Apps in de gezondheidszorg: een mensenrechtelijk vraagstuk

van Kolfschooten, H.; Wallage, B.

Publication date
2022
Document Version
Author accepted manuscript
Published in
Digitalisering in de rechtsverhouding tussen burger en overheid

Apps in de gezondheidszorg: een mensenrechtelijk vraagstuk

Hannah van Kolfschooten en Bastiaan Wallage[*]

1. Inleiding

Digitale consulten door middel van beeldbellen met de behandelend arts in het ziekenhuis,[1] met je telefoon foto's van medische ongemakken delen met de huisarts via een applicatie (hierna ook: 'app')[2], en thuismonitoring van vitale functies, zoals bloeddruk en zuurstofgehalte.[3] Door de coronacrisis is de digitalisering van de gezondheidszorg in een stroomversnelling geraakt. Begin 2021 was meer dan 30% van alle ziekenhuiszorg digitaal. In 2019, voor de pandemie, was dat hooguit 10%.[4] Nederland is inmiddels Europees koploper geworden op het gebied van inzet van gezondheidsapps en wearables in de gezondheidszorg. Artsen maken in toenemende mate gebruik van digitale ontwikkelingen in de behandelrelatie, waaronder de inzet van mobiele apps. Ook steeds meer zorgverzekeraars vergoeden dergelijke digitale zorg, zoals apps.[5]

Ook buiten de behandelrelatie wenden Nederlanders zich steeds vaker tot de 'digitale dokter': de populariteit van fitnesstrackers, hartslagmeters en mindfulness-apps neemt gestaag toe. In 2021 zei meer dan de helft van de Nederlanders minstens één device te gebruiken om de eigen gezondheid te monitoren.[6] Deze gezondheidsapps zijn alom beschikbaar in appstores, al dan niet tegen betaling.

Daarnaast zet ook de overheid steeds vaker gezondheidsapps in voor screeningsdoeleinden ter bescherming van de publieke gezondheid.[7] Hiermee vindt de digitalisering van de zorg niet alleen in ziekenhuizen plaats, maar ook (via de overheid) bij mensen thuis.

Innovatieve gezondheidsapps en wearables – denk hierbij bijvoorbeeld aan een 'smartwatch' – bieden mogelijkheden om de zorg te ondersteunen en verbeteren. Het gebruik kan bijdragen aan effectievere zorgverlening en daarmee aan het oplossen van belangrijke maatschappelijke problemen, zoals toenemende vergrijzing, toename van leefstijlziekten, stijgende zorgkosten en oplopende personeelstekorten in de zorg.[8] Daarnaast kunnen gezondheidsapps op positieve wijze bijdragen aan de individuele gezondheid van gebruikers. Wanneer apps in de behandelrelatie worden ingezet, kan de zorg mogelijk beter worden afgestemd op de persoonlijke situatie van de patiënt en kan de regie van de

[*] Mr. H,B, van Kolfschooten en mr. B. Wallage zijn beiden verbonden aan het Law Centre for Health and Life, Universiteit van Amsterdam.

[1] 'Toekomst kankerzorg: fysieke afspraak blijft belangrijk, videobellen heeft potentie', 15 december 2020, https://nfk.nl/nieuws/toekomst-kankerzorg-fysieke-afspraak-blijft-belangrijk-videobellen-heeft-potentie.

[2] Zie bijvoorbeeld de MedGemak-app.

[3] M.C. van Herwerden e.a., 'Thuisbehandeling van covid-19-patiënten met zuurstof en telemonitoring. Veiligheid, patiënttevredenheid en kosteneffectiviteit', *Nederlands Tijdschrift voor Geneeskunde* 2021/165.

[4] NVZ, Factsheet digitale zorg, juni 2021.

[5] 'Zorgprimeur: eHealth toepassing definitief in zorgaanbod', 11 februari 2022, https://www.icthealth.nl/nieuws/zorgprimeur-e-health-toepassing-definitief-in-zorgaanbod/.

[6] '57 procent Nederlanders meet vitale functies via zelfmeting', 22 maart 2021, https://icthealth.nl/nieuws/57-procent-nederlanders-meet-vitale-functies-via-zelfmeting/.

[7] Advies van de Gezondheidsraad aan de Minister van VWS, 'Verantwoorde inzet van apps voor publieke gezondheid', nr. 2021/32, Den Haag, 7 juli 2021, https://www.gezondheidsraad.nl/binaries/gezondheidsraad/documenten/adviezen/2021/07/07/verantwoorde-inzet-van-apps-voor-publieke-gezondheid/Advies_Verantwoorde-inzet-van-apps-voor-publieke-gezondheid.pdf.

[8] R. van der Vaart e.a., *E-healthmonitor 2021: stand van zaken digitale zorg*, Bilthoven: RIVM 2022.

patiënt over zijn eigen gezondheid en behandeling worden vergroot.[9] Apps maken tegenwoordig ook een belangrijk onderdeel uit van het infectieziektebestrijdingsprogramma van de overheid en kunnen helpen om verspreiding van ziektes te beperken.[10]

Tegelijkertijd brengt toenemend gebruik van gezondheidsapps grote veranderingen met zich mee, wat leidt tot nieuwe risico's. Die risico's zijn veelal verbonden aan de verwerking van bijzondere persoonsgegevens – gezondheidsgegevens – bij het gebruik van de app. Het voorgaande roept de vraag op of het steeds vaker inzetten van applicaties louter positief is of nadelen met zich meebrengt, bijvoorbeeld op het gebied van privacy en de waarborging van het medisch beroepsgeheim. In deze bijdrage zullen wij deze mogelijk bijkomende nadelen onderzoeken, uiteenzetten en aanbevelingen doen om deze – voor zover mogelijk – te voorkomen.

Deze bijdrage is als volgt opgebouwd. Allereerst zullen wij in de volgende paragraaf drie categorieën apps van elkaar onderscheiden en daarbij inzichtelijk maken welke persoonsgegevens worden verwerkt en welke mogelijke nadelen c.q. risico's het gebruik van deze apps met zich meebrengen. In paragraaf drie zullen wij vervolgens het privacyrechtelijke kader uiteenzetten – wat is privacy? – en in het bijzonder aandacht besteden aan de mensenrechtelijke component; het recht op privacy is namelijk een mensenrecht en is onder andere onderdeel van artikel 8 lid 1 van het Europees Verdrag voor de Rechten van de Mens (hierna: EVRM). In paragraaf vier zullen wij vervolgens per categorie app – zoals in paragraaf twee uiteengezet – beschrijven op welke wijze risico's mogelijk kunnen worden beperkt en zullen in dat kader aanbevelingen doen. Wij ronden af met een slotbeschouwing.

2. Gezondheidsapps en privacy in de zorgpraktijk

In dit hoofdstuk zullen wij drie categorieën van applicaties van elkaar onderscheiden. Allereerst zullen wij de gezondheidsapps bespreken die worden gebruikt in de behandelrelatie (tussen arts en patiënt). Vervolgens zullen wij de apps bespreken die raken aan de gezondheidszorg maar niet worden gebruikt in de behandelrelatie. Ten slotte zullen wij ingaan op de applicaties die worden ontwikkeld en aangeboden door de overheid in het kader van gezondheid.

2.1 Gezondheidsapps in de behandelrelatie

Zoals in de inleiding beschreven is het gebruik van medische applicaties in de behandelrelatie niet ongebruikelijk. In de behandelrelatie worden veelal gezondheidsgegevens verwerkt, medische gegevens die de behandelaar nodig heeft voor de behandeling. Hierbij valt bijvoorbeeld te denken aan een mobiele app die de dermatoloog gebruikt om patiënten een foto te laten nemen van de huid en alwaar het algoritme in de applicatie een eerste beoordeling maakt of aanleiding bestaat om de dermatoloog te bezoeken.

Hetgeen bovenstaande app van andere apps onderscheidt is dat de app wordt ingezet in de behandelrelatie tussen de arts en de patiënt. Bij het aangaan van de behandeling komt tussen de zorgverlener en de patiënt een geneeskundige behandelingsovereenkomst tot stand.[11] Als onderdeel van de voornoemde overeenkomst is het de zorgverlener niet toegestaan om inlichtingen over de patiënt – dan wel inzage of afschrift van de gegevens uit het dossier – te delen met derden. Een BIG-

[9] B. Schmietow & G. Marckmann, 'Mobile health ethics and the expanding role of autonomy', *Medicine, Health Care and Philosophy* (22) 2019, afl. 4, p. 623-630.
[10] H.B. van Kolfschooten, 'Gegevensbescherming in gezondheidscrises in de EU: apps in de strijd tegen COVID-19', *Ars Aequi* 2021, afl. 7/8, p. 766-775.
[11] Zie Wet op de geneeskundige behandelingsovereenkomst (WGBO).

geregistreerde hulpverlener is daarnaast op grond van artikel 88 van de Wet op de beroepen in de individuele gezondheidszorg (hierna: Wet BIG) gebonden aan geheimhouding. Dit wordt ook wel het medisch beroepsgeheim van de hulpverlener genoemd.[12]

Indien en voor zover een app wordt gebruikt in de behandelrelatie en in dat kader gezondheidsgegevens worden gedeeld, loopt de hulpverlener daarmee het risico het medisch beroepsgeheim te doorbreken. De informatie die wordt verwerkt door de app komt namelijk op een (externe) server te staan – buiten het directe bereik van de hulpverlener. Daarnaast bestaat het risico dat apps – althans de informatie die via de apps is verkregen – voor andere doeleinden worden ingezet dan waar de app oorspronkelijk voor bedoeld was ('secundary use') en ligt het risico van doelverschuiving op de loer ('function creep'), waarbij de verwerkte gegevens – die kwalificeren als zeer gevoelige persoonsgegevens[13] – worden gebruikt buiten de behandelrelatie om.[14] De hulpverlener heeft daar niet altijd invloed op, aangezien de hulpverlener weinig grip heeft op de verwerkte data. Dat was voor het digitale tijdperk anders, toen de hulpverlener een papieren patiëntendossier bijhield.

2.2 Gezondheidsapps in de appstore

De tweede categorie gezondheidsapps die wij onderscheiden zijn de apps die door zorgconsumenten vrij zijn te downloaden (mogelijk tegen betaling) maar niet worden gebruikt in de behandelrelatie. Hierbij valt te denken aan bijvoorbeeld lifestyle- of mindfulness-apps. Deze apps worden veelal ontwikkeld door commerciële partijen.[15] Ook deze apps verwerken in gevallen gezondheidsgegevens, althans gegevens die in beginsel de gezondheid van een gebruiker kunnen waarderen. Te denken valt bijvoorbeeld aan een lifestyle-app, waarin wordt bijgehouden hoe vaak de gebruiker sport of gezond eet of mindfulness-apps waaruit is op te maken of de gebruiker mogelijk psychische problematiek heeft. Ook bij het gebruik van dergelijke apps bestaat het risico dat de data die worden verwerkt worden gebruikt voor andere doeleinden. Alhoewel dat in het huidige Nederlandse gezondheidsstelsel niet valt voor te stellen, aangezien dit stelsel is gebaseerd op solidariteit[16] en het differentiëren in premie bijvoorbeeld niet is toegestaan[17], valt in theorie te denken aan de zorgverzekeraar die dergelijke data gebruikt voor het accepteren van verzekerden of het bepalen van de hoogte van de premie. Op dit moment zijn er overigens al wel zorgverzekeraars die verzekerden belonen bij een gezonde levensstijl, die gemeten wordt via een applicatie.[18]

2.3 Gezondheidsapps door de overheid

[12] Zie ook KNMG richtlijn 'Omgaan met medische gegevens', KNMG april 2021.
[13] Met zeer gevoelige persoonsgegevens bedoelen wij gezondheidsgegevens (bijzondere persoonsgegevens). Dit zijn gegevens die iets zeggen over de gezondheid van een betrokkene.
[14] Advies van de Gezondheidsraad aan de Minister van VWS, 'Verantwoorde inzet van apps voor publieke gezondheid', nr. 2021/32, Den Haag, 7 juli 2021, https://www.gezondheidsraad.nl/binaries/gezondheidsraad/documenten/adviezen/2021/07/07/verantwoorde-inzet-van-apps-voor-publieke-gezondheid/Advies_Verantwoorde-inzet-van-apps-voor-publieke-gezondheid.pdf.
[15] Rapport "Digitale waardigheid. Bescherming van publieke waarden in de digitale samenleving", blg-798995, februari 2017, https://www.tweedekamer.nl/downloads/document?id=66ec55ae-f2b8-4c28-b775-054fd8b0a81f&title=Rapport%20%22Digitale%20waardigheid.%20Bescherming%20van%20publieke%20waarden%20in%20de%20digitale%20samenleving%22.pdf.
[16] Binnen het Nederlandse gezondheidsstelsel zijn zorgverzekeraars bijvoorbeeld gehouden om alle verzekerden te accepteren, ongeacht leeftijd, leefstijl of gezondheid (zie art. 3 Zorgverzekeringswet).
[17] Zie artikel 17 Zorgverzekeringswet. Uit de parlementaire geschiedenis volgt: *"Om risicoselectie te voorkomen, dient de zorgverzekeraar iedere verzekerde voor iedere variant die hij in de woonprovincie van de verzekerde aanbiedt, te accepteren (art. 3, tweede lid). Een dergelijk gebod heeft niet het gewenste effect, indien de verzekeraar vervolgens de premie per variant wèl zou mogen laten afhangen van verzekerdenkenmerken, en derhalve voor personen met een slechte gezondheid een hogere premie zou mogen vragen dan voor personen met een goede gezondheid", Kamerstukken II* 2003/04, 29763, nr. 3, p. 114.
[18] Zie bijvoorbeeld de app 'a.s.r. Vitality': https://www.asr.nl/vitality.

Een derde te onderscheiden categorie betreft de gezondheidsapps die door de overheid zelf worden ingezet. Vooral tijdens de coronapandemie zijn op Europees niveau door nationale lidstaten – waaronder de Nederlandse overheid – een groot aantal medische applicaties ontwikkeld. Te denken valt bijvoorbeeld aan de welbekende coronacheck-applicatie, die zijn grondslag kent in de Wet publieke gezondheid[19] en die recentelijk de rechterlijke toets heeft doorstaan.[20] Deze categorie van applicaties is – met het oog op het leerstuk van de klassieke grondrechten – het meest risicovol, aangezien de overheid persoonsgegevens verwerkt en daar direct gevolgen aan kan verbinden. Als voorbeeld noemen wij de applicatie die in Polen is ontwikkeld tijdens de coronapandemie.[21] Deze app vraagt de gebruiker in quarantaine – bijvoorbeeld vanwege een vastgestelde COVID-besmetting – op willekeurige momenten om een selfie te maken, die vervolgens rechtstreeks gedeeld wordt met de autoriteiten. Deze autoriteiten beoordelen aan de hand van gezichtherkenning en de locatiedata of de gebruiker inderdaad thuis in quarantaine zit. Deze app verwerkt niet alleen gezondheidsgegevens (namelijk in de relatie tot de COVID-besmetting) maar ook het BSN-nummer van de gebruiker. Indien blijkt dat een gebruiker niet thuis in quarantaine zit, kunnen de daartoe bevoegde autoriteiten direct de politie inzetten en heeft dit derhalve consequenties voor de gebruiker.

Gezien bovenstaande voorbeelden behoeft het geen betoog dat gezondheidsdata een bepaalde (economische) waarde vertegenwoordigen, aangezien partijen – of dit nu de overheid betreft of een commerciële partij – met deze data een inschatting kunnen maken van de gezondheidssituatie van de maatschappij op collectief niveau of van de gebruiker van een app op individueel niveau. Het is dan ook geen verrassing dat de gezondheidszorg een sector is die gevoelig is voor cybercriminaliteit.[22]

De gevolgen van het gebruik van de voornoemde medische applicaties in de gezondheidszorg en bovenal de verwerking van gezondheidsgegevens voor andere doeleinden – bijvoorbeeld als gevolg van een datalek[23] – kunnen maatschappelijk groot zijn. In dat kader wijzen wij bijvoorbeeld op het datalek zoals dat zich tijdens de coronapandemie heeft voorgedaan bij de GGD, waardoor een grote hoeveelheid medische data werd verwerkt voor andere doeleinden. Zo werden persoonsgegevens van miljoenen Nederlanders te koop aangeboden. De Autoriteit Persoonsgegevens (hierna: AP) gaf naar aanleiding van haar onderzoek naar dit incident aan:

Hoewel wij als AP begrip hebben voor hoe lastig deze opgave was, is het hoe dan ook essentieel dat mensen vertrouwen houden in de GGD. En dat zij niet gaan aarzelen om zich te laten vaccineren of testen door de angst dat daarna hun persoonsgegevens op straat belanden.

Dat mag nooit een drempel zijn. Vooral ook omdat het hier om een uitzonderlijk grote groep mensen gaat. Zeker nu het virus weer zo snel om zich heen grijpt, moet dit bij de GGD echt in orde zijn.[24]

Dit voorbeeld onderstreept het belang van zorgvuldige verwerking van persoonsgegevens en de waarborging van de veiligheid van de verwerking. Zoals wij in het volgende hoofdstuk zullen toelichten,

[19] 'Gezond gedrag belonen met korting of wearable?', *ICThealth.nl*, 6 januari 2020.
[20] Gerechtshof Den Haag, 15 februari 2022, ECLI:NL:GHDHA:2022:144.
[21] H.B. van Kolfschooten, 'Gegevensbescherming in gezondheidscrises in de EU: apps in de strijd tegen COVID-19', *Ars Aequi* 2021, afl. 7/8, p. 766-775; H.B. van Kolfschooten & B. Wallage, 'Europese harmonisatie van privacy – óók in crisistijd', *NJB.nl* 8 juli 2020.
[22] E.G. Spanakis, Emmanouil e.a., 'Cyber-attacks and threats for healthcare–a multi-layer thread analysis', 2020 42nd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC), IEEE, 2020.
[23] AP, 'Zorgsector opnieuw koploper datalekmeldingen bij AP', 19 september 2019.
[24] AP, 'GGD moet persoonsgegevens beter beschermen', 9 november 2021.

is dit binnen de gezondheidszorg noodzakelijk om te kunnen spreken van een goed werkend gezondheidsstelsel.

3. Juridisch kader: het concept van privacy en gegevensbescherming in de zorg

Privacy is een oud concept en vormt van oudsher – bijvoorbeeld met het oog op het medisch beroepsgeheim – een belangrijk uitgangspunt in de gezondheidszorg. De eed van Hippocrates sprak in 400 v. Chr. al over het belang van geheimhouding door artsen.[25] In de (rechts)wetenschap was echter een lange tijd onduidelijk wat privacy precies inhield. Zo schreef Thomson in 1975: '*The most striking thing about the right to privacy is that nobody seems to have any clear idea of what it is'.*[26] Inmiddels wordt geaccepteerd dat het recht op privacy een verzamelnaam is voor verschillende rechten die de persoonlijke levenssfeer betreffen.[27] Zo beschouwt de klassieke benadering van Warren en Brandeis privacy als '*the right to be let alone*' (**relationele privacy**, zoals het huisrecht).[28] Het klassieke **communicatiegeheim** houdt de vertrouwelijkheid in van een medium dat wordt gebruikt (bijvoorbeeld het briefgeheim).[29] **Lichamelijke privacy** betreft de onaantastbaarheid van het eigen lichaam, zoals het afnemen van lichaamsmateriaal voor strafrechtelijk onderzoek.[30] Westins klassieke definitie van privacy ziet op **informationele privacy**.[31] Dit houdt de aanspraken in van het individu om zelf te bepalen hoe, wanneer en welke informatie over hem of haar wordt gedeeld. Informationele privacy is daarmee nauw verbonden met het recht op gegevensbescherming.[32]

In dit hoofdstuk focussen wij voornamelijk op de informationele privacy. De in de vorige paragraaf beschreven risico's van apps in de gezondheidszorg zijn namelijk veelal gerelateerd aan de grootschalige verwerking van gevoelige gezondheidsgegevens. Bovendien is – zo zal blijken – informationele privacy van essentieel belang in de gezondheidszorg.

3.1 Het recht op privacy en gegevensbescherming als mensenrechten

Informationele privacy is een mensenrecht en wordt vanuit mensenrechtelijk perspectief vaak beschouwd als onderdeel van het recht op eerbiediging van de persoonlijke levenssfeer.[33] Alhoewel dit ook in artikel 10 van de Grondwet is verankerd, is binnen de Nederlandse rechtsorde vooral artikel 8 van het EVRM van belang.[34] Dit komt omdat Nederlandse wetgeving – zijnde wetten in formele zin – door de nationale rechter niet aan de Grondwet – maar wel aan het EVRM – mogen worden getoetst.[35] Artikel 8 lid 1 EVRM beschermt het recht op eerbiediging van de persoonlijke levenssfeer, of bescherming van het privéleven. Dit recht heeft een brede reikwijdte; vele aspecten worden door dit grondrecht beschermd.[36] Hierbij valt bijvoorbeeld te denken aan de bescherming van de seksuele

[25] A.C. Hendriks, 'Het medisch beroepsgeheim anno 2016: gewenste en ongewenste veranderingen', *Tijdschrift voor Gezondheidsschade, Milieuschade en Aansprakelijkheidsrecht* 2015, afl. 4, p. 164-168.
[26] J.J. Thomson, 'The right to privacy', *Philosophy & Public Affairs* (4) 1975, afl. 4, p. 295.
[27] B.J. Koops, 'Privacyconcepten voor de 21e eeuw', *Ars Aequi* 2019, p. 532-544.
[28] S.D. Warren & L.D. Brandeis, 'The right to privacy. The implicit made explicit', *Harvard Law Review* 1890, p. 193-220.
[29] Art. 13 Gw.
[30] Art. 11 Gw.
[31] A. Westin, *Privacy and Freedom*, New York: Atheneum Press 1967.
[32] Koops 2019, p. 532-544.
[33] B.W. Schermer & B. van der Sloot, *Het recht op privacy in horizontale verhoudingen*', WODC 2020.
[34] NB. Het Handvest van de grondrechten van de Europese Unie bevat een soortgelijk recht. Artikel 52 lid 3 van het Handvest bepaalt dat de inhoud en reikwijdte van de grondrechten die corresponderen met die in het EVRM gelijk zijn. Dit geldt ook voor artikel 8 Handvest en artikel 8 EVRM.
[35] Art. 120 Gw.
[36] De AVG en art. 8 EVRM.

geaardheid van een persoon,[37] de bescherming tegen inmenging van de staat in het familieleven[38] en het recht op gezondheidsinformatie.[39] Het Europees Hof voor de Rechten van de Mens (hierna: EHRM) leest hier ook een recht op gegevensbescherming in.[40] Hieronder valt ook het recht om *informed consent* te geven voor het verzamelen van gezondheidsgegevens.[41] Daarnaast geldt dat de rechten die voortvloeien uit art 8 EVRM niet alleen verplichtingen met zich meebrengen voor de staat, maar ook horizontaal doorwerken.[42] Het recht op privacy reguleert zodoende ook de privacyrechtelijke verhouding tussen privaatrechtelijke partijen.

Het EHRM heeft meermaals het fundamentele belang van bescherming van gezondheidsgegevens in het licht van het recht op privéleven erkend.[43] Medische gegevens vereisten meer bescherming dan andere persoonsgegevens vanwege de persoonlijke en gevoelige aard.[44] Het EHRM heeft geoordeeld dat het openbaar maken van gezondheidsinformatie zeer nadelige gevolgen kan hebben voor het privé- en familieleven van een betrokkene, bijvoorbeeld in het geval van delen van medische informatie in een publiek debat over abortus of in een strafrechtelijke procedure.[45] Beperkingen op artikel 8 EVRM door het openbaar gezag zijn – zoals wij later in dit hoofdstuk verder zullen uitwerken – alleen mogelijk indien dit bij wet is voorzien en noodzakelijk is in een democratische samenleving in het belang van een legitiem doel zoals bescherming van de volksgezondheid of nationale veiligheid.[46]

Nu de inzet van apps in de gezondheidszorg al snel leidt tot grootschalige verzameling van persoonsgegevens, levert het gebruik in sommige gevallen een vergaande beperking op van het grondrecht op informationele privacy van individuen onder artikel 8 EVRM. Dit mag onder voorwaarden – het recht is immers niet absoluut –, maar dat betekent niet dat privacy zomaar aan de kant kan worden geschoven in de naam van gezondheid. Vooral in tijden van crisis – zoals de afgelopen jaren in meer of mindere mate het geval is geweest – vormt het EVRM een rechtsstatelijke bescherming die op individueel niveau waarborgen biedt. Het verbaast dan ook niet dat dit artikel uit het EVRM in het bijzonder een van de belangrijkste waarborgen biedt in de gezondheidszorg.

3.2 Het belang van privacy voor de toegang tot de gezondheidszorg

Zoals hierboven toegelicht is het van groot belang dat de gezondheidsinformatie die wordt gedeeld met de arts vertrouwelijk kan worden gedeeld, zodat eenieder zich veilig voelt om zich te wenden tot een arts. In de rechtspraak van het EHRM komen in dat kader bijvoorbeeld uitspraken terug waarin – als gevolg van het doorbreken van het medisch beroepsgeheim – over een betrokkene bekend wordt dat

---

[37] EHRM 15 maart 2012, ECLI:NL:XX:2012:BW7989 (*Gas en Dubois t. Frankrijk*), par. 37; EHRM 26 februari 2002, ECLI:NL:XX:2002:AE7843 (*Fretté t. Frankrijk*), par. 37-39; EHRM 22 januari 2008, ECLI:NL:XX:2008:BC5672 (*E.B. t. Frankrijk*), par. 49.

[38] EHRM 12 juli 2001, ECLI:NL:XX:2001:AP0817 *(K. en T. t. Finland*), par. 166; EHRM 22 juni 1989, ECLI:NL:XX:1989:AD0829 (*Eriksson t. Zweden*), par. 81; EHRM 7 augustus 1996, ECLI:NL:XX:1996:AB9924 (*Johansen t. Noorwegen*), par. 64.

[39] Zie EHRM 25 februari 1997, ECLI:CE:ECHR:1997:0225JUD002200993 (*Z. t. Finland*), par. 71.

[40] F. Fabbrini, 'The EU Charter of Fundamental Rights and the Rights to Data Privacy: The EU Court of Justice as a Human Rights Court', in: S. de Vries e.a. (red.), *The EU Charter of Fundamental Rights as a Binding Instrument. Five Years Old and Growing*, Oxford: Hart Publishing 2015, p. 261-287.

[41] EHRM 29 april 2014, ECLI:CE:ECHR:2014:0429JUD005201907 (*L.H. t. Letland*).

[42] Zie bijvoorbeeld: L.F.M. Verhey, *Horizontale werking van grondrechten, in het bijzonder van het recht op privacy* (diss. RUU), Zwolle 1992 en Overkleeft-Verburg 1995, hfdst. 4.

[43] Zie o.m. EHRM 29 april 2014, ECLI:CE:ECHR:2014:0429JUD005201907 (*L.H. t. Letland*), r.o. 56.

[44] EHRM 10 oktober 2006 ECLI:NL:XX:2006:AZ4345 (*L.L. t. Frankrijk*), r.o. 32 en 44.

[45] EHRM 30 oktober 2012, ECLI:CE:ECHR:2012:1030JUD005737508 (*P. en S. t. Polen*) par. 128 en EHRM 25 februari 1997, ECLI:CE:ECHR:1997:0225JUD002200993 (*Z. t. Finland*), par. 96.

[46] Art. 8 lid 2 EVRM.

hij hiv-positief is.[47] Het EHRM komt tot het oordeel dat dit valt onder de reikwijdte van artikel 8 lid 1 EVRM, nu het gevolg hiervan kan zijn dat de betrokkene daardoor wordt blootgesteld aan het risico van minachting en uitsluiting.[48] In een andere uitspraak oordeelt het EHRM: '*(…) people living with HIV are a vulnerable group with a history of prejudice and stigmatisation*'.[49] Daarmee vormt het privacyrecht in de gezondheidszorg – inhoudende het recht op informationele privacy – een van de belangrijkste grondbeginselen. Indien en voor zover een patiënt niet zeker is dat hij zich in vertrouwen kan wenden tot een arts, bestaat het risico dat de patiënt in het geheel niet gaat en gezondheidsschade oploopt. Op het niveau van de patiënt leidt dit tot individuele gezondheidsrisico's. Op het niveau van de maatschappij – indien en voor zover meer personen zich niet wenden tot een arts terwijl dit wel nodig is – vormt dit vervolgens een potentieel risico voor de volksgezondheid. In de coronapandemie – waaronder het voorbeeld van de GGD – is dat wederom bevestigd.

Ook uit de rechtspraak van het EHRM volgt dit belang, een belang dat raakt aan de toegang tot de gezondheidszorg in het algemeen. Zo oordeelt het Hof:

> *It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general. Without such protection those in need of medical assistance may be deterred, when revealing such information of a personal and intimate nature as may be necessary in order to receive the appropriate treatment, from seeking such assistance thereby endangering their own health but, in the case of transmissible diseases, that of the community. The domestic law must therefore afford appropriate safeguards so there may be no such communication or disclosure of personal health data as may be inconsistent with the guarantees of Article 8 of the Convention.*[50]

Op grond van artikel 8 EVRM heeft de Staat kortom los van voor haar geldende negatieve verplichtingen tevens de positieve verplichting om dergelijke rechten – voortvloeiende uit artikel 8 lid 1 EVRM – actief te beschermen.

Alhoewel innovatie in de gezondheidszorg – waaronder de ontwikkeling van apps – zoals beschreven kansen met zich meebrengt, te meer in een stelsel dat financieel zwaar onder druk staat[51] – brengt een dergelijke innovatie kortom ook potentiële risico's met zich mee. Risico's die raken aan de toegang tot het stelsel van de gezondheidszorg in het algemeen en aan de bescherming van fundamentele mensenrechten. Dat roept de vraag op of de wetgever deze rechten momenteel daadwerkelijk actief beschermt op basis van regulering. Deze vraag staat centraal in het vervolg van deze bijdrage.

3.3 Versnipperde regelgeving omtrent gezondheidsapps

De risico's voor het recht op informationele privacy bij de inzet van apps in het kader van gezondheidsrecht worden versterkt door een gebrek aan een eenduidig juridisch beschermingskader.

---

[47] EHRM 25 februari 1997, ECLI:CE:ECHR:1997:0225JUD002200993 (*Z. t. Finland*); EHRM 17 juli 2008, ECLI:NL:XX:2008:BF0246 (*I. t. Finland*); EHRM 25 november 2008, ECLI:NL:XX:2008:BH0401 (*Biriuk t. Litouwen*).

[48] EHRM 17 januari 2012, ECLI:CE:ECHR:2012:0117JUD002037605, (*Varapnickaitė-Mažylienė t. Litouwen*) par. 44; EHRM 25 februari 1997, ECLI:CE:ECHR:1997:0225JUD002200993 (*Z. t. Finland*); EHRM 6 oktober 2009, ECLI:CE:ECHR:2021:0511JUD004356417 (*C.C. t. Spanje*) par. 33.

[49] EHRM 10 maart 2011, ECLI:CE:ECHR:2011:0310JUD000270010 (*Kiyutin t. Rusland*) par. 64.

[50] EHRM 25 februari 1997, ECLI:CE:ECHR:1997:0225JUD002200993 (*Z. t. Finland*).

[51] De Nederlandse Zorgautoriteit en Zorginstituut Nederland constateren dat het Nederlandse zorgstelsel onbetaalbaar is geworden. In 2019 werd 13% van het bruto binnenlands product uitgegeven aan de zorg, zie www.nza.nl/actueel/nieuws/2020/11/30/zorginstituut-en-nza-schetsen-in-advies-randvoorwaarden-passende-zorg.

Dit komt ten eerste doordat er voor elk soort gebruik (in de behandelrelatie, in de appstore en door de overheid) andere juridische kaders gelden. Als een arts een gezondheidsapp die vrij verkrijgbaar is in een app store adviseert aan een patiënt en deze gebruikt in de behandelrelatie, verandert het juridisch kader. Dit zorgt voor verwarring, ook onder appontwikkelaars. Ten tweede is het voor gebruikers (patiënten, artsen én overheden) vaak onduidelijk welke gegevens er precies verwerkt worden en waar deze worden opgeslagen, waardoor het moeilijk is om daadwerkelijke risico's in te schatten en actie te ondernemen in geval van schade. Ten derde worden de rechten van patiënten bij het gebruik van apps op twee niveaus beschermd: nationaal (via o.a. patiëntenrechten zoals het medisch beroepsgeheim) en Europees (via o.a. de regulering van medische hulpmiddelen). Dit leidt tot versnipperde regulering.[52] Tot slot speelt er ook een handhavingsprobleem: er zijn zóveel gezondheidsapps op de markt dat de (toch al overbelaste) AP en Inspectie Gezondheidszorg en Jeugd (IGJ) onmogelijk toezicht kunnen houden op de kwaliteit en veiligheid van alle apps.[53] Dit komt onder andere omdat het toezicht op het gebruik van gezondheidsapps in Nederland zo is ingeregeld dat het toezicht achteraf plaatsvindt; eenieder kan in beginsel een gezondheidsapp aanbieden in een appstore, tenzij sprake is van een medisch hulpmiddel.[54]

3.3.1 Algemeen kader: Algemene Verordening Gegevensbescherming

Op alle drie de categorieën gezondheidsapps is de Algemene Verordening Gegevensbescherming (hierna: AVG) van toepassing. Het grondrecht op gegevensbescherming is op Europees niveau uitgewerkt in de AVG.[55] De AVG harmoniseert de regels over rechtmatigheid van het verwerken van persoonsgegevens in de Europese Unie met als doel een effectieve en uniforme bescherming van persoonsgegevens in de hele Unie. Kort gezegd omschrijft de AVG de rechten van betrokkenen en de plichten van degenen die persoonsgegevens verwerken.[56] Daarnaast wordt invulling gegeven aan de wettelijke grondslagen die gebruikt kunnen worden om persoonsgegevens te verwerken.[57] Zonder een dergelijke grondslag is het juridisch niet mogelijk (c.q. rechtmatig) om persoonsgegevens te verwerken. Ook de AVG biedt de mogelijkheid om de rechten van betrokkenen[58] en de beginselen inzake verwerking van persoonsgegevens[59] te beperken met het oog op de bescherming van de volksgezondheid.[60] Dergelijke beperkingen moeten wel worden opgenomen in de wet, proportioneel en noodzakelijk zijn en geen afbreuk doen aan de wezenlijke inhoud van grondrechten. Ook moeten er in de wet specifieke bepalingen worden opgenomen over, onder andere, de categorieën te verwerken persoonsgegevens, de bewaartermijnen en waarborgen ter voorkoming van misbruik.[61]

Bij het verwerken van gezondheidsgegevens (gegevens over medicijngebruik, een COVID-19-testuitslag, Body Mass Index etc.) geldt een strenger regime: deze verwerkingen zijn in principe verboden, aangezien het hier bijzondere persoonsgegevens betreft[62], tenzij er sprake is van een van de genoemde uitzonderingssituaties en daarnaast een grondslag voor de verwerking aanwezig is.[63] Een

[52] H.B. van Kolfschooten, 'The mHealth Power Paradox: Improving Data Protection in Health Apps through Self-Regulation in the European Union', in: I. Glenn Cohen e.a. (red.), *The Future of Medical Device Regulation: Innovation and Protection*, Cambridge: Cambridge University Press 2022, p. 63-76.
[53] CEG, 'CEG Signalement Gezondheidsapps en wearables – De ethiek van eHealth deel 1', 2020.
[54] A. Loohuis & N.H. Chavannes, 'Medische apps: zorg voor de toekomst?', *Huisarts en Wetenschap* 2017.
[55] Zie preambule AVG.
[56] Punt 11, preambule AVG. Voorbeelden van rechten en plichten zijn: de plicht tot het verstrekken van informatie bij verzameling van persoonsgegevens (art. 11), recht van inzage (art. 15) en recht op gegevenswissing (art. 17).
[57] Artikel 6 AVG.
[58] Artikelen 12-22 AVG.
[59] Artikel 5 AVG.
[60] Artikel 23 lid 1 AVG.
[61] Artikel 23 lid 1 en 2 AVG.
[62] Artikel 9 lid 1 AVG.
[63] Artikel 6 en Artikel 9 lid 1 en 2 AVG.

gezondheidscrisis kan zo'n uitzonderingssituatie vormen, ofwel via de weg van de uitdrukkelijke toestemming van betrokkene voor de verwerking van zijn gezondheidsgegevens,[64] ofwel indien verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang[65] of algemeen belang op het gebied van de volksgezondheid.[66] Ook verwerking in het kader van de behandelrelatie kan een uitzondering vormen. Verwerkingen moeten in elk geval wel proportioneel zijn en er moeten passende en specifieke maatregelen zijn opgenomen ter bescherming van de rechten en vrijheden van de betrokkene.[67] Daarnaast bestaan er in de AVG ruime uitzonderingen voor het gebruik van medische gegevens voor het doen van wetenschappelijk onderzoek.

3.3.2 Gezondheidsapps in de behandelrelatie: algemeen gezondheidsrecht en medisch hulpmiddel
Voor de eerste categorie apps, gezondheidsapps in de behandelrelatie, is het juridisch raamwerk het duidelijkst, omdat het algemene gezondheidsrecht van toepassing is, waaronder de WGBO. Bij het aangaan van de behandeling komt tussen de zorgverlener en de patiënt een geneeskundige behandelingsovereenkomst tot stand, waaruit bepaalde rechten voor de patiënt en plichten voor de arts voortvloeien, ook met betrekking tot geheimhouding.[68] Ook op grond van de Wet BIG moeten artsen zich houden aan het medisch beroepsgeheim.[69] Dit is in het geval van de inzet van apps niet anders.

De app kan daarnaast gezien worden als een 'medisch hulpmiddel' als de app – kort gezegd – wordt ingezet voor de diagnose, preventie, monitoring, voorspelling, prognose en behandeling of verlichting van ziekte van een individuele patiënt.[70] In dat geval moet de app voldoen aan de eisen van de Verordening Medische Hulpmiddelen, de Wet op de medische hulpmiddelen en onder meer een CE-keurmerk krijgen. Hierbij wordt overigens niet specifiek gekeken naar privacywaarborgen, maar met name naar veiligheid en kwaliteit.

Artsen kunnen in principe aansprakelijk worden gesteld voor schade bij het gebruik van een medisch hulpmiddel, waaronder een app, op grond van artikel 6:77 BW. Het is wel de vraag wanneer er sprake is van schade bij bijvoorbeeld een datalek. Ook is het nog niet uitgemaakt in hoeverre het redelijk is om een arts aansprakelijk te houden voor misstanden met persoonsgegevens, nu de arts in de praktijk weinig controle heeft over de app. De Koninklijke Nederlandsche Maatschappij tot bevordering der Geneeskunst legt de verantwoordelijkheid voorlopig bij de arts, en heeft een handreiking ontwikkeld voor artsen om te bepalen wanneer een gezondheidsapp veilig kan worden ingezet. Hierbij zijn ook specifieke *checks* voor privacy inbegrepen.[71] Daarnaast stelt de KNMG richtlijnen voor het omgaan met medische gegevens.[72] Hoewel dergelijke richtlijnen en gedragscodes niet juridisch bindend zijn, kunnen ze in de rechtbank gebruikt worden om te beoordelen in hoeverre de arts handelde in lijn met de wettelijke verplichting tot 'goede zorg'.[73]

3.3.3 Gezondheidsapps in de appstore: consumentenrechten
Voor de tweede categorie apps, gezondheidsapps in de appstore, geldt dat deze worden ingezet buiten een behandelrelatie om. In dit artikel gaan wij in dat kader uit van de apps die gezondheid meten (een

[64] Zie artikel 9 lid 2 onder a AVG.
[65] Artikel 9 lid 2 onder g AVG.
[66] Artikel 9 lid 2 onder i AVG.
[67] Artikel 9 lid 2 onder g en i AVG.
[68] Zie artikel 7:457 lid 1 BW.
[69] Zie ook KNMG richtlijn 'Omgaan met medische gegevens', KNMG april 2021.
[70] CEG, 'CEG Signalement Gezondheidsapps en wearables – De ethiek van eHealth deel 1', 2020.
[71] KNMG, 'Medische App Checker: beoordeling van medische apps' 2016.
[72] KNMG, 'Omgaan met medische gegevens', 2021.
[73] Artikel 2 Wkkgz.

zogenoemde ‘lifestyle app’). Alhoewel een ‘lifestyle app’ ook kan kwalificeren als een medisch hulpmiddel, geldt daarnaast teleurstellend weinig regulering, bijvoorbeeld alwaar het gaat om consumentenbescherming. Het betreft hier veelal zelfregulering en niet rechtstreeks afdwingbare toezeggingen vanuit de markt.[74]

3.3.4 Gezondheidsapps door de overheid

Indien en voor zover de overheid apps ontwikkelt, kan zij dat onder meer doen in het kader van haar publieke taak, zoals het ontwikkelen van gezondheidsapps met het oog op het bevorderen van de volksgezondheid. Hierbij valt bijvoorbeeld te denken aan de coronacheck-app die is ontwikkeld door de overheid. Voor deze app bestaat – zoals reeds beschreven – een wettelijke grondslag om persoonsgegevens te verwerken.

De overheid heeft bij de ontwikkeling van apps – zoals toegelicht – wel een andere positie dan private partijen. Ten eerste heeft de overheid meer mogelijkheden om op grote schaal persoonsgegevens te verzamelen (en uit te wisselen tussen de verschillende overheidsdiensten) voor de uitvoering van publieke taken. Ook kan de overheid te verkrijgen gezondheidsdata eenvoudiger gebruiken voor overige doeleinden en daar gevolgen aan verbinden. Dat is op grond van het recht op privacy en het principe van doelbinding in beginsel niet toegestaan, tenzij bijvoorbeeld sprake is van een wettelijke uitzonderingsgrond.[75] Daarbij is ook het bestuursrechtelijke specialiteitsbeginsel relevant, waaruit volgt dat de overheid alleen mag handelen in lijn met het belang waarvoor de desbetreffende regeling is opgesteld.[76]

Ook mensenrechtelijk neemt de overheid – in vergelijking met private partijen – een andere positie in. Allereerst heeft de Staat op grond van artikel 8 EVRM de negatieve verplichting om zich te onthouden van inmenging in het privéleven van burgers. Op grond van artikel 8 lid 2 EVRM kan een inmenging gerechtvaardigd zijn. In dat geval dient de inbreuk wel een legitiem doel te dienen, dient de beperking bij wet te worden voorzien en dient de beperking te zijn ingegeven door een dringende maatschappelijke behoefte.[77] Daarnaast dient de inbreuk proportioneel en subsidiair te zijn.[78] De bescherming van de gezondheid kan bijvoorbeeld een legitiem doel vormen op grond waarvan onder andere het recht op gegevensbescherming ingevolge artikel 8 lid 2 EVRM door een nationale lidstaat kan worden beperkt. Daarnaast blijkt uit de rechtspraak van het EHRM dat uit artikel 8 EVRM ook positieve verplichtingen voor de Staat volgen om de rechten die voortvloeien uit voornoemd artikel te waarborgen. Alhoewel de voornoemde rechten ook doorwerken in horizontale relaties (tussen private partijen en inwoners),[79] volgt uit artikel 8 EVRM de expliciete verplichting voor de Staat om te voorzien in een ‘legislative and administrative framework’.[80] Dit houdt in dat de staat ervoor moet zorgen dat de rechten die voortvloeien uit artikel 8 EVRM dienen te worden gewaarborgd in nationale wet- en regelgeving. Dit betekent overigens niet dat het recht op privacy absoluut is en de nationale wetgever in dat kader geen beoordelingsvrijheid (‘margin of appreciation’) toekomt. Uit de rechtspraak van het EHRM volgt dat een nationale lidstaat op grond van artikel 8 EVRM een evenwicht dient te vinden (‘fair balance’) tussen enerzijds het belang van het individu en anderzijds het algemeen belang.[81] Ook gedurende de

[74] Van Kolfschooten 2022.
[75] Zie artikel 9 AVG.
[76] Zie bijv. ABRvS 12 november 2014, ECLI:NL:RVS:2014:4117.
[77] Zie bijv. EHRM 25 februari 1997, ECLI:CE:ECHR:1997:0225JUD002200993 (*Z. t. Finland*).
[78] Idem.
[79] Schermer & Van der Sloot 2020.
[80] EHRM 20 maart 2008, ECLI:NL:XX:2008:BD6179 (*Budayeva t. Rusland*).
[81] Zie bijv. EHRM 9 december 1994, ECLI:CE:ECHR:1994:1209JUD001679890 (*López Ostra t. Spanje*).

coronapandemie is bovenstaand kader het privacyrechtelijk relevante toetsingskader geweest, bijvoorbeeld in de afweging tussen het belang van vrijheid van meningsuiting (artikel 11 EVRM) en de bescherming van de volksgezondheid.[82]

4. Regulering van de digitale dokter: oplossingsrichtingen

In het voorgaande betoogden wij dat het juridisch kader omtrent gezondheidsapps onvoldoende duidelijk is en dat daardoor het recht op informationele privacy van patiënten op losse schroeven komt te staan. Hiermee komt mogelijk ook de toegang tot gezondheidszorg onder druk te staan. Zonder de voordelen van gezondheidsapps tekort te doen – deze kunnen de kwaliteit en toegankelijkheid van de zorg immers sterk verbeteren – menen wij dat het reguleringskader van gezondheidsapps op bepaalde punten moet worden aangescherpt. We zien mogelijkheden om op verschillende niveaus aanpassingen te doen die uiteindelijk zullen leiden tot een betere bescherming van patiënten bij toenemende inzet van gezondheidsapps. In het vervolg van deze paragraaf belichten we enkele oplossingsrichtingen. Voor een effectieve bescherming moeten de door ons voorgestelde maatregelen integraal worden doorgevoerd, nu de juridische problemen omtrent gezondheidsapps op verschillende niveaus plaatsvinden.

4.1 Concretisering van de AVG: 'Wet verwerking persoonsgegevens mobiele applicaties in de zorg'

De risico's voor de rechten op privacy en gegevensbescherming van betrokken patiënten ontstaan met name vanwege de grootschalige verwerking van bijzondere persoonsgegevens – zijnde gezondheidsgegevens – die de meeste apps vereisen. De AVG werkt het recht op gegevensbescherming in de hele Europese Unie uit in rechten en plichten, maar is een algemene wet die op alle sectoren – niet alleen de zorg – van toepassing is. Bovendien laat het beschermingskader veel ruimte voor interpretatie, terwijl er juist behoefte is aan duidelijke richtlijnen.[83] Daarmee biedt de AVG niet direct handvatten voor de bescherming van persoonsgegevens die worden verwerkt in het kader van het gebruik van apps in de zorg. Op nationaal niveau bieden de Uitvoeringswet AVG en de Wet aanvullende bepalingen verwerking persoonsgegevens onder andere enkele extra waarborgen voor de bescherming van informationele privacy in de zorg, maar zien ook zij niet specifiek op apps. De wetgever zou deze leemte in het wettelijk kader kunnen vullen door een nieuwe wet 'Wet verwerking persoonsgegevens mobiele applicaties in de zorg' in het leven te roepen met specifieke bepalingen voor gezondheidsapps. Deze wet zou concrete beschermingsmaatregelen moeten bevatten, zoals maximale bewaartermijnen, specifieke beveiligingsmaatregelen[84] en handvatten voor een effectieve informed consent-procedure.[85] Een dergelijke wet zou duidelijkheid creëren voor fabrikanten in het kader van het ontwikkelen van gezondheidsapps, en voor artsen en patiënten in het gebruik ervan.

4.2 Vergunningsstelsel voor gezondheidsapps

In bepaalde gevallen moeten apps die in het kader van een behandelrelatie worden ingezet voldoen aan de eisen van de Verordening Medische Hulpmiddelen. De Inspectie Gezondheidszorg en Jeugd houdt toezicht op medische hulpmiddelen, maar kijkt hierbij met name naar veiligheid en kwaliteit. Een 'privacycheck' vormt dan ook geen onderdeel van de vereisten tot het verkrijgen van een CE-markering

[82] Zie bijv. EHRM 15 maart 2022, ECLI:CE:ECHR:2022:0315JUD002188120 (*Communaute genevoise d'action syndicale (CGAS) t. Zwitserland*).
[83] L. Marelli, E. Lievevrouw & I. van Hoyweghen, 'Fit for purpose? The GDPR and the governance of European digital health', *Policy studies* (41) 2020, afl. 5, p. 447-467.
[84] NB. Er is op grond van de AVG geen concrete bewaartermijn voor persoonsgegevens. Organisaties bepalen zelf hoe lang zij persoonsgegevens bewaren, mits dit proportioneel is voor het doel.
[85] Zie ook EHRM 29 april 2014, ECLI:CE:ECHR:2014:0429JUD005201907 (*L.H. t. Letland*).

en toelating tot de markt. Het toezicht op verwerking van persoonsgegevens – ook door middel van gezondheidsapps – wordt uitgeoefend door de AP. Het belang van een zorgvuldige verwerking van persoonsgegevens en de risico's van gezondheidsapps staan op de radar van de AP: zij gaf al eens een waarschuwing aan de lifestyle-app 'Nike+ Running' voor het onzorgvuldig verwerken van gezondheidsgegevens.[86] Toch zijn de capaciteiten van de AP beperkt, ook omdat de AP privacybreed toezicht dient te houden en zich daarbij niet beperkt tot de gezondheidszorg.

Het toezicht van de AP vindt daarnaast per definitie pas *achteraf* plaats, als de gezondheidsgegevens al verwerkt zijn. Het is praktisch onmogelijk om toezicht te houden op de verwerking van gezondheidsgegevens die op grote schaal verwerkt worden, bijvoorbeeld met het gebruik van applicaties. Voor een effectieve bescherming van de rechten van appgebruikers pleiten wij er daarom voor om een vergunningsstelsel in te richten voor gezondheidsapps. Appontwikkelaars die gezondheidsgegevens verwerken moeten vóórdat ze hun app ter beschikking mogen stellen op de markt toestemming krijgen van een onafhankelijk orgaan dat specifiek kijkt naar privacywaarborgen. Een dergelijk vergunningsstelsel zou bovendien goed aansluiten bij de onlangs ingevoerde Wet toetreding zorgaanbieders (Wtza), die een vergunningsplicht invoert voor zorginstellingen.[87] Nu het CBIG (uitvoeringsorgaan van het ministerie van Volksgezondheid, Welzijn en Sport) onder andere verantwoordelijk is voor de afgifte van vergunningen die zorgaanbieders toegang geeft tot het leveren van zorg,[88] ligt het voor de hand om een vergunningsstelsel voor gezondheidsapps ook onder de verantwoordelijkheid van het CBIG te brengen. Nu een dergelijk vergunningsstelsel tijds- en kostenintensief is, zal voor apps die minder gevoelige gegevens verwerken – denk aan voedingsapps of hardloopapps – een *melding* kunnen volstaan voor het verkrijgen van een vergunning. Apps die gezondheidsgegevens zoals medische gegevens verwerken zullen een extensieve toetsing moeten doorlopen. Zowel de AP als de IGJ zou in dat kader een rol kunnen krijgen bij de inhoudelijke beoordeling van de app. Met een dergelijk vergunningsstelsel vindt de privacycheck *vooraf* plaats, en zijn de rechten van betrokkenen beter gewaarborgd.

4.3 Mensenrechtelijke check voor overheidsapps

Een mensenrechtelijke check bij de ontwikkeling van applicaties door de overheid die grootschalig wordt ingezet, zoals bij een pandemie, is naar ons oordeel wenselijk. Indien het inzetten van een app een wetswijziging vereist, ligt het voor de hand dat de Afdeling advisering van de Raad van State advies uitbrengt over het wetsvoorstel. Dit gebeurde bijvoorbeeld bij het gebruik van digitale coronatoegangsbewijzen (de coronacheck-app)[89] en de notificatieapp 'CoronaMelder'.[90] Ook vroeg het ministerie van Volksgezondheid, Welzijn en Sport advies aan de AP bij de keuze voor bron- en contactopsporingsapps in de coronacrisis,[91] en werd om een spoedadvies verzocht bij het College voor de Rechten van de Mens.[92] Hoewel deze gang van zaken aantoont dat de Nederlandse overheid het belang van mensenrechtenbescherming bij apps hoog acht, zijn deze adviezen niet juridisch bindend. Bovendien vereist niet elke inzet van een gezondheidsapp door de overheid een wetswijziging, waardoor de noodzaak tot het vragen van advies aan autoriteiten voor de overheid minder sterk zal zijn. Ook was er bij de apps ter bestrijding van de covidpandemie een stuk meer democratische controle dan

[86] CBP, Onderzoek Nike+ Running app, 11 november 2015.
[87] Wet toetreding zorgaanbieders (Wtza).
[88] Wet toetreding zorgaanbieders (Wtza).
[89] Raad van State, Samenvatting advies voorstel inzet coronatoegangsbewijs niet-essentiële detailhandel en dienstverlening, 12 november 2021.
[90] Raad van State, Samenvatting advies voorstel Tijdelijke wet notificatieapp covid-19, 21 augustus 2020.
[91] AP, Onderzoeksrapportage bron- en contactopsporingsapps, 20 april 2020.
[92] College voor de Rechten van de Mens, Spoedadvies aan minister Hugo de Jonge van Volksgezondheid, Welzijn en Sport over het aanbouwdocument juridische verantwoording corona-apps, 18 april 2020.

er gewoonlijk is voor het gezondheidsbeleid van de overheid. Ter vergelijking: bij de ontwikkeling van de 'JouwGGD-app' voor jongeren, waar jongeren online gezondheidsadvies en -hulp kunnen inroepen, werden er geen adviezen ingewonnen. Wij pleiten ervoor om gezondheidsapps die door de overheid worden ingezet en grootschalig gezondheidsgegevens verzamelen altijd vooraf een – onafhankelijke – mensenrechtelijke check te laten ondergaan, die bovendien juridisch-bindend is. Er kan hiervoor aangesloten worden bij het 'stappenplan grondrechten' van het Impact Assessment voor Mensenrechten bij de inzet van Algoritmen (hierna: IAMA), een instrument om vooraf de risico's voor mensenrechten bij de inzet van algoritmen in kaart te brengen, waarover in maart 2022 een motie werd aangenomen om deze verplicht te stellen bij het inzetten van algoritmen voor evaluaties van of beslissingen over mensen.[93] In de mensenrechtelijke check van gezondheidsapps moet in ieder geval worden beoordeeld welke grondrechten in welke mate worden geraakt, of de app een effectief en noodzakelijk middel is om het doel van gezondheidsbescherming te bereiken, en of de inzet van de app voor publieke gezondheidsdoeleinden in redelijk evenwicht staat tot en de beperking van mensenrechten. Hoe ernstiger de verwachte mensenrechteninbreuk, hoe zwaarder de publieke doeleinden moeten wegen die daartegenover staan. Als de app niet door de test komt, kan de overheid de app niet op de voorgestelde wijze inzetten. Een positieve uitkomst van de mensenrechtelijke check staat er uiteraard niet aan in de weg dat de inzet van gezondheidsapps door de overheid jegens individuen disproportioneel en daarom in strijd met de bescherming van mensenrechten kan zijn.

5. Slotbeschouwing

Het mensenrechtelijk kader roept voor de overheid verplichtingen in het leven om het recht op informationele privacy van appgebruikers te waarborgen, bijvoorbeeld door feitelijke of wetgevende maatregelen te nemen. Het is de vraag of de Nederlandse overheid daar momenteel aan voldoet bij de waarborging van de bescherming van persoonsgegevens bij het gebruik van medische applicaties in de gezondheidszorg. Los van deze juridische vraag, is het naar ons oordeel ook met het oog op de werking van het gezondheidsstelstel van essentieel belang dat gezondheidsapps veilig kunnen worden gebruikt (zonder dat het risico bestaat dat zeer gevoelige informatie wordt gedeeld met derden of voor andere doeleinden wordt gebruikt). Indien dat niet het geval is, bestaat het risico dat het vertrouwen van een individuele gebruiker in de applicatie en/of de arts afneemt en de betrokkene zich niet langer wendt tot deze arts. Dat risico bestaat vooral bij het gebruik van applicaties in de behandelrelatie en dat is dan ook de reden dat wij pleiten voor een stringenter juridisch kader van deze groep applicaties, in vergelijking met overige gezondheidsapps die worden gebruikt buiten de behandelrelatie om.

Indien en voor zover een betrokkene zich niet langer wendt tot de arts omdat het vertrouwen is geschaad, bijvoorbeeld door een datalek, komt daarmee de gezondheid van deze betrokkene in het geding. Op collectief niveau levert dit een potentieel gevaar voor de volksgezondheid op. In een dergelijke uiterste situatie wegen de voordelen van het gebruik van medische applicaties in de zorg niet op tegen de nadelen; die raken aan het fundament van het gezondheidsstelsel. Om een dergelijke situatie dan ook te kunnen voorkomen is naar ons oordeel regulering nodig in aanvulling op de reeds bestaande privacy gerelateerde wet- en regelgeving die zich veelal niet focust op een sector. Zo kan met een vergunningstelsel worden gewaarborgd dat niet achteraf maar vooraf wordt gecontroleerd of gezondheidsapps veilig zijn en afdoende rekening wordt gehouden met de privacy van de gebruiker. Met dergelijke waarborgen wordt innovatie in de gezondheidszorg duurzamer gemaakt en kan bovenal worden genoten van de bijkomende voordelen in een stelsel dat (financieel) zwaar onder druk staat.

[93] Impact Assessment Mensenrechten en Algoritmes (IAMA), Universiteit Utrecht, juli 2021.