

Gegevensbescherming in gezondheids crises in de EU: apps in de strijd tegen COVID-19

Hannah van Kolschooten*

In crisissituaties – waaronder de coronacrisis – wordt steeds meer gebruik gemaakt van mobiele technologie. Apps verwerken grote hoeveelheden persoonsgegevens van individuen, met gevolgen voor het grondrecht op gegevensbescherming. Deze bijdrage gaat in op de rol van gegevensbescherming in crisisbeheersing en -bestrijding in de EU en bespreekt in hoeverre het recht op gegevensbescherming kan worden ingeperkt in het kader van een gezondheids crisis.

1 Inleiding

Mobiele technologie heeft een belangrijke rol verworven binnen de crisisbeheersing en rampenbestrijding in lidstaten van de Europese Unie (EU). Zo maakt de Nederlandse overheid sinds 2012 gebruik van mobiele NL-Alerts bij noodsituaties en gebruikt de Duitse overheid de mobiele applicatie 'Katwarn' in crisissituaties.¹ Google heeft sinds 2010 een online platform voor opsporing van vermiste personen in crisissituaties, zoals aardbevingen, overstromingen en aanslagen.² Facebook brengt met 'Facebook Disaster Maps' op basis van locatiegegevens van gebruikers in kaart welke gebieden zijn geraakt door natuurrampen, zoals vulkaanuitbarstingen en bosbranden.³ Ook in de strijd tegen COVID-19 maken EU-lidstaten veel gebruik van apps. Het gaat dan bijvoorbeeld om symptomencheckers en notificatie-apps.⁴ Met name op het gebied van bron- en contactonderzoek voorziet het merendeel van de Europese overheden in een app.⁵

Met de coronacrisis en het veelvuldig gebruik van corona-apps in de strijd tegen COVID-19 is de bescherming van de volksgezondheid op gespannen voet komen te staan met het recht op gegevensbescherming

De Europese Commissie moedigt de ontwikkeling en het gebruik van apps voor het indammen van de verspreiding van het coronavirus in de EU aan. Tegelijkertijd is de Commissie zich bewust van de gevaren voor de bescherming van het privéleven.⁶ De corona-apps die momenteel in Europa in de omgang zijn, hebben gemeen dat ze in grote mate afhankelijk zijn van persoonsgegevens, waaronder gevoelige gegevens over de gezondheid. Met de coronacrisis en het

- * Mr. H.B. van Kolschooten is promovendus en docent Gezondheidsrecht aan de Universiteit van Amsterdam. Zij doet promotieonderzoek naar EU-regulering van artificiële intelligentie in de zorg en patiëntenrechten.
- 1 M. Grinko, M. Kaufhold & C. Reuter, 'Adoption, Use and Diffusion of Crisis Apps in Germany: A Representative Study', *Proceedings of Mensch Und Computer 2019*, p. 263-274.
 - 2 T. van Soest, 'Google Person Finder dient ook in Japan als noodprikbord', *de Volkskrant* 11 maart 2011.
 - 3 P. Maas e.a., 'Facebook Disaster Maps: Aggregate Insights for Crisis Response & Recovery', *Proceedings of the 16th ISRAM Conference*, mei 2019, <https://research.fb.com/publications/facebook-disaster-maps-aggregate-insights-for-crisis-response-recovery/>.
 - 4 M.C. Ploem & T.F.M. Hooghiemstra, 'Corona te lijf via een app', *TvGR* 2020, afl. 5, p. 509.
 - 5 Zie voor een overzicht: European Commission, 'Mobile contact tracing apps in EU Member States', https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic/mobile-contact-tracing-apps-eu-member-states_en en S. Eskens, 'Contact tracing app laws in the EU', www.saraheskens.eu/blog/contact-tracing-laws.html 19 december 2020.
 - 6 Aanbeveling (EU) 2020/518 van de Commissie van 8 april 2020 over een gemeenschappelijke



CoronApp

Voornaam *

Achternaam *

locatie *

Snotneus?

Toelichting

Hoe wij omgaan met je persoonsgegevens
[privacystatement](#)

VERZENDEN

veelvuldig gebruik van corona-apps in de strijd tegen COVID-19 is de bescherming van de volksgezondheid op gespannen voet komen te staan met het recht op gegevensbescherming. In de afweging tussen beide belangen lijkt de laatste het onderspit te delven: het recht op gegevensbescherming verdwijnt in heel Europa naar de achtergrond met het oog op de crisisbestrijding.⁷ Dit is frappant gezien het strikte regime voor gegevensbescherming dat de EU sinds de inwerkingtreding van de Algemene Verordening Gegevensbescherming (AVG) kent. Daarmee dringt zich de vraag op in hoeverre het recht op gegevensbescherming mag worden ingeperkt in het kader van een gezondheids crisis en wat de rol van de EU is in deze kwestie.

Deze bijdrage bespreekt de reikwijdte van het recht op gegevensbescherming in gezondheids crises. Hierbij staat de rol van de EU bij de inzet van 'corona-apps' in EU-lidstaten centraal

Deze bijdrage bespreekt de reikwijdte van het recht op gegevensbescherming in gezondheids crises. Hierbij staat de rol van de EU bij de inzet van 'corona-apps' in EU-lidstaten centraal. Eerst geeft paragraaf 2 een overzicht van apps die Europese overheden momenteel inzetten in de strijd tegen COVID-19. Paragraaf 3 zet het juridisch kader van het grondrecht op gegevensbescherming in de EU uiteen en tekent de grenzen van dit recht in crisistijd af. Paragraaf 4 bespreekt de positie die de EU inneemt in het gegevensbeschermingsbeleid omtrent corona-apps. Daarna bespreekt paragraaf 5 de risico's van het gebruik van corona-apps voor gegevensbescherming en wordt een analyse gemaakt van het niveau van bescherming. Paragraaf 6 concludeert.

2 Europese apps in de strijd tegen COVID-19

In het kader van crisismanagement worden over het algemeen vier fasen onderscheiden: de preventiefase, de preparatiefase, de repressiefase en de nazorgfase. Elke fase vereist andersoortige maatregelen.⁸ Waar het in de beginfase van gezondheids crises

voornamelijk gaat om het inschatten van risico's, gaat het in latere fasen meer om het indammen van besmettingen. De corona-apps die momenteel door Europese lidstaten worden ingezet zijn grofweg in vier categorieën in te delen: epidemiologische apps, screeningsapps, contactopsporingsapps en handhavingsapps. Alle categorieën hebben gemeen dat ze in grote mate afhankelijk zijn van persoonsgegevens, waaronder gevoelige gegevens over de gezondheid.

2.1 Epidemiologische apps

Een belangrijke stap in het voorkomen van grootschalige ziektenuitbraken is epidemiologische surveillance: het doorlopend verzamelen, analyseren en interpreteren van gegevens over infectieziekten. In Nederland voeren de GGD en het RIVM deze surveillance uit. Informatie komt voort uit verschillende surveillancebronnen, zoals bijvoorbeeld sterftcijfers van het CBS en routinetesten van bloeddonoren.⁹ Het Europees Centrum voor ziektepreventie en -bestrijding (ECDC) is verantwoordelijk voor de monitoring op Europees niveau: aan de hand van de surveillancegegevens uit de lidstaten brengen zij de stand van zaken op het gebied van infectieziekten in kaart. De Europese Unie bundelt de wekelijkse rapportages over COVID-19 in de app 'Re-open EU'.¹⁰ Daarnaast zijn er ook apps voor *real time tracking* van ziekteverspreiding op de markt. Zo heeft Zweden de app 'COVID Symptom Study' waarmee door middel van informatie over symptomen, positieve testuitslagen en locatie verstrekt door individuele gebruikers in kaart wordt gebracht waar op dat moment COVID-19 *hot spots* zijn.¹¹

2.2 COVID-19-screeningsapps

Als een besmettelijke ziekte eenmaal in de omloop is, is het van belang besmettingsgevallen te isoleren. In het geval van COVID-19 is het zaak dat mensen zich laten testen. Om de gang naar de teststraat te bespoedigen, zijn er verschillende COVID-19-screeningsapps voor zelfdiagnose en symptoomcontrole in de omloop. Gebruikers verstrekken informatie over hun gezondheidstoestand en mogelijke symptomen via de app, waarop de app een medisch advies baseert. Soms gebeurt dit op basis van een simpel algoritme, zoals bij de 'NHS 24 COVID-19 and flu information' app van de Schotse overheid.¹² In Nederland wordt de app 'De Corona Check' aangeboden, waarbij medische teams van verschillende zieken-

toolbox voor het gebruik van technologie en gegevens om de COVID-19-crisis te bestrijden en te boven te komen, met name wat mobiele applicaties en het gebruik van geanonimiseerde mobiliteitsgegevens betreft, *PbEU* L 114/7.

- 7 E. Sánchez Nicolás, 'Coronavirus: Are we trading privacy for security?', <https://euobserver.com/coronavirus/148041> 14 april 2020; P. Balboni, "PUBLIC HEALTH AND PRIVACY" and not "PUBLIC HEALTH OR PRIVACY": Surveillance in the fight against COVID-19, *Law Blogs Maastricht* 24 april 2020.
- 8 D. Fischer, O. Posegga, & K. Fischbach, *Communication Barriers in Crisis Management: A Literature Review* (Twenty-Fourth European Conference on Information Systems (ECIS)), juni 2016, p. 1-18.
- 9 RIVM, 'Soa surveillance', www.rivm.nl/seksueel-overdraagbare-aandoeningen/soa-surveillance, laatst gewijzigd 14 juni 2019.
- 10 'Re-open EU': Commissie lanceert website voor een veilige hervatting van reizen en toerisme in de EU, www.europa-nu.nl/id/vl9jfo4eoss/ 15 juni 2020.
- 11 W. Froelich, 'COVID Symptom Study Tracks Risks in Real Time', *Oncology Times* (42) 2020, afl. 17, p. 31.
- 12 'NHS 24 Coronavirus (COVID-19) and flu information app', www.nhsinform.scot/care-support-and-rights/tools-and-apps/nhs-24-coronavirus-covid-19-and-flu-information-app 7 december 2020.

huizen telefonische begeleiding kunnen bieden op basis van de ingevoerde informatie in de app.¹³

2.3 Contactopsporingsapps

Om het aantal besmettingen in te dammen, is het noodzakelijk om besmettingsgevallen in een vroeg stadium op te sporen. Steeds meer lidstaten maken voor bron- en contactonderzoek bij een coronavirus-besmetting gebruik van contactopsporingsapps.¹⁴ De Europese apps werken op vrijwillige basis en maken gebruik van bluetooth-technologie: als de app-gebruiker enige tijd in de buurt is geweest van iemand die positief is getest op het coronavirus, en deze persoon de app ook geïnstalleerd heeft, krijgt hij daarvan een melding. Er bestaan wel enkele verschillen tussen de Europese contactopsporingsapps. Zo registreert de Hongaarse app ‘VirusRadar’ telefoonnummers van gebruikers en bewaart deze gegevens in de centrale, beveiligde opslag van de overheid.¹⁵ De Deense app ‘Smitte | stop’ en de Nederlandse app ‘CoronaMelder’ verwerken geen telefoonnummers of andere directe identificatoren en persoonsgegevens worden lokaal, op de eigen telefoon, bewaard. Ook de bewaartermijn verschilt per app. Veel apps hanteren veertien dagen, maar de Italiaanse app ‘Immun’ stelt de bewaartermijn afhankelijk van de duur van de noodtoestand.¹⁶ De Europese Commissie heeft in samenwerking met lidstaten een systeem voor interoperabiliteit tussen Europese contactopsporingsapps opgezet. Informatie van de nationale apps wordt doorgegeven aan een Europese gateway, die de informatie doorgeeft aan aangesloten nationale apps. Dat betekent dat gebruikers van de Nederlandse ‘CoronaMelder’, ook een melding krijgen indien een gebruiker van de Duitse ‘CoronaWarnApp’ in de buurt is geweest en in zijn app aangeeft besmet te zijn met het coronavirus.¹⁷

2.4 Handhavingsapps

In de repressiefase van een infectieziekten-uitbraak worden verschillende maatregelen ingezet, variërend van quarantaine en inreisverboden tot samscholingsverboden. Voor de handhaving van deze maatregelen in de bestrijding van COVID-19 worden in EU-lidstaten steeds vaker apps ingezet. Verschillende Nederlandse gemeenten hebben aan de ‘MijnGemeente’-app een functie toegevoegd waarmee bewoners illegale groepsvorming kunnen melden.¹⁸ De ge-

meente Texel ontwikkelde de app ‘TexelMap’ waarmee de drukte op populaire plekken op het eiland in kaart werd gebracht ten behoeve van ‘crowd control’.¹⁹ De Europese app ‘Co-Aps’ is ontwikkeld om drukte in het openbaar vervoer te verminderen en zo de verspreiding van COVID-19 te voorkomen. Deze app verzamelt *real time* data uit verschillende bronnen, zoals camerabeelden op stations, aantal gescande vervoersbewijzen en gewicht van treinen. Daarbij gebruikt de app ook ‘crowdsourced data’: appgebruikers worden gevraagd om persoonlijke informatie te verstrekken via questionnaires, zoals leeftijd, beroep en e-mailadres. Er worden ook locatiegegevens verzameld. Overheden, vervoersbedrijven en passagiers kunnen deze informatie gebruiken om drukte in het openbaar vervoer te vermijden.²⁰

De Poolse overheid heeft een app verplicht gesteld voor burgers die thuis in verplichte quarantaine moeten. De app vraagt op willekeurige momenten om een selfie. Deze selfie wordt gedeeld met de autoriteiten en vervolgens wordt door middel van facial recognition en locatiedata gecontroleerd of de gebruiker inderdaad thuis is

Daarnaast zijn er in de EU twee apps voor handhaving van quarantaine in gebruik. De Poolse overheid heeft de app ‘Kwarantanna domowa’ verplicht gesteld voor burgers die thuis in verplichte quarantaine moeten. De app vraagt op willekeurige momenten om een selfie. Deze selfie wordt gedeeld met de autoriteiten en vervolgens wordt door middel van *facial recognition* en locatiedata gecontroleerd of de gebruiker inderdaad thuis is. De app verzamelt BSN-nummers, namen, telefoonnummers, adresgegevens, foto’s en locatiegegevens (GPS) en stuurt deze gegevens door naar centrale servers van de overheid. De gegevens worden zes jaar bewaard.²¹ Hongarije stelt de app ‘Hází Karantén Rendszer’ verplicht voor burgers in verplichte thuisquarantaine. De app vraagt om naam, geboorteplaats, geboortedatum, e-mailadres en telefoonnummer. Vergelijkbaar met de Poolse app, krijgen ge-

13 ‘De Corona Check: de app met ondersteuning van Nederlandse ziekenhuizen’, decoronacheck.nl 17 september 2020 (laatst geraadpleegd op 22 maart 2021).

14 Eskens 2020.

15 ‘Hogyan működik a VirusRadar?’, <https://virusradar.hu/> (automatisch vertaald van Hongaars naar Engels met Google Translate).

16 ‘Informativa privacy’, www.immuni.italia.it/app-pn.html (automatisch vertaald van Italiaans naar Engels met Google Translate).

17 Europese Commissie, ‘Coronavirus: EU interoperability gateway goes live, first contact tracing and warning apps linked to the system’, https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1904 19 oktober 2020; ‘Samenwerking CoronaMelder met andere landen’, <https://coronamelder.nl/nl/faq/13-gebruik-app-uit-ander-land>.

18 E. de Joode, ‘Corona-overtredingen melden via app: “Mensen zelf aanspreken is spannend”’, NOS 31 maart 2020; ‘MijnGemeente app nu ook voor melding groepsvorming’, rijswijk.nl 30 april 2020 (laatst geraadpleegd op 22 maart 2021); ‘Purmerend laat inwoners via app groepsvorming melden’, www.security.nl/posting/649594/26 maart 2020.

19 ‘Nieuwe “crowd control” app voor Texel’, texel.net 12 mei 2020 (laatst geraadpleegd op 22 maart 2021).

20 ‘Terms and conditions of the Co-Aps application’, <https://coaps.eu/tc/>.

21 Norton Rose Fulbright, ‘Contact tracing apps in Poland. A new world for data privacy’, www.nortonrosefulbright.com/en-pl/knowledge/publications/d7a9a296/ 2 februari 2021.

bruikers op willekeurige momenten per sms een ‘remote monitoring’-verzoek, waarbij de app vraagt om een selfie. De foto wordt dan tezamen met de locatiegegevens gedeeld met de autoriteiten. De gegevens worden zestig dagen na het einde van de quarantaine verwijderd van de centrale servers.²²

Ook in crisissituaties moeten beperkingen van grondrechten in redelijke verhouding staan tot het bestrijden van de crisis: er moet een duidelijke noodzaak voor zijn en er moet voldaan zijn aan de eisen van proportionaliteit en subsidiariteit

3 Het recht op gegevensbescherming in tijden van gezondheidscrisis

Het verwerken van persoonsgegevens is in alle fasen van een gezondheidscrisis vereist, al dan niet door middel van apps. Dit kan zelfs noodzakelijk zijn vanwege de positieve verplichtingen die lidstaten vanuit het Europees Verdrag tot bescherming van de Rechten van de Mens en de fundamentele vrijheden (EVRM) hebben tot bescherming van de levens van burgers.²³ Vaak wordt gevreesd dat het verwerken van persoonsgegevens in het kader van het algemeen belang van volksgezondheid niet samen kan gaan met effectieve bescherming van het individuele recht op gegevensbescherming.²⁴ In dit kader wordt ook wel geroepen ‘nood breekt wet’. Critici noemen deze belangenafweging echter een ‘vals dilemma’: privacy en volksgezondheid worden ten onrechte als twee elkaar uitsluitende waarden gepresenteerd.²⁵ Ook de EU stelt dat de bescherming van beide belangen hand in hand kunnen gaan in een gezondheidscrisis.²⁶ Het Europees juridisch kader voor gegevensbescherming voorziet ook in de mogelijkheid om het publiek belang mee te wegen. In hoeverre is het juridisch kader voor gegevensbescherming in de EU *fit for purpose* in het geval van een gezondheidscrisis zoals de COVID-19-crisis?

3.1 Gegevensbescherming als grondrecht

Het recht op gegevensbescherming is sterk ingekaderd in de Europese mensenrechtenwetgeving. Artikel 8 van het Handvest van

de grondrechten van de Europese Unie bepaalt dat eenieder het recht heeft op bescherming van zijn persoonsgegevens. Dit betekent dat individuen het recht hebben om informatie die zij liever niet met anderen delen, privé te laten zijn. Daaruit volgt ook dat de gegevens eerlijk moeten worden verwerkt, voor een bepaald doel, en dat hier een gerechtvaardigde grondslag voor moet zijn. Daarnaast moet er een mogelijkheid tot inzage en rectificatie zijn. Een onafhankelijke autoriteit moet op de naleving van deze regels toezien.²⁷ Uit het recht op privé-, familie- en gezinsleven van artikel 8 EVRM wordt ook een recht op gegevensbescherming afgeleid.²⁸ Het recht op gegevensbescherming is echter niet absoluut, wat betekent dat het beperkt mag worden indien dit nodig is met het oog op de bescherming van legitiem belang.²⁹ Bescherming van de publieke gezondheid is zo’n gerechtvaardigd belang.³⁰ Dat betekent echter niet dat privacy zomaar aan de kant kan worden geschoven in een gezondheidscrisis. Ook in crisissituaties moeten beperkingen van grondrechten in redelijke verhouding staan tot het bestrijden van de crisis: er moet een duidelijke noodzaak voor zijn en er moet voldaan zijn aan de eisen van proportionaliteit en subsidiariteit. Lidstaten hebben in de afweging hiervan wel een bepaalde *margin of appreciation*.³¹ Daarnaast moet een beperking een grondslag hebben in een duidelijke, voorzienbare en toegankelijke regel van nationale recht.³² De inzet van corona-apps leidt tot grootschalige verzameling van persoonsgegevens en levert in sommige gevallen een vergaande beperking op van het grondrecht op gegevensbescherming van individuen, met name in het geval van de handhavingsapps. Dat betekent dat lidstaten bij het introduceren van corona-apps steeds moeten afwegen of een dergelijke beperking in overeenstemming is met de vereisten van het Handvest en het EVRM.

Dit is alleen anders indien lidstaten van mening zijn dat er sprake is van een noodsituatie die noopt tot afwijken van de verplichtingen onder het Handvest en EVRM.³³ In dat geval kan, voor zover de ernst van de noodsituatie geen andere mogelijkheid biedt, het recht op gegevensbescherming tijdelijk worden beperkt zonder inachtneming van de gebruikelijke beperkingssystematiek.³⁴ Opschorting van grondrechten in geval van een noodsituatie moet worden gemeld bij de Europese Commissie voor de Rechten van de Mens.³⁵ Estland,

22 ‘Töltse le a Házi Karantén Rendszer alkalmazást’, <https://hazikaranten.hu/> (automatisch vertaald van Hongaars naar Engels met Google Translate); ‘The Hungarian Quarantine App’, <https://helpers.hu/other/the-hungarian-quarantine-app/> 5 november 2020.

23 Art. 2 EVRM beschermt het recht op leven. Zie over positieve verplichtingen onder art. 2 EVRM in verband met gezondheid onder meer EHRM 30 november 2004, ECLI:CE:ECHR:2004:1130JUD004893999 (Öneryıldiz/Turkije).

24 E. Ventrella, ‘Privacy in emergency circumstances: data protection and the COVID-19 pandemic’, *ERA Forum* (21) 2020, afl. 3, p. 379-393.

25 J. Goldenfein, B. Green & S. Viljoen, ‘Privacy Versus Health Is a False Trade-Off’, *Jacobin Magazine* 2020.

26 W. Wiewiórowski, ‘Carrying the torch in times of darkness’, https://edps.europa.eu/press-publications/press-news/blog/carrying-torch-times-darkness_en 30 april 2020.

27 Zie art. 8 lid 2 en 3 Handvest.

28 NB: art. 52 lid 3 Handvest bepaalt dat de inhoud en reikwijdte van de grondrechten die corresponderen met die in het EVRM gelijk zijn. Dit geldt ook voor art. 8 Handvest en art. 8 EVRM.

29 Zie art. 8 lid 2 EVRM en art. 8 en 52 Handvest.

30 Zie art. 8 lid 2 EVRM.

31 EHRM 25 februari 1997, ECLI:CE:ECHR:1997:0225JUD0022000993 (*Z/Finland*), par. 99.

32 Zie de eisen voor beperking in art. 8 lid 2 EVRM en art. 52 Handvest; nader uitgewerkt in onder meer EHRM 26 april 1979, ECLI:NL:XX:1979:AC6568 (*Sunday Times*).

33 Art. 15 EVRM.

34 A. Lebreton, ‘Covid-19 pandemic and derogation to human rights’, *Journal of Law and the Biosciences* (7) 2020, afl. 1.

35 Art. 15 lid 1 EVRM.

36 Council of Europe, ‘Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 5) Notifications under Article 15 of the Convention in the context of the COVID-19 pandemic’, versie van 18 februari 2021, www.coe.int/en/web/conventions/full-list/-/conventions/webContent/199943603.

Letland en Roemenië zijn de enige EU-lidstaten die afwijkingen van het EVRM op basis van artikel 15 hebben gemeld. Deze meldingen hadden echter geen betrekking op afwijking van het recht op gegevensbescherming.³⁶

Ook de AVG biedt de mogelijkheid om de rechten van betrokkenen en de beginselen inzake verwerking van persoonsgegevens te beperken met het oog op de bescherming van de volksgezondheid

3.2 De Algemene Verordening Gegevensbescherming

Het Europees grondrecht op gegevensbescherming is uitgewerkt in de AVG. De AVG harmoniseert de regels over rechtmatigheid van het verwerken van persoonsgegevens in de EU met als doel een effectieve bescherming van persoonsgegevens in de hele Unie. Kort gezegd omschrijft de AVG de rechten van betrokkenen en de plichten van degenen die persoonsgegevens verwerken.³⁷ Daarnaast wordt invulling gegeven aan de wettelijke grondslagen die gebruikt kunnen worden om persoonsgegevens te verwerken.³⁸ Ook de AVG biedt de mogelijkheid om de rechten van betrokkenen³⁹ en de beginselen inzake verwerking van persoonsgegevens⁴⁰ te beperken met het oog op de bescherming van de volksgezondheid.⁴¹ 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.⁴² Bij het verwerken van gezondheidsgegevens (e.g. gegevens over medicijngebruik, een COVID-19-testuitslag, Body Mass Index) geldt een strengere regime: deze verwerkingen zijn in principe verboden, tenzij er sprake is van een van de genoemde uitzonderingssituaties en daarnaast een grondslag voor de verwerking aanwezig is.⁴³ Een gezondheids crisis kan zo'n uitzonderingssituatie vormen, ofwel via de weg van de uitdrukkelijke toestemming van betrokkene voor de

verwerking van zijn gezondheidsgegevens,⁴⁴ ofwel indien verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang⁴⁵ of algemeen belang op het gebied van de volksgezondheid.⁴⁶ Verwerkingen moeten wel proportioneel zijn en er moeten passende en specifieke maatregelen zijn opgenomen ter bescherming van de rechten en vrijheden van de betrokkene.⁴⁷

4 De EU en gegevensbescherming in (nationale) corona-apps

De bevoegdheid van de EU in het vormen van regelgeving en beleid op het gebied van volksgezondheid is wettelijk ingeperkt tot de coördinatie van lidstaten.⁴⁸ Op het gebied van gegevensverwerking zijn de bevoegdheden ruimer.⁴⁹ De EU heeft zich al vroeg in de COVID-19-crisis opgeworpen als coördinator van digitale hulpmiddelen, met name in het kader van de corona-apps die in veel lidstaten als paddenstoelen uit de grond schoten. De veelzijdigheid aan apps en het gebruik van persoonsgegevens daarin liet zien dat de uniforme toepassing van de AVG nog te wensen overlaat, met name op het gebied van gezondheidsgegevens.⁵⁰ Het optreden van EU-instanties richtte zich met name op de ontwikkeling van contactopsporingsapps en heeft het recht op gegevensbescherming op verschillende manieren beïnvloed.⁵¹

4.1 Initiatieven van de Europese Commissie

De Europese Commissie heeft zich al vroeg in de coronapandemie ingezet voor het gebruik van mobiele technologie bij de bestrijding van COVID-19. Zo vroeg de Commissie telecombedrijven in maart 2020 om metadata van mobiele telefoons van miljoenen Europeanen te delen. De Commissie wilde de (geanonimiseerde en geaggregeerde) data gebruiken om mobiliteitspatronen te analyseren om de verspreiding van het virus te monitoren.⁵² De Europese Toezichthouder voor gegevensbescherming (EDPS), die toezicht houdt op gegevensbescherming door de Europese instellingen zoals de Europese Commissie, wees op moeilijkheden met betrekking tot effectief anonimiseren van data en benadrukte het tijdelijke karakter van een dergelijke maatregel.⁵³ Deze actie van de Europese Commissie past in de nieuwe Europese datastrategie. De EU zet in op de 'datagestuurde economie', waarin Europese burgers gestimuleerd worden om vaker hun data te delen.⁵⁴ Op 8 april 2020

37 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).

38 Art. 6 AVG.

39 Art. 12-22 AVG.

40 Art. 5 AVG.

41 Art. 23 lid 1 AVG.

42 Art. 23 lid 1 en 2 AVG.

43 Art. 9 lid 1 en 2 AVG.

44 Zie art. 9 lid 2 onder a AVG.

45 Art. 9 lid 2 onder g AVG.

46 Art. 9 lid 2 onder i AVG.

47 Art. 9 lid 2 onder g en i AVG.

48 Zie art. 168 VWEU.

49 Dit heeft te maken met de ruimere bevoegdheden van de EU op het gebied van de (digitale) interne markt onder het VWEU.

50 Communication from the Commission to the European Parliament and the Council. Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation, COM(2020)264 final, Brussels, 24 juni 2020. Zie ook: Europese Commissie, *Assessment of the EU Member States' rules on health data in the light of GDPR*, Luxembourg: Publications Office of the European Union 2021.

51 M. Kędzior, 'The right to data protection and the COVID-19 pandemic: the European approach', *ERA Forum* (21) 2021, afl. 4, p. 533-543.

52 M. Scott, L. Cerulus & L. Kayali, 'Commission tells carriers to hand over mobile data in coronavirus fight', www.politico.eu/article/european-commission-mobile-phone-data-thierry-breton-coronavirus-covid19/ 23 maart 2020. De data werd bewaard op de servers van het Gemeenschappelijk Centrum voor Onderzoek (JRC).

53 W. Wiewiórowski, 'Monitoring spread of COVID-19', https://edps.europa.eu/data-protection/our-work/publications/consultations/monitoring-spread-covid-19_en, 25 maart 2020, kenmerk WRW/NC/mt/D(2020)0724, C2020-0337.

54 *Commission proposes measures to boost data sharing and support European data spaces*, persbericht Europese Commissie, https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2102, 25 november 2020.

presenteerde de Europese Commissie een aanbeveling over een gemeenschappelijke ‘toolbox’ voor digitale middelen zoals apps in de COVID-19-crisis.⁵⁵ In de aanbeveling gaat de Commissie eerst in op het nut van corona-apps voor het indammen van de pandemie. De Commissie is met name enthousiast over contactopsporingsapps.⁵⁶ Over COVID-19-screeningsapps zegt de Commissie dat deze apps relevante informatie kunnen opleveren over het aantal besmettingen.⁵⁷ Daarnaast pleit de Commissie voor een pan-Europese en op Unieniveau gecoördineerde aanpak.⁵⁸ Op 17 april 2020 publiceerde de Commissie richtsnoeren met betrekking tot gegevensbescherming van corona-apps.⁵⁹ Hierin wordt gesteld dat apps moeten voldoen aan het beginsel van gegevensminimalisatie, strikte bewaartermijnen moeten hanteren en gebruikers volledige zeggenschap moeten geven over hun gegevens. Daarnaast moet de beveiliging op orde zijn en moeten de nationale gegevensbeschermingsautoriteiten betrokken worden bij de ontwikkeling.⁶⁰ Ook speelt de Commissie een coördinerende rol in het ontwikkelen van interoperabiliteit tussen Europese contactopsporingsapps.⁶¹

De European Data Protection Board stelt dat het Europees juridisch kader voor gegevensbescherming geen enkele belemmering vormt voor het nemen van maatregelen ter bestrijding van COVID-19

4.2 Europees Comité voor gegevensbescherming

De European Data Protection Board (EDPB), oftewel het Europees Comité voor gegevensbescherming, houdt toezicht op de toepassing van de AVG in Europese lidstaten. De EDPB bestaat uit alle nationale privacytoezichthouders uit de EU. De toezichthouder heeft zich in een vroeg stadium hard gemaakt voor het belang van gegevensbescherming in een gezondheids crisis.⁶² De EDPB stelt dat het Europees juridisch kader voor gegevensbescherming, waaronder de AVG, geen enkele belemmering vormt voor het nemen van maatregelen ter bestrijding van COVID-19.⁶³ De wetgeving voorziet in de mogelijkheid persoonsgegevens te

verzamelen in het geval van een pandemie en er is dus geen noodzaak om de wet terzijde te schuiven.⁶⁴ In reactie op de ontwikkeling van de eerste corona-apps vaardigde de EDPB op 21 april 2020 een richtsnoer uit in de context van de COVID-19-uitbraak. Dit eerste richtsnoer had betrekking op het gebruik van locatiegegevens en instrumenten voor contacttracing.⁶⁵ Over locatiegegevens benadrukt de EDPB dat deze alleen door telecomaandieners gedeeld mogen worden indien ze zijn geanonimiseerd of als gebruikers van tevoren toestemming hebben gegeven.⁶⁶ De EDPB wijst daarnaast op de complexiteit van anonimiseringsprocessen en stelt dat, als locatiegegevens kunnen worden gekoppeld aan een individu, de AVG onverkort van toepassing is. Over contactopsporingsapps stelt de EDPB dat het systematisch en grootschalig monitoren van de locatie en contacten van individuen een ernstige inbreuk op het recht op privacy vormt. Om deze beperking te rechtvaardigen moet de inzet van contactopsporingsapps altijd vrijwillig zijn. Daarnaast moeten er geen locatiegegevens worden getraceerd, maar moet gebruik worden gemaakt van bluetooth-technologie. Ook moet directe identificatie van personen worden uitgesloten, de verzamelde informatie op de mobiele telefoon zelf worden opgeslagen en de bewaartermijn redelijk zijn.⁶⁷ De EDPB bracht op 16 juni 2020 daarnaast een verklaring naar buiten over de gevolgen van de interoperabiliteit van Europese contactopsporingsapps voor gegevensbescherming.⁶⁸ De EDPB stelt vast dat het koppelen van verschillende contactopsporingsapps de risico's voor gegevensbescherming vergroot: er worden meer gegevens verwerkt en gegevens worden aan meer entiteiten doorgegeven. De EDPB benadrukt dat het voor het vertrouwen in de app van groot belang is dat er voldoende transparantie is en dat gebruikers voldoende controle over hun gegevens hebben. Daarnaast wordt opnieuw gewezen op het tijdelijke karakter van een dergelijke maatregel, en het belang om doorlopend te blijven beoordelen of de maatregel nog doeltreffend is, en of er geen minder ingrijpend middel aangewezen is.⁶⁹

Samengevat, de Europese Commissie stelt zich vooruitstrevend op wat betreft het gebruik van corona-apps, en het EDPB stelt zich tot taak om de Commissie en de lidstaten te overtuigen van het belang van het recht op gegevensbescherming, óók in tijden van gezondheids crises. Uit het voorgaande

55 Aanbeveling (EU) 2020/518 van de Commissie van 8 april 2020 over een gemeenschappelijke toolbox voor het gebruik van technologie en gegevens om de COVID-19-crisis te bestrijden en te boven te komen, met name wat mobiele applicaties en het gebruik van geanonimiseerde mobiliteitsgegevens betreft, *PbEU* L 114/7 (hierna: Aanbeveling (EU) 2020/518).

56 Aanbeveling (EU) 2020/518, par. 15.

57 Aanbeveling (EU) 2020/518, par. 16.

58 Aanbeveling (EU) 2020/518, onder (1), doel van de aanbeveling.

59 Mededeling van de Commissie: Richtsnoeren in verband met gegevensbescherming voor apps ter ondersteuning van de bestrijding van de COVID-19-pandemie, 17 april 2020, *PbEU* C 124 I/1.

60 Mededeling van de Commissie: Richtsnoeren in verband met gegevensbescherming voor apps ter ondersteuning van de bestrijding van de COVID-19-pandemie, 17 april 2020, *PbEU* C 124 I/1.

61 'Coronavirus: EU interoperability gateway goes live, first contact tracing and warning apps linked to the system', persbericht Europese Commissie https://ec.europa.eu/commision/presscorner/detail/en/IP_20_1904 19 oktober 2020; Hiertoe heeft het Europees e-Health Network op 13 mei 2020 interoperabiliteitsrichtsnoeren voor goedgekeurde mobiele applicaties voor contactonderzoek in de EU aangenomen, zie: eHealth Network, *Interoperability guidelines for approved contact tracing mobile applications in the EU*, Brussel 13 mei 2020, https://ec.europa.eu/health/sites/default/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf.

62 European Data Protection Board, 'Statement by the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak', 16 maart 2020.

63 European Data Protection Board, 'Verklaring inzake de verwerking van persoonsgegevens in het kader van de COVID-19-uitbraak', aangenomen op 19 maart 2020.

64 Op 2 juni 2020 reageerde de European Data Protection Board op een Hongaars besluit om de AVG (ten dele) tijdelijk buiten werking te stellen en stelt dat de garanties van art. 23 lid 2 AVG in ieder geval in acht moeten worden genomen. Zie: European Data Protection Board, 'Verklaring inzake de beperkingen van rechten van betrokkenen in

verband met de noodtoestand in bepaalde lidstaten', https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-restrictions-data-subject-rights-connection-state_nl, vastgesteld op 2 juni 2020.

65 European Data Protection Board, *Richt snoeren 04/2020 voor het gebruik van locatiegegevens en instrumenten voor contacttracering in het kader van de uitbraak van COVID-19*, 21 april 2020.

66 Dit is bepaald in art. 6 en 9 van de E-privacyrichtlijn.

67 European Data Protection Board, *Richt snoeren 04/2020 voor het gebruik van locatiegegevens en instrumenten voor contacttracering in het kader van de uitbraak van COVID-19*, 21 april 2020.

68 European Data Protection Board, 'Verklaring over de gevolgen van de interoperabiliteit van contactonderzoeksapps voor de gegevensbescherming', vastgesteld op 16 juni 2020. Op 16 juni 2020 sprak de European Data Protection Board zich ook uit over de gevolgen voor gegevensbescherming van het heropenen van de grenzen, zoals testbewijzen, zie: European Data Protection Board, 'Verklaring over de verwerking van persoonsgegevens in de context van het heropenen van de grenzen na de uitbraak van COVID-19', vastgesteld op 16 juni 2020.

69 European Data Protection Board, 'Verklaring over de gevolgen van de interoperabiliteit van contactonderzoeksapps voor de gegevensbescherming', vastgesteld op 16 juni 2020.

70 Deze conclusie wordt ook getrokken in de eerste wetevaluatie van de AVG, zie: 'Communication from the Commission to the European Parliament and the Council. Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation', Europese Commissie 24 juni 2020, COM(2020)264 final.

71 J. Horowitz & A. Satariano, 'Europe Rolls Out Contact Tracing Apps, With Hope and Trepidation', *The New York Times* 16 juni 2020.

72 Art. 23 AVG, art. 8 lid 2 EVRM en art. 51 Handvest.

73 Gegevens over de gezondheid worden beschouwd als 'bijzondere gegevens' en verdienen extra bescherming op grond van art. 9 AVG.

74 Autoriteit Persoonsgegevens, Advies over het concept voor wijziging van de Telecommunicatiewet in verband met informatieverstrekking aan het RIVM

volgt dat nood geen breken van de wet behoeft in het geval van gezondheids crises; het Europese juridische kader voorziet in de mogelijkheid tot bepaalde beperkingen ter bestrijding van noodsituaties. De AVG is flexibel genoeg voor gebruik in bijvoorbeeld een infectieziektenuitbraak.⁷⁰ Toch lijken veel lidstaten in de strijd tegen COVID-19 het grondrecht op gegevensbescherming op disproportionele wijze te beperken, bijvoorbeeld in corona-apps.

Veel lidstaten lijken in de strijd tegen COVID-19 het grondrecht op gegevensbescherming op disproportionele wijze te beperken, bijvoorbeeld in corona-apps

5 Europese corona-apps en gevolgen voor het recht op gegevensbescherming

In heel Europa heeft de invoering van corona-apps tot discussie geleid over de waarborgen voor gegevensbescherming.⁷¹ De verschillende categorieën apps die in Europa worden ingezet in de strijd tegen COVID-19 verwerken persoonsgegevens, waardoor ze onder de werkingssfeer van de AVG en binnen de reikwijdte van het recht op privéleven vallen. Lidstaten mogen het recht op gegevensbescherming beperken, mits hier een duidelijke noodzaak voor is, voldaan is aan de eisen van proportionaliteit en subsidiariteit en voldoende waarborgen ingebouwd zijn, en een grondslag bestaat, dit transparant gebeurt en alleen de noodzakelijke persoonsgegevens worden verwerkt.⁷² Ondanks de geharmoniseerde wetgeving en coördinatie vanuit de EU zijn er grote verschillen tussen beperkingen. De impact op het recht op gegevensbescherming is vooral afhankelijk van het type app, de te verwerken persoonsgegevens, ingebouwde waarborgen en proportionaliteit.

5.1 Typen persoonsgegevens

De meeste corona-apps verzamelen persoonsgegevens zoals telefoonnummers en IP-adressen, maar soms ook gevoelige informatie zoals gegevens over de gezondheid.⁷³ Zo werken *epidemiologische apps* op basis van grote hoeveelheden (persoons)gege-

vens uit verschillende bronnen. Er wordt hiervoor soms gebruik gemaakt van telecomdata. Deze data zegt veel over een individu, namelijk waar hij zich op welk moment bevindt. Hoewel de locatiegegevens gepseudonimiseerd zijn, kan nog steeds worden achterhaald om wie het gaat.⁷⁴ *COVID-19-screeningsapps* verzamelen naast reguliere persoonsgegevens ook vaak gezondheidsgegevens.⁷⁵ Indien de apps zelfdiagnoses en symptoomcontroles uitvoeren, wordt er informatie verwerkt over welke ziektesymptomen gebruikers hebben. Apps met een telegeneeskunde-functie, zoals de telefonische begeleiding, kunnen ook contactgegevens verwerken. De meeste Europese *contactopsporingsapps* verwerken relatief weinig persoonsgegevens: ze wisselen gerandomiseerde codes uit met andere telefoons. Ontwikkelaars stellen daarom dat deze codes in principe niet tot personen herleidbaar zijn, waardoor de bepalingen van de AVG niet van toepassing zijn.⁷⁶ In de praktijk lijkt het echter het voor gebruikers mogelijk de identiteit van de besmette persoon te achterhalen, door simpelweg in kaart te brengen wie er de afgelopen dagen langer dan 15 minuten in de buurt was. Ook kunnen de gerandomiseerde codes die appgebruikers uitzenden, door middel van technologie ontvangen en geregistreerd worden door anderen. Indien er weinig personen in de omgeving zijn, kan er een code aan een naam worden gekoppeld. Wanneer een persoon later een positieve testuitslag meldt in de app, is bekend welke naam bij de code hoort.⁷⁷ Sommige Europese contactopsporingsapps verwerken, ondanks de richtsnoeren van de EDPB, meer persoonsgegevens, zoals telefoonnummers. Ook de Poolse en Hongaarse *handhavingsapps* verwerken gevoelige persoonsgegevens en gezondheidsgegevens, zoals bijvoorbeeld selfies en locatiegegevens van patiënten in quarantaine, en het feit dat gebruikers (mogelijk) besmet zijn met het coronavirus.⁷⁸

5.2 Effectieve waarborgen

Onder artikel 23 AVG is beperken van de rechten van betrokkenen en de beginselen inzake verwerking van persoonsgegevens met het oog op de bescherming van de volksgezondheid toegestaan mits er bepaalde wettelijke waarborgen zijn.⁷⁹ Uit de jurisprudentie van het EHRM en het HvJ EU over het recht op privéleven blijkt het belang van voldoende waarborgen voor de beoordeling van de proportionaliteit van

een beperking.⁸⁰ Het gaat dan met name om effectieve bescherming, effectieve controlemechanismen, minimale gegevensverwerking, gespecificeerde bewaartermijnen en het waarborgen van specifieke rechten en plichten.⁸¹ De EDPB heeft gesteld dat het verwerken van telecomgegevens voor *epidemiologische apps* alleen mag indien strikt noodzakelijk voor de bescherming van de volksgezondheid, en de verwerking redelijk en proportioneel is. Ook moet de voorkeur worden gegeven aan verwerking van geanonimiseerde datasets.⁸² De Raad van State adviseerde om in het Nederlandse wetsvoorstel over telecomdata⁸³ op te nemen dat de noodzaak voor de bestrijding van COVID-19 periodiek getoetst moet worden.⁸⁴ Omdat *COVID-19-screeningsapps* veelal gezondheidsgegevens verwerken, moeten deze apps aan extra waarborgen voldoen. In de meeste *privacy policies* wordt gespecificeerd welke categorieën persoonsgegevens worden verzameld, wat de bewaartermijn per categorie is, met wie gegevens worden gedeeld, en hoe gebruikers hun rechten kunnen uitoefenen.⁸⁵ Indien een arts betrokken is, worden gebruikers ook nog beschermd door diens beroepsgeheim.⁸⁶ Ook de *contactopsporingsapps* voorzien in veel waarborgen: de apps zijn vrijwillig, de meeste apps slaan persoonsgegevens lokaal op en hebben een korte bewaartermijn. Ook de Poolse en Hongaarse *handhavingsapps* hebben voorzieningen getroffen ten aanzien van de opslagbeperking en minimale gegevensverwerking. De enige waarborg die in de meeste apps in alle categorieën mist is de effectieve controle op het gebruik van gegevens: het ontbreekt aan effectieve controlemechanismen.⁸⁷

De enige waarborg die in de meeste apps in alle categorieën mist is de effectieve controle op het gebruik van gegevens: het ontbreekt aan effectieve controlemechanismen

5.3 Noodzakelijkheid, proportionaliteit en subsidiariteit

In het geval van *epidemiologische apps*, en dan met name de apps die werken op basis van telecomdata, speelt de noodzakelijkheid een grote rol. In hoeverre is het

verzamenen van deze gegevens noodzakelijk voor het in kaart brengen van de verspreiding van COVID-19? Zijn er geen middelen voorhanden die minder ingrijpend zijn? Argumenten met betrekking tot noodzakelijkheid, subsidiariteit en proportionaliteit wegen zwaarder in het geval van telecomdata dan andere bronnen, omdat er geen toestemming wordt gevraagd van betrokkenen en dit type gegevens grote inbreuk maakt op het privéleven van betrokkenen. Hoewel wetgeving op het gebied van telecommunicatie deels geharmoniseerd is in Europa, is de belangenafweging tussen het recht op privéleven en bescherming van het algemeen belang aan de lidstaten zelf. De *COVID-19-screeningsapps* verwerken veel persoonsgegevens, waaronder gezondheidsgegevens. Vragen over de rechtmatigheid van de beperking van het recht op gegevensbescherming zullen bij deze apps voornamelijk zien op de proportionaliteit van de hoeveelheid persoonsgegevens: in hoeverre zijn deze gegevens echt nodig om het doel te bereiken? Kunnen er ook minder gegevens verwerkt worden om een algoritme een diagnose te laten stellen? De Europese *contactopsporingsapps* zijn het meest gescreend op effecten voor databescherming en privacy, en bevatten vaak dan ook strikte waarborgen. Toch zijn er verschillen in de waarborgen van Europese apps die gevolgen kunnen hebben voor de proportionaliteit van de gegevensverwerking, bijvoorbeeld wat de bewaartermijn betreft. Sommige apps verwijderen persoonsgegevens gerelateerd aan besmettingen automatisch na 14 dagen na de notificatie, anderen stellen de bewaartermijn afhankelijk van de duur van de noodtoestand.⁸⁸ Met betrekking tot *contactopsporingsapps* lijkt het grootste bezwaar in de noodzakelijkheid van de beperking te liggen: in hoeverre dragen deze apps echt bij aan het beschermen van de volksgezondheid? De EDPB stelt dat wetenschappelijke onderbouwing hierbij van groot belang is, en bij de meeste *contactopsporingsapps* ontbreekt deze tot op heden.⁸⁹ De twee Europese *handhavingsapps* voor verplichte quarantaine lijken, van de vier categorieën apps, de grootste impact te hebben op het privéleven van gebruikers. Niet alleen is het gebruik van de apps verplicht, ook verwerken de apps de meeste persoonsgegevens, waaronder gevoelige gegevens zoals foto's en langdurige monitoring van locatie. Daarnaast zijn de waarborgen beperkt: de

(COVID-19 crisis) vastgesteld en per e-mail toegezonden op donderdag 14 mei jl., DGBI-DE / 20144557.

75 Art. 4 lid 15 AVG.

76 Art. 4 lid 1 AVG.

77 M. van Dongen, 'Techcriticus: "CoronaMelder is niet anoniem, maar pseudoniem"', *de Volkskrant* 2 november 2020.

78 Norton Rose Fulbright 2021.

79 Art. 23 lid 1 AVG.

80 H.B. van Kolschooten & A. de Ruijter, 'COVID-19 and privacy in the European Union: A legal perspective on contact tracing', *Contemporary Security Policy* (41) 2020, afl. 3, p. 478-491.

81 Deze aanknopingspunten uit de rechtspraak komen overeen met de gegevensbeschermingsbeginselen van de AVG. Zie art. 23 lid 1 en 2 AVG en Article 29 Working Party, 'Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector', 27 februari 2014 (536/14/EN WP 211).

82 European Data Protection Board, *Richtlijn 04/2020 voor het gebruik van locatiegegevens en instrumenten voor contacttracing in het kader van de uitbraak van COVID-19*, 21 april 2020.

83 Tijdelijke wet informatieverstrekking RIVM in verband met COVID-19.

84 Advies Tijdelijke wet informatieverstrekking RIVM i.v.m. COVID-19, 25 mei 2020, W18.20.0144/IV.

85 Zie bijvoorbeeld de privacy policy van de Schotse 'NHS 24 COVID-19 and flu information'-app. De privacy policy kan geraadpleegd worden bij downloaden van de app.

86 Dit is het geval bij de Nederlandse 'De Corona Check'-app, zie: 'Gebruiksvoorwaarden en privacy statement', <https://decoronacheck.nl/gebruiksvoorwaarden-en-privacystatement/> 17 september 2020.

87 J. van Dijk & A. Meijer, 'Een goede corona-app vergt publieke controle', *de Volkskrant* 22 april 2020.

88 Zoals de Italiaanse app 'Im-muni', zie: 'Informativa privacy', www.immuni.it/it/app-pn.html (automatisch vertaald van Italiaans naar Engels met Google Translate).

89 European Data Protection Board, *Richtlijn 04/2020 voor het gebruik van locatiegegevens en instrumenten voor contacttracing in het kader van de uitbraak van COVID-19*, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_nl 21 april 2020.

bewaartermijnen zijn lang (zes jaar), en gegevens worden niet op het toestel zelf opgeslagen, maar op de centrale servers van de overheid. Hier kunnen beveiligingsproblemen bij komen kijken.⁹⁰ Gelet op het doel – controleren van de verplichte quarantaine met het oog op het beschermen van de volksgezondheid – is het de vraag of het verplicht stellen van deze app niet te ver gaat. Er zijn minder ingrijpende middelen beschikbaar om dit doel te bereiken, zoals bijvoorbeeld steekproefsgewijze controles per telefoon, en de app zou kunnen volstaan met een minder ruime verwerking van persoonsgegevens. Hoewel veel Europese corona-apps het belang van de bescherming van volksgezondheid laten prevaleren, komt deze belangenafweging het duidelijkst naar voren in de twee handhavingsapps.

Het is de taak van de EU om lidstaten te blijven wijzen op het belang van het recht op gegevensbescherming, óók in tijden van gezondheids crises. Anders is de langdurige strijd voor het meest privacyvriendelijke continent voor niets gestreden

6 Conclusie

In de strijd tegen de COVID-19-pandemie vertrouwen miljoenen Europeanen gevoelige persoonsgegevens toe aan corona-apps. Aan de veelzijdigheid van corona-apps is te zien dat Europese lidstaten het recht op gegevensbescherming niet allemaal op dezelfde manier beschermen. Het doel van

de AVG, het bieden van een hoog en gelijkwaardig niveau van gegevensbescherming voor elke Unieburger, lijkt daarmee op scherp te staan. In de eerste paniek over de uitbraak van het coronavirus hebben meerdere lidstaten het grondrecht op gegevensbescherming beperkt, onder het mom van ‘uitzonderlijke tijden vragen om uitzonderlijke maatregelen’. In de retoriek van het valse dilemma lijkt deze weg gerechtvaardigd: wie geeft nog om privacy als *big data* potentieel levens kan redden? Hiermee begeven we ons op een hellend vlak. Het beperken van gegevensbescherming zal vermoedelijk steeds gebruikelijker worden in het kader van de bescherming van het algemeen belang. Bovendien is gegevensbescherming van groot belang voor de doeltreffendheid van digitale maatregelen: adequate bescherming van persoonsgegevens is noodzakelijk voor het opbouwen van vertrouwen, en daarmee voor de maatschappelijke aanvaardbaarheid van een crisismaatregel zoals de inzet van een corona-app.

Wat de lidstaten daarnaast over het hoofd zien, is dat het Europees juridisch kader crisissituaties incalculeert en in de mogelijkheid voorziet tot bepaalde beperkingen ter bestrijding van noodsituaties, waaronder gezondheids crises. Dat betekent dat bescherming van het recht van burgers op gegevensbescherming hand in hand kan gaan met de bescherming van de samenleving tegen de gevolgen van infectieziekten uitbraken. Lidstaten kunnen de balans opmaken binnen de grenzen van de wet. Het is de taak van de EU om lidstaten te blijven wijzen op het belang van het recht op gegevensbescherming, óók in tijden van gezondheids crises. Anders is de langdurige strijd voor het meest privacyvriendelijke continent voor niets gestreden.

90 Norton Rose Fulbright 2021.