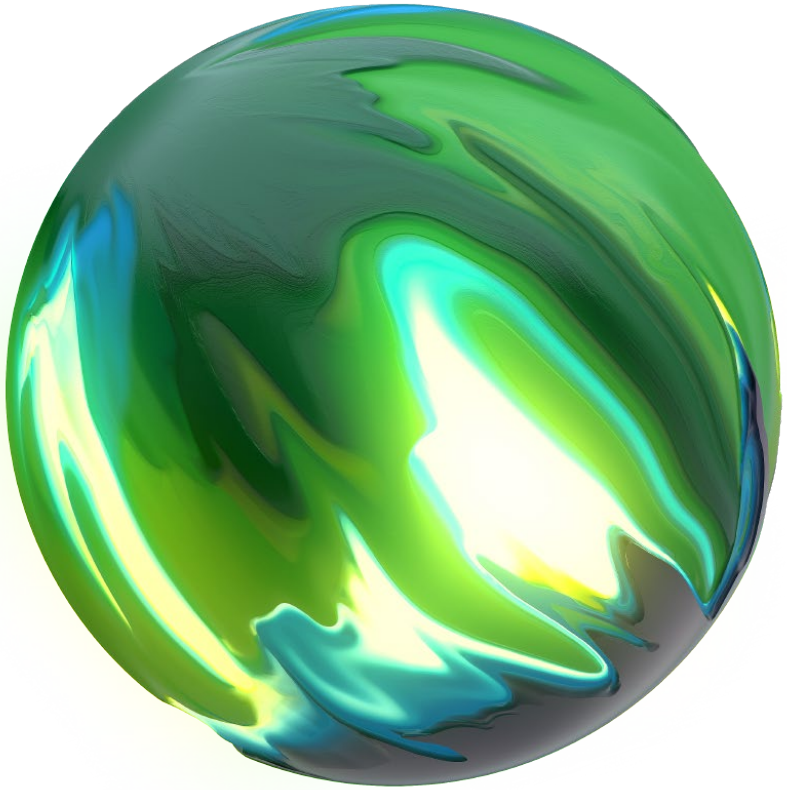
Deloitte.

Ministerie van Economische Zaken en Klimaat



Samen veilig: de toekomst van mobiel online

Rapport Onderzoek cybersecurity van mobiele toestellen en apps | september 2022: AS/ms/22-1544

Inhoudsopgave

Samenvatting

"We no longer live online or offline but 'onlife', that is, we increasingly live in that special space or infosphere, that is seamlessly analogue and digital, offline and online" aldus Luciano Floridi, director van het Digital Ethics Lab aan de Oxford University. Hiermee beschrijft hij de huidige periode waarin het online en offline leven samen beginnen te smelten. Het gebruik van mobiele toestellen en apps is hier een belangrijk onderdeel van en versnelt dit proces. Hoewel de positieve impact evident is brengt deze ontwikkeling ook risico's met zich mee voor individuele gebruikers waaronder minderjarigen. Wetgeving kan gaan helpen maar de échte oplossing zal ook moeten komen van de individuele gebruiker en de maatschappij als geheel.

In dit rapport wordt op verzoek van het Ministerie van Economische Zaken en Klimaat verkend hoe cyberveiligheid, gegevensbescherming en ethische principes (kunnen) worden geborgd om risico's bij het gebruik van mobiele toestellen en apps te mitigeren, met specifieke aandacht voor minderjarigen. Hiervoor wordt gekeken naar de kaders van vigerende en opkomende wetgeving en naar verdere handelingsopties die kunnen worden ingezet om risico's te verminderen. Aan de hand van bestaande kwalitatieve en kwantitatieve onderzoeksrapporten, overige deskresearch en inzichten uit interviews is een analyse gemaakt van het ecosysteem, de risico's voor gebruikers, relevante wet- en regelgeving en andersoortige maatregelen en handelingsopties. Het onderzoek is uitgevoerd van december 2021 tot mei 2022, met een update in augustus 2022.

Het ecosysteem van mobiele toestellen en apps bestaat uit diverse partijen die betrokken zijn bij de ontwikkeling en levering van hardware en software. Zij opereren in een keten en binnen een veranderlijke maatschappelijke context. Verschillende type gebruikersgroepen, belangenorganisaties en overheidsinstanties stellen kaders en grenzen aan hoe mobiele toestellen gemaakt en gebruikt (zouden moeten) worden. De problematiek die verbonden is aan mobiele toestellen en apps staat niet los van bredere vraagstukken rondom de digitale transitie en raakt de hele maatschappij. Daarbij betreft het een *moving target* door de snelle ontwikkelingen die het speelveld transformeren.

Sociale aspecten: expliciteren van normen en waarden

De nabijheid en continue beschikbaarheid van mobiele apparaten zijn cruciale kenmerken die de kans op specifieke risico's voor individuele gebruikers vergroten. Maar behalve de aard van mobiele toestellen en apps, speelt de aard van de mens zelf en haar omgeving ook een rol bij incidenten. Er vinden bijvoorbeeld allerlei vormen van pesten plaats op mobiele toestellen en apps. Bij dergelijke interacties tussen gebruikers onderling, zijn met name het civielrecht en het strafrecht belangrijke kaders. Indirecte interacties en individuele kwetsbaarheden hebben ook invloed. De aantrekkingskracht van de producten en diensten kan groot zijn en de bijkomende sociale verwachtingen kunnen leiden tot negatieve impact. Behalve in wettelijke kaders, moet er geïnvesteerd worden in voorlichting, digitale vaardigheden, technische hulpmiddelen ter preventie van o.a. stress en verslaving en hulpverlening voor wanneer het alsnog misgaat.

Privacy en ethiek aspecten: grip op de impact van nieuwe wetgeving

Datastromen zijn een belangrijke factor in verdienmodellen en algoritmen die ten grondslag liggen aan diverse typen apps. Het verwerken van grote hoeveelheden data vraagt om privacy- en informatiebeveiligingsmaatregelen. Er zijn allerlei open normen, standaarden en verplichtingen geëxpliciteerd in wetgeving, maar het is ook belangrijk om praktischere oplossingsrichtingen te verkennen. Er wordt veel wet- en regelgeving gemaakt omtrent het beperken van de mogelijkheden om gebruikers te beïnvloeden via mechanismes in en eigenschappen van digitale omgevingen. Het gaat daarbij niet alleen om de ontwikkelaars met commerciële belangen, maar ook om overheden, NGO's,

charitatieve organisaties en overige partijen. Als ontwerper van de digitale omgeving zelf, hebben sommige partijen in het ecosysteem daarbovenop nog een unieke machtspositie. Zij kunnen “onder de motorkap” beslissingen maken en inzetten op een inrichting van de omgeving die hun eigen belang dient.

Consumentenbescherming en het mededingingsrecht bieden al op verschillende vlakken bescherming, maar juist op dit gebied is er ook veel Europese wetgeving in de maak, zoals de Digital Services Act (DSA) en de Digital Markets Act (DMA). Dit onderhoud aan wettelijke kaders door het Europese wetgevings- en investeringsprogramma ‘A Europe fit for the Digital Age’ is een indicatie dat bestaande kaders niet voldoende aansluiten bij de huidige staat van de technologie, bedrijfsvoering en markten. Al dan niet aangemoedigd door wet- en regelgeving werken allerlei organisaties aan beleid en hulpmiddelen om risico’s te mitigeren en gebruikers meer ondersteuning en controle te geven. Voor overheden is het dan ook zaak om niet alleen in te zetten op het dichten van hiaten in de wet, maar ook invulling te geven aan behoeften en zorgen door behulpzame initiatieven vanuit het ecosysteem te stimuleren en te ondersteunen.

Cyberveiligheid aspecten: standaardisering en voorzorgsmaatregelen

Ongeacht de wetgeving en aanvullende maatregelen zullen kwaadwillende derden ook actief blijven. Zij zullen nieuwe manieren vinden om veiligheidsmaatregelen te omzeilen en kwetsbaarheden in de technologie uit te buiten, via het manipuleren van een gebruiker of een mobiel toestel. Het strafrecht biedt ook binnen deze categorie van risico’s soelaas. Bepaalde handelingen, zoals computervredebreuk, aftappen van gegevens en het installeren van malware, zijn bij wet verboden. Daarnaast zijn er wettelijke kaders en certificeringschema’s in ontwikkeling om verantwoordelijkheden bij organisaties in de kritieke infrastructuur te beleggen op Europees en nationaal niveau. Aanbieders van digitale diensten zoals sociale media platforms vallen daar inmiddels ook onder. Deze maatregelen kunnen de weerbaarheid van deze aanbieders vergroten. De ontwikkeling van goede certificeringschema’s en standaarden draagt bij aan de integratie en afstemming van open normen. Het vergt echter veel expertise en overleg tussen zowel ontwikkelaars als toezichthouders om tot gezamenlijke interpretaties van einddoelen, een bruikbaar instrumentarium en dekkende taakverdelingen te komen.

Onvoldoende afgedekte risico’s

Gesignaleerde kwesties worden momenteel met name op Europees niveau omgezet in beleidsmaatregelen. Echter, het zijn vaak niet alleen hiaten in wettelijke kaders, maar ook gebrekkige naleving en uitdagingen in het toezicht die voor problemen zorgen. In het digitale domein is de interpretatie en uitvoering van wetten en regels een grote uitdaging. Toezichthouders investeren duidelijk in kennisopbouw en in samenwerking met andere toezichthouders. En behalve acties van de overheid, worden tegelijkertijd stappen gezet vanuit het bedrijfsleven en het maatschappelijk middenveld. Door het actualiseren van wettelijke kaders, worden ook andere processen in gang gezet. Bedrijven investeren in beleid, gebruikersvoorwaarden en creëren technische hulpmiddelen voor gebruikers en ouders. Hulp- en belangenorganisaties steunen gebruikers en hebben een belangrijke signaleringsfunctie om problemen aan de kaak te stellen en te komen tot alternatieven.

Om gebruikers van mobiele toestellen en apps beter te beschermen, moeten verbeteringen dus niet alleen worden gezocht in wet- en regelgeving. Gebruikers van mobiele toestellen en apps worden in ruime mate beschermd door vigerende en opkomende wet- en regelgeving, maar het vereist een integrale aanpak en samenwerking om incidenten te voorkomen en adequaat te reageren op problemen. Mitigerende acties kunnen van technische, organisatorische en maatschappelijke aard zijn. Overheden, bedrijven, het maatschappelijk middenveld en gebruikers zelf kunnen bijdragen aan het verkleinen van de eerder genoemde risico’s. Daarbij moet gedacht worden aan het expliciteren van (gebruikers)normen, certificering van producten en diensten, standaardisatie en het vergroten van de digitale geletterdheid en weerbaarheid van zowel gebruikers als de overheid.

“Het vereist een integrale aanpak en samenwerking om incidenten te voorkomen en adequaat te reageren op problemen”

Aandachtspunten & aanbevelingen

Het doel van dit onderzoek is om zicht te krijgen op de mogelijkheden om gebruikers van mobiele toestellen en apps – en minderjarigen in het bijzonder – beter te beschermen. Aangezien er verschillende soorten risico's bestaan, zijn er ook verschillende ingrepen mogelijk.

1

Uitvoerbaarheid van wettelijke eisen

Een belangrijk criterium voor een wet is dat deze uitvoerbaar moet zijn voor diegene voor wie de wet geldt. Ketenverantwoordelijkheden en de praktische vertaling van wettelijke vereisten, vormen knelpunten in de praktijk. Het is daarom aan te raden om het bedrijfsleven en toezichthouders te betrekken bij het opstellen van wetteksten en te investeren in impactonderzoek.

2

Toegerust toezicht

Om van de huidige en opkomende wetgeving tot betere praktijken te komen, moeten toezichthouders hun rol goed kunnen uitvoeren. Door de toekomstige nieuwe wetgeving vanuit Europa wordt het takenpakket van de toezichthouders vergroot en gecompliceerder. De huidige toezichthoudende instanties en de overlap en relatie tussen taken en focusgebieden zullen verder veranderen. Dit zet druk op de capaciteit van toezichthouders, zowel budgettair als qua kennis en kunde.
Het is daarom aan te raden dat de betrokken toezichthouders hun focusgebieden en onderzoeksagenda's bijstellen en het contact met de praktijk gezamenlijk vormgeven.

3

Bewustwording is niet genoeg

Gebruikers hebben digitale vaardigheden nodig om zichzelf afdoende te beschermen tegen risico's. Overheden en maatschappelijke organisaties kunnen helpen bij het creëren van bewustwording, maar beleid louter gericht op bewustwording zorgt niet voor het gewenste effect. Het is daarom aan te raden om te investeren in praktijkgericht gedragsonderzoek met aandacht voor persoonlijke motivatie, gelegenheid en culturele aspecten. Met name om jongeren effectief te bereiken dient de kennisoverdracht aan te sluiten bij de behoeftes en belevingswereld van die groep.

4

Aandacht voor de signaleringsfunctie

Dit rapport biedt geen uitputtend overzicht van incidenten en risico's. De digitale omgeving is continu in ontwikkeling en het is dus van belang om te kunnen anticiperen op technologische en maatschappelijke veranderingen die hierdoor ontstaan. Om problemen tijdig te kunnen adresseren, is het daarom aan te raden om signaleringsfuncties op verschillende niveaus vanuit de overheid te stimuleren en (financieel) te ondersteunen.

5

Standaardisering en voorzorgsmaatregelen

Tot slot zijn er ook effectieve voorzorgsmaatregelen en best practices die voor de nodige standaardisatie kunnen zorgen. Dit kan zowel binnen industrieën zelf plaatsvinden, als ook worden gestimuleerd door de overheid. Het is daarom aan te raden om in te zetten op samenwerking tussen maatschappelijke (hulp- en onderzoeks)organisaties, bedrijven en overheden.

Inleiding

Dit rapport is opgesteld in opdracht van het Ministerie van Economische Zaken en Klimaat (EZK). De opdracht voor het onderzoek is geformuleerd naar aanleiding van een op 6 juli 2021 unaniem aangenomen motie van het kamerlid Van Dijk. In deze motie wordt de regering verzocht om "een analyse te maken van de rol van cyberveiligheid bij (het gebruik van) apps en mobiele toestellen, en risico's en kwetsbaarheden in kaart te brengen."[1]

Deze motie werd ingediend tijdens een debat over buitenlandse spionage via mobiele netwerken. In dat debat werd onder andere gesproken over geopolitieke vraagstukken, zoals inmenging en ontwrichting van democratische processen, en over economische belangen van buitenlandse overheden en bedrijven. Hierbij kwamen de kwetsbaarheden binnen de telecomnetwerken van Nederland, de komst van 5G en maatschappelijke gevolgen hiervan aan de orde.

De motie riep echter op tot aandacht voor andersoortige risico's met betrekking tot cyberveiligheid, namelijk de kleinschaligere inbreuken op hardware en software gericht op individuen, en de gevolgen van dit soort dreigingen voor deze gebruikers. In de motie wordt gerefereerd naar de Chinese applicatie (app) TikTok die zeer populair is bij onder relatief jonge doelgroep, maar ook onder vuur ligt vanwege omstreden datapraktijken.[2] Volgens de stichting Take Back Your Privacy, de stichting Massaschade & Consument en stichting Onderzoek Marktinformatie (SOMI) misleidt TikTok haar gebruikers, hanteert TikTok onduidelijke en oneerlijke voorwaarden en beschermt het kinderen onvoldoende tegen advertenties en ongepaste inhoud.[3] Bovendien hebben diverse beveiligingsonderzoekers de afgelopen jaren gemeld meerdere beveiligingsproblemen in de sociale media-app te hebben gevonden.[4] Gegeven het feit dat dergelijke sociale media-apps toegang hebben tot veel persoonlijke en persoonsgevoelige informatie van gebruikers, werden de sociale media-apps de favoriete route voor veel hackers met alle gevolgen van dien.

Zowel de anekdote van het Kamerlid Van Dijk (zie Kader 1) alsook de referentie naar TikTok vraagt om een bredere verkenning van risico's voor gebruikers. Dit is door EZK vertaalt in een uitvraag voor nader onderzoek naar de cyberveiligheid-, privacy- en bredere risico's die gepaard gaan met het gebruik van mobiele toestellen en apps. Hierbij is aangemerkt dat de risico's voor particuliere gebruikers, en minderjarigen als kwetsbare gebruikersgroep in het bijzonder, verder dienen te worden onderzocht. Dit onderzoek gaat niet in op risico's omtrent het gebruik van infrastructuur en discussies over de nationale veiligheidsrisico's.[5] Denk hierbij aan de discussies over het 5G-netwerk of over de opslag van data in de cloud van een buitenlandse aanbieder.[6]

Zoals wordt verzocht in de motie, ligt de focus van dit onderzoek op de risico's die komen kijken bij het gebruik van mobiele toestellen en apps. Hierbij wordt specifiek geredeneerd vanuit de particuliere gebruiker als individu.

Deloitte heeft in de periode van december 2021 tot mei 2022 onderzoek gedaan en voorliggend rapport opgesteld. Vervolgens is er in augustus 2022 een update gedaan aan de hand van de toen geldende stand van zaken. Dit rapport is opgesteld door het Cyber, Privacy, Digital Ethics en Digital Regulations team Deloitte Risk Advisory in Nederland.

[1] *Kamerstukken II* 2020/21, 30821, nr. 148.
[2] Nederlandse Autoriteit Persoonsgegevens (AP) een nader onderzoek naar dit platform verricht. In juli 2021 heeft AP dit platform een boete van € 750.000 opgelegd wegens schenden van privacy van kinderen, zie 'Boete van 750.000 euro voor TikTok vanwege uitleg privacy in Engels', nos.nl 22 juli 2021.
[3] Deze organisaties hebben het platform gedagvaard, zie: 'Nederlandse ouders dagen TikTok voor de rechter met een schadeclaim van 1,4 miljard', parool.nl 21 juli 2021; 'Actie tegen TikTok', stichtingtakebackyourprivacy.nl; 'Stop de illegale handel in TikTok profielen', massaschadeconsument.nl.
[4] Boxiner et. al. *CheckPoint Research* 2019; Wouters en Paterson *Pursuit* 2021.
[5] '5G: The outsourced elephant in the room', berthub.eu 20 januari 2020.
[6] *Advies opslag medische data in de cloud* 2019.

Kader 1:

Van motie tot onderzoeksvraag

Het lid Van Dijk vertelt: “Onze Jip van 11 kwam afgelopen woensdag bij me zitten. Tranen in de ogen, want ze werd uitgelachen op TikTok. Als bepaalde filmpjes openden, dan hoorde ze een keiharde lach door het filmpje heen, een beetje The Jokerachtig. Ze had verdriet om het lachje, want ze voelde zich uitgelachen. Ik heb dan altijd een beetje verdriet om haar tranen, maar ik voelde me eigenlijk ook uitgelachen, maar dan om een andere reden. **Hier was duidelijk sprake van een indringer die in staat was door alle beveiligingen heen te hacken en die ons, met al onze goede beveiligingsbedoelingen, uit ging lachen**. Dit was wederom een bewijs hoever men is op het gebied van indringing en hoe relatief eenvoudig het is. […] Wanneer het gaat om het beveiligen van onze mobiele netwerken, ligt de focus vaak op de telecomnetwerken zelf, terwijl de rol van cyberveiligheid bij het gebruik van apps en mobiele toestellen veel minder aandacht krijgt. Eigenlijk ten onrechte, want als de Chinese app TikTok stiekem en op grote schaal informatie van kinderen kan verzamelen en verhandelen, dan moeten toch echt alle alarmbellen afgaan.”

Hierop volgt een oproep tot nader onderzoek naar de kwetsbaarheden van appgebruik, zowel onder kinderen als onder volwassenen, en waar dit kan worden verbeterd. Hiervoor is een focus op cyberveiligheid alleen te beperkt. Het is immers de vraag of wat Jip overkwam, puur een cyberveiligheidskwestie was. Cyberveiligheid betreft in dit onderzoek de veiligheid van systemen en de informatie die op die systemen staat. De inrichting, ontwikkeling en het beheer van systemen en apps hebben allemaal invloed op de cyberveiligheid van mensen en hun informatie. Echter, er zijn meer risico’s omtrent appgebruik dan alleen cyberveiligheid voor de gebruiker van een app. Appgebruik kent ook andere risico’s zoals privacyrisico’s (bijv. overmatig datagebruik door derde partijen) en sociale risico’s zoals pesterijen en manipulatie. De brede onderzoeksvragen die door het ministerie van EZK zijn opgesteld, zijn in overleg teruggebracht tot de hoofd- en deelvragen die in dit rapport worden behandeld.

Doel en onderzoeksopzet

Dit rapport is bedoeld om een zo globaal en zo compleet mogelijk beeld te schetsen van de risico's omtrent cyberveiligheid, privacy en overige risico's die voortvloeien uit interacties op mobiele toestellen en apps. Het zijn de fysieke apparaten en de softwareonderdelen die daarop draaien, die voor velen het meest zichtbare deel van de digitale wereld vormen. Hoe mobiele toestellen en apps zijn vormgegeven en worden gebruikt, hangt samen met de geschiedenis van het internet en nieuw ontstane verdienmodellen. In dit rapport worden relevante elementen binnen het ecosysteem beschreven en diverse risico's ontward. Een analyse van de huidige wet- en regelgeving en mogelijke aanvullende maatregelen geeft inzicht in hoe de gebruikersveiligheid te verbeteren is.

Onderzoeksvragen

Voor dit onderzoek is door EZK een lijst met onderzoeksvragen opgesteld. Deze onderzoeksvragen zijn vervolgens door Deloitte vertaald naar één hoofdvraag met vier deelvragen.

De hoofdvraag luidt:

Op welke manier worden cyberveiligheid, gegevensbescherming en ethische principes geborgd binnen de kaders van vigerende en opkomende wetgeving en hoe kunnen Nederlanders - minderjarigen het bijzonder - beter beschermd worden tegen risico's bij het gebruik van mobiele toestellen en apps?

Om deze vraag te kunnen beantwoorden, worden de volgende deelvragen gehanteerd:

1. Hoe ziet het ecosysteem van mobiele toestellen en apps eruit?
2. Wat zijn risico's en kwetsbaarheden bij het gebruik van mobiele toestellen en apps voor gebruikers in het algemeen en voor minderjarigen in het bijzonder?
3. Welke vigerend en opkomende Europese- en Nederlandse wet- en regelgeving adresseren deze risico's en cyberveiligheid, gegevensbescherming en ethische principes in het bijzonder?
4. Welke aanvullende maatregelen kunnen worden getroffen om gebruikers van mobiele toestellen en apps beter te beschermen?

Aanpak

Om de onderzoeksvragen te beantwoorden, is allereerst een analyse gemaakt van bestaande kwalitatieve en kwantitatieve onderzoeken en inzichten uit interviews met marktpartijen op het gebied van soft- en hardware, overheidsinstanties, belangenorganisaties en toezichthouders (zie bijlage 3 voor een overzicht van de verschillende respondenten).[7] Gezien de continue ontwikkeling op het gebied van dit onderzoek is in eerste instantie, ten behoeve van de uitvoerbaarheid, de stand van zaken op 23 april 2022 als uitgangspunt genomen voor de analyse van vigerende en aankomende Nederlandse- en Europese wettelijke kaders die van toepassing zijn op de geïdentificeerde risico's. Eind augustus 2022 is een aanvullende opdracht verstrekt door EZK die gericht was op de vertaling van het rapport in het Engels en een algemene update op basis van de meest recente stand van zaken. Daardoor is de definitieve stand van zaken waarop dit rapport gebaseerd is gesteld op 31 augustus 2022.

De inzichten die zijn opgehaald uit de diverse bronnen, zijn verzameld en gestructureerd in een referentiekader. Hierin is per onderzoeksvraag opgesteld welke inzichten bijdragen aan de beantwoording van de vraag en uit welke bronnen deze inzichten komen. Dit overzicht is uitgewerkt in verschillende hoofdstukken die zijn geverifieerd in wekelijkse bijeenkomsten met het onderzoeksteam.

Op 12 april 2022 zijn de bevindingen voorgelegd aan vertegenwoordigers van de het ministeries en toezichthouders in een klankbordbijeenkomst. Het doel van deze sessie was om oplossingsrichtingen verder te concretiseren. Het conceptrapport is op 3 mei 2022 ter validatie voorgelegd en op 10 mei 2022 mondeling doorgesproken tijdens een tweede klankbordbijeenkomst met dezelfde groep (zie bijlage 2).

In dit rapport zijn diverse problemen met betrekking tot het gebruik van mobiele toestellen en elementen binnen het ecosysteem uitgelicht. Hiervoor zijn geen specifieke apps of bedrijven onder de loep genomen. Het rapport bevat daarnaast

[7] De respondenten hebben meegewerkt aan het onderzoek en hun kijk op de zaak gegeven in de beginfase van het onderzoek. Dit betekent niet dat de respondenten de conclusies en inzichten in dit rapport onderschrijven.

ook geen technische analyse van het ecosysteem. Uitputtende overzichten met betrekking tot verschillende mobiele toestellen, applicaties, risico's, wettelijke kaders, zijn in dit rapport vermeden. De focus is gelegd op een generiek overzicht. Het onderzoek heeft tevens niet als doel de ernst van de risico's te evalueren. Daar waar toepasselijk, is wel beschikbaar cijfermateriaal gebruikt om de situatieschets te ondersteunen.

Centrale begrippen

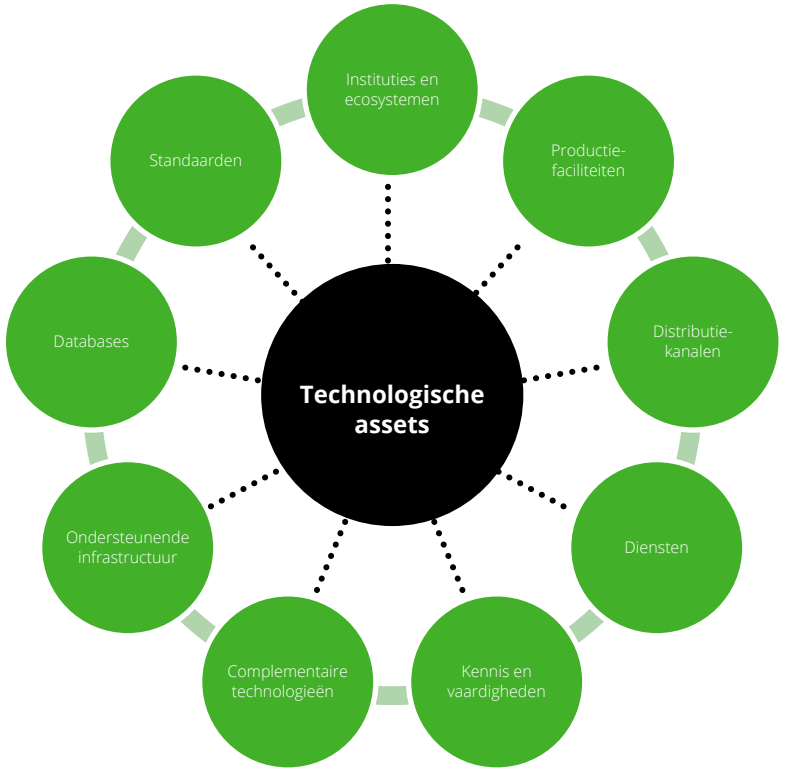
Een aantal centrale begrippen voor dit onderzoek zijn hieronder toegelicht om de aard en omvang van het onderzoek te verhelderen.

Ecosysteem

Om mobiele toestellen en apps te kunnen laten functioneren, is een samenspel van technologieën, standaarden en instituties, en een diversiteit aan kennis en expertise nodig. Dit wordt in technologie- en innovatiestudies op verschillende manieren geconceptualiseerd. Daarbij is er behalve voor technische aspecten ook oog voor contextfactoren en netwerken van menselijke en niet menselijke actoren.[8] Een socio-technische ecosysteembenadering wordt ook door de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) gehanteerd.[9] Inzicht in de rol van instituties en netwerken is immers ook voor beleidsmakers zeer relevant. Zo ontwikkelde het ministerie van EZK met TNO de aanpak Strategic Innovation Assets om zicht te krijgen op de waardeketens en (innovatie-)ecosystemen (zie figuur 1).[10]

Om eenduidigheid in dit rapport te kunnen hanteren, wordt echter teruggegrepen op de definitie van het woord 'ecosysteem' dat stamt uit de biologie en de natuurwetenschap en beschrijft: "Het geheel van de planten en dieren in een territorium, gezien in hun wisselwerking met hun omgeving"- Van Dale. Dit onderzoek richt zich op de interactie tussen diverse partijen in de keten van hard- en software, bezien vanuit gebruikersperspectief. De beschrijving van locaties (technologielagen), actoren (betrokken partijen), omgevingsfactoren en relaties daartussen (bredere context) vormen de basis voor de verdere uitwerking van dit onderzoek. De vier elementen zijn breed opgevat om een solide contextschets te kunnen geven waar in de rest van het rapport naar kan worden teruggegrepen. De weergave van dit ecosysteem biedt geen uitputtend overzicht van alle actoren en componenten die relevant zijn en zich vertalen in kansen en barrières voor technologische veranderingen of innovatie.

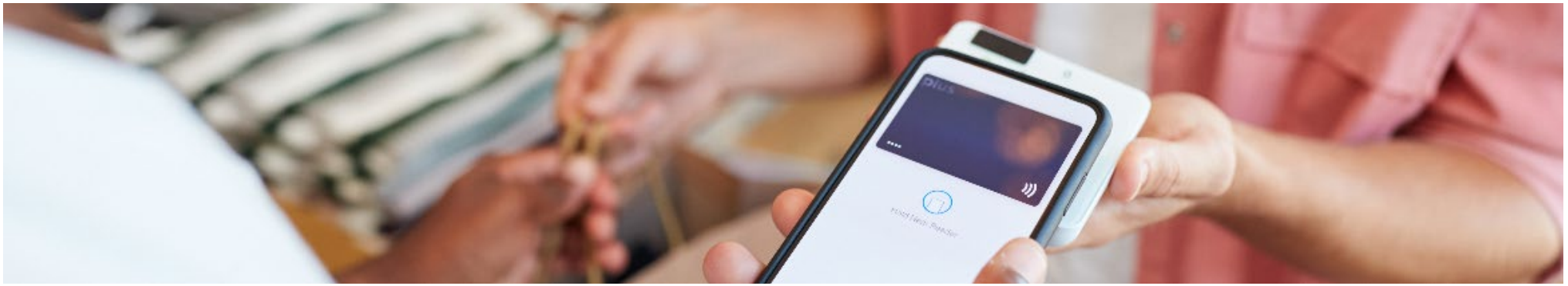
Figuur 1: Innovatie assets: een combinatie van technologische en complementaire assets



[8] Het interdisciplinair veld van "Science and Technology Studies" onderzoekt de creatie, ontwikkeling en gevolgen van wetenschap, technologie en innovatie in hun historische, culturele en sociale context. Een overzicht van wetenschappelijke literatuur en recente discussies over het gebruik van de term "ecosysteem" vallen buiten de scope van dit onderzoek.

[9] Prins et. al. 2021, p. 225.

[10] Dit raamwerk van TNO wordt ook aangehaald in het Working Paper *Het technologisch ecosysteem van AI in Nederland* 2019. Hierin laat de WRR zien dat een krachtige technologiepositie in AI meer vergt dan alleen inzet op AI en de software en algoritmen die er de kern van vormen.



Mobiele toestellen en apps

Onder mobiele toestellen worden in dit onderzoek smartphones, smartwatches (en -armbanden) en tablets te verstaan. Andere 'slimme' apparatuur en zelfs elektrische auto's kunnen worden gezien als mobiele toestellen, maar zijn net als mobiele telefoons zonder internetconnectie (die louter werken op het telefoonnetwerk) en laptops in dit onderzoek buiten beschouwing gelaten. De beperking tot smartphones, -watches en tablets heeft te maken met de technologie, firmware, besturingssystemen en infrastructuur die voor deze toestellen vergelijkbaar is.

In het rapport wordt doorgaans de noemer "mobiele toestellen en apps" gehanteerd. Dit dient aan te geven dat het specifieke type apparaat dat wordt gebruikt niet de (meest) bepalende factor is voor de risico's die in dit rapport worden uitgediept. Wel speelt het kleine formaat, de aard van het gebruik en alomtegenwoordigheid van de apparaten waarop diverse apps worden gebruikt een belangrijke rol. Het abstractieniveau waarvoor is gekozen, heeft tot gevolg dat ketens van afnemers en leveranciers van componenten (zoals de code en chips) die over de hele wereld worden ontwikkeld en geproduceerd, in dit rapport niet worden uitgediept.[11]

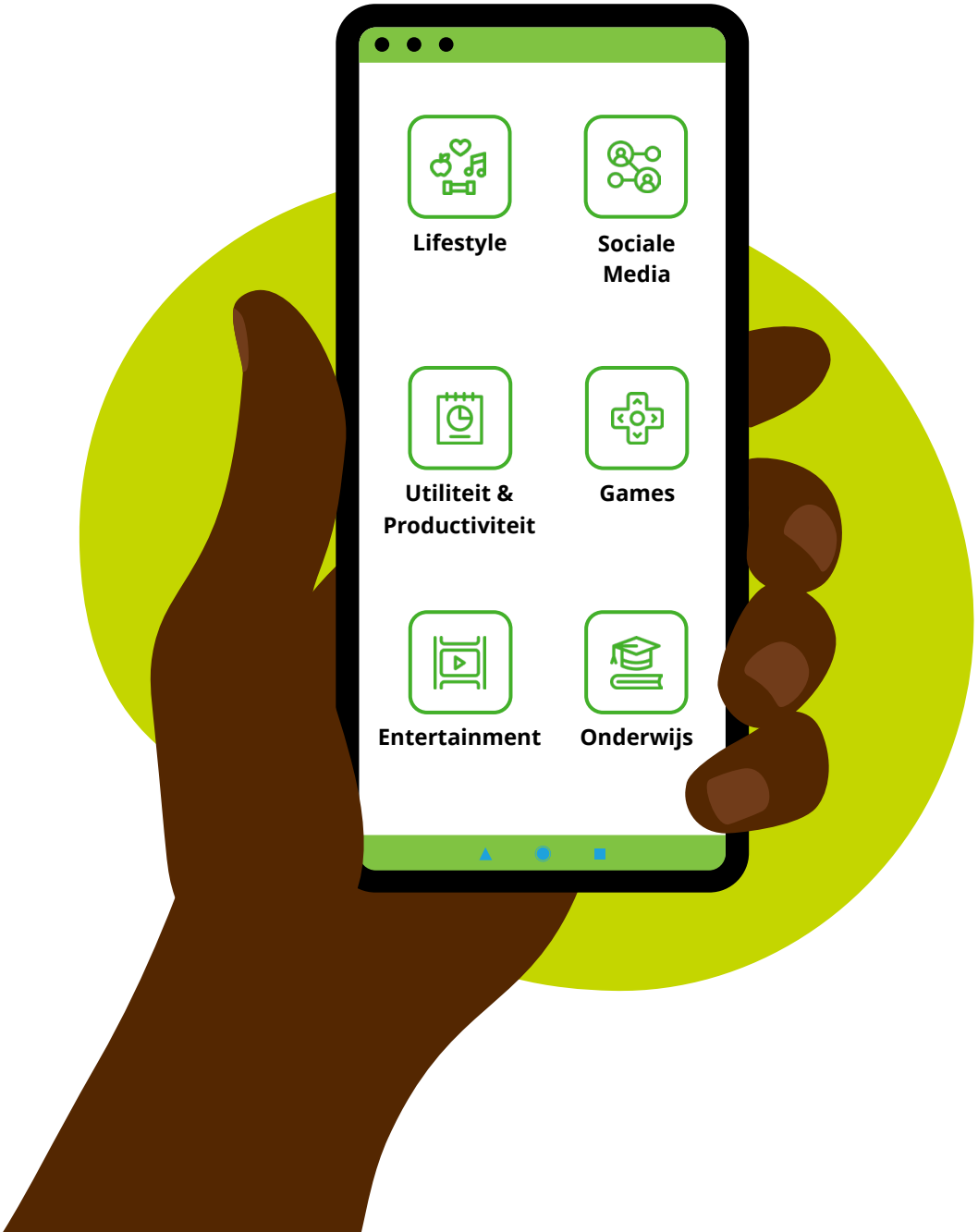
Het type relatie tussen enerzijds het mobiele toestel en de daarop draaiende apps en anderzijds de gebruiker vormt tevens onderdeel van de afbakening. Dit onderzoek focust zich nadrukkelijk op de "gewone gebruiker" die als consument op persoonlijke titel een relatie aangaat met een app ontwikkelaar die als marktpartij fungeert. Apps die niet op eigen initiatief worden gedownload en gebruikt, worden buiten beschouwing gelaten. Daaronder vallen bijvoorbeeld: de apps die door een individu verplicht moeten worden gebruikt in de context van werk, in een zorgcontext[12] of in relatie tot overheidsdiensten.

Het aanbod consumentenapps is echter ook nog zeer divers. Op basis van de categorisering[13] die in app winkels wordt gebruikt, kan een onderscheid gemaakt worden tussen verschillende type apps (zie volgende pagina). Afhankelijk van het type app en het type functionaliteit, zullen andere ontwerpkeuzes worden gemaakt en zullen mobiele apps sterk van elkaar verschillen op het gebied van snelheid, toegankelijkheid, betrouwbaarheid, kracht, benodigde opslagcapaciteit, verdienmodel, werving van persoonlijke data en andere zaken. Dit soort karakteristieken zullen verder worden aangestipt.

[11] In diverse studies worden de onzichtbare en materiële lagen van technologie uiteengerafeld. Zie bijvoorbeeld: Crawford, *The Atlas of AI* 2021.

[12] Dat neemt niet weg dat er gezondheidsgegevens of andere soorten bijzondere persoonsgegevens worden verzameld en gebruikt.

[13] Gebaseerd op de categorisering in appstores zoals die van Apple. Lees 'Choosing a Category', developer.apple.com, en op een simpele categorisering gemaakt door Software bedrijf 'Duckma' blog.duckma.com,



Categorisering apps

Lifestyle apps
Gericht op het stimuleren van specifieke elementen die onderdeel zijn van de levensstijl van een gebruiker. Het kan hierbij gaan om apps die te maken hebben met bijvoorbeeld koken, eten en drinken, fitness, relaties en daten, reizen en shoppen.

Sociale media apps
Gemaakt zodat gebruikers een netwerk met medegebruikers kunnen opbouwen en zodat content op een snelle en efficiënte manier gedeeld kan worden via dit netwerk. Sociale media functionaliteiten komen ook voor op apps die niet per se in de sociale media categorie vallen. Vaak zitten “deel”-mogelijkheden ook in andere apps verwerkt. Zo kunnen high-scores bij game-apps bijvoorbeeld vaak gedeeld worden met het sociale media netwerk van de gebruiker met één druk op de knop.

Utiliteits- en productiviteitsapps
Kunnen helpen bij het uitvoeren van specifieke en/of complexe taken. Voorbeelden van productiviteitsapps zijn tekstverwerkers, e-mail apps, apps om bankzaken mee te regelen, kalenders, rekenmachines, etc.

Games
Spellen zijn er in allerlei soorten en maten, van online games en co-op games, tot solo games en spelletjes speciaal gemaakt voor minderjarigen.

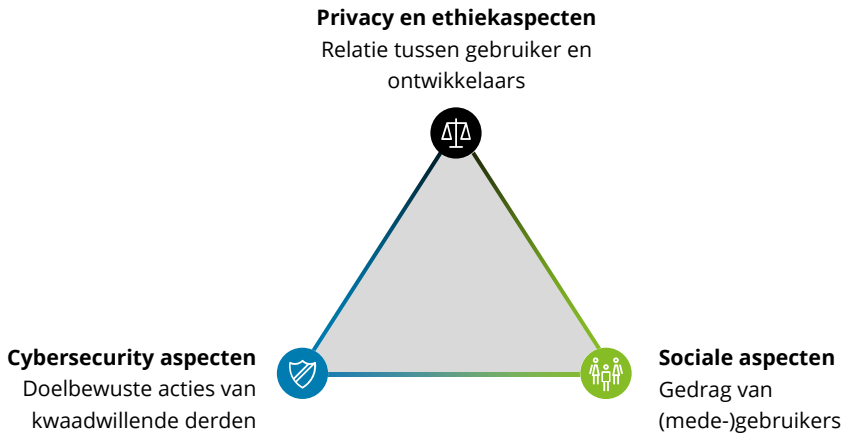
Entertainment apps
Hebben als doel om een gebruiker zoveel mogelijk te vermaken. Onder dit soort apps vallen bijvoorbeeld, video streaming diensten, e-readers en audio-apps.

Onderwijs apps
Hebben als hoofddoel om de gebruiker iets bij te brengen. Het kan hierbij gaan om het aanleren van nieuwe vaardigheden zoals taaltrainers, maar bijvoorbeeld ook om nieuwsapps.

Risico's en maatregelen

Risico's die gepaard gaan met het gebruik van mobiele toestellen en apps zijn divers. Enkel een focus op bijvoorbeeld cyberrisico's geeft niet voldoende weer welke problematiek er speelt. Dit onderzoek bevat geen kwantitatieve analyse om te bepalen welke risico's het grootst of het meest zorgelijk zijn. Wel biedt dit onderzoek een overzicht van de risico's die gepaard gaan met het gebruik van mobiele toestellen en apps. Om deze risico's op een inzichtelijke manier aan elkaar te verbinden, is ervoor gekozen de risico's te categoriseren. Deze categorisering is driedelig (zie figuur 2). Zo zijn er risico's die hun oorsprong vinden in de interactie tussen de gebruiker en de ontwikkelaar (**privacy en ethiek aspecten**), in het gedrag van gebruikers (**sociale aspecten**) en in acties van kwaadwillende derden (**cyberveiligheid aspecten**). Deze categorisering staat aan de basis van het vervolg van dit rapport.

Figuur 2: Schematische weergave van categorieën kwetsbaarheden en risico's



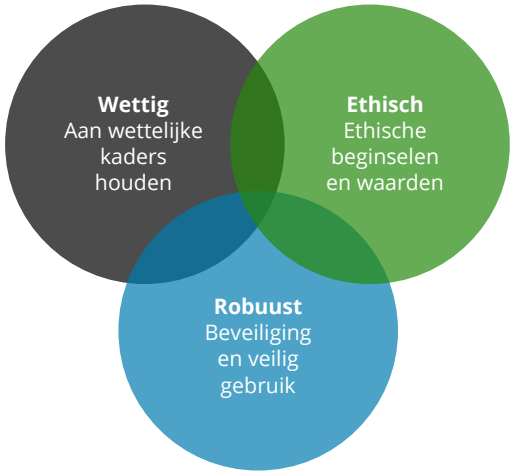
Om deze risico's te mitigeren en een betrouwbaar ecosysteem van mobiele toestellen en apps te organiseren, zijn verschillende type maatregelen nodig. Het raamwerk van Betrouwbare Kunstmatige Intelligentie (KI) van de Europese Commissie laat zien dat aan drie componenten moet worden voldaan: "de KI moet a) **wettig** zijn, door te voldoen aan alle toepasselijke wet- en regelgeving, b) **ethisch** zijn, door naleving van ethische beginselen en waarden te waarborgen, en c) **robuust** zijn uit zowel technisch als sociaal oogpunt, aangezien KI-systemen ongewild schade kunnen aanrichten, zelfs al zijn de bedoelingen goed."[14]

Deze drie componenten zijn verder door de commissie uitgewerkt in vereisten[15] en zowel technische als niet-technische methoden om die vereisten te verwezenlijken.[16] Veel van de vereisten en methoden zijn ook relevant voor de wereld van mobiele toestellen en apps.

In dit rapport komen zaken zoals technische robuustheid en veiligheid, privacy en data governance, maar ook het belang van onderzoek en innovatie en het informeren/onderwijzen van verschillende belanghebbenden (onderwijs & verwachtingenmanagement) naar voren in verschillende hoofdstukken. De aandachtspunten die in dit rapport worden geëxpliciteerd, komen overeen met ambities die worden beschreven in de brief "Hoofdlijnen beleid voor digitalisering" van staatssecretaris Van Huffelen.[17] De insteek van Nederlandse overheden om te "reguleren, normeren en standaardiseren, samenwerking orkestreren, investeren, randvoorwaarden scheppen en bovendien zélf het goede voorbeeld geven" sluit goed aan bij de breedte en reikwijdte van de aanbevelingen in dit rapport.

[14] European Commission, Directorate-General for Communications Networks, Content and Technology, *Ethics guidelines for trustworthy AI*, Publications Office, 2019, https://data.europa.eu/doi/10.2759/346720
[15] Namelijk: 1) menselijke controle en menselijk toezicht, 2) technische robuustheid en veiligheid, 3) privacy en datagovernance, 4) transparantie, 5) diversiteit, nondiscriminatie en rechtvaardigheid, 6) milieu- en maatschappelijk welzijn en 7) verantwoordingsplicht.
[16] Waaronder onderzoek en innovatie, het verspreiden van informatie naar belanghebbenden in de vorm van onderwijs en verwachtingenmanagement.
[17] *Kamerstukken II* 2021/22, 26643, nr. 843.

Figuur 3: Schematische weergave van componenten van maatregelen



Leeswijzer

Dit rapport bestaat uit de volgende onderdelen:

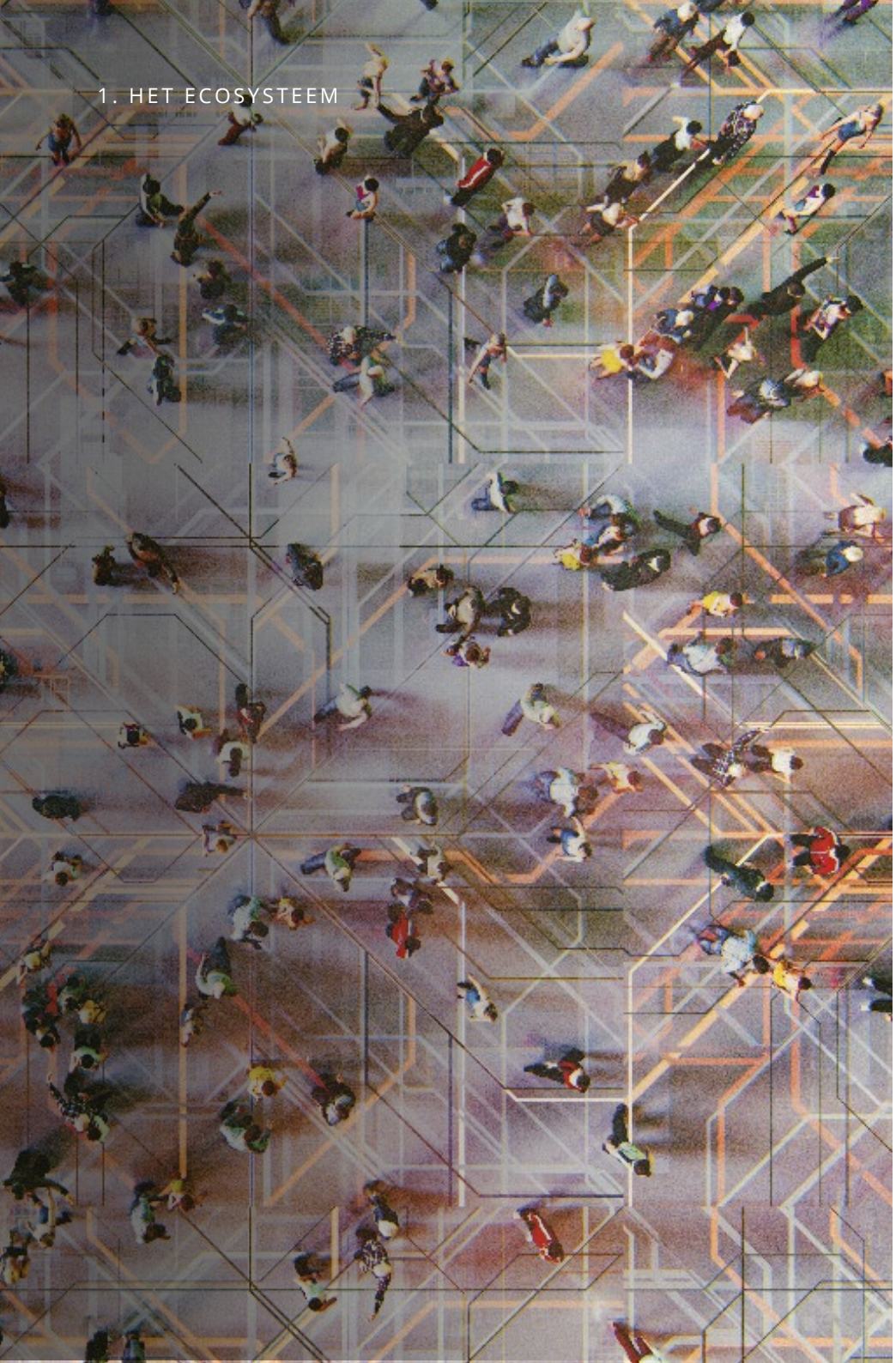
Hoofdstuk 1 geeft en omschrijving van het ecosysteem van mobiele toestellen en apps, waarbij wordt ingegaan op de locaties (technologie), actoren (verschillende stakeholders die een bepaalde rol vervullen binnen het ecosysteem) en omgevingsfactoren en relaties (*beantwoording deelvraag 1*).

Hoofdstuk 2 biedt een uitgebreide maar niet uitputtende klassieke risicoanalyse, waarbij cyberveiligheid-, privacy- en ethische risico's worden benoemd. Ook wordt in deze risicoanalyse stil gestaan bij specifieke risico's die al dan niet gelden voor minderjarige gebruikers (*beantwoording deelvraag 2*).

Hoofdstuk 3 beschrijft de Nederlandse en Europese wettelijke kaders die van toepassing zijn (zowel vigerend als opkomend) op elk type risico dat is benoemd in hoofdstuk 3, inclusief relevante uitdagingen op de toepasbaarheid van deze wetgeving (*beantwoording deelvraag 3*).

Hoofdstuk 4 bevat een overzicht van de maatregelen en initiatieven die buiten wetgeving om – zowel preventief als regressief – worden genomen om veilig gebruik van mobiele toestellen en apps te verbeteren (*beantwoording deelvraag 4*).

Hoofdstuk 5 vat de belangrijke inzichten die zijn opgedaan in het onderzoek samen, met daarbij de belangrijkste conclusies, en een overzicht van mogelijke maatregelen die kunnen worden genomen om veilig gebruik van mobiele apps nog verder te kunnen verbeteren (*beantwoording hoofdvraag*).



1. Het ecosysteem

In dit hoofdstuk zijn de verschillende onderdelen van het ecosysteem uitgewerkt.

1.1 **Locaties: verschillende technologielagen**
Allereerst wordt een beeld geschetst van de locaties waar de interacties tussen actoren plaatsvinden. Hiervoor worden verschillende lagen van technologie uiteengezet die bijdragen aan het functioneren van mobiele toestellen en apps.

1.2 **De stakeholders: diverse actoren en rollen**
Daarna wordt een overzicht gegeven van relevante actoren die een rol hebben binnen het ecosysteem. Het betreft hier partijen die betrokken zijn bij enerzijds het ontwikkelen en beheren van mobiele toestellen en apps (incl. ondersteunende platformen en infrastructuur), en anderzijds de gebruikers en misbruikers ervan. Ook wordt uitgelicht welke actoren betrokken zijn bij het stellen van kaders rond en het beoordelen en controleren van de ontwikkeling en het gebruik van de technologie.

1.3 **Omgevingsfactoren en relaties**
Vervolgens zijn onderdelen van de omgeving uitgediept die medebepalend kunnen zijn voor het functioneren van het ecosysteem en de wisselwerkingen die tussen deze omgevingsfactoren, actoren en locaties plaatsvinden, zoals verdienmodellen, dataverzameling en ontwerpkeuzes.

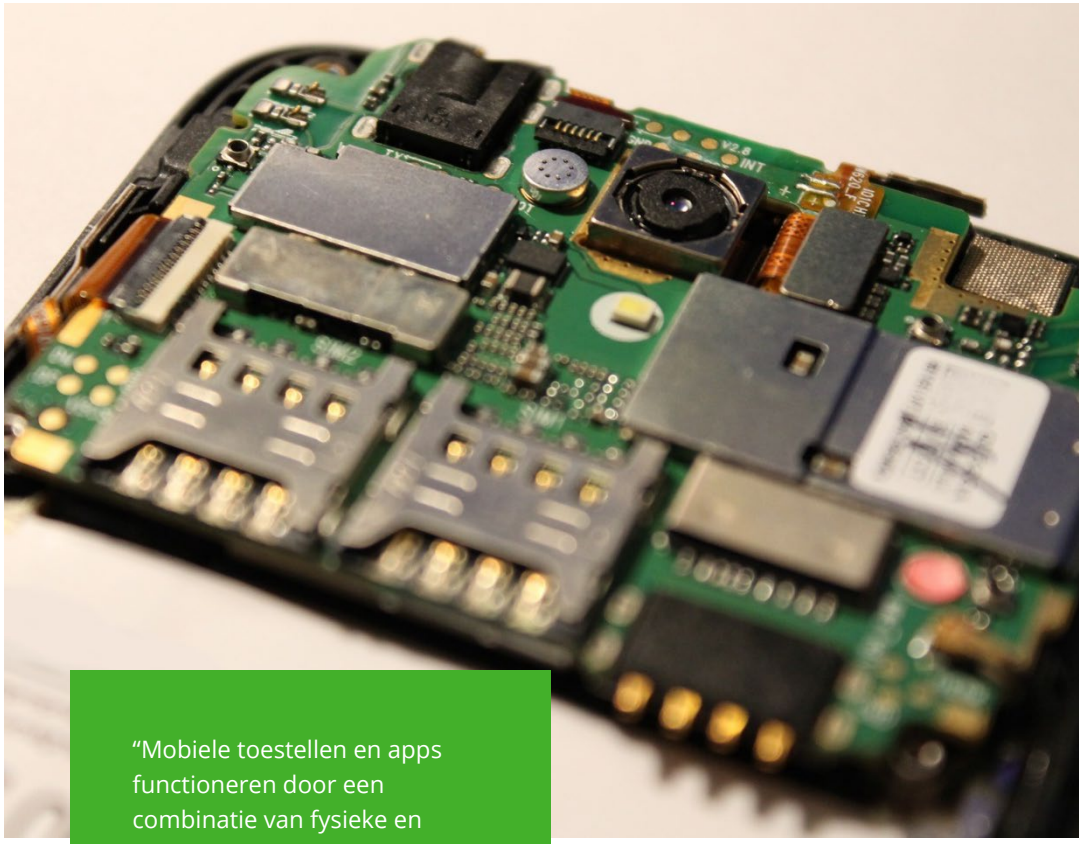
1.4 **Conclusie: elementen van het ecosysteem in beeld**
Gezamenlijk bieden deze elementen de basis om meer zicht te krijgen op risico's voor gebruikers (H2), relevante wet- en regelgeving (H3), en overige handelingsopties en maatregelen die kunnen worden getroffen om gebruikers beter te beschermen (H4).

1.1. Locaties: verschillende technologielagen

Er gaan meerdere technologielagen schuil onder de ‘applicatielaag’. Mobiele toestellen en apps functioneren door een combinatie van fysieke en virtuele lagen die nagenoeg constant met elkaar communiceren om zo de gewenste dienst aan de gebruiker te kunnen verlenen.

Om de wereld achter digitale diensten inzichtelijk te maken, ontwikkelde en visualiseerde onderzoeksinstelling Waag[18] een stack-model. In een breder verhaal waarin ook het fundament, het designproces en het perspectief van de burger wordt meegenomen, identificeert Waag verschillende technologielagen in de zogenaamde “Tech Stack”.[19] Het gaat om vijf lagen: infrastructuur, apparatuur, firmware en drivers, besturingssysteem en applicatie (zie figuur 4). Een viertal contextlagen wordt door Waag gezien als het cement tussen die technische lagen. Daarbij gaat het om (1) data en algoritmen in elke technologie laag, maar ook (2) standaarden en protocollen, (3) robuuste beveiliging tegen misbruik, en (4) de “dienst” die de technologielagen mogelijk maakt.[20] Data en algoritmen spelen bijvoorbeeld een rol in elke technologielaag en vormen tevens een verbindende factor tussen de lagen. In dit rapport komen de contextlagen op verschillende plekken in dit rapport aan de orde. Om het ecosysteem van mobiele toestellen en apps in kaart te brengen, worden op de volgende pagina allereest de vijf technologielagen nog kort toegelicht.

Bij elke laag zijn verschillende functionaliteiten van een mobiel toestel en de app gebaat. Een korte toelichting verheldert in het vervolg de rol van elke actor door de lagen heen.



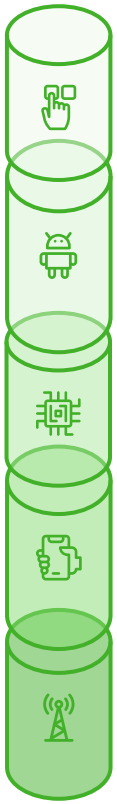
“Mobiele toestellen en apps functioneren door een combinatie van fysieke en virtuele lagen die nagenoeg constant met elkaar communiceren”

[18] Waag is een onderzoekinstelling die vanuit verschillende onderzoeklabs thema’s omtrent technologie en samenleving onderzoekt. Daarbij verkent Waag bijvoorbeeld de sociale en culturele impact van nieuwe technologieën, waarbij het handelingsperspectief van de burger centraal staat. Zie: https://waag.org/nl/over-waag.

[19] In opdracht van de Tijdelijke Commissie Digitale Toekomst van de Tweede Kamer ontwikkelde Waag De routekaart Digitale toekomst, waarin 'de Public Stack' wordt gepresenteerd. Deze wordt als alternatief gepresenteerd op “Private Stack” (van bedrijven met commerciële belangen) en de “State Stack” (van de overheid om burgers te bedienen en te begrijpen). Het streven van Waag is om iedere laag toegankelijk te maken en alternatieve technologie in kaart brengen of te ontwerpen. Zie: https://publicstack.net/

[20] In de praktijk wordt technologie vaak gebruikt als een service, zoals *het luisteren van nummer* via de Spotify-app op een telefoon en gekoppelde speakers of een koptelefoon (die al dan niet ook via een app – of besturingssystemen en firmware op de telefoon - worden aangestuurd. Zie: https://publicstack.net/layers/#service

Figuur 4: Onderdelen van de technology stack en de belangrijkste spelers op elke laag



Laag	Partijen
Applicatie De applicatielaag bevat de apps – software (bijv. Mail) – die kunnen draaien op een mobiel apparaat. Er zijn inmiddels miljoenen apps ontwikkeld die een gebruiker kan installeren op een mobiel toestel	App aanbieders, internet browsers en appwinkels (Apple AppStore en Google Play Store)
Besturingssysteem Een besturingssysteem is software die ervoor zorgt dat alle onderdelen van een toestel samenwerken en toegankelijk zijn voor apps. Bekende besturingssystemen binnen het ecosysteem van mobiele toestellen en apps zijn Android (Google) en iOS (Apple).	Apple OS, Google Android, op Android gebaseerde alternatieven, en op Linux gebaseerde systemen
Firmware en drivers De firmware laag verbindt de fysieke componenten van het apparaat met het besturingssysteem waarop het apparaat draait.	Drivers en firmware worden gemaakt door apparatuurfabrikanten
Apparatuur In de apparatuur laag valt alle apparatuur waar de gebruiker gebruik van maakt. Dit zijn laptops, smartphones, tablets, wearables, monitors, opladers etc. Binnen het kader van dit onderzoek betreft dit mobiele toestellen, bestaande uit smartphones, tablets en wearables zoals 'slimme' horloges en armbanden.	Aanbieders van mobiele telefoons, tablets, laptops, wearables, zoals Apple, Samsung, Huawei, LG, etc.
Infrastructuur Als onderste laag dient de fysieke infrastructuur van het netwerk die alle lagen verbindt. Hieronder vallen onder andere de internetkabels en telefoonmasten die de telecommunicatie faciliteren.	Netwerkaanbieders zoals T-Mobile, KPN en VodafoneZiggo

1.2. De stakeholders: diverse actoren en rollen

Aan de verschillende lagen in de technologie zijn ontwikkelaars te koppelen. Er zijn echter meer actoren die een rol hebben binnen het ecosysteem. Hieronder worden drie categorieën onder de loep genomen: de ontwikkelaars, de gebruikers en beïnvloeders. Gezamenlijk zijn zij verantwoordelijk voor functionaliteiten en mogelijkheden die mobiele toestellen en apps momenteel bieden.

De ontwikkelaars: betrokkenen bij het functionerend krijgen van toestellen en apps

Binnen het ecosysteem van mobiele toestellen en apps zijn een aantal rollen gerelateerd aan het ontwerp, de productie en het aanbieden van apps en mobiele toestellen. Dit zijn de 'ontwikkelaars'. Hieronder worden de rollen van ontwikkelaars die relevant zijn binnen dit onderzoek kort beschreven. Zoals hieronder naar voren komt is er een zekere keten in de tech stack en in het ecosysteem. De focus van dit onderzoek gaat specifiek in op de verantwoordelijkheden van de ontwikkelaars richting eindgebruikers.

Netwerkproviders (infrastructuur laag)

Netwerkproviders zijn beheerders van de infrastructuur van communicatienetwerken zoals vaste- en mobiele telefonie en 3G/4G/5G-internet. De dekking van mobiele netwerken in Nederland is bijna geheel onderverdeeld onder drie grote providers, namelijk, KPN, T-Mobile en VodafoneZiggo. Tele2 was tot kort geleden ook een van de grote netwerkproviders, maar is in 2018 gefuseerd met T-Mobile. Het dekkingsgebied van Tele2 is toen samengevoegd met het gebied van T-Mobile en is verder gegaan onder diens naam.[21]

De drie grote providers in Nederland bezitten ieder tussen de 20% en de 30% van het marktaandeel op het gebied van mobiele aansluitingen. Wanneer wordt gekeken naar het mobiele dataverbruik is T-Mobile koploper met meer dan 50% van de data. Het aandeel van KPN ligt rond de 25% en dat van VodafoneZiggo op ongeveer 15% tot 20%.[22] VodafoneZiggo is de grootste partij op het gebied van breedband met ongeveer 40% tot 45% van het marktaandeel. KPN volgt met 35% tot 40%. T-Mobile en Delta Fiber Nederland hebben beide een relatief klein marktaandeel van 5-10%. Overige netwerkaanbieders hebben een aandeel van maximaal 5%.[23]

Providers als Youfone en Ben – ook wel Mobile Virtual Network Operators (MVNO's) genoemd - maken gebruik van deze drie netwerkproviders. De drie grote providers verzorgen een hoge dekkingsgraad binnen Nederland wat betreft internet en mobiele telefonie[24] en waarborgen daarmee continuïteit, beschikbaarheid en veiligheid van netwerken.

Toestelfabrikanten (apparatuur laag)

Zoals eerder aangegeven, wordt in dit rapport gerefereerd aan smartphones, tablets en smartwatches wanneer er wordt gesproken over mobiele toestellen. Mobiele toestellen worden gemaakt door verschillende fabrikanten. Omdat smartphones het meest worden ontwikkeld, verkocht en gebruikt, ligt de focus hier op smartphonefabrikanten. Samsung en Apple zijn de grootste spelers op de Nederlandse smartphone markt. Samsung is koploper met 40% van het marktaandeel in 2020, gevolgd door Apple wat goed is voor 32% van het marktaandeel. De top 5 wordt verder aangevuld door Huawei (8%), Nokia (4%) en Motorola (4%).[25] Op het wereldtoneel ziet de top 5 van grootste merken er heel anders uit en wordt deze aangedreven door Aziatische merken als Xiaomi, OPPO, Huawei en Samsung.

"Samsung en Apple zijn de grootste spelers op de Nederlandse smartphone markt"

De smartphone markt is een erg competitieve markt waarbinnen continue innovatie een belangrijke rol speelt bij het verbeteren van de klantbinding en bij het behouden en vergroten van het marktaandeel.[26] Smartphonefabrikanten houden zich bezig met het ontwikkelen en aanbieden van een werkende smartphone. Dat wil zeggen dat fabrikanten primair verantwoordelijk zijn voor de ontwikkeling van de hardware – met

[21] 'Fusie T-Mobile en Tele2', t-mobile.nl
[22] *Telecommonitor Q1 2020* p. 3
[23] 'ACM Telecommonitor eerste kwartaal 2022 met nieuw interactief dashboard', acm.nl
[24] 'Welke provider heft het beste bereik?', unitedconsumers.com
[25] 'Nederland is koning smartphone, Samsung groter dan Apple', consultancy.nl 23 maart 2021.
[26] Cecere et. al., *Telecommunications Policy* 2014

daarbij horende specificaties als opslagcapaciteit, geheugen en batterijduur – en dat zij er daarnaast voor zorgen dat een besturingssysteem met bijbehorende appwinkel op het toestel wordt ingeladen.

Programmeurs (firmware laag)

De firmware laag verbindt de fysieke componenten van het apparaat met het besturingssysteem en draait direct op de hardware van het apparaat. Firmware vertaalt de input op de fysieke componenten naar een digitaal input die het besturingssysteem kan verwerken.. Ter illustratie: bij het gebruik van een toetsenbord, vertaalt de firmware de fysieke click op een letter naar een digitaal bericht dat verwerkt kan worden door het besturingssysteem.[27] Complexere onderdelen van een device gebruiken ook software componenten die 'drivers' genoemd worden. In gesimplificeerde termen faciliteert een driver, evenals firmware, ook de communicatie tussen het besturingssysteem en hardware componenten.[28]

Firmware en drivers worden normaal gesproken geschreven door de fabrikant van het betreffende apparaat, hoewel voor sommige apparaten ook open source firmware en drivers gemaakt worden. Een gebruiker van een apparaat interacteert niet zelf met de firmware en drivers en in de meeste apparaten werken firmware en drivers onzichtbaar op de achtergrond. Voor cyberveiligheid is het met name van belang dat firmware en drivers up-to-date gehouden worden, omdat geregeld ook in deze software laag kwetsbaarheden gevonden worden welke door hackers kunnen worden misbruikt.

Besturingssysteemontwikkelaars (besturingssysteem laag)

Een besturingssysteem is een stuk software dat ervoor zorgt dat alle onderdelen van een toestel samenwerken en toegankelijk zijn voor apps.[29] Er zijn twee marktpartijen die leidend zijn op het gebied van besturingssystemen, namelijk Apple (iOS) en Google (Android). Apple is dus zowel een grote ontwikkelaar op het gebied van hardware als op het gebied van software. Ook Google is een toestelfabrikant[30] maar heeft op dit gebied een zeer klein marktaandeel. Met het besturingssysteem Android, is Google echter een gigant op het wereldtoneel omdat deze kan worden ingeladen op veel verschillende smartphone merken.

De meeste versies van Android bevat kerncomponenten die onderdeel zijn van de Android Open Source Project[31]. Op veel van deze kerncomponenten zijn ook andere, minder bekende besturingssystemen gebaseerd, zoals FireOS[32] (een besturingssysteem dat draait op de Fire tablets van Amazon), LineageOS[33] en CalyxOS[34] (een besturingssysteem dat met name focust op privacy en cyberveiligheid van de gebruiker). Er is ook nog een groot aantal op Linux-gebaseerde open source besturingssystemen, en besturingssystemen die deels open source zijn.

Appwinkels (applicatie laag)

Een appwinkel is voor gebruikers een *app* op de smartphone, maar vormt ook een digitaal *distributieplatform* voor mobiele apps. Een appwinkel is bedoeld om het zoeken, beoordelen, kopen en downloaden van nieuwe functionaliteiten voor het mobiele toestel mogelijk te maken. Daarbij is het cruciaal gebleken dat de appwinkel een veilige en uniforme ervaring biedt voor de gebruiker. Om vertrouwen te genereren, hebben de huidige grootste appwinkels van Google (de Google Play Store, die draait op het Android besturingssysteem) en Apple (de App Store, die draait op het iOS-besturingssysteem) een rol gepakt om ontwikkelkaders vast te stellen waarbinnen de appontwikkelaars hun apps moeten bouwen en waarbinnen app ontwikkelaars hun apps moeten aanbieden.

Daarnaast zorgen de huidige appwinkels er momenteel voor dat ontwikkelde apps worden beoordeeld aan de hand van de omschreven ontwikkelcriteria en de aanwezigheid van andere beleidsstukken die gebruikers informeren en voorzien van een betere gebruikerservaring te faciliteren.[35] De appwinkel biedt een omgeving voor de ontwikkelaars, waar zij hun software kunnen presenteren. In zo'n winkel hebben ontwikkelaars dezelfde toegang tot hetzelfde publiek. De regels die appwinkels

[27] 'Firmware and drivers., publicstack.net
[28] 'What is a driver?', microsoft.com
[29] 'Operating system.', publicstack.net
[30] 'The helpful Google Phones.', store.google.com.
[31] 'Android Open Source Project', source.android.com
[32] 'Fire OS Overview', developer.amazon.com
[33] 'LineageOS Android Distribution', lineageos.org
[34] 'Your Phone Should be Private', calyxos.org
[35] Developer Policy Center, play.google.com; Apple Store Review Guidelines, developer.apple.com.

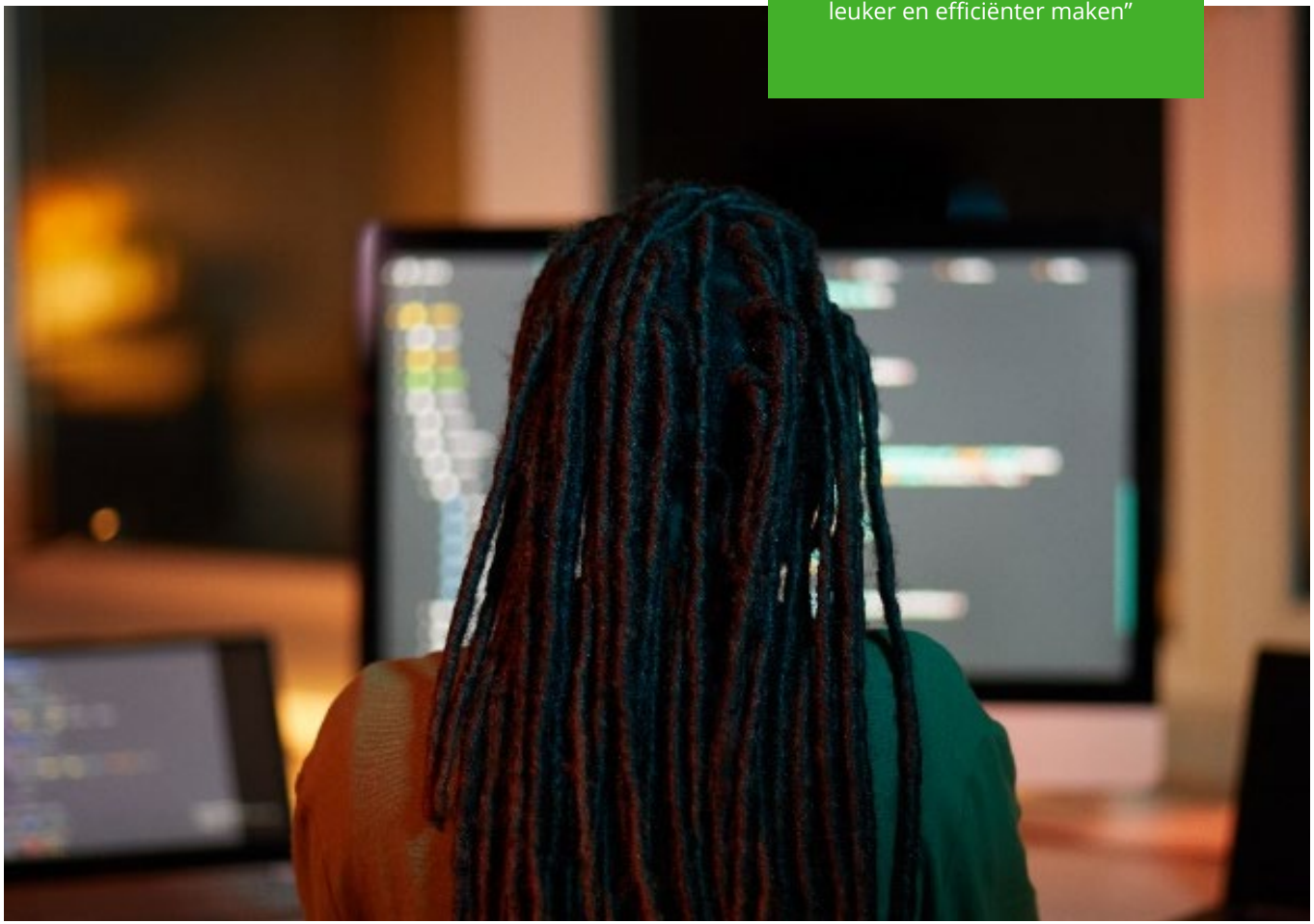
stellen, gelden voor alle ontwikkelaars die van de winkels gebruik willen maken. Appwinkels profileren zichzelf door strengere eisen of ontwikkelcriteria te formuleren op het gebied van cyberveiligheid en privacy. Gebruikers kunnen in bepaalde gevallen apps ook downloaden of aankopen buiten een appwinkel om. Dit wordt sideloading genoemd.

App ontwikkelaars (applicatie laag)

De app ontwikkelaar is het bedrijf, de instantie of de individuele personen die een app aanbieden aan gebruikers via een browserpagina of een van de appwinkels. In sommige situaties programmeert de ontwikkelaar de app zelf en zorgt zij ervoor dat deze volgens de aangegeven specificaties functioneert. Specificaties voor het ontwerp van de app en het beheer ervan na de ontwikkeling kunnen ook door andere partijen worden bepaald; de ontwikkeling van een app kan worden uitbesteed. Zo zijn er gespecialiseerde bureaus die apps bouwen, welke vervolgens door een andere partij – zoals de overheid of een commerciële partij – worden aangeboden.

App ontwikkelaars zijn continu op zoek naar manieren om apps te bedenken en aan te bieden die het leven simpeler, leuker en efficiënter maken. Tegelijkertijd zijn app-ontwikkelaars er vanuit commerciële drijfveren ook vaak op uit om gebruikers zoveel mogelijk tijd op hun app te laten spenderen. App ontwikkelaars zijn er in allerlei soorten en maten, van particuliere ontwikkelaars, tot enorme bedrijven en vanuit alle hoeken van de wereld. App ontwikkelaars zijn ook verantwoordelijk voor het ontwikkelen en beheren van de backbone van de app en hebben vaak eigenaarschap over de data die door de app wordt gegenereerd. Afhankelijk van hoe app ontwikkelaars hun app aanbieden (via een appwinkel of niet), zijn ze ook verantwoordelijk voor het informeren van gebruikers over zaken als privacy en cyberveiligheid.

“App ontwikkelaars zijn continu op zoek naar manieren om apps te bedenken en aan te bieden die het leven simpeler, leuker en efficiënter maken”



De gebruikers: betrokkenen bij interacties met toestellen en apps

Gebruiker zijn de consumenten van de apps en gebruiker van toestellen. Zij hebben regie over welk toestel zij aanschaffen en de apps die zij installeren – naast de soms standaard meegeleverde (en niet te verwijderen) apps. Er is echter een gelaagdheid van gebruikersposities: er valt een onderscheid te maken tussen de mate van gebruik (actieve of minder actieve gebruikers), en mate van bewustzijn van risico's die bijvoorbeeld worden bepaald door het al dan niet beschikken over kennis van achterliggende mechanismen en algemene digitale vaardigheden. Leeftijdsgroepen – ouderen en minderjarigen – houden hiermee verband. Ook zijn er groepen die wegens fysieke of mentale beperkingen minder gemakkelijk om kunnen gaan met mobiele toestellen en apps.

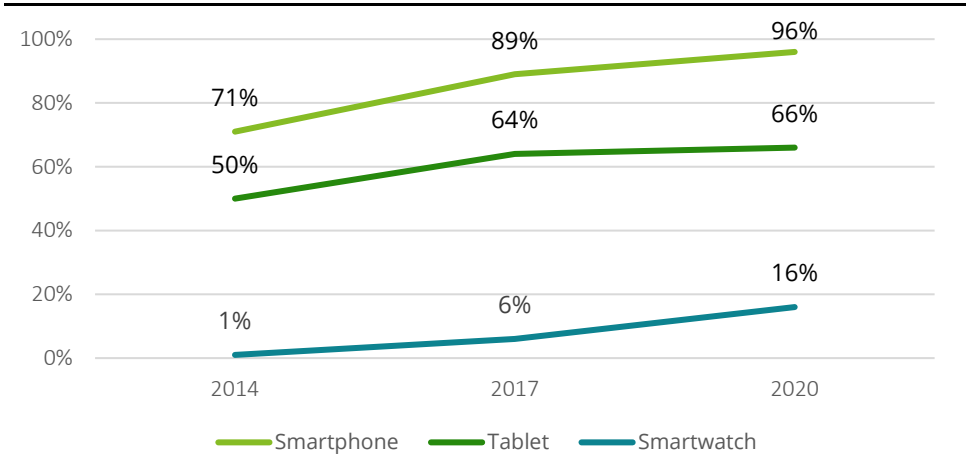
Gebruikers Algemeen

De afgelopen jaren (tussen 2014 en 2020), is het gebruik van mobiele toestellen gestaag toegenomen over alle leeftijdsgroepen vanaf 18 jaar oud. Dit blijkt uit het Global Mobile Consumer Survey Rapport 2020 van Deloitte (zie figuur 5). Van de landen die zijn onderzocht in dit onderzoek (o.a. China, Zweden, Duitsland en Groot-Brittannië), heeft Nederland met 96% de grootste smartphone adoptie.[36]

Ook gebruikers hebben een bepaalde rol in het ecosysteem; zij zijn medeverantwoordelijk voor het verantwoord gebruik van hun mobiele toestel en bijbehorende apps. De gebruiker is bijvoorbeeld zelf verantwoordelijk voor het instellen van pincodes en toegangscodes, het installeren van de aangeboden updates op de telefoon, alertheid bij het downloaden van apps (al dan niet via een appwinkel) en het niet onbeheerd achterlaten van het mobiele toestel.[37]

Om bovenstaande verantwoordelijkheden te kunnen dragen, is het belangrijk dat een gebruiker voldoende digitale vaardigheden heeft. Uit onderzoek van onder anderen het CBS blijkt dat Nederland het grootste aantal inwoners telt dat vaardig is met internet, computers en software van de onderzochte Europese landen. Ongeveer de helft van de Nederlanders tussen de 16 en 75 jaar oud had in 2019 meer dan

Figuur 5: Adoptie van mobiele apparaten in Nederland van 2014 tot aan 2020



basiskennis wat betreft digitale vaardigheden. Het gemiddelde in Europa ligt hier op 33% van de inwoners[38]. Bij basiskennis digitale vaardigheden moet worden gedacht aan zaken als:

- Informatie opzoeken op internet
- Bestanden verplaatsen en/of opslaan in de Cloud
- E-mailen, bellen via internet en het gebruik van sociale netwerken
- Online winkelen en apps installeren
- Tekstverwerkers en spreadsheets gebruiken
- Computerprogramma's schrijven en simpel programmeren

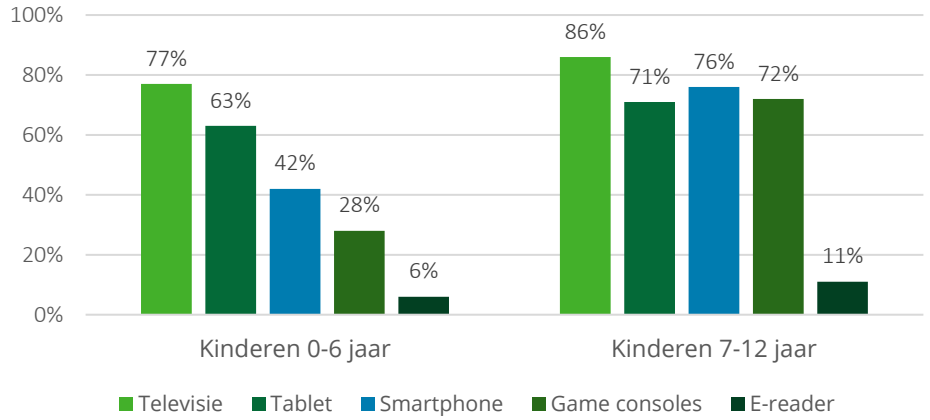
Bovenstaande zaken geven informatie over de gemiddelde gebruiker in Nederland. Echter, er zijn twee gebruikersgroepen of gebruiksondersteuners die in dit rapport expliciet extra aandacht krijgen: minderjarigen en ouders.

[36] 'Global Mobile Consumer Survey 2020: Dutch Edition', deloitte.com.
[37] 'Telefoon en tablet', laatjeniethackmaken.nl.
[38] 'Nederlanders in Europese kopgroep digitale vaardigheden', cbs.nl 12 februari 2020.

Toestelgebruik onder minderjarigen

Over de jaren heen wordt duidelijk dat minderjarigen steeds meer gebruik maken van technologische apparatuur, waaronder ook mobiele toestellen. Zoals in onderstaande cijfers te zien is (figuur 6), maken niet alleen volwassenen, maar ook minderjarigen gebruik van mobiele toestellen als smartphones en tablets.

Figuur 6: Gebruik van digitale apparatuur onder minderjarigen van 0 tot en met 12 jaar[39][40]



Zo'n 92% van de minderjarigen tussen de 10 en 18 jaar oud, gebruiken een mobiele telefoon. Het overgrote deel van deze mobiele telefoons betreft een smartphone met toegang tot het internet.[41] Minderjarigen gebruiken smartphones met name voor communicatiedoeleinden, informatievoorzieningen en entertainment.[42] Het belangrijkste doel voor minderjarigen om een smartphone te gebruiken, is om op die manier contact te kunnen onderhouden met hun vrienden of om nieuwe vrienden te maken.[43]

Hoewel jongeren verwachten dat ze digitaal vaardig zijn, blijkt uit onderzoek dat daar nog winst te behalen valt. Ondanks dat veel jongeren zijn opgegroeid met technologie, en ze dus ook goed weten hoe een apparaat moet worden opgestart en waar bepaalde knopjes voor dienen, weten ze vaak niet hoe veilig en slim gebruik te maken van deze technologie. Jongeren hebben bijvoorbeeld moeite met het beoordelen van de kwaliteit en betrouwbaarheid van informatie.[44] In vergelijking met volwassenen kunnen de apparaten en apps vaak beter besturen maar weten ze minder goed welke gevaren achter het besturingssysteem schuilen.

Ouders

Bij minderjarige gebruikers kunnen ouders (hiermee worden juridische ouders bedoeld) onderdeel worden van het ecosysteem. Het is namelijk mogelijk voor ouders van minderjarigen om "ouderlijk toezicht"-functionaliteiten te installeren op het mobiele toestel van hun kind. Met deze functionaliteiten, is het voor ouders mogelijk om beperkende maatregelen voor hun kinderen in te stellen op mobiele apparaten en apps.[45] Ook kunnen zij regels omtrent het gebruik van mobiele toestellen en apps opleggen aan hun kinderen, bijvoorbeeld hoeveel er dagelijks gebruik kan worden gemaakt van sociale media of over toestelvergrendeling. Om die reden kunnen ouders onderdeel zijn van het ecosysteem van mobiele toestellen en apps, en fungeren als actoren met een specifieke rol.

[39] *Iene Miene Media* 2021, p. 12.
[40] *Monitor Mediagebruik* 7-12 jaar 2021, p. 9.
[41] 'Jeugd en Mediagebruik', bibliotheeknetwerk.nl, bijgewerkt: 18 maart 2022
[42] *Jaarrapport Landelijke Jeugdmonitor*, 2019, p.161 - 164
[43] *Vanzelf Mediawijs?* 2016, p.23-24
[44] *Vanzelf Mediawijs?* 2017, p. 8.
[45] 'Ouderlijk toezicht gebruiken op de iPhone, iPad of iPod touch van uw kind', support.apple.com; 'Ouderlijk toezicht instellen op Google Play', support.google.com.

De beïnvloeders: betrokkenen bij het stellen van kaders en grenzen

Beïnvloeders zijn actoren die indirect invloed kunnen uitoefenen op het ecosysteem door de kaders te bepalen waarbinnen ontwikkelaars het ecosysteem kunnen ontwikkelen en gebruikers van het ecosysteem gebruik kunnen maken. Door het sturen van ontwikkelaars en het afbakenen van de manieren waarop gebruik gemaakt kan worden van het ecosysteem zorgen zij dat ontwikkelaars en gebruikers dus niet geheel vrij zijn (ofwel, los van externe invloeden) om hun eigen gang te gaan.

Beïnvloeders zijn onder andere regelgevers, handhavers, belangenorganisaties en bepaalde partijen of instituties, maar ook gebruikers zelf kunnen van invloed zijn op hetgeen de ontwikkelaars produceren. Andersom geldt dit ook: ontwikkelaars, wet- en regelgevers, handhavers, belangenorganisaties en partijen (zoals grote platforms) kunnen van invloed zijn op hetgeen gebruikers kunnen gebruiken binnen het ecosysteem.[46] In hoofdstuk 3 wordt dieper ingegaan op de bestaande en komende regelgeving die mede van invloed kan zijn op het gedrag van de ontwikkelaars en gebruikers binnen het ecosysteem, waarna in hoofdstuk 4 overige mogelijke maatregelen vanuit de overheid en andere belangenorganisaties worden besproken.

[46] Zie Gokzog et. al., *Journal of Business Research* 2021, p. 430-433; 'EU stemt in met een wet die apps als iMessage en Whatsapp laat samenwerken', nl.mashable.com 28 maart 2022; 'Deal on Digital Markets Act: EU rules to ensure fair competition and more choice for users', europarl,europa.eu 24 maart 2022.

1.3. Omgevingsfactoren en relaties

Binnen het ecosysteem zijn ook specifieke omgevingsfactoren en karakteristieken van belang die impact hebben op de werking van het ecosysteem en op de relaties tussen actoren.

Staat van technologie

Mobiele toestellen hebben een enorme ontwikkeling doorgemaakt in korte tijd. Deze revolutie van mobiele apparatuur biedt een gebruiker nieuwe manieren van werken, communiceren en informatievergaring. De efficiëntie en het gemak waarmee gebruikers toegang hebben tot informatie, andere gebruikers, bedrijven, overheden en andere onderdelen van een gebruikersomgeving, enorm toe.[47] Deze toename in gemak en comfort kan echter ook voor veiligheidsrisico's zorgen.[48] Diverse recente en opkomende technologische innovaties zijn (maar niet exclusief) van invloed op mobiele toestellen en apps.

Hierbij valt te denken aan de diverse sensoren die voor de nodige data-invoer zorgen, waaronder een camera, microfoon, en het touchscreen. Door dit soort sensoren kunnen fysieke karakteristieken, zoals een vingerafdruk, gezicht, iris of stem, van een gebruiker als invoerdata worden gebruikt voor identiteitsverificatie.[49] Daarnaast stellen allerlei netwerktechnologieën, zoals Bluetooth, WiFi, LiFi, 4G en 5G en NFC-technologie, de gebruiker in staat stellen om via hardware contact te maken met een netwerk of andere apparatuur. En wordt 'Global Positioning System' (GPS) gebruikt op mobiele toestellen, zoals smartphones, om te kunnen navigeren of te bepalen wat voor restaurants er bijvoorbeeld in de omgeving van de gebruiker. Ontwikkelingen op het gebied van post-kwantumcryptografie, web3.0 (incl. de metaverse en NFT's) zullen in de toekomst ook gereflecteerd worden in het gebruik van mobiele toestellen en apps, maar worden buiten beschouwing gelaten in dit onderzoek.

Verdienmodellen

Voordat wordt ingezoomd op dreigingen en risico's bij het gebruik van mobiele toestellen, is het relevant om inzicht te krijgen in welke verdienmodellen zoal worden gebruikt voor apps. Verdienmodellen zijn raamwerken die een bedrijf of ontwikkelaar kan toepassen zodat aan zijn of haar app geld kan worden verdiend. Dit is een integraal onderdeel van het business concept. Een business concept is een document wat doorgaans voorafgaand aan de ontwikkeling van de app wordt geschreven, en waar dus ook specifieke ontwerpkeuzes van zullen afhangen. Er zijn meerdere verdienmodellen denkbaar wanneer men geld wil verdienen aan apps. Ook zijn combinaties van onderstaande modellen mogelijk om app-inkomsten te kunnen maximaliseren.[50]

[47] *Digital Economy Outlook* 2020, p. 221.
[48] Kadëna, *Conference Budapest* 2017, p. 141.
[49] Kadëna en Ruiz, *Conference Budapest* 2017, p.140
[50] '8 Proven App Revenue Models for Your Mobile App', mobileaction.co 28 november 2019.

In-app adverteren

In-app adverteren is een van de meest populaire verdienmodellen in apps en wordt tegenwoordig ingezet op de meerderheid van apps. In dit model is de app zelf gratis te downloaden en te gebruiken. De ontwikkelaar van de app krijgt betaald door het weergeven van advertenties aan de gebruikers van de app. Om dat te kunnen doen, moet de ontwikkelaar samenwerken met een platform dat inkomsten uit advertenties genereert. Dit verdienmodel werkt alleen als er voldoende mensen aangesloten zijn op de app en dat deze mensen de app op regelmatige basis gebruiken, zodat er ook voldoende op in-app advertenties kan worden geklikt.

Om ervoor te zorgen dat mensen op advertenties klikken, is het steeds belangrijker geworden om advertenties te tonen die daadwerkelijk relevant zijn voor de individuele gebruiker. Dit vergt profiling en microtargetting. Het is voor advertentiebedrijven belangrijk om te weten wat voor gebruiker zij bedienen. Om deze reden worden (persoons)gegevens, die bij het gebruik van de app worden verzameld en profielen die op basis van die gegevens zijn ontwikkeld, gedeeld met de advertentiebedrijven zodat alleen relevante advertenties kunnen worden geplaatst.[51]

Betaalde Apps

De meeste apps in de verschillende appwinkels zijn gratis om te downloaden. Echter zijn er ook apps die alleen tegen betaling kunnen worden gedownload en gebruikt. Zodra de gebruiker heeft betaald en de app heeft gedownload, kan de app met alle daarbij horende attributen worden gebruikt. In dit model wordt alleen geld gegenereerd wanneer een nieuwe gebruiker de app koopt en download en dus is de ontwikkelaar erg afhankelijk van het aantrekken van nieuwe gebruikers in plaats van het behouden van gebruikers.[52]

In-app aankopen

Met in-app aankopen kunnen gebruikers functies, inhoudelijke zaken of diensten binnen een app aankopen. Er zijn verschillende typen in-app aankopen te onderscheiden.[53]

A. Aankopen van verbruiksartikelen en niet-verbruiksartikelen

Verbruiksartikelen zijn virtuele items die slechts één keer kunnen worden ingezet. Dit verdienmodel wordt bijvoorbeeld vaak toegepast in mobiele spelletjes waarbij extra levens, virtueel geld of andere ruilmiddelen kunnen worden aangeschaft. Als deze middelen eenmaal zijn gebruikt, kunnen ze niet nog een keer worden ingezet.

Niet-verbruiksartikelen zijn vaak premiumfuncties of virtuele items die kunnen worden aangekocht en niet verlopen. Deze artikelen kunnen dus meerdere keren worden gebruikt. Een voorbeeld van een niet-verbruiksartikel is bijvoorbeeld een extra “skin” voor een karakter in een mobiel spel.

B. Freemium model

Met freemium wordt een model bedoeld waarbij apps gratis zijn om te downloaden en twee typen functies hebben: basisfuncties die gratis te gebruiken zijn, en geavanceerdere functies die te gebruiken zijn wanneer de gebruiker daarvoor betaalt. Het doel is om de gebruiker de mogelijkheid te geven om alle basisfuncties uit te proberen en ervan te genieten, op zo’n manier dat hij of zij dan voor de geavanceerde functies wil gaan betalen. Voorbeelden hiervan zijn het aanbieden van demo’s of gratis proefperiodes waarbij sommige functies nog afgesloten zijn totdat de gebruiker daadwerkelijk betaalt.

[51] A. Priester, ‘Data Privacy in Mobile Marketing: Contradictory or Complementary?’, customlytics.com 8 oktober 2021.
[52] ‘8 Proven App Revenue Models for Your Mobile App’, mobileaction.co 28 november 2019.
[53] Onderstaande beschrijvingen (voor in-app aankopen) zijn gebaseerd op ‘8 Proven App Revenue Models for Your Mobile App’, mobileaction.co 28 november 2019.

Verdienen aan data

Om een app gratis te houden en volledig de focus te houden op de gebruikerservaring, kan ervoor worden gekozen om gebruikersdata te verkopen.[54] Het gaat hier vaak om informatie over de apparaten van de gebruikers, zoals netwerktypes, locaties, IP-adressen etc. Gebruikers moeten – onder Nederlandse wetgeving – ervan op de hoogte worden gebracht dat dit soort gegevens kunnen worden verstrekt aan derde partijen. Het is hierbij belangrijk dat de gebruiker wordt geïnformeerd over dit verdienmodel, bijvoorbeeld middels een privacyverklaring of de algemene voorwaarden van de app en het is volgens wetgeving in veel gevallen noodzakelijk dat een gebruiker toestemming geeft voor het delen van data met derde partijen. Toestemming is in deze gebaseerd op het idee van een contract en dient volledig geïnformeerd ondubbelzinnig gegeven te worden. Waar de data in werkelijkheid terecht komt en op welke wijze daar gebruik van wordt gemaakt is in de werkelijkheid niet te controleren voor een individuele gebruiker. Het aantal databases waarin persoonsgegevens te vinden zijn is voor zowel een gebruiker, als voor bedrijven, niet te overzien en de herkomst niet makkelijk te herleiden. Dat compliceert de waarde van het geven van toestemming.[55].

Donaties en crowdfunding

Met crowdfunding kan een project – zoals het bouwen van een mobiele app – worden gefinancierd door een grote groep mensen die allemaal een klein deel van het totale bedrag investeren.[56] Meestal wordt er van crowdfunding gebruik gemaakt aan het begin van een project, wanneer de ontwikkelaar niet over de financiële middelen beschikt om het project te bekostigen, maar er wel een hoop potentie en waarde in het project wordt gezien.
Er kan ook gebruik worden gemaakt van donaties als verdienmodel. Dit model is echter over het algemeen niet erg betrouwbaar of consistent.[57]

Abonnementen

Abonnementen worden vaak gebruikt voor streamingdiensten en nieuwsapps. Dit verdienmodel wordt tegenwoordig ook veel gebruikt in andere app categorieën, zoals in lifestyle apps. Wanneer de gebruiker ergens een abonnement op heeft dan wordt er een zeker bedrag van het account van de gebruiker afgeschreven op regelmatige basis, meestal maandelijks of jaarlijks.[58] In veel gevallen verloopt verlenging van het abonnement automatisch maar soms vereist dit ook een jaarlijkse of periodieke handmatige vernieuwing van de gebruiker.

[54] 'Mobile App Monetization Strategies – Which Model to Choose to Make a Profit?', asperbrothers.com 15 november 2021; Cecere et. al, *Conference of IAOS* 2018, p. 7.
[55] *Factsheet Bescherming Persoonsgegevens*, 2021, p. 1.
[56] F. Lewis, 'What Is Crowdfunding?', thebalance.com bijgewerkt 31 december 2021.
[57] B. Kontsevoi, 'Mobile App Monetization Part 4: Revenue Generation Models', forbes.comv 30 juni 2020.
[58] '8 Proven App Revenue Models for Your Mobile App', mobileaction.co 28 november 2019.

Relevante ontwerpkeuzes
De verschillende verdienmodellen die hierboven staan beschreven, zijn vaak gericht op het aantrekken en behouden van gebruikers. Als gebruikers vaker en langer van een app gebruikmaken, is de kans namelijk groter dat ze op advertenties klikken of aankopen doen binnen de app en dit genereert omzet. Dit impliceert dat ontwikkelaars ontwerpkeuzes moeten maken die ervoor zorgen dat gebruikers continu geboeid en behouden blijven. Dit wordt ook wel gebruikersbetrokkenheid en gebruikersbehoud genoemd. Hieronder worden een aantal relevante strategieën voor betrokkenheid en behoud kort toegelicht.

Efficiënte onboarding

Wanneer een gebruiker een bepaalde app voor het eerst downloadt, installeert en gebruikt, is het belangrijk dat het eerste gebruik zo ongecompliceerd mogelijk gebeurt. Een van de middelen die app-ontwikkelaars daarvoor kunnen inzetten, is door het aantal noodzakelijke stappen om een account aan te maken of in te loggen, zo minimaal mogelijk te houden. Om die reden geven app-ontwikkelaars gebruikers vaak de mogelijkheid om snel in te loggen via een ander bestaand account zoals een Google-, Facebook- of Apple-account, zodat de gebruiker niet de moeite hoeft te nemen om een extra account voor een specifieke app aan te maken.[59]

In-app berichten en push-notificaties

Afhankelijk van de functionaliteit van een app, zullen gebruikers meer of minder geneigd zijn om continu gebruik te maken van de app. De app-ontwikkelaar heeft als doel om de gebruiker zo veel en zo lang mogelijk gebruik te laten maken van de app en dus zal de ontwikkelaar middelen inzetten om gebruikers continu ervan te overtuigen en herinneren om gebruik te maken van de app. Dit gebeurt onder andere door middel van push-notificaties en in-app berichten.

Bij dit soort berichten is het van belang dat ze goed afgestemd zijn op de behoeften en wensen van de gebruiker. Niet elke gebruiker heeft behoefte aan dezelfde typen berichten. Daarom is het ook belangrijk dat de gebruikersgroep wordt gesegmenteerd, zodat gebruikers alleen berichten krijgen die ervoor zorgen dat ze worden geactiveerd om weer gebruik te maken van de app. Berichten die niet interessant zijn voor de gebruiker zouden namelijk een averechts effect van irritatie tot gevolg kunnen hebben.[60]

Het gebruikersbehoud kan nog verder worden verhoogd door middel van locatie-gebaseerde berichten. Dit is bijvoorbeeld het geval wanneer een gebruiker met zijn of haar mobiele apparaat een winkel binnenloopt en meteen een bericht ontvangt waarop nieuwe aanbiedingen van die winkel worden afgekondigd.[61] In dit soort berichten staat dus content die voor de gebruiker zeer relevant en actueel is op dat moment.

[59] '5 Methods For Increasing App Engagement & User Retention', clearbdridgemobile.com.
[60] '5 Methods For Increasing App Engagement & User Retention', clearbdridgemobile.com.
[61] '25% of Users Abandon Apps After One Use', uplandsoftware.com.

Algoritmen

Een algoritme kan worden gedefinieerd als een goed gedefinieerde rekenprocedure die een waarde(reeks) als invoer neemt, en aan de hand daarvan vervolgens een uitvoer waarde(reeks) produceert.[62] Een simpel offline-praktijkvoorbeeld hiervan is bijvoorbeeld: zodra de hoeveelheid toiletpapier in huis is gereduceerd tot nog maar één rol, wordt toiletpapier op het boodschappenlijstje bijgeschreven. Tegenwoordig, wordt met algoritme een systeem bedoeld waarmee bepaalde processen kunnen worden geautomatiseerd, bijvoorbeeld filteren, ordenen, zoeken, etc. Deze algoritmen worden vaak toegepast in digitale omgevingen, zo ook in apps.

Simpele algoritmen kunnen al voor de nodige efficiëntie en gebruikersgemak zorgen, zoals sorteer-algoritmen, zoek-algoritmen, en hashing-algoritmen.[63] Maar tegenwoordig worden ook enorm complexe algoritmen gebruikt om gebruikers (betrokken) te houden en om inhoud of diensten te personaliseren. In recente jaren is door meerdere onderzoeken aangetoond, dat gebruikers naar die bedrijven of services gaan waar naar ze geluisterd wordt en waar producten en diensten op hun voorkeuren worden afgestemd.[64] Dit betekent dat bedrijven hun klanten en de gebruikers van de apps moeten leren kennen. Hiervoor worden veel gebruikersdata verzameld: Wie zijn ze? Waar houden ze van? Op deze zaken wil een app ontwikkelaar namelijk kunnen inspelen. Omzet is ervan afhankelijk. Daarmee kan het verdienmodel achter een app een perverse prikkel betekenen.

Hieronder zullen een aantal voorbeelden kort worden geschetst om het gebruik van algoritmen en personalisatie beter toe te lichten.

- Om de gebruikersbetrokkenheid te verhogen, maakt een foto-gedreven sociaal netwerk gebruik van machine learning voor computervisie. Met dit algoritme is het sociale netwerk in staat om gezichten in foto's en filmpjes te onderscheiden om er vervolgens leuke elementen aan toe te kunnen voegen, zoals een bril, hoeden, konijnenoren en regenbogen.[65]
- Een dating app gebruikt een algoritme om ervoor te zorgen dat de gebruiker makkelijker een match kan vinden. De app toont gebruikersfoto's in willekeurige volgorde aan andere gebruikers. Vervolgens analyseert het op machine learning gebaseerde algoritme hoe vaak zo'n foto leuk gevonden wordt en hoe vaak zo'n foto wordt afgewezen. Zo leert het algoritme welke foto's de meest aantrekkelijke foto's zijn. Aan de hand van deze kennis verandert het algoritme vervolgens de volgorde van gebruikersfoto's door de meest leuk gevonden foto's als eerste te plaatsen.[66]
- Content-gebaseerde filters zijn filters die gebruikersvoorkeuren over typen items verkrijgen en vervolgens vergelijkbare items aanbevelen. Dit gebeurt bijvoorbeeld in streamingdiensten, waar bijvoorbeeld nieuwe true crime documentaires worden aanbevolen, nadat een gebruiker een aantal films in dit genre heeft gekeken. Dit heeft bepaalde voordelen. Namelijk een gebruiker zal content te zien krijgen waar hij of zij in is geïnteresseerd, maar het kan ook filterbubbels met zich meebrengen.[67] Het algoritme baseert zich namelijk op bestaande interesses van de gebruiker, maar het algoritme is niet zo gemaakt dat deze de interesses van de gebruiker uitbreid. [68]

Doordat algoritmes steeds 'slimmer' en geavanceerder worden – denk bijvoorbeeld aan op neurale netwerken gebaseerde algoritmes – zijn deze algoritmes steeds vaker bruikbaar om (complexe) problemen op te lossen.

[62] Cormen et. al 2009.
[63] Krishnakumar, '5 Algorithms Every App Developer Should Know and Understand', blog.eduopnix.com 10 augustus 2017.
[64] Dit geldt voor zowel online als offline producten en diensten. Zie: *The Deloitte Consumer Review. Made-to-order: The rise of mass personalization,* 2015, p. 5.
[65] 'Top Machine Learning Mobile Application Examples', theappsolutions.com.
[66] 'Introducting Smart Photos – For The Most Swipeworthy You', tinderpressroom.com.
[67] *Filterbubbels in Nederland* 2019, p. 2-13.
[68] 'Content-based Filtering Advantages & Disadvantages', developers.google.com.

Karakteristieken van de digitale wereld
Veel mobiele apps en functionaliteiten worden gefaciliteerd door een internetverbinding. Om die reden is het ook belangrijk om een aantal karakteristieken van het internet te benoemen die relevant zijn binnen dit onderzoek. De drie karakteristieken die hieronder worden beschreven zijn eerder geduid als onderdeel van 28 mechanismen van immoreel en schadelijk gedrag in het rapport 'Online Ontspoord' dat in 2021 door het Rathenau Instituut is gepubliceerd.[69] Er is voor gekozen om de onderste drie uit te lichten omdat deze het meest relevant zijn voor het verder duiden van de risico's (H2).

Anonimiteit
De meest basale definitie van anonimiteit is "zijn zonder naam". Iemand is dus anoniem als zijn of haar identiteit niet bekend is.[70] Anonimiteit is inherent verbonden aan het gebruik van internet. Het feit dat er, anders dan in de fysieke wereld, geen ogen lijken te zijn die meekijken, is voldoende om anonimiteit te ervaren. Anonimiteit heft remmingen op en kan leiden tot onverwacht vriendelijke en vrijgevige handelingen, of het kan leiden tot wangedrag zoals grof taalgebruik en illegale praktijken.[71] Beide kenmerken zijn zichtbaar in online gemeenschappen, waar individuen veilig hun hart kunnen luchten en hun mening kunnen uiten – meningen die vaak ontmoedigd of ontkent worden in hun offline dagelijks leven – hoe hatelijk of beledigend dat ook zou kunnen zijn voor hun virtuele medegebruikers.[72]

Continue beschikbaarheid
Het internet is voor vrijwel alle mensen in Nederland op ieder moment beschikbaar. Er zit geen stopknop op het internet en het wordt door de meesten (87% van mensen boven de 12 jaar oud) dagelijks gebruikt, met name via smartphones.[73] Dit betekent ook dat het internet van cruciaal belang is geworden voor zowel individuen als bedrijven. Er is een afhankelijkheid ontstaan van het internet. Vaak is het een gegeven dat internet nodig is en is er geen compleet vrije keuze om van het internet gebruik te maken. Daarnaast is het internet onmiddellijk voorhanden. Op elk gewenst moment kan een gebruiker gebruik maken van services die door middel van het internet beschikbaar worden gesteld. [74]

Ogenschijnlijke wetteloosheid
In de offline wereld zijn normen en waarden vrij duidelijk vastgesteld. Het is voor de meeste mensen duidelijk dat sommige gedragingen in het openbaar niet door de beugel kunnen. Echter zijn deze omgangsnormen op het internet aanzienlijk minder duidelijk. Er wordt al sinds het begin van interacties op het internet gezocht naar de juiste etiquette in hoe met andere gebruikers moet worden omgegaan. Andere gebruikers lijken op het internet ook minder "echt" omdat interacties op het internet vaak niet 'oog in oog' verlopen.[75]

Daarnaast is er sprake van een ogenschijnlijke wettenloosheid, omdat de interacties op het internet niet vallen onder een specifieke jurisdictie waarbinnen bepaalde wetten gelden. Het internet is grensoverschrijdend en er zijn per land verschillende wetten op de interacties die plaatsvinden middels deze mobiele online ecosystemen. Een gebruiker kan op één dag interacties hebben met instanties en gebruikers vanuit verschillende landen. Wanneer er misstanden plaatsvinden op het internet, kan de dader dus vaak niet worden gepakt omdat opsporing in het buitenland lastiger is omdat daar samenwerking voor nodig is en omdat er in andere landen allicht andere regels gelden.[76]

[69] Van Huijstee et. al. 2021, p. 76 – 91,
[70] Chauhan en Kumar Panda 2015.
[71] Kang et. al. 2013, p 2.
[72] Brabazon 2012.
[73] J. Arends, 'Interetgebruik van huishoudens en personen', longreads.cbs.nl 2021.
[74] Van Huijstee et. al. 2021, p. 80-81.
[75] V. Shea, *The core rules of netiquette*, albion.com.
[76] Van Huijstee et. al. 2021, p. 90-91.

1.4. Conclusie: elementen van het ecosysteem in beeld

Dit hoofdstuk geeft een inzicht in het complexe ecosysteem van mobiele toestellen en apps, wat volgens de gehanteerde definitie het geheel van locaties, actoren, omgevingsfactoren en de relaties daartussen omvat. Verschillende actoren kunnen worden geïdentificeerd en begrepen als een keten; iedere actor oefent op één of meerdere 'locaties' invloed uit op dit ecosysteem, waardoor bepaalde afhankelijkheden en kwetsbaarheden ontstaan.

De verschillende actoren opereren niet in een vacuüm. Zo worden de ontwikkelaars van apps in hun doen en laten gestuurd (en soms beperkt) door de wetgevende, uitvoerende en rechterlijke machten, toezichthouders en belangenorganisaties. Een complicerende factor is dat de omgevingsfactoren, die de relaties tussen de verschillende actoren op de verschillende locaties beïnvloeden, aan verandering onderhevig zijn. Zo stellen innovatieve op machine learning gebaseerde modellen de ontwikkelaars van apps in staat om het ontwerp van een specifieke app dusdanig te verbeteren dat bepaalde verdienmodellen aantrekkelijker worden. Hierdoor zullen gebruikers langduriger gebruik maken van de app, waardoor er meer aan de gebruiker verdient kan worden.

Het ecosysteem dat in dit hoofdstuk is beschreven is dus complex en versnipperd. Doordat ongeveer elke Nederlander onderdeel is van dit ecosysteem en door diffuse spreiding van verantwoordelijkheden, door de verschillende technologielagen en door de aanwezige omgevingsfactoren (zoals verdienmodellen die bepaalde prikkels behelzen), kunnen er kwetsbaarheden en risico's ontstaan die een grote impact kunnen hebben op gebruikers. In het volgende hoofdstuk wordt hier verder op in gegaan.

2. Kwetsbaarheden en risico's

In dit hoofdstuk worden de kwetsbaarheden en risico's voor de gebruiker van mobiele toestellen en apps onder de loep genomen. In het publieke en politieke debat worden diverse zorgen geuit over gevolgen van mobiele toestellen en apps voor gebruikers. Daarbij is er nadrukkelijke aandacht voor negatieve gevolgen voor minderjarigen als bijzondere gebruikersgroep.[77] De debatten worden grotendeels gedreven door incidenten, die verschillen in aard en omvang. In dit hoofdstuk zijn de belangrijkste zorgen geduid en geclusterd.

Binnen de drie clusters (sociaal, privacy & ethiek, cyberveiligheid) worden in totaal acht typen incidenten in detail toegelicht. Middels een klassieke risicoanalyse wordt zo een – niet uitputtend – overzicht gecreëerd van verschillende incidenten. Het doel hiervan is om inzichtelijk te maken hoe kwetsbaarheden en risico's zich verhouden tot verschillende lagen in de technologie (locaties), spelers binnen het ecosysteem (actoren) en de omgevingsfactoren die daarbij een rol spelen. De categorisering op hoger abstractieniveau vormt de basis voor de verdere bestudering van mogelijke en effectieve maatregelen.

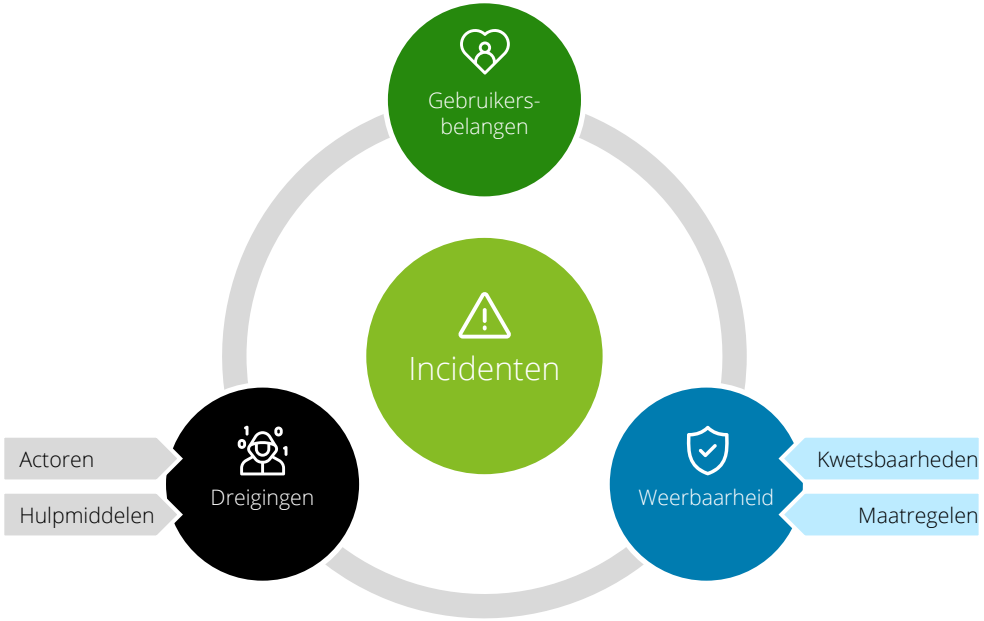
[77] Zie bv. *Factsheet beeldschermgebruik van dichtbij* 2019; *Tipsheet Mediagebruik* 2017; 'Jonge kinderen zitten graag op TikTok. Maar hoe veilig is het daar?', nrc.nl 27 januari 2020.

De dreigingen voor en kwetsbaarheden van *individuele gebruikers* van mobiele toestellen en apps staan centraal in deze risicoanalyse. De alomtegenwoordigheid van mobiele toestellen en apps heeft daarnaast een impact op grotere maatschappelijke en geopolitieke vraagstukken, maar dat is niet de focus van dit onderzoek. Om incidenten te kunnen categoriseren, is het behulpzaam om voor verschillende typen incidenten die ontstaan bij het gebruik van mobiele toestellen en apps de dreigingen, de gebruikersbelangen[78] en de weerbaarheid te identificeren.

Figuur 7 is een schematische weergave van de verschillende risico-componenten. In de volgende paragrafen worden de verschillende typen incidenten, per categorie, geanalyseerd met behulp van dit raamwerk. In acht tabellen wordt steeds op eenzelfde manier een type incidenten uitgelicht:

- De eerste kolom bevat een aantal concrete voorbeelden van **incidenten** die gerelateerd zijn aan het gebruik van mobiele toestellen en apps en de negatieve gevolgen voor gebruikers.
- De tweede kolom benoemd de **dreiging**. De incidenten zijn het gevolg van de dreiging die zich manifesteert. Om te duiden wat de dreiging behelst wordt gekeken naar de actoren die betrokken zijn en naar de middelen die door deze actoren worden ingezet om hun doelen te bereiken.
- De derde kolom stipt aan welke **gebruikersbelangen** onder druk staan in zo'n situatie. De **gebruikersbelangen** zijn hetgeen dat bescherming behoeft.
- De vierde kolom gaat over de **weerbaarheid** tegen de dreiging. Dit wordt bepaald door de kwetsbaarheden die er zijn (waarlangs actoren bij de gebruiker kunnen komen) en de maatregelen die worden getroffen (om de gebruikersbelangen te beschermen tegen deze actoren). Maatregelen die worden getroffen kunnen technisch, juridisch, of van sociaal-maatschappelijke aard zijn. In dit hoofdstuk beperkt de analyse zich tot waar momenteel op wordt ingezet. In H3 en H4 zijn de relevante wettelijke kaders en andersoortige drukmiddelen, die de weerbaarheid tegen risico's op incidenten kunnen vergroten, uitgebreider uitgewerkt.

Figuur 7: Een schematische weergaven van de risico-elementen



[78] In de context van risicomanagement waarin het model normaliter wordt ingezet, wordt gesproken van "assets" die veelal tastbaar zijn. In het kader van dit onderzoek wordt gesproken van "gebruikersbelangen' en worden naast tastbare ook niet-tastbare zaken meegenomen, zoals belangen, eigendommen en kwetsbaarheden die een sociale of psychische aard hebben.

2.1. Sociale aspecten: schadelijk gedrag van (mede)gebruikers

Het eerste type incidenten ontstaat door sociale aspecten en schadelijk gedrag van (mede)gebruikers. Wanneer het gaat om risico's of ongewenst en schadelijk gedrag, is een focus op technische aspecten en relaties binnen het ecosysteem van mobiele toestellen en apps, niet voldoende om de problematiek te verklaren. Verschillende problemen waar gebruikers mee worden geconfronteerd, hangen samen met eigenschappen die nou eenmaal onderdeel zijn van de aard van de mens en het menselijk gedrag. Wat gebruikers van mobiele toestellen en apps doen en laten, is in sommige opzichten een *reflectie* of een *uitvergroting* van grotere sociale en maatschappelijke kwesties. Gedragingen van gebruikers kunnen echter worden versterkt door karakteristieken van de omgevingsfactoren in het ecosysteem, zoals ogenschijnlijke wetteloosheid, anonimiteit en continue beschikbaarheid. Daarnaast is het bereik op online omgevingen vele malen groter en is de controle op hoe informatie wordt verspreid vele malen kleiner dan in de offline wereld.

In het rapport "Online Ontspoord" van het Rathenau Instituut worden diverse voorbeelden van immoreel en schadelijk gedrag besproken die ofwel alléén online kunnen plaatsvinden, ofwel een online variant zijn van gedrag dat ook in de offline wereld voorkomt.[79] Wat er in de digitale wereld aan gebruikersinteracties via apps op mobiele toestellen gebeurt, kan daarnaast ook effect hebben op de fysieke realiteit en de belevingswereld van de gebruikers. De negatieve gevolgen van dit soort schadelijke interacties hebben met name betrekking op de mentale- en fysieke gesteldheid van de gebruiker die het doelwit is. Allerlei nieuwe vormen van pesten ontstaan online, waaronder intimidatie, haatzaaiing en laster. Wraakporno, een vorm van intimidatie is bijvoorbeeld een fenomeen dat via het internet is ontstaan. Hierbij worden seksueel expliciete afbeeldingen of video's van een persoon online geplaatst, zonder dat deze persoon daarmee heeft ingestemd. Vaak worden hier ook persoonlijke gegevens van het slachtoffer aan toegevoegd zoals adresgegevens en telefoonnummers.[80]

Ook op sociale media platformen kunnen zaken als smaad en laster op grote schaal voorkomen. Roddels, nepnieuws en berichten die de intentie hebben om mensen te schaden, kunnen elk moment van de dag de wereld in worden geslingerd, waardoor mensen aan de publieke schandpaal kunnen worden genageld en 'trial by media' – wanneer mediaberichtgeving een wijdverbreide perceptie van schuld of onschuld creëert voordat er überhaupt gedegen onderzoek is gedaan of een uitspraak van de rechtbank is geweest – op de loer ligt.[81] Opjutten tot schadelijk gedrag kan ook veel voorkomen op online platformen. Dit is bijvoorbeeld goed zichtbaar bij populaire maar extreme "challenges"[82] of trends, die soms het nieuws halen vanwege de gevaarlijke situaties, verwondingen of verslavingen die erdoor kunnen ontstaan.[83] Ook strafbare feiten zoals kinderlokkerij, chantage en afpersing (bijvoorbeeld 'sextortion'), worden online gepleegd en ook zaken als excessief en ongecontroleerd gebruik van mobiele toestellen, apps en online omgevingen zijn een grote zorg.

De problematiek en het schadelijke gedrag dat hierboven wordt beschreven is niet alleen zichtbaar of mogelijk op mobiele toestellen of mobiele apps. Op elk type apparaat waar dit soort interacties tussen gebruikers kunnen plaatsvinden, zal dit schadelijke gedrag voorkomen. Echter, dit soort interacties vinden wel vaak plaats op mobiele toestellen en apps, door de specifieke karakteristieken van de digitale wereld, zoals continue beschikbaarheid. Hierdoor kunnen gebruikers hun medegebruikers (het eerste type dreiging in deze categorie, zie tabel 1) of zichzelf (het tweede type dreiging in deze categorie, zie tabel 2) extra gemakkelijk dwarszitten via de kanalen die op mobiele toestellen en via mobiele apps worden geboden.

[79] Er wordt een taxonomie geïntroduceerd waarin 22 fenomenen van online schadelijk en immoreel gedrag worden gecategoriseerd in: (1) online informatie-manipulatie, (2) digitaal vigilantisme, (3) online haat, (4) online pesterij en geweld, (5) cyberbedrog, (6) online zelfbeschadiging.
[80] 'Wat betekent sextortion en wat kunnen we betekenen voor slachtoffers?', fondsslachtofferhulp.nl.
[81] Zie bv. E. Kreulen, 'The Voice: Trial by media?', trouw.nl 28 januari 2022.
[82] Voorbeelden van populaire challenges zijn: de Cinnamon Challenge (grote hoeveelheden kaneel doorslikken), de Choking Challenge (wurgen tot bewusteloos raken) en De Blue Whale Challenge (automutilatie). Dergelijke challenges worden bijvoorbeeld via YouTube en TikTok verspreid en leiden tot letsel of andere negatieve offline impacts. (zie: Van Huijstee et. al. 2021)
[83] T. de Kreij, 'Veel slachtoffers na TikTok-challenge: kindervuurwerk blijkt niet zo kindvriendelijk', nhnieuws.nl 6 januari 2022. TikTok is een sociale media-app waarmee korte muziekvideo's gemaakt en gedeeld kunnen worden.

Tabel 1: Digitaal sociaal verkeer (directe interactie via toestellen en apps)

⚠ Incident	Dreiging	Gebruikersbelang	Weerbaarheid
De gebruiker wordt **belaagd** door -al dan niet anonieme- **medegebruikers**; schade door interacties met andere mensen (denk aan: intimidatie, vernedering, pesterij, extreme content, doxing, laster en smaad) [84] Concrete voorbeelden • Er wordt iets vervelends over een gebruiker gezegd op een sociaal media platform, online forum of recensiekanaal. • De persoonlijke adresgegevens van een politica worden online gezet omdat een andere gebruiker niet gediend is van haar ideologie. **Gevolg** De gebruiker voelt zich, zowel online als offline, onveilig of bedreigd. De autonomie wordt beperkt door het zogenaamde **chilling** effect.[85]	De dreiging zit verscholen in de interactie met andere mensen. De problemen ontspringen uit gedragingen van iemand anders, en ontstaan dus in het **sociale verkeer.** **Actor** Eén of meerdere - vaak semi-anonieme - **medegebruikers**. **Middel** De mogelijkheden die apps faciliteren voor gebruikers om zich te uiten en in contact te komen met anderen.[86] Vaak gaat het om het plaatsen van teksten of video's.	• Vertrouwen en veiligheid • Menselijke waardigheid • Fysieke en emotionele gezondheid	**Kwetsbaarheden** • Menselijke psychologie en interacties, zowel bij de dader als bij het slachtoffer. • Het grote bereik van berichten en de moeilijkheid om iets te (laten) verwijderen op internet. • De anonimiteit binnen en ogenschijnlijke wetteloosheid van digitale omgevingen. **Maatregelen** Gebruikers: • Expliciete omgangsvormen en normen vaststellen en elkaar daarop aanspreken. • Weerbaarheid vergroten door bijvoorbeeld een dikkere huid te ontwikkelen. Ontwikkelaars: • Modereren van content • Verifiëren van accounts • Mechanismen voor het melden van schadelijk gedrag Beïnvloeders: • Bepalen wat strafbaar is en de juiste kaders stellen. • Strafbaar stellen en handhaven. • Voorlichtingscampagnes en voldoende educatie aanbieden

[84] Later meer over: slecht gedrag wordt beloond; extreme content doet het goed in algoritme van sociale media.
[85] Het chilling effect is wanneer mensen monddood raken doordat zij zien dat anderen die zich uitspreken worden gestraft. Daardoor kan o.a. een onderdrukking van mensen- en democratische rechten zoals vrijheid van meningsuiting ontstaan (*The Concept of Chilling Effect*, 2021, p.4).

[86] Sommige handelingen zijn strafbaar (zie H3). Het verschil met tabel 7 (over *social engineering*) zit in de bedoelingen en de middelen. Bij *social engineering* wordt een gebruiker aangezet tot risicovolle handelingen (bijv. om opgeworpen barrières over te gaan of regels te overtreden). In tabel 1 is het een gebruiker die (sociale) normen overschrijd en een ander bewust of onbewust schaad.

Tabel 2: Aantrekkingskracht en verwachtingspatronen (indirecte interacties)

⚠ Incident	Dreiging	Gebruikersbelang	Weerbaarheid
De gebruiker **lijdt** door de interactie met de **app/het toestel.** De technologie brengt (sociale) verwachtingen met zich mee en kan leiden tot sociale druk of stress. Concrete voorbeelden • Een oudere met beperkte digitale vaardigheden die zich genoodzaakt maar onzeker voelt om via een mobiel toestel en een app te internetbankieren. • Een minderjarige die dagelijks foto's of filmpjes post en continu bezig is met reacties daarop van anderen. [87] **Gevolg** De gebruiker kan niet aan verwachtingen voldoen of de aantrekkingskracht van mobiele toestellen en apps niet weerstaan. De drang om continu bereikbaar en zichtbaar te zijn, kan negatieve gevolgen hebben op iemands zelfbeeld en gezondheid (bijv. vanwege slaaptekort, verslaving).	De dreiging zit verscholen in (elk) individu. De gebruiker kan namelijk gedrag vertonen waarmee hij/zij **zichzelf** schaad. **Actoren** • De individuele gebruiker en de manier waarop hij/zij het toestel of de app gebruikt. • De ontwikkelaars en de ontwerpkeuzes die negatieve neveneffecten hebben.[88] **Middel** • Ontwerpkeuzes (zoals mogelijkheden om eindeloos te scrollen) en andere technieken (belonen en verrassen) die menselijke neigingen benutten om betrokkenheid of activiteit op een app of toestel te vergroten. • Het succes (de aantrekkelijkheid en effectieve marketing) die ertoe leidt dat een kritieke massa gebruik maakt van een specifiek type toestel of app.	Een goede mentale en fysieke **gezondheid** van de gebruiker.	**Kwetsbaarheid** Neigingen die menseigen zijn, zoals te verleiden of te manipuleren zijn en de zoektocht naar plezier, de drang om ergens bij te horen, niet achter te willen blijven. **Maatregelen** De gebruiker zelf: • Persoonlijke weerbaarheid vergroten Ouders (in het geval van minderjarigen): • Regels opleggen en/of ouderlijk toezicht instellen. Ontwikkelaars: • Leeftijdsgrenzen invoeren op apps waar minderjarigen extra kwetsbaar zijn • Hulpmiddelen voor zelfregulering en beheersing (zoals timers en blockers). Beïnvloeders: • Voorlichting en bescherming via leeftijdseisen en classificaties • Hulpverlening en educatie voor extra kwetsbare groepen • Verboden op bepaalde beïnvloedingstechnieken

[87] Gebruikers kunnen last hebben van het "fantoomvibratiesyndroom". Dit betekent dat iemand zijn of haar mobiele telefoon voelt trillen of hoort rinkelen, terwijl deze dat in feite niet doet.

[88] Ontwikkelaars hebben niet de bedoeling om gebruikers te schaden en ongezonde gewoonten te voeden. Toch kunnen bijvoorbeeld verslavende elementen een onderdeel worden van het product vanwege achterliggende verdienmodellen. Zie 1.3.

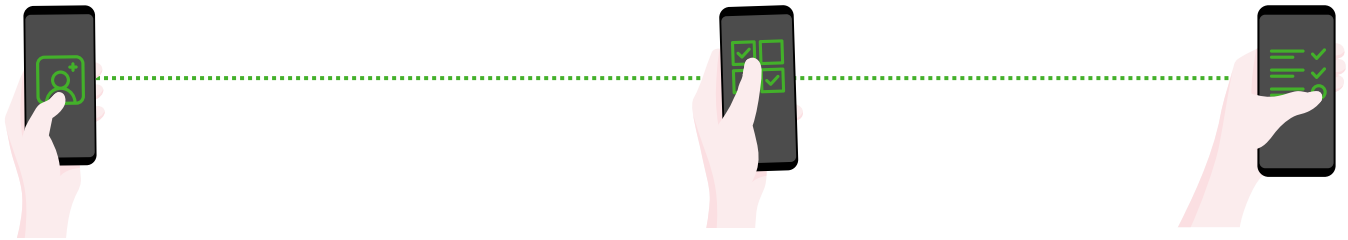
2.2. Privacy & ethiek aspecten: datagebruik binnen het ecosysteem

Een tweede type incidenten speelt zich af tussen de gebruikers en de ontwikkelaars van mobiele toestellen en apps. Achter de interface van de app die de gebruiker ziet, zitten diverse (markt)partijen (zie H1), wiens afwegingen op basis van hun prioriteiten, belangen en waarden, nadelig kunnen uitpakken voor de gebruiker. Veel van de negatieve gevolgen die de gebruiker kan ondervinden aan het type incident dat in deze paragraaf wordt beschreven, kunnen worden beschouwd als het resultaat van de gekozen verdienmodellen achter en ontwerpkeuzes binnen een app. Dit wil niet zeggen dat een ontwikkelaar altijd kwade bedoelingen heeft met deze verdienmodellen en ontwerpkeuzes. Het is vaak een kwestie van marktwerking en binnen de grenzen blijven van wat acceptabel wordt geacht door de gebruiker. Ook onvoorziene uitwassen van het gekozen verdienmodel of de werking van de technologie kunnen een rol spelen.

Onderstaande praktijkvoorbeelden raken aan allerlei vraagstukken over het (vermeende) recht om niet gemeten, geanalyseerd of beïnvloed te worden.[89] Er zijn vier grote typen incidenten die voortkomen uit de (grootschalige) dataverzameling die is ontstaan in de industrie van mobiele toestellen en apps. In tabel 3 worden incidenten met betrekking tot het monitoren van gebruikers voorgelegd. In tabel 4 wordt het risico op lekken van data besproken. Vervolgens wordt in tabel 5 ingegaan op het inzetten van data-mechanismen om het gedrag van gebruikers te kunnen beïnvloeden en de risico's die daarbij op de loer kunnen liggen voor de gebruiker. Als laatst zal worden ingegaan op de risico's die worden veroorzaakt door de technische mogelijkheden en configuraties die kunnen worden ingezet om het gedrag van de gebruiker te beïnvloeden.

[89] Zie: *Mensenrechten in het robottijdperk* 2017.

Praktijkvoorbeelden



Om een **toestel** met bijbehorende functionaliteiten te kunnen gebruiken, moeten individuen vaak persoonsgegevens delen en accounts aanmaken. Vaak heeft de consument daarin weinig keuze. Wanneer de gebruiker bijvoorbeeld een nieuwe smartphone installeert, dan wordt de gebruiker ook gevraagd een account aan te maken waarmee automatische back-ups in de Cloud kunnen worden bewerkstelligd, of via waar aankopen kunnen worden gedaan in een app winkel. Aan zo'n account zijn dan bijvoorbeeld gegevens als e-mailadres, telefoonnummer, voor- en achternaam, geboortedatum en creditcard gegevens gekoppeld. De mogelijkheden om van een toestel gebruik te maken zonder een account of zonder in te loggen via een bestaand account waar dit soort gegevens ook in zijn opgeslagen, zijn beperkt.

Om vervolgens een **app** te kunnen downloaden en installeren, moeten gebruikers vaak ook weer akkoord gaan met het delen van allerhande gegevens. Het is aan de gebruiker om per app een afweging te maken of hij of zij akkoord gaat met de dataverwerking zoals deze wordt voorgelegd.[90] Zodra de app is geïnstalleerd, kan deze soms ook niet zomaar worden gebruikt. Dit is verschillend per app, maar vaak moet er een type profiel worden aangemaakt of moet een gebruiker allerlei voorkeuren en gegevens opgegeven voordat de app gebruiksklaar is.

Wanneer de gebruiker de app dan kan gebruiken, heeft de gebruiker (afhankelijk van het type app) soms ook te maken met **moderatie**. Bij sociale media apps worden allerlei typen data van de gebruiker opgeslagen en verwerkt om diensten te personaliseren. Het gaat daarbij niet alleen om gegevens die de gebruiker zelf deelt of actief invult, maar ook om metadata en afgeleide data. Hier kunnen waardevolle inzichten uit voortkomen. Inzichten uit deze data zijn interessant voor zowel bedrijven (commerciële belangen) als overheden (burgers beschermen en bedienen), als medegebruikers of overige partijen (om elkaar te beïnvloeden voor bijvoorbeeld politieke of ideologische doeleinden). De inzichten uit data kunnen ook worden ingezet voor algoritmen of andere ontwerpkeuzes binnen een app. Hierdoor is het mogelijk om gebruikers op grote schaal te sturen om bepaalde keuzes te maken, zoals via persuasieve technologie, *dark patterns*[91] en *nudging*.[92]

[90] Als consument valt er iets te kiezen: bijvoorbeeld tussen Signal, Telegram en Whatsapp. Toch werkt dit in de praktijk vaak nog anders. Wanneer iedereen op de sportclub WhatsApp gebruikt, gaan veel mensen voor gemak en kiezen zij voor de meest populaire app. Bovendien gaan veel mensen uit enthousiasme en goedgelovigheid, vaak zonder bewuste afwegingen te maken akkoord met het delen van gegevens. Ook wanneer die niet strikt noodzakelijk lijken voor de dienst/het product.

[91] Dark Patterns zijn mechanismen die worden ingebouwd in gebruikersinterfaces op bijvoorbeeld een app om ervoor te zorgen dat gebruikers dingen gaan doen op die app die ze anders niet zouden doen. Dark patterns worden bijvoorbeeld ingezet om het voor gebruikers moeilijk te maken om zich ergens voor af te melden (zoals nieuwsbrieven of cookies), om gebruikers spullen te laten kopen, of om gebruikers meer persoonsgegevens te laten delen dan ze normaal zouden doen. ('Dark patterns: zo word je online verleid (of misleid) om iets te doen wat je anders niet had gedaan', opgelicht.avrotros.nl, 25 maart 2021)

[92] Een nudge is een duwtje in de gewenste richting. Het is een instrument voor gedragsbeïnvloeding (Thaler en Sunstein, 2009) en een vorm van persuasieve technologie waarin gebruikers worden verleidt tot 'goede' keuzes. Grondlegger B.J. Fogg definieert het als interactieve informatietechnologie ontworpen voor het veranderen van attitudes of het gedrag van gebruikers, zie Fogg, 2002.

Tabel 3: Monitoren (het opslaan van data)

⚠ Incident	Dreiging	Gebruikersbelang	Weerbaarheid
De gebruiker wordt **gemonitord** en kan zich niet onbespied wanen op zijn/haar mobiele toestel. Concrete voorbeelden • Het gebruik van een toestel laat een dataspoor achter. Al is de inhoud van berichten versleuteld, dan is er bijvoorbeeld vaak nog zogeheten metadata over met wie, wanneer en met welke frequentie berichten worden uitgewisseld. **Gevolg** De **privacy** van de gebruiker wordt geschonden door de grootschalige dataverzameling. De autonomie wordt beperkt door het zogenaamde **panopticon** effect.[93]	Het verzamelen, opslaan en verwerken van gegevens van gebruikers en/of data over app- en toestelgebruik. [94] **Actor** De ontwikkelaars. **Middel** Online formulieren, de aanmoediging of verplichting om accounts te creëren, de inzet van cookies, website analytics, etc.	• Controle over eigen (persoons)gegevens • Online anonimiteit • Respect voor de persoonlijke levenssfeer	**Kwetsbaarheden** • Ontwikkelaars van mobiele toestellen en apps verzamelen en bewaren soms veel gegevens van gebruikers tijdens het aanbieden van hun producten of diensten. In sommige gevallen worden gebruikers verleid om meer gegevens te delen dan noodzakelijk voor het product of de dienst. • Gebruikers zijn niet voldoende kritisch of een app daadwerkelijk bepaalde gegevens nodig heeft om de functionaliteit te kunnen bieden. Gebruikersgemak, kennisgebrek en onverschilligheid winnen het vaak van de tijd en moeite die het zou kosten om de voorwaarden goed te bestuderen en een gefundeerde keuze te maken. **Maatregelen** Gebruikers: • Kennis en bewustzijn vergroten om voorkeuren zorgvuldiger aan te geven en toestemmingen te verlenen Ontwikkelaars: • Privacy-maatregelen (incl. doelbinding, verantwoordelijkheden rondom gegevensminimalisatie, nauwkeurigheid, opslagbeperking, speciale categorieën en privacy verklaringen) Beïnvloeders: • Verplichtingen omtrent transparantie en keuzevrijheid, zodat de gebruiker daadwerkelijk zelf kan kiezen welke gegevens van hem/haar mogen worden verzameld

[93] Het panoticon-effect gaat over het disciplinerende effect van (zichtbare en onzichtbare) surveillance. Zolang iemand het idee heeft dat hij/zij wordt geobserveerd, zal hij/zij daar ook naar handelen ('Ethics Explainer: the Panopticon', ethics.org). Tegenwoordig wordt dit concept in relatie gebracht met het effect van dataverzameling en digitale surveillance.

[94] Het opslaan van gegevens van de gebruiker en/of over het gebruik is ook een "middel" in andersoortige incidenten (tabel 5 en 6). Er valt een onderscheid te maken tussen commerciële, ideële of charitatieve doelstellingen (waarvoor de data wordt verzameld), en of de data noodzakelijk is voor het product/dienst waarvoor de gebruiker het toestel/de app gebruikt of een ander doel dient. Hierbij spelen prikkels achter verdienmodellen (dat data geld waard zijn) een belangrijke rol. Zie ook telecommunicatiewet (art. 11.7).

Tabel 4: Lekken (het openbaren van data)

⚠ Incident	Dreiging	Gebruikersbelang	Weerbaarheid
Gegevens van de gebruiker worden **gelekt** doordat toegang aan onbevoegden wordt verleend, gegevens openbaar worden gemaakt, of doordat er niet secuur met data wordt omgegaan. Concrete voorbeelden • Een gebruiker van een sociaal media platform maakt per ongeluk iets openbaar wat voor één medegebruiker bedoeld was. • Een medewerker van een bedrijf heeft toegang gekregen tot (persoonlijke) data waar hij of zij niet voor geautoriseerd zou mogen zijn. • Gegevens komen op straat te liggen omdat een hergebruikte datadrager niet goed is gewist voordat het opnieuw in gebruik werd genomen. **Gevolg** De **privacy** van de gebruiker wordt geschonden doordat gegevens bruikbaar worden voor andere doeleinden dan waar ze voor verzameld zijn, of omdat mensen toegang krijgen tot gegevens die daar niet voor zijn geautoriseerd.	Het **openbaren** van (persoons)gegevens van de gebruiker. **Actor** De ontwikkelaars; partijen die vanuit hun positie of rol geautoriseerd zijn om toegang te hebben tot deze gegevens. **Middel** • (Mobiele) datadragers, bijvoorbeeld wanneer deze niet goed gewist zijn alvorens ze worden gerecycled.[95] • Toegang die te ruim wordt verleend aan onbevoegden. • Operationele fouten waardoor gegevens op straat terecht kunnen komen.	**Privacy** van de gebruiker	**Kwetsbaarheid** Data die verzameld wordt, kan op verkeerde plekken terecht komen (zonder kwade opzet). **Maatregelen** Gebruikers: • Bewust omgaan met het genereren en delen van data Ontwikkelaars: • **Privacy**-maatregelen, zoals beschreven in de AVG die eisen stelt aan dataprotectie en beheer • Cyberveiligheid maatregelen zoals goede protocollen voor de data management lifecycle Beïnvloeders: • Verantwoordelijkheden beleggen en voorzorgsmaatregelen verplichten

[95] Een voorbeeld hiervan is de case uit 2016 van Morgan Stanley, een Amerikaanse investeringsbank. De bank had een externe partij ingeschakeld om data van hun servers te wissen, om de servers vervolgens te kunnen doorverkopen voor recycling. Echter werd de data niet secuur genoeg gewist, waardoor in 2019 een enorme hoeveelheid klantdata op straat kwam te liggen. Zie: 'Morgan Stanley Pays $60M to Settle Data Breach LitigationCISOMAGon January 7, 2022 at 9:21 am Feedzy', itsecurity.org januari 2022.

Tabel 5: Sturen (het inzetten van data-analyses/mechanismen in apps voor gedragsbeïnvloeding)

⚠ Incident	Dreiging	Gebruikersbelang	Weerbaarheid
De gebruiker wordt **doelbewust** geanalyseerd *(*om bijvoorbeeld een profiel te kunnen vaststellen), waarna deze analyse gebruikt kan worden om de gebruiker te **beïnvloeden**. Concrete voorbeelden • Afhankelijk van het vastgestelde profiel krijgt de ene gebruiker A te zien, de ander B. Het kan hierbij bijvoorbeeld gaan om content, zoals nieuws of berichten op een sociaal mediaplatform, maar ook over prijzen of aanbiedingen in bijvoorbeeld webwinkels. **Gevolg** Het gedrag van de gebruiker wordt gestuurd voor commercieel of politiek gewin, met bijvoorbeeld filterbubbels, echokamers, rabbit holes, polarisatie en informatiebeperking tot gevolg.[96]	Het **benutten** van (persoons)gegevens om de gebruiker te leren kennen en gepersonaliseerd te bedienen en/of te manipuleren. **Actoren** • **Ontwikkelaars** die ontwerpkeuzes hier speciaal op afstemmen – al dan niet t.b.v. **adverteerders die** profielen gebruiken om gericht te targetten.[97] • Gebruikers die de normale functionaliteiten en mechanismen op apps benutten om hun doel te bereiken. Dit kunnen bijvoorbeeld ook **statelijke actoren** en overige actoren **met politiek motief** die dat openlijk dan wel onder een dekmantel doen **Middel** De "openbare **mechanismen**", profielen die gebaseerd zijn op algoritmen en persoonlijke data, aanbevelingsengines, persuasieve technologie, nudging, neuromarketing en bots.	Een goede mentale en fysieke **gezondheid** van de gebruiker.	**Kwetsbaarheid** Ongeacht de intenties kan het benutten van data(analyses) leiden tot ongewenste beïnvloeding van gebruikers . **Maatregelen** Gebruikers: • Kennis en bewustzijn vergroten Ontwikkelaars: • Transparantie en communicatie over transacties (wat geef je en wat krijg je) Beïnvloeders: • Consumenten-beschermingsmaatregelen

[96] De volgorde van berichten op een sociale media platform of resultaten uit zoekmachines worden bepaald door algoritmen (een type aanbevelingssysteem). Als gebruiker met een ideëel of charitatief doel, kun je dergelijke algoritmes bewust of onbewust voeden met content om uitkomsten te beïnvloeden, zonder toegang tot "onder de motorkap. Zie *Filterbubbels in Nederland* 2019, p. 13.

[97] Targeted advertising wordt gebruikt om de gebruiker van gepersonaliseerde advertenties te voorzien waar hij/zij gevoelig voor is. Content kan op een manier worden gerangschikt waardoor de kans gemaximaliseerd wordt dat de gebruiker op een advertentie klikt. De advertentie wereld is een opzichzelfstaand netwerk van bedrijven, tussenpartijen (zoals reclamebureaus, brokers, veilingen, etc.) en organisaties.

Tabel 6: Beperken (het inzetten van ontwerpkeuzes/machtspositie voor gedragsbeïnvloeding)

⚠ Incident	Dreiging	Gebruikersbelang	Weerbaarheid
De gebruiker wordt **beïnvloed** door de (technische) mogelijkheden (opties en **configuraties**)[98] op de app of het toestel. Het gaat hier om een incident op het niveau van de gebruikersgroep omdat dat wat technisch (on)mogelijk is niet op individueel niveau wordt bepaald. Concrete voorbeelden • Gebruikers hebben vaak beperkte mogelijkheden om keuzes te maken over het ontwerp van- of de mogelijkheden binnen een app, bijvoorbeeld over hoe content wordt gerangschikt, gefilterd en gepresenteerd aan de gebruiker. **Gevolg** Het gedrag van de gebruiker wordt gestuurd door beperkte keuzemogelijkheden of toegang tot informatie.	Het **beïnvloeden** van toegankelijkheid en/of aanvoer van informatie of bepaalde producten of diensten. **Actor** Ontwikkelaars die ontwerpkeuzes maken en daarin hun eigen belangen prioriteren. **Middel** Censureren, gatekeeping, rangschikken van content en self-preferencing (bijvoorbeeld wanneer een zoekmachine-bedrijf mechanismen in hun zoekmachine inbouwt waardoor hun eigen content altijd bovenaan komt te staan bij de zoekresultaten).	• De autonomie van de gebruiker • Eerlijke marktwerking en eerlijke concurrentie	**Kwetsbaarheid** Een klein aantal **dominante** marktpartijen binnen de makers, die de spelregels en technische mogelijkheden bepalen. **Maatregelen** Gebruikers: • Wensen en eisen kenbaar maken Ontwikkelaars: • Technische mogelijkheden implementeren om keuze aan de gebruiker te laten, bijvoorbeeld bij het aanbieden van rangschik- of filteropties Beïnvloeders: • Maatregelen om markttoezicht te verbeteren en een gelijk speelveld te creëren (zoals het voorkomen van monopolies, interoperabiliteit en dataportabiliteit stimuleren)

[98] Op veel mobiele toestellen en apps is het mogelijk om de "look & feel" te personaliseren. Fundamentelere keuzes over de architectuur of interface van de digitale omgeving worden doorgaans niet aan gebruikers voorgelegd. Discussies hierover komen opgang. Zo zijn er ontwikkelingen om niet-gepersonaliseerde tijdslijnen op sociale media platforms als optie aan te bieden. Ook is er aandacht voor de manier en locatie waar privacy instellingen kunnen worden aangepast. Soms zijn schuifjes of vinkjes uitermate ambigu of misleidend, en is het een zoektocht in instellingsmenu's.

2.3. Cyberveiligheid aspecten: doelbewuste acties van kwaadwillenden

De laatste groep incidenten die moet worden onderscheiden, betreft doelbewuste acties van kwaadwillende derden. Kwaadwillenden kunnen onderdeel zijn van verschillende actorgroepen in het ecosysteem. Het kan een maker zijn, bijvoorbeeld een ontwikkelaar die een malafide app bouwt om op die manier op mobiele toestellen van gebruikers binnen te komen. Ook kan het een andere gebruiker zijn, bijvoorbeeld iemand die zich voordoet een bekende om zo geld of andere middelen bij de gebruiker af te kunnen troggelen. Daarnaast is het ook mogelijk dat de gebruiker in eerste instantie niet het doelwit is van een kwaadwillende derde, maar dat deze activiteiten uitvoert om onderdelen van het technische systeem uit te schakelen, bijvoorbeeld wanneer een hacker een appwinkel platlegt. De gebruiker is in dat geval niet het doelwit, maar ondervindt er wel last van omdat hij of zij door de hack (tijdelijk) geen gebruik meer kan maken van de faciliteiten.

Het kan ook zijn dat de problemen in eerste instantie niet door de gebruiker worden ervaren, maar dat de gebruiker daar op een later moment wel last van krijgt. Bijvoorbeeld, wanneer een sociale media platform wordt gehackt, dan kan de hacker ervoor kiezen om de persoonlijke gegevens die zijn buitgemaakt openbaar te maken of te verkopen, met een negatieve impact voor de gebruiker tot gevolg.[99] Tot slot kunnen mobiele toestellen ook gebruikt worden door kwaadwillenden voor criminele doeleinden. Denk hierbij aan het minen van cryptovaluta. [100] Verder kunnen mobiele toestellen zelf ook gebruikt worden door kwaadwillenden om een DDoS aanval uit te voeren zonder dat een gebruik dat wellicht merkt.

Om incidenten te voorkomen, kunnen cyberveiligheid maatregelen[101] worden getroffen door ontwikkelaars en beheerders. Er zijn talloze maatregelen om assets (bijv. servers) te beschermen, maar deze zijn nooit volledig effectief (lees: er bestaat geen 100% veilig). Naast ontwikkelaars en beheerders hebben ook gebruikers een verantwoordelijkheid om hun cyberveiligheid te verhogen, bijvoorbeeld door middel van het gebruik van sterke en unieke wachtwoorden en door niet blind op linkjes in mails te klikken. Echter, de gebruiker is niet altijd de aangewezen partij om actie te ondernemen. In sommige gevallen ligt het duidelijk buiten de macht van de gebruiker om zich te weren tegen risico's (lees een onveilig platform).

In tabel 7 worden incidenten beschreven die te maken hebben met het binnendringen van mobiele toestellen of apps via de gebruiker zelf. In tabel 8 worden incidenten beschreven die te maken hebben aanvallen waarbij de gebruiker wordt beïnvloed en/of misleid en technologie een middel is.

[99] Zie voor de situatie in Nederland 'Hoe zit het met cybercrime?', longreads.cbs.nl; *Digital Economy Outlook* 2020, p. 178-179.
[100] 'Android security: This malware will mine cryptocurrency until your smartphone fails', znet.com 29 maart 2018.
[101] Er kan een verschil gemaakt worden tussen cybersecurity en informatiebeveiliging, zie ook P. Franken, 'Wat is het verschil tussen informatiebeveiliging en cyber security?', rootsec.nl 22 juli 2021.

Tabel 7: Social engineering (inbreken via de gebruiker)

⚠ Incident	Dreiging	Gebruikersbelang	Weerbaarheid
De gebruiker is **misleid** door een kwaadwillende derde (ook wel: **social engineering**) Concrete voorbeelden • Een gebruiker ontvangt een betaalverzoek van een ogenschijnlijke bekende, maar het was een oplichter.[102] Hierbij wordt de gebruiker bijvoorbeeld geld afhandig gemaakt. **Gevolg** • Verlies van *controle* over of toegang tot gegevens en/of het toestel. • Potentiële financiële schade. • Emotionele schade (bijvoorbeeld een gevoel van onveiligheid, schaamte, onzekerheid en geschaad vertrouwen in eigen oordeelsvermogen)	De gebruiker wordt gemanipuleerd iets te doen wat hij/zij normaal niet zou (willen) doen. Zijn toestel kan onderdeel worden van een botnet dat bijvoorbeeld DDoS aanvallen uitvoert. **Actor** Kwaadwillende derden. Dit kunnen bijvoorbeeld ontwikkelaars of gebruikers zijn, als de intentie maar is om schade bij een ander aan te richten. **Middel** Inspelen op de psychologie van de **gebruiker** en de gebruiker persoonlijk (vaak onder valse voorwendselen) benaderen om een actie te ondernemen (bijvoorbeeld door ergens op te klikken, iets te betalen of gegevens delen).	**Data** en **eigendommen** van de gebruiker en de wil en durf om de functionaliteiten van het toestel of de app te blijven gebruiken.	**Kwetsbaarheid** Een gebruiker herkent **malafide praktijken** niet altijd en kan zich onbewust problemen op zijn of haar hals halen door te reageren op verzoeken van kwaadwillende derden. **Maatregelen** Gebruikers: • **Kennis** en **bewustzijn** (digitale geletterdheid) vergroten om oplichting en andere malafide praktijken te herkennen Ontwikkelaars: • **Technische maatregelen** om ongewenste activiteiten te weren of te voorkomen (bijvoorbeeld een functie die ervoor zorgt dat als je een bericht krijgt van een onbekend nummer dit gevlagd wordt als een mogelijk onveilig bericht) Beïnvloeders: • Maatregelen om ter preventie (voorlichting) en afschrikking (de pakkans te vergroten)

[102] P. Vogel, 'Man door 'dochter' opgelicht via WhatsApp: 'Je voelt je enorm bescheten'', ad.nl 11 april 2019. Tikkie is een gratis app waarmee je betaalverzoeken verstuurt naar vrienden, familie of bekenden; zie voor meer voorbeelden *Digital Economy Outlook* 2020, p. 179.

Tabel 8: Hacking (inbreken via de technologie)

⚠ Incident	Dreiging	Gebruikersbelang	Weerbaarheid
De app of het toestel van de gebruiker wordt **geïnfiltreerd**, via een ingebouwde backdoor of een onbekende software-kwetsbaarheid (zeroday) met als gevolg dat de vertrouwelijkheid, beschikbaarheid of integriteit van het toestel, apps of data worden geschonden. **Gevolg** • Verlies van *controle* over of toegang tot gegevens en/of het toestel. • Potentiële financiële schade. • Emotionele schade (bijvoorbeeld een gevoel van onveiligheid, schaamte, onzekerheid en geschaad vertrouwen in eigen oordeelsvermogen)	Ongeoorloofde toegang tot gegevens of installatie van malware. **Actor** Kwaadwillende derden. Dit kunnen bijvoorbeeld ontwikkelaars of gebruikers zijn, als de intentie maar is om schade bij een ander aan te richten. **Middel** Omzeilen of benutten van het ontbreken van veiligheidsmaatregelen zoals updates of goede basismaatregelen als wachtwoorden en sterke encryptie.	**Data** en **eigendommen** van de gebruiker & **functionaliteit** van het toestel voor de gebruiker.	**Kwetsbaarheid** Elke actor met een kwade wil (gebruikers, ontwikkelaars of beïnvloeders) kan interesse hebben in de beschikbare data of de functionaliteit beïnvloeden. Achterdeurtjes in de technologie, softwarefouten of ondermaatse basisbeveiliging maken mobiele toestellen en apps extra kwetsbaar voor (ver)storingen en schendingen van vertrouwelijkheid, beschikbaarheid of integriteit. **Maatregelen** Gebruikers: • Cyberveiligheid maatregelen als sterkere wachtwoorden, twee-factor authenticatie en verplichte updates. • Kennis en bewustzijn Ontwikkelaars: • Cyberveiligheid maatregelen (zoals het verbeteren van state-of-the-art technologie en het vaststellen van industriebrede standaarden en certificering) Beïnvloeders: • Beleid over de omgang met backdoors en zerodays

2.4. Extra kwetsbare gebruikersgroepen

Er is een aantal gebruikersgroepen te identificeren die extra kwetsbaar zijn. Zo zijn er mensen die – om diverse redenen – minder digitaal vaardig zijn. Dit kan gekoppeld zijn aan leeftijdsgroepen, verschillen in economische stand – bijvoorbeeld omdat mensen in financiële nood minder gemakkelijk toegang kunnen krijgen tot state-of-the-art technologie – en toegang tot kennis, begeleiding of hulp bij onzekerheden. Daarnaast kunnen verstandelijke en lichamelijke beperkingen mensen extra kwetsbaar maken. Ook kunnen mensen situationeel in een kwetsbare positie verkeren, bijvoorbeeld wanneer een netwerkprovider plots een storing heeft en een gebruiker daarom maar even verbinding maakt via de onbeveiligde, openbare Wi-Fi.

Dit onderzoek beperkt zich tot *algemene* beschrijvingen van risico's en zorgen, maar kijkt daarnaast ook nadrukkelijk naar één kwetsbare groep, namelijk naar minderjarigen, zoals expliciet is benoemd in de uitvraag voor dit onderzoek. Minderjarigen lopen op sommige vlakken meer risico dan volwassenen, omdat zij minder goed overzicht hebben welke risico's er voor hun op de loer kunnen liggen,[103] bijvoorbeeld met betrekking tot het onbewust delen van persoonlijke data, het downloaden van malafide apps of het te maken krijgen met grooming. Minderjarigen zien gevaar minder scherp, hebben minder ervaringen opgedaan en zijn dus ook minder uitgerust om bepaalde narigheid op de juiste manier in te kunnen schatten[104]. De keuzevaardigheid van minderjarigen ligt daarnaast ook gemiddeld lager dan bij volwassenen. Zo hebben minderjarigen bijvoorbeeld een ander gevoel bij wat geld waard is, zeker wanneer dit bijvoorbeeld wordt omgezet in de munteenheid van de game.

Ook sociale druk speelt een belangrijke rol bij de handelingsbekwaamheid van minderjarigen om zich te kunnen wapenen tegen de risico's die in dit hoofdstuk staan beschreven. Elk mens is in zekere mate ontvankelijk voor groepsdruk. Echter zijn de hersenen van minderjarigen nog in ontwikkeling, wat betekent dat met name de hersengebieden die verantwoordelijk zijn voor planning en het controleren van gedrag, nog niet volgroeid zijn. Om die reden zullen pubers dus meer grenzen opzoeken, doen zonder eerst na te denken, en bezig zijn met leeftijdsgenoten.[105] Al deze zaken samen zorgt ervoor dat minderjarigen dus ontvankelijker zijn voor sociale druk van hun leeftijdsgenoten.

Ook al lopen minderjarigen niet de kans op meer risico's dan de risico's die in dit hoofdstuk staan beschreven, ze lopen wel meer risico omdat ze kwetsbaarder zijn. Dit wordt ook erkend door zowel de wet, als door de maatregelen die door bedrijven zelf worden genomen om minderjarigen beter te beschermen tegen risico's met betrekking tot het gebruik van mobiele toestellen en apps.

> "Minderjarigen zien gevaar minder scherp, hebben minder ervaringen opgedaan en zijn dus ook minder uitgerust om bepaalde narigheid op de juiste manier in te kunnen schatten"

[103] *Children and the GDPR* 2018, p. 11.
[104] 'Child sexual exploitation and grooming', education.vic.gov.au.
[105] 'Puberhersenen', hersenstichting.nl.

2.5. Conclusie: gebruikers in de knel

Er is een grote variëteit aan risico's en kwetsbaarheden bij het gebruik van mobiele toestellen en apps voor gebruikers in het algemeen, en voor minderjarigen in het bijzonder. Hoewel extra attentie voor minderjarigen noodzakelijk, zijn ook andere gebruikersgroepen mogelijk kwetsbaar. Zo zijn er bijvoorbeeld minderheden die – op grond van etniciteit, seksuele voorkeur of geloofsovertuiging - het slachtoffer kunnen zijn van pesterij en intimidatie, profilering of acties van kwaadwillenden.

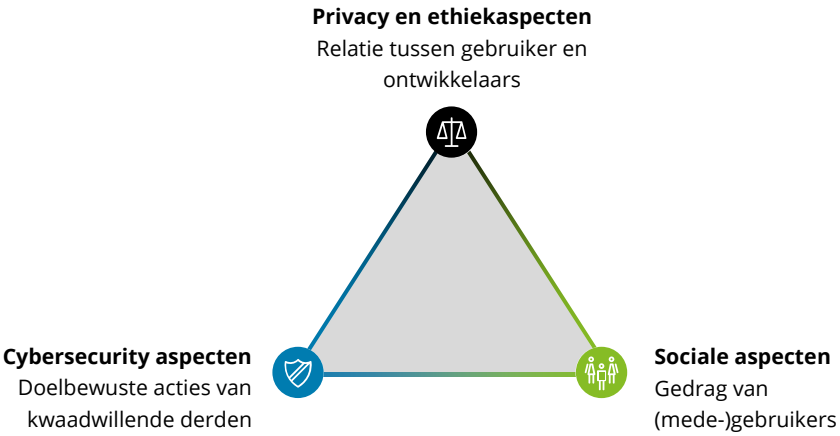
Dit hoofdstuk heeft inzichtelijk gemaakt dat de risico's en kwetsbaarheden verschillende oorsprongen binnen het ecosysteem kunnen hebben. Als ontwerper van de digitale omgeving, hebben ontwikkelaars bijvoorbeeld een unieke machtspositie. Zij benutten niet alleen de technologische mogelijkheden, maar spelen ook in op menselijke gedragingen. Dit gebeurt ook bij interacties tussen gebruikers, en in relatie tot kwaadwillende derden. De acht uitgewerkte type incidenten ontstaan door wisselwerkingen tussen de aantrekkingskracht van de producten en diensten, en de invloeden van omgevingsfactoren die zijn beschreven in H1.

De dreigingen lopen uiteen van schadelijke interacties met medegebruikers tot manipulatie door adverteerders en oplichting door een kwaadwillende derde. In de meeste gevallen zijn de bedreigde gebruikersbelangen ('assets') gerelateerd aan de fysieke en/of emotionele gezondheid van de gebruiker zelf en/of het verlies van eigendommen.

Diverse maatregelen en hulpmiddelen worden momenteel benut om de weerbaarheid tegen de dreigingen te vergroten. Toch zijn deze maatregelen niet waterdicht en gaat met enige regelmaat nog mis, ook als de maatregelen technisch en organisatorisch op orde lijken. In sommige gevallen kan de schade verder gaan dan de gebruiker zelf, bijvoorbeeld wanneer het toestel van een gebruiker wordt gehackt zodat deze vervolgens kan worden gebruikt voor illegale praktijken. Om incidenten te voorkomen moeten niet alleen specifieke groepen beter worden beschermd, maar moeten verschillende onderdelen van en verantwoordelijkheden binnen het ecosysteem nader worden bestudeerd en uitgewerkt.

In de volgende hoofdstukken wordt teruggegrepen op de aard van de incidenten zoals die in dit hoofdstuk zijn geclusterd tot de beschreven drie hoofdcategorieën. In hoofdstuk 3 zal worden toegelicht welke wetgeving van toepassing is op elke categorie en op welke manier.

Figuur 8: Drie hoofdcategorieën van kwetsbaarheden en risico's



3. Relevante Europese en Nederlandse wet- en regelgeving

In dit hoofdstuk worden de relevante wettelijke kaders uitgediept. Hierbij worden de relevante onderdelen van het recht omtrent gegevensbescherming, consumentenbescherming, mededinging, strafrecht, en algemeen civielrecht meegenomen. Specifiek wordt aandacht besteed aan nieuwe wetgeving vanuit de Europese Unie.[106] Er is een groot aantal nieuwe wetgevingen in de maak die specifiek gecreëerd zijn voor de online omgeving en een aanvulling bieden op het conventionele wettelijk kader dat de offline omgeving reguleert.

[106] Op Europees niveau wordt een onderscheid gemaakt tussen voorgestelde wetten, aangekondigde wetten, en vigerende wetten. De term 'voorgesteld' omvat alle wetsvoorstellen die door de Europese Commissie gepubliceerd zijn maar nog niet geaccepteerd zijn of in werking zijn getreden. De term 'aangekondigd' omvat alle initiatieven tot wetsvoorstellen die door de Europese Commissie zijn aangekondigd, al dan niet op instructie van het Europese Parlement. Hierbij is dus nog geen wettekst gepubliceerd. Onder de term 'vigerend' vallen alle wetten die de hele wetgevingsprocedure succesvol hebben doorlopen en reeds in werking zijn getreden.

Verschillende typen wettelijke kaders

Om de verschillende wettelijke kaders te duiden, kan er onderscheid worden gemaakt tussen verschillende type werkingen. Enerzijds kunnen wetten een afschrikkend element hebben:[107] de strafbaarstelling van bepaalde handelingen dient als afschrikmiddel om zo de gebruiker te beschermen. Anderzijds kunnen wetten een werking hebben op de weerbaarheid:[108] door het stellen van minimumeisen voor ontwikkelaars vergroot hun weerbaarheid tegen dreigingen en worden zijzelf en de gebruiker beter beschermd.

Daarnaast bestaat er onderscheid tussen wetgeving die *principle-based* is en wetgeving die *rule-based* is. Bij *principle-based* wetgeving worden algemene en brede principes gecodificeerd. Hierdoor is dit type wetgeving meer technologie-neutraal. *Rule-based* wetgeving is juist gericht op het gedetailleerd voorschrijven van regels en processen. In *principle-based* wetgeving wordt vaak een aanzienlijk deel van de exacte invulling van de gecodificeerde principes opengelaten, waar toezichthouders, adviesorganen en (internationale) samenwerkingsverbanden via richtlijnen vervolgens praktische invulling aan geven.

Specifiek voor wetgeving vanuit de Europese Unie valt verder onderscheid te maken tussen verordeningen (*regulations*) en richtlijnen (*directives*). Een verordening is een bindende wetgevende handeling met onmiddellijke rechtstreekse werking in de lidstaten. Een richtlijn legt een bepaald doel vast waar alle lidstaten binnen een bepaalde termijn aan moeten voldoen, maar staat daarbij een relatief ruime marge toe in de wijze van implementatie.[109] Er is een trend zichtbaar naar steeds meer *principle-based* verordeningen die principiële hoofdlijnen schetsen welke overal in de EU gelden. Het voordeel is dat deze duurzamer zijn in het licht van de snel veranderende technologie. De keerzijde is dat het meer vergt van (Europees) toezicht, hetgeen soms uitblijft met praktijkhiaten en beperkte naleving als gevolg.

Minderjarigen en de wet

Voor de wet is een individu minderjarig indien hij of zij de leeftijd van 18 jaar nog niet heeft bereikt.[110] Een minderjarige is in Nederland bekwaam om rechtshandelingen te verrichten indien hij of zij met toestemming van zijn of haar wettelijk vertegenwoordiger handelt of indien het een handeling betreft waarvan in het maatschappelijk verkeer gebruikelijk is dat een minderjarige van de betreffende leeftijd een dergelijke handeling zelfstandig verricht. Daarnaast genieten minderjarigen onder de leeftijd van 16 of 12 jaar (en soms op een andere afwijkende leeftijd onder de 16 jaar) volgens de wet op veel vlakken additionele beschermingen. Zo worden in Nederland onder de Algemene Verordening Persoonsgegevens minderjarigen onder de 16 jaar extra beschermd.[111]

De rol van de toezichthouder

Op veel vlakken is door de overheid bij of krachtens de wet een toezichthouder aangewezen. De toezichthouder vervult als een onafhankelijk en onpartijdig orgaan een cruciale rol in enerzijds het toezien op naleving van het wettelijk kader, en anderzijds het vervullen van een voorlichtende en bewustmakende rol voor zowel de kant van de ontwikkelaars als de kant van de gebruikers. Voor de bescherming van de gebruiker binnen het ecosysteem van mobiele toestellen en apps is een belangrijke rol weggelegd voor het Agentschap Telecom, de Autoriteit Consument en Markt, de Autoriteit Financiële Markten, de Autoriteit Persoonsgegevens, en het Commissariaat voor de Media. Daarnaast heeft het College voor de Rechten van de Mens ook aangegeven zich de komende jaren bezig te houden met digitalisering en rechtsbescherming.[112]

"In Nederland worden onder de Algemene Verordening Persoonsgegevens minderjarigen onder de 16 jaar extra beschermd"

[107] Werken op de dreiging: de actoren die betrokken zijn en naar de middelen die door deze actoren worden ingezet om hun doelen te bereiken (zie model in H2).
[108] Werken op de weerbaarheid: bepaald door de kwetsbaarheden die er zijn (waarlangs actoren bij assets kunnen komen) en de maatregelen die worden genomen/beschikbaar zijn (om de "assets" te beschermen tegen deze actoren). (zie model in H2)
[109] 'Types of legislation', european-union.europa.eu.
[110] Hiervoor geld één enkele uitzondering die betrekking heeft tot de leeftijd van een zwangere vrouw onder de 18 jaar. Zie art. 1:233 jo. art. 1:253ha BW.
[111] Zie ook: https://codevoorkinderrechten.nl/wp-content/uploads/2021/10/Code-voor-kinderrechten-NL.pdf
[112] Zie: https://mensenrechten.nl/nl/publicatie/5e900b741e0fec037359c173

3.1. Wet- en regelgeving m.b.t. Sociale Aspecten: Schadelijk gedrag van (mede)gebruikers

In paragraaf 2.1 zijn verschillende type incidenten besproken die te maken hebben met sociale aspecten en schadelijk gedrag van (mede)gebruikers. Deze gedragingen, zoals pesten, intimidatie, haatzaaiing en laster, kennen ook een online variant. Mobiele toestellen en apps bieden gebruikers nieuwe mogelijkheden voor en vormen van dergelijk gedrag, die in sommige gevallen ook nieuwe maatregelen vereisen. Aangezien het meeste online wangedrag interacties tussen gebruikers onderling betreft, vormen het **civiel- en strafrecht** belangrijke uitgangspunten bij de aanpak hiertegen. Vanuit deze wettelijke kaders zijn bepaalde handelingen die zowel online als offline kunnen plaatsvinden reeds verboden. Voorbeelden hiervan zijn:

- **Opruiing** tot strafbare feiten middels geschrift of afbeelding is strafbaar volgens art. 131, lid 1 van het Wetboek van Strafrecht. Lid 2 voegt daar een verzwarende omstandigheid aan toe indien er sprake is van opruiing met terroristisch oogmerk.
- **Smaad**, waarbij de eer of goede naam aangetast wordt door openbaarmaking van een bepaald feit met als doel de reputatie van het slachtoffer te schaden, is strafbaar gesteld in art. 261 Sr. Lid 2 voorziet in smaad door middel van schrift of afbeelding die verspreid of openlijk tentoongesteld wordt.
- **Belediging**, die niet voldoet aan het karakter van smaad of smaadschrift, is strafbaar onder art. 266 Sr. (belediging). Beledigende uitlatingen die betrekking hebben op ras, godsdienst of levensovertuiging, seksuele geaardheid of handicap zijn daarnaast strafbaar op grond van art. 137c Sr, lid 1. Belediging met betrekking tot de voorgenoemde eigenschappen door een groep personen, dan wel iemand die van dergelijke belediging een gewoonte maakt, is strafbaar op grond van art. 137c, lid 2 Sr.
- **Aanzetten tot haat of discriminatie** op basis van het voorgenoemde is strafbaar op grond van art. 137d, lid 1 Sr. Aanzetten tot haat of discriminatie op basis van het voorgenoemde door een groep mensen, dan wel iemand die daar een gewoonte van maakt, is strafbaar op grond van art. 137d, lid 2.

Er zijn echter ook typen interacties ontstaan die exclusief aan het digitale domein (niet per se louter mobiele toestellen en apps) gekoppeld zijn. Er is dan ook wetgeving ontwikkeld rondom nieuwere fenomenen:

- Het benaderen van een persoon onder de 16 middels een geautomatiseerd werk of **communicatienetwerk** met als doel om een ontmoeting voor te stellen met het oogmerk op het plegen van **ontucht** is strafbaar onder art. 248e Sr. Hiervoor wordt ook wel de term 'grooming' gebruikt.
- Het verspreiden en misbruik maken van **naaktafbeeldingen** van anderen is verboden onder art. 139h, lid 2 Sr indien de dader wist of had kunnen weten dat daar nadelige gevolgen voor het slachtoffer uit zouden ontspringen. Met dit relatief nieuwe wetsartikel is bijvoorbeeld wraakporno strafbaar gesteld.[113]

Tot slot is er ook nog relevante wetgeving in ontwikkeling:

- **Conceptwetsvoorstel doxing**: Onder voormalig minister van Justitie en Veiligheid Grapperhaus is een wetsvoorstel ter strafrechtelijke verbieding van het delen van privégegevens ter intimidatie gedaan. Onder dit voorstel zou het verspreiden van persoonsgegevens ter intimidatie, ook wel 'doxing', een strafbaar feit worden waar een gevangenisstraf van maximaal een jaar op komt te staan. Ook schrijft het voorstel online platform eigenaren een verantwoordelijkheid toe om berichten met doxing te verwijderen. Indien platformen dat nalaten, kan het individu een stap naar de rechter afdwingen. Het wetsvoorstel is op 8 juli 2022 naar de Tweede Kamer gestuurd om daar inhoudelijk behandeld te worden.[114]
- **Wetsvoorstel seksuele misdrijven**: Het Wetsvoorstel seksuele misdrijven zal onder andere toezien op een betere strafrechtelijke bescherming tegen nieuwe online delictsvormen, specifiek online seksueel kindermisbruik. Het voorstel omvat het strafbaar stellen van seksuele interacties waarbij de dader op afstand de regie voert over de handelingen die worden verricht aan of met het lichaam van het slachtoffer, of die direct het gevolg zijn of rechtstreeks verband houden

[113] 'Wraakporno', rijksoverheid.nl.
[114] 'Gebruik van persoonsgegevens met als doel intimidatie wordt strafbaar', rijksoverheid.nl, 8 juli 2022

met een onderling contact op afstand tussen dader en slachtoffer. Hiermee is het online seksualiserend benaderen van minderjarigen, ook wel sexchatting, expliciet strafbaar gesteld.[115] De afdeling advisering van de Raad van state heeft op 8 juni haar advies vastgesteld over dit wetsvoorstel. Dit advies is op 13 juni 2022 gepubliceerd. Hierin wordt onder andere geconstateerd dat verwachtingen over de mogelijkheden tot handhaving niet te hoog moeten liggen. Daarnaast wordt geadviseerd om een aantal onderdelen in het wetsvoorstel verder te verduidelijken.[116]

Zoals hoofdstuk 2 uiteenzet, lopen gebruikers ook risico op dreigingen die ontspringen uit de individuele kwetsbaarheden van de gebruiker zelf. In sommige gevallen kan de online zorgen voor (versterkte) manifestatie van die kwetsbaarheden. Hierbij moet bijvoorbeeld gedacht worden aan onzekerheid, stress, verslaving en depressie. Binnen deze categorie ontstaat de dreiging vanuit de gebruiker zelf in de interactie met het ecosysteem. Hoewel de gevolgen op de fysieke en mentale gezondheid van gebruikers leiden tot grote zorgen, zijn deze risico's in sommige gevallen beperkt te vangen in een wettelijk kader. Alternatieve routes om risico's te mitigeren komen aan bod in hoofdstuk 4.

[115] 'Wetsvoorstel seksuele misdrijven', rijksoverheid.nl.
[116] 'Samenvatting advies over Wet seksuele misdrijven', raadvanstate.nl, 13 juni 2022

3.2. Wet- en regelgeving m.b.t. Privacy en Ethiek: Datagebruik binnen het ecosysteem

Hoofdstuk 2.2 bespreekt hoe binnen het kader van privacy en ethiek vier categorieën van dreigingen ontspringen: dreigingen omtrent monitoren, het lekken van data, het sturen van gebruikers, en het beperken van gebruikers. Het verzamelen en beheren van grote hoeveelheden data gaat gepaard met risico's, zoals onrechtmatigheid en datalekken. De wet is hier in toenemende mate aandacht aan gaan besteden. In 2015 kwam er bijvoorbeeld een meldplicht voor datalekken, waardoor bedrijven extra werden geprikkeld om datalekken te voorkomen. Vervolgens trad in 2018 de AVG in werking, die voor meer bewustzijn zorgde over privacy-gerelateerde vraagstukken bij zowel bedrijven als consumenten. Voor het inperken van de hiervoor genoemde dreigingen vormen de AVG, met principes zoals dataminimalisatie, transparantie, en doelbinding, en de ePrivacy Directive belangrijk kaders.

- **Algemene Verordening Gegevensbescherming (AVG):** Met de introductie van de AVG in 2016 zijn bestaande regels voor het verzamelen en verwerken van persoonsgegevens vernieuwd. De AVG is als Europese verordening in de plaats gekomen van de Wet bescherming persoonsgegevens (Wbp) en legt meer dan voorheen de verantwoordelijkheid voor het correct omgaan met persoonsgegevens bij de organisaties die deze persoonsgegevens verwerken. Ook verhoogt het de boetes die kunnen worden opgelegd voor overtredingen. De AVG biedt aanbieders binnen het ecosysteem duidelijke regels omtrent de verzameling van persoonsgegevens en biedt gebruikers een verbeterde bescherming tegen overschrijdende verzamelingspraktijken… In Nederland is de Autoriteit Persoonsgegevens bij wet als toezichthoudend orgaan aangesteld voor het toezicht op de verwerking van persoonsgegevens onder de AVG.
- **ePrivacy Directive / Telecommunicatiewet:** In Nederland is de ePrivacy Directive opgenomen in de Telecommunicatiewet. De wet schrijft regels voor die betrekking hebben op bijvoorbeeld radio en televisie, maar ook spam en cookies. Cookies worden door ontwikkelaars onder andere gebruikt om de online activiteit van de gebruiker te volgen om zo de gebruiker op basis van de over hem of haar verzamelde gegevens een aangepaste online ervaring te geven en producten en services te kunnen aanraden.[117] In het ecosysteem van mobiele toestellen en apps geeft de Telecommunicatiewet de gebruiker meer controle over zijn of haar blootstelling aan cookies en aanverwante technieken welke voor vergelijkbare doelen worden ingezet. Toezicht op de naleving van de Telecommunicatiewet valt onder verschillende toezichthouders, afhankelijk van het onderwerp; de Autoriteit Consument en Markt is als toezichthoudend orgaan aangesteld voor het toezicht op het gebruik van cookies.
- **Mediawet**: De Mediawet reguleert sinds de wijziging door de Europese Richtlijn voor Audiovisuele Media Services ook de content op videoplatformdiensten zoals Youtube en Netflix. Ook afzonderlijke videokanalen op video- en sociale media platforms kunnen worden gekenmerkt als 'commerciële mediadienst op afstand' en daarmee vallen onder het regime van (een deel van) de mediawet. Eén van de regels die dan van toepassing wordt is de bescherming van minderjarigen voor schadelijke content. Denk hierbij onder andere aan transparantievereisten bij reclame en productplaatsing maar ook een verbod op illegale content door uitingen van discriminatie of het aanzetten tot geweld of haat. Het Commissariaat voor de Media is belast met de naleving van de Mediawet en voorziet in het opstellen van gedragscodes zoals de Code Social Media & Influencer Marketing. Per 1 juli 2022 moeten invloedrijke video-uploaders op sociale media zich houden aan strengere reclameregels die opgesteld zijn door het Commissariaat. Het gaat hierbij om accounts die geld verdienen aan reclame, staan ingeschreven bij de Kamer van Koophandel en meer dan 500.000 volgers hebben. Middels deze regels moeten met name minderjarigen beter worden beschermd. Toezicht op deze regels zal meer gericht zijn op betere voorlichting dan op bestraffing bij een overtreding, maar dit kan veranderen als in de praktijk blijkt dat dit nodig is.[118]

Op het gebied van privacy is echter ook nog additionele wetgeving in de maak. Een voorbeeld hiervan is de ePrivacy Regulation.

- **Voorgesteld: ePrivacy Regulation**: De ePrivacy Regulation is al in 2017 voorgesteld maar heeft tot op heden nog geen definitieve doorgang gevonden.

[117] P. Kulche, 'Wat zijn cookies?', consumentenbond.nl 1 maart 2022.
[118] 'Commissariaat voor de Media start toezicht op video-uploaders', cvdm.nl, 17 mei 2022

De Regulation breidt de strekking van de ePrivacy Directive uit naar 'electronic communications content', zoals tekst, video en foto's. Daarnaast valt ook 'electronic communications metadata' (data die gebruikt wordt om de bron en bestemming van communicatie te volgen), locatie data, en de data over de tijd, duur en type communicatie binnen de strekking van de ePrivacy Regulation. Het stelt ook striktere regels aan het gebruik van cookies dan de huidige Telecommunicatiewet. Tevens staat de Regulation direct marketing alleen nog toe indien de gebruiker daar toestemming voor heeft gegeven. In februari 2021 zijn de onderhandelingen tussen lidstaten ten aanzien van de Regulation weer herstart.[119]

Kenmerkend voor de categorie "privacy en ethiek" zijn de verhoudingen tussen de gebruiker en de ontwikkelaar van mobiele toestellen en apps. Diverse dreigingen en de mogelijke negatieve gevolgen die daaruit ontstaan voor gebruikers komen voort uit de verdienmodellen en ontwerpkeuzes die gemaakt worden door de ontwikkelaars van de toestellen en apps. Een deel van de **consumentenbescherming en het mededingingsrecht** vormen dan ook een belangrijk wettelijk kader dat de consument in het ecosysteem bescherming biedt. Hierop houden de Autoriteit Consument en Markt en de Autoriteit Financiële Markten toezicht. Daarnaast speelt de Consumentenbond ook een cruciale rol in de bescherming van consumenten. Daarbij wordt onder andere, als het gaat om Europese wetgeving, samengewerkt met *Bureau Européen des Unions de Consommateurs* (BEUC), een Europese koepelorganisatie van consumentenbonden uit 32 landen.

Boek 6 van het Burgerlijk Wetboek bevat bedingen die beogen de consument te beschermen tegen oneerlijke handelspraktijken.

- Art. 193b, lid 2 sub b verbiedt handelspraktijken die het vermogen van de consument beperken om een geïnformeerd besluit te nemen. Hieronder vallen onder andere misleidende reclame, het verstrekken van onvolledige, valse of onduidelijke informatie, en agressieve verkoopmethoden. De Autoriteit Consument en Markt (ACM) heeft een uitgebreide leidraad over de bescherming van de online consument getiteld Grenzen aan Online Beïnvloeding. [120]
- In art. 193 c tot en met 193g Boek 6 BW zijn de misleidende handelspraktijken opgenomen. Een handelspraktijk is misleidend indien informatie wordt verstrekt die feitelijk onjuist is of die de gemiddelde consument misleidt of kan misleiden.
- In art. 193h tot en met 193i zijn agressieve handelspraktijken opgenomen.

De genoemde leidraad is door de ACM gesuppleerd met een leidraad voor Online Platformen.[121] Deze leidraad ziet toe op online platformdiensten die in het faciliteren van interacties of transacties tussen gebruikers en ontwikkelaars een belangrijke rol spelen. Behalve deze leidraden is er ook voorgestelde en aankomende wetgeving op Europees niveau die erop gericht is om de manieren waarop gebruikers worden gestuurd/beïnvloed in te perken. Dit "onderhoud" aan wettelijke kaders is een indicatie dat bestaande kaders niet voldoende aansluiten bij de huidige staat van de technologie, bedrijfsvoering en markten.

- **Politieke overeenstemming bereikt, nog niet in werking getreden: Digital Services Act (DSA):** De DSA is een Europese verordening die de toekomstige basis gaat vormen voor digitale diensten zoals online zoekmachines, content platformen, markten en sociale media. Het verduidelijkt de regels omtrent content moderatie en verdeelt de verantwoordelijkheden daaromtrent over de actoren binnen het online ecosysteem. Door een duidelijke verdeling van verantwoordelijkheden moet de hoeveelheid illegaal en schadelijk materiaal online gereduceerd worden, waardoor de gebruikers van mobiele toestellen en apps online betere bescherming tegen dergelijke content genieten. De naleving van de DSA zal onder de autoriteit gaan vallen van zogenoemde Digital Services Coordinators, waarvan elke lidstaat er een moet aanstellen.[122] Na de adoptie van de gefinaliseerde tekst in september, zal de tekst worden gepubliceerd in het publicatieblad van de Europese Unie. Twintig dagen later zal de wet in werking

[119] 'Legislative train schedule. Proposal for a regulation on privacy and electronic communications', europarl.europa.eu.
[120] *Leidraad Bescherming van de online consument* 2020.
[121] *Vuistregels Online platformen* 2020.
[122] 'Digital Services Act: Commission welcomes political agreement on rules ensuring a safe and accountable online environment', ec.europa.eu 23 apriil 2022; *De toekomst van online platformen* 2021, p. 2-4.

treden. De DSA zal daarna óf 15 maanden later, óf per 1 januari 2024 van toepassing zijn.[123]

- **Politieke overeenstemming bereikt, nog niet in werking getreden: Digital Markets Act (DMA)**: De DMA is een Europese verordening die de mededinging in de online omgeving adresseert. Het ziet specifiek toe op het terugdringen van de macht die grote online partijen op dit moment, om zo de consument beter te beschermen. Daarbij verbiedt de DMA bedrijven bijvoorbeeld om hun eigen services en producten gunstiger te ranken dan die van concurrenten, en het combineren van persoonlijke data verzameld via hun services met die verzameld via andere services. Tevens moet het voor gebruikers makkelijker worden om te wisselen tussen concurrerende services. Mobiele toestellen en apps worden hierdoor een stuk gebruiksvriendelijker: de consument krijgt een groter aanbod, betere diensten en eerlijkere prijzen. De naleving van de DMA zal onder de verantwoordelijkheid gaan vallen van de Europese Commissie. De Digital Markets Act zal direct in werking treden na publicatie in het Publicatieblad van de EU en zal zes maanden later binnen de gehele EU van toepassing zijn.[124]
- **Voorgesteld: Artificial Intelligence Act (AI Act):** De AI Act is een Europese verordening die voorziet in een juridisch raamwerk voor de ontwikkeling, verkoop en gebruik van artificiële intelligentie (AI). Het gebruikt een risico gebaseerde benadering die algoritmes indeelt op basis van het risiconiveau voor de gebruiker. De niveaus zijn onderverdeeld in de categorieën onacceptabel risico, hoog risico, matig risico, en beperkt tot geen risico. De AI Act verbiedt onder andere onderbewuste manipulatie van kwetsbare groepen door middel van AI, en het verbindt een groot aantal toepassingen van AI met een hoog-risico classificatie aan een aanzienlijke hoeveelheid eisen. Systemen die gebruik maken van AI, waaronder content algoritmes en aanbevelingssystemen, moeten daarom geëvalueerd worden onder de eisen van de AI Act. De bescherming van gebruikers van mobiele toestellen of apps die gebruik maken van AI wordt met deze verordening verder versterkt. Elke lidstaat zal een toezichthouder aan moeten wijzen die toeziet op de naleving van de AI Act. Er zijn duizenden amendementen op het wetsvoorstel ingediend, bijvoorbeeld over een verbreding van de definitie van AI, of over het volledig verbieden van gezichtsherkenning . Het is daarom waarschijnlijk dat de tekst van het wetsvoorstel op een aantal (mogelijk kritieke) punten zal wijzigen.[125]
- **Voorgesteld: Data Act:** De Data Act is een Europese verordening die dient om eerlijkheid in de digitale omgeving te verhogen, competitie in de data-economie te vergroten, en te zorgen dat data toegankelijker wordt zodat eenieder optimaal gebruik kan maken van de mogelijkheden van data. De Data Act probeert gebruikers meer controle te geven over de data die ze genereren en meer vrijheid te geven in de derde partijen waar ze die data mee willen delen. Gebruikers van mobiele toestellen en apps kunnen bijvoorbeeld inzien welke data van hen is verzameld en er (tot op een bepaalde hoogte) over beschikken. Elke lidstaat zal een toezichthouder aan moeten wijzen die toeziet op de naleving van Data Act.[126]
- **Aangenomen door het Europees Parlement: Data Governance Act (DGA):** De DGA is een Europese verordening die de EU moet transformeren tot een data gestuurde samenleving. Het stelt regels die het makkelijker moeten maken om data tussen sectoren binnen de EU uit te wisselen om zo maatschappijbreed de mogelijkheden van data beter te kunnen benutten. De DGA voorziet ook in het creëren van een gegevensbemiddeling raamwerk waardoor particulieren en bedrijven in een veilig, vertrouwde, en gecontroleerde omgeving gebruik kunnen maken van data. Elke lidstaat zal een toezichthouder aan moeten wijzen die toeziet op de naleving van DGA. De wet is aangenomen op 23 juni 2022 en zal na een respijtperiode van 15 maanden van toepassing zijn vanaf 24 september 2023.[127]

[123] 'What are the key goals of the Digital Services Act', ec.europa.eu
[124] 'The Digital Markets Act: ensuring fair and open digital markets', ec.europa.eu; *De toekomst van online platformen* 2021, p. 2-4.
[125] 'Thousands of amendments submitted for EU's AI Act', iapp.org, 3 juni 2022
[126] 'Data Act: Commission proposes measures for a fair and innovative data economy', ec.europa.eu 23 februari 2022.
[127] 'European Data Governance Act', digital-strategy.ec.europe.eu

De actoren waaruit de dreiging ontspringt (veelal ‘ontwikkelaars’ van de producten en diensten) zullen worden geraakt door deze nieuwe wettelijke kaders. Er gaat een afschrikkende werking uit van dergelijke wettelijke kaders, maar ze expliciteren ook bepaalde verantwoordelijkheden en standaarden om de weerbaarheid te vergroten. Met name dat laatste wordt aangevuld door de hiervoor genoemde voorgestelde en aankomende wetgeving. Deze wetten vallen onder het Europese wetgevings- en investeringsprogramma ‘A Europe fit for the Digital Age’. Dit programma moet er voor zorgen dat technologie eerlijk en betrouwbaar is en in dienst staat van de mens. Het is de belichaming van de digitale strategie van de Europese Unie.

“Systemen die gebruik maken van AI, waaronder content algoritmes en aanbevelingssystemen, moeten geëvalueerd worden onder de eisen van de AI Act”

3.3. Wet- en regelgeving m.b.t. cyberveiligheid: Doelbewuste acties van kwaadwillenden

Verschillende aspecten van cyberveiligheid en doelbewuste acties of "aanvallen" van criminelen/hackers (zoals besproken in 2.3) worden gedeeltelijk afgedekt door het strafrecht. Het Wetboek van Strafrecht is in 2018 gemoderniseerd onder de Wet Computercriminalitiet III, om zo beter aan te sluiten bij de online realiteit. Opdat duidelijk is welke wetgeving effectief kan zijn is het belangrijk aan te wijzen tussen welke actoren de dreiging plaatsvindt. In het geval van cyberveiligheid wordt de dreiging voor de gebruiker over het algemeen bewerkstelligd door een kwaadwillende derde. De online realiteit evolueert snel en de wet moet daar zo nauw mogelijk bij aansluiten. Daarbij werkt een combinatie van al bestaande wetsartikelen in samenhang met artikelen die relatief recent zijn toegevoegd om de gebruiker een zo'n volledig mogelijke bescherming te bieden. Bepaalde handelingen, zoals computervredebreuk, het aftappen van gegevens, en het voorhanden hebben van malware, zijn bijvoorbeeld bij wet verboden.

Computervredebreuk is de term die in het Nederlandse rechtssysteem gebruikt wordt voor de strafbare vorm van hacking. Computervredebreuk wordt omschreven als het 'opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd werk of in een deel daarvan'. Met geautomatiseerd werk wordt in het Wetboek van Strafrecht bedoeld een apparaat of groep van onderling verbonden of samenhangende apparaten waarvan er een of meer op basis van een programma automatisch computergegevens verwerken. Van binnendringen in een geautomatiseerd werk is sprake indien de toegang tot het werk wordt verworven door het doorbreken van een beveiliging, middels een technische ingreep, met behulp van een valse sleutel, of door het aannemen van een valse hoedanigheid. Computervredebreuk is strafbaar gesteld in Art. 138ab van het Wetboek van Strafrecht.

- Het wetsartikel voor computervredebreuk geldt als basis artikel voor veel vormen van cybercriminaliteit. Vaak moet dit artikel in samenhang gelezen worden met andere artikelen omtrent cybercriminaliteit Daarmee zijn er vervolg feiten die ook strafbaar gesteld zijn. Al dan niet na het plegen van computervredebreuk zijn de volgende handelingen strafbaar gesteld[128]:
  - **Het aftappen van gegevens** die worden verwerkt of overgedragen door middel van telecommunicatie of een geautomatiseerd werk is strafbaar gesteld onder art. 139c Sr.
  - **Diefstal van geld, goederen of gegevens** door het inloggen met een valse sleutel (zoals gestolen wachtwoorden) is strafbaar onder art. 311 Sr.
  - **Het wijzigen van wachtwoorden**, ontoegankelijk maken van gegevens of gegevens wijzigen of verwijderen is strafbaar onder art. 350a Sr.
  - **Het verspreiden van virussen** is strafbaar onder 350a, lid 3 Sr.
  - **Diefstal van digitale goederen** is strafbaar onder art. 310 Sr.
  - **Het gebruik van ransomware** is additioneel strafbaar onder art. 350a lid 1 Sr in geval van gegevensmanipulatie, onder art. 284 Sr. in geval van dwang, of onder art. 317 Sr in geval van afpersing.
- Andere strafbare feiten die verband houden met cyberveiligheid zijn:
  - Het **voorhanden hebben van malware** of middels een onrechtmatig verkregen wachtwoorden of andere inloggegevens is strafbaar onder art. 139d, sub a & b Sr.
  - Ook **het wedderrechtelijk de toegang ontnemen** tot het gebruik van een geautomatiseerd werk door daaraan gegevens aan te bieden, zoals het geval is bij een Distributed Denial of Service aanval (DDoS) is strafbaar onder 138b Sr.. Daarbij zijn de schaal, methode en het doelwit van de aanval straf verzwarende omstandigheden.

[128] 'Richtlijn voor strafvordering cybercrime', om.nl; Richtlijn voor strafvordering cybercrime', wetten.overheid.nl.

- Bij veel vormen van **social engineering** is de facto sprake van oplichting. In 2019 is de wet aangepast waardoor praktijken als phishing ook onder dit artikel strafbaar gesteld zijn. Daarmee is social engineering strafbaar onder art. 316 Sr. Voor het binnendringen van een digitaal werk door middel van gegevens die door social engineering zijn verkregen geldt ook het hoofdartikel 138ab betreffende computervredebreuk. Het zonder toestemming binnendringen van een geautomatiseerd werk door zich voor te doen als de gebruiker is daarmee tevens strafbaar onder art. 138ab lid 1.
- Diefstal van digitale goederen of geld middels een valse sleutel verkregen door middel van **phishing** is strafbaar onder art. 310 en 311 Sr. Ook is phishing, waarbij normaliter sprake is van vervalsing, strafbaar onder art. 225 Sr, het artikel dat valsheid met geschriften strafbaar stelt. Als laatste wordt er bij phishing vaak gebruik gemaakt van de naam van een ander ten behoeven van het veinzen van authenticiteit. Wanneer een merk gekopieerd wordt is dit strafbaar onder het merkenrecht, specifiek het Benelux Verdrag Inzake de Intellectuele Eigendom.

Daarnaast zijn er allerlei wettelijke kaders op Europees niveau en vertaald in nationale wetgeving die zowel een afschrikkend effect hebben alsook gericht zijn op het vergroten van de weerbaarheid.[129] Zo worden er bijvoorbeeld eisen gesteld aan de ontwikkelaars van apps en mobiele toestellen via de Wbni.

- **Wet beveiliging netwerk- en informatiesystemen (Wbni):** De Wbni is de Nederlandse implementatie van de Europese Network and Information Security Directive (NIB Richtlijn). De Wbni stelt minimale eisen voor vitale aanbieders en digitale dienstverleners met betrekking tot de technische en organisatorische maatregelen ter beveiliging van hun netwerk- en informatiesystemen. Toezicht op naleving van de Wbni is, afhankelijk van de sector, verdeeld over het Agentschap Telecom, De Nederlandse Bank, Inspectie Leefomgeving en Transport, en Inspectie Gezondheidszorg en Jeugd.[130] Om digitale dienstverleners op weg te helpen bij het naleven van de wet, heeft Agentschap Telecom op 1 juli 2022 de Wbni-zelftest gelanceerd. Deze test moet voor digitale dienstverleners duidelijk maken of ze onder de wet vallen en of ze voldoen aan de zorgplicht.[131]
- **Cybersecurity Act:** De Cybersecurity Act, ook wel de Cyberveiligheidsverordening, is een Europese Verordening inzake ENISA en de certificering van cyberveiligheid van informatie- en communicatietechnologie. Vanaf 2019 gelden er vanuit de EU nieuwe regels voor de cyberveiligheid waarmee grensoverschrijdende cyberaanvallen beter het hoofd geboden kunnen worden. De nieuwe regels betreffen een Europees kader voor de certificering van producten, processen en diensten op het gebied van cyberveiligheid. Ook het toezicht op de naleving van de Cybersecurity Act valt sinds kort onder het Agentschap Telecom.
- **Radio Equipment Directive (RED):** De Radio Equipment Directive is een Europese richtlijn die een wettelijk kader vaststelt voor het op de markt brengen van radio equipment. Daarbij worden ook eisen gesteld aan de cyberveiligheid van de apparatuur. In de RED worden daarnaast eisen gesteld aan netwerk bescherming, waarbij fabrikanten van apparatuur maatregelen moeten nemen ter bescherming van het communicatie netwerk en ter voorkoming van een verstoring van de functionaliteit van websites en services. Ook moeten fabrikanten persoonlijke data beschermen en de privacy waarborgen door er bijvoorbeeld voor te zorgen dat er geen ongeoorloofde toegang verschaft kan worden tot de persoonlijke data van consumenten. Het toezicht op de naleving van de Radio Equipment Directive valt onder de autoriteit van het Agentschap Telecom.

Aankomende wetten omtrent Cyberweerbaarheid

Naast de bovengenoemde geldende wetten en regels is er ook een aantal wetten die de dreigingen omtrent cyberveiligheid verder proberen in te perken. Sommige van deze wetten hebben ogenschijnlijk geen direct effect op de bescherming van de gebruiker binnen het ecosysteem van mobiele toestellen en apps, maar bieden via het stellen van eisen aan de cyberveiligheid van ontwikkelaars indirect een verbeterde weerbaarheid tegen aanvallen van kwaadwillenden.

- **Politieke overeenstemming bereikt, nog niet in werking getreden: Network and Information Security Directive II (NIS II)** [132]: De concept versie is door de

[129] *Bijlage. Overzicht wet- en regelgeving cybersecurity* 2021.
[130] 'Bevoegde autoriteiten', nctv.nl.
[131] 'Agentschap Telecom lanceert Wbni-zelftest voor digitale dienstverleners', agentschaptelecom.nl, 1 juli 2022
[132] 'The NIS2 Directive: A high common level of cybersecurity in the EU', europarl.europa.eu 1 december 2021.

Europese Commissie gepresenteerd in December 2020 en politieke overeenstemming is op 13 mei 2022 bereikt.. Het doel van NIS II is het aanpakken van de huidige beperkingen van de NIS I Directive en is daarmee ook een antwoord op het veranderde cyberveiligheid landschap. De voorgestelde NIS II zou de scope van de huidige NIS I stevig uitbreiden en daarbij ook sociale media platformen onder de werking van de wet brengen. NIS II moet, door het stellen van eisen aan de cyberveiligheid van ontwikkelaars in de sectoren die onder NIS II vallen, het niveau van de cyberveiligheid van ontwikkelaars verbeteren. Daarmee zouden ook gebruikers beter beschermd zijn tegen dreigingen met betrekking tot cyberveiligheid binnen het ecosysteem van mobiele toestellen en apps.

- **Voorgesteld: Directive on the Resilience of Critical Entities (CER):** De CER Directive breidt de scope uit van de European Critical Infrastructure Directive. Landen zijn verplicht om voor kritieke infrastructuur in de sectoren van energie, transport, banken, financiële market, gezondheid en digitale infrastructuur een nationale strategie te ontwikkelen om ze zo weerbaarder te maken tegen onder andere cyberdreigingen.
- **Politieke overeenstemming bereikt, nog niet in werking getreden: Digital Operational Resilience Act for the Financial Sector (DORA):** DORA is een Europese Verordening die dient om een basiskader te scheppen voor de cyberveiligheid van financiële organisaties. Het stelt eisen aan IT-incidenten en risicomanagement en vereist het periodiek testen van de digitale weerbaarheid. De gevolgen van cyberaanvallen kunnen voor zowel financiële organisaties als voor hun klanten groot zijn. Gezien het feit dat financiële apps een belangrijk onderdeel vormen van het ecosysteem, komt een verbetering van de digitale weerbaarheid onder een dergelijke verordening ook de bescherming van de gebruiker ten goede. Op 11 mei 2022 is politieke overeenstemming bereikt. De wet zal in werking treden na publicatie in het Publicatieblad van de EU. Na een respijtperiode van 24 maanden zal de wet van toepassing zijn (kwartaal 4, 2024).[133]
- **Gepland: Cyber Resilience Act:** Volgens het werkprogramma van de Europese Commissie wordt er in Q3 van 2022 een voorstel gedaan voor de Cybersecurity Resilience Act. Deze Verordening zal een gemeenschappelijke EU-brede standaard voor cyberveiligheid gerelateerde producten creëren.[134] Gezien het feit dat dit voorstel pas in Q3 van 2022 gepresenteerd wordt is er op dit moment weinig bekend over de inhoud.

[133] 'The EU's Digital Operational Resilience Act has been agreed: implications for the financial services sector', deloitte.com, 25 juli 2022

[134] 'the new European Cyber Resilience Act', europarl.europa.eu

Kader 2:

Naleving buiten de Europese Economische Ruimte (EER)

Sinds het aannemen van de Algemene Verordening Persoonsgegevens heeft veel nieuwe Europese wetgeving zogenoemd extraterritoriaal effect gekregen. Dit betekent dat wetten die door de EU gemaakt zijn in sommige gevallen ook toepassing vinden buiten de grenzen van de EU. Dit extraterritoriale effect kan betekenen dat, ook al is een bedrijf niet gevestigd in de Europese Unie, het soms alsnog gebonden is aan Europese regels. Echter, handhaving van dit extraterritoriale effect brengt uitdagingen met zich mee wanneer ontwikkelaars niet gevestigd zijn in de Europese Unie en EER. Het internationale en grenzeloze karakter van de digitale omgeving maakt handhaving van Europese regels gecompliceerder.

In navolging van de AVG vereist veel Europese wetgeving dat bedrijven die niet in de EU gevestigd zijn een vertegenwoordiger in de EU aanstellen die dient als vertegenwoordiger van het bedrijf omtrent de handelingen waar de betreffende wet toepassing op heeft.[135] In het geval dat een bedrijf de wet overtreedt dient de vertegenwoordiger als aanspreekpunt. Wanneer een bedrijf niet in de EU gevestigd is en geen vertegenwoordiger heeft aangesteld wordt handhaving moeilijk.[136]

De middelen die door Europese toezichthouders gebruikt kunnen worden om compliance af te dwingen, zijn over het algemeen beperkt tot het uitschrijven van boetes en het opleggen van dwangsommen. Wanneer een buiten de EER gevestigde ontwikkelaar daar niet responsief voor is wordt handhaving door een Europese toezichthouder minder effectief.[137] In de realiteit ligt de handhaving van dit extraterritoriale effect dus gecompliceerder dan op papier. In dergelijke gevallen is het mogelijk dat, hoewel toezichthouders de overtreder zelf moeilijk kunnen sanctioneren, zij wel afnemers van services die de overtreder aanbiedt kunnen aanspreken en daarmee de markt sterk kunnen beïnvloeden.[138] Ook kunnen onder strikte voorwaarden de bestuurders van gesanctioneerde bedrijven verantwoordelijk worden gehouden voor overtredingen van de wet.

[135] *Richtsnoeren 3/2018 over het territoriale toepassingsgebied van de AVG (artikel 3)* 2019, p. 26.
[136] In een zaak tegen de Washington Post van 2018 gaf de ICO, privacy toezichthouder van het Verenigd Koninkrijk, al aan dat het weinig middelen in handen had om de Washington Post te dwingen te voldoen aan de AVG. Zie: 'ICO tells Washington Post it offers invalid cookie consent under GDPR', iapp.org 20 november 2018.
[137] De Italiaanse privacy toezichthouder heeft recentelijk het Amerikaanse bedrijf Clearview AI een boete opgelegd voor schending van de AVG. Clearview AI heeft geen vestiging in de EU. Zie: 'Facial recognition: Italian SA fines Clearview AI 20 million', edpb.europa.eu 10 maart 2022.
[138] De Zweedse toezichthouder heeft op deze manier een Zweedse politie eenheid een boete opgelegd voor het gebruik van de software van Clearview AI. Zie: 'Swedish DPA: Police unlawfully used facial recognition app', edpb.europa.eu 12 februari 2021.

3.4. Conclusie: hiaten en aandachtpunten

Conventionele wettelijke kaders zoals het strafrecht en het civielrecht zijn ook van toepassing op de online omgeving. Veel van de strafbare handelingen die offline gebeuren, hebben een online variant die eveneens strafbaar is. Online varianten zijn echter vaak lastiger te bestrijden vanwege technologische omzeilmogelijkheden en de internationale beperkingen. Naast het strafrecht en algemeen civielrechtelijke regels zijn er specifiekere wetgevingskaders zoals wetgeving omtrent mededinging, persoonsgegevens, en consumentenbescherming die effect hebben op het ecosysteem van mobiele toestellen en apps.

Hoewel conventionele wettelijke kaders ook online van toepassing zijn, zijn zij in sommige gevallen ontoereikend om online risico's te beperken. In online situaties waar conventionele wettelijke kaders ontoereikend zijn, is nieuwe regelgeving wenselijk. Daarom worden vanuit de Nederlandse overheid nieuwe wetsvoorstellen geïntroduceerd.

Ook vanuit de Europese Unie zijn wetten in de maak die van toepassing gaan zijn op de in dit onderzoek geïdentificeerde dreigingen. Veel van deze Europese wetgeving gebruikt een principle-based aanpak, waardoor duidelijkheid over de exacte invulling van de principes die daarin vastgelegd zijn vaak nog geruime tijd op zich kan laten wachten. De grote hoeveelheid nieuwe en aankomende wetgeving is een reactie op de veranderende online omstandigheden en het toenemend maatschappelijk belang van de online omgeving. De complexiteit en hoeveelheid van dit wetgevingspakket kan voor een deel van de marktpartijen problematisch gaan worden. Ook voor toezichthouders wordt handhaving een uitdaging. Met een grote hoeveelheid nieuwe wetgeving aan de horizon worden de verantwoordelijkheden en middelen van toezichthouders op de proef gesteld. Het is cruciaal dat toezichthouders optimaal gebruik maken van de onderlinge expertise en op sommige vlakken in staat zijn tot nauwe samenwerking.

Ook zijn er andere problemen. Sommige unieke aspecten van de online omgeving zorgen bij toepassing van de wettelijke kaders voor knelpunten en bemoeilijken handhaving en genoegdoening. Ook is het internationale karakter van de online omgeving een uitdaging voor het effectueren van de wettelijke kaders. Daarnaast zijn er technische uitdagingen die implementatie en handhaving van regels bemoeilijken. Indien er bijvoorbeeld een regel is tegen het creëren van een marketing profiel en het aanbieden van persoonlijke advertenties aan minderjarigen, vereist dit een verificatie van de leeftijd. Echter is identiteitsverificatie niet altijd in harmonie met de Algemene Verordening Gegevensbescherming. In sommige gevallen vereist dit bijvoorbeeld de verzameling van méér data, wat indruist tegen kernbegrippen als dataminimalisatie en doelbinding.

Er is daarnaast sprake van een complex ecosysteem waarin grote bedrijven en platformen een bepalende rol hebben ingenomen. De macht in de online omgeving is gecentraliseerd geraakt bij een relatief klein aantal spelers. Een gebrek aan alternatieven zorgt ervoor dat de gebruiker weinig tot geen keuze heeft en zet de belangrijke rol van zaken als toestemming onder druk. Niets voor niets wordt toestemming gezien als een van de grootste misverstanden van de digitale economie.[139] Bedrijven kunnen regels opleggen aan gebruikers die in veel gevallen voor de gebruiker suboptimaal zijn. Aan de macht van de grote ontwikkelaars in het ecosysteem wordt in nieuwe stukken wetgeving zoals de Digital Markets Act en de Digital Services Act meer aandacht besteed.

Wetgeving is in veel gevallen in staat om dreigingen te beperken, maar niet om ze af te dekken. Alleen wetgeving is niet genoeg om de gebruiker te beschermen. Hulp en bijstand bij incidenten, is van groot belang om het effect van wetgeving op de gebruiker te kunnen bepalen. Wetgeving moet dan ook gezien worden in een breder samenhangend geheel van handhaving, genoegdoening, richtlijnen, standaarden (ISO/NEN) en zelfregulering die samen zorgen voor een zo optimaal mogelijke bescherming van de gebruiker. Hier wordt in hoofdstuk 4 verder aandacht aan besteed.

"Met een grote hoeveelheid nieuwe wetgeving aan de horizon worden de verantwoordelijkheden en middelen van toezichthouders op de proef gesteld"

[139] Buitenweg 2021.

4. Overige maatregelen en drukmiddelen

Dit hoofdstuk gaat in op de overige maatregelen en drukmiddelen voor het mitigeren van risico's voor gebruikers van mobiele toestellen en apps. Naast het vaststellen van wettelijke kaders en het toezicht en de handhaving van die kaders (zie hoofdstuk 3), zijn er ook andersoortige maatregelen en handelingsopties. Deze zullen hieronder worden toegelicht. Verschillende partijen hebben een rol om problemen te signaleren, te voorkomen en te reageren op eventuele negatieve effecten voor gebruikers die zich ondanks wet- en regelgeving voordoen. Dit hoofdstuk is gebaseerd op bevindingen uit 'Online ontspoord' van het Rathenau Instituut[140], aangevuld met desk research van andere bronnen en bevindingen uit de gehouden interviews.

[140] Van Huijstee et. al. 2021, p. 95 – 125.

Kader 3:

De gang naar de rechter

Civielrechtelijke procedure: Civielrecht kan van toepassing zijn als een gebruiker verwikkeld is geraakt in een conflict met een ander persoon of met een bedrijf. Als het conflict niet zondermeer kan worden opgelost, dan kan de gebruiker de rechter om een oordeel vragen door een civiele procedure te starten.[141] Civielrecht is van toepassing wanneer er bijvoorbeeld een overeenkomst is gesloten tussen twee gebruikers, of tussen een gebruiker en bedrijf, en een van de partijen daarbij een gemaakte afspraak niet nakomt. Dit is bijvoorbeeld het geval wanneer online aangekochte goederen niet (of niet op tijd) worden betaald.[142]

Strafrechtelijke procedure: In het strafrecht wordt door een strafrechter beoordeeld of iemand een strafbaar feit heeft gepleegd. Wanneer een bedrijf of een persoon een strafbaar feit pleegt op een gebruiker van een mobiel toestel, dan kan deze persoon daarvoor worden gestraft. Als je als gebruiker slachtoffer bent van een strafbaar feit, dan is het in eerste instantie van belang dat er aangifte wordt gedaan bij de politie. Er zijn meerdere instanties waarbij de strafrechtprocedure gevolgd kan worden in het geval van negatieve consequenties of gedragingen met betrekking tot het gebruik van mobiele toestellen, o.a. op het gebied van: sextortion of revenge porn, Oplichting, (Identiteits)fraude, Computervredebreuk (hacken/kraken), Bedreiging, Discriminatie, Laster, Diefstal. Bezit of verspreiding van Kinderpornografie, Smaad(schrift), Verspreiding van propaganda (voorbeeld van IS-propaganda op uitspraken.rechtspraak.nl)

In hoger beroep en in cassatie: Meestal worden strafrechtelijke- of civielrechtelijke procedures eerst behandeld bij een lager gerecht. Echter kan het zo zijn dat de rechtelijke beslissing die daar wordt genomen, niet naar bekoren is voor de dader of het slachtoffer. Dan kan er nog een gang worden gezet richting hoger beroep. Dit is een rechtsmiddel waarbij een beslissing van een lager gerecht wordt bestreden bij een hoger gerecht. Hierbij wordt de zaak volledig opnieuw in behandeling genomen. In Nederland kan maar eenmaal hoger beroep worden ingesteld tegen een uitspraak.[143] Na hoger beroep is alleen beroep in cassatie bij de Hoge Raad der Nederlanden nog mogelijk. Dit is de hoogste rechtsprekende instantie van Nederland op civielrechtelijk en strafrechtelijk vlak. Hier wordt de zaak niet inhoudelijk behandeld maar wordt alleen beoordeeld of het recht op de juiste manier is toegepast en geïnterpreteerd in het hoger beroep.[144]

Class action: Dit is een bekende benaming uit de Verenigde Staten. In Nederland wordt een class action een representatieve actie of groepsvordering genoemd. Het is een vorm van rechtszaak waarin een grote groep mensen als collectief een vordering bij de rechter brengt, of waarin een bepaalde klasse verdachten vervolgd wordt. Vaak is consumentenbescherming een van de hoofddoelen van een class action. Het Europees parlement en de Council van de Europese Unie zijn in 2020 nieuwe regels wat betreft class actions overeengekomen in de 'Class Actions'-richtlijn. Deze richtlijn moet consumentenrechten versterken wanneer er sprake is van massale schade op Europees niveau.[145] Uit het rapport 'European Class Action Report 2021' opgesteld door CMS, blijkt onder andere dat class actions tegen de technologiesector enorm stijgen. Een groei van 1400% tussen 2017 en 2020 is te detecteren. Ook databeschermingsclaims zijn 11 keer zo vaak aangevraagd tussen 2016 en 2020.[146]

[141] 'Civiel recht', rechtspraak.nl.
[142] Rb Gelderland 15 december 2021, ECLI:NL:RBGEL:2021:6632.
[143] 'Hoger beroep', rechtspraak.nl.
[144] 'Cassatieberoep', rechtspraak.nl.
[145] 'Class Actions in Europe', jonesday.com.
[146] *European Class Action Report* 2021, p. 25 + 27.

4.1. Signalering en hulpverlening door maatschappelijke organisaties

Hieronder wordt de rol van het maatschappelijk middenveld bij de (1) structuren voor genoegdoening, (2) preventieve maatregelen en (3) de beïnvloeding van 'ontwikkelaars' en wetgevers, besproken.

Genoegdoening en hulp voor de gebruiker

Wanneer zich vervelende of strafbare zaken voordoen, kan een gebruiker van mobiele toestellen en apps verschillende routes bewandelen om zaken te herstellen of te rapporteren. Als het leed al is geleden en als de consequenties niet alleen tot de online omgeving zijn beperkt, dan kan het zijn dat de gebruiker de behoefte krijgt om hulp te vragen bij het verhelpen van het probleem of de geleden schade. Afhankelijk van de situatie die zich heeft voorgedaan zijn er civielrechtelijke-, strafrechtelijke- of class-action-procedures mogelijk waarmee de gebruiker genoegdoening kan halen (zie Kader 3).

Gebruikers ondersteunen en onderwijzen

Naast de vervolging van eventuele daders, is het voor slachtoffers ook belangrijk dat ze serieus worden genomen en dat naar hen wordt geluisterd. Zo bestaan er kanalen om te kunnen praten met vertrouwenspersonen, ervaringsdeskundigen of slachtofferhulpspecialisten[147] en kunnen er meldingen worden gemaakt bij belangenorganisaties gericht op consumenten. De modellen van MiND en Meldknop.nl zijn interessante voorbeelden. Via Meldknop.nl kunnen gebruikers uitleg en tips vinden over verschillende categorieën van cyberpesten, seks, oplichting en lastig vallen. Ook kan er via een te downloaden app, per mail, via een chat of per telefoon hulp worden inroepen van aangesloten organisaties, zoals Helpwanted, vraaghetdepolitie en pestweb. Bestaande hulporganisaties hebben met name aandacht voor fenomenen waarvan ook "offline varianten" bestaan en die dus al een plek hebben in het zorglandschap.[148] Voor nieuwe fenomenen die zijn ontstaan vanuit omgang met technologie, is hulp of zorg nog weinig geprofessionaliseerd. Hierbij speelt ook dat er in veel gevallen geen sprake is van een eenduidige dader-slachtoffer relatie.

Via een centraal meldpunt zou het desalniettemin mogelijk zijn om expertise en hulpverlening samen te brengen. Veel slachtoffers of gedupeerden doen momenteel echter geen melding of aangifte.[149] Meldpunten zijn echter van groot belang om zicht te krijgen op de aard en omvang van de problemen op mobiele toestellen en apps. Behalve goede structuren om te reageren op problemen die zijn ontstaan, is het ook van belang om problemen te voorkomen. Diverse maatschappelijke organisaties leveren daarom een bijdrage aan het creëren van bewustzijn over de risico's van mobiele toestellen en apps, zoals Waag, Bits of Freedom en de Open State foundation.[150]

Zo is er ook een groot aantal gespecialiseerde mediawijsheid-organisaties, waarvan er meer dan duizend werkzaam zijn onder de noemer Netwerk Mediawijsheid.[151] De organisaties die zich binnen dit netwerk inzetten op het gebied van mediawijsheid richten zich vaak op cyberveiligheid en -weerbaarheid. Daarnaast hebben zij steeds meer aandacht voor minderjarigen en hun ouders en proberen daarin nieuwere fenomenen als desinformatie en nepnieuws ook uit te lichten. De aandacht voor het onderwerp mediawijsheid lijkt daarmee te groeien en voorlichting over nieuwe digitale ontwikkelingen (en wat dit betekent in de sociale omgeving) lijkt meer belangstelling en relevantie te krijgen.[152] Het belang van het bevorderen van mediawijsheid voor alle burgers wordt ook onderschreven door het Commissariaat van de Media en ook zij levert hier een bijdrage aan.[153]

Voor de bevordering van mediawijsheid met betrekking tot apps, zou extra uitleg over de werking van populaire apps, de betekenis van gebruikersvoorwaarden en de

[147] Zoals helpwanted.nl of slachtofferhulp Nederland; praten met betrokkenen als ouders of vertrouwenspersonen van bijvoorbeeld school of werkgever, hulp zoeken bij hulplijnen, zie: 'Een app gezien die niet deugt? Je kunt het bij Apple rapporteren', iculture.nl 10 juni 2021; 'Een nummer rapporteren aan Whatsapp', fraudehulpdesk.nl; 'Informatiepagina's', helpwanted.nl; 'Hulp na sextortion', slachtofferhulp.nl; 'Cyberpesten', pestenislaf.nl; 'De kindertelefoon', kindertelefoon.nl; '113 zelfmoordpreventie', 113.nl; 'SMS-abonnement via frauduleuze Android-apps', consumentenbond.nl.

[148] Van Huijstee et. al. 2021, p. 125.

[149] Van Huijstee et. al. 2021, p. 138.

[150] 'Waag futurelab', waag.org; 'Bits of freedom', bitsoffreedom.nl; 'Open state foundation', openstate.eu.

[151] 'Over Netwerk Mediawijsheid', netwerkemediawijsheid.nl.

[152] Zie: Van Huijstee et. al. 2021, p. 120-121; 'Kinderen moeten internetdiploma halen', nos.nl 2 november 2015 ; 'Voor scholen: Lesmateriaal', mediawijsheid.nl; 'Goed in gesprek over verkeerde informatie', netwerkmediawijsheid.nl ; 'De Internethelden' bureaujeugdenmedia.nl, 2020.

[153] Commissariaat voor de Media, 2022, p. 2 + 4.

toevoeging van keurmerken behulpzaam kunnen zijn.[154] Zo kunnen er icoontjes worden toegevoegd aan apps met bijbehorende risico-classificaties, zoals eerder is gedaan voor televisie met de kijkwijzer. Op die manier kan een betere afweging worden gemaakt of een bepaalde app geschikt is voor bepaalde gebruikers, zoals minderjarigen. Ook kunnen voorlichtingscampagnes worden opgetuigd zoals wordt gedaan met betrekking tot het bewust omgaan met vuurwerk. Bureau Halt, die dit soort voorlichting ook verzorgt op scholen, zou hier bijvoorbeeld een rol bij kunnen spelen.

"Belangrijk is dat leerlingen leren om media bewust, verantwoordelijk, kritisch en creatief te gebruiken"

Er wordt ook gekeken naar mogelijkheden om digitale vaardigheden en mediawijsheid onderdeel te laten worden van het curriculum op Nederlandse scholen. In 2018 en 2019 is onderzoek gedaan naar welke onderwijselementen onderdeel moeten worden van een nieuw landelijk curriculum. Digitale geletterdheid is nadrukkelijk opgenomen als advies, onder andere omdat het "belangrijk is dat leerlingen leren om media bewust, verantwoordelijk, kritisch en creatief te gebruiken. Behalve noodzakelijk als voorbereiding op deelname aan de samenleving, vervolgopleiding en beroep kan digitale geletterdheid ook verrijkend zijn voor het persoonlijke leven en leren van leerlingen".[155] De minister voor Primair en Voortgezet onderwijs, Dennis Wiersma, heeft op 6 april 2022 bij de Tweede Kamer aangegeven dat hij zo snel mogelijk met dit nieuwe leergebied aan de slag wil. Op 19 mei 2022 heeft de Tweede Kamer hiermee ingestemd. Dit betekend dat aan het begin van schooljaar 2022-2023 zal worden gestart met het bijstellen van het kerndoel digitale geletterdheid.[156]

Beïnvloeden van "de ontwikkelaars" en wetgevers

Diverse maatschappelijke organisaties – zoals onderzoeksinstituten, belangenorganisaties en andere meldpunten – doen vervolgonderzoeken naar aanleiding van meldingen en klachten van gebruikers. Met resultaten uit dergelijke onderzoeken, kunnen zij bijvoorbeeld druk uitoefenen op 'ontwikkelaars' om misstanden te lijf te gaan.[157] Hulpverleners en maatschappelijke organisaties vervullen dan ook een belangrijke signalerende functie. Vanuit hun kennis van de online wereld of hun expertise op een specifiek fenomeen, krijgen zij risico's met betrekking tot mobiele toestellen en apps soms eerder in het vizier dan overheden of bedrijven.

Door gebreken aan de kaak te stellen en bedrijven die onvoldoende doen publiekelijk te vermanen[158] kunnen maatschappelijke organisaties bedrijven onder druk zetten om meer te doen. Uit vrees voor reputatieschade volgen andere bedrijven in sommige gevallen vervolgens hun voorbeeld. Zo zijn er voorbeelden van oproepen tot openheid over hoe gebruikersdata worden verzameld en gebruikt, hoe er op

[154] 'Leeftijdsadvies van PEGI', kijkwijzer.nl; P. Kulche, 'Sociale media ongeschikt voor kinderen', consumentenbond.nl.
[155] *Leergebied Digitale Geletterdheid*, 2019, p. 10.
[156] 'Digitale geletterdheid in het curriculum: na de zomer eindelijk aan de slag!', nldigital.nl, 24 mei 2022

[157] o.a. 'Digital Youth. Publicaties', uu.nl; Orben et. al. 2019; Orben et. al. 2022.
[158] o.a. 'Facebook', Last Week Tonight with John Oliver. 'As Silicon Valley Faces Greater Scrutiny, the Public Increasingly Views Big Tech as Powerful and in Need of More Regulation', morningconsult.com.

(sociale media) platformen wordt gemodereerd en over ontwerpkeuzes die daarin worden gemaakt.[159] Het negatief uitlichten van organisaties is echter niet voldoende. Er zal moeten worden gewerkt aan een verbeterde samenwerking.

Uit deskresearch en interviews blijkt dat de consument een machtige positie heeft, wanneer zij de kans krijgt om mee te denken over wat er wordt ontwikkeld en haar wensen en eisen articuleert. Forbes schrijft bijvoorbeeld dat inspraak van consumenten positieve effecten heeft op bedrijven die dit soort co-creaties faciliteren. Gebruikers zullen deze bedrijven namelijk positiever benaderen wanneer ze mee hebben kunnen denken over productontwikkeling. [160]

Naast het samenwerken met gebruikers zouden ontwikkelaars ook meer samenwerking met belangenorganisaties en het maatschappelijk middenveld kunnen opzoeken. Maatschappelijke organisaties zijn vaak vertegenwoordigd in overleggen of adviesraden binnen de overheid alsook bij bedrijven. Op die manier hebben zij een stem in beleidsontwikkeling en kunnen invloed uitoefenen op praktische onderwerpen zoals rechten van gebruikers en het beoordelen van bezwaarschriften. Uit interviews met verschillende typen organisaties blijkt dat samenwerking hierbij essentieel is, omdat op deze manier verschillende invalshoeken worden geraadpleegd om problemen aan te kaarten en op te lossen. Indien er samengewerkt wordt, moeten de uitdagingen van verscheidene belanghebbenden serieus genomen worden. Zo dient rekening gehouden te worden met zowel de innovatievrijheden van de ontwikkelaars, alsook de consumentenbelangen en de praktische uitwerking van wetten en andere verplichtingen. De kennis die ligt bij verschillende partijen moet worden samengebracht om de praktijk daadwerkelijk te verbeteren.[161] Het is daarbij ook van belang dat er transparantie is over de verschillende afwegingen die zijn gemaakt en dat er een motivatie wordt gegeven over de conclusie die aan de hand daarvan is getrokken. Op die manier kan er bijvoorbeeld door middel van co-creatie gewerkt worden aan cyberveiligheidsstandaarden.[162]

Uitdagingen voor maatschappelijke organisaties
Door het brede scala aan incidenten, dreigingen en risico's (zie H2) is er ook een breed scala aan mitigerende maatregelen en responses. Veel van de negatieve gevolgen waar gebruikers mee geconfronteerd worden, vallen niet in gebruikelijke noties van dader- en slachtofferschap en hebben te maken met grotere, onderliggende sociaalmaatschappelijke factoren. Het valt buiten de omvang van dit onderzoek om een verdere analyse te maken van wat wel en wat niet op de radar staat van maatschappelijke organisaties en hulpverleningsfaciliteiten. Het is echter voorstelbaar dat nieuwere problematiek tussen wal en schip valt, omdat de aandacht vrij ad hoc (door aandacht van schandalen of na ongelukken) pas op gang komt.

Er zijn ook organisaties die constructief meedenken of alternatieven ontwerpen om gebruikers beter te beschermen of te kunnen interveniëren online. Vaak zijn dergelijke initiatieven gericht op het ontwikkelen van alternatieve verdienmodellen of kleinschalige alternatieven op grote apps. De huidige verdienmodellen van sociale media platformen zijn op advertentie-inkomsten gebaseerd. Er kan echter ook gewerkt worden met abonnementen of lidmaatschappen, al kan dit gevolgen hebben voor de toegankelijkheid van apps, wat de verhoudingen tussen ontwikkelaars en aanbieders verandert. Wanneer consumenten de belangrijkste inkomstenbron zijn van een digitaal product of digitale service zullen hun belangen automatisch belangrijker worden dan de belangen van adverteerders. Diverse methoden voor waarde-gedreven ontwerpen stellen dat nadelige gevolgen tijdiger kunnen worden geïdentificeerd en geadresseerd wanneer specifieke waarden, zoals mensenrechten en cyberveiligheid, als uitgangspunten worden genomen in de ontwikkelfases en impact assessments tijdig worden uitgevoerd.[163]

[159] o.a. 'Facebook onder vuur: de klokkenluider, de beschuldigingen en de betekenis', nos.nl; 'Obama calls for tech regulation to combat disinformation on social media', cnbc.com.
[160] 'Customer Co-Creation is the Secret Sauce to Success', 10 juni 2016, forbes.com ; 'The Power of Consumer Collaboration', 24 mei 2020, forbes.com .
[161] Nieuwesteeg et al. 2021, p. 3.
[162] Nieuwesteeg et al. 2021, p. 4.
[163] Friedman et al. 2013, p. 2 + 12; '*The Assessment List for Trustworthy Artificial Intelligence (ALTAI)*' 2020, p. 3-4.

4.2. Afspraken binnen bedrijven en sectoren

Hieronder wordt de rol van private organisaties en sectorale samenwerkingen nader besproken. In H1 werden de ontwikkelaars al uitgelicht. Hier wordt breder gekeken naar wat de ontwikkelaars – individueel en gezamenlijk – kunnen bijdragen om risico's voor gebruikers te mitigeren. Er zijn grofweg drie invalshoeken: (1) manieren om interacties van gebruikers te modereren via beleid, gebruikersvoorwaarden en gedragscodes, (2) technische hulpmiddelen en ontwerpkeuzes die gebruikers in staat stellen zichzelf beter te beschermen, (3) standaardisering en ketenafspraken rondom cyberveiligheid.

Beleid, gebruikersvoorwaarden en gedragscodes

Commerciële organisaties die mobiele toestellen en apps op de markt brengen, zijn gemotiveerd om een goede gebruikerservaring te realiseren. In de interviews kwam naar voren dat de ontwikkelaars veelal goede intenties hebben. Uit onderzoek van statista.com, blijkt ook dat ontwikkelaars met name gemotiveerd worden door intrinsieke factoren als 'een gevoel van zelfprestatie krijgen', 'creatief bezig kunnen zijn' en het simpelweg 'leuk vinden om een app te bouwen'. Hieruit blijkt niet dat een ontwikkelaar erop uit is om gebruikers te manipuleren of te schaden.[164] Bovendien hebben de ontwikkelaars en de digitale producten en diensten die zij leveren, ook veel positieve invloeden op de ontwikkeling van gebruikers en de samenleving als geheel. Bepaalde ontwerpkeuzes of verdienmodellen werken echter mogelijk negatieve consequenties in de hand. Een ontwikkelaar zal namelijk een product willen bouwen waar hij of zij zelf ook aan verdient en dus zal een product of dienst zo aantrekkelijk mogelijk worden gemaakt om gebruikers aan zich te kunnen binden (zie hoofdstuk 1). Naast ontwerpkeuzes en verdienmodellen zullen 'ontwikkelaars' ook kijken naar wenselijk gedrag. Immers, wanneer er alleen maar narigheid op een app te vinden is, zullen gebruikers er minder graag aan verbonden blijven.

Apps waarin op diverse manieren geïnteracteerd kan worden tussen gebruikers onderling, expliciteren doorgaans gedragsregels of -codes in gebruikersvoorwaarden. Op deze manier proberen ontwikkelaars voorkeursgedrag te stimuleren. Met name bij grotere sociale media apps, maar ook bij kleinere ontwikkelaars, wordt verhelderd wat de gebruiker wel of niet mag doen, bijvoorbeeld als het gaat om het delen van content, maar ook het ontraden of verbieden van bepaald gedrag.

Bedrijven hebben zelf baat bij een gezonde online sfeer en hebben ook een zorgplicht. Ambities om gebruikers – minderjarigen in het bijzonder – te beschermen, worden door grote ontwikkelaars zoals Meta, Tiktok, Apple en Google uitgesproken. Hier wordt allerlei beleid op bedacht en expliciet gemaakt, bijvoorbeeld door middel van "community guidelines".[165] Via deze route bepalen de ontwikkelaars bepaalde spelregels en kunnen zij gebruikers sanctioneren die zich daar niet aan conformeren.[166] Daarnaast hebben verscheidene ontwikkelaars en marktpartijen een aangescherpte praktijkcode inzake desinformatie op 16 juni 2022 opgeleverd, naar aanleiding van de richtsnoeren die in 2021 door de Europese Commissie zijn opgesteld. In deze code is onder andere gekeken naar verbeteringen ten opzichte van het demoniseren van de verspreiding van desinformatie en het verzorgen van meer transparantie omtrent politieke advertenties.[167] Diverse partijen profileren zich via hun merk of kernprincipes en door extra maatregelen betreft veiligheid en privacy te treffen.[168]

Hoewel dergelijk beleid van de ontwikkelaars van mobiele toestellen en apps een belangrijke rol speelt in het reguleren van de mogelijkheden en het beschermen van gebruikers, zijn dit niet altijd de meest effectieve middelen. Een groot deel van de gebruikers stemt in met deze regels en voorwaarden zonder deze te hebben gelezen. In veel gevallen is het taalgebruik juridisch en niet toegankelijk voor de diverse gebruikersgroepen. Men kan niet verwachten dat gebruikers "de kleine lettertjes" bestuderen en een weloverwogen beslissing maken. Het kost simpelweg te veel tijd voor een gebruiker om zich in de voorwaarden van elke app te verdiepen.[169] Ook uit interviews blijkt dat verschillende partijen pleiten om de leesbaarheid van dit soort voorwaarden te vergroten, bijvoorbeeld door zaken summier en in gemakkelijke taal leesbaar te maken. Voor minderjarigen is het nog lastiger om in te kunnen schatten

[164] 'App developer motivation trends as of July 2013', 2013, statista.com.
[165] 'Facebook Community Standards', transparency.fb.com; 'TikTok Community Guidelines', tiktok.com; 'Instagram Community Guidelines FAQ's', about.instagram.com.
[166] Denk bijvoorbeeld aan het opheffen van bepaalde gebruikersaccounts, zoals o.a. is gedaan tegen Donald Trump, zie: 'Trump voorgoed van Twitter geweerd' 9 januari 2021, nos.nl.
[167] 'The 2022 Code of Practice on Disinformation', digital-strategy.ec.europe.eu
[168] Zie o.a. 'Google plans privacy change similar to Apple's, which wiped $230 billion off Facebook's market cap', cnbc.com 16 februari 2022.
[169] 'Click to agree with what? No one reads terms of service, studies confirm', theguardian.com, 13 maart 2017.

wat mogelijke gevolgen van een app kunnen zijn aan de hand van de algemene voorwaarden. In een aantal interviews is daarom benoemd dat de algemene voorwaarden zo worden geschreven dat deze voor een minderjarige te begrijpen is, zeker wanneer een app toegespitst is op minderjarige gebruikers.

Technische hulpmiddelen

Naast het bepalen van beleid, kunnen 'ontwikkelaars' ook technische hulpmiddelen creëren en inzetten om risico's voor gebruikers te mitigeren. Zo worden er in apps allerlei laagdrempelige opties aangeboden om de weerbaarheid en de mate van controle van de gebruiker te vergroten. Dit gebeurt op verschillende vlakken die kunnen worden gerelateerd aan de in hoofdstuk 2 benoemde risicocategorieën. De onderstaande opsomming geeft een beeld van de technische mogelijkheden die op dit moment worden ingezet, maar is geen uitputtende lijst.

Op het gebied van sociale aspecten

Ontwikkelaars willen over het algemeen dat er op een fijne manier met hun producten en diensten door gebruikers wordt omgegaan. Wanneer gebruikers ontevreden zijn over hoe wordt geïnteracteerd op een platform, kan dit namelijk negatieve effecten hebben voor het bedrijf dat deze interactie faciliteert middels dat platform. Daarnaast zijn ontwikkelaars over het algemeen gericht op het genereren van een positieve gebruikerservaring en is negatief gedrag van medegebruikers daarbij onwenselijk. Mede om die redenen worden technische middelen ingericht om de gebruiker tegen onwenselijk gedrag van medegebruikers te beschermen. Zo krijgen gebruikers de optie om vervelende berichten te verwijderen, om accounts of berichten van medegebruikers te rapporteren, of om klachten te melden bij de ontwikkelaar. Door middel van andere technische maatregelen wordt ook getracht gebruikers te waarschuwen voor bijvoorbeeld nepnieuws door *factchecking*-mechanismen[170] in te bouwen.

Naast dit soort controlerende of rapporterende mechanismen, wordt er, zeker door grote ontwikkelaren van sociale media (apps),op grote schaal gemodereerd op de content die door gebruikers wordt aangeboden. Grote topics zijn bijvoorbeeld haatzaaiing, discriminatie, desinformatie, politieke advertenties, misleidende advertenties, deepfakes, nepaccounts, kindermisbruik en zelfbeschadiging/-doding. Modereren kan plaatsvinden op verschillende manieren. Zo kunnen er professionele moderatoren worden ingezet die worden betaald door de ontwikkelaar. Op sommige platformen wordt ingezet op vrijwilligers of gebruikers zelf die toezien op de naleving van gebruikersvoorwaarden. Zij kunnen "gemachtigd" worden om iets of iemand te blokkeren of te rapporteren. Daarnaast kan er ook gewerkt worden met algoritmes om problemen te detecteren en door zaken zoals identiteit en leeftijd (zie kader 4) te controleren.[171] Het modereren van content op diverse platforms is echter een ingewikkeld vraagstuk.[172] Het grootste struikelbok is de beoordeling van wat schadelijk of illegaal is. Behalve dat een menselijk oordeel hier lastig te vellen is, verdwijnt de discussie uit het publieke domein wanneer dit wordt gedelegeerd aan technische hulpmiddelen (ontwikkeld door de grote app ontwikkelaars). Het bepalen van criteria en definities zijn gevoelig voor context en lokale culturen. Een belangrijke stap die zou kunnen bijdragen aan een verbeterd moderatielandschap is meer transparantie in het contentmoderatiebeleid. Als voorbeeld kunnen traditionele mediaorganisaties genomen worden, die contentmoderatiebeleid hebben vastgelegd in de vorm van redactiestatuten, journalistieke codes en ombudsmannen[173]. De Digital Services Act voorziet gedeeltelijk in een verhoogde transparantie ten aanzien van contentmoderatiebeleid.

> "In apps worden allerlei laagdrempelige opties aangeboden om de weerbaarheid en de mate van controle van de gebruiker te vergroten"

[170] 'About Fact-Checking on Facebook', facebook.com ; 'Introducing Birdwatch, a community-based approach to misinformation', blog.twitter.comt.
[171] Van Huijstee et. al. 2021, p. 117.
[172] O.a. '*Is Social Media Content Moderation an Impossible Task?*', forbes.com, 8 september 2018; Rathenau Instituut, 2022.
[173] O.a. 'Why social media can't keep moderating content in the shadows', technologyreview.com, 6 november 2020.

Kader 4:

Identiteits- en leeftijdsverificatie

In zijn algemeenheid wordt er door ontwikkelaars gezocht naar mogelijkheden om identiteits- en leeftijdsverificatie te verbeteren, om er onder andere voor te zorgen dat minderjarige gebruikers worden beschermd tegen schadelijke content. Via bijvoorbeeld 'attribute-based identity management' kunnen dit soort mechanismen worden ingezet om te verifiëren of gebruikers aan bepaalde identificatievereisten voldoen, zonder dat zij daar overmatig veel privacygevoelige informatie voor hoeven prijs te geven.[174]

Identiteitsverificatiemechanismen worden op verschillende manieren toegepast, bijvoorbeeld:

- Wanneer een nieuwe gebruiker van **YouTube** toegang wil krijgen tot alle content die op YouTube te vinden is, moet de gebruiker, bij registratie, fotografisch bewijs leveren dat hij of zij boven de 18 jaar oud is. Zodra de verificatie aan de hand van de foto is gedaan, wordt het fotografisch bewijs ook weer verwijderd.[175]
- Met **IRMA**, een in Nederland ontwikkeld 'attribute-based identity management'-mechanisme, is het mogelijk om in te loggen en kenmerken van je identiteit prijs te geven wanneer hiernaar wordt gevraagd online. Bijvoorbeeld, als een gebruiker toegang wil krijgen tot een website waar alcoholische versnaperingen worden verkocht, kan de gebruiker via IRMA bewijzen dat hij of zij ouder dan 18 jaar is en worden andere identiteitskenmerken verder niet gedeeld.[176]
- Ook op datingapp **Tinder** wordt identiteitsverificatie toegepast. Bij online daten zijn nepprofielen en misleidende informatie een probleem, met mogelijk catfishing[177] tot gevolg. Daarom biedt Tinder gebruikers de mogelijkheid om hun identiteit te verifiëren, zodat andere gebruikers kunnen zien dat je echt bent wie je zegt dat je bent. Dit wordt gedaan middels fotoverificatie. Een gebruiker upload een aantal profielfoto's. Vervolgens vraagt Tinder om een ad-hoc te maken foto, zodat deze kan worden vergeleken, door middel van gezichtsherkenning en menselijke moderatoren, met de foto's die zijn geüpload.[178] Op deze manier probeert Tinder catfishing tegen te gaan.

Soms schuren manieren van identiteitsverificatie met wetten als de AVG, maar er wordt op meerdere fronten gezocht naar mogelijkheden om ervoor te zorgen dat minderjarigen geen toegang krijgen tot schadelijke content die niet voor hen is bedoeld, zonder dat dit een enorme inbreuk heeft op de privacy van de gebruiker.

[174] Van Huijstee et. al. 2021, p. 117.
[175] 'YouTube introduces age verification for users', agechecked.com.
[176] 'Kies IRMA. Zet een digitaal paspoort op je eigen mobiel', irma.app.
[177] 'Catfishing: wat is het en hoe voorkom je het?', bnnvara.nl, 8 mei 2021.
[178] 'Wat is fotoverificatie?', help.tinder.com.

Op het gebied van privacy en ethiek aspecten

Op het gebied van privacy en ethiek worden mechanismen ingebouwd om gebruikers bewuster te maken van risico's die gepaard gaan met grootschalige dataverzameling. Apple maakt bijvoorbeeld sinds kort gebruik van 'Privacy Nutrition Labels' die snel inzichtelijk maken welke data door een app worden verzameld. Ook laat ze in één oogopslag zien welke van deze verzamelde data aan een gebruiker kunnen worden gekoppeld, en welke data niet.[179] Zo wordt transparantie over datagebruik bevorderd en kunnen gebruikers betere keuzes maken over welke apps ze wel of niet downloaden. Huawei gebruikt een andere technische methode. Huawei stuurt notificaties naar gebruikers wanneer zij een app hebben gedownload. In deze notificaties wordt beknopt beschreven welke data van de gebruiker door de app wordt verwerkt en wordt de gebruiker gevraagd of hij of zij daar akkoord mee gaat. Op deze manier worden gebruikersbewust gemaakt van welke afwegingen zij daadwerkelijk hebben. Echter zijn partijen als Huawei en Apple uiteindelijk niet verantwoordelijk voor de keuzes die de gebruiker maakt. Bovendien spelen marktmotieven een rol in de keuze voor bepaalde maatschappelijk verantwoorde ingrepen.

Daarnaast proberen ontwikkelaars minderjarigen beter te beschermen door *parental controls* aan te bieden, zoals ook wordt gedaan in de verschillende appwinkels.[180] Een minderjarige kan dan bijvoorbeeld niet zomaar een account aanmaken, omdat dit eerst moet worden goedgekeurd door de ouder. Ook kan een minderjarige dan niet zondermeer een app aankopen of downloaden, want ook daar moet dan eerst toestemming van de ouder voor komen. Recentelijk heeft Apple het installeren van parental controls verder versimpeld om minderjarigen beter te kunnen beschermen.[181] Naast de appwinkels zijn ook sociale media platformen bezig met het verstrekken en verbeteren van parental controls. Zo heeft Snapchat een nieuwe in-app tool ontwikkeld "Family Center" waarmee ouders meer inzicht krijgen in met wie hun kinderen contact maken op Snapchat en hoe frequent deze contacten plaatsvinden.[182] Ook Meta heeft de parental controls van Instagram aangescherpt. Zo krijgen ouders de mogelijkheid om toezichttools op te starten waarmee ze bijvoorbeeld specifieke tijden in kunnen stellen die moeten beperken hoelang hun kind op Instagram spendeert. Daarnaast kunnen ouders via deze tools ook zien wanneer hun kind een account of bericht rapporteert.[183] Er worden dus middelen ontwikkeld die ouders kunnen helpen bij het beschermen van hun kinderen. Echter kwam in interviews ook expliciet naar voren dat het niet zo zou moeten zijn dat de overheid, een app ontwikkelaar of een appwinkel de rol van ouder zou overnemen.

Bovenstaande ontwikkelingen zijn allemaal ingevoerd om gebruikers beter te kunnen beschermen, maar natuurlijk zijn er nog verbeteringen mogelijk. In het *position paper* van Bits of Freedom naar aanleiding van van een rondetafelgesprek dat plaatsvond op donderdag 10 februari 2022 inzake de rol van sociale mediaplatformen, komt bijvoorbeeld naar voren dat gebruikers van platformen (of andere apps) beter beschermd zouden kunnen worden wanneer manipulatieve ontwerpkeuzes worden verboden. Dit zijn ontwerpkeuzes die de gebruiker sturen in het maken van een bepaalde keuze en die vaak niet in het voordeel van de gebruiker zijn. Een voorbeeld hiervan zijn 'cookiemuren' die ontworpen worden om het makkelijk te maken om cookies te accepteren en het juist moeilijk maken om ze te weigeren. Er wordt gepleit om dit soort ontwerpkeuzes niet meer mogelijk te maken, en juist de gebruiker meer in zijn of haar kracht te zetten.[184] Op die manier kan de gebruiker beschermd worden tegen de commerciële belangen van machtige ontwikkelaars.

Een ander voorbeeld benoemd door Bits of Freedom tijdens het rondetafelgesprek is het feit dat privacy-instellingen op platformen vaak lastig te vinden zijn. Er moet eerst door een aantal menu's worden doorgeklikt alvorens men de privacyinstellingen vindt, vaak op een plek waar gebruikers het niet zouden verwachten. Vervolgens is het lastig om te weten welke instellingen precies waarvoor gebruikt wordenen wat het effect op je gebruikerservaring hiervan is. Dat soort trucjes maken het voor een gebruiker lastig te bepalen wat voor hen de juiste instellingen zijn en hoe dit aan te passen.[185] Dat kan verbeteren.

[179] 'Transparency is the best policy', apple.com.
[180] 'How to set up parental controls on Google Play', support.google.com; 'Use parental controls on your child's iPhone, iPad, and iPod touch' support.apple.com.
[181] 'Apple makes it easier to use parental controls and Screen Time with iOS 16', techcrunch.com, 6 juni 2022
[182] 'Snapchat introduces first parental controls', nytimes.com, 9 augustus 2022
[183] 'Meta expands parental control for Instagram and VR', cnet.com, 14 juni 2022
[184] Position Paper Bits of Freedom t.b.v. rondetafelgesprek inzake de rol van sociale mediaplatformen, 2022 p. 2.
[185] *Verslag van een rondetafelgesprek, gehouden op 10 februari 2022, over de rol van socialmediaplatformen,* 2022, p. 11.

Op het gebied van cyberveiligheid aspecten

Op het gebied van cyberveiligheid worden ook technische middelen ingezet. Zoals eerder benoemd maken veel telefoonfabrikanten gebruik van biometrische ontgrendeling, zodat ongewenste toegang tot apparatuur niet gemakkelijk kan plaatsvinden. Ook encryptie wordt door veel ontwikkelaars ingezet om gebruikersgegevens te versleutelen en geschreven of ontvangen berichten niet gemakkelijk toegankelijk te maken bij een hack.

Specifiek op het gebied van cyberveiligheid zijn er een aantal maatregelen op het gebeid van mensen, proces en technologie die veel van de cyber-specifieke risico's al kunnen verkleinen. Op menselijk gebied loont het om zowel gebruikers en ontwikkelaars te onderwijzen in het veilige gebruik van apps en cyberveiligheid. Het is tegenwoordig veel aannemelijker om 'gehackt' te worden via een phish dan daadwerkelijk een hacker die technisch inbreekt in een systeem. Dit geldt ook voor ontwikkelaars. Ontwikkelaars zijn steeds vaker doelwit van social engineering van hackers om toegang te krijgen tot de beheerssystemen van een ontwikkelaar. Zoals onlangs de LAPSUS$[186] aanvallen lieten zien is dat een hacker ondanks goed beveiligde systemen nog steeds binnen kan komen via het manipuleren van mensen.[187]

Procesmatig valt er in de gehele keten winst te behalen mits bedrijven meer doen aan Security by Design. Bij Security by Design is veiligheid vanaf het begin af aan meegenomen in het ontwerp en productieproces van een product of service. Hierdoor is er sprake van een verbeterde fundamentele veiligheid van het product. In deze context houdt dat in dat cyberveiligheid heel vroeg in het ontwikkelproces betrokken wordt. Security by Design zorgt ervoor dat risico's in mindere mate pas na ontwikkelen worden ontdekt en afgedicht. Tot slot helpen technische maatregelen zoals sterkere authenticatievormen (multi-factor authenticatie), veilige standaardinstellingen, en het versleutelen van gebruikersdata in opslag en transport voor veiligere apps.

Er zijn ook een hoop middelen ontwikkeld om onrechtmatige toegang tot een apparaat te bemoeilijken. Zoals eerder gezegd, worden functies aangeboden met betrekking tot het instellen van wachtwoorden en biometrische technologie. Er worden echter meer maatregelen getroffen. Een nieuwe functionaliteit van bijvoorbeeld Huawei – de 'Maintenance Mode', dient ook onrechtmatige toegang tot een apparaat te bemoeilijken. Wanneer een Huawei toestel moet worden gerepareerd, kan de gebruiker de maintenance mode aanzetten alvorens hij of zij het toestel indient ter reparatie. De Maintenance Mode versleuteld alle aspecten van private data door middel van veiligheidsalgoritmen. Alleen de vooraf-geïnstalleerde apps zijn dan nog zichtbaar. Alle apps die zijn geïnstalleerd door de gebruiker zelf zijn niet meer zichtbaar op het toestel, net als foto's, e-mails, contacten, berichten, login informatie en betalingsinformatie. De Maintenance Mode kan worden vergeleken met een tijdelijke fabrieksinstelling.[188]

> "Het is tegenwoordig veel aannemelijker om 'gehackt' te worden via een phish dan daadwerkelijk een hacker die technisch inbreekt in een systeem"

Bovenstaande stipt echter ook meteen een moeilijkheid op het gebied van cyberveiligheid aan. De gebruiker is namelijk medeverantwoordelijk voor de effectiviteit van de middelen die door ontwikkelaars worden gebouwd. Het is immers zo dat 'ontwikkelaars' allerlei mechanismen kunnen maken, maar gebruikers zullen bijvoorbeeld zelf voor een sterk wachtwoord moeten zorgen. Ook is de gebruiker zelf verantwoordelijk voor het tijdig updaten van zijn of haar apparaat, al wordt de gebruiker tegenwoordig wel gewaarschuwd middels notificaties dat hij of zij een update moet doorvoeren. Ontwikkelaars kunnen dus zeker zorgen voor technische hulpmiddelen, maar deze moeten veelal door de gebruiker zelf worden ingezet om cyberveiligheid zoveel mogelijk te garanderen.

[186] Lapsus$ is een criminele hackergroep die afgelopen Jaren veelal in het nieuws kwam om grote hacks bij bedrijven zoals Microsoft. De groep speelde voornamelijk in op binnenkomen via mensen die hun wachtwoorden deelden (via phishing of omkoping).

[187] 'Lapsus$: Oxford teen accused of being multi-millionaire cyber-criminal', https://www.bbc.com/news/technology-60864283

[188] 'Discover the Maintenance mode', consumer.huawei.com.

Standaardisering & ketenafspraken
Behalve dat ieder bedrijf individueel iets kan doen, is er ook afstemming onderling nodig. Er zijn diverse nationale en internationale samenwerkingsverbanden waarin gezamenlijke praktijk- en gedragscodes, toegespitst op specifieke problemen, fenomenen en typen content worden afgesproken. Via branchevereniging en andere soorten sector- of professional-specifieke clubs worden ervaringen en *best practices* uitgewisseld.

In sommige gevallen is de uitwisseling het resultaat van (of aangemoedigd door) ontwikkelingen in wet- en regelgeving. Zo zal NISII veel meer verantwoordelijkheden bij organisaties in de kritieke infrastructuur neerleggen en ingrijpen op ketenverantwoordelijkheden (zie hoofdstuk 4). Brancheorganisaties vertegenwoordigen toeleveranciers van diensten en vormen ook een vehikel om standaarden op het gebied van cyberveiligheid, privacy en andere risico's te introduceren. Het is dan ook mogelijk om meer te bewerkstelligen in de keten van mobiele toestellen, zonder dat daar specifiek wetgeving bij aan te pas hoeft te komen. Zelfregulering is sneller en kan minstens net zo effectief zijn. Zo zijn er ook al keurmerken voor pentesten[189] waaraan marktpartijen zich committeren.

Het voordeel van dergelijke vormen van zelfregulering is dat deze veel vaker en sneller kan worden geactualiseerd ten opzichte van een wet. Zelfregulering zorgt voor snelle reacties op nieuwe bedreigingen die oprukken en is als zodanig effectiever in het beschermen van gebruikers. Daarnaast kunnen keurmerken en certificeringen bedrijven helpen bij het maken van keuzes over leveranciers en ketenpartners. Op deze manier kan een bedrijf zelf ook een eiser zijn van bepaalde zekerheden over de bescherming van gebruikers. Bedrijven willen dat hun toeleveranciers zich net zo opstellen tegenover hun klanten als zij zelf zouden doen wat betreft de in acht neming van bepaalde waardes. Via certificering kunnen afspraken en standaarden worden vastgelegd en kunnen bedrijven bij hun leveranciers aangeven wat ze daarin belangrijk vinden, zodat de leverancier aan kan tonen dat hun dienst op een dergelijke wijze is samengesteld.

Opkomende EU-wetgeving zoals de Cybersecurity Act heeft onder andere als doel om EU-breed gedragen certificeringschema's te introduceren. Hoewel de Cybersecurity Act zelf geen verplichting stelt aan deze certificering zijn er al wel andere wetten zoals de Digital Operational Resiliency Act die eisen stellen aan in dit geval de financiële sector om certificaten te hanteren die erkend worden door certificeringinstanties zoals aangemerkt in de Cybersecurity Act. Dit signaleert een bredere trend dat er opkomende certificaten zijn die steeds meer gehanteerd zullen worden.

Uitdagingen voor ontwikkelaars
Voor ontwikkelaars is het ingewikkeld en riskant om beslissingen te maken in "grijze gebieden". 'Wanneer wordt *online shaming* laster?', 'wanneer slaat het modereren van content om in mogelijke censuur?' en 'hoe kan er worden omgegaan met kwakzalverij?' zijn onderwerpen waar ontwikkelaars mee worstelen. Een ontwerpkeuze of manier van modereren heeft al snel invloed op zaken zoals de vrijheid van meningsuiting, toegang tot informatie, persvrijheid en vrijheid van ondernemerschap. Dergelijke vrijheden kunnen op gespannen voet staan met het recht op persoonlijke integriteit, de bewegingsruimte en veiligheid van mensen online en van minderheden in het bijzonder – en ook aan democratische en rechtstatelijke beginselen. Een veelbesproken voorbeeld van dit spanningsveld is de schorsing van Donald Trump door Twitter na de bestorming van het Capitool. Critici benadrukken dat dit zonder democratische controle kon plaatsvinden en dat de macht om dergelijke besluiten te nemen schadelijk kan zijn voor democratische normen en waarden.. Zulke contentmoderatie zou niet binnen het takenpakket van de ontwikkelaar moeten liggen, maar zou ook niet de verantwoordelijkheid van de staat moeten zijn.[190] In de Digital Services Act wordt getracht hier een balans in te vinden.

Daarnaast is het ook een grijs gebied waar verantwoordelijkheden eindigen en beginnen. Uiteindelijk is het gebruik van mobiele toestellen en apps een gedeelde verantwoordelijkheid van alle schakels in de keten. Zowel netwerkaanbieders, toestelfabrikanten, appwinkels en app-ontwikkelaars, als gebruikers zelf, zullen een deel van de verantwoordelijkheid op zich moeten nemen en zij zullen hier gezamenlijk duidelijkere afspraken over moeten maken.

[189] 'Keurmerk voor pentesten beschikbaar', cyberveilignederland.nl.

[190] *Verslag van een rondetafelgesprek, gehouden op 10 februari 2022, over de rol van socialmediaplatformen,* 2022, p. 8.

Hoewel ontwikkelaars vaak zelf onderzoek doen naar de impact van bepaalde keuzes, is er weinig ruimte voor publiek debat over alternatieve opties. Onderzoeksresultaten, rapportages van verschillend formaat en allerlei cijfermateriaal kan worden geclassificeerd als “bedrijfsgeheim”.[191] Om meer inzicht te krijgen in de mechanismen en impact van bepaalde ontwerpkeuzes, zou openbaarheid wenselijk zijn. Er gaan dan ook stemmen op om voorlichtings- of transparantieverplichtingen op te leggen die onafhankelijk onderzoek zou faciliteren. Dit zou kunnen bijdragen aan betere – democratisch gelegitimeerde - afspraken.[192]

Juist door nieuwe en opkomende wet- en regelgeving zal het speelveld weer transformeren. Dit zal ook invloed hebben op de organisatie van toezicht vanuit de markt zelf. Uit de interviews komen verschillende signalen over de DMA/DSA en de manier waarop met name de filterrol van appwinkels (wat heeft bijgedragen aan veiligheid en vertrouwen) wordt ondermijnd door het verruimen van sideloading praktijken via de DMA.[193]

Daarnaast is door een aantal geïnterviewden benoemd dat het van belang is om kleinere ontwikkelaars niet uit het oog te verliezen. Bij ontwikkelaars wordt vaak gedacht aan de grootste marktpartijen en daar is opkomende EU-wetgeving, zoals de DMA, ook op gericht. Echter vallen kleine bedrijven ook onder de noemer ‘ontwikkelaar’ wanneer zij een app voor een bepaalde dienst hebben gebouwd en gepubliceerd. Ook zij zullen de gevolgen van nieuwe wetgeving ervaren. Zij hebben dan ook de extra uitdaging om opkomende wetgeving uitvoerbaar te maken, zeker wanneer zij geen juridische expertise in huis hebben.

[191] Rathenau Instituut, 2022, p. 3.
[192] ‘Whistleblower says Bill must include tool that forces Facebook to publish data’, independent.ie, 23 februari 2022.
[193] ‘Apple would be forced to allow sideloading and third-party app stores under new EU law’, theverge.com, 25 maart 2022.

4.3. Meer dan wetgeving & toezicht vanuit de overheid

In H3 is de inhoud van relevante wettelijke kaders behandeld, alsook de rol van toezichthouders, zoals de Autoriteit Persoonsgegevens (AP), Autoriteit Consument en Markt (ACM) en Agentschap Telecom (AT), en de rechterlijke macht om toe te zien op de naleving ervan. Hieronder wordt ingezoomd op overige maatregelen en drukmiddelen die de overheid kan inzetten om risico's te mitigeren en gebruikers beter te beschermen. Er valt een onderscheid te maken tussen interventies gericht op (1) ontmoediging en stimulering bij voorkeur met behulp van op open normen, certificering, en standaardisatie (2) het stellen van eisen door de overheid in de hoedanigheid van afnemer, en (3) het organiseren of steunen van initiatieven voor begeleiding en praktijkonderzoek.

Als algemeen punt van aandacht is het belangrijk om te benoemen dat het voor elk van de onderstaande drukmiddelen en maatregelen noodzakelijk is dat de overheid digitaal onderlegd is. Wanneer dit onvoldoende het geval is, kunnen onderstaande middelen niet adequaat worden gewaarborgd.

Ontmoedigen en stimuleren

De primaire taak van de overheid is om de rechten van burgers te beschermen, ook online. Specifieke groepen die online kwetsbaar zijn, zoals minderheden en minderjarigen, hebben hier de meeste baat bij.

Iets bestraffen – incl. boetes opleggen, partijen verantwoordelijk stellen voor schade en compensatie afdwingen – kan een effectief drukmiddel zijn, maar niet voor alle spelers in het ecosysteem. Zo hebben grote ontwikkelaars de luxe om een kosten-batenanalyse te maken, omdat zij voldoende middelen ter beschikking hebben om eventuele boetes te incasseren.[194]Kleine bedrijven daarentegen zullen veel harder geraakt worden. Hoewel het bestraffen van mensen of organisaties die zich onrechtmatig of strafbaar gedragen belangrijk is voor genoegdoening, laat de schaal en aard van de fenomenen dit niet altijd toe. Een juridische aanpak gericht op verbieden en bestraffen is dus niet voldoende om gebruikers te beschermen.

Ter illustratie: in de fysieke wereld is de politie zichtbaar op straat. Politie op straat heeft een afschrikwekkende werking op strafbare praktijken omdat de pakkans wordt vergroot. "Blauw op straat" heeft dus een preventieve werking en dit fenomeen zal ook online verder kunnen worden doorgevoerd.[195] Door ook online ruimte in te nemen, bijvoorbeeld met advertenties of via afspraken met platformen, worden gebruikers er online aan herinnerd dat het internet geen wetteloze omgeving is. Het is belangrijk dat de pakkans en kans op vervolging naar aanleiding van aangifte of melding van klachten, hoog is. Dat betekent dat politie, het Openbaar Ministerie en toezichthouders actief optreden tegen onveilige digitale producten, en toezien op de naleving van zorgplichten voor veilige digitale producten door ontwikkelaars. Hiervoor moeten zij voldoende middelen tot hun beschikking krijgen om klachten te kunnen onderzoeken en eventueel te bestraffen.

De overheid zou zich kunnen laten inspireren door o.a. de Online Safety Bill die wordt besproken binnen het Verenigd Koninkrijk. In dit voorstel worden meer eisen gesteld aan gebruikersvoorwaarden, klachten- en verhaalprocedures van platformen en wordt ook extra aandacht besteed aan het verwijderen van illegale content. Ook het beter beschermen van minderjarigen online wordt expliciet benoemd. Er wordt gesteld dat de overheid actief zal optreden tegen platformen en andere online omgevingen die zich niet houden aan het voorstel, door bijvoorbeeld forse boetes uit te delen en toegang tot deze online omgevingen en platformen te blokkeren.[196] De Nederlandse overheid zou, met het oog op aankomende wetgeving zoals de Digital Services Act, hier een voorbeeld aan kunnen nemen.[197]

Naast het (juridisch) afdwingen of dichttimmeren door middel van regels, waar allerlei actoren zich aan dienen te houden, kan de overheid ook inzetten om het stimuleren van samenwerking tussen platformen en het maatschappelijk middenveld. Wettelijke kaders zijn belangrijk, maar wetten zijn niet altijd nodig om een bepaalde risicobeperking te genereren. Er kunnen ook zachtere middelen, zoals stimuleringssubsidies en onderzoeksprogramma's worden ingezet. Wanneer een bedrijf zich houdt aan opgestelde kwaliteitsnormen of branchestandaarden omtrent cyberveiligheid en privacy van hun gebouwde software, kan dit bedrijf worden

[194] 'Can fines break Big Tech monopolies?', techmonitor.ai, 15 maart 2022.
[195] 'Versterking politie in wijken, op internet, voor opsporing en voor boa's', rijksoverheid.nl, 13 oktober 2021.
[196] 'Policy Paper. Online Safety Bill: factsheet', gov.uk, 19 april 2022.
[197] Van Huijstee et. al. 2021, p. 141.

beloond. Daarnaast kunnen fiscale stimulansen mogelijk ook effectief zijn, afhankelijk van hoe deze worden ingezet.

Eisen stellen als grootgebruiker
De overheid is zelf ook een grote afnemer/gebruiker van software van derde partijen. In die hoedanigheid kan zij ook voorwaarden formuleren en standaarden of kwaliteitseisen opleggen. Op die manier kan er al heel wat aan standaardisering worden afgedwongen bij een specifieke toeleverancier, wat vervolgens door kan sijpelen naar andere branches en de rest van de bedrijfswereld.[198] De overheid is daar momenteel te terughoudend in uit angst zichzelf te veel te beperken. Toch is eerder gebleken dat zulke kwaliteitseisen effectief kunnen zijn en dat ze op een hoger tempo kunnen worden opgesteld.

Impact onderzoeken en begeleiding bieden
Zoals eerder is benoemd en in diverse interviews is aangegeven, kan de grote hoeveelheid aan opkomende wetgeving, bijvoorbeeld uit de EU, met name bij de kleinere partijen voor moeilijkheden zorgen. Grotere ontwikkelaars hebben over het algemeen meer capaciteit om nieuwe regels en vereisten te implementeren. Goede begeleiding voor de kleinere bedrijven is daarom erg belangrijk en de overheid zou hierbij meer kunnen ondersteunen.

Ook geven geïnterviewden aan dat wet- en regelgeving om risico's voor gebruikers van mobiele toestellen en apps (of digitale technologieën in het algemeen) te mitigeren gebaseerd zou moeten zijn op principes (niet gericht op regulatie van een specifieke technologie). Ook is er een duidelijke roep om *evidence-based* regulering. Dit betekent onder andere dat nieuwe wet- en regelgeving op de juiste manier moet worden getoetst op gevolgen en of deze gevolgen proportioneel en eerlijk zijn. Om een voorbeeld te geven: de Europese Commissie is op 11 mei 2022 met een voorstel gekomen om het verkeerd gebruik van online diensten met als doel het seksueel misbruiken van kinderen, te voorkomen.[199] In het voorstel wordt aangegeven dat bedrijven moeten kunnen worden gedwongen om mee te kijken met wat internetgebruikers in bijvoorbeeld chat-apps doen, Het maatschappelijk middenveld vraagt zich af of dit voorstel nog wel redelijk en proportioneel is. Bovendien vraagt men zich af of zulke regelgeving überhaupt wel technisch haalbaar is.[200] Daarnaast zal er samenhang in wetgeving moeten worden gezocht. Op dit moment is dat niet altijd het geval en zijn er wetten die elkaar tegenspreken en zijn er wetten die bepaalde overlap met elkaar hebben. Aan de ene kant zal de *Digital Services Act* platforms bijvoorbeeld meer verantwoordelijkheid geven, maar de *Digital Markets Act* holt bepaalde rollen uit die in de afgelopen jaren zijn ontwikkeld en hebben gezorgd voor een veilige, betrouwbare app omgeving. Dat komt voor sommige spelers niet consequent over. Ook op de Data Act is er kritiek omtrent onduidelijkheden ten opzichte van andere wetgeving. Toezichthouders hebben bijvoorbeeld aangegeven dat de huidige, voorgestelde tekst afbreuk kan doen aan de AVG.[201] Dit soort overlap en discongruenties tussen wetten en regels kunnen een bron van verwarring zijn.

"Er is een duidelijke roep om evidence-based regulering"

Uitdagingen voor de overheid

Zoals eerder genoemd is het zaak dat de overheid voldoende digitaal onderlegd is om problematiek adequaat aan te pakken. In verschillende interviews wordt gesuggereerd dat de digitale kunde van de overheid nog ondermaats is. Daarnaast lijkt de besluitvormingscultuur vaak geen stimulans voor doordacht beleid.

Er wordt wisselend gebruik gemaakt van principle-based en rule-based wet- en regelgeving (zie ook H3). Behalve snelle ontwikkelingen in de technologie, veranderen ook de normen in de samenleving. Aan de ene kant is er een roep tot open normen, aan de andere kant leert de praktijk dat dit veel ruimte laat voor interpretatie waardoor risico's in de praktijk alsnog niet voldoende afgedekt worden. Toch is het lastig om tot uniforme regels en eenduidige aanpak te komen, omdat de hoeveelheid en diversiteit van apps en diensten enorm is. Het is een grote opgave om zicht te houden op wat er "te koop" is, hoe mensen interacteren met het aanbod en waar het toe leidt. Er is een spanning tussen het observeren en signaleren van risico's en het onnodig surveilleren.

[198] *Cyberweerbaarheid met nieuwe technologie* 2020, p. 56
[199] 'Fighting child sexual abuse: Commission proposes new rules to protect children', ec.europa.eu, 11 mei 2022
[200] 'Europese Commissie wil vertrouwelijkheid op internet opheffen', bitsoffreedom.nl, 11 mei 2022
[201] 'Toezichthouders willen verbeteringen Data Act', autoriteitpersoonsgegevens.nl, 6 mei 2022

Toezichthouders hebben de taak om toe te zien op de juiste uitvoering van specifieke wet- en regelgeving. In de praktijk blijkt dat dit bijwijlen onvoldoende gebeurt. Dit komt mede doordat sommige toezichthouders onvoldoende capaciteit en andere noodzakelijke middelen krijgen om het werk adequaat uit te kunnen voeren.

Een andere uitdaging voor de overheid ligt bij het uitvoerbaar maken van bepaalde wetgeving en het ondersteunen van kleine en middelgrote bedrijven. De omvang van de opkomende Europese wetgeving is aanzienlijk. Wanneer een bedrijf geen beschikking heeft tot juridische expertise wordt de uitvoerbaarheid van deze wetgeving bemoeilijkt. De overheid zal dus adequate uitleg moeten geven over opkomende veranderingen en middelen moeten inzetten om deze bedrijven te helpen bij de invulling en naleving van deze wetten.

4.4. Conclusie: hiaten & aandachtspunten

Om een betrouwbaar ecosysteem van mobiele toestellen en apps te organiseren, zijn verschillende type maatregelen nodig. Zoals de besproken in de inleiding, heeft betrouwbare technologie drie componenten: wettig, ethisch en robuust.[202] In het vorige hoofdstuk kwam naar voren dat de wettelijke kaders momenteel worden geactualiseerd, maar dat er meer nodig is om gebruikers, ontwikkelaars en derden aan toepasselijke wet- en regelgeving te houden. Daarnaast zijn additionele maatregelen nodig om ervoor te zorgen dat mobiele apps niet alleen wettig, maar ook ethisch en robuust zijn. De verschillende stakeholders in het ecosysteem, waaronder het maatschappelijk middenveld, ontwikkelaars en de overheid, dragen allen een verantwoordelijkheid in het ontwikkelen van betrouwbare technologie.

Het maatschappelijk middenveld is in staat invloed uit te oefenen op alle drie de componenten. Belangenorganisaties, journalisten, onderzoeksinstituten en hulpverleners zijn bijvoorbeeld bij uitstek in staat om wensen en grenzen van gebruikers te signaleren. Deze organisaties kunnen deze wensen en grenzen vervolgens agenderen bij ontwikkelaars en de overheid en daarmee invulling geven aan de definitie van ethische en robuuste technologie.

Ontwikkelaars ondernemen actie op het gebied van zelfregulering en standaardisering, vooral op het gebied van cyberveiligheid. Op die manier dragen zijn bij aan robuuste technologie. Ontwikkelaars zijn doordrongen van het belang van cyberveiligheid: het vertrouwen van de gebruiker is hierbij een sleutelbegrip. Adequate cyberveiligheid draagt namelijk bij aan het vertrouwen van de gebruiker. Ontwikkelaars beseffen dat inadequate cyberveiligheid kan resulteren in een verlies van gebruikersvertrouwen.

Vanuit de overheid is toezicht en handhaving belangrijk om risico's betreft het gebruik van mobiele toestellen en apps op basis van wetgeving verder in te perken. Het is essentieel dat toezichthouders en handhavers daarbij voldoende (financiële) middelen ter beschikking hebben om partijen die de wet niet naleven te kunnen onderzoeken en waar nodig te bestraffen. De geschetste risico's in dit onderzoek zijn echter niet volledig te elimineren door wetgeving. Iedere technologie kent namelijk een periode waarin de wetgeving nog niet toepasbaar is op deze technologie, er altijd individuen of organisaties zijn die loopholes vinden in de wet en er zaken zijn die nooit volledig wettelijk gedekt kunnen worden. De overheid kan daarom ontwikkelaars stimuleren om gebruikers beter te beschermen en ethisch te handelen, bijvoorbeeld door het verstrekken van subsidies of het opleggen van kwaliteitseisen bij haar eigen leveranciers.

Het is vooral belangrijk dat het maatschappelijk middenveld, ontwikkelaars en de overheid niet in een vacuüm opereren, maar juist samenwerking opzoeken in het bepalen van wat wettige, ethische en robuuste technologie behelst. Op het gebied van onderwijs en voorlichting is samenwerking bijvoorbeeld zeer gewenst. Het is bijvoorbeeld onduidelijk tot waar de invloedsfeer van de ontwikkelaar reikt en wanneer een ouder verantwoordelijk wordt voor wat een minderjarige online te zien krijgt. Daarnaast is de behoefte om samen te werken ook duidelijk gemaakt door de verschillende partijen. Wanneer een integrale aanpak wordt gehanteerd om risico's te mitigeren, en de verschillende kennisgebieden met elkaar kunnen zoeken naar oplossingen, zullen er verbeteringen op dit gebied kunnen plaatsvinden.

[202] *Ethics guidelines for trustworthy AI* 2019, p. 5.

Een overzicht van de gereedschapskist

Wettelijke kaders (als zijnde democratisch gelegitimeerde afspraken en regels)	Internationaal OECD, UNESCO, etc.)	Europees (A Europe Fit for the Digital Age)	Nationaal (Beleid voor digitalisering)
Normen en regels waarop wordt toegezien vanuit overheidsinstanties (al dan niet via een verdere (formele) uitwerking van open normen)	Open normen (ver- en geboden)	Leidraad van toezichthouders	Interpretaties van ontwikkelaars
Instructies, standaarden en certificering die worden ontwikkeld om in de praktijk houvast te bieden (door bedrijven of toezichthouders ontwikkeld; maar nog niet getoetst voor de rechter)	NEN, ISO, standaarden en certificaten	Gedragsregels (afspraken in branche/sector)	Best practices (gedeeld binnen sector of in bredere samenwerkingsverbanden)
Ontwerpkeuzes die kunnen worden ontwikkeld en ingebouwd (bijv. op eigen initiatief of n.a.v. geëxpliciteerde wensen van de markt)	Eigen beleid (individuele bedrijven /organisaties)	Opties in de instellingen (individuele apps/per type apps)	Opties in webdesign (keuzes voor/tegen endless scrolling, below/above the fold, etc.)
Begeleiding bij problemen (bijv. bijstand door NGO's, hulpverleners, etc.)	Rapporteren van problemen (in the app)	Support vanuit de ontwikkelaar of hulporganisaties (geld terug, excuses, etc.)	Juridisch loket (escaleren van problemen; bij rechter of toezichthouder – compensatie, etc.)
Handelingsmogelijkheden van het individu (de gebruiker zelf)	App verwijderen; afstand doen van toestel	Opties in de app gebruiken (mensen blokkeren, melding doen, etc.)	Additionele hulpmiddelen; blockers/timers, etc om eigen gebruik te beheersen.

5. Conclusie

In opdracht van EZK is onderzocht in welke mate de risico's en kwetsbaarheden van mobiele toestellen en apps worden geadresseerd binnen de vigerende en opkomende wet- en regelgeving en hoe Nederlandse gebruikers - minderjarigen in het bijzonder - beter kunnen worden beschermd.

In dit rapport zijn daarvoor het ecosysteem (H1), de risico's (H2), de wet- en regelgeving (H3) en andere typen maatregelen en handelingsopties (H4) uitgediept. Op basis van desk research en interviews met marktpartijen, brancheverenigingen en belangenorganisaties, zijn de hiaten en aandachts- en verbeterpunten geanalyseerd.

5.1. Zicht op de risico's voor gebruikers van mobiele toestellen en apps

Het ecosysteem in beeld

Het gebruik van mobiele toestellen en apps gaat gepaard met risico's voor de individuele gebruiker, en minderjarigen in het bijzonder. Om de risico's en kwetsbaarheden te kunnen duiden, is allereerst inzicht vereist in de verschillende onderdelen van het ecosysteem. Hoofdstuk 1 licht de verschillende elementen uit: actoren, locaties, omgevingsfactoren en relaties. Verschillende partijen en lagen in de technologie zorgen gezamenlijk voor het functioneren van mobiele toestellen en apps. De partijen die betrokken zijn bij de ontwikkeling, productie en levering van deze technologielagen, opereren in een keten én een maatschappelijke context.

Verschillende type gebruikersgroepen, maar ook maatschappelijke organisaties en overheidsinstanties stellen eisen, kaders en grenzen aan hoe mobiele toestellen gemaakt en gebruikt (zouden moeten) worden. Op die manier hebben gebruikers en ontwikkelaars, en allerlei partijen in de hoedanigheid van "beïnvloeder" een rol in het borgen van cyberveiligheid, privacy en andere ethische waarden. Omgevingsfactoren – zoals de aard en omvang van de app-economie, achterliggende verdienmodellen, en ontwerpkeuzes binnen en karakteristieken van de digitale omgeving – geven vorm aan de belevingswereld en de handelingsmogelijkheden van alle actoren binnen het ecosysteem.

Door het uiteenrafelen van de ecosysteemelementen is verhelderd dat de afhankelijkheden en kwetsbaarheiden niet louter betrekking hebben op mobiele toestellen en apps. Het raakt aan grotere vraagstukken over de digitale wereld, dat door de snelle ontwikkelingen een moving target is geworden en het speelveld voortduren zal veranderen.

De risico's in beeld

Om die risico's uit te diepen, zijn in hoofdstuk 2 diverse incidenten onder de loep genomen die een impact hebben op gebruikers. Via een klassieke risicoanalyse zijn componenten die nodig zijn om tot zo'n incident te komen uitgelicht. **De acht uitgewerkte type incidenten zijn op hoger abstractieniveau geclusterd in:**

(1) problemen die te maken hebben met sociale aspecten (schadelijk gedrag van gebruikers)
(2) privacy & ethische aspecten (die verbonden zijn met grootschalige dataverwerking binnen het ecosysteem van toestellen en apps),
(3) cyberveiligheid aspecten (waarbij de focus ligt op acties van criminelen).

Behalve de aard van mobiele toestellen en apps, speelt de aard van de mens en omgeving door in risico's op incidenten.

Allerlei vormen van pesten, intimidatie, haatzaaiing en laster vinden momenteel plaats op mobiele toestellen en apps. Ook indirecte interacties en individuele kwetsbaarheden zorgen voor problemen: de aantrekkingskracht van de producten en diensten kan enorm zijn en sociale verwachtingen over bereikbaarheid en zichtbaarheid, kunnen kwetsbare gebruikersgroepen onder druk zetten en/of leiden tot stress, verslaving of andere ongezonde gewoonten.

De aantrekkelijkheid en mechanismes van mobiele toestellen en apps hangen samen met de datastromen en algoritmen die worden ingezet. Het verzamelen en beheren van grote hoeveelheden data vraagt om privacy- en informatiebeveiligingsmaatregelen. Maar behalve juridische en cyberveiligheid aspecten, is er ook aandacht nodig voor de diverse mogelijkheden die ontstaan om gebruikers te beïnvloeden – en hoe daar verantwoord mee om te gaan. Het gaat daarbij niet alleen om commerciële partijen, maar ook om overheden en overige partijen met eventuele politieke of ideologische doeleinden.

De data uit of mechanismen in mobiele toestellen en apps kunnen door vele actoren worden benut. Dit roept tal van maatschappelijke, ethische en politieke vragen op. Als ontwerper van de digitale omgeving zelf, hebben sommige partijen in het ecosysteem daarbovenop nog een unieke machtspositie. Zij kunnen achter de schermen beslissingen en designkeuzes maken en inzetten op een inrichting die hun eigen belang dient. Hoe deze macht in te kaderen, is

"Als ontwerper van de digitale omgeving zelf, hebben sommige partijen in het ecosysteem een unieke machtspositie"

een belangrijk onderwerp binnen nieuwe wetsvoorstellen. Toch zal ethische reflectie – en niet louter naleving – ingebed moeten worden binnen de ontwikkeling en het gebruik van technologie.

Ten slotte moet er rekening mee worden gehouden dat, zolang personen of organisaties met kwaadwillende intenties actief zijn, er altijd mogelijkheden zullen zijn om veiligheidsmaatregelen te omzeilen en kwetsbaarheden in de technologie uit te buiten, al dan niet via het manipuleren van een gebruiker. In sommige gevallen zijn minderjarigen extra kwetsbaar. **Toch zijn ook andere gebruikersgroepen vatbaar voor risico's en ligt de oplossing ogenschijnlijk niet in het beschermen van specifieke groepen, maar in het transformeren van praktijken**.

De wettelijke kaders in beeld
In hoofdstuk 3 zijn deze categorieën gehanteerd om in te zoomen op de wettelijke kaders die reeds bestaan of in ontwikkeling zijn om gebruikers te beschermen tegen de vastgestelde risico's. De wereld van mobiele toestellen en apps is niet wetteloos. Gegevensbescherming, consumentenbescherming, mededinging, maar ook algemeen straf- en civiel recht spelen een rol bij het gebruik van mobiele toestellen en apps. Bepaalde wet- en regelgeving werkt op gebruikers, ontwikkelaars en kwaadwillende derden door handelingen strafbaar te stellen. Anderzijds werkt sommige wetgeving juist op het verbeteren van de weerbaarheid van dat wat ontwikkelaars aanbieden, om zodoende gebruikers beter te beschermen.

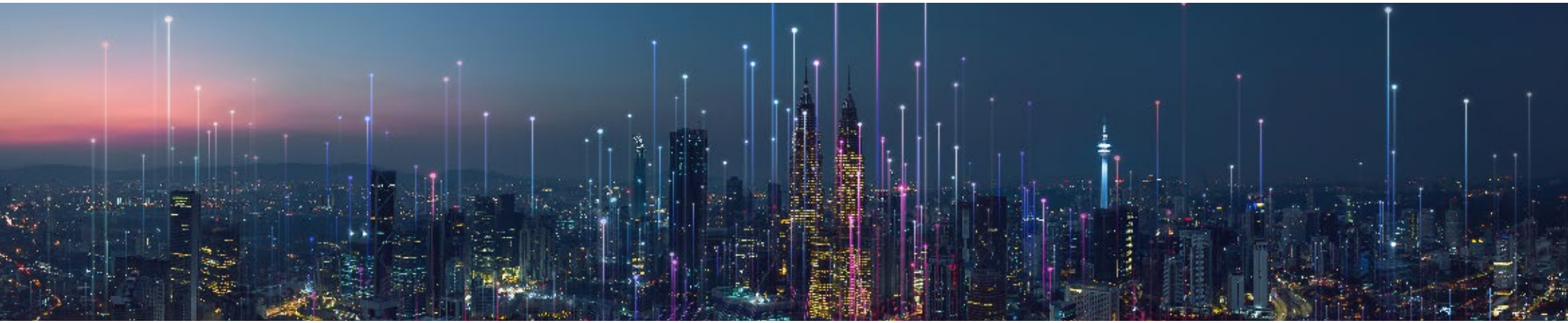
"Om recht te doen aan het pakket wat vanuit Europa onderweg is, zullen toezichthouders op zowel nationaal als Europees niveau meer met elkaar moeten samenwerken en duidelijke afspraken maken over waar ieders verantwoordelijkheid begint en eindigt. Hiervoor is capaciteit, kennis en kunde nodig.

Het Europese wetgevings- en investeringsprogramma 'A Europe fit for the Digital Age ' laat zien dat bestaande kaders niet voldoende aansloten bij de huidige staat van de technologie, bedrijfsvoering en markten. Veel van de wetsvoorstellen hebben een afschrikwekkend effect, maar zijn daarnaast ook gericht op het vergroten van de weerbaarheid. Zo legt bijvoorbeeld de NIS II meer verantwoordelijkheden bij organisaties in de kritieke infrastructuur (waaronder ontwikkelaars van digitale diensten, zoekmachines, marktplaatsen en sociale media platforms). Ook zijn bijvoorbeeld de Digital Markets Act en Digital Services Act voor een groot deel gericht op het beleggen van verantwoordelijkheden bij de ontwikkelaars en het egaliseren van machtsverhoudingen.

Ook worden er standaarden en kwaliteitsnormen geëist waarmee de gebruiker beter beschermd kan worden. Om die reden moeten niet alleen wetsteksten, maar ook, de instituties met de juiste kennis en bevoegdheden worden geüpdatet. **Diverse partijen hebben een rol bij de verdere uitwerking, uitvoering en handhaving van de wet- en regelgeving**. Met name op het gebied van toezicht en handhaving ontstaan extra uitdagingen. Om recht te doen aan het pakket wat vanuit Europa onderweg is, zullen toezichthouders op zowel nationaal als Europees niveau meer met elkaar moeten samenwerken en duidelijke afspraken maken over waar ieders verantwoordelijkheid begint en eindigt. Hiervoor is capaciteit, kennis en kunde nodig.

De overige maatregelen en drukmiddelen in beeld
In hoofdstuk 4 is uitgewerkt hoe ook andere maatregelen en handelingsopties – aanvullend op of in de geest van de wettelijke kaders – van belang kunnen zijn bij het beter beschermen van gebruikers en het mitigeren van risico's. Zo staan hulpverleners en maatschappelijke organisaties direct in contact met gebruikers en zijn deze partijen daardoor in staat te signaleren waar het misgaat. Deze kennis en ervaring kan worden benut om beleid te agenderen en beïnvloeden. Daarnaast zijn er tal van mogelijkheden voor de ontwikkelaars van apps en toestellen om risico's te mitigeren – al dan niet aangemoedigd door wet- en regelgeving.

Via eigen bedrijfsprincipes en -waarden, gebruikersvoorwaarden en kwaliteits- en zorgvuldigheidseisen, geven bedrijven vorm aan praktijken. Ontwikkelaars zijn hier duidelijk al stappen in aan het zetten. Zo worden diverse technische hulpmiddelen ontwikkeld om gebruikers meer regie en keuzevrijheid te geven. Voor de overheid is het dan ook zaak om niet alleen in te zetten op het dichten van hiaten in de wet, maar ook praktisch invulling te geven aan behoeften en zorgen. Zo kan de overheid bijvoorbeeld zelf standaarden hanteren en behulpzame initiatieven stimuleren via subsidies en (onderzoeks-)programma's.



5.2. Complexe ketens en gezamenlijke verantwoordelijkheden

Het doel van dit onderzoek was om zicht te krijgen op de knoppen waaraan gedraaid kan worden om gebruikers van mobiele toestellen en apps – en minderjarigen in het bijzonder – beter te beschermen. Het is duidelijk dat er verschillende soorten risico's bestaan. Daardoor is de aard van handelingsopties ook divers.

Gesignaleerde kwesties worden momenteel met name op Europees niveau omgezet in beleidsmaatregelen. **Echter, het zijn vaak niet alleen hiaten in wettelijke kaders, maar ook gebrekkige naleving en toezicht die voor problemen zorgen**. Toezichthouders investeren duidelijk in kennisopbouw en in samenwerking met collega-toezichthouders op nationaal en internationaal niveau. Buitenom de overheid worden tegelijkertijd stappen gezet vanuit het bedrijfsleven en het maatschappelijk middenveld. Door het updaten van wettelijke kaders worden ook andere processen – bij zowel bedrijven, brancheverenigingen, maatschappelijke organisaties en overheidsinstanties – in gang gezet. Bedrijven investeren in beleid en gebruikersvoorwaarden en creëren technische hulpmiddelen voor gebruikers en ouders. Daarnaast steunen hulp- en belangenorganisaties gebruikers en hebben zij een belangrijke signaleringsfunctie om problemen aan de kaak te stellen en te komen tot alternatieven.

De maatregelen die getroffen kunnen worden om gebruikers van mobiele toestellen en apps beter te beschermen, moeten dus niet alleen gezocht worden in wet- en regelgeving. Gebruikers van mobiele toestellen en apps – en minderjarigen in het bijzonder – worden in ruime mate beschermd door vigerende en opkomende wet- en regelgeving. Echter, het vereist een integrale aanpak en samenwerking om incidenten te voorkomen en adequaat te reageren op problemen. Mitigerende acties kunnen van technische, organisatorische en maatschappelijke aard zijn. Overheden, bedrijven, het maatschappelijk middenveld en gebruikers zelf kunnen bijdragen aan verbeteren van de huidige situatie omtrent cyberveiligheid bij mobiele toestellen en apps. Daarbij moet gedacht worden aan het expliciteren van normen (al dan niet via wetgeving en gedragscodes), certificering van producten en diensten (minimum eisen, richtlijnen), standaardisatie (protocollen, afstemming in complexe ketens) en het vergroten van de digitale geletterdheid van zowel burgers (gebruikers) als de overheid zelf.

Op basis van de desk research en de interviews met diverse stakeholders, is de onderstaande top vijf van aandachtspunten en aanbevelingen geformuleerd:

1 Uitvoerbaarheid van wettelijke eisen

Een belangrijk criterium voor een wet is dat deze uitvoerbaar moet zijn voor diegene voor wie de wet geldt. Ketenverantwoordelijkheden en de praktische vertaling van wettelijke vereisten, vormen knelpunten in de praktijk.

- Om wettelijke eisen in de praktijk te brengen, zijn *organisatorische* stappen nodig. Er is bijvoorbeeld een vertaalslag nodig van wettelijk opgelegde verantwoordelijkheden naar taakomschrijvingen binnen de organisatie van app-ontwikkelaars en andere betrokken partijen. Of bijvoorbeeld bij contractuele afspraken tussen verschillende ontwikkelaars, producenten, leveranciers en afnemers.
- Om wettelijke eisen in de praktijk te brengen, moeten ook *technische* uitdagingen het hoofd worden geboden. Zeker wanneer wetgeving steeds meer techniek-neutraal wordt opgesteld is de vertaalslag naar de meest effectieve technische oplossing niet eenvoudig. Ontwikkelaars, overheden en maatschappelijke organisaties moeten gezamenlijk kijken naar technische mogelijkheden om verbeteringen te faciliteren.
- Om wettelijke eisen in de praktijk te brengen, moeten *sociale en culturele* aspecten worden meegewogen. Het kan bijvoorbeeld nuttig zijn om te onderzoeken hoe het staat met de bereidheid van ouders en leerkrachten op scholen om erop toe te zien dat minderjarigen geen gebruik maken van specifieke apps die niet geschikt zijn voor minderjarigen.

Het is aan te raden om het bedrijfsleven en toezichthouders te betrekken bij het ontwikkelen van wet- en regelgeving. Dit levert in een vroeg stadium de juiste inzichten rondom de effectiviteit en haalbaarheid van wetgevingsdoelen. Daarnaast is impactonderzoek van belang om tegenstrijdigheden in een wet en de uitwerking van deze wet op verschillende groepen tijdig te identificeren. Uit zowel deskresearch als diverse interviews bleek dat het 'A Europe fit for the Digital Age' positieve invloeden zal hebben, maar ook veel nieuwe uitdagingen zal creëren. Het lijkt erop dat sommige wetten gemaakt worden met een specifiek doel of doelgroep voor ogen. Echter ontstaat de mogelijkheid dat dezelfde wetten ook invloed hebben op andere partijen of onbedoelde (bij-)effecten zullen hebben die negatieve gevolgen voor de gebruiker opleveren.

2 Toegerust toezicht

Om van de huidige en opkomende wetgeving tot betere praktijken te komen, moeten toezichthouders, maar ook Openbaar Ministerie en politie, hun rol goed kunnen uitvoeren. **Door de toekomstige nieuwe wetgeving vanuit de EU wordt het takenpakket van de toezichthouders vergroot en gecompliceerder. De huidige toezichthoudende instanties en de overlap en relatie tussen taken en focusgebieden zullen verder veranderen. Dit zet druk op de capaciteit van toezichthouders, zowel budgettair als qua kennis en kunde**.

- Op het gebruik van mobiele toestellen en apps zijn vele verschillende wetten en daarmee vaak ook verschillende toezichthouders betrokken, ieder met hun eigen bevoegdheden en expertises. Om effectief te kunnen zijn is heldere en logische verdeling en samenwerking van belang.
- Gezien het feit dat elk bedrijf, elke organisatie en elk individu tegenwoordig een app op de markt kan brengen, waardoor er miljoenen apps in omloop zijn, is het niet haalbaar om al deze apps te controleren of actief te monitoren. Toezichthouders zullen daarom stevig moeten investeren in voorlichting over (zorg)plichten en moeten meedenken om tot werkbare vormen van certificering en keurmerken te komen om goed gedrag te stimuleren.
- Om de pakkans en/of kans op succesvolle handhaving te vergroten moeten er strategische keuzes gemaakt worden met betrekking tot rolopvatting en taken. Met name door beperkte toerusting (met betrekking tot capaciteit, budget en expertise) is het (jaarlijks) vaststellen van de juiste focusgebieden zeer van belang.

Toezichthouders zoals de AP, ACM en het AT spelen een belangrijke rol bij het maken van de vertaalslag van open normen uit wettelijke kaders naar concretere uitgangspunten en plichten. Om dit nog beter te doen moeten onderzoeksagenda's worden bijgesteld en op elkaar worden afgestemd. **Behalve boetes uitdelen en klachten afhandelen, zou met name geïnvesteerd moeten worden in manieren om nieuwe ontwikkelingen en problemen tijdig te signaleren** en de markt en samenleving te faciliteren doormiddel van juiste informatie en praktische uitleg.

3 Bewustwording is niet genoeg

Gebruikers hebben digitale vaardigheden nodig om zichzelf voldoende te beschermen tegen risico's. Overheden en maatschappelijke organisaties kunnen helpen, maar beleid en acties die louter gericht zijn op "bewustwording" zorgen niet voor het gewenste effect.

- Er zal meer aandacht moeten worden besteed aan cyberveiligheid, illegale praktijken en de nieuwste aanvalsmethoden van criminelen. Hierbij moet de focus liggen op een leven lang leren via praktische tips en oefeningen zodat gebruikers zich toegerust voelen om zichzelf te wapenen tegen risico's.
- Het visualiseren van en waarschuwen voor risico's middels consumentenwijzers, classificaties en icoontjes, gepaard gaande met consistente voorlichting vanuit de overheid en maatschappelijke organisaties, kunnen ouders en docenten helpen bij het voeren van het gesprek over de geschiktheid van apps voor minderjarigen. Dit zal technisch en economisch goed doordacht moeten gebeuren om een herhaling van de cookiewet te voorkomen.
- De overheid zal moeten investeren in de digitale geletterdheid van de maatschappij in het algemeen, met speciale aandacht voor kwetsbare groepen zoals minderjarigen. Het integreren van digitale vaardigheden in onderwijscurricula in het basis- en voortgezet onderwijs draagt hieraan bij. Ook zal er gekeken moeten worden naar manieren om juist ouderen of mensen met een beperking te bereiken en te voorzien in hun behoefte om kennis en kunde te verbeteren.

Verlies daarbij het individu niet uit het oog. Gebruikers gedragen zich soms bewust of onbewust onveilig. Toch is het inmiddels wel duidelijk dat het niet alleen gaat om bewustwording of kennis en dat er voor de overdracht hiervan niet voor een 'one size fits all' oplossing moet worden gekozen. **Het is daarom aan te raden om te investeren in praktijkgericht gedragsonderzoek met aandacht voor persoonlijke motivatie, gelegenheid en culturele aspecten. Met name om jongeren effectief te bereiken dient de kennisoverdracht aan te sluiten bij de behoeftes en belevingswereld van die groep.**

4 Aandacht voor de signaleringsfunctie

Dit rapport biedt geen uitputtend overzicht van incidenten en risico's. De digitale omgeving is continu in ontwikkeling en het is dus van belang om te kunnen anticiperen op technologische en maatschappelijke veranderingen die hierdoor ontstaan.

- De signaleringsfunctie van maatschappelijke organisaties, hulpverleners, wetenschappers en de journalistiek vormen de eerste lijn wanneer het gaat om het observeren van belangrijke veranderingen en effecten op gebruikers.
- Het is van belang om continue de vinger aan de pols te houden en met enige regelmaat een situatieschets te maken van de stand van de technologie en risico's voor gebruikers. Op die manier kunnen beleidsmaatregelen en hulpverlening worden ingesteld en nieuwe problemen mogelijk beter in een vroeg stadium inperken.

Stimuleer en ondersteun maatschappelijke organisaties om het gefragmenteerde en reactieve karakter van huidige debatten en beleidsvorming te transformeren. Het is aan te raden om instanties met een signaleringsfunctie verder te professionaliseren met (financiële) steun van de overheid. Het is daarnaast ook zaak deze instanties serieus te nemen wanneer zij een dreigende ontwikkeling constateren en met regelmaat uit te nodigen voor updates en input.

"Het visualiseren van en waarschuwen voor risico's middels consumentenwijzers, classificaties en icoontjes [...] kunnen ouders en docenten helpen bij het voeren van het gesprek over de geschiktheid van apps voor minderjarigen"

5 Standaardisering en voorzorgsmaatregelen

Tot slot zijn er ook effectieve voorzorgsmaatregelen en 'best practices' die voor de nodige standaardisatie kunnen zorgen. Dit kan zowel binnen industrieën zelf plaatsvinden, als ook worden gestimuleerd door de overheid.

- De ontwikkelaars hebben een verantwoordelijkheid om technische vraagstukken te tackelen, maar ook om goede risicoanalyses te maken en impact assessments uit te voeren van producten die zij ontwikkelen en aanbieden. Een integrale aanpak is nodig om ethische reflecties te implementeren in hun organisatie en ontwikkelprocessen.
- Dominante spelers in het ecosysteem, zoals de appwinkels en populaire apps, hebben een verantwoordelijkheid om zichzelf en elkaar te controleren op kwaliteitseisen op het gebied van privacy, cyberveiligheid en andere ethische normen en waarden. Zij zouden zich meer kunnen verenigen en openlijk uitspreken tegen nalatigheid van andere spelers.
- De overheid kan als gebruiker van mobiele toestellen en diverse apps ook een voorbeeld stellen. Door kritisch te kijken naar wat zij aan software en hardware inkoopt, kan zij een programma van eisen formuleren die aanzetten tot standaardisering en afspraken in ketens.

App ontwikkelaars, producenten van mobiele toestellen, brancheverenigingen, belangenorganisaties en onafhankelijke experts/ wetenschappers moeten om tafel met de overheid om uitdagingen te identificeren en complexe vraagstukken te vertalen in beleid. Het is aan te raden om in te zetten op tri-sector (publiek, privaat, maatschappelijk middenveld) samenwerking op nationaal en in Europees verband om tot certificering en standaardisering te komen.

Literatuur- en bronnenlijst

Artikelen en boeken

Bits of Freedom 2022
Bits of Freedom, *Position Paper Bits of Freedom t.b.v. rondetafelgesprek inzake de rol van social mediaplatformen*, Tweede Kamer, 10 februari 2022**.**

Boxiner et. al. *CheckPoint Research* 2019
A. Boxiner, E. Vaknin, A. Volodin, D. Barda, en R. Zaikin, 'Tik or Tok? Is TikTok secure enough?' *CheckPoint Research* december 2019.

Brabazon 2012
T. Brabazon, *Digital Dialogues and Community 2.0. After Avatars, Trolls and Puppets*, Oxford: Woodhead Publishing Limited 2012.

Buitenweg 2021
K. Buitenweg, *Datamacht en tegenkracht. Hoe we de macht over onze gegevens kunnen terugkrijgen*, Amsterdam: De Bezige Bij 2021.

Cecere, *Telecommunications Policy* 2014
G. Cecere, N. Corrocher en R.D. Battaglia, 'Innovation and competition in the smartphone industry: Is there a dominant design?', *Telecommunications Policy* 2014, vol. 39/3-4, p. 162-175.

Cecere et. al, *Conference of IAOS* 2018
G. Cecere, F. Le Guel en V. Lefrere, 'Economics of free mobile applications: Personal data as a monetization strategy', *Conference of IAOS* 2018.

Chauhan en Kumar Panda 2015
S. Chauhan en N. Kumar Panda, *Hacking Web Intelligence. Open Source Intelligence and Web Reconnaissance Concepts and Techniques*, Waltham: Elsevier 2015.

***Children and the GDPR* 2018**
Children and the GDPR, Information Commissioner's Office 2018.

Commissariaat voor de Media, 2022
Commissariaat voor de Media, *Position Paper Commissariaat voor de Media t.b.v. rondetafelgesprek inzake de rol van social mediaplatformen*, Tweede Kamer, 10 februari 2022.

Cormen et. al. 2009
T.H. Cormen, C.E. Leiserson, R.L. Rivest en C. Stein, *Introduction to algorithms. The third edition*, Massachusetts: The MIT Press 2009.

Crawford, *The Atlas of AI* 2021
K. Crawford, *The Atlas of AI*, Yale: Yale University Press 2021.

Evgenia en Maria, *Journal of Information Technology Management* 2016
F. Evgenia en M. Maria, 'Exploring the profile of smartphone users and determining the factors affecting the smart intense use (SMI) through the technology acceptance model: a Greek case study', *Journal of Information Technology Management* 2016, vol. XXVII/3, p. 121-137.

Fogg, 2002
B.J. Fogg, *Persuasive Technology: Using Computers to Change What We Think and Do*, Burlington: Morgan Kaufmann 2002.

Friedman et al. 2013
B. Friedman, P.H. Kahn Jr., A. Borning, A. Huldtgren, 'Value Sensitive Design and Information Systems', In: *Early engagement and new technologies: Opening up de laboratory. Philosophy of Engineering and Technology*, vol 16. Springer, 2013, p. 55 – 95.

Kadëna, *Conference Budapest* 2017
E. Kadëna, 'Smartphone Security Threats', *Management, Enterprise and Benchmarking in the 21st Century*, Budapest: 2017, p. 141-155.

Kadëna en Ruiz, *Conference Budapest* 2017
E. Kadëna en L. Ruiz, 'Adoption of biometrics on mobile devices', *Symposium for Young Researchers: Proceedings*, Budapest, 2017, p. 140-148

Kang et. al. 2013
R. Kang, S. Brown en S. Kiesler, 'Why Do People Seek Anonymity on the Internet? Informing Policy and Design', *Human Computer Interaction Institute: Department of Psychology* 2013, p. 1-10.

Leukfeldt et. al. 2021
R. Leukfeldt et. al., 'Nederlands Cyber Security Lab Labsessie #2. "Beyond awareness: Maar hoe!?"', *Cyberveilig Nederland 2021.*

Malavolta, *Association for Computing Machinery* 2016
I. Malavolta, 'Beyond native apps: web technologies to the rescue! (keynote)', *Association for Computing Machinery* 2016, p. 1-2.

Nieuwesteeg et. al. 2021
B. Nieuwesteeg et. al., 'Nationaal Cyber Security Lab Labsessie #1. "Op naar een zorgplichtstandaard voor cybersecurity", *Cyberveilig Nederland 2021.*

Obaidat et. al. 2019
M.S. Obaidat, I. Traore en I. Woungang, *Biometric-Based Physical and Cybersecurity Systems*, Switzerland: Springer 2019.

Orben et. al. 2019
A. Orben, T. Dienlin en A.K. Przybylski, 'Social media's enduring effect on adolescent life satisfaction', *PNAS* 2019, vol. 116/21.

Orben et. al. 2022
A. Orben, A.K. Przybylski, S.J. Blakemore en R.A. Kievit, 'Windows of developmental sensitivity to social media', *Nature Communications* 2022.

Rathenau Instituut 2022
Rathenau Instituut, *Position Paper Rathenau Instituut t.b.v. rondetafelgesprek inzake de rol van social mediaplatformen*, Tweede Kamer, 10 februari 2022.

Thaler en Sunstein, 2009
R.H. Thaler en C.R. Sunstein, *Nudge. Improving decisions abouth health, wealth and happiness*, New York: Penguin Putnam Inc 2009.

Whittaker et. al., *Internet Policy Review* 2021
J. Whittaker, S. Looney en F. Votta, 'Recommender systems and the amplification of extremist content', *Internet Policy Review* vol. 10/2, p. 2-29.

Wouters en Paterson *Pursuit* 2021
N. Wouters en J. Paterson, 'TikTok captures your face', *Pursuit Engineering & Technology* 26 juli 2021.

Jurisprudentie en parlementaire stukken

Kamerstukken II 2020/21, 30821, nr. 148

Kamerstukken II 2021/22, 26643, nr. 843.

Rechtbank Gelderland 15 december 2021, ECLI:NL:RBGEL:2021:6632.

Rapporten & onderzoeken

***Advies opslag medische data in de cloud* 2019**
Advies opslag medische data in de cloud, ICTRecht 27 september 2019.

Assessment List for Trustworthy AI (ALTAI), 2020
Assessment List for Trustworthy AI (ALTAI), Independent High-Level Expert Group on Artificial Intelligence set up by de European Commission, 2020.

***Bijlage. Overzicht wet- en regelgeving cybersecurity* 2021**
Bijlage. Overzicht wet- en regelgeving cybersecurity, Rijksoverheid 2021.

***Building a Trusted Ecosystem for Millions of Apps* (Apple) 2021.**
Building a Trusted Ecosystem for Millions of Apps (rapport van Apple over App Store bescherming), Apple 2021.

***Cyberweerbaarheid met nieuwe technologie* 2020**
Cyberweerbaarheid met nieuwe technologie (rapport over kans en noodzaak van cyberweerbaarheid binnen en door digitale innovatie), Rathenau Instituut 2020.

***De toekomst van online platformen* 2021**
De toekomst van online platformen. Twee Europese wetsvoorstellen onder de loep, Rathenau Instituut 2021.

***Digital Economy Outlook* 2020**
Digital Economy Outlook, Organisation for Economic Co-operation and Development 2020.

***Digital 2021: The Netherlands* 2021**
Hootsuite, *Digital 2021: The Netherlands* (rapport over het gebruik van digitale diensten in Nederland) datareportal.com 2021.

***European Class Action Report* 2021**
European Class Action Report, CMS 2021.

***Ethics guidelines for trustworthy AI* 2019**
Ethics guidelines for trustworthy AI, European Commission 2019.

***Factsheet beeldschermgebruik van dichtbij* 2019**
Factsheet beeldschermgebruik van dichtbij (een factsheet over de effecten van beeldschermgebruik voor minderjarigen), AJN Jeugdartsen 2019.

***Factsheet Bescherming Persoonsgegevens* 2021**
Factsheet Bescherming Persoonsgegevens (een factsheet over de (on)mogelijkheden van bescherming van persoonsgegevens onder de AVG), TNO 2021.

***Filterbubbels in Nederland* 2019**
Filterbubbels in Nederland, Commissariaat voor de Media 2019.

***Het technologisch ecosysteem van AI in Nederland* 2019**
Het technologisch ecosysteem van AI in Nederland (een working paper waarin het technologisch ecosysteem van AI in Nederland onder de loep wordt genomen), WRR, 2021

***Gijsbers et. al.* 2019**
G. Gijsbers, B. Bakker, T. van Bree en A. Geurts, *Strategic Innovation Assets voor Nederland* (een hulpmiddel bij het analyseren van assets in het Nederlandse innovatiesysteem), TNO 2019.

***Iene Miene Media* 2021**
Iene Miene Media (rapport over het mediagebruik van kinderen van 0-6 jaar), Netwerk Mediawijsheid 2021.

Jaarrapport Landelijke Jeugdmonitor, 2019
Jaarrapport Landelijke Jeugdmonitor (rapport over trends en ontwikkeling onder jeugd in Nederland), Ministerie van Volksgezondheid, Welzijn en Sport, 2019.

***Leergebied Digitale Geletterdheid*, 2019**
Leergebied Digitale Geletterdheid, curriculum.nu, 2019.

***Leidraad Bescherming van de online consument* 2020**
Leidraad Bescherming van de online consument. Grenzen aan online beïnvloeding, ACM 2020.

***Mensenrechten in het robottijdperk* 2017**
Mensenrechten in het robottijdperk (rapport over de uitdagingen door het gebruik van robots, AI, virtual & augmented reality), Rathenau Instituut 2017.

***Monitor Mediagebruik* 2021**
Monitor Mediagebruik (rapport over het mediagebruik van kinderen van 7-12 jaar), Netwerk Mediawijsheid 2021.

***OECD Digital Economy Outlook* 2020**
OECD Digital Economy Outlook, OECD Publishing, Parijs 2020.

Van Huijstee et. al. 2021
M. van Huijstee, W. Nieuwenhuizen, M. Sanders, E. Masson en P. van Boheemen, *Online ontspoord – Een verkenning van schadeling en immoreel gedrag op het internet in Nederland*, Rathenau Instituut 2021.

Prins et. al. 2021
J.E.J. Prins, H. Sheikh, E.L. de Jong, M. Steijns en M.A.O. Bovens, *Opgave AI. Nieuwe systeemtechnologie* (advies aan de regering uit naam van de WRR), WRR 2021.

***Richtsnoeren 3/2018 over het territoriale toepassingsgebied van de AVG (artikel 3)* 2019**
Richtsnoeren 3/2018 over het territoriale toepassingsgebied van de AVG (artikel 3), European Data Protection Board 2019.

***Telecommonitor Q1*, 2020**
Telecommonitor Q1 (kwartaalrapportage van de ACM met de marktcijfers van de telecomsector), Autoriteit Consument en Markt, 2020.

***The Concept of Chilling Effect*, 2021**
The Concept of Chilling Effect. Its untapped potential to better protect democracy, the rule of law and fundamental rights in the EU, Open Society European Policy Institute, 2021.

***The Deloitte Consumer Review. Made-to-order: The rise of mass personalisation* 2015**
The Deloitte Consumer Review. Made-to-order: The rise of mass personalisation (rapport over personalisatie in marketing), Deloitte 2015.

***Tipsheet Mediagebruik* 2017**
Tipsheet Mediagebruik (een tipsheet voor ouders ten aanzien van de risico's van minderjarigen op het internet), Nederlands Jeugdinstituut 2017.

Vanzelf Mediawijs? 2016
Vanzelf Mediawijs? (rapport over de mediawijsheid van kinderen), Mediawijzer.net 2016.

***Vanzelf Mediawijs?* 2017**
Vanzelf Mediawijs? (een rapport over de mediawijsheid van kinderen), Mediawijzer.net 2017.

Verslag van een rondetafelgesprek, gehouden op 10 februari 2022, over de rol van socialmediaplatformen, 2022
Verslag van een rondetafelgesprek, gehouden op 10 februari 2022, over de rol van socialmediaplatformen, Tweede Kamer, 10 maart 2022.

***Vuistregels Online platformen* 2020.**
Vuistregels Online platformen. Supplement bij de Leidraad bescherming online consument. Grenzen aan Online Beïnvloeding, ACM 2020.

Online bronnen

'About Fact-Checking on Facebook', facebook.com.

'ACM Telecommonitor: aantal mobiele aansluitingen voor apparaten stijgt naar 8,8 miljoen', acm.nl 27 december 2021.

'ACM Telecommonitor eerste kwartaal 2022 met nieuw interactief dashboard', acm.nl

'Actie tegen TikTok', stichtingtakebackyourprivacy.nl.

'Agentschap Telecom lanceert Wbni-zelftest voor digitale dienstverleners', agentschaptelecom.nl, 1 juli 2022

'Android populairste besturingssysteem in Nederland', telecomnieuws.online 13 november 2019.

'Android Open Source Project', source.android.com.

'Android security: This malware will mine cryptocurrency until your smartphone fails', znet.com

'App developer motivation trends as of July 2013', statista.com 2013.

Apple Store Review Guidelines, developer.apple.com.

'Apple would be forced to allow sideloading and third-party app stores under new EU law', theverge.com, 25 maart 2022.

'Apple makes it easier to use parental controls and Screen Time with iOS 16', techcrunch.com, 6 juni 2022

'As Silicon Valley Faces Greater Scrutiny, the Public Increasingly Views Big Tech as Powerful and in Need of More Regulation', morningconsult.com 10 februari 2022.

Bevoegde autoriteiten', nctv.nl.

'Bits of Freedom', bitsoffreedom.nl.

B. Kontsevoi, 'Mobile App Monetization Part 4: Revenue Generation Models', forbes.com 30 juni 2020.

'Boete van 750.000 euro voor TikTok vanwege uitleg privacy in Engels', nos.nl 22 juli 2021.

'Can fines break Big Tech monopolies?', techmonitor.ai, 15 maart 2022.

'Catfishing: wat is het en hoe voorkom je het?', bnnvara.nl, 8 mei 2021.

'Cassatieberoep', rechtspraak.nl.

'Child sexual exploitation and grooming', education.vic.gov.au.

'Choosing a Category', developer.apple.com.

'Click to agree with what? No one reads terms of service, studies confirm', theguardian.com, 13 maart 2017.

'Commissariaat voor de Media start toezicht op video-uploaders', cvdm.nl, 17 mei 2022

'Content-based Filtering Advantages & Disadvantages', developers.google.com.

'CoronaCheck', coronacheck.nl.

'Customer Co-Creation is the Secret Sauce to Success', 10 juni 2016, forbes.com.

'Cyberpesten', pestenislaf.nl.

'Data Act: Commission proposes measures for a fair and innovative data economy', ec.europa.eu 23 februari 2022.

A. Priester, 'Data Privacy in Mobile Marketing: Contradictory or Complementary?', customlytics.com 8 oktober 2021.

'De Internethelden' bureaujeugdenmedia.nl, 2020.

'De kindertelefoon', kindertelefoon.nl.

'De scheiding der machten', prodemos.nl.

Developer Policy Center, play.google.com.

'DigiD Home', digid.nl.

'Digital Services Act: Commission welcomes political agreement on rules ensuring a safe and accountable online environment', ec.europa.eu 23 apriil 2022.

'Digital Youth. Publicaties', uu.nl.

'Digitale geletterdheid in het curriculum: na de zomer eindelijk aan de slag!', nldigital.nl, 24 mei 2022

'Discover the Maintenance mode', consumer.huawei.com.

'Een app gezien die niet deugt? Je kunt het bij Apple rapporteren', iculture.nl 10 juni 2021.

'Een categorie kiezen voor en tags toevoegen aan je app of game', support.google.com.

'Een goed curriculum', curriculumcommissie.nl.

'Een nummer rapporteren aan WhatsApp', fraudehelpdesk.nl.

'European Data Governance Act', digital-strategy.ec.europe.eu

'Europese Commissie wil vertrouwelijkheid op internet opheffen', bitsoffreedom.nl, 11 mei 2022

'Ethics Explainer: the Panopticon', ethics.org.

F. Laricchia, 'Tablet shipments market share by vendor worldwide from 2nd quarter 2011 to 4th quarter 2021', statista.com 7 februari 2022.

F. Lewis, 'What Is Crowdfunding?', thebalance.com bijgewerkt 31 december 2021.

'Facebook Community Standards', transparency.fb.com.

'Facebook onder vuur: de klokkenluider, de beschuldigingen en de betekenis', nos.nl 4 oktober 2021.

'Facial recognition: Italian SA fines Clearview AI 20 million', edpb.europa.eu 10 maart 2022.

'Fighting child sexual abuse: Commission proposes new rules to protect children', ec.europa.eu, 11 mei 2022

'Fire OS Overview', developer.amazon.com.

'Fusie T-Mobile en Tele2', t-mobile.nl.

'Gebruik van persoonsgegevens met als doel intimidatie wordt strafbaar', rijksoverheid.nl, 8 juli 2022

'Global Mobile Consumer Survey 2020: Dutch Edition', deloitte.com.

'Goed in gesprek over verkeerde informatie', netwerkmediawijsheid.nl.

'Google plans privacy change similar to Apple's, which wiped $230 billion off Facebook's market cap', cnbc.com 16 februari 2022.

G. van der Zwaag, ‘Een app gezien die niet deugt? Je kunt het bij Apple rapporteren’, iculture.nl 10 juni 2021.

‘Hardware security overview’, support.apple.com.

‘Hoe zit het met cybercrime?’, longreads.cbs.nl

‘Hoger beroep’, rechtspraak.nl.

‘How to set up parental controls on Google Play’, support.google.com.

‘Hulp na sextortion’, slachtofferhulp.nl.

‘ICO tells Washington Post it offers invalid cookie consent under GDPR’, iapp.org 20 november 2018.

‘In-App Messaging Explained’, airship.com.

‘Informatiepagina’s’, helpwanted.nl.

‘Instagram Community Guidelines FAQ’s’ about.instagram.com.

‘Introducing Birdwatch, a community-based approach to misinformation’, blog.twitter.com.

‘Introducting Smart Photos – For The Most Swipeworthy You’, tinderpressroom.com.

‘Is Social Media Content Moderation an Impossible Task?’, forbes.com, 8 september 2018.

‘Jeugd en Mediagebruik’, bibliotheeknetwerk.nl, bijgewerkt: 18 maart 2022.

‘Jonge kinderen zitten graag op TikTok. Maar hoe veilig is het daar?’, nrc.nl 27 januari 2020.

‘Keurmerk voor pentesten beschikbaar’, cyberveilignederland.nl.

‘Kies IRMA. Zet een digitaal paspoort op je eigen mobiel’, irma.app.

‘Kinderen moeten internetdiploma halen’, nos.nl 2 november 2015.

‘KopieID-app’, rijksoverheid.nl.

Krishnakumar, ‘5 Algorithms Every App Developer Should Know and Understand’, blog.eduopnix.com 10 augustus 2017.

‘Leeftijdsadvies van PEGI’, kijkwijzer.nl.

‘Legislative train schedule. Proposal for a regulation on privacy and electronic communications’, europarl.europa.eu.

‘LineageOS Android Distribution’, lineageos.org.

‘5 Methods For Increasing App Engagement & User Retention’, clearbdridgemobile.com.

M. Iqbal, ‘App Download Data (2022)’, businessofapps.com 20 april 2022.

‘Mobile App Monetization Strategies – Which Model to Choose to Make a Profit?’, asperbrothers.com 15 november 2021.

‘Morgan Stanley Pays $60M to Settle Data Breach LitigationCISOMAGon January 7, 2022 at 9:21 am Feedzy’, itsecurity.org januari 2022.

M. Kataria, ‘App Usage Statistics 2021 That’ll Surprise You (Updated)’, simsform.com 14 februari 2022.

‘Meta expands parental control for Instagram and VR’, cnet.com, 14 juni 2022

M. van Wageningen, ‘Social media cijfers 2021: wat je moet weten’, afix.nl 6 april 2021.

N. Chandler, ‘How secure is NFC tech?’ electronics.howstuffworks.com.

'NCSL labsessie #2: Beyond awareness: Maar hoe?' cyberveilignederland.nl.

'Nederlanders in Europese kopgroep digitale vaardigheden', cbs.nl 12 februari 2020.

'Nederland is koning smartphone, Samsung groter dan Apple', consultancy.nl 23 maart 2021.

'Nederlandse ouders dagen TikTok voor de rechter met een schadeclaim van 1,4 miljard', parool.nl 21 juli 2021.

'25% of Users Abandon Apps After One Use', uplandsoftware.com.

'Obama calls for tech regulation to combat disinformation on social media', cnbc.com 21 april 2022.

'Open State foundation', openstate.eu.

'Ouderlijk toezicht gebruiken op de iPhone, iPad of iPod touch van uw kind', support.apple.com.

'Ouderlijk toezicht instellen op Google Play', support.google.com.

'Over agentschap Telecom', agentschaptelecom.nl.

'Over Netwerk Mediawijsheid', netwerkemediawijsheid.nl.

'Over ons', acm.nl.

P. Franken, 'Wat is het verschil tussen informatiebeveiliging en cyber security?', rootsec.nl 22 juli 2021.

P. Kulche, 'Sociale media ongeschikt voor kinderen', consumentenbond.nl.

P. Kulche, 'Wat zijn cookies?', consumentenbond.nl 1 maart 2022.

P. McCarthy, 'NFC tag: a close look at near field communication technology', offgridweb.com 30 september 2021.

'Policy Paper. Online Safety Bill: factsheet', gov.uk, 19 april 2022.

'Post-Quantum Cryptography', csrc.nist.gov bijgewerkt 10 maart 2022.

'8 Proven App Revenue Models for Your Mobile App', mobileaction.co 28 november 2019.

'Puberhersenen', hersenstichting.nl.

P. Vogel, 'Man door 'dochter' opgelicht via WhatsApp: 'Je voelt je enorm bescheten'', ad.nl 11 april 2019.

'Richtlijn voor strafvordering cybercrime', om.nl.

'Richtlijn voor strafvordering cybercrime', wetten.overheid.nl.

'Samenvatting advies over Wet seksuele misdrijven', raadvanstate.nl, 13 juni 2022

'SMS-abonnement via frauduleuze Android-apps', consumentenbond.nl.

'Snapchat introduces first parental controls', nytimes.com, 9 augustus 2022

'Stop de illegale handel in TikTok profielen', massaschadeconsument.nl.

'Strategy Analytics: Global Smartwatch Shipments Leap 47 Percent to Pre-Pandemic Growth Levels in Q2 2021', news.strategyanalytics.com 27 augustus 2021.

'Swedish DPA: Police unlawfully used facial recognition app', edpb.europa.eu 12 februari 2021.

'Taken en bevoegdheden', autoriteitpersoonsgegevens.nl.

'Telefoon en tablet', laatjeniethackmaken.nl.

'Tem Big Tech: stop data in privékluizen', nrc.nl 28 juli 2020.

'The NIS2 Directive: A high common level of cybersecurity in the EU', europarl.europa.eu 1 december 2021.

T. de Kreij, 'Veel slachtoffers na TikTok-challenge: kindervuurwerk blijkt niet zo kindvriendelijk', nhnieuws.nl 6 januari 2022.

'The 2022 Code of Practice on Disinformation', digital-strategy.ec.europe.eu

'The Digital Markets Act: ensuring fair and open digital markets', ec.europa.eu.

'The EU's Digital Operational Resilience Act has been agreed: implications for the financial services sector', deloitte.com, 25 juli 2022

'The helpful Google Phones.', store.google.com.

'The mobile landscape in The Netherlands', deviceatlas.com 4 februari 2019.

'the new European Cyber Resilience Act', europarl.europa.eu

'The Power of Consumer Collaboration', 24 mei 2020, forbes.com.

'Thousands of amendments submitted for EU's AI Act', iapp.org, 3 juni 2022

'5G: The outsourced elephant in the room', berthub.eu 20 januari 2020.

E. Kreulen, 'The Voice: Trial by media?', trouw.nl 28 januari 2022.

'Tik Tok Community Standards', tiktok.com.

'Toezichthouders willen verbeteringen Data Act', autoriteitpersoonsgegevens.nl, 6 mei 2022

'Top Machine Learning Mobile Application Examples', theappsolutions.com.

'Transparency is the best policy', apple.com.

'Trump voorgoed van Twitter geweerd' 9 januari 2021, nos.nl.

'Types of legislation', european-union.europa.eu.

'Use parental controls on your child's iPhone, iPad, and iPod touch' support.apple.com.

'Versterking politie in wijken, op internet, voor opsporing en voor boa's', rijksoverheid.nl, 13 oktober 2021.

'Voor scholen: Lesmateriaal', mediawijsheid.nl.

'Waag futurelab', waag.org.

'Wat is fotoverificatie?', help.tinder.com.

'Welke provider heft het beste bereik?', unitedconsumers.com.

'Wetsvoorstel seksuele misdrijven', rijksoverheid.nl.

'What are the different types of mobile apps?', blog.duckma.com

'What are the key goals of the Digital Services Act', ec.europa.eu

'What exactly is LiFi?', lifi.co.

'Whistleblower says Bill must include tool that forces Facebook to publish data', independent.ie, 23 februari 2022.

'Why social media can't keep moderating content in the shadows', technologyreview.com, 6 november 2020.

'Wraakporno', rijksoverheid.nl.

‘YouTube introduces age verification for users’, agechecked.com.

‘Your Phone Should be Private’, calyxos.org.

‘113 zelfmoordpreventie’, 113.nl.

Bijlage 1: Begrippenlijst

Cyber	Hetgeen dat digitale informatie en systemen die verbonden zijn met het internet omvat
Software	Het geheel van computerprogramma's, vooral besturingsprogramma's en toepassingsprogramma's, waarmee computers bewerkingen en taken uitvoeren.
Firmware	Software die als onderdeel van hardware in een apparaat geprogrammeerd is en ervoor zorgt dat de hardware kan functioneren.
Drivers	Softwarebestanden die gebruikt worden voor het aansturen van computeronderdelen. De driver zorgt ervoor dat computer en randapparaten met elkaar kunnen communiceren.
Besturingssysteem	Basisprogramma van elke computer. Een besturingssysteem is voor een computer noodzakelijk om met softwarecomponenten te kunnen werken. Voorbeelden: Windows, Linux en Mac-OS X.
Post-kwantumcryptografie	Post-kwantumcryptografie is de wetenschap van versleutelingsmethoden die bedoeld zijn om zich te verdedigen tegen een kwantumcomputer.
Web 3.0	De opkomende derde generatie van het internet waarbij websites en apps op een intelligente manier kunnen verwerken. Hierbij zijn internettoepassingen onderling meer geïntegreerd. Web 3.0 wordt beschouwd van Web 2.0, en is zo de derde fase van de ontwikkeling van het internet.
Metaverse	Metaverse of metaversum is het gehele netwerk van aan elkaar gekoppelde virtuele 3D-ruimtes waarin de gebruikers, vaak door middel van avatars, interactief kunnen rondkijken en interageren.
NFT (non-fungible token)	Een non-fungible token is een koppeling (een soort eigendom) op een blockchain van een account aan een uniek (niet uitwisselbaar) digitaal item via een smart contract.
Profiling	Het proces van het creëren van een digitaal profiel op basis van verzamelde en geaggregeerde informatie over een gebruiker.
Microtargetting	Een manier van adverteren waarbij een zeer specifieke doelgroep wordt geselecteerd.

Algoritme	Een proces, stappenplan of een serie regels die een computer moet volgen om een probleem of rekensom op te lossen.
Sorteer-algoritme	Een sorteeralgoritme is een algoritme om elementen van een lijst in een bepaalde volgorde te zetten. https://nl.wikipedia.org/wiki/Sorteeralgoritme
Zoek-algoritme	Een zoekalgoritme is een algoritme dat in brongegevens zoekt naar bepaalde objecten. https://nl.wikipedia.org/wiki/Zoekalgoritme
Hashing-algoritme	Een methode om met een speciaal algoritme een unieke code te berekenen voor een bestand of een stuk tekst of andere informatie. Deze unieke code heet hash of hashwaarde en is een soort digitale vingerafdruk. SHA-2 en Bcrypt zijn veelgebruikte algoritmes. Men gebruikt bijvoorbeeld SHA-2 om te controleren of een bestand, tekst of informatie niet is aangepast.
Personalisatie	Een ontwikkeling binnen de digitale marketing waarbij de gebruikerservaring aangepast wordt op de interesses van de gebruiker.
Machine learning voor computervisie	Machinaal begeleide leeralgoritmen, ook wel te vangen onder de koepelterm Machine Learning, is een vorm van kunstmatige intelligentie die kan leren van de verwerkte data om beter te presteren. Deze vorm betreft specifiek het verwerken en leren van afbeeldingen.
Machine Learning	Een vorm van kunstmatige intelligentie die kan leren van de verwerkte data om beter te presteren.
Artificiële intelligentie	Technologie waarbij digitale systemen door middel van data, bijvoorbeeld afkomstig uit sensoren, zelfstandig acties kunnen ondernemen.
Op content-gebaseerde filters	Het proces van het screenen en uitsluiten van content die aan de gebruiker worden getoond.
Filterbubbels	Het proces waarbij content en zoekresultaten aangepast worden op basis van het eerdere zoekgedrag van de gebruiker. Hierbij kan de informatievoorziening aan de gebruiker beperkt raken tot hetgeen de gebruiker reeds interesseert. Zo kan er een spreekwoordelijke bubbel ontstaan om de gebruiker heen.
Neuraal netwerk (algoritme)	Een vorm van artificiële intelligentie waarbij gebruikt wordt gemaakt van processoren met een sterke onderlinge connectie. Deze connecties kunnen worden verzwakt, versterkt, aangemaakt of verbroken op basis van de trainingsdata en het doel van het algoritme. Hiermee bootst het algoritme als het ware het biologische neurale netwerk van ons brein na.
Dark patterns	Een gebruiksinterface die op een zodanige manier is ontworpen om gebruikers ertoe te sturen dingen te doen en keuzes te maken die ze zonder deze sturing wellicht niet hadden gemaakt.
Nudging	Een keuzearchitectuur en motivatietechniek die ten doel heeft het gedrag van de gebruiker te beïnvloeden om deze zo op de gewenste manier te laten gedragen.
Echokamers	Het principe dat een gebruiker zijn of haar ideeen bevestigd krijgt wanneer de gebruiker omringd wordt door

	mensen die op eenzelfde wijze denken of aan hetzelfde gedachtengoed onderhevig zijn.
Rabbit holes	Vaak gebruikt in de context van complottheorieën als metafoor voor het verzeilen in een werkelijkheid van alternatieve wereldbeelden.
Aanbevelingsengines	Het systeem dat online aanbevelingen doet aan de gebruiker en zodoende de gebruiker van een gepersonaliseerde online ervaring voorziet,
Persuasieve technologie	Onderzoeksgebied dat zich richt op de ontwikkeling van interactieve technologieën die bedoeld zijn om het gedrag van gebruikers te sturen.
Neuromarketing	Het gebruik van neurowetenschap om inzichten te verkrijgen in de reactie van het rbein op marketingstimuli.
Bot	Een computerprogramma dat zelfstandig taken kan uitvoeren. Bot is een afkorting van robot. Een bot kan onschuldig zijn, bijvoorbeeld als zoekmachines bots gebruiken om websites te vinden. Maar bots kunnen ook gebruikt worden om in te breken in een computer of om de computer klaar te maken zodat een ander kan inbreken. Een computer die besmet is met een bot, noemt men ook wel een zombie. De gebruiker van een computer merkt vaak niets van een bot.
Gatekeeping	Vaak gebruikt om te verwijzen naar een entiteit die informatiestromen controleert of beïnvloed en zo een bepalende rol speelt in de informatie die een gebruiker te zien krijgt.
Self-preferencing	Vaak gebruikt om te verwijzen naar het misbruik maken van een dominante positie, in de online context vaak een groot platform, waarbij de eigen producten en services gunstiger behandeld worden dan die van concurrenten.
Mining	Het proces waarbij transacties worden geverifieerd en toegevoegd aan de blockchain binnen een Proof of Work systeem.
Cryptovaluta	Digitale munteenheid. . De bekendste cryptovaluta is de Bitcoin.
Social engineering	Technieken die vaak gebruikt wordt door cybercriminelen. Hierbij wordt gebruik gemaakt van psychologische manipulatie om gebruikers te verleiden tot het delen van gegevens die gebruikt worden voor het inbreken van een digitaal systeem of het stelen van geld. Er wordt vaak misbruik gemaakt van de nieuwsgierigheid, hebberigheid of goedgelovigheid van de gebruiker. Een bekende vorm van social engineering is phishing.
Botnet	Een netwerk van computersystemen die zelfstandig kwaadaardige taken uitvoeren, zoals het versturen van spam of het uitvoeren van een DDoS-aanval. Een command-and-control server stuurt dit netwerk aan.
DDos aanval	Aanval waarbij men probeert om een computer, netwerk of dienstverlening uit te schakelen door het overweldigen van de infrastructuur met een overdosis aan internetverkeer.
Backdoor	Een manier om buiten de beveiligingssystemen om toegang te verkrijgen tot een computer of netwerk.
Zeroday	1. Afkorting voor zero day vulnerability. Een zwakke plek in software of hardware die nog niet bij de leverancier bekend is en dus ook nog niet is hersteld. Omdat de

	zwakke plek nog niet bekend is, kan niemand zich er goed tegen beschermen. De zwakke plek is pas een risico als er een exploit voor is gemaakt die de zwakke plek effectief weet te misbruiken. 2. Afkorting voor zero day exploit. Bij een zero day exploit is de zwakke plek die wordt misbruikt nog niet bekend bij de leverancier en kan zodanig nog niet hersteld worden. misbruikt niet bij de Een zero day exploit is heel waardevol voor aanvallers. Ontdekkers van zero days kunnen deze voor veel geld verkopen aan criminelen of inlichtingendiensten.
Phishing	Een vorm van internetfraude waarbij de gebruiker middels valse berichten verleid wordt om bijvoorbeeld inloggegevens of bank informatie te delen. . Phishing gebeurt vaak via e-mail of sms.
Panopticon-effect	Het panopticon-effect omvat het disciplinerende effect van zichtbare of onzichtbare surveillance maatregelen. Zolang een individu het idee heeft dat hij/zij wordt geobserveerd zal hij/zij daar ook naar handelen. Tegenwoordig wordt dit concept in relatie gebracht met het effect van dataverzameling en digitale surveillance.
Chilling effect	Omvat het process waarbij mensen monddood raken doordat zij zien dat anderen die zich uitspreken worden gestraft. Hierbij kan o.a. een onderdrukking van mensen en democratische rechten zoals vrijheid van meningsuiting ontstaan.
Impact assessment	Instrument waarmee de risico's van een bepaalde handeling in kaart worden gebracht.
Encryptie	Het versleutelen van informatie (zoals een tekstbestand of netwerkverkeer) voor anderen. Dit wordt gedaan met één of twee sleutels (symmetrische danwel asymmetrische versleuteling). De informatie wordt onleesbaar gemaakt door de zender waarna de ontvanger deze weer leesbaar maakt, met behulp van de sleutel(s). Men versleutelt informatie bijvoorbeeld om deze veilig te versturen of bijvoorbeeld om vast te stellen dat een bericht ook echt komt van degene die zegt dat hij het heeft verstuurd.
LAPSUS$	Groep van hackers die verantwoordelijk zijn voor cyberaanvallen tegen verscheidene grote tech-bedrijven.
Sideloading	Het installeren van software van een derde partij op een device buiten de officiële applicatie distributie methoden van de aanbieder om.
Multi-factor authenticatie	Een authenticatiemethode waarbij gebruikers online twee of meer stappen moeten doorlopen om in te loggen of ergens toegang toe te krijgen. Dit verbetert de cyberveiligheid vergeleken met single-factor authenticatie.
Catfishing	Catfishing is een misleidende online activiteit waarbij een persoon een nepprofiel aanmaakt om mensen onder een andere identiteit te benaderen. Dit wordt vaak gedaan in het kader van online dating.
Deepfake	Een soort synthetische media waarbij een bestaande persoon in een video of foto door middel van artificiële intelligentie gemanipuleerd wordt of een beeld van een artificiële persoon wordt gecreëerd. Met een deepfake kan je het doen lijken alsof iemand in een foto of video iets doet of zegt terwijl dit in de realiteit niet is gebeurd.
Grooming	Het proces waarbij een volwassene digitaal contact legt met een kind met de intentie om dat kind te ontmoeten om seksueel misbruik te plegen of pornografische afbeeldingen te produceren.

Cloud	Gesimplificeerd is de Cloud een manier van online gegevensopslag. De gegevens zijn daarbij niet opgeslagen op de device zelf, maar op een externe server van de Cloud aanbieder.
Doxing	Het online openbaren van identificerende informatie over een individu (zoals het woonadres, telefoonnummer of werkplek) zonder toestemming van het slachtoffer.

Bijlage 2: Respondenten

Tussen januari en maart 2022 interviewden het onderzoeksteam van Deloitte 30 experts. Het doel van deze interviews was om in kaart te brengen welke risico's konden worden geïdentificeerd vanuit ieders expertisegebied. Daarnaast gaven de interviews inzicht in perspectieven op de toereikendheid van wetgeving en maatregelen om de gebruiker te beschermen.

	Organisatie	**Naam geïnterviewde**
1	*The App Association*	Morgane Taylor Onderwerpexpert vanuit The App Association Onderwerpexpert vanuit The App Association
2	*VNO NCW*	Nicole Mallens Irvette Tempelman
3	*ECP*	Onderwerpexpert vanuit ECP Jelle Attema
4	*Cyberveilig Nederland*	Liesbeth Holterman Petra Oldengarm
5	*Meta*	Edo Haveman
6	*Apple*	Bart de Liefde Onderwerpexpert vanuit Apple Onderwerpexpert vanuit Apple
7	*The Developers Alliance*	Karina Stan Bruce Gustafson
8	*ACM*	Evert Jan Hummelen
9	*Consumentenbond*	Silvia Smit
10	*Google*	Arjan El Fassed Onderwerpexpert vanuit Google Onderwerpexpert vanuit Google
11	*AT*	Gürkan Kirca Jean-Paul Assche Ruud Kerssens
12	*TikTok*	Thierry Marchand Onderwerpexpert vanuit TikTok Onderwerpexpert vanuit TikTok
13	*Huawei*	Joepke van der Linden Jaap Meijer
14	*AP*	Onderwerpexpert vanuit AP Onderwerpexpert vanuit AP

Klankbordbijeenkomst

Op 12 april 2022 organiseerde het onderzoeksteam van Deloitte een klankbordbijeenkomst met de ministeries van Economische Zaken en Klimaat, Binnenlandse Zaken, Justitie en Veiligheid en een aantal toezichthouders (t.w. Autoriteit Persoonsgegevens, Commissariaat voor de Media, Autoriteit Consument en Markt en Agentschap Telecom) waarin de aanpak, de analyse en de voorlopige onderzoeksresultaten werden besproken en getoetst. Het doel van deze sessie was om deze onderdelen te verifiëren en om opkomende oplossingsrichtingen verder te concretiseren. De onderdelen die tijdens de discussie naar voren zijn gekomen, zijn verwerkt in het conceptrapport.

	Organisatie	**Naam geïnterviewde**
1	*Ministerie van Economische Zaken en Klimaat*	Roman Volf René van Eijk Nelly Ghaoui
2	*Ministerie van Binnenlandse Zaken*	Tony van der Togt
3	*Ministerie van Justitie en Veiligheid*	Michiel van Well
4	*Agentschap Telecom*	Ruud Kerssens Gürkan Kirca
5	*Autoriteit Persoonsgegevens*	K Wijnands
6	*Autoriteit Consument en Markt*	Evert Jan Hummelen
7	*Commissariaat voor de Media*	Gerda van Hekesen

Validatiebijeenkomst

Op 10 mei 2022 organiseerde het onderzoeksteam een validatiebijeenkomst met medewerkers van de ministeries van Economische Zaken en Klimaat, Binnenlandse Zaken, Justitie en Veiligheid en een aantal toezichthouders (t.w. Autoriteit Persoonsgegevens, Commissariaat voor de Media, Autoriteit Consument en Markt en Agentschap Telecom). Voorafgaand kregen de deelnemers op 3 mei 2022 het conceptrapport doorgestuurd. Tijdens de bijeenkomst hebben de verschillende genodigden de gelegenheid om op de onderzoeksresultaten te reageren. Het doel van de sessie was om gezamenlijk te reflecteren op het rapport en om tot prioritering te komen van onderzoeksresultaten die nadrukkelijker zouden moeten worden belicht. Aan de hand van deze feedback is het definitieve rapport opgeleverd aan EZK als opdrachtgever.

	Organisatie	**Naam geïnterviewde**
1	*Ministerie van Economische Zaken en Klimaat*	Roman Volf René van Eijk Nelly Ghaoui
2	*Ministerie van Binnenlandse Zaken*	Tony van der Togt
3	*Ministerie van Justitie en Veiligheid*	Christian Muller
4	*Agentschap Telecom*	Ruud Kerssens
5	*Autoriteit Persoonsgegevens*	Desmond de Haan (ook namens K Wijnands)
6	*Autoriteit Consument en Markt*	Evert Jan Hummelen
7	*Commissariaat voor de Media*	Gerda van Hekesen

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our global network of member firms and related entities in more than 150 countries and territories (collectively, the “Deloitte organization”) serves four out of five Fortune Global 500® companies. Learn how Deloitte’s approximately 330,000 people make an impact that matters at www.deloitte.com.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

© 2022. For information, contact Deloitte Global.