Bachelorscriptie
Informatica

Radboud Universiteit

Online verificatie van leeftijd en gezag

Auteur:
Arie-Jan Kruijsse
s1010823

Inhoudelijk begeleider:
Prof. dr. B.P.F. Jacobs
bart@cs.ru.nl

Tweede lezer:
Dr. H.K. Schraffenberger
H.Schraffenberger@ru.nl

June 26, 2020

Samenvatting

De digitale samenleving vraagt om een nieuwe manier om leeftijden en gezagsrelaties te kunnen verifiëren. Het wettelijke kader dat de digitale samenleving gedeeltelijk reguleert is te vinden in de vorm van de AVG. Voor producten als alcoholische drank en games met leeftijdsrestricties geldt dat minderjarigen deze niet mogen kopen. Ook zijn minderjarigen onder bepaalde leeftijdsgrenzen niet bevoegd om zelfstandig handelingen uit te voeren. Voorbeelden hiervan zijn het nemen van beslissingen in de medische sector en de registratie bij sociale media. Hiervoor hebben zij toestemming nodig van hun gezagsdrager(s). Er is een manier nodig om de leeftijd en gezagsverhoudingen te kunnen aantonen. In de realisatie van deze verificatie moet rekening gehouden worden met de aanvullende eisen van data-minimalisatie en betrouwbaarheid van de verificatie. Ook moet het systeem met betrekking tot het gebruik van de gezagsrelaties bestand zijn tegen misbruik van de gezagsrelaties.

In deze scriptie worden eerst de wettelijke eisen van de verificatie van leeftijd en gezagsrelaties onderzocht. Daarna worden problemen die spelen in de huidige leeftijds- en gezagsverificatie aan het licht gebracht. Tenslotte wordt een aanbeveling gemaakt voor hoe de problemen in de huidige manier van verificatie opgelost kunnen worden door middel van het identiteitsplatform IRMA.

Inhoud

1 Inleiding **3**
- 1.1 Gerelateerd werk . . . 4
- 1.2 Bijdrage van dit onderzoek . . . 5

2 Juridische achtergrond **7**
- 2.1 Algemene Verordening Gegevensbescherming . . . 7
- 2.2 Uitvoeringswet AVG . . . 8
- 2.3 Ouderlijk gezag en wettelijke vertegenwoordiging . . . 9
  - 2.3.1 Huwelijk of geregistreerd partnerschap . . . 9
  - 2.3.2 Kinderen geboren buiten een huwelijk of partnerschap 10
  - 2.3.3 Tienermoeders . . . 10
  - 2.3.4 Adoptie . . . 11
  - 2.3.5 Pleegkinderen . . . 11
- 2.4 Waar wordt de gezagsrelatie geregistreerd? . . . 11
- 2.5 Alcohol . . . 13
- 2.6 Games . . . 13
- 2.7 Medische sector . . . 14
  - 2.7.1 Patiëntenrechten . . . 14
  - 2.7.2 Inzage medisch dossier en het uitvoeren van medische handelingen . . . 15
- 2.8 Sociale media . . . 16

3 Verificatie in de praktijk **17**
- 3.1 Alcohol . . . 17
  - 3.1.1 Nationaal preventieakkoord . . . 17
  - 3.1.2 Aanpak van de fysieke alcoholverkoop . . . 18
  - 3.1.3 Aanpak van de online alcoholverkoop . . . 19
  - 3.1.4 Statistieken . . . 19
- 3.2 Games . . . 19
  - 3.2.1 Aanpak van de fysiek gameverkoop . . . 20
  - 3.2.2 Aanpak van de online gameverkoop . . . 21
- 3.3 Medische sector . . . 22
  - 3.3.1 Fysiek . . . 23

3.3.2 Digitaal . . . 24
3.3.3 Pilot Ouderlijk gezag in de zorg . . . 25
3.4 Sociale media . . . 26
3.4.1 WhatsApp . . . 27
3.4.2 Facebook . . . 27
3.4.3 YouTube . . . 27
3.4.4 Instagram . . . 28
3.4.5 Snapchat . . . 28
3.4.6 Tiktok . . . 28

4 Mogelijke oplossingen 30
4.1 Verbeterpunten . . . 30
4.1.1 Weinig toezicht op verificatie thuisbezorgkanalen . . . 30
4.1.2 Leeftijdsverificatie bij gameverkoop . . . 31
4.1.3 Onduidelijkheid in de medische zorg over gezagsrelaties 32
4.1.4 Leeftijd en gezagsrelaties worden niet geverifieerd door sociale media . . . 32
4.1.5 Leeftijdsverificatie door middel van de geboortedatum is niet privacy-vriendelijk . . . 34
4.2 Attribute-based credentials systemen . . . 34
4.3 IRMA . . . 36
4.3.1 De verschillende partijen van een ABC in de context van IRMA . . . 36
4.3.2 Eigenschappen van credentials in IRMA . . . 37
4.3.3 Hoe IRMA past in dit onderzoek . . . 38

5 Een protocol voor verificatie gebaseerd op IRMA 42
5.1 De registratie van het gezagscredential . . . 42
5.1.1 Het gezagscredential . . . 43
5.1.2 Meerdere gezagsrelaties per persoon . . . 45
5.2 Het gebruik van het gezagscredential in de medische sector . 46
5.2.1 Gebruik van het gezagscredential in de medische sector 46
5.2.2 Hoe het ziekenhuisportaal weet of de gegevens geldig zijn . . . 47
5.2.3 Hoe wordt omgegaan met de gegevens van de gezagsdragers? . . . 47
5.3 Gebruik van het gezagscredential bij registratie sociale media 48
5.4 Registratie van het gebruik van de gezagsattributen . . . 49
5.4.1 Kan een minderjarige de uitoefening van het gezag inzien? . . . 51

6 Conclusies 52

Hoofdstuk 1

Inleiding

De samenleving is sinds de eeuwwisseling steeds verder gedigitaliseerd. Hiermee verplaatst een steeds groter deel van ons leven zich naar het digitale domein. Zo is het bijvoorbeeld normaal dat we producten online kunnen bestellen. Ook in de medische sector komt er alsmaar meer de mogelijkheid om digitaal dossiers in te zien of afspraken met zorgverleners te plannen. En natuurlijk zijn er de vele populaire sociale media. Voor verschillende handelingen in de fysieke wereld zijn we gewend om een aantal persoonlijke gegevens te verstrekken om een dienst of product te verkrijgen. Hiervoor moet vaak het identiteitsbewijs getoond worden. Een voorbeeld waar een identiteitsbewijs getoond moet worden is bij de aankoop van alcohol om te controleren of de klant ouder is dan achttien jaar. Een ander voorbeeld is te vinden in de medische sector. Daar moet de identiteit van de patiënt vastgesteld worden om bijvoorbeeld het medisch dossier in te kunnen zien. In de medische sector komt het ook voor dat ouders voor hun minderjarige kinderen bepaalde handelingen moeten goedkeuren waarvoor de kinderen zelf niet bevoegd zijn. Hiervoor moet dan ook de gezagsrelatie tussen ouders en de minderjarigen worden geverifieerd. In de fysieke wereld, waar de zorgverlener persoonlijk contact heeft met de ouders en minderjarigen, vindt deze controle van de gezagsrelatie plaats op basis van de identiteitsbewijzen van ouder en minderjarige. In de digitale wereld is er echter nog geen dergelijk identiteitsbewijs wat hier geschikt voor is. Er moet goed nagedacht worden over die digitale identiteit, omdat het in de digitale wereld van groot belang is om zorgvuldig om te gaan met persoonlijke gegevens. Informatie die ooit online is weggegeven kan immers altijd opgeslagen worden zonder dat de gebruiker daarvan afweet. Door zo weinig mogelijk gegevens achter te laten in de digitale wereld kunnen de gevolgen voor de privacy tot een minimum beperkt worden. Dit is wat in deze scriptie geprobeerd zal worden.

Er moet dus een digitale manier zijn om bepaalde eigenschappen te kunnen aantonen, zonder daarbij overbodige gegevens weg te geven. In dit onder-

zoek gaat het specifiek om het aantonen van een bepaalde leeftijd, voor de aankoop van alcoholische drank en games, om handelingen uit te kunnen voeren in de medische wereld en te registreren bij sociale media. Dat middel moet, naast dat het geen overbodige gegevens mag weggeven, ook objectief zijn. Dit houdt bijvoorbeeld in het geval van leeftijdsverificatie in dat de verificatie niet afhankelijk mag zijn van de bewering van de gebruiker dat hij de vereiste leeftijd bereikt heeft. De controlerende partij moet dit kunnen controleren aan de hand van een gegeven wat de gebruiker niet ten gunste van zichzelf kan beïnvloeden.

Tevens moeten gezagsverhoudingen aangetoond kunnen worden in situaties waar een gezagdrager het gezag over een minderjarig kind wilt uitoefenen. Dit is het geval in de medische sector waar minderjarigen nog niet bevoegd zijn tot zelfstandige keuzes. Ook voor registratie bij sociale media is er onder een bepaalde leeftijd toestemming van de gezagsdrager van de minderjarige nodig. Het ligt echter niet voor de hand wie de gezagsdrager is van een minderjarige. In veel gevallen in Nederland zijn de biologische ouders de gezagsdragers. Door tussenkomt van een rechter kan hier echter verandering in komen. Een rechter kan het gezag overdragen aan een wettelijke vertegenwoordiger waardoor de biologische ouders het gezag niet behouden. Er zijn ook situaties mogelijk waarbij maar een van de ouders het gezag draagt. Tevens kan een minderjarige opgenomen worden in de pleegzorg. Het is dus niet vanzelfsprekend dat de biologische ouders de gezagsdragers zijn. Het is derhalve noodzakelijk om alle gezagsrelaties inzichtelijk te krijgen. Zodra dat gerealiseerd is, kunnen de gezagsrelaties vervolgens gebruikt worden om de wettelijke gezagsdragers het gezag te laten uitvoeren.

1.1 Gerelateerd werk

Naar het vertonen van enkel de benodigde eigenschap voor verificatie is al onderzoek gedaan. Toonaangevend in dit gebied zijn de *attribute based credentials* (ABC) systemen[17]. Dit onderzoek zal gebruik maken van het identiteitsplatform IRMA,[1] dat een implementatie is van een ABC systeem. Hoofdstuk 4 zal ingaan op de mogelijkheden die IRMA te bieden heeft voor de genoemde verificatieproblemen.

Online leeftijdsverificatie is tegenwoordig vaak volledig afhankelijk van de input van de gebruiker; de gebruiker geeft een leeftijd of geboortedatum op, waarna de controlerende partij geen mogelijkheid heeft om de juistheid van die input te beoordelen. Vanwege die onmacht van de controlerende partij kunnen gebruikers eenvoudig de leeftijdsgrens ontduiken door foutieve informatie te verstrekken. ABC's bieden hiervoor een oplossing door middel van attributen die verkregen zijn van betrouwbare uitgevers. Zulke controles

[1] `https://privacybydesign.foundation/irma/` en `https://irma.app/docs/what-is-irma/`

kunnen in de praktijk al geïmplementeerd worden omdat de techniek al beschikbaar is, een voorbeeld hiervan zal behandeld worden in sectie 4.3.3. Er is echter nog maar weinig aansporing om dit daadwerkelijk in te zetten.

Verificatie van gezag is nog niet mogelijk. In IRMA is een subset van alle gezagsrelaties beschikbaar via de Basisregistratie Personen (BRP) maar vanwege de verschillende locaties waar de gezagsrelatie wordt opgeslagen heeft IRMA geen toegang tot een totaalbeeld van alle gezagsrelaties. Hier zal in deze scriptie verdere aandacht aan worden besteed.

1.2 Bijdrage van dit onderzoek

Dit onderzoek zal trachten te verkennen in hoeverre IRMA gebruikt kan worden voor leeftijds- en gezagsverificatie. Hiervoor zullen zowel situaties in de fysieke wereld worden onderzocht als situaties in de digitale wereld.

Er zal onderzocht worden wanneer kinderen onder gezag staan en vanaf wanneer zij zelfstandig keuzes mogen en kunnen maken. Alleen het gezag over minderjarige kinderen zal in deze scriptie onderzocht worden. Het is ook mogelijk dat meerderjarigen onder een vorm van gezag geplaatst worden. We spreken dan over curatele, bewind of mentorschap[20]. Een meerderjarige kan hieronder gesteld als blijkt dat hij niet bekwaam is om zelf verantwoordelijkheid te dragen. Omdat dit verschilt van het gezag over minderjarige kinderen zal hier enkel het gezag over minderjarigen behandeld worden. Om alle gezagsrelaties in kaart te brengen moet duidelijk worden welke verschillende gezagsrelaties er zijn en waar deze relaties worden bijgehouden. Ook zullen vier sectoren onderzocht worden waar de leeftijds- en gezagsverificatie wettelijk vereist is. In die sectoren zullen een aantal verificatieproblemen in de huidige praktijk belicht worden. De mogelijkheid om deze verificatieproblemen op te lossen met IRMA zal onderzocht worden. De oplossing moet voldoen aan de wettelijke norm die in het eerste hoofdstuk zal worden behandeld. Ook moeten de aanvullende eisen van dataminimalisatie, objectiviteit en het bestand zijn tegen misbruik van de gezagsrelatie gerealiseerd worden.

In hoofdstuk 2 zullen de wettelijke kaders rondom leeftijdsgrenzen en gezag onderzocht worden. Daar zal duidelijk gemaakt worden wanneer leeftijdsverificatie vereist is en welke leeftijdsgrenzen er in die situaties gelden. Ook zullen de verschillende gezagsrelaties uitgewerkt worden. Uiteindelijk wordt in dat hoofdstuk de wetgeving behandeld in de vier sectoren die onderzocht worden: het kopen van alcoholische drank, het kopen van games, toestemming geven voor handelingen in de medische sector waaronder inzage in het medisch dossier en tenslotte de leeftijdsverificatie die nodig is voor het gebruik van sociale media. In hoofdstuk 3 wordt vervolgens in deze vier sectoren onderzocht hoe de wetten in de praktijk uitgevoerd worden. Daarna volgt in het vierde hoofdstuk een analyse van de hoofdstukken

2 en 3, waaruit een aantal verbeterpunten aan bod komen om de praktijk beter aan te laten sluiten bij de wetgeving. Tevens bevat dat hoofdstuk een oplossing waarmee de verbeterpunten kunnen worden opgelost. Hier zal het eerder genoemde concept de ABC systemen uitgelegd worden, met de mogelijkheden die deze systemen te bieden hebben voor het verificatieprobleem. Het laatste hoofdstuk zal er op ingaan hoe het proces van leeftijds- en gezagsverificatie eruit moet zien in IRMA. In dat hoofdstuk zullen de verschillende keuzemomenten in de stappen van het proces overwogen worden. Gebaseerd daarop wordt een voorstel gedaan voor een implementatie van het gezagsattribuut in IRMA. Tenslotte wordt het onderzoek afgesloten met een conclusie en aanbevelingen voor vervolgonderzoek.

Hoofdstuk 2

Juridische achtergrond

In dit hoofdstuk wordt het wettelijke kader rondom leeftijdsverificatie behandeld. Eerst zal onderzocht worden wat de Algemene Verordening Gegevensbescherming (AVG) zegt over het verwerken van gegevens van minderjarigen en wanneer iemand minderjarig is. Vervolgens gaat sectie 2.3 over wie de gezagsdragers van minderjarigen zijn; hiervoor moeten een aantal verschillende gezagssituaties behandeld worden. Daaropvolgend gaat sectie 2.4 over de plaats waar de gezagsrelatie geregistreerd wordt. Dit is nodig om te weten omdat de gezagsrelatie opgevraagd moet kunnen worden. Tenslotte worden de specifieke wetten en regels voor leeftijdsgrenzen onderzocht voor de alcohol- en gameverkoop, het inzien van medische dossier en toestemming geven voor medische handelingen en het gebruiken van sociale media.

2.1 Algemene Verordening Gegevensbescherming

Sinds mei 2018 is de omgang met persoonsgegevens in Nederland gereguleerd door de AVG, die in heel Europa geldt. De AVG legt de belangrijkste regels vast voor de omgang met persoonsgegevens.[1] Op sommige gebieden geeft de AVG de lidstaten echter de ruimte om zelf keuzes in beleid te maken. Voor dit onderzoek is het van bijzonder belang dat de lidstaten zelf de minimumleeftijdsgrens voor toestemming voor verwerking van persoonsgegevens kunnen bepalen. Deze minimumleeftijd moet echter wel tussen de 13 en 16 jaar liggen. Dit geeft lidstaten de mogelijkheid om de AVG zodanig toe te passen dat het goed in de nationale wetgeving past. In Nederland zijn deze nationale keuzes in de Uitvoeringswet AVG (UAVG) vastgelegd. De UAVG zal in de volgende sectie behandeld worden. Kinderen zijn voor de AVG minderjarig totdat zij de leeftijd van 16 jaar bereikt hebben. Boven die leeftijd worden zij behandeld als volwassenen. De verwerking van persoonsgegevens is alleen rechtsgeldig wanneer aan minimaal een van de zes voorwaarden uit artikel 6.1 van de AVG is voldaan. Deze voorwaarden zijn

[1] `https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten;AVGlid8`

voor volwassenen en minderjarigen gelijk, met uitzondering van de eerste voorwaarde: het geven van toestemming voor de verwerking.[2] In artikel 8 wordt namelijk gesteld dat de toestemming van kinderen voor de verwerking van persoonsgegevens alleen rechtmatig is als het kind minstens 16 jaar oud is.[3] Als de betrokkene jonger is dan 16 jaar, dan is hij zelf nog niet gerechtigd om toestemming te geven en heeft hij voor verwerking van zijn gegevens de toestemming van zijn wettelijke vertegenwoordiger nodig. Een wettelijke vertegenwoordiger is iemand die het gezag en de verantwoordelijkheid draagt over een minderjarige; dit zijn echter niet vanzelfsprekend de biologische ouders. Dit wordt in sectie 2.3 nader toegelicht. Tenslotte moet de partij die de verantwoordelijkheid draagt voor de verwerking van de gegevens controleren of de gekregen toestemming voor verwerking van de daadwerkelijke vertegenwoordiger(s) van de minderjarige afkomstig is.[4] Het is dus van belang dat de relatie tussen de minderjarige en zijn gezagsdrager bewezen kan worden omdat alleen de wettelijke gezagsdrager van de minderjarige toestemming kan en mag geven.

2.2 Uitvoeringswet AVG

Lidstaten kunnen de AVG op kleine punten wijzigen om deze in hun nationale wetgeving in te passen. Deze wijzigingen kunnen zij in een eigen uitvoeringswet vastleggen. Vanwege die mogelijke wijzigingen is het noodzakelijk om de Nederlandse uitvoeringswet hier ook te onderzoeken.

Op het gebied van leeftijdsgrenzen hanteert de UAVG dezelfde lijn voor het zelfstandig toestemming geven voor de verwerking van persoonsgegevens als in de AVG, namelijk de leeftijd van 16 jaar.[5] Er is toestemming van een wettelijke vertegenwoordiger voor de verwerking van de gegevens van de betrokkene nodig zolang de betrokkene nog niet zelfstandig toestemming mag geven. De wettelijke vertegenwoordiger kan op elk moment besluiten de toestemming in te trekken; daar heeft de minderjarige geen invloed over.[6] Net als in de AVG, is deze toestemming niet van toepassing op "hulp- en adviesdiensten die rechtstreeks en kosteloos aan een minderjarige ... worden aangeboden."[7] Hieruit kan geconcludeerd worden dat de UAVG op het gebied van de leeftijdsgrens voor het geven van toestemming voor verwerking van persoonsgegevens niet verschilt van de AVG.

[2] AVG 6.1a
[3] AVG 8.1
[4] AVG 8.2
[5] UAVG 5.1
[6] UAVG 5.3
[7] UAVG 5.5

2.3 Ouderlijk gezag en wettelijke vertegenwoordiging

Minderjarigen zijn zelf niet bevoegd om toestemming te geven tot verwerking van hun persoonsgegevens volgens artikel 6.1a en 8.1 van de AVG. Zoals hierboven al beschreven is, hebben jongeren onder de 16 jaar de toestemming nodig van hun wettelijke vertegenwoordiger voor de verwerking van hun gegevens.[8] Wie de wettelijke vertegenwoordiger van de minderjarige is, is afhankelijk van de gezagssituatie waarin de minderjarige verkeerd. Om voor elk geval de juiste wettelijke vertegenwoordiger aan te kunnen wijzen, is het daarom nodig dat de verschillende mogelijke gezagsverhoudingen hier uitgewerkt worden.

De wetgeving met betrekking tot gezag over minderjarige kinderen is vastgelegd in Burgerlijk Wetboek Boek 1 Titel 14. Deze wet zegt in zijn algemeenheid dat alle minderjarigen onder gezag staan en dat met gezag zowel ouderlijk gezag dan wel voogdij bedoeld is.[9] De persoon die het gezag draagt over een minderjarige wordt ook vaak aangeduid als gezagsdrager, wat tevens de term is die in deze scriptie gebruikt zal worden. Verder geldt dat minderjarigen zelf nog onbevoegd zijn tot het gezag over andere minderjarigen.[10] In de context van dit onderzoek is het belangrijk om te weten wie het gezag dragen over welke minderjarigen. Daarom worden onderstaande situaties uitgewerkt.

2.3.1 Huwelijk of geregistreerd partnerschap

Voor minderjarigen die geboren zijn bij ouders die gehuwd zijn, dan wel een geregistreerd partnerschap hebben, geldt dat zij onder het gezag van beide ouders staan.[11] Deze ouders oefenen samen het gezag over hun biologische kinderen uit zolang de ouders in het huwelijk of geregistreerd partnerschap verbonden zijn, of totdat het kind de leeftijd van 16 jaar bereikt heeft. Als het huwelijk of partnerschap ontbonden wordt, anders dan door de dood, blijven de ouders samen het gezag uitoefenen over de minderjarige.[12] Een uitzondering hierop is dat de rechter de beslissing kan nemen om het ouderlijk gezag van één van de ouders te ontnemen.[13] Dit gebeurt op verzoek van één of beide ouders en wordt door de rechter goedgekeurd als dit in het belang van de minderjarige is. In het geval dat het huwelijk of het partnerschap wordt ontbonden door de dood, krijgt de overlevende ouder het ouderlijk gezag over de minderjarigen voor zover hij of zij dat gezag al

[8] AVG 8.2
[9] BW 1:14 245
[10] BW 1:14 246
[11] BW 1:14 251.1; BW 1:14 253aa
[12] BW 1:14 251.2
[13] BW 1:14 251a.1

had.[14] Als de overlevende ouder geen gezag over de minderjarigen had op het tijdstip van overlijden bepaalt de rechter wie de voogd van de minderjarigen moet worden.[15] De rechter kan het besluit nemen om de overlevende ouder alsnog het gezag te laten uitoefenen, of om een derde als voogd over de minderjarigen aan te wijzen. Deze voogd kan van tevoren door de ouders worden aangewezen door middel van een aanvraag in het gezagsregister bij de rechtbank of door middel van de wens voor een zeker persoon als voogd vast te laten leggen in een testament bij de notaris.[16] Elke rechtbank houdt een openbaar gezagsregister bij waarin rechtsfeiten vermeld worden aangaande de gezagsuitoefening over minderjarigen.[17] Wat dit gezagsregister inhoudt wordt in sectie 2.4 van dit hoofdstuk nader behandeld. De persoon die wordt aangewezen als voogd heeft altijd nog het recht om het gezag niet over te nemen. In dat geval wijst de rechter een andere voogd aan.

2.3.2 Kinderen geboren buiten een huwelijk of partnerschap

Als een kind geboren is buiten een huwelijk of geregistreerd partnerschap heeft alleen de biologische moeder het ouderlijk gezag over die minderjarige.[18] Als de biologische ouders samen het gezag willen dragen, dan moeten zij beiden hiervoor een verzoek indienen in het gezagsregister.[19]

2.3.3 Tienermoeders

Zoals eerder genoemd kan een minderjarige geen gezag uitoefenen.[20] Als een minderjarige vrouw een kind krijgt, mag zij dus in feite niet het gezag dragen over dat kind. Wanneer de vrouw echter tenminste 16 jaar oud is en zij het gezag over haar kind wenst te dragen, is het mogelijk voor de moeder om een meerderjarigheidsverklaring aan te vragen bij de kinderrechter.[21] Zodra zij die verklaring heeft gekregen mag zij zelfstandig het gezag over het kind gaan dragen. Als deze verklaring niet gegeven is, en de moeder bereikt de leeftijd van 18 jaar, dan krijgt zij op dat moment alsnog het gezag over het kind. Zolang zij nog niet meerderjarig (verklaard) is, draagt een door de rechter aangestelde voogd het gezag over het kind.

[14] BW 1:14 253f
[15] BW 1:14 253g
[16] `https://www.rijksoverheid.nl/onderwerpen/ouderlijk-gezag/vraag-en-antwoord/hoe-krijg-ik-de-voogdij-over-een-kind`
[17] BW 1:14 244; Besluit gezagsregisters 1
[18] BW 1:14 253b
[19] BW 1:14 252
[20] BW 1:14 246
[21] BW 1:14 253ha.1

2.3.4 Adoptie

Door adoptie wordt er een familierechtelijke betrekking gecreëerd tussen de geadopteerde en de adoptieouder(s).[22] Zowel in een huwelijk of geregistreerd partnerschap als daarbuiten oefenen de adoptieouders gezamenlijk het gezag uit over het adoptiekind. Dit betekent dat de gezagsrelatie tussen ouders en hun adoptiekind hetzelfde is als de relatie tussen ouders en hun biologische kind. Geadopteerde kinderen worden ingeschreven in de Basisregistratie Personen, net zoals biologische kinderen. Van de adoptie, en daarbij ook de gezagsrelatie, wordt echter melding gemaakt in het gezagsregister.[23] In de Basisregistratie Personen wordt bij het adoptiekind echter niet de gezagsverhouding vastgelegd. Sectie 2.4 zal verder ingaan op hoe en waar de gezagsverhoudingen worden opgeslagen. Omdat de gezagsrelatie met betrekking tot adoptiekinderen gelijk is aan die met betrekking tot biologische kinderen, geldt ook hier dat het gezag vervalt zodra het adoptiekind meerderjarig wordt en bekwaam is om zelfstandig te zijn.

2.3.5 Pleegkinderen

Een minderjarige die geplaatst is in een pleeggezin staat niet vanzelfsprekend onder het wettelijke gezag van de pleegouders. De biologische ouders blijven het gezag dragen over hun kind. Voor beslissingen waarvoor toestemming van de gezagsdrager van de minderjarige nodig is, moeten de pleegouders daarom overleggen met de biologische ouders. Een aantal beslissingen kunnen ook van tevoren worden vastgelegd in een pleegcontract tussen de biologische ouders en de pleegouders.[24] Dit maakt het voor de pleegouders eenvoudiger om het pleegkind op te voeden, omdat beslissingen die al besloten zijn alleen nog maar uitgevoerd hoeven te worden. De pleegouders functioneren dan meer als uitvoerders van het gezag, maar dragen nog steeds niet het wettelijke gezag. De rechter kan besluiten om het gezag van de biologische ouders over te dragen naar de pleegouders; we spreken dan van een pleegoudervoogd.[25] Een pleegoudervoogd heeft dezelfde plichten als een voogd, maar dan dus over een pleegkind.

2.4 Waar wordt de gezagsrelatie geregistreerd?

Nu de verschillende gezagsverhoudingen hierboven zijn behandeld, rest ons nog te onderzoeken waar deze verhoudingen worden opgeslagen.

Elk kind dat in Nederland geboren wordt, moet binnen drie dagen bij

[22] BW 1:12 229
[23] Besluit gezagsregisters 2 onder k
[24] Jeugdwet 5.2 lid 1
[25] Jeugdwet 1.1

de gemeente worden aangegeven.[26] Het kind wordt dan door de ambtenaar van de burgerlijke stand ingeschreven in de Basisregistratie Persoonsgegevens (BRP). In de BRP wordt van iedere persoon een 'persoonslijst' bijgehouden.[27] Op deze persoonslijst worden een aantal algemene- en administratieve gegevens opgeslagen. Zo worden hier bijvoorbeeld gegevens over ouders en hun kinderen vastgelegd. Ook staan er in de BRP gegevens met betrekking tot gezag over minderjarige kinderen.[28] Deze gezagsverhoudingen zijn afkomstig van het moment dat de geboorte van de minderjarige werd aangegeven bij de burgerlijke stand, zoals hierboven beschreven. Op het moment dat de informatie over gezag niet meer actueel is, ontleent de basisregistratie gegevens over het gezag aan het openbaar gezagsregister.[29] In het gezagsregister staan "besluiten van de rechter over het gezag."[30] Deze besluiten over het gezag houden een wijziging van de gezagsverhouding in. De gezagsverhoudingen die bij de geboorteaangifte van het kind geregistreerd zijn, zijn dus niet meer geldig. Bij de oude gezagsverhoudingen in de BRP wordt dan een aantekening gemaakt zodra de rechtvank melding heeft gemaakt van een wijziging in de gezagsrelatie.[31] De rechtbank geeft dan aan "welke minderjarige [het] betreft, welke wijziging in het gezag heeft plaatsgevonden alsmede de datum waarop de wijziging ingaat."[32] Van de in sectie 2.3 beschreven situaties geldt dat het gezag over minderjarigen geboren uit een huwelijk of geregistreerd partnerschap in de BRP opgeslagen wordt. Voor minderjarigen die geboren zijn buiten een huwelijk of partnerschap wordt de gezagsrelatie tussen de moeder en de minderjarige ook opgeslagen in de BRP. Hier komt echter geen gezagsrelatie tussen de vader en de minderjarige te staan omdat de ouders niet in een huwelijk of partnerschap verbonden zijn. Als de vader ook het gezag wil dragen, dan moeten de vader en de moeder dit samen aanvragen bij het gezagsregister. Na goedkeuring van de rechter wordt dan het gezag van de vader in het register vastgelegd. Van de overige situaties die hierboven behandeld zijn geldt dat de gezagsrelatie enkel in het openbaar gezagsregister van de rechtbank opgeslagen.

Het register is openbaar, wat inhoudt dat iedereen een uittreksel kan opvragen bij de griffier van de rechtbank.[33] Wel moet de aanvraag gericht zijn op een specifieke minderjarige; er kunnen dus niet zomaar gegevens over

[26] `https://www.rijksoverheid.nl/onderwerpen/aangifte-geboorte-en-naamskeuze-kind/vraag-en-antwoord/aangifte-geboorte`

[27] BRP 1.1c

[28] BRP 2.7 onder 1a nummer 4

[29] BRP 2.13 lid 2

[30] `https://www.nvo.nl/beroepscode-en-tuchtrecht/veelgestelde-vragen/hoe-weet-ik-welke-ouder-gezag-heeft.aspx`

[31] BRP 2.28 lid 3

[32] BRP 2.28 lid 4

[33] `https://www.rechtspraak.nl/Registers/Gezagsregister`

het gezag over een willekeurig persoon worden opgevraagd.[34]

Nu de wet- en regelgeving rondom leeftijd en gezagsrelaties behandeld is, worden vervolgens de vier gebieden beschreven waar leeftijd en toestemming van gezagsdragers een rol spelen.

2.5 Alcohol

Met ingang van de vernieuwde Drank- en Horecawet in 2013 is het in Nederland verboden om alcoholische drank te verkopen aan personen onder de 18 jaar. Dit is onder meer vanwege schadelijke gevolgen van alcoholgebruik voor jongeren.[35] Om deze leeftijdsgrens te handhaven, is er in de Drank- en Horecawet een identificatieplicht ingesteld om de koper te laten aantonen daadwerkelijk de leeftijd van 18 jaar bereikt te hebben.[36] In dit onderzoek wordt een scheiding gemaakt tussen de verkoop aan klanten in een fysieke winkel (met name de supermarkten) en de verkoop van alcohol via internet. Vanzelfsprekend geldt voor beide categorieën dat de leeftijdsnorm gehanteerd moet worden. In een fysieke winkel hoeft een caissière niet om een legitimatie te vragen als de klant onmiskenbaar de vereiste leeftijd bereikt heeft. Als de klant mogelijk nog niet de vereiste leeftijd bereikt heeft, dan is de verkoopmedewerker verplicht om naar een legitimatie te vragen. Voor bestellingen die gedaan zijn via internet, geldt dat de verkoper de verantwoordelijkheid draagt voor een goede leeftijdscontrole van bestelling tot bezorging.[37] De bezorger zou aan de deur de leeftijdscontrole moeten uitvoeren. In 2019 drong staatssecretaris Paul Blokhuis aan op een nieuw leeftijdsverificatiesysteem wat de bezorgers zouden kunnen gebruiken om de levering van alcohol aan minderjarigen tegen te gaan.[38] Hoe dat systeem precies vorm gaat krijgen moet nog nader worden uitgewerkt.

2.6 Games

Op het gebied van de verkoop van games is het ook noodzakelijk dat er minimumleeftijdsgrenzen gehandhaafd worden. Om dit onderzoek in te perken wordt enkel de verkoop van console- en pc-games onderzocht. Deze games worden zowel in fysieke als in digitale vorm verkocht. In dit onderzoek wordt aan beide categorieën afzonderlijk aandacht besteed. Er zijn verschillende onderzoeken die aantonen dat het spelen van gewelddadige games

[34] Besluit gezagsregisters 10

[35] `https://www.rijksoverheid.nl/onderwerpen/alcohol/documenten/brochures/2012/08/16/hanreiking-drank-en-horecawet-voor-gemeenten`

[36] DHW 20.3

[37] `https://www.rijksoverheid.nl/actueel/nieuws/2019/03/28/blokhuis-verscherpt-regels-en-toezicht-voor-internetverkoop-alcohol`

[38] Kamerbrief - naleving leeftijdsgrenzen alcohol 2018 – 14 maart 2019

door kinderen kan leiden tot ongewenst gedrag[10]. Kinderen kunnen hierin zelf niet goed beslissen welke games wel, en welke games niet voor hen geschikt zijn. Daarom is het essentieel dat er een systeem is dat kinderen verhoedt om ongeschikte games te kopen. Om consumenten en ouders te helpen beslissen welke games geschikt zijn voor een kind zijn er classificatiesystemen voor games die games voorzien van een minimumleeftijd.[39] Het classificatiesysteem dat het meeste gebruikt wordt in Europa is Pan European Game Information (PEGI). PEGI classificeert een game in een van de volgende leeftijdscategorieën: geschikt vanaf 3, 7, 12, 16 of 18 jaar. Een leeftijdsklasse zegt niets over de moeilijkheidsgraad van een game, maar geeft enkel de geschiktheid van die game voor een bepaalde leeftijd aan. De verkoper die een game met een bepaalde leeftijdsgrens verkoopt aan een kind wat duidelijk nog niet de vereiste leeftijd heeft, is persoonlijk strafbaar op grond van artikel 240a Wetboek van Strafrecht.[40] Het PEGI-systeem heeft als hoogste klasse de leeftijd van 18 jaar, maar in Nederland mogen 16-jarigen ook games kopen die geclassificeerd worden in de categorie 18 jaar.[41] In Nederland is deze hoogste PEGI-klasse daarom niet van toepassing.

2.7 Medische sector

In de zorgverlening ligt sterk de nadruk op het persoonlijke contact tussen de patiënt en de zorgverlener. Daarom is er geen scheiding tussen een fysiek en een digitaal component zoals bij de twee vorige behandelde categorieën, maar is het in feite vooral fysieke contacten die hier spelen. Een ander verschil met de hiervoor behandelde onderdelen, is dat we het bij alcohol en games over het consumeren van producten hebben, op medisch gebied hebben we het over dienstverlening. Dienstverlening is minder uniform dan de verkoop van een product. Dit maakt dat afspraken met betrekking tot medische diensten gecompliceerder zijn dan de koopafspraken die gemaakt worden bij het kopen van alcohol of games.

2.7.1 Patiëntenrechten

Patiënten in Nederland hebben een aantal rechten, welke leiden tot verplichtingen voor zorgverleners.[42] Een aantal van deze rechten zijn bijvoorbeeld het recht op informatie over de behandelingen, het recht op het nemen van medische beslissingen, en het recht op het opvragen van een kopie van het medisch dossier. Zolang de patiënt nog niet de leeftijd van 12 jaar bereikt heeft, heeft de zorgverlener deze verplichtingen niet naar de patiënt zelf, maar naar de wettelijke vertegenwoordiger die het gezag uitoefent over

[39] `https://pegi.info/nl/node/19`
[40] WvS 240a; `https://www.kijkwijzer.nl/pegi`
[41] `https://www.kijkwijzer.nl/pegi`
[42] WGBO 448.1, AVG 58

de minderjarige.[43] De minderjarige heeft echter wel altijd recht op informatie. De zorgverlener moet ervoor zorgen dat de informatie die verstrekt wordt aan het minderjarige kind ook daadwerkelijk voor het kind begrijpelijk is.[44] De zorgverlener moet altijd zelf beoordelen of de wettelijke vertegenwoordigers van de minderjarige in het belang van de minderjarige handelen.[45] Minderjarige patiënten tussen de 12 en 16 jaar krijgen meer verantwoordelijkheden. De ouders blijven nog wel het recht op inzage en informatie behouden, maar naast de toestemming van de ouders voor medische handelingen, is nu ook de toestemming van de minderjarige noodzakelijk.[46] Als de ouders een andere wens hebben dan de minderjarige, dan is het aan de zorgverlener om te besluiten aan welke wens gehoor gegeven wordt. Hij zal dan de wil van de jongere opvolgen tenzij dit nadelig is voor de jongere. Als een behandeling of onderzoek heeft plaatsgevonden zonder instemming van de wettelijke vertegenwoordigers, dan hebben zij slechts recht op informatie en inzage na toestemming van de jongere.

Jongeren vanaf 16 jaar zijn voor de wet zelfstandig op medisch gebied.[47] Ook al hebben ze nog niet de leeftijd van 18 jaar bereikt, wat vaak als volwassen leeftijd gehanteerd wordt, worden 16-jarigen dus als volwassen behandeld. Er is geen toestemming meer nodig van de ouders of wettelijke vertegenwoordigers van de jongere. Verder hebben de gezagsdragers geen inzagerecht meer in het medische dossier van hun kind. Jongeren boven de 16 jaar mogen natuurlijk wel toestemming geven aan hun ouders om mee te beslissen of hun dossier in te zien. De ouders kunnen dan echter niet meer het dossier van hun kind inzien buiten de toestemming van het kind.

2.7.2 Inzage medisch dossier en het uitvoeren van medische handelingen

In het medisch dossier slaat de zorgverlener gegevens op over de patiënt, samen met alle andere informatie die van belang kan zijn voor de gezondheid van de patiënt.[48] Er staan aantekeningen in over de gezondheid van de patiënt, en informatie over de behandelingen die bij de patiënt zijn uitgevoerd. Verder kunnen er schriftelijke wilsverklaringen van de patiënt in toegevoegd worden.[49] Elke patiënt van 12 jaar en ouder heeft het recht om mondeling of schriftelijk een kopie van zijn medisch dossier op te vragen. Voor minderjarigen onder de 12 jaar kan een kopie van het dossier

[43] WGBO 465

[44] `https://www.knmg.nl/advies-richtlijnen/dossiers/rechten-minderjarigen.htm`; WGBO 448.1

[45] `https://www.huisartsenpraktijk-dewaterlelie.nl/hoe-zit-nu-precies-verstrekken-medische-informatie/`

[46] WGBO 450.2

[47] WGBO 447.1

[48] WGBO 454.1

[49] WGBO 454.2

door de gezagsdragers van de minderjarige aangevraagd worden. Onder 'schriftelijke aanvraag' wordt ook een digitale aanvraag bedoeld. Voor deze aanvraag, zowel mondeling als digitaal, is authenticatie noodzakelijk. Een patiënt kan zich door middel van bijvoorbeeld een identiteitsbewijs, of digitaal door middel van DigiD, authentiseren. Als de patiënt die het dossier wil opvragen echter nog geen 16 jaar is, is voor inzage ook de toestemming van de gezagsdrager van de minderjarige vereist. Ook voor het uitvoeren van medische handelingen moeten minderjarigen toestemming krijgen van hun gezagsdragers. Hiervoor gelden dezelfde leeftijdscategorieën als bij de inzage in het medisch dossier. Zo hebben kinderen onder de 12 jaar nog geen mogelijkheid om mee te beslissen, kunnen kinderen ouder dan 12 en jonger dan 16 jaar wel meebeslissen met hun gezagsdragers, en dragen kinderen boven de 16 jaar zelf de volledige verantwoordelijkheid voor handelingen die hen aangaan.

Uit het bovenstaande volgt dat het essentieel is dat bekend is wie het gezag dragen over minderjarigen. Er is hiervoor een oplossing nodig waarmee deze gezagsrelatie bewezen kan worden aan de zorgverlener.

2.8 Sociale media

Verwerking op basis van expliciete toestemming is de enige rechtvaardiging voor sociale media om persoonsgegevens te verwerken; de andere rechtsgronden uit artikel 6.1 van de AVG zijn hier niet van toepassing. Zoals eerder vermeld, is de verwerking van persoonsgegevens op basis van consent alleen rechtmatig als de betrokkene de leeftijd van 16 jaar bereikt heeft, of wanneer er toestemming gegeven is door de wettelijke vertegenwoordiger van de minderjarige. Daaruit volgt dat sociale media de leeftijd van hun gebruikers moeten verifiëren. Als het bovendien om een minderjarige gebruiker gaat, moet ook gecontroleerd worden of hij toestemming heeft gekregen van zijn gezagsdrager. Om die toestemming te controleren moet de gezagsrelatie tussen de minderjarige en zijn gezagsdrager aangetoond kunnen worden. Als de gezagsdrager dit bewijs levert is dat een teken dat hij toestemming geeft voor de verwerking.

Hoofdstuk 3

Verificatie in de praktijk

Nu de juridische context behandeld is in het eerste hoofdstuk, gaat dit hoofdstuk in op hoe de wettelijke kaders in de praktijk gehandhaafd worden. Het hoofdstuk is ingedeeld in vier secties; leeftijdsverificatie bij alcoholverkoop, gameverkoop, de medische zorg en sociale media. Bij de laatste twee onderwerpen zal ook de daarbij horende gezagsverificatie behandeld worden. Afhankelijk van het onderwerp wordt er de scheiding gemaakt tussen fysieke en digitale verificatie. Het hoofdstuk is beperkt tot het weergeven van de huidige situatie, eventuele verbeterpunten die hieruit kunnen voortvloeien, komen in een later hoofdstuk aan bod.

3.1 Alcohol

3.1.1 Nationaal preventieakkoord

In 2018 publiceerde het Ministerie van Volksgezondheid, Welzijn en Sport (VWS) het 'Nationaal Preventieakkoord'[19]. Dit akkoord heeft de ambitie om "Nederland gezonder te maken."[1] Er wordt in dit akkoord ingezet op vermindering van roken, overgewicht en overmatig alcoholgebruik. Voor dit onderzoek is enkel het laatste van toepassing. Het ministerie constateert dat de naleving van de leeftijdsgrens van 18 jaar bij alcoholverkoop een belangrijk onderdeel is van een verantwoorde verstrekking[19]. De laatste jaren is er een stijgende lijn te zien van het nalevingsniveau. Deze trend wil het ministerie doorzetten. De ambitie is om in 2030 de naleving van de leeftijdsgrens bij de verkoop van alcohol op 100% te krijgen[19]. Om dit te behalen werkt het ministerie nauw samen met het Trimbos Instituut en de brancheverenigingen van de supermarkten, het Centraal Bureau Levensmiddelenhandel (CBL). Hierdoor kunnen de betrokken partijen kennis en ervaring uitwisselen en daarmee een effectievere aanpak bereiken. Het

[1] https://www.rijksoverheid.nl/documenten/kamerstukken/2018/11/23/kamerbrief-over-nationaal-preventieakkoord

ministerie zorgt voor de actieve verspreiding van campagnemateriaal en de verkoopbranches maken zelf e-learning methoden. Voor de supermarkten wordt dit gedaan door het CBL. De e-learnings zijn gericht op het trainen van het personeel om de richtlijnen voor alcoholverkoop goed te handhaven. De ontwikkelde e-learning methoden worden voorgelegd aan het Trimbos Instituut, die de kwaliteit van de e-learning beoordeeld. Na goedkeuring wordt de e-learning in de praktijk ingezet.

3.1.2 Aanpak van de fysieke alcoholverkoop

Om een uniforme aanpak van het identificeren bij aankoop van alcohol te realiseren heeft het CBL bepaald dat klanten tot de leeftijd van 25 jaar gevraagd moeten worden om legitimatie als zij alcoholische dranken willen kopen.[2] Omdat klanten met de leeftijd van 18 jaar en ouder alcoholische drank mogen kopen, geeft de grens van 25 jaar een ruime marge van 7 jaar met de wettelijke minimumleeftijd. Het nadeel aan deze afspraak van het CBL is dat de kassamedewerker de inschatting moet maken of iemand jonger is dan 25 jaar of niet, om vervolgens om identificatie te vragen. Hierdoor is deze manier van handhaving gevoelig voor menselijke fouten. Om de doelstelling van het ministerie van VWS te bereiken, neemt het CBL verschillende maatregelen. Middelen die het CBL inzet zijn bijvoorbeeld campagnes gericht op klanten en trainingsmethoden voor verkopers. De belangrijkste campagne die het CBL ondersteunt, is de NIX18-campagne. Deze campagne is een initiatief van het ministerie van Volksgezondheid, Welzijn en Sport en is gericht op het veranderen van gedrag rondom alcoholgebruik.[3] Het doel is dat het de sociale norm wordt dat jongeren geen alcohol drinken voor hun 18e verjaardag. Dit wordt verwezenlijkt door gebruik van TV- en radio-spots, posters, en online video's. Deze middelen worden ingezet om het vanzelfsprekend te maken dat jongeren niet drinken onder de achttien jaar en dat het juist vreemd is als een jongere onder de 18 jaar wél alcohol nuttigt.[4]

Verder zet het CBL in op trainingsmethoden om de verkopers van alcoholische dranken beter te laten controleren op de leeftijd van de klant. Hiervoor heeft het CBL de e-learningmodule 'Soms moet je nee verkopen' ontwikkeld.[5] Deze module legt de legitimatieverplichting en de wetgeving rondom de alcoholverkoop uit aan de verkoopmedewerkers. Elke kassamedewerker in de supermarkt moet verplicht deze module met succes hebben afgerond voordat zij achter de kassa mogen zitten.

[2] `https://www.cbl.nl/onderwerpen/verkoop-van-alcohol/`

[3] `https://www.rijksoverheid.nl/onderwerpen/campagnes/campagnes-2018/nix18`

[4] `https://www.rijksoverheid.nl/onderwerpen/campagnes/campagnes-2018/nix18`

[5] `https://www.cbl.nl/onderwerpen/verkoop-van-alcohol/`

3.1.3 Aanpak van de online alcoholverkoop

De aanpak van de online verkoop, en vervolgens bezorging, van alcoholische dranken is gecompliceerder dan in de winkels. Vanzelfsprekend worden voor de online verkoop dezelfde campagnes ingezet als voor de fysieke verkoop. De enige echte maatregel die een verkoper van alcohol via internet kan inzetten is het controleren van de leeftijd op het moment van bezorging. Dit geeft een vergelijkbare situatie met hoe een caissière vraagt om legitimatie aan de kassa[13]. Als extra drempel kiezen sommige verkopers ervoor om de gebruiker eerst zijn geboortedatum te laten invoeren voordat de website bekeken kan worden. Dit wordt bijvoorbeeld gedaan door bierbrouwer Heineken.[6] De gebruiker moet dit zelf invullen en deze input wordt vervolgens niet geverifieerd. Daarom kan met deze maatregel niet worden vastgesteld dat de gebruiker de vereiste leeftijd bereikt heeft en is dit daarom een schijnmaatregel. Omdat er weinig toezicht is op hoe en of de bezorgers aan leeftijdsverificatie doen, wordt het aanbevolen om de bezorgers hier een speciale cursus in te geven. Ook raadt het CBL aan om technische hulpmiddelen in te zetten en gebruik te maken van zelfcontroles of mystery shoppers. Hoe dit in de praktijk vorm kan krijgen, wordt niet voorgeschreven.

3.1.4 Statistieken

Er is in de supermarkten al jaren een stijgende lijn te zien in de naleving van de legitimatieplicht[21]. In 2016 was het nalevingspercentage van de supermarkten 63,3%. Het jaar daarvoor was dit nog 52,2%. De doelstelling van de overheid is om in 2030 een naleving van 100% bereiken. Deze ambitie wil de overheid realiseren met een lineaire stijging vanaf 2018, zoals weergegeven is in onderstaande tabel uit het Nationaal Preventieakkoord:

	2018	2020	2022	2024	2026	2028	2030
Keten supermarkten	63,3	69,4	75,5	81,6	87,7	93,8	100
Slijters	61,8	68,2	74,6	81	87,4	93,8	100
Horeca	26,6	38,8	51	63,2	75,4	87,6	100
Thuisbezorgkanalen	9,1	24,3	39,5	54,7	69,9	85,1	100
Sportkantines	16,7	30,6	44,5	58,4	72,3	86,2	100
Cafetaria	28,6	40,5	52,4	64,3	76,2	88,1	100

Aangaande de verkoop via internet, valt het op dat in 2016 het nalevingspercentage slechts 2% was[21]. Op dat vlak valt er dus nog veel te verbeteren.

3.2 Games

In het vorige hoofdstuk is de PEGI-richtlijn beschreven, waarmee aan elke game een minimumleeftijd gekoppeld wordt. Deze richtlijn wordt echter

[6] `https://www.heineken.nl`

nog niet voldoende gehandhaafd. Er lijkt vanuit de overheid weinig druk te zitten achter de handhaving; er wordt wel gesproken over de naleving "optimaliseren", maar het is onduidelijk hoe dit sindsdien in de praktijk heeft uitgepakt.[7] Er zijn wel publicaties van campagnes die de overheid inzet, maar er zijn geen resultaten van deze campagnes gepubliceerd.[8] De bijbehorende branchevereniging Nederlands Instituut voor de Classificatie van Audiovisuele Media (NICAM) houdt zich wel bezig met PEGI, maar schijnt meer aandacht te besteden aan de regels rondom Kijkwijzer dan PEGI.[9]

3.2.1 Aanpak van de fysiek gameverkoop

Het is onduidelijk of er in de fysieke winkels waar games verkocht worden, vergelijkbare maatregelen genomen worden als bij de alcoholverkoop. Het NICAM biedt de verkopers geen handvatten om de leeftijd van de koper te verifiëren, zoals het CBL wel doet voor de supermarkten. Het is mogelijk dat verkopers van games ook een kassa-blokkade systeem gebruiken, zoals ook in de supermarkten gebruikelijk is bij producten met een leeftijdsrestrictie. In een game-winkel zou de kassa dan ook kunnen vragen om de geboortedatum van de klant om de kassa weer te deblokkeren. Het is echter onduidelijk of dit daadwerkelijk gebeurt. In 2019 bleek uit een onderzoek van Kassa, het consumentenplatform van BNNVARA, dat het voor minderjarigen vaak totaal geen moeite kost om games te kopen die zij eigenlijk nog niet zouden mogen kopen.[10] Uit de steekproef van Kassa bleek dat de gameverkoper Game Mania, in drie verschillende winkels, niet om legitimatie vroeg aan de mystery shoppers van Kassa.[11] Omdat het onderzoek in drie winkels van Game Mania werd uitgevoerd, kan er geen sprake zijn van een toevalstreffer. Deze uitkomst is opvallend omdat Game Mania slechts enkele maanden voor de uitzending van het programma op hun website bekendmaakte zich te houden aan de PEGI normen.[12] Bij de uitzending van Kassa was Angeline van Dijk namens Agentschap Telecom aanwezig. Agentschap Telecom houdt het toezicht op de uitvoering van de Telecommunicatiewet. Van Dijk stelde dat het agentschap 1200 bedrijven met mystery shoppers bezocht heeft sinds 2014, en dat daar geen overtredingen waren gevonden. Hierbij moet echter wel de kanttekening gemaakt worden dat het agentschap geen gebruik maakt van minderjarige mystery shoppers, terwijl deze juist

[7] https://zoek.officielebekendmakingen.nl/kst-28684-279.html

[8] https://www.kijkwijzer.nl/upload/zijbalk3/294_BURO240a_folder_Winkelmedewerkers.pdf

[9] https://nicam.nl/

[10] https://www.bnnvara.nl/kassa/artikelen/game-mania-en-diverse-webshops-verkopen-ongeschikte-16-spellen-aan-jonge-kinderen

[11] https://www.bnnvara.nl/kassa/videos/519747

[12] https://www.gamemania.nl/Articles/koop-de-juiste-games-voor-je-kind-dankzij-pegi

nodig zijn om te proberen een game onder de minimumleeftijd te kopen. Agentschap Telecom kan niet op basis van het bewijsmateriaal van Kassa een boete uitdelen; dit kan alleen door inspecteurs van het agentschap op het aantreffen van een heterdaad. Van Dijk geeft wel aan met Game Mania en de branchevereniging NICAM in gesprek te gaan. Ook gaan ze over tot extra controle op de fysieke winkels. Het effect van deze maatregelen kan echter niet vooraf worden vastgesteld. Omdat de televisie-uitzending in oktober 2019 plaatsvond, zullen daarom de resultaten nog niet bekend zijn op de publicatiedatum van dit onderzoek.

3.2.2 Aanpak van de online gameverkoop

Kassa liet hun minderjarige mystery shoppers ook via webwinkels games kopen. Voorwaarde was dat zij niet zouden liegen over hun leeftijd als hen gevraagd werd deze in te vullen. Het bleek dat slechts twee van de zes onderzochte sites vragen om de leeftijd van de koper. Dat meer dan de helft van de winkels niet vraagt om een leeftijd is zorgwekkend. In het onderzoek van Kassa is het populaire game-platform Steam niet meegenomen in het onderzoek. Omdat dit een grote verstrekker is van downloadbare games (dus niet fysiek), neem ik deze wel mee in deze scriptie om te onderzoeken of dit platform wél leeftijd verifieerd.

Vooraf is het belangrijk om te weten dat niet elke game op Steam een PEGI rating heeft.[13] Dit zijn met name de kleinere games, afkomstig van onbekende uitgevers. Deze games spreken vaak niet de grote massa gamers aan en worden ook niet veel verkocht. Voor dit soort games hanteert Steam een eigen content rating systeem. Bij het aanmaken van een account, wat nodig is om games te kopen, wordt al gevraagd of de gebruiker 13 jaar of ouder is.[14] Als de klant vervolgens een game wil kopen waarvoor een leeftijdsrestrictie geldt, dan wordt de pagina eerst nog afgeschermd door een verzoek om de geboortedatum zelf in te vullen om door te gaan. Als de gebruiker de vereiste minimumleeftijd nog niet bereikt heeft, dan wordt de pagina geblokkeerd.

De overeenkomst die alle verkopers van digitale games hebben, is dat er overal vanuit gegaan wordt dat de klant eerlijk is over de geboortedatum.[15] Hiervoor wordt als excuus aangedragen dat er nog niet de technische mogelijkheden zijn om deze verificatie goed uit te voeren. Zoals we in hoofdstuk 4.2 zullen zien, zijn er echter wel degelijk middelen voor. Deze worden echter nog niet op grote schaal ingezet.

[13] `https://www.askaboutgames.com/beyond-the-box-understanding-content-ratings-on-steam/`

[14] `https://store.steampowered.com/privacy_agreement/`

[15] `https://www.bnnvara.nl/kassa/videos/519747`

3.3 Medische sector

Ook op medisch gebied speelt leeftijdsverificatie een rol. We zagen dat in het vorige hoofdstuk, waar er verschillende procedures bleken te gelden voor verschillende leeftijdscategorieën. Minderjarige patiënten zijn nog niet bevoegd om zelfstandig op te treden. Zij hebben daarom toestemming van hun gezagsdragers nodig. Er is dus behoefte aan een systeem om de leeftijd te controleren en te verifiëren wie het gezag dragen over de minderjarige patiënten. Deze manieren van verificatie zullen in deze sectie onderzocht worden op het gebied van inzage in het medisch dossier. De problemen in verificatie die we daar tegenkomen kunnen breder getrokken worden naar andere handelingen in de medische sector waar dezelfde verificatie vereist is.

Er zijn verschillende manieren waarop een patiënt medische informatie kan inzien. Deze zijn echter niet allemaal relevant voor dit onderzoek. Wat in dit kader niet relevant is, is een 'Persoonlijke Gezondheidsomgeving' (PGO).[16] Een patiënt kan zelf een PGO aanmaken en daarin al zijn medische gegevens verzamelen en samenvoegen. Op deze manier kan een patiënt dus een eigen medisch dossier opstellen uit gegevens van verschillende zorgverleners. Artsen of andere hulpverleners hebben geen inzage in de PGO, deze is alleen door de patiënt toegankelijk. De patiënt kan er wel voor kiezen om bepaalde gegevens met zorgverleners te delen. Omdat de patiënt zelf de PGO beheert, hoeft hij dus geen verificatie te doen richting een arts om de PGO in te zien. Daarom is het in dit geval vanzelfsprekend niet nodig dat een arts onderzoek moet doen naar de gezagsverhouding tussen minderjarigen en hun wettelijke vertegenwoordigers om hen medische gegevens te laten inzien in een PGO.

Iedere zorgverlener houdt een persoonlijk medisch dossier bij voor iedere patiënt, volgens de 'dossierplicht' in de Wet op de Geneeskundige Behandelingsovereenkomst (WGBO).[17] De patiënt kan een fysieke of digitale kopie van dit dossier aanvragen bij de zorgverlener. Een manier waarop de digitale kopie gerealiseerd kan worden, is via een zogeheten 'patiëntenportaal.'[18] Vanaf 1 juli 2020 moet elke zorgverlener een patiëntenportaal aanbieden. Hierin kan hij allerlei gegevens rondom de patiënt en zijn behandeling opslaan. Omdat medische gegevens gevoelige informatie zijn, moet er een verificatie plaatsvinden om te garanderen dat de gegevens niet door onbevoegden kunnen worden ingezien. Dit hoofdstuk zal eerst de fysieke- en digitale verificatie behandelen. Daarna wordt er aandacht besteedt aan een pilot met betrekking tot ouderlijk gezag in de zorg.

[16] https://www.rijksoverheid.nl/onderwerpen/digitale-gegevens-in-de-zorg/vraag-en-antwoord/wat-is-een-persoonlijke-gezondheidsomgeving-pgo

[17] https://www.patientenfederatie.nl/themas/inzage-in-uw-medisch-dossier/; WGBO art 454

[18] https://www.hulpmiddelenwijzer.nl/hulpmiddelen/patientportalen

3.3.1 Fysiek

Patiënten kunnen een afspraak maken bij hun arts om samen met de arts hun medisch dossier door te nemen. Hiervoor geldt vanzelfsprekend dat de patiënt zich moet kunnen legitimeren, zoals gebruikelijk is in de zorgverlening.[19] Het wordt echter ingewikkelder als het gaat over het inzien van het dossier van minderjarige kinderen. Voor kinderen jonger dan 12 jaar geldt dat gezagsdragers het dossier mogen inzien op vertoon van hun eigen legitimatie. Zorginstellingen mogen zelf beslissen of zij hiervoor om legitimatie van één of van beide gezagsdragers vragen. Bij inzage van het medisch dossier van kinderen vanaf 12 jaar tot 16 jaar zijn zowel de legitimatie(s) van de ouder(s) als van het kind vereist. Dit komt voort uit de wet die stelt dat kinderen tussen de 12 en 16 samen met hun wettelijke vertegenwoordigers de patiëntenrechten uitoefenen, zoals in het vorige hoofdstuk beschreven is. Vanaf 16 jaar wordt het kind door de medische sector als volwassene gezien, waardoor het zelfstandig kan vragen om inzage in of een kopie van het medisch dossier.

Voor de minderjarigen in de leeftijdscategorie 0-16 jaar is er ondanks de verstrekte identiteitsdocumenten nog een probleem: het is niet bewezen dat de 'ouders' daadwerkelijk de gezagsdragers van de minderjarige zijn van wie het dossier wordt opgevraagd. Op geen enkel identiteitsdocument staat de relatie tussen een gezagsdrager en een minderjarige geregistreerd. De dossierbeheerder heeft deze informatie echter wel nodig. Anders zouden de medische dossiers van minderjarigen kunnen worden ingezien door mensen die niet hun gezagsdragers zijn. Normaalgesproken maakt de arts de afweging of de 'ouders' en de minderjarige bij elkaar horen. Als de arts hieraan twijfelt, dan wordt er aanbevolen om inlichtingen in te winnen bij een persoon van wie de arts zeker weet dat hij gezagsdrager is.[20] Als dit niet mogelijk is, kan de arts informatie verzamelen van de kinderbescherming, of van het gezagsregister van de rechtbank, of van de burgerlijke stand. Zodra de gezagsdrager bekend is, is het mogelijk om hiervan een aantekening te maken in het dossier van de minderjarige. De keerzijde van deze optie is dat die informatie kan verouderen. Om dit te verhinderen zou bij elke gezagswijziging vervolgens ook nog het medisch dossier moeten worden aangepast, wat extra administratieve rompslomp met zich meebrengt. Als laatste beveelt het Nederlands Tijdschrift voor Geneeskunde nog aan dat de huisarts, die het dichtst bij de patiënten staat, bij een doorverwijzing naar een medisch specialist direct informatie meegeeft over gezagsrelaties.[21] Hiermee wordt het onderzoeken van gezagsrelaties de verantwoordelijkheid van huisartsen.

[19] `https://www.rijksoverheid.nl/onderwerpen/identificatieplicht/vraag-en-antwoord/identificatieplicht-zorg`

[20] `https://www.ntvg.nl/artikelen/wettelijke-vertegenwoordigers-van-het-kind-ten-aanzien-van-de-wet-op-de-geneeskundige/volledig`

[21] `https://www.ntvg.nl/artikelen/wettelijke-vertegenwoordigers-van-het-kind-ten-aanzien-van-de-wet-op-de-geneeskundige/volledig`

Dit lijkt echter meer een verplaatsing van het probleem dan een oplossing. Hier zijn echter geen verdere gegevens over bekend.

Inzage in het dossier kan via een brief aangevraagd worden bij de zorgverlener.[22] De consumentenbond verstrekt een formulier dat gebruikt kan worden voor de aanvraag.[23] De aanvrager moet zich legitimeren door een kopie van een wettig identiteitsbewijs met de brief mee te sturen[16]. Wanneer het dossier van een minderjarig kind wordt opgevraagd, moet zowel een kopie van het identiteitsbewijs van het kind als van de gezagsdrager meegestuurd worden. Afhankelijk van de zorgaanbieder kan het dossier dan op locatie worden ingezien, of wordt een kopie via de post verstuurd. Hoewel het over gevoelige informatie gaat, is het onder de AVG wel toegestaan om dit te versturen via de reguliere post.[24] Extra maatregelen, zoals de post aangetekend versturen, worden geadviseerd, maar zijn niet verplicht.

3.3.2 Digitaal

Naast een papieren uittreksel van het medisch dossier, is iedere zorgaanbieder vanaf 1 juli 2020 verplicht om ook een digitale versie van het dossier aan te bieden.[25] Deze digitale versie is nog steeds een kopie van het dossier, net als de papieren versie. De manier die veel zorgaanbieders sinds kort aanbieden of binnenkort willen gaan aanbieden zijn de al eerder genoemde patiëntenportalen. In een fysieke zorgomgeving moet een patiënt zich authentiseren om gegevens, zoals in het patiëntenportaal staan opgeslagen, in te zien. Omdat de patiëntenportalen digitaal aangeboden worden, moet de patiënt zich in dit geval dus digitaal authentiseren. De medische informatie die in de patiëntenportalen staat opgeslagen valt volgens de AVG onder "gevoelige" gegevens en moeten daarom proportioneel beschermd worden. Het Europese initiatief 'Electronic IDentification Authentication and trust Services' (eIDAS) deelt diensten in op betrouwbaarheidsniveaus. De betrouwbaarheidsniveaus zijn: Geen, Laag, Substantieel en Hoog. Elk niveau heeft een aanbevolen authenticatiemiddel; hoe hoger het niveau, hoe hoger het niveau van authenticatie moet zijn. Onderzoekers van PrivacyCare en PBLQ bevelen vanwege de gevoelige gegevens een authenticatieniveau van substantieel of hoger aan voor de patiëntenportalen aan[18]. Dit houdt in dat de gebruiker van het patiëntenportaal zich de eerste keer moet identificeren door middel van een legaal identificatiedocument. Verder gaat de authenticatie via 2-factor authenticatie, waarbij de gebruiker dus op twee manieren moet bewijzen dat hij daadwerkelijk de echte gebruiker is.

[22] `https://www.patientenfederatie.nl/themas/inzage-in-uw-medisch-dossier/`

[23] `https://www.consumentenbond.nl/juridisch-advies/zorg-zorgverzekering/medisch-dossier-inzien`

[24] `https://www.avghelpdeskzorg.nl/onderwerpen/post/122---post-medische-gegevens-per-post`

[25] Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg 15a lid 1

Het medisch dossier mag ook via e-mail uitgewisseld worden. Hierbij wordt wel dringend verzocht om het dossier te beveiligen.[26] Dit kan door het dossier te versleutelen en de bijbehorende sleutel via een andere weg aan de patiënt te geven. Het wordt ook aangeraden om gebruik te maken van een beveiligde e-mailverbinding. Authenticatie werkt hier hetzelfde als bij de aanvraag per brief: een kopie van het identiteitsbewijs kan worden toegevoegd als bijlage aan de e-mail waarin inzage wordt aangevraagd.

3.3.3 Pilot Ouderlijk gezag in de zorg

Om de patiëntenrechten voor minderjarigen uit te voeren, is het noodzakelijk dat het duidelijk is wie er bevoegd zijn om deze rechten voor de minderjarigen uit te voeren. Er moet daarom een digitale methode zijn in het patiëntenportaal die kan aantonen wie de wettelijke vertegenwoordiger(s) is/zijn van de minderjarige. Een veel gebruikte manier om in te loggen op een patiëntenportaal is het elektronische identiteitssysteem DigiD.[27] Dit is in overeenstemming met de eisen van eIDAS, want DigiD kan gebruikt worden op het niveau van eIDAS substantieel[23]. Als een patiënt DigiD gebruikt om in te loggen, weet de zorgverlener op basis van het BSN dat de juiste patiënt ingelogd heeft en daarom toegang mag krijgen tot zijn medische gegevens. Wanneer een ouder de medische gegevens van zijn minderjarige kind wil inzien, ontstaat er echter een probleem. Er is in DigiD geen manier om te bewijzen wie het gezag over welke minderjarigen draagt. Met DigiD is het dus niet mogelijk om de patiëntenrechten van de minderjarigen door de gezagsdragers te laten uitvoeren. Een manier om dit probleem te omzeilen is om een DigiD voor de minderjarige aan te maken en dan via dat DigiD de gegevens van de minderjarige te bekijken.[28] Dit is echter niet legaal omdat het DigiD strikt persoonlijk is en dus zelfs niet door gezagsdragers gebruikt mag worden. Bovendien geeft dit problemen voor minderjarigen tussen de 12 en 16 jaar, die samen met hun ouders medische besluiten moeten maken. Als de ouders namelijk de inloggegevens van de DigiD van de minderjarige in handen krijgen, is er geen toezicht meer op wie er nu precies handelingen uitvoeren op naam vna de minderjarige. De minderjarige zou dan zelf moeten controleren of zijn ouders daar geen misbruik van maken. Er is in veel gevallen wel een officiële machtigingsprocedure van de zorgaanbieder, maar dit gaat vaak via een complexe route.[29] Om deze problemen op te lossen werkt Logius, de dienst achter DigiD, aan de pilot "Ouderlijk gezag

[26] https://www.knmg.nl/advies-richtlijnen/artseninfolijn/praktijkdilemmas-1/praktijkdilemma/mag-ik-volgens-de-privacywet-avg-medische-gegevens-verstrekken-per-e-mail-1.htm

[27] https://www.digid.nl/

[28] https://www.digitaleoverheid.nl/dossiers/digid-machtigen/dossier-berichten/veilig-en-eenvoudig-toegang-tot-medisch-dossier-kind/

[29] https://www.tjongerschans.nl/over-ons/nieuws/met-je-eigen-digid-toegang-tot-het-medisch-dossier-van-je-kind.htm

in de zorg."[30] In deze pilot streeft Logius ernaar om het voor ouders mogelijk te maken om, met hun eigen DigiD, toegang te krijgen tot het medisch dossier van de minderjarige waarover zij het gezag dragen.[31] Als de ouder inlogt met zijn eigen DigiD, vindt er een controle plaats van het gezag via de nieuwe machtigingsfunctionaliteit die in de pilot wordt ingevoerd. Als de ouder bevoegd is, dan krijgt hij toegang tot het medisch dossier van de minderjarige. De pilot wordt uitgevoerd in het ziekenhuis Tjongerschans te Heerenveen. Dit ziekenhuis is ideaal voor dit onderzoek omdat er al veel gewerkt is met het aanbieden van digitale dossiers.[32] Daarbij komt dat het een middelgroot ziekenhuis is, waardoor de schaal van het onderzoek niet te klein en niet te groot is. Vooralsnog gaat het alleen om toegang tot het dossier van kinderen onder de 12 jaar en kunnen nu alleen moeders een machtiging aanvragen. Hier is voor gekozen om het onderzoek zo eenvoudig te houden als mogelijk is. Later zal het onderzoek uitgebreid worden met de deelname van vaders en de groep van 12- t/m 16-jarigen.

3.4 Sociale media

Sociale media zijn erg populair onder jongeren. Omdat er door sociale media persoonlijke gegevens van de gebruikers verwerkt worden, moeten de sociale media ook voldoen aan de AVG. Daarom hebben minderjarige gebruikers toestemming nodig van hun ouders om de sociale media te gebruiken. In deze sectie wordt onderzocht voor een aantal verschillende sociale media welke minimumleeftijden zij hanteren, en hoe de ingevoerde leeftijd vervolgens geverifieerd wordt. Er zijn teveel verschillende sociale media om stuk voor stuk te onderzoeken hoe zij zich aan de wettelijke normen houden. Daarom is een selectie gemaakt gebaseerd op de meest gebruikte sociale media onder jongeren, op basis van onderzoek door onderzoeksbureau Newcom. Dit bureau produceert elk jaar een onderzoek naar het sociale media gebruik onder de Nederlandse bevolking. Voor dit onderzoek is het rapport 'Nationale Social Media Onderzoek 2020' gebruikt[14]. Uit dit rapport blijkt dat de populairste media onder jongeren zijn: WhatsApp, Facebook, YouTube, Instagram en Snapchat. Aan deze rij voegen we nog het sociale medium TikTok toe. TikTok is een nieuw medium wat erg populair is onder jongere gebruikers. Daarom is het ook interessant om deze ook mee te nemen in de vergelijking; sectie 3.4.6 gaat verder in op de motivatie om TikTok te onderzoeken.

[30] https://magazines.logius.nl/koppelvlak/2019/01/pilot-ouderlijk-gezag

[31] https://www.nictiz.nl/wp-content/uploads/Factsheet-Veilig-en-eenvoudig-toegang-tot-medisch-dossier-kind.pdf

[32] https://magazines.logius.nl/koppelvlak/2019/01/pilot-ouderlijk-gezag

3.4.1 WhatsApp

Om aan de AVG te voldoen heeft WhatsApp in 2018 in Europa de minimumleeftijd voor gebruik van hun dienst verhoogd van 13 jaar naar 16 jaar.[33] In de rest van de wereld waar WhatsApp beschikbaar is, blijft de grens op 13 jaar liggen. Om de app te gebruiken hoeft de gebruiker alleen maar aan te vinken 16 jaar of ouder te zijn.[34] Het bedrijf stelt duidelijk op haar website dat het verkeerd aangeven van de leeftijd van de gebruiker een schending is van de Terms of Service.[35]

3.4.2 Facebook

Hoewel Facebook het moederbedrijf is van WhatsApp, hebben ze een verschillend beleid op het gebied van minimumleeftijden voor gebruik. De minimumleeftijd voor het gebruiken van Facebook is 13 jaar.[36] Om aan de AVG te voldoen moeten jongeren tot de leeftijd van 15 jaar echter wel toestemming krijgen van hun gezagsdrager. De jongere moet zelf aangeven op Facebook wie zijn ouder is. Zolang de minderjarige jonger is dan 16 jaar en geen toestemming heeft van de aangewezen ouder, kan hij enkel een beperkte versie van Facebook gebruiken waarin geen informatie gedeeld kan worden. Voor Facebook geldt ook dat de gebruiker zelf zijn leeftijd moet aangeven bij de registratie.

3.4.3 YouTube

Omdat YouTube-accounts standaard gekoppeld zijn aan bestaande Google-accounts, heeft YouTube hetzelfde beleid voor minimumleeftijden als Google. De leeftijdsgrens voor het zelfstandig beheren van een account ligt in de meeste situaties op 13 jaar.[37] Een aantal landen heeft hier een andere grens aan gesteld, zoals bijvoorbeeld Nederland waar de leeftijdsgrens op 16 jaar ligt. Voor minderjarigen onder de 16 jaar kunnen ouders een account aanmaken en beheren.[38] Net als Facebook en WhatsApp, vertrouwt ook Google er op dat de leeftijd eerlijk ingevuld wordt bij het maken van een account. YouTube heeft een extra maatregel ingesteld om jongeren onder de 18 jaar te beschermen door aan video's een 18+ label te kunnen hangen.[39] Video's

[33] https://www.reuters.com/article/us-whatsapp-privacy-eu/whatsapp-raises-minimum-age-in-europe-to-16-ahead-of-data-law-change-idUSKBN1HV2C5

[34] https://www.bright.nl/nieuws/artikel/4123631/minimumleeftijd-whatsapp-slechts-voor-de-vorm

[35] https://faq.whatsapp.com/en/iphone/26000151/

[36] https://www.reuters.com/article/us-whatsapp-privacy-eu/whatsapp-raises-minimum-age-in-europe-to-16-ahead-of-data-law-change-idUSKBN1HV2C5

[37] https://support.google.com/accounts/answer/1350409

[38] https://support.google.com/families/answer/7103338

[39] https://support.google.com/youtube/answer/2802167?visit_id=637208339087133257-2537821303&rd=1

met dat label kunnen schadelijk zijn voor jonge kijkers (volgens Google's beleid) en kunnen daarom alleen bekeken worden door accounts waarvan de gebruiker ouder is dan 18 jaar. Dit is echter niet effectief als minderjarigen liegen over hun leeftijd.

3.4.4 Instagram

Instagram hanteert dezelfde lijnen als de al hierboven behandelde sociale media. De uiterste minimum leeftijdsgrens is 13 jaar, maar in landen die een hogere grens stellen, zoals Nederland, mag een 16-jarige pas zelfstandig een account beheren.[40] Vanaf 13-jarige leeftijd mag een minderjarige wel een account hebben, maar hiervoor moet door een ouder toestemming gegeven worden. De gebruiker moet zelf eerlijk zijn leeftijd invullen. Instagram gaat geen geboortedata verifiëren, omdat "tieners vaak hun leeftijd niet kunnen bewijzen" en het bedrijf nooit van alle gebruikers gegevens over de leeftijd zal kunnen verkrijgen.[41]

3.4.5 Snapchat

Ook Snapchat hanteert de ondergrens van 13 jaar voor het zelfstandig beheren van een account.[42] Anders dan de eerder genoemde sociale media lijkt Snapchat zich niet aan te passen aan de AVG op het gebied van de leeftijdsgrens die lidstaten van de EU kunnen instellen. Het is dus mogelijk om als 14-jarige een account aan te maken op Snapchat, terwijl dat volgens de Uitvoeringsweg AVG in Nederland niet toegestaan is. Onder de 13 jaar is het niet mogelijk om een account aan te maken, ook niet met toestemming van de ouders[22].

3.4.6 Tiktok

TikTok is een razend populaire nieuwe app, die vooral aantrekkelijk is voor de jongere gebruiker[14].[43] Hoewel het nog niet zo groot is als de reeds gevestigde sociale media, die hierboven al beschreven zijn, is het goed om deze app toch mee te nemen in het onderzoek. Over een aantal jaar kan de groei namelijk doorgezet hebben en dan zou TikTok een groot sociaal medium kunnen zijn. Het platform houdt een minimumleeftijd van 13 jaar aan voor gebruikers wereldwijd.[44] Onder de 18 jaar moeten de gebruikers

[40] https://help.instagram.com/154475974694511/?helpref=hc_fnav&bc[0]=Instagram\%20Help&bc[1]=Privacy\%20and\%20Safety\%20Center

[41] https://www.reuters.com/article/us-facebook-instagram-children/instagram-to-collect-ages-in-leap-for-youth-safety-alcohol-ads-idUSKBN1Y826Z

[42] https://www.snap.com/en-US/safety/safety-center/

[43] https://www.nytimes.com/2018/12/03/technology/tiktok-a-chinese-video-app-brings-fun-back-to-social-media.html

[44] https://www.tiktok.com/legal/terms-of-use?lang=en

toestemming hebben van hun gezagsdrager; dit past binnen de norm die de AVG stelt. Het is echter, zoals ook bij de eerder behandelde sociale media, niet moeilijk om een onjuiste leeftijd aan te geven omdat die door TikTok niet gecontroleerd wordt.

Opvallend is het feit dat de behandelde sociale media platforms dezelfde minimumleeftijd van 13 jaar hanteren. Dit is te danken aan de Amerikaanse 'Children's Online Privacy Protection Act' (COPPA).[45] Deze Amerikaanse wet heeft op het gebied van verwerking van gegevens van kinderen een vergelijkbare aanpak als de AVG.[46] Onder deze wet is het toegestaan om gegevens van kinderen van alle leeftijden te verwerken, maar dan moeten de bedrijven wel kunnen aantonen dat deze kinderen hiervoor toestemming hebben van hun ouders. Veel sociale media kiezen ervoor om hun diensten slechts aan 13-jarigen en ouder aan te bieden zodat er geen rekening gehouden hoeft te worden met allerlei beperkende maatregelen rondom gegevensverwerking die de COPPA hen anders zou opleggen.

[45] `https://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16\%3A1.0.1.3.36&rgn=div5`

[46] COPPA §312.5 Parental Consent

Hoofdstuk 4

Mogelijke oplossingen

In de voorgaande hoofdstukken is een aantal zaken aan de orde gekomen rondom (digitale) leeftijdsverificatie. Dit hoofdstuk zal de verschillen tussen de wettelijke kaders en de praktijk onderzoeken. Elk van die tekortkomingen zal in een aparte alinea worden beschreven met een daarbij passende aanpak. Vervolgens worden alle aanbevelingen die hieruit voortkomen samengevoegd, en wordt er een suggestie gedaan voor een oplossing voor de huidige problemen in de leeftijds- en gezagsverificatie.

4.1 Verbeterpunten

4.1.1 Weinig toezicht op verificatie thuisbezorgkanalen

In sectie 3.1.3 is de leeftijdsverificatie rondom alcoholverkoop bij bezorging aan de deur behandeld. Er zijn op dat gebied een aantal dingen die nog niet voldoende gereguleerd zijn. Deze sectie zal onderzoeken hoe de leeftijdsverificatie bij bezorging beter gereguleerd kan worden. In sectie 2.5 kwam al kort een idee van staatssecretaris van Volksgezondheid, Welzijn en Sport, Paul Blokhuis, aan bod. Blokhuis pleit voor een nieuw verificatiesysteem wat bezorgers kunnen gebruiken om leeftijden aan de deur te verifiëren. In de kamerbrief van de staatssecretaris staat dat er meer toezicht nodig is op de thuisbezorgkanalen. Verschillende partijen die Blokhuis gesproken heeft zeggen namelijk dat "de prikkel om de wet na te leven ontbreekt als er niet gehandhaafd wordt."[1] Er is dus een sterke mate van controle nodig op de bezorgers om de wet toch na te leven. Dit kan verwezenlijkt worden door eenzelfde vorm van verificatie toe te passen bij het bezorgen als bij de kassa's in de supermarkten al gebruikt wordt. In de supermarkt blokkeert de kassa bij het scannen van alcoholhoudende drank. De caissière kan deze blokkade omzeilen als de klant overduidelijk ouder is dan 18 jaar. Als dit niet duidelijk

[1] `https://www.rijksoverheid.nl/documenten/kamerstukken/2019/03/14/kamerbrief-over-nalevingscijfer-leeftijdsgrenzen-alcohol-2018`

is moet de geboortedatum van de klant worden ingevoerd. Omdat er bij een bezorging aan huis nauwelijks toezicht is op de bezorger, zou er idealiter een strikter systeem in de bezorging moeten komen. Dit kan bijvoorbeeld gerealiseerd worden door aan elke klant, ongeacht of de bezorger denkt dat de klant oud genoeg is, te vragen om legitimatie. Hierdoor kan bij elke bezorging worden nagegaan in het systeem of er daadwerkelijk een verificatie van de leeftijd is uitgevoerd. Daarmee kan er dus een verificatie bij elke bezorging gerealiseerd worden. Zolang hiervoor in de verificatie rekening wordt gehouden met de privacy van de gebruikers zou dit geen gevaren voor de privacy moeten opleveren. Sectie 4.1.5 gaat verder in op de zorgen rondom privacy die naar voren komen bij het verifiëren van leeftijd.

4.1.2 Leeftijdsverificatie bij gameverkoop

Uit het onderzoek van Kassa wat in 3.2 behandeld werd, bleek dat gameverkopers de richtlijnen voor leeftijdscontrole niet in acht nemen. Zowel de fysieke verkoop als de digitale verkoop van games laat nog veel te wensen over. Vanuit de overheid zijn er naast het PEGI-systeem geen beleidslijnen om de verkoop aan minderjarigen terug te dringen. Ook wordt er nauwelijks bestraft bij overtreding van de verificatieplicht. In de uitzending van Kassa, die in het vorige hoofdstuk genoemd is, werd door de vertegenwoordiger van Agentschap Telecom al gesteld dat er alleen boetes worden uitgedeeld bij een betrapping op heterdaad.[2] Omdat echter alleen meerderjarigen inspecties bij de winkels mogen uitvoeren, kan een winkel per definitie geen game verkopen aan een minderjarige controleur die de vereiste leeftijd niet bereikt heeft. Hierdoor is het lastig om een verkoper daadwerkelijk op een overtreding te betrappen. Omdat de handhaving van overheidswege zo goed als achterwege blijft, is er in de sector weinig druk op het naleven van de wet.[3] Er moet bij de gameverkopers meer bewustwording komen over de wettelijke kaders rondom de verkoop aan minderjarigen. Verder zou Agentschap Telecom er goed aan doen om gebruik te maken van minderjarige mystery shoppers (uiteraard onder begeleiding van een volwassene), om daarmee verkopers op heterdaad te kunnen betrappen zodra er een ongepaste game verkocht wordt aan een kind. Deze combinatie van bewustwording bij de verkopers en handhaving vanuit de overheid kan er aan bijdragen dat de leeftijdsverificatie in de gameverkoop beter wordt nageleefd.

[2] `https://www.bnnvara.nl/kassa/videos/519747`

[3] `https://www.bnnvara.nl/kassa/artikelen/game-mania-en-diverse-webshops-verkopen-ongeschikte-16-spellen-aan-jonge-kinderen`

4.1.3 Onduidelijkheid in de medische zorg over gezagsrelaties

In sectie 3.3.1 werd beschreven dat de verantwoordelijkheid voor het achterhalen van de juiste gezagsrelaties in de zorg op de schouders van de artsen neerkomt. Omdat deze relatie ook niet duidelijk op een plek staat, moeten de artsen in sommige situaties veel moeite doen om dit uit te zoeken. Dit leidt ertoe dat de gezagsrelatie zomaar wordt aangenomen of verondersteld om maar de zorg te kunnen verlenen, wat natuurlijk de primaire taak is van het medisch personeel. Hierdoor wordt het wettelijke gezag echter niet altijd op de juiste wijze vastgesteld. De medische sector zou er bij gebaat zijn als de gezagsrelaties makkelijk en betrouwbaar te bewijzen zijn. Om de gezagsrelatie te bewijzen is er informatie nodig uit de BRP en het openbaar gezagsregister. Hier zijn namelijk alle gezagsrelaties uit te halen, zie hiervoor hoofdstuk 2.4. Er is dus een systeem nodig wat dit uit de BRP en het gezagsregister haalt, en vervolgens aan de arts presenteert. Dit maakt het nagaan van de gezagsverhoudingen voor de arts eenvoudiger en betrouwbaarder. De pilot van Nictiz, die in hoofdstuk 3.3.3 behandeld is, gebruikt de DigiD van moeders om dossiers van hun minderjarige kinderen in te zien. Hierbij gebruikte Nictiz een nieuw ontwikkelde machtigingsprocedure waarbij het gezag van de moeder gecontroleerd kan worden. Omdat deze pilot echter nog steeds bezig is, is het nog niet mogelijk om vast te stellen of dit een effectieve manier is voor de gezagsverificatie. Daarnaast zou dit alleen nog maar het verificatie probleem op het medische gebied oplossen, voor bijvoorbeeld de verkoop van alcohol is DigiD een verificatiemiddel wat meer dan alleen strikt noodzakelijke informatie geeft.

4.1.4 Leeftijd en gezagsrelaties worden niet geverifieerd door sociale media

In hoofdstuk 3.4 viel op dat sociale media zich niet volledig aan de AVG houden op het gebied van verwerking van gegevens van minderjarigen. Uit de behandelde sociale media kwamen een aantal gevallen waar de minimumleeftijdsgrenzen niet gehanteerd werd, of de controle van het ouderlijk gezag bleef achterwege. Een verklaring die de NOS voor deze gebreken geeft, is dat een aantal sociale media niet zozeer een professionele uitstraling hoeven te hebben vanwege de jeugdige doelgroep.[4] Een bedrijf als Facebook, wat een oudere doelgroep en bovendien ook bedrijven als gebruikers heeft, steekt wél meer moeite in het controleren van de ouderlijke toestemming. Dit zal ook zeker bijdragen aan de mate van professionaliteit die Facebook wenst uit te dragen naar haar gebruikers. Verschillende sociale media gaan er echter

[4] `https://nos.nl/artikel/2231111-kinderen-geweerd-van-instagram-maar-is-dat-wel-nodig.html`

eenvoudigweg vanuit dat de leeftijd eerlijk wordt ingevuld.[5] Dit terwijl de drempel voor een minderjarige om te liegen over zijn leeftijd laag is, omdat hij anders misschien geen gebruik zou kunnen maken van het medium. Een voorbeeld van een sociaal medium wat hier geen rekening mee lijkt te houden is Instagram. Instagram verwacht dat de meeste mensen eerlijk zijn over hun leeftijd, en voor de resterende groep zou het bedrijf Artificial Intelligence in kunnen zetten.[6] De AI zou felicitaties aan gebruikers lezen, en daaruit kunnen afleiden hoe oud iemand is. Dit wordt echter nog niet in de praktijk ingezet. Als Instagram erachter komt dat een gebruiker nog geen 16 jaar is, en ook geen toestemming van ouders heeft, dan wordt het account verwijderd.[7] Het is echter, met de huidige maatregelen die Instagram inzet, zeker niet gegarandeerd dat alle minderjarigen op het netwerk zullen worden opgespoord. Of het gebruik van AI zou helpen om minderjarigen van het sociale medium te weren zal de praktijk nog moeten leren.

Een mogelijke oplossing om online het opgeven van onjuiste leeftijden tegen te gaan, is het invoeren van een digitale identiteit. In veel voorstellen voor zo'n identiteit gaat het in feite om een digitale versie van de identiteit die we momenteel al gebruiken (zoals paspoort of id-kaart).

Op het moment zijn er een viertal pilots voor een vorm van een digitale identiteit.[8] Deze pilots lopen nog en moeten in 2020 geëvalueerd worden voor er verdere stappen kunnen worden ondernomen. Het is belangrijk dat deze initiatieven niet zoveel inbreuk doen op de privacy van de gebruiker zoals het fysieke legitimatiemiddel nu wel doet.[9] Een voorbeeld hiervan is het tonen van een fysiek identiteitsbewijs aan de kassa, sectie 4.1.5 gaat hier dieper op in.

Een andere geschikte manier van digitale identificatie zou gebaseerd zijn op 'attribute-based authentication.'[10] Hierbij toont een gebruiker niet zijn hele identiteit, maar alleen de eigenschap die aangetoond moet worden. Er wordt dus minder informatie van de gebruiker weggeven, dit wordt ook wel 'dataminimalisatie' genoemd. Dataminimalisatie wordt vereist in de AVG en zorgt voor een beter beschermde privacy van de gebruikers doordat alleen de noodzakelijke gegevens verwerkt worden.[11]

[5] https://www.reuters.com/article/us-facebook-instagram-children/instagram-to-collect-ages-in-leap-for-youth-safety-alcohol-ads-idUSKBN1Y826Z

[6] https://www.reuters.com/article/us-facebook-instagram-children/instagram-to-collect-ages-in-leap-for-youth-safety-alcohol-ads-idUSKBN1Y826Z

[7] https://nos.nl/artikel/2231111-kinderen-geweerd-van-instagram-maar-is-dat-wel-nodig.html

[8] https://www.vngrealisatie.nl/onderwerpen/digitale-identiteit

[9] https://digitaleidentiteit.waag.org/artikel/wat-is-er-eigenlijk-mis-met-digitale-identiteit/

[10] https://digitaleidentiteit.waag.org/artikel/tools-voor-digitale-identiteit-hoe-wat-waarom/

[11] AVG 5.1c

4.1.5 Leeftijdsverificatie door middel van de geboortedatum is niet privacy-vriendelijk

In alle situaties die behandeld zijn in de voorgaande hoofdstukken, van alcoholverkoop tot het gebruik van sociale media, wordt er gebruik gemaakt van een leeftijdsverificatie waarbij de geboortedatum door de gebruiker moet worden ingevoerd. Aan de hand daarvan wordt dan berekend hoe oud de persoon is. De berekende leeftijd wordt vervolgens met de vereiste leeftijd vergeleken, en aan de hand daarvan wordt bepaald of de gebruiker oud genoeg is of niet. Het nadeel aan deze manier van verifiëren is dat de volledige geboortedatum wordt gebruikt. Voor alle vormen van verificatie van leeftijd die hier eerder besproken zijn, geldt echter dat de exacte geboortedatum niet nodig is. Het is alleen nodig om te weten of iemand een bepaalde leeftijd bereikt heeft. De complete geboortedatum laat meer zien dan alleen de leeftijd van die persoon. Er wordt dus op deze manier meer persoonlijke informatie weggegeven dan strikt noodzakelijk is.

Omdat de geboortedatum dus persoonlijke informatie is, is er het gevaar dat deze informatie misbruikt kan worden. Hoewel de geboortedatum op zichzelf nergens voor misbruikt kan worden, is het wel een stukje informatie dat met andere persoonlijke gegevens te combineren zou zijn die openbaar op het internet staan.[12] Een geboortedatum kan dan een missend stukje in de puzzel zijn om bijvoorbeeld iemands identiteit te stelen.[13] Wat echter voor de meeste internetgebruikers gevaarlijker zal zijn, is dat een geboortedatum vaak gebruikt wordt als wachtwoord of als security question om wachtwoorden te resetten.[14] Als een aanvaller dan de geboortedatum in handen krijgt, heeft hij dus waarschijnlijk toegang tot accounts van die persoon. Het is daarom beter om het gebruik van een geboortedatum voor verificatie zoveel mogelijk te beperken.

Uit wat hierboven behandeld is komt naar voren dat een digitale identiteit hiervoor een oplossing kan zijn. Hier worden bepaalde eigenschappen van een persoon door vertrouwde instanties in vastgelegd. Het laatste deel van dit onderzoek zal zich richten op een attribute-based credentials systeem waarmee dit geïmplementeerd kan worden.

4.2 Attribute-based credentials systemen

In sectie 4.1.4 werd al kort het begrip attribute-based authentication genoemd, waarbij gezegd werd dat een gebruiker hiermee enkel een bepaalde

[12] `https://defendingdigital.com/dont-share-your-birth-date-online/`

[13] `https://clark.com/technology/how-your-facebook-profile-can-lead-to-identity/`

[14] `https://www.howtogeek.com/402929/why-its-dangerous-to-share-your-birthday-online/`

eigenschap laat zien zonder daarmee een groter deel van zijn identiteit openbaar te maken[9]. Deze sectie zal nader toelichten hoe dit principe werkt. Een attribute-based credentials systeem (ABC) heeft doorgaans een coördinerende eenheid die 'issuers' aanstelt om 'credentials' uit te geven aan gebruikers, welke dan gebruikt kunnen worden om eigenschappen te bewijzen naar 'verifiers.'[15] Een issuer is dus de partij die de gegevens over de gebruiker bezit, en deze gegevens vervolgens aan de gebruiker beschikbaar stelt om te gebruiken als attributen tegenover verifiers. De issuer geeft deze attributen uit in een *credential*. Een voorbeeld van een verifier is de supermarkt, wanneer de caissière wil controleren of de klant ouder is dan 18 jaar. In dat voorbeeld kan de BRP de issuer van het attribuut 'ouder dan 18 jaar' zijn. De gebruiker hoeft nu niet een identiteitsbewijs te tonen waar nog veel overbodige persoonlijke informatie mee zou worden weggegeven; enkel het selectief tonen van een of meerdere eigenschappen die de persoon bezit is afdoende. Door het weglaten van overbodige informatie wordt de privacy van de gebruiker hier dus beter gewaarborgd.

Attributen zijn grofweg in te delen in twee categorieën. Sommige attributen zijn terug te leiden naar een specifiek persoon; dit geldt bijvoorbeeld voor banknummers en BSN's, deze zijn namelijk uniek voor elke persoon[9]. Als zulke attributen getoond moeten worden is de gebruiker dus niet anoniem. Er zijn echter ook attributen die niet zijn terug te leiden naar een specifiek persoon; voorbeelden hiervan zijn 'geslacht', 'woonplaats' en 'ouder dan 18 jaar.' Meerdere mensen hebben deze eigenschappen en daarom kan met alleen die informatie niet achterhaald worden wie deze gegevens getoond heeft. Voor beide categorieën van attributen is een ABC nuttig om te gebruiken. Een ABC maakt het namelijk moeilijker om meerdere attributen samen te voegen tot een profiel van elke gebruiker. Als zo'n profiel wel opgesteld zou kunnen worden, zouden attributen niet meer anoniem gebruikt kunnen worden. Om de privacy goed te waarborgen is het dus verstandig om een ABC te gebruiken om daarmee de anonimiteit van de gebruiker te beschermen.

Sectie 4.1.4 noemde al kort dat er vier pilots lopen die gericht zijn op een vorm van een digitale identiteit. Hier willen we verder onderzoeken hoe een van die pilots, het IRMA-platform, kan bijdragen aan het verifiëren van de gezagsrelatie. Het is niet mogelijk om alle vier de pilots dieper te onderzoeken, dus uiteindelijk is de keuze gevallen op IRMA omdat dit een platform een grote potentie heeft als oplossing.

[15] `https://privacypatterns.org/patterns/Attribute-based-credentials`

4.3 IRMA

Om de leeftijd en gezagsrelaties te bewijzen voor de situaties die in de voorgaande hoofdstukken beschreven zijn, kijken we naar het identiteitsplatform IRMA.[16] IRMA is een afkorting die staat voor 'I Reveal My Attributes.' Het is een privacy-vriendelijk platform waarin een gebruiker attributen kan gebruiken om bepaalde eigenschappen te bewijzen zonder daarbij zijn identiteit te tonen. IRMA is een attribute-based authentication systeem, gebaseerd op het IBM Idemix scheme[11, 12].

Figuur 4.1: Gebruik van IRMA

Zonder op de details van Idemix in te gaan, is het van belang voor dit onderzoek dat IRMA hierdoor een decentrale structuur heeft. Een centrale structuur laat alle handelingen via een vertrouwde partij gaan. Daartegenover is in een decentrale structuur geen vertrouwde centrale partij meer nodig; alle handelingen gaan dan via de gebruiker. Zo worden in IRMA daarom de credentials opgeslagen in de app van de gebruiker, en niet op een centrale server. Hierdoor zijn de issuers en de gebruikers zelf de enigen die credentials in handen hebben. Dit is het minimale aantal partijen dat deze informatie moeten hebben, en daardoor zorgt een decentrale structuur voor meer privacy voor de gebruikers. Vanwege de decentrale structuur beheert de gebruiker zelf zijn credentials, waardoor hij niet afhankelijk is van de server in het aanvragen en tonen van attributen uit zijn verzameling van credentials.

4.3.1 De verschillende partijen van een ABC in de context van IRMA

Zoals in 4.2 beschreven is, zijn er vier relevante partijen in een attribute-based credentials systeem en dus ook in IRMA. Alle vier partijen zullen hier

[16] `https://privacybydesign.foundation/irma/`

nu uitgewerkt worden. De credentials worden in IRMA aan de gebruikers uitgegeven door de *issuers*. Elke partij die betrouwbare gegevens heeft over mensen kan in principe een issuer zijn of worden. De issuer staat garant voor de juistheid van de gegevens die hij verstrekt. Elk credential dat een issuer uitgeeft, wordt voorzien van een verloopdatum, en wordt vervolgens cryptografisch ondertekend met de private key van de issuer. Hiermee wordt de betrouwbaarheid van het credential bevestigd. De tweede partij die een rol speelt in IRMA zijn de *gebruikers*, die zojuist al kort aan bod zijn gekomen. Gebruikers verzamelen hun credentials, die ze van de issuers krijgen, in de IRMA app. Als de gebruiker credentials in de app heeft zitten, kunnen deze gebruikt worden om bewijs te leveren van een eigenschap naar de verifiers. De *verifiers* vragen om bepaalde attributen om gebruikers toegang te geven tot de diensten die de verifiers aanbieden. Zo kan een verifier bijvoorbeeld vragen om de woonplaats van de gebruiker. De gebruiker kan dit attribuut bewijzen door de QR-code te scannen die door de verifier getoond wordt. Door de QR-code te scannen weet de app welk attribuut bewezen moet worden, en bewijst het in dit voorbeeld enkel het woonplaats-attribuut. Andere attributen die de gebruiker mogelijk in de app heeft staan zijn op dat moment niet zichtbaar voor de verifier. De verifier controleert vervolgens de handtekening van de issuer op het attribuut, en of het attribuut nog steeds geldig is. Als hieraan voldaan is, geeft de verifier toestemming tot het gebruik van zijn dienst. De laatste partij die een rol speelt in IRMA is de stichting *Privacy by Design*. De stichting ontwikkelt IRMA, doet onderzoek gerelateerd aan IRMA en zorgt ervoor dat de IRMA app functioneert. Tevens kan de stichting zelf ook credentials uitgeven. Tenslotte wordt de IRMA server door de stichting beheerd. Deze server speelt een cruciale rol in het verzorgen van sessies wanneer er credentials verstrekt of gebruikt worden.

4.3.2 Eigenschappen van credentials in IRMA

Nu zal nog worden ingegaan op wat credentials in de context van IRMA zijn. Er is in de voorgaande sectie al genoemd dat credentials een vooraf bepaalde verloopdatum kunnen hebben. Deze datum is bedoeld om te voorkomen dat verstreken credentials nog steeds voor authenticatie zouden worden gebruikt. In IRMA wordt er momenteel ook gewerkt aan een manier om credentials voortijdig te herroepen.[17] Een issuer zou dit kunnen gebruiken om onverwacht ongeldig geworden credentials te blokkeren zodat ze niet meer gebruikt kunnen worden voor authenticatie terwijl ze ongeldig zijn. Er kan bijvoorbeeld gedacht worden aan een attribuut als 'woonplaats', wat bij een verhuizing kan veranderen. Het is in de praktijk vaak niet mogelijk dat er bij uitgifte van dat specifieke attribuut 'woonplaats' al een termijn bekend

[17] `https://irma.app/docs/revocation/`

is hoelang dit geldig is, daarom kan een herroeping van het attribuut hier nodig zijn. Zo zijn er meer attributen waarvoor het nodig kan zijn om ze onverwacht in te kunnen trekken zodra ze onjuist geworden zijn. Dit geldt bijvoorbeeld ook voor het gezagscredential. Als het kind meerderjarig geworden is, en bekwaam om zelf de vroegere taken van de gezagsdrager(s) op zich te nemen, dan is het gezagscredential niet meer geldig. Het gezagscredential moet dan dus ook herroepen kunnen worden.

Als de gebruiker doorheeft dat een credential vernieuwd of aangepast moet worden, dan kan hij zelf opnieuw dat specifieke credential opvragen. In zulke gevallen is er geen noodzaak om credentials te kunnen herroepen. Het herroepen van credentials is wel nuttig als de gebruiker, bewust of onbewust, gebruik blijft maken van een ongeldig credential. Dan kan het credential geblokkeerd worden zonder tussenkomst van de gebruiker.

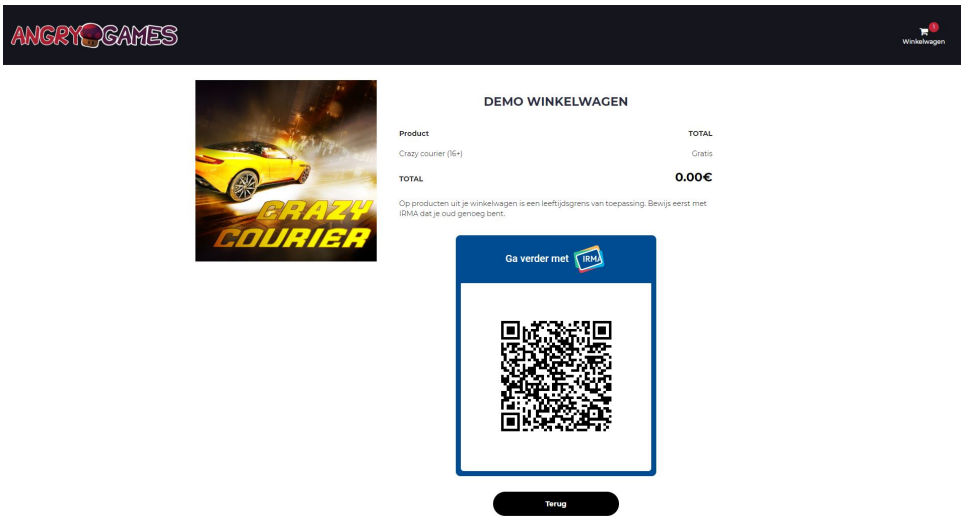
Belangrijke kenmerken in IRMA zijn de 'issuer unlinkability' en 'multi-show unlinkability.' Het eerste houdt in dat een issuer niet kan zien waar de gebruiker zijn attributen laat zien. Het tweede garandeert dat het meerdere malen tonen van hetzelfde attribuut niet zal leiden tot een koppeling van het gebruik van het attribuut aan een persoon. Dit geldt natuurlijk alleen voor attributen die niet uniek zijn, want een unieke eigenschap zoals BSN is altijd één op één terug te leiden op een persoon. Deze twee eigenschappen in IRMA met betrekking tot attributen geven dus een mate van anonimiteit aan de gebruiker, wat een gewenste eigenschap is voor de uiteindelijke oplossing voor gezagsverificatie.

4.3.3 Hoe IRMA past in dit onderzoek

Ten slotte zal nu behandeld worden hoe IRMA gebruikt kan worden om leeftijd en gezagsrelaties, zoals die behandeld zijn in hoofdstuk 2, te verifiëren. Omdat IRMA gebaseerd is op authenticatie door middel van attributen, moeten er dus attributen zijn die leeftijd en gezagsrelaties kunnen bewijzen. IRMA haalt al de geboortedatum en attributen die aangeven of de persoon ouder is dan 12, 15, 18 of 65 uit een credential dat afkomstig is van de Basisregistratie Personen. Met die informatie kan de IRMA app dus bewijzen dat iemand een bepaalde leeftijd bereikt heeft. Dit is iets wat al geïmplementeerd is in IRMA. Er is echter geen druk op organisaties om daadwerkelijk deze techniek toe te passen. Om dat te veranderen zou de overheid het moeten bevorderen om dit in de praktijk in te zetten. Hiermee zou de leeftijdsverificatie in de alcohol- en gamesverkoop opgelost kunnen worden.

Om te illustreren wat er mogelijk is in IRMA zal nu een voorbeeld bestudeerd worden van een demo van een webshop met games met een leeftijdsrestrictie.[18] Op de pagina waar de game gekocht kan worden wordt een

[18] `www.angrygames.nl`

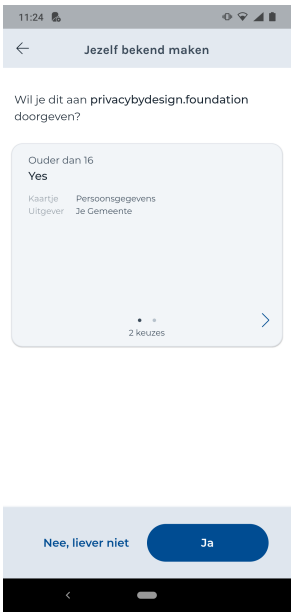


Figuur 4.2: Winkelpagina van de game met leeftijdsrestrictie

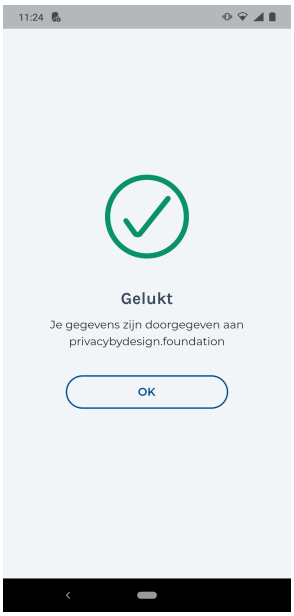
QR-code getoond, zie figuur 4.2. De instructies op de pagina geven aan dat IRMA gebruikt moet worden om te bewijzen dat de koper de vereiste leeftijd bereikt heeft.

De gebruiker opent dan de IRMA app op zijn telefoon. Daar krijgt hij te zien wat in figuur 4.3 is getoond. In deze app is te zien dat de gebruiker een IRMA-kaartje met de titel 'Persoonsgegevens' heeft. Dit kaartje bevat attributen over de leeftijd van de gebruiker en kan daarom gebruikt worden voor deze demo.

Figuur 4.3: De IRMA app



Figuur 4.4: Na scannen van de QR-code

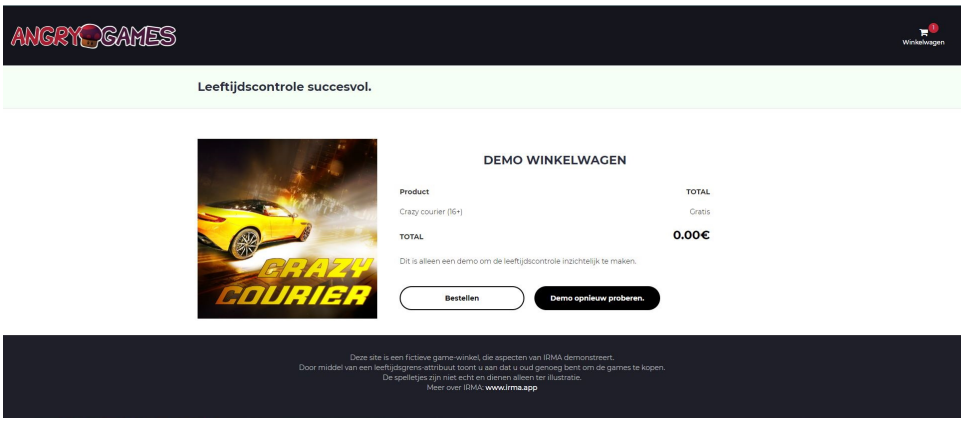


Figuur 4.5: Verificatie geslaagd

Om de QR-code te scannen moet de gebruiker op het icoontje rechts onderin het scherm klikken. Als de code gescand is krijgt de gebruiker de gegevens te zien die doorgegeven moeten worden. Zie hiervoor figuur 4.4. Hier kan de gebruiker nog kiezen om de verificatie niet te laten doorgaan als hij vindt dat er teveel gegevens voor de verificatie gebruikt zouden worden. Als de gebruiker akkoord gaat en hij is oud genoeg voor de game, dan krijgt hij het scherm te zien wat in 4.5 is weergegeven. De verificatie is dan gelukt. Vervolgens kan de gebruiker weer terug naar de website. De website weet dan dat de gebruiker oud genoeg is. Dan kan dus uiteindelijk de game aan de gebruiker verkocht worden, dit is weergegeven in figuur 4.6.

Deze demo laat zien dat het verkopen van games met een leeftijdsrestrictie in IRMA al mogelijk is. Voor deze verificatie was slechts het attribuut 'ouder dan 16' nodig, zonder daarbij meer gegevens te laten zien. Dit maakt IRMA interessant voor dit onderzoek omdat hiermee de problemen rondom de alcohol- en gamesverkoop al grotendeels verholpen kunnen worden.

Met betrekking tot de gezagsrelaties is er nog geen bestaand credential in IRMA wat daarvoor gebruikt zou kunnen worden. Zoals in sectie 2.4 getoond is, staan de gezagsrelaties zowel gedeeltelijk in de BRP als gedeeltelijk in het openbaar gezagsregister geregistreerd. Er zou dus een issuer bij moeten komen om alle gezagsrelaties in kaart te kunnen brengen. Naar deze issuer zal in deze scriptie echter niet gezocht worden. In het volgende hoofdstuk zal wel onderzocht worden welke rol IRMA kan spelen als alle gezagsrelaties bij elkaar op één plek gebracht zijn.



Figuur 4.6: Verificatie geslaagd

Er zijn in dit hoofdstuk een aantal verbeterpunten gepasseerd rondom leeftijds- en gezagsverificatie. We hebben gezien dat de meeste van deze punten in een attribute-based credentials systeem, en dan specifiek IRMA, opgelost kunnen worden. Met name bij de leeftijdsverificatie rondom gameverkoop zagen we echter dat de overheid nog maar weinig aan handhaving van de wettelijke eisen doet. Het is dus ook van belang dat de overheid in beweging komt op dit gebied door hier meer sturing in te geven.

Hoofdstuk 5

Een protocol voor verificatie gebaseerd op IRMA

In het voorgaande hoofdstuk is onderzocht waar de probleempunten rondom leeftijds- en gezagsverificatie liggen, en hoe deze opgelost kunnen worden. Specifiek is onderzocht welke rol IRMA in deze oplossing zou kunnen spelen. Dit hoofdstuk zal hier verder op ingaan. Er zal onderzocht worden hoe het protocol van gezagsverificatie eruit kan zien met gebruik van IRMA. Hierbij wordt de aanname gemaakt dat er een centraal punt is waar alle gezagsrelaties toegankelijk zijn en dat deze in credentials uitgegeven kunnen worden. Met die aanname kan dit onderzoek volledig op het protocol van verificatie focussen zonder afgeleid te worden door hoe de gezagsrelaties bij elkaar op een centrale plek beschikbaar zijn. De nadruk zal in dit hoofdstuk liggen op het onderzoeken van de keuzemomenten die zich voordoen in de procedure van de gezagsverificatie.

5.1 De registratie van het gezagscredential

Zoals hierboven al beschreven is, wordt de aanname gemaakt dat er een centraal punt is waar de gezagsrelaties toegankelijk zijn. Dit centrale punt kan daarmee functioneren als de issuer van het gezagscredential in IRMA. Er wordt ook vanuit gegaan dat dit centrale punt in de vorm van een website beschikbaar is, zodat de gebruikers na passende authenticatie eenvoudig het gezagscredential kunnen ophalen zonder fysiek aanwezig te hoeven zijn. Het centrale punt bevat veel persoonsgegevens over gezagsdragers en minderjarigen. Veel van deze gegevens komen rechtstreeks uit de BRP, het is daarom aan te bevelen om dit centrale punt ook door de overheid te laten beheren. Het gezagscredential wordt vanuit het centrale punt aan de gebruikers verstrekt, waarna de gebruikers dit credential op allerlei plaatsen in kunnen zetten. Er is sprake van een groot aantal partijen waar dit credential potentieel ingezet kan worden. Zeker omdat er van gezag eenvoudig misbruik

gemaakt kan worden door de gezagsdrager is het essentieel om het gebruik van het credential vast te leggen in de centrale site. Sectie 5.4 zal hier nog verder op ingaan.

Het verkrijgen van het gezagscredential in de IRMA app gaat op de manier zoals deze in 4.3.1 al beschreven is. Bij de mogelijkheid van het opvragen van het credential rijst al direct de vraag welke personen dit credential mogen opvragen. De twee potentiele gebruikers van het gezagscredential zijn de gezagdrager(s) en de minderjarige. Er zijn verschillende soorten gezagsdragers, zoals behandeld is in sectie 2.3. De gezagsdragers moeten het gezag kunnen bewijzen als zij handelingen met betrekking tot de minderjarige willen uitvoeren. Een voorbeeld hiervan is het nemen van medische beslissingen (zie hiervoor sectie 2.7). Het gezag heeft echter vanzelfsprekend ook veel te maken met de minderjarige. Daarom zou de minderjarige ook een interesse in dit gezagscredential kunnen hebben. Er zijn echter geen situaties bekend waar het de minderjarige daadwerkelijk moet kunnen aantonen wie zijn gezagsdragers zijn. Daarom is het vooralsnog beter om het gezagscredential alleen aan de gezagdragers te verstrekken. Wel is het redelijk om de minderjarige inzage te geven in het gebruik van deze gezagsattributen. Hier zal sectie 5.4.1 verder op ingaan.

5.1.1 Het gezagscredential

Vervolgens is het de vraag welke attributen er in een gezagscredential moeten zitten. Er moet van zowel de minderjarige als de bijbehorende gezagsdrager een identificerende eigenschap in zitten. De eigenschappen die hier het meest bruikbaar zijn, zijn de voornamen samen met de achternaam en het BSN van minderjarige en gezagsdrager. Een combinatie van voor- en achternaam is echter niet altijd uniek. Toch is de naam een bruikbaar identificatiemiddel in situaties waar het niet toegestaan is om het BSN te gebruiken. Door zowel de naam als het BSN van de minderjarige en de gezagsdrager in het credential te plaatsen kan per situatie de beslissing genomen worden om een van beide te gebruiken. In gevallen waar een perfecte identificatie nodig is, zoals in de medische sector, kan dan het BSN gebruikt worden. In de situaties waar dit niet noodzakelijk of wettelijk niet toegestaan is kan er worden volstaan met de namen.

Verder moet het credential ook een uniek nummer of ID hebben. Een gezags-ID is nodig om het gebruik van het credential te registreren, zonder daarbij direct persoonsgegevens te hoeven registreren. Hiermee kan het gebruik van het credential dus op een meer anonieme manier worden vastgelegd.

De beschreven verificatieproblemen in de voorgaande hoofdstukken hebben ook met de leeftijd van de kinderen te maken. Er is immers noodzaak voor gezagsverificatie als kinderen nog niet oud genoeg zijn om zelfstandig handelingen uit te voeren. Omdat de leeftijd rondom gezagsverificatie belangrijk

is, is het nuttig om de geboortedatum van het kind ook in het gezagscredential te plaatsen. Met deze geboortedatum kunnen dan een aantal attributen in het credential worden toegevoegd die aangegeven of het kind ouder is dan 12, 16 of 18 jaar. In hoofdstuk 2 is naar voren gekomen dat deze drie leeftijden alle gebruikelijke grenzen beschrijven die gehanteerd worden bij leeftijdsverificatie. Als een 15-jarig kind dan een account op sociale media wilt aanmaken, ziet de verifier aan het attribuut dat het kind niet ouder is dan 16. Dan heeft de verifier dus nog de toestemming van de gezagsdrager nodig. Als het echter om een 17-jarig kind gaat, dan weet de verifier dat het kind oud genoeg is om zelfstandig een account aan te maken en is de toestemming van de gezagsdrager niet nodig. Door de geboortedatum, en daarmee de "ouder dan" attributen, toe te voegen krijgt de verifier de benodigde informatie over de leeftijd.

Het credential moet ook een attribuut hebben waarin staat om wat voor volmacht het gaat. Dit is nuttig voor als het credential voor meer zaken dan alleen het gezag over minderjarigen gebruikt zou worden. In dit attribuut zou er een tweedeling gemaakt kunnen worden tussen ouderlijk gezag en gezag dat door tussenkomst van een rechter ontstaan is. Ouders en wettelijke vertegenwoordigers zijn echter bevoegd tot dezelfde gezagsuitoefeningen, een dergelijke tweedeling is daardoor niet noodzakelijk. Daarom heeft het de voorkeur om in het machtigingsattribuut alleen te vermelden dat het om gezag over een minderjarige gaat, waarmee beide vormen van gezag bedoeld zijn. Anders zou dat attribuut onnodig informatie weggeven over welke vorm de gezagsrelatie is, wat niet voldoet aan het principe van dataminimalisatie uit artikel 5.1 van de AVG. Ten slotte is er nog het attribuut dat de verloopdatum van het credential aangeeft. Hieronder is te zien hoe het credential er met al deze attributen schematisch komt uit te zien.

Machtigings-ID	Naam kind	BSN kind	Naam ouder	BSN ouder	Type machtiging	Verloop-datum	Geboorte-datum kind	Kind >12 jaar	Kind >16 jaar	Kind >18 jaar
123	Bob	456	John	789	Gezag	1-1-2021	1-1-2008	Ja	Nee	Nee

Figuur 5.1: Het gezagscredential

In sectie 4.3.2 is al genoemd dat het gezagscredential moet kunnen worden opgeheven zodra het kind meerderjarig wordt en zelf verantwoordelijkheid kan gaan dragen. Het is mogelijk om de verloopdatum te zetten op de achttiende verjaardag van de minderjarige in kwestie. Hieruit kan echter de geboortedatum achterhaald worden omdat die datum dan in het credential staat. Bovendien zou het gezag ook voor de achttiende verjaardag al niet meer geldig kunnen zijn door tussenkomst van een rechter, het zetten van de verloopdatum op die verjaardag heeft dan weinig nut. Het is beter om het gezagscredential voor een vaste tijdsduur uit te geven. Hierin kan

een voorbeeld genomen worden aan de BRP attributen in IRMA, die een geldigheidsduur van vijf jaar hebben. Dezelfde termijn kan ook voor het gezagscredential ingesteld worden. Als het credential al binnen die termijn vervangen moet worden omdat er een andere gezagsverhouding gekomen is, dan kan de issuer het credential alsnog herroepen. Over deze mogelijkheid is in sectie 4.3.2 al gesproken. Aan het credential wat de gezagsdrager heeft is dan te zien dat het herroepen is, en daarom niet meer gebruikt mag worden. Voor de nieuwe gezagsrelatie zou de gebruiker dan opnieuw het credential bij de issuer moeten ophalen.

Als het kind inmiddels meerderjarig is, en tevens bekaam is om zelf de verantwoordelijkheid van zijn vertegenwoordiger(s) over te nemen, moet het credential ook herroepen worden. Omdat er dan geen sprake meer is van een gezagsverhouding kan de gezagsdrager vervolgens niet een nieuwe variant van het credential opvragen. De gezagsdrager kan dan geen handelingen meer uitvoeren voor het kind. De verifier weet vervolgens alleen dat het credential herroepen is, maar niet de oorzaak hiervan. Er wordt hiermee dus geen informatie over de geboortedatum of leeftijd van het kind verstrekt want de verifier weet niet de exacte datum waarop het credential herroepen is.

5.1.2 Meerdere gezagsrelaties per persoon

Tot nu toe is nog niet behandeld wat er gebeurt als een minderjarige meerdere gezagsdragers heeft. Andersom zou het ook kunnen dat een ouder of wettelijke vertegenwoordiger het gezag heeft over meerdere minderjarigen. Het is belangrijk om deze situaties helder te definiëren in het verificatieproces omdat dergelijke gevallen veelvuldig voorkomen. Hierboven is al genoemd dat het gezagscredential de relatie tussen een minderjarige en een gezagsdrager vastlegt. Ook hebben al deze een-op-een relaties een uniek ID, waarmee dus elke gezagsdrager-minderjarige relatie beschreven kan worden. Als er bijvoorbeeld drie mensen het gezag over dezelfde minderjarige hebben, dan zijn er drie afzonderlijke gezagscredentials. Dit geldt ook voor situaties waar één gezagsdrager het gezag heeft over meerdere minderjarigen. Doordat elke relatie tussen een gezagsdrager en een minderjarige een eigen credential heeft, is het mogelijk om deze relaties uit elkaar te houden. Op die manier kan dan geregistreerd worden voor welke minderjarige en door welke gezagsdrager er gebruikt gemaakt wordt van het gezag. Dit is van belang voor het bijhouden van een logboek, sectie 5.4 zal daar verder op ingaan.

5.2 Het gebruik van het gezagscredential in de medische sector

Nu in het voorgaande gedeelte alles behandeld is rondom het opzetten van het gezagscredential, zal deze sectie toegespitst zijn op hoe het credential vervolgens gebruikt kan worden. Er zal worden gewerkt met een voorbeeld van een gezagsdrager met een gezagscredential waarin de gezagsrelatie met betrekking tot een minderjarig kind staat uitgewerkt. Als verifier aan wie de attributen uit het credential getoond worden, nemen we hier een digitaal portaal van een ziekenhuis. Er is gekozen voor een casus met een ziekenhuis omdat die nauw aansluit bij de behandelde situaties uit de eerdere hoofdstukken. Sectie 5.3 zal de situatie behandelen waar een gezagsdrager toestemming moet geven voor de registratie van een minderjarige bij een sociaal medium.

5.2.1 Gebruik van het gezagscredential in de medische sector

Figuur 5.2: Gebruik van het gezagscredential door een gezagsdrager richting een portaal van een ziekenhuis

Er is een gebruiker die het gezagscredential wil gebruiken om aan te tonen dat hij de verantwoordelijkheid over een minderjarig kind draagt. Dit zal er uiteindelijk op moeten uitlopen dat de gezagsdrager toestemming krijgt om voor het kind bepaalde handelingen via het portaal van de verifier uit te voeren. Om die handelingen te kunnen uitvoeren moet de dienstverlener weten voor welke minderjarige de handelingen uitgevoerd moeten worden. Zoals hierboven in sectie 5.1.1 al is aangetoond is het in de medische sector noodzakelijk om het BSN te gebruiken als identificatiemiddel vanwege de unieke identificatie die vereist is. De ouder hoeft geen identificatie van zichzelf te geven, het machtigings-ID impliceert immers dat er een gemachtigde is. Omdat er verder alleen met de gegevens van de minderjarige handelingen worden uitgevoerd, heeft het geen toevoegde waarde om gegevens over de gezagsdrager te laten zien.

Een ander essentiele eigenschap die getoond moet worden is het machtigings-ID, het unieke nummer wat elk gezagscredential heeft. De verifier kan de handelingen van de gezagsdrager registreren door ze te koppelen aan dit ID en dat op te slaan in zijn database. Hiervoor hoeven geen persoonsgegevens van de gezagsdrager opgeslagen te worden, het machtigings-ID is voldoende om te verwijzen naar de bijbehorende gezagsdrager. Op die manier zijn uit de registratie van de verifier niet direct persoonsgegevens van de gezagsdrager af te leiden.

Tenslotte zou de gebruiker ook nog kunnen laten zien om wat voor type machtiging het gaat. Dit kan handig zijn voor de verifier, omdat de verifier wellicht verschillende diensten aanbiedt voor verschillende soorten machtigingen.

5.2.2 Hoe het ziekenhuisportaal weet of de gegevens geldig zijn

Nu bevindt het protocol zich in de situatie waar het portaal zojuist het eerste contact met de gebruiker heeft gehad, en van hem gegevens heeft gekregen over de minderjarige en het bijbehorende machtigings-ID. De verifier kan van het credential zien of het door de issuer herroepen is of niet. Als daarbij nog niet de verloopdatum van het credential bereikt is gaat het dus om een geldig gezagscredential. De verifier heeft geen controlestap met de issuer nodig om deze conclusie te bereiken omdat het protocol berust op het feit dat ongeldige attributen direct herroepen worden. Ook hoeft de verifier niet te controleren of de combinatie van machtigings-ID, gezagsdrager en minderjarige correct is. Er mag namelijk worden verondersteld dat de attributen in IRMA alleen aan de juiste personen uitgereikt worden. Daardoor kan een gebruiker per definitie niet een gezagscredential bezitten wat hem niet toebehoord.

5.2.3 Hoe wordt omgegaan met de gegevens van de gezagsdragers?

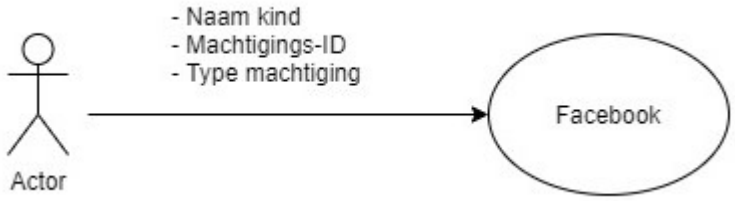
In het protocol voor de medische sector valt op dat er geen gegevens van de gezagsdrager nodig zijn voor het ziekenhuisportaal. Aan het portaal is een geldig ID getoond door de gezagsdrager, samen met gegevens over de minderjarige. Het ziekenhuis hoeft niet te weten wie de specifieke gezagsdrager is. De handelingen van de gezagsdrager hebben namelijk betrekking tot de gegevens van de minderjarige, daarom zijn alleen de gegevens van de minderjarige nodig. Handelingen waar toestemming van de gezagsdrager voor nodig zijn, zijn geautoriseerd doordat er een geldig machtigings-ID aanwezig is. Het ID impliceert namelijk dat de gebruiker gemachtigd is om dat gezag uitvoeren. Nadat de sessie is afgelopen hoeft de verifier enkel de gegevens van de minderjarige en het machtigings-ID op te slaan. De verifier moet nog wel het gebruik van het machtigings-ID doorgeven aan de centrale website

zodat dit bij de centrale site geregistreerd kan worden (zie hiervoor sectie 5.4). Alle handelingen die door de gezagsdrager gedaan zijn worden dan opgeslagen op naam van de minderjarige. Het voordeel hieraan is dat de handelingen niet aan een specifieke gezagsdrager verbonden zijn. Hierdoor kunnen eventuele andere gezagsdragers van de minderjarige ook het gezag uitoefenen zonder daarbij andere de gezagsdragers te hinderen.

5.3 Gebruik van het gezagscredential bij registratie sociale media

Nu volgt nog een uitwerking van het protocol als een minderjarige een account op een sociaal medium wil maken. Voor het aanmaken van een account geldt vaak een minimumleeftijd zoals die in sectie 2.8 onderzocht is.

Als een minderjarige een account wil aanmaken zal eerst gevraagd worden of hij de vereiste leeftijd bereikt heeft. Om de leeftijd te bewijzen kan er gebruikgemaakt worden van het gezagscredential omdat daarin een attribuut staat dat aangeeft of de minderjarige ouder of jonger is dan zestien jaar (zie sectie 5.1.1. Als de minderjarige al oud genoeg is om zelfstandig een account te maken, dan is het proces van gezagsverificatie niet nodig omdat de minderjarige geen toestemming van de gezagsdrager nodig heeft.



Figuur 5.3: Gebruik van het gezagscredential bij registratie van een Facebook-account

Als de minderjarige echter nog niet zelfstandig een account mag maken is vervolgens het machtigings-ID nodig. De verifier toont een QR-code die de gezagsdrager van de minderjarige moet scannen met zijn IRMA-app. De app laat dan, zoals bij het protocol in de medische sector, het machtigings-ID zien aan de verifier. Wat verschilt met de medische sector is dat er voor sociale media geen gebruik gemaakt mag worden van het BSN.[1] In deze context moet daarom gewerkt worden met de naam van gezagsdrager en minderjarige. Als de procedure echter is afgerond en de minderjarige een

[1] `https://www.rijksoverheid.nl/onderwerpen/privacy-en-persoonsgegevens/vraag-en-antwoord/welke-organisaties-mogen-mijn-burgerservicenummer-bsn-gebruiken`

account heeft op het sociale medium, treedt er nog een ander verschil op met de medische sector. De minderjarige kan namelijk op het sociale media account allerlei activiteiten zelfstandig uitvoeren. Dit in tegenstelling tot de medische sector waar de minderjarige in feite geen handelingen kan uitvoeren. Zolang het kind minderjarig is blijven de gezagsdragers voor hem aansprakelijk. Minderjarigen kunnen op de sociale media berichten plaatsen en vaak ook digitale aankopen doen voor games op het sociale medium. Omdat de gezagsdragers hiervoor verantwoordelijk gehouden kunnen worden, moet er een manier zijn om hen op de hoogte te houden van de activiteiten van de minderjarige. Hiervoor kan een e-mailadres van de gezagsdrager gebruikt worden. Dit geeft zo min mogelijk informatie over persoonlijke kenmerken van de gezagsdrager (zijn naam wordt hiermee bijvoorbeeld niet bekend), terwijl het wel mogelijk is om contact met hem op te nemen. Dit e-mailadres kan door middel van het e-mailcredential in IRMA aan het sociale medium verstrekt worden. De gezagsdrager krijgt dan inzage in de handelingen van de minderjarige, en kan naar aanleiding daarvan indien nodig actie ondernemen.

Ook hier geldt dat het niet nodig is om het machtigings-ID te controleren op geldigheid omdat het centrale punt dit namelijk al garandeert als het credential niet herroepen is. Net als in de medische sector moet het gebruik van de gezagscredentials in de sociale media ook geregistreerd worden. De volgende sectie gaat er verder op in hoe voor beide casussen gestalte kan krijgen.

5.4 Registratie van het gebruik van de gezagsattributen

Nu het proces van registratie en gebruik van het gezagscredential in de medische sector en bij sociale media behandeld is, is het nog nodig om te onderzoeken hoe deze handelingen bijgehouden wordt. De onderstaande afbeelding gaat specifiek over het voorbeeld van het ziekenhuisportaal. Een afzonderlijke afbeelding voor de sociale media is overbodig omdat de registratie van het gebruik van het gezagscredential op dezelfde wijze plaatsvind. Enkel de naam van het ziekenhuis die uitgewisseld wordt moet vervangen worden door de naam van het sociale medium.
Een vorm van registratie van wat er met het gezag is gedaan is nodig om te voldoen aan de 'verantwoordingsplicht' uit de AVG; er moet namelijk kunnen worden aangetoond dat er volgens de regels van de AVG met data wordt omgegaan. Er zijn twee mogelijkheden om dit te registeren:

a. Alle handelingen van de gezagsdragers worden enkel opgeslagen bij de dienstverleners, de centrale site houdt niet het gebruik van attributen bij

Figuur 5.4: Logging van het moment waarop het gezagscredential gebruikt is

b. De centrale site houdt bij wanneer elk gezagscredential gebruikt wordt en bij welke dienstverlener. De dienstverlener houdt bij welke handelingen er gedaan zijn bij een bepaald machtigings-ID

Bovenstaande twee opties zullen nu uitgewerkt worden. Optie *a* heeft als voordeel dat er weinig data centraal wordt opgeslagen. Hierdoor is het centrale punt minder gevoelig voor datalekken, omdat er eenvoudigweg minder te lekken valt. Vanwege de hoge mate van decentrale opslag is het echter voor de minderjarigen lastig om inzicht te krijgen in de uitoefening van het gezag door hun gezagsdragers. Dit komt doordat er te weinig data centraal wordt opgeslagen in deze situatie. Hierdoor is het moeilijk om vanuit het centrale punt uit te zoeken op welke plaatsen het gezag gebruikt is.

In situatie *b* registreert de centrale site wanneer een credential gebruikt wordt, en waar dit credential gebruikt wordt. De dienstverlener houdt bij welke handelingen er gedaan worden door de gebruiker door de handelingen te koppelen aan het machtigings-ID van het credential. Inzage in het gebruik van een credential is nu centraal geregeld: er kan in de centrale site gevonden worden wanneer welk gezagscredential waar gebruikt is. Met die gegevens kunnen minderjarigen bij de dienstverlener uitzoeken welke handelingen er plaatsgevonden hebben. Doordat de inzage hier centraal is, is het eenvoudig om via de centrale site uit te zoeken waar een credential gebruikt is. Door de handelingen zelf wel bij de dienstverleners op te slaan, wordt de data in het centrale punt ook minimaal gehouden.

Van de hierboven behandelde opties is optie *b* de meest bruikbare. In dat geval is eventueel misbruik van het gezag na te zoeken in het centrale systeem. Doordat er bijgehouden wordt welk machtigings-ID, waar en op welk tijdstip gebruikt is, kan hiermee uitgezocht worden hoe het gezag gebruikt is. Het is dus niet mogelijk dat een ouder of vertegenwoordiger handelingen zou kunnen uitvoeren die niet zijn na te gaan. Hiermee wordt de veiligheid voor de kinderen die onder het gezag geplaatst zijn gewaarborgd. Mijns inziens is er hier behoefte aan een toezichthouder die het gezagsgebruik monitort.

Een toezichthouder zou op een onpartijdige manier kunnen controleren of het gezag niet gebruikt wordt ten nadele van de mindejarigen.

5.4.1 Kan een minderjarige de uitoefening van het gezag inzien?

Het protocol draait om gezag dat gezagsdragers uitvoeren over minderjarigen. Hiervoor is in principe geen toestemming van de minderjarigen zelf nodig. Maar zouden minderjarigen de handelingen van hun gezagsdragers wel moeten kunnen inzien? Is een minderjarige wel ertoe in staat hierop toe te zien? Om een voorbeeld te nemen aan de leeftijdscategorieën die de medische wereld hanteert voor minderjarige kinderen, zou het een optie kunnen zijn om kinderen van 0-12 jaar geen inzage hierin te geven, en kinderen vanaf 12 jaar wel. Deze suggestie laten we hier echter rusten omdat dit meer een sociaal-ethisch dilemma is en daarmee buiten het bereik valt van dit onderzoek. Het is daarentegen wel nuttig om hier te onderzoeken hoe een dergelijke suggestie in de praktijk vorm zou moeten krijgen. Hierbij splitsen we minderjarigen in twee categorieën: minderjarigen die de gezagsuitoefening niet mogen inzien, en minderjarigen die dit wel mogen inzien. De grens wordt hier getrokken door een nader te bepalen leeftijd van de minderjarige. Om inzage te kunnen doen moet een minderjarige toegang hebben tot de plaats waar het uitoefenen van gezag wordt bijgehouden, in dit geval dus de centrale website. Om hier toegang toe te krijgen moet de minderjarige zich online kunnen authenticeren. Hiervoor kan DigiD worden gebruikt. Voor het aanvragen van een DigiD geldt namelijk geen minimumleeftijd dus alle minderjarigen kunnen hier gebruik van maken. IRMA zou dan ook gebruikt kunnen worden om te bewijzen dat het minderjarige kind oud genoeg is om de gezagsuitoefeningen in te zien. Omdat een minderjarige pas vanaf een bepaalde leeftijd hierin inzage mag krijgen, is het wellicht nodig om alle gezagsuitoefeningen uit het leven van de minderjarige te tonen. Daardoor krijgt de minderjarige een volledig beeld van wat er door zijn gezagsdragers is gedaan, zelfs wat er gedaan is in de periode dat hij nog niet de mogelijkheid had om dit in te zien. Zo'n inzage komt de transparantie van de gezagsuitoefening richting de minderjarige ten goede.

Hoofdstuk 6

Conclusies

In deze scriptie is onderzocht in welke mate IRMA gebruikt kan worden om de leeftijds- en gezagsverificatie goed in te richten. Er moest eerst onderzocht worden welke leeftijdsgrenzen er gelden en welke verschillende gezagsrelaties er zijn. Hierbij lag de nadruk op de volgende vier gebieden: het kopen van alcoholische drank, het kopen van games, het uitoefenen van patiëntenrechten in de medische wereld en de registratie van een account bij sociale media. Uit hoofdstuk 3 bleek dat er behoefte is aan een verbeterde verificatie. De praktijk van de verificatie bleek namelijk niet aan te sluiten op de wettelijke richtlijnen uit hoofdstuk 2. In hoofdstuk 4 kwamen een aantal tekortkomingen aan de huidige stand van verificatie expliciet aan bod: er is te weinig toezicht op leeftijdsverificatie bij thuisbezorgingskanalen, leeftijdsverificatie bij gameverkoop wordt nauwelijks gehandhaafd, er is in de medische wereld geen eenduidige controle van de gezagsverhoudingen en bij registratie bij sociale media wordt de leeftijd van de gebruiker niet voldoende gecontroleerd. Tenslotte is geconstateerd dat leeftijdsverificatie door middel van de geboortedatum teveel gegevens van de gebruiker gebruikt. De verifier zou alleen aan het binaire gegeven, of de gebruiker oud genoeg is of niet, genoeg moeten hebben. Na deze verbeterpunten is in hetzelfde hoofdstuk een mogelijke oplossing gepresenteerd door middel van IRMA.

In hoofdstuk 5 is de aanname gemaakt dat er een centraal punt is waar het gezagscredential kan worden opgehaald door de gebruiker. Gebaseerd op die aanname is toen onderzocht hoe het protocol van het uitoefenen van gezag vorm kan krijgen. Eerst is er onderzocht hoe het gezagscredential eruit moet zien. Hier zijn overwegingen gemaakt welke gegevens er nodig zijn in het gezagscredential. Omdat het protocol voor leeftijdsverificatie al mogelijk is in IRMA, is het kopen van alcoholische drank en games niet nader behandeld in dit hoofdstuk. Wel is er aandacht besteed aan hoe het protocol vorm moet krijgen in de medische sector en bij het registreren van een account bij sociale media. Deze bleken niet dezelfde persoonsgegevens

nodig te hebben maar waren verder vergelijkbaar met elkaar. Tenslotte is er in hoofdstuk 5 onderzocht hoe het gebruik van het gezagscredential moet worden bijgehouden.

Het protocol dat in het laatste hoofdstuk is opgesteld voldoet aan de eerder gestelde eisen van data-minimalisatie, objectiviteit en het bestand zijn tegen misbruik van de gezagsverhoudingen. Dataminimalisatie wordt gerealiseerd door het gebruik van attributen. De objectiviteit van het protocol is te danken aan de vertrouwde issuer die het credential digitaal ondertekent; hierdoor weet de verifier zeker dat de gebruiker de correcte gezagsrelatie weergeeft in het credential. De gebruiker kan hier dus niet liegen over welke minderjarige hij het gezag heeft. Misbruik van het gezag wordt tegengegaan door de registratie van het gebruik van het gezagscredential in het centrale punt. Dit maakt het gebruik van de attributen eenvoudig te coördineren door een nader aan te stellen toezichthouder.

Er zijn echter nog een aantal punten die nog verder onderzoek vereisen. Ten eerste moet er gezocht worden naar een manier om alle gezagsrelaties bij elkaar op een centraal punt te krijgen. In sectie 3.4 hebben we gezien dat de gezagsrelatie nu op twee plaatsen wordt opgeslagen: in de Basisregistratie Personen, en in het centraal gezagsregister. Om de aanname van hoofdstuk 5 te realiseren moeten de gezagsrelaties bij elkaar gebracht worden in een centraal punt. Hiervoor is overleg met de rechtbanken, of wellicht met een overkoepelende organisatie boven de rechtbanken, nodig om te onderzoeken wat de mogelijkheden hiervoor zijn.

Om het probleem van de leeftijdsverificatie in de alcohol- en gameverkoop te verhelpen zou de overheid beleid moeten maken om deze verificatie beter te reguleren (zie sectie 4.3.3). Er zijn al mogelijkheden in IRMA om leeftijdsverificatie te realiseren. De overheid zou meer aandacht moeten besteden aan een goede manier van verificatie, en bij gebrek daaraan ook harder moeten optreden. Hier moet onderzoek gedaan worden naar de manier waarop de overheid daar invulling aan zou kunnen geven door bijvoorbeeld campagnes en een inspectie om op de verificatie toe te zien. Bij een ondermaatse uitvoering van leeftijds- en gezagsverificatie zou de overheid bovendien sancties kunnen opleggen om instanties te motiveren de verificatie te verbeteren. Dit zou voor zowel leeftijdsverificatie als gezagsverificatie een waardevolle toevoeging zijn.

In sectie 5.4.1 is kort het dilemma aangestipt of minderjarige kinderen inzage zouden moeten hebben in het gebruik van het gezagscredential door hun gezagsdrager(s). Dit sociaal-ethische vraagstuk behoeft nader onderzoek. Aan de hand van de uitkomst van een dergelijk onderzoek kan daarna de keuze gemaakt worden of en hoe minderjarigen inzagerecht zouden moeten

krijgen in het in deze scriptie voorgestelde proces.

Tenslotte moet er nog onderzocht worden hoe er toezicht wordt gehouden op het gebruik van de attributen bij de centrale site. De issuer zou hier zelf het gebruik van de gezagsattributen kunnen controleren, maar wellicht is het beter dat dit ook door een andere onafhankelijke instantie gedaan wordt. Die controle is gericht op het nagaan of de uitoefening van het gezag door de gezagsdrager niet nadelig is voor de minderjarige. Ook is het de vraag of een dergelijke controle op periodieke momenten moet plaatsvinden, of dat er alleen onderzoek naar het gezagsgebruik wordt gedaan zodra er aanleiding is om te denken aan misbruik van de gezagsrelatie. Deze zaken moet verder onderzocht worden in een vervolgonderzoek.

Uit dit onderzoek is gebleken dat IRMA een waardevolle toevoeging kan bieden op het gebied van leeftijds- en gezagsverificatie. Het behandelde proces van leeftijds- en gezagsverificatie biedt een oplossing voor de eerder beschreven problemen. Ook voldoet het proces aan de eisen van dataminimalisatie, objectiviteit en controleerbaarheid. Zoals hierboven is aangegeven zijn er echter nog wel een aantal onvolkomenheden in het huidige voorstel die in later onderzoek verholpen moeten worden. De voorgestelde oplossing is echter een solide eerste stap in het verhelpen van het dringende probleem van leeftijds- en gezagsverificatie in de digitale samenleving.

Bibliografie

[1] Drank- en horecawet, 2017. https://wetten.overheid.nl/BWBR0002458/2017-12-31.

[2] Wetboek van strafrecht, 2017. https://wetten.overheid.nl/jci1.3:c:BWBR0001854&z=2017-09-01&g=2017-09-01.

[3] Besluit gezagsregisters, 2018. https://wetten.overheid.nl/BWBR0002685/2018-08-01.

[4] Uitvoeringswet algemene verordening gegevensbescherming, 2018. https://wetten.overheid.nl/BWBR0040940/2018-05-25.

[5] Besluit jeugdwet, 2019. https://wetten.overheid.nl/BWBR0035779/2019-08-01.

[6] Wet basisregistratie personen, 2019. https://wetten.overheid.nl/BWBR0033715/2019-02-03.

[7] Burgerlijk wetboek boek 1 titel 14, 2020. https://wetten.overheid.nl/jci1.3:c:BWBR0002656&boek=1&titeldeel=14&z=2020-01-01&g=2020-01-01.

[8] Wet op de geneeskundige behandelingsovereenkomst, 2020. https://wetten.overheid.nl/jci1.3:c:BWBR0005290&boek=7&titeldeel=7&afdeling=5&z=2020-04-01&g=2020-04-01.

[9] Jacobs B. Alpár, G. Credential design in attribute-based identity management. https://www.cs.ru.nl/~gergely/objects/TILTing_Alpar-Jacobs_CredentialDesign.pdf.

[10] R. Bushman, B. en Huesmann. Short-term and long-term effects of violent media on aggression in children and adults. *Archives of Pediatric Adolescent Medicine*, 160(4):348–352, 2006.

[11] J. Camenisch. Specification of the identity mixer cryptographic library. Technical report, IBM Research - Zürich, 2010. https://domino.research.ibm.com/library/cyberdig.nsf/papers/EEB54FF3B91C1D648525759B004FBBB1/$File/rz3730_revised.pdf.

[12] Lysyanskaya A. Camenisch, J. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In *Advances in Cryptology — EUROCRYPT 2001*, pages 93–118. Springer Berlin Heidelberg, 2001.

[13] CBL. Online verkoop van alcohol controlelijst. https://supermarkt.nl/uploads/files/Controlelijst_online_verkoop_van_alcohol.pdf.

[14] Newcom Reseach & Consultancy. Nationale social media onderzoek 2020. https://www.newcom.nl.

[15] Council of European Union. Richtlijn (EU) 2016/680 van het Europees parlement en de Raad, 2016. https://eur-lex.europa.eu/legal-content/NL/TXT/?qid=1527490238163&uri=CELEX%3A32016L0680.

[16] KNMG. Richtlijn omgaan met medische gegevens, 2020. https://www.knmg.nl/advies-richtlijnen/knmg-publicaties/omgaan-met-medische-gegevens.htm.

[17] Korenhof P. Alpár G. Hoepman J.H. Koning, M. The abc of abc: An analysis of attribute-based credentials in the light of data protection, privacy and identity. *Balcells, J. (ed.), Internet, Law & Politics : A decade of transformations. Proceedings of the 10th International Conference on Internet, Law & Politics. Universitat Oberta de Catalunya, Barcelona, 3-4 July*, pages 357–374, 2014. https://www.cs.ru.nl/J.H.Hoepman/publications/abc-of-abcs.pdf.

[18] PBLQ PrivacyCare. Onderzoek betrouwbaarheidsniveau patiëntauthenticatie bij elektronische gegevensuitwisseling in de zorg. https://www.nictiz.nl/wp-content/uploads/2018/03/PrivacyCare-PBLQ-Onderzoek-betrouwbaarheidsniveau-pati%C3%ABntauthenticatie-bij-elektronische-gegevensuitwisseling-in-de-zorg-1.pdf.

[19] Rijksoverheid. Nationaal Preventieakkoord, 2018. https://www.rijksoverheid.nl/onderwerpen/gezondheid-en-preventie/documenten/convenanten/2018/11/23/nationaal-preventieakkoord.

[20] Rijskoverheid. Curatele, bewind en mentorschap, 2019. https://www.rijksoverheid.nl/documenten/brochures/2015/04/14/curatele-bewind-en-mentorschap.

[21] K. Roodbeen, R. en Schelleman-Offermans. Alcohol- & tabaksverkoop aan jongeren in 2016. Technical report, Nuchter Kenniscentrum Leeftijdsgrenzen, 2016.

[22] Snapchat. A Parent's Guide To Snapchat. https://storage.googleapis.com/sc-support-web/safety/parents-guide-en.pdf.

[23] Forum Standaardisatie. Betrouwbaarheidsniveaus voor digitale dienstverlening. https://www.nictiz.nl/wp-content/uploads/2018/03/Forum-Standaardisatie-handreiking-betrouwbaarheidsniveaus-voor-digitale-dienstverlening-november-2016.pdf.