Lee, J. Tang, J. He, & J. Saltz (Eds.), 2018 IEEE INTERNATIONAL CONFERENCE ON BIG DATA (BIG DATA) (pp. 5027–5033).

Hofmann, J., Katzenbach, C., & Gollatz, K. (2017). Between coordination and regulation: Finding the governance in Internet governance. NEW MEDIA \& SOCIETY, 19(9), 1406–1423. https://doi.org/10.1177/1461444816639975

Jain, A. K., Sahoo, S. R., & Kaubiyal, J. (2021). Online social networks security and privacy: comprehensive review and analysis. COMPLEX \& INTELLIGENT SYSTEMS, 7(5, SI), 2157–2177. https://doi.org/10.1007/s40747-021-00409-7

Kshetri, N. (2014). Big data's impact on privacy, security and consumer welfare. Telecommunications Policy, 38(11), 1134–1145. https://doi.org/https://doi.org/10.1016/j.telpol.2014.10.002

Kuneva, M. (2009). Roundtable on Online Data Collection, Targeting and Profiling. Keynote Speech. Brussels: European Commision.

Kye, B., Han, N., Kim, E., Park, Y., & Jo, S. (2021). Educational applications of metaverse: possibilities and limitations. JOURNAL OF EDUCATIONAL EVALUATION FOR HEALTH PROFESSIONS, 18, 1–13. https://doi.org/10.3352/jeehp.2021.18.32

Legrand, R. (2021). Facebook wordt Meta. De Tijd. Geraadpleegd op 16 mei 2021, via: https://www.tijd.be/de-tijd-vooruit/tech/Facebook-wordt-meta/10342580?loginSuccess=true

Liberati, A., Altman, D. G., Tetzlaff, J., Mulrow, C., Gøtzsche, P. C., Ioannidis, J. P. A., Clarke, M., Devereaux, P. J., Kleijnen, J., & Moher, D. (2009). The PRISMA Statement for Reporting Systematic Reviews and Meta-Analyses of Studies That Evaluate Health Care Interventions: Explanation and Elaboration. PLOS Medicine, 6(7), 1–28. https://doi.org/10.1371/journal.pmed.1000100

Liu, F., Fan, H.-Y., & Qi, J.-Y. (2022). Blockchain Technology, Cryptocurrency: Entropy-Based Perspective. ENTROPY, 24(4). https://doi.org/10.3390/e24040557

Medzini, R. (2021). Governing the shadow of hierarchy: enhanced self-regulation in European data protection codes and certifications. INTERNET POLICY REVIEW, 10(3). https://doi.org/10.14763/2021.3.1577

Meltzer, J. P. (2015). The Internet, Cross-Border Data Flows and International Trade. ASIA \& THE PACIFIC POLICY STUDIES, 2(1), 90–102. https://doi.org/10.1002/app5.60

Miyazaki, A. (2008). Online Privacy and the Disclosure of Cookie Use: Effects on Consumer Trust and Anticipated Patronage. Journal of Public Policy & Marketing, 27, pp. 19-33.

Montes, R., Sand-Zantman, W., & Valletti, T. (2015). The value of personal information in markets with. RESEARCH PAPER SERIES, Vol. 13, Issue 8, No. 352, (pp. 2-15).

Nakamoto, S. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. http://www.bitcoin.org/bitcoin.pdf

Nalla, M. K., & Gurinskaya, A. (2020). Private Police and Security Governance: Mapping Emerging Trends and Future Directions. Journal of Contemporary Criminal Justice, 36(1), 101–109. https://doi.org/10.1177/1043986219890208

Ning, H., Dhelim, S., Bouras, M. A., Khelloufi, A., & Ullah, A. (2018). Cyber-Syndrome and its Formation, Classification, Recovery and Prevention. IEEE Access, 6, 35501–35511. https://doi.org/10.1109/ACCESS.2018.2848286

Obar, J. A. (2022). Defining and Assessing Data Privacy Transparency: A Third Study of Canadian Internet Carriers. INTERNATIONAL JOURNAL OF COMMUNICATION, 16, 1688–1712.

OESO. (2011). The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines. OESO Digital Economy Papers.

Omnicore (2022). 63 Facebook Statistics You Need to Know in 2022. Geraadpleegd op 9 mei 2022, via: https://www.omnicoreagency.com/Facebook-statistics/#:~:text=The%20largest%20demographic%20group%20of,group%20on%20Facebook%20(4.8%25).

Ozcinar, Z., Sakhieva, R. G., Pozharskaya, E. L., Popova V, O., Melnik V, M., & Matvienko, V. V. (2020). Student's Perception of Web 2.0 Tools and Educational Applications. INTERNATIONAL JOURNAL OF EMERGING TECHNOLOGIES IN LEARNING, 15(23), 220–233. https://doi.org/10.3991/ijet.v15i23.19065

Park, S.-M., & Kim, Y.-G. (2022). A Metaverse: Taxonomy, Components, Applications, and Open Challenges. IEEE ACCESS, 10, 4209–4251. https://doi.org/10.1109/ACCESS.2021.3140175

Pasquale, F. (2014, oktober 16). The Dark Market for Personal Data. The New York Times. Geraadpleegd op 10 mei 2022, via: https://www.nytimes.com/2014/10/17/opinion/the-dark-market-for-personal-data.html

Renwick, R., & Gleasure, R. (2021). Those who control the code control the rules: How different perspectives of privacy are being written into the code of blockchain systems. JOURNAL OF INFORMATION TECHNOLOGY, 36(1), 16–38. https://doi.org/10.1177/0268396220944406

Romansky, R. P., & Noninska, I. S. (2020). Challenges of the digital age for privacy and personal data protection. MATHEMATICAL BIOSCIENCES AND ENGINEERING, 17(5), 5288–5303. https://doi.org/10.3934/mbe.2020286

Rosenberg, L. (2021a). Metaverse: Augmented reality pioneer warns it could be far worse than social media. Think Big. Geraadpleegd op 30 mei 2022, via: https://bigthink.com/the-future/metaverse-augmented-reality-danger/

Rosenberg, L. (2021b). The Metaverse needs Aggressive Regulation. VentureBeat Magazine. Geraadpleegd op 30 mei 2022, via: https://venturebeat.com/2021/12/04/the-metaverse-needs-aggressive-regulation/

Rosenberg, L. (2022). Regulation of the Metaverse: A Roadmap.

Shen, B., Tan, W., Guo, J., Zhao, L., & Qin, P. (2021). How to Promote User Purchase in Metaverse? A Systematic Literature Review on Consumer Behavior Research and Virtual Commerce Application Design. APPLIED SCIENCES-BASEL, 11(23). https://doi.org/10.3390/app112311087

Special Eurobarometer 359. (2011). Attitudes on Data Protection and Electronic Identity in the European Union. EU.

Sterling, G. (2018). Consumers say they want much more control over their personal data. Geraadpleegd op 10 juni 2022, via Martechtoday: https://martechtoday.com/consumers-say-they-want-much-more-control-over-their-personal-data-226815

Thakuria, A., & Baruah, B. (2022). An Overview of Web 3.0 applications in Libraries (pp. 280–289).

Thienpont, A., & Herman, C. (2009). Mensenrechten een kennismaking. (L. v. Mensenrechten, Ed.) Druk in de weer.

Tucker, C. E. (2012). The economics of advertising and privacy. International Journal of Industrial Organization, 30(3), 326–329. https://doi.org/https://doi.org/10.1016/j.ijindorg.2011.11.004

Van der Haegen, M., Sebbahi, Marwa., Samain, M. (2022). Alles wat u moet weten over het metaversum, in zes vragen. De Tijd. Geraadpleegd op 16 mei 2022, via: https://multimedia.tijd.be/uitgelegd/metaverse/#wat-is-de-metaverse

Van Haver, K., Serrure, B. (2022). EU-akkoord tempert macht van Meta, Google en co. De Tijd. Geraadpleegd op 23 mei 2022, via: https://www.tijd.be/politiek-economie/europa/economie/eu-akkoord-tempert-macht-van-meta-google-en-co/10376212

van Schaik, P., Jansen, J., Onibokun, J., Camp, J., & Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour. COMPUTERS IN HUMAN BEHAVIOR, 78, 283–297. https://doi.org/10.1016/j.chb.2017.10.007

Verrycken, R. (2021). Klokkenluider Frances Haugen: 'Facebook subsidieert elke dag haat en verdeeldheid'. De Tijd. Geraadpleegd op 16 juni 2022, via: https://www.tijd.be/ondernemen/technologie/klokkenluider-frances-haugen-Facebook-subsidieert-elke-dag-haat-en-verdeeldheid/10355428.html

Verrycken, R. (2022). Klokkenluidster Haugen vreest problemen in de metaverse. De Tijd. Geraadpleegd op 16 juni 2022, via: https://www.tijd.be/dossiers/metaverse/klokkenluidster-haugen-vreest-problemen-in-de-metaverse/10388175

Vlaamse Overheid. (z.d). Beheer en beveiliging van persoonlijke gegevens van Europese burgers (GDPR of AVG). Geraadpleegd op 10 juni 2022, via Vlaanderen: https://www.vlaanderen.be/uw-overheid/werking-en-structuur/hoe-werkt-de-vlaamse-overheid/beheer-en-beveiliging-van-persoonlijke-gegevens-van-europese-burgers-gdpr-of-avg

Yamada-Rice, D., Mushtaq, F., Woodgate, A., Bosmans, D., Douthwaite, A., Douthwaite, I., Harris, W., Holt, R., Kleeman, D., Marsh, J., Milovidov, E., Williams, M. M., Parry, B., Riddler, A., Robinson, P., Rodrigues, D., Thompson, S., & Whitley, S. (2017).

Children and Virtual Reality: Emerging Possibilities and Challenges. Dubit. https://researchonline.rca.ac.uk/3553/

Yu, R. P., Ellison, N. B., & Lampe, C. (2018). Facebook Use and Its Role in Shaping Access to Social Benefits among Older Adults. JOURNAL OF BROADCASTING \& ELECTRONIC MEDIA, 62(1), 71–90. https://doi.org/10.1080/08838151.2017.1402905

Zhao, R., Zhang, Y., Zhu, Y., Lan, R. and Hua, Z. (2021). Metaverse: Security and Privacy Concern. JOURNAL OF LATEX CLASS FILES, VOL. 14, NO. 8.