Body surveillance in de coronacrisis:
Welke gegevens worden verzameld en wie kan erbij?

Sarah Stapel

CREDITS: MAXIM HOPMAN ON UNSPLASH

BITS OF FREEDOM

Inhoud

1. Inleiding
2. Body surveillance
3. De selectie: Vier corona-maatregelen
4. Welke gegevens worden verzameld?
5. Waar komen de gegevens terecht en wie kan erbij?
6. Overzicht van gegevensverwerking
7. De aandachtspunten: normalisering en noodzakelijkheid
8. Conclusie

1. Inleiding

Tijdens de corona-crisis is de overheid druk bezig met het uitvoeren van maatregelen ter bestrijding van het virus. Beleid en nieuwe technologieën worden met spoed ontwikkeld. Vaak gaat dit hand in hand met de verwerking van gevoelige gegevens, bijvoorbeeld gegevens over de gezondheid van burgers. Wat houden deze maatregelen in voor ons recht op gegevensbescherming? Hoe verhouden de nieuwe wetten zich tot de vereisten en waarborgen die van toepassing zijn op de verwerking van bijzondere gegevens?

Dit onderzoek richt zich op de gegevensverwerking van vier 'corona-maatregelen': **de CoronaMelder, de wijziging van de Telecommunicatiewet, de Corona Opt-in en het gezondheidspaspoort**. Waarbij twee vragen centraal staan: 1) Welke gegevens worden er met deze maatregelen verzameld? en 2) Waar komen deze gegevens terecht?

De theorie van *body surveillance* wordt als selectiemechanisme ingezet om de omvang van het onderzoek te beperken. *Body surveillance* verwijst naar de praktijk en het beleid waarmee instanties de controle uitoefenen op individuen met betrekking tot hun lichaam. Bijvoorbeeld bij gezondheids- en locatiegegevens.

In het tweede hoofdstuk wordt de theorie van *body surveillance* behandeld. In het derde hoofdstuk wordt de selectie van corona-maatregelen geïntroduceerd en wordt gekeken naar hoe deze maatregelen betrekking hebben op *body surveillance*. In het vierde hoofdstuk wordt in kaart gebracht welke *body data* (gegevens over je lichaam) er per maatregel worden verwerkt. In het vijfde hoofdstuk wordt er gekeken naar waar deze gegevens terechtkomen en wie er bij kan. In het zesde hoofdstuk worden de normalisering en noodzakelijkheid van de verwerking van *body data* behandeld.

2. Body Surveillance

De theorie van *body surveillance* maakt het mogelijk op een gerichte wijze te kijken naar welke gegevens er worden verwerkt en waar die terechtkomen. Volgens deze theorie is het lichaam een belangrijk symbool voor de fysieke, sociale en politieke autonomie van individuen. De verwerking van gegevens over het lichaam heeft een impact op deze autonomie. *Body surveillance* kijkt verder dan de juridische definities en rechtvaardiging van gegevensverwerking en geeft daardoor inzicht in de bredere impact van de corona-maatregelen.

2.1. Wat is surveillance?

Body surveillance is een specifieke vorm van surveillance die bovenal kennis vereist van het begrip surveillance. David Lyon, directeur van het Surveillance Studies Center, heeft aanzienlijk bijgedragen aan surveillancestudies en een veel geciteerde definitie van surveillance ontwikkeld:[1]

Lyon definieert surveillance als de *"gerichte, systematische en routinematige aandacht voor persoonlijke gegevens met het oog op beïnvloeding, controle, bescherming of richting."*[2]

De definitie van Lyon omschrijft een vorm van surveillance die meerdere middelen kan gebruiken en op meerdere manieren invloed heeft. Het is belangrijk om surveillance niet als totalitaire machtsuitoefening te zien. Surveillance bestaat uit meerdere en vaak juist subtiele vormen van beïnvloeding en controle. Surveillance kan ook voor 'positieve' doelen ingezet worden, bijvoorbeeld voor hulp en genezing en bijvoorbeeld ook voor bevordering van de volksgezondheid. Hiernaast betoogt Lyon dat de gegevens van de gegevensverwerking *niet herleidbaar tot echte personen of zaken behoeven te zijn*. Het kan bijvoorbeeld voorkomen dat er geen sprake is van een persoon op wie de surveillance gericht is maar bijvoorbeeld op een bedrijf of een grotere entiteit.

2.2. Wat is body surveillance?

Body surveillance, met verwijzing naar de definitie van Lyon, is het *gericht, systematisch en routinematig aandacht geven aan gegevens met betrekking tot het lichaam, met het oog op beïnvloeding, controle, bescherming of richting.*

Of er sprake is van *body surveillance* wordt beoordeeld op grond van de vraag hoe er aandacht wordt gegeven aan persoonsgegevens met betrekking tot het lichaam, en in het verlengde daarvan hoe systematisch het is, hoe routinematig het is en wat de doeleinden zijn.

Politieke en sociale autonomie

1 The Electronic Eye: The Rise of Surveillance Society (1994); Surveillance Society: Monitoring Everyday Life (2001); Surveillance after September 11 (2003); Surveillance Studies: An Overview (2007); Surveillance After Snowden (2015).

2 David Lyon, Surveillance Studies: An Overview (2007): "the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction."

Body surveillance betreft meer dan alleen een privacy perspectief in termen van gegevensverwerking maar kijkt ook naar de politieke en sociale gevolgen. Zo'n beoordeling plaatst vraagtekens bij de grotere invloed die deze maatregelen hebben op de samenleving en de relaties en verhoudingen daarin.

Natali Helberger, hoogleraar recht en digitale technologie aan de Universiteit van Amsterdam zegt hierover het volgende: "De apps [die worden uitgerold met de maatregelen, zoals de CoronaMelder] hebben impact op meer dan (data)privacy alleen. Ze raken ook aan de vrijheid van vereniging, het recht op veiligheid, de menselijke waardigheid, het recht op gezondheid en het recht op non-discriminatie."[3]

Een *body-surveillance*-analyse benadrukt verder de relatie en de machtsverhouding tussen degenen die surveilleren en degenen die gesurveilleerd worden. Dit volgt uit het werk van de Franse filosoof Michel Foucault.[4] Foucault beweerde dat overheden vaak sociale controle proberen vast te leggen door macht uit te oefenen over de lichamen, en dus de autonomie, van burgers.[5]

***Biomacht*: het monitoren van de gezondheid**

Michel Foucault's concept van *biomacht* omschrijft de sinistere kant van machtsuitoefening in de zorg: wanneer de overheid zich beroept op het gerechtvaardigde belang om de volksgezondheid te beschermen kan deze grondslag altijd worden gebruikt als rechtvaardigingsgrond.[6] Dit kan leiden tot een routinematige vorm van *body surveillance*. Zo kunnen gegevens over jouw locatie, gezondheid en gedrag worden verwerkt zonder de strenge voorwaarden die daar normaal gesproken aan verbonden zijn.

Body data geven inzicht in jouw mentale en fysieke staat en zijn daardoor hoogstpersoonlijk. Het is niet wenselijk dat deze data met meerdere mensen en instanties wordt gedeeld. Het is niet wenselijk dat deze data worden gebruikt om belangrijke keuzes te maken over individuen met informatie die in eerste instantie privé hoort te zijn. Individuele controle over deze gevoelige informatie is belangrijk voor de autonomie en moet vervolgens niet zomaar worden verwerkt.

---

3 Brief aan het Ministerie van Algemene Zaken, het Ministerie van Volksgezondheid, Welzijn en Sport en het Ministerie van Justitie en Rechtsbescherming inzake: COVID-19 tracking- en tracingapp en gezondheidapp (2020, 13 april). Geraadpleegd via https://www.uva.nl/content/nieuws/nieuwsberichten/2020/04/kijk-kritisch-naar-nut-en-noodzaak-corona-apps.html.

4 Foucault, M. 1973. *The Birth of the Clinic: An Archaeology of Medical Perception*. New York Random House; Foucault, M. 1977. *Discipline and Punish: The Birth of the Prison*. New York: Random House.

5 Foucault, M. 1977. *Discipline and Punish: The Birth of the Prison*. New York: Random House, p. 208.

6 Foucault, M. 1973. *The Birth of the Clinic: An Archaeology of Medical Perception*. New York Random House, p. 1977.

3. De selectie: Vier corona-maatregelen

De overheid en andere instanties hebben meerdere maatregelen afgekondigd ter bestrijding van het coronavirus. Vier maatregelen waar dit onderzoek zich op zal richten zijn **de CoronaMelder, de tijdelijke wijziging van de Telecommunicatiewet, de Corona opt-in en het gezondheidspaspoort.** Dit hoofdstuk legt uit wat deze maatregelen inhouden, hoe zij werken en hoe zij betrekking hebben op *body surveillance*.

3.1. CoronaMelder

De *CoronaMelder* is de Nederlandse 'exposure-notification'-applicatie met als doel het traceren en melden van de risico op coronabesmettingen om daardoor verdere besmettingen te voorkomen (de Nederlandse corona-app). Het ministerie van Volksgezondheid, Welzijn en Sport (VWS) heeft begin oktober de *CoronaMelder* landelijk beschikbaar gesteld.[7]

Hoe werkt het?

De *CoronaMelder* is een mobiele applicatie die vrijwillig kan worden gebruikt. De app gebruikt door Apple en Google ontwikkelde technologie. Via Bluetooth Low Energy houdt de app bij of je in contact bent gekomen met een andere app-gebruiker. De telefoons wisselen unieke codes en signaalsterkte met elkaar uit, die om de 10 tot 20 minuten veranderen om zo de herleidbaarheid te voorkomen. De gebruiker kan vrijwillig in de app invoeren of hij/zij/hen positief is getest op corona. Zodra een positief testresultaat (goedgekeurd door de GGD) is ingevoerd krijgt iedereen waarmee zij/hij/hen contact heeft gehad een melding. 'Contact' wordt gezien als een interactie van minstens vijftien minuten binnen of op anderhalve meter van een andere gebruiker. Deze melding stimuleert de gebruiker om zich te laten testen op corona.

Bekijk hier een filmpje van de NOS dat de technische werking samenvat.

Wat is het doel?

De *CoronaMelder* is ontwikkeld als aanvulling op de bron- en contactopsporing van de GGD. Het doel ervan is om gebruikers met een verhoogde besmettingskans snel en op eenvoudige wijze te informeren, met een hoge mate van anonimiteit.[8]

CoronaMelder en *body surveillance*

Sociale controle over het menselijk lichaam, de kern *van body politics*, is een principieel doel van de corona-app. Het feit dat de medische gegevens worden gepseudonimiseerd betekent echter niet dat er geen sprake kan zijn van surveillance. Pseudonimisering is een proces waarbij identificeerbare gegevens worden omgezet in versleutelde

[7] Wet van 6 oktober 2020, houdende tijdelijke bepalingen in verband met de inzet van een notificatieapplicatie bij de bestrijding van de epidemie van covid-19 en waarborgen ter voorkoming van misbruik daarvan (Tijdelijke wet notificatieapplicatie covid-19), Stb. 2020, 374.

8 Privacyverklaring CoronaMelder. Geraadpleegd via https://coronamelder.nl/nl/privacy-in-app.

gegevens.[9] Het is een proces die vaak wordt uitgevoerd om het risico tot herleidbaarheid te minimaliseren. Maar het versleutelproces is omkeerbaar waardoor het *alsnog* mogelijk is om een persoon te identificeren.[10] Bijzondere en gevoelige informatie, met name medische gegevens, worden met deze maatregel routinematig verwerkt.

3.2. Wijziging Telecommunicatiewet

De Tijdelijke wet informatieverstrekking RIVM in verband met COVID-19 is op 29 mei 2020 in de Tweede Kamer ingediend door de staatssecretaris van Economische Zaken en Klimaat. Het wetsvoorstel "creëert een grondslag in hoofdstuk 14 van de Telecommunicatiewet om aanbieders van openbare mobiele telecommunicatienetwerken te verplichten informatie te verstrekken aan het Rijksinstituut voor volksgezondheid en milieu (RIVM)."[11]

Hoe werkt het?

Het wetsvoorstel maakt tellingen mogelijk van het aantal personen dat per uur in een gemeente aanwezig is. Dit wordt uitgerekend op grond van locatie- en verkeersgegevens van mobiele apparaten binnen een gemeente. Op grond van deze tellingen krijgt het RIVM een goed inzicht in de mate van 'menging' tussen gemeentes.

In de Memorie van Toelichting wordt een voorbeeld van de toepassing van deze maatregel genoemd: "Als bekend is dat er veel meer mensen dan normaal op eenzelfde tijdstip uit Bergen op Zoom in Roosendaal zijn geweest op een zaterdagmiddag, en als de gegevens voor de rest van Nederland normaal zijn, dan kan dit voor het RIVM aanleiding zijn om het signaal te geven aan de GGD West-Brabant dat als er COVID-19 patiënten in Roosendaal worden gevonden, er ook een verhoogd risico is geweest op transmissie van COVID-19 voor inwoners in Bergen op Zoom."[12] Het voorbeeld dat hier wordt gegeven ontbreekt een aantal details, namelijk waarom er naar deze locaties wordt gekeken en waarom deze informatie belangrijk is. Die aanvullende informatie moet in de praktijk ook worden uitgelegd.

Wat is het doel?

In de wetsgeschiedenis wordt verwezen naar meerdere doelen:

1. **Om stelselmatige drukte te monitoren**[13]

9 Zie Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene verordening gegevensbescherming) overweging 28.

10 Houwing, L. (2020, 15 juli) De corona-app: technische vooruitgang, nog steeds een surveillancemiddel. Geraadpleegd via https://www.bitsoffreedom.nl/2020/07/15/de-corona-app-technische-vooruitgang-nog-steeds-een-surveillancemiddel/.

11 Tijdelijke bepaling in verband met de informatieverstrekking aan het RIVM bij de bestrijding het novel coronavirus (2019-nCoV) (Tijdelijke wet informatieverstrekking RIVM i.v.m. COVID-19).

12 Memorie van Toelichting op de Tijdelijke wet informatieverstrekking RIVM i.v.m. COVID-19, p. 3.

13 Tijdelijke wet informatieverstrekking RIVM i.v.m. COVID-19.

2. **Om verplaatsingen te monitoren**[14]
3. **Om regionale signalen af te geven:** "het kunnen signaleren van een verhoogd risico op besmettingen aan de hand van de mate van drukte in een gemeente en het aantal bezoekers uit andere gemeenten, om daarmee het lokale bestuur te kunnen waarschuwen en adviseren over handelingsperspectief"[15]
4. **Om de effectiviteit van de maatregelen te monitoren:** "neemt de drukte in een bepaalde regio of op een bepaald tijdstip, zoals de spits of in de avond, af als gevolg van maatregelen?"[16]
5. **Om "snel en gericht op het virus te kunnen reageren"**[17]
6. **"Het verder versoepelen van de beperkingen die de intelligente lockdown met zich brengt"**[18]

Wijziging Telecommunicatiewet en *body surveillance*

Het monitoren van de verplaatsing van bevolking (mensen, populaties) is een vorm van *body surveillance*. Deze maatregel richt zich op het systematisch en routinematig aandacht geven aan de locatie- en verkeersgegevens met het oog op controle.

Locatiegegevens zijn extreem gevoelige gegevens die veel inzicht geven over de identiteit en het gedrag van de betrokkenen. Het wetsvoorstel betoogt dat er alleen zal worden gekeken naar de verplaatsing van bevolking (mensen, populaties) per gemeente op het moment dat de telefoon een actieve verbinding maakt met de zendmast. Om dit te realiseren vindt er echter verwerking plaats op een individueel niveau en dus niet alleen op een groepsniveau. Voor dit wetsvoorstel was er al sprake van verwerking op en individueel niveau door de telecomproviders. Maar vindt die verwerking plaats op een *nieuwe* server wat een verhoogd risico van een datalek of onrechtmatige verwerking met zich meeneemt.

3.3. Corona opt-in

In reactie op de toenemende druk tijdens de coronacrisis op de huisartsenposten (HAP) en de spoedeisende hulp (SEH), heeft het ministerie van Volksgezondheid, Welzijn en Sport op 8 april 2020 een maatregel genomen om gemakkelijker toegang te krijgen tot huisartsgegevens. Deze maatregel heeft *nog geen juridische basis*, maar hier wordt volgens het ministerie aan gewerkt.[19]

Het ministerie heeft ervoor gekozen om toegang te verlenen tot

14 Tijdelijke wet informatieverstrekking RIVM i.v.m. COVID-19.
15 Keijzer, M.C.G. (2020, 2 oktober) Tijdelijke wet informatieverstrekking RIVM ivm COVID-19 (35 479) [Kamerbrief] p. 7 jo. 9.
16 Keijzer, M.C.G. (2020, 2 oktober) Tijdelijke wet informatieverstrekking RIVM ivm COVID-19 (35 479) [Kamerbrief] p. 7 jo. 9
17 Keijzer, M.C.G. (2020, 2 oktober) Tijdelijke wet informatieverstrekking RIVM ivm COVID-19 (35 479) [Kamerbrief] p. 9; Tijdelijke bepaling in verband met de informatieverstrekking aan het RIVM bij de bestrijding het novel coronavirus (2019-nCoV) (Tijdelijke wet informatieverstrekking RIVM i.v.m. COVID-19) [MvT] p. 4.
18 Tijdelijke wet informatieverstrekking RIVM i.v.m. COVID-19. [MvT] p. 2.
19 Van Ark, T. (2020, 2 oktober) Elektronische gegevensuitwisseling in de zorg [Kamerbrief].

huisartsgegevens van meerdere patiënten. De gegevens betreffen de "professionele samenvatting" van het medisch dossier. Deze samenvatting bevat volgens het ministerie alleen de "belangrijkste gegevens".[20] Artsen van de HAP en SEH krijgen toegang tot deze gegevens op grond van deze maatregel. Ook andere zorgverleners kunnen door deze maatregel de medische gegevens van hun patiënten via het Landelijke Schakelpunt (LSP) opvragen en uitwisselen.[21]

Hoe werkt het?

Vóór deze maatregel was toegang van de HAP en SEH tot deze gegevens alleen mogelijk met voorafgaande toestemming (opt-in) van de patiënt. Met deze maatregel wordt dit omgedraaid: Iedereen die niet actief opt-out wordt automatisch als opt-in geregistreerd.

Dit zorgt er dus voor dat jouw gezondheidsgegevens worden gedeeld, tenzij jij aangeeft dat je dat niet wilt.

Volgens de Autoriteit Persoonsgegevens zijn er maatregelen genomen om voldoende waarborgen te bieden, met name de mogelijkheid om bezwaar te maken, het alsnog verplichten van toestemming tot inzage en het beperken van toegang tot de HAP en de SEH. Technisch gezien, is het niet mogelijk om toegang in deze mate te beperken. Het LSP maakt het niet mogelijk om gericht, dus over een specifieke patiënt via een specifieke zorgverlener, informatie te ontvangen. Dit houdt in dat iedere zorgverlener in principe toegang heeft tot de de gehele professionele samenvatting van de medische gegevens van patiënten.

Wat is het doel?

Het doel, volgens het ministerie van VWS is om de gezondheidszorg te helpen sneller en effectiever te kunnen reageren tijdens de coronacrisis. Als jij opeens behandeld moet worden door een andere arts dan van jouw vaste zorgverlener, is het noodzakelijk dat zij spoedig toegang kunnen krijgen tot jouw medische gegevens zodat zij weten hoe zij jou wel/niet moeten behandelen. Denk hier bijvoorbeeld aan allergieën voor bepaalde medicijnen.

Corona opt-in en *body surveillance*

De professionele samenvatting bevat patiëntendossiers met gegevens over de gezondheid. Hierdoor is er sprake van verwerking van *body data*. Daarnaast is er ook sprake van *body surveillance*, gezien de machtsverhouding die er ontstaat door de *opt-in methode*. Het automatisch registeren van patiënten als *opt-in* zonder dat ze daar toestemming voor hebben verleend maakt inbreuk op het privacyrecht. Het argument dat patiënten alsnog toestemming moeten verlenen voor inzage tot hun gegevens, is zoals genoteerd door Privacy First, een "holle formaliteit"[22]: ongeacht of de

20 Van Ark, T. (2020, 2 oktober) Elektronische gegevensuitwisseling in de zorg [Kamerbrief] p. 6.
21 Zie ook Jongejan W. J (2020, 30 maart) Corona-opt-in voor LSP: haken en ogen plus proportionaliteit. Geraadpleegd via https://www.zorgictzorgen.nl/corona-opt-in-voor-lsp-haken-en-ogen-plus-proportionaliteit/.
22 Privacy First (2020, 15 april) 'Corona opt-in' zet medisch beroepsgeheim buitenspel. Geraadpleegd via

patiënt toestemming geeft, zal diens dossier namelijk technisch al openstaan voor raadpleging vanuit tienduizenden toegangspunten. Met het geven van toestemming als de hoeksteen van het privacyrecht en de individuele autonomie, is de opheffing ervan zorgelijk. Zo heeft ruim de helft van de bevolking geen uitdrukkelijke toestemming gegeven.[23] Zonder die toestemming worden patiënten in een nadelige positie geplaatst als hun gegevens op een server met veel toegangspoortjes terechtkomen.

3.4. Gezondheidspaspoort

Meerdere internationale ontwikkelaars hebben een zogenaamd digitaal 'gezondheidspaspoort' gecreëerd om geleidelijk de corona-beperkingen op te heffen.[24] Zo'n digitaal bewijs van gezondheid wordt vaak gekoppeld aan een 'sneltest'. Dit is een nieuwe manier van testen op het coronavirus dat sneller resultaten kan opleveren. In Nederland zijn er voornamelijk twee partijen bezig met het ontwikkelen van een paspoort. Ten eerste heeft het **uNLock** consortium een initiatief genomen om een non-profit applicatie te ontwikkelen die een bewijs van coronatest of vaccinatie aan kan geven.[25] Dit consortium bestaat uit onder andere de Organisatie voor toegepast-natuurwetenschap (TNO), Dutch Blockchain Coalition, CMS Advocaten en professoren van de Universiteit Leiden en de Technische Universiteit Delft. De pilot van deze app werd 10 december 2020 uitgevoerd. Ten tweede heeft het ministerie van Volksgezondheid, Welzijn en Sport plannen om een nieuwe **Coronatester App** te ontwikkelen. Dit blijkt uit een vacature die 20 november in een blog hebben geplaatst.[26]

Hoe werkt het?

Omdat er meerdere aanbieders zijn, zijn er ook meerdere versies van het gezondheidspaspoort. Zie bijvoorbeeld hier een filmpje over het paspoort dat wordt ontwikkeld door uNLock. Volgens uNLock is het gebruik van de app afhankelijk van de specifieke context, wat iedere keer weer een nieuwe analyse vereist. Verder zei een woordvoerder van het ministerie met betrekking tot de Coronatester app dat alle opties nog open zijn.[27] Toch zijn er

https://www.privacyfirst.nl/aandachtsvelden/wetgeving/item/1179-corona-opt-in-zet-medisch-beroepsgeheim-buitenspel.html.

23 Volg je zorg (2020) Tijdelijk inzage in uw medische gegevens bij de huisartsenpost en SEH als u geen keuze heeft doorgegeven. Geraadpleegd via https://www.volgjezorg.nl/corona-opt.

24 TNO (2020, 14 april) Consortium bouwt corona-test applicatie met privacy-by-design. Geraadpleegd via https://www.tno.nl/nl/over-tno/nieuws/2020/4/consortium-bouwt-corona-test-applicatie-met-privacy-by-design/.

25 Dutch Blockchain Coalition (2020, 14 april) Het uNLock consortium komt met een Blockchain/SSI oplossing voor privacy-vriendelijke corona-verklaringen. Geraadpleegd via https://dutchblockchaincoalition.org/nieuws/blockchain-ssi-voor-privacy-vriendelijke-corona-verklaringen; CMS Advocaten (2020, 16 april) Consortium uNLock presenteert privacyproof corona-applicatie. Geraadpleegd via https://cms.law/nl/nld/news-information/consortium-unlock-presenteert-privacyproof-corona-applicatie.

26 Blogpost is destijds verwijderd. De originele post was hier geraadpleegd: http://ww17.kivi-corona.blogpost.com/2020/11.

27 Schellevis, J. (2020, 25 november) Overheid overweegt speciale corona-app met 'test-paspoort'. Geraadpleegd via https://nos.nl/artikel/2358056-overheid-overweegt-speciale-corona-app-met-test-paspoort.html.

overeenkomsten in hoe zo'n digitaal paspoort werkt. In algemene lijnen is een gezondheidspaspoort een ID-applicatie op smartphones die de gezondheid van de gebruiker aangeeft:

1. De gebruiker moet zijn/haar gegevens in de app registeren. Toegang tot de app zou ook mogelijk kunnen zijn op grond van een vingerafdruk of gezichtsscan.
2. De gebruiker kan zo via deze app een afspraak maken voor het laten afnemen van een coronatest.
3. De arts/verpleegkundige kan via de app snel bij de gegevens van de gebruiker en vervolgens een coronatest afnemen – ook wel een 'sneltest' genoemd.
4. De resultaten worden in de applicatie geregistreerd en dan krijgt het digitale paspoort een kleur om aan te geven of hij/zij/hen besmet is (rood) of niet (groen) – Sommige apps geven ook meerdere opties qua kleur om aan te geven dat de test bijna verlopen is.
5. Het paspoort kan door andere gebruikers (vrienden, werkgevers, openbaar vervoer, horecaondernemers etc.) op afstand worden gescand.
6. Als het gezondheidspaspoort roodkleurig is, wordt de gebruiker in principe niet binnengelaten. / Als het gezondheidspaspoort groenkleurig is, wordt de gebruiker in principe wel binnengelaten,

De sneltest is een aangepaste testmethode die, anders dan de reguliere PCR-test, binnen een uur vast kan stellen of iemand besmet is. Zie hier een animatie van TNO over hun sneltest.

Wat is het doel?

Het doel van het gezondheidspaspoort is volgens meerdere ontwikkelaars om geleidelijk en gecontroleerd de lockdown-beperkingen op te heffen en terug te keren naar het "normale leven" op een veilige manier.[28] Verder richt TNO ook onderzoek naar het gebruik van een paspoort *na corona*. Het breder doel van het uNLock consortium is om het individu meer controle te geven over zijn/haar/hun medische gegevens op een digitale wijze.

Gezondheidspaspoort en *body surveillance*

De gepresenteerde doelen van het gezondheidspaspoort is het monitoren van gezondheid om zodoende terug te keren naar het normale leven en om op een verantwoorde wijze individuen meer vrijheid te kunnen geven. Daarentegen is het juist een maatregel waarmee toegang tot bepaalde plekken en deelname in het

28 TNO (2020, 14 april) Consortium bouwt corona-test applicatie met privacy-by-design. Geraadpleegd via https://www.tno.nl/nl/over-tno/nieuws/2020/4/consortium-bouwt-corona-test-applicatie-met-privacy-by-design/; Dutch Blockchain Coalition (2020, 14 april) Het uNLock consortium komt met een Blockchain/SSI oplossing voor privacy-vriendelijke corona-verklaringen. Geraadpleegd via https://dutchblockchaincoalition.org/nieuws/blockchain-ssi-voor-privacy-vriendelijke-corona-verklaringen; CMS Advocaten (2020, 16 april) Consortium uNLock presenteert privacyproof corona-applicatie. Geraadpleegd via https://cms.law/nl/nld/news-information/consortium-unlock-presenteert-privacyproof-corona-applicatie.

sociale, werkende en politieke leven wordt *beperkt*. Als zo'n paspoort geen vrijwillig karakter heeft, maakt het een zware inbreuk op de privacy en lichamelijke integriteit van burgers. Als het wordt verplicht door onder meer werkgevers, het openbaar vervoer en het onderwijs sluit het daarbij veel mensen uit. De afhankelijkheid van een groen schermpje brengt surveillance dicht op de huid.[29] Verder vereist het gebruik van het paspoort dat er regelmatig getest wordt op corona. Dit is niet voor iedereen mogelijk of gewenst. Niet iedereen heeft een smartphone, wat voor het gebruik van een paspoort is vereist.

Het paspoort verwerkt biometrische en gezondheidsgegevens. Ook al werken apps zoals uNLock met gegevensbeschermende waarborgen, het risico van verwerking is niet voldoende weggehaald. Deze gegevens worden beheerd door en gedeeld met meerdere partijen, wat effectieve gegevensbescherming ondermijnt. Vooral in geval van commerciële dataverwerking moet er kritisch worden gekeken naar de app. Er moeten voldoende waarborgen zijn zodat het gebruik van de gegevens voor andere doeleinden wordt beperkt. Als deze gegevens worden gebruikt voor andere doeleinden, zoals voor advertenties, verkoop of zelfs het berekenen van zorgpremies, heeft dat behoorlijke gevolgen voor de sociale en politieke vrijheden van individuen.

[29] Houwing, L. (2020, 25 november) Een testsamenleving mag niet uitmonden in een douane- en controlesamenleving. Geraadpleegd via https://www.bitsoffreedom.nl/2020/11/25/een-testsamenleving-mag-niet-uitmonden-in-een-douane-en-controlesamenleving/.

3.5. Tijdelijke maatregelen?

Deze maatregelen zijn ingezet als tijdelijke maatregelen. Dat wil zeggen dat zij alleen worden ingezet tijdens de coronacrisis. Maar hoe tijdelijk is dat precies? Heeft de coronacrisis echt een tijdelijk karakter? En een duidelijk eind? Het is vaak onvoldoende vastgelegd tot wanneer een maatregel van toepassing is, en in hoeverre deze mag worden verlengd. De tijdelijke aard van gegevensverwerking is een essentiële waarborg die is vastgelegd in de AVG. Door geen tijdslimiet te noemen zijn er onvoldoende waarborgen voor de betrokkenen. Het is dan bijvoorbeeld onvoldoende duidelijk of de verwerking van gegevens op enig moment kan veranderen.[30] Hier een overzicht van de "tijdelijkheid" van de gegevensverwerking van deze maatregelen:

Maatregel	Hoe lang worden gegevens verwerkt?	Hoe lang worden de gegevens bewaard?
CoronaMelder	Het wetsvoorstel vervalt na zes maanden, tenzij het parlement instemt met een verlenging (van maximaal drie maanden) **Of…** Het wetsvoorstel vervalt wanneer de app niet meer effectief is – wanneer de CoronaMelder "geen bijdrage levert aan het breder, efficiënter en sneller opsporen van mensen die met het virus geïnfecteerd zijn of als er onacceptabele niet beoogde effecten optreden."[31]	"Niet langer bewaard dan noodzakelijk…om gebruikers in voorkomende gevallen te kunnen waarschuwen over een mogelijke infectie met het virus"[32]
Wijziging Telecommunicatiewet	Artikel 14.7 vervalt "met ingang van zes maanden na het tijdstip van inwerkingtreding van deze wet" [33] **Of** Bij koninklijk besluit[34]	"Tot uiterlijk zes maanden."[35]
Corona opt-in	"Voor de duur van de COVID-19-epidemie in Nederland"[36] Hiernaast komt er eind 2021 een nieuw wetsvoorstel om gegevensuitwisseling in de acute zorg de versnellen op een gelijke wijze als met deze maatregel.[37]	Niet duidelijk vermeld. Een zorgverlener moet in beginsel uw medisch dossier 20 jaar lang bewaren.[38] Maar dit kan langer/korter zijn. Als dit beginsel niet van toepassing is, is de regel dat de gegevens niet langer dan noodzakelijk worden bewaard.
Gezondheidspaspoort	*Dit is nog niet bekend.*	*Dit is nog niet bekend.*

[30] Zie ook Austin, E. en Zenger R. (2020, 8 april) Bescherm onze gezondheid, maar bescherm ook onze rechten. Geraadpleegd via https://www.bitsoffreedom.nl/2020/04/08/bescherm-onze-gezondheid-maar-bescherm-ook-onze-rechten/.
31 Tijdelijke bepalingen in verband met de inzet van een notificatieapplicatie bij de bestrijding van de epidemie van covid-19 en waarborgen ter voorkoming van misbruik daarvan (Tijdelijke wet notificatieapplicatie covid-19) (2020, 28 september) [MvA] p. 55.
32 Tijdelijke wet notificatieapplicatie covid-19, Artikel 6d lid 3 sub a.
33 Tijdelijke wet informatieverstrekking RIVM i.v.m. COVID-19, Artikel II lid 2.
34 Tijdelijke wet informatieverstrekking RIVM i.v.m. COVID-19, Artikel II lid 2.
35 Tijdelijke wet informatieverstrekking RIVM i.v.m. COVID-19 [Tweede nota van wijziging] p. 3.
36 Volg je zorg (2020) Tijdelijk inzage in uw medische gegevens bij de huisartsenpost en SEH als u geen keuze heeft doorgegeven. Geraadpleegd via https://www.volgjezorg.nl/corona-opt.
37 Richtlijn 'Gegevensuitwisseling tussen huisarts, huisartsenpost, ambulancedienst en spoedeisende hulp' (2014, 23 mei).
38 Wet op de geneeskundige behandelingsovereenkomst.

Van tijdelijk naar vast

Wat op dit moment een tijdelijke maatregel is zou zich kunnen ontwikkelen tot een vaste maatregel.

Ten eerste veroorzaakt de onzekerheid over de duur van deze pandemie onzekerheid over de duur van deze maatregelen. Zo is een maatregel van toepassing voor de duur van een crisis waarvan het einde niet in zicht is.

Ten tweede is een breder doel het versoepelen van gegevensuitwisseling in de zorg. Dit doel plaatst vraagtekens bij de duur van deze mate van gegevensverwerking. In de zorg wordt bijvoorbeeld gewerkt aan een wetswijziging die de gegevensuitwisseling van patiënten zou versoepelen.[39] Zo wordt het concept van de Corona opt-in omgezet naar een vaste maatregel.

Ten derde is er onvoldoende vastgelegd in de maatregelen en de toelichtingen hiervan over de tijdelijkheid. De Corona-opt-in en gezondheidspaspoorten hebben bijvoorbeeld geen juridische basis. Zonder een juridische basis is er gebrek aan een duidelijke omvang van de maatregel wat veel onzekerheid over de tijdelijkheid van de maatregel veroorzaakt.

Onduidelijke doelbinding

De doelstelling van een maatregel is heel belangrijk. Gegevens mogen namelijk alleen worden verwerkt als er sprake is van een *gerechtvaardigd doel* en als de verwerking overeenkomt met dit doel. De wetgeving die een nieuwe maatregel aankondigt moet duidelijk kunnen aangeven waarom gegevensverwerking nodig is om dit doel te bereiken. Het beleid moet ook vast kunnen stellen dat de methodes die worden genoemd ook echt nodig zijn om het doel te bereiken. Voor de landelijke uitvoering van deze maatregelen is het belangrijk "dat deze technologie[ën] zich wel voor dit doel laat misbruiken."[40] Als het niet duidelijk staat vermeld dan is het moeilijk de doelbinding van een maatregel te monitoren. De maatregelen die hier worden besproken geven niet altijd even overzichtelijk de doelen van verwerking aan.

De toelichting van de wijziging van de Telecommunicatiewet noemt een lange lijst met verschillende doelen. Het doel is onvoldoende duidelijk waardoor het ook onduidelijk is *hoe* de gegevens en *welke* gegevens worden verwerkt.[41] Verder staat de Europese wetgeving verwerking van locatie- en verkeersgegevens maar in zeer beperkte gevallen toe. [42] Toegang tot

39 Van Ark, T. (2020, 2 oktober) Elektronische gegevensuitwisseling in de zorg [Kamerbrief] p. 7.

40 Zenger, R. (2020, 20 mei) Kun je Bluetooth wel misbruiken voor een corona-app? Geraadpleegd via https://www.bitsoffreedom.nl/2020/05/20/kun-je-bluetooth-wel-misbruiken-voor-een-corona-app/.

41 Benaissa, N. (2020, 15 oktober) Massasurveillance zonder duidelijk doel. Geraadpleegd via https://www.bitsoffreedom.nl/2020/10/15/de-vraag-blijft-waarom-moet-deze-wet-er-komen/.

42 HvJEU 21 december 2016, C-203/15 en C-698/15, ECLI:EU:C:2016:970 (Tele2 Sverige), punten 105 en 89 verwijzend naar analogie van HvJEU 22 november 2012, C-119/52, ECLI:EU:C:2012:748 (Probst), punt 23.

locatiegegevens kan alleen met een heldere omschrijving en doelstelling.

Ook is er een gebrek aan doelstelling wat betreft de gezondheidspaspoorten. Er worden meerdere versies ontwikkeld door verschillende partijen wat veel onduidelijkheid veroorzaakt. Zo is de doelstelling van de ene partij anders dan van de andere partij. Verder wordt er vooral veel onderzoek gedaan naar wat *technisch* mogelijk is en niet naar hoe deze technologie moet worden gebruikt. De ontwikkeling van technologie die gevoelige informatie over burgers wil verwerken *zonder* een doelstelling is zorgelijk.

Doelbinding is een belangrijke waarborg voor gegevensbescherming die in veel van deze maatregelen nog niet voldoende aandacht krijgt.

4. Welke gegevens worden verzameld?

Welke gegevens worden er met de corona-maatregelen in dit onderzoek verzameld, en waarom zijn deze gegevens belangrijk in het kader van *body surveillance?* Er is veel onbegrip over de mate van gegevensverwerking, de datastromen en de aard en het belang van de gegevens die hierbij een rol spelen. Dit hoofdstuk kijkt naar welke gegevens er worden verzameld.

4.1. Gegevensverwerking en *body data*

Body data verwijzen naar de informatie met betrekking tot het lichaam die over individuen en groepen worden verzameld. De technologische ontwikkelingen lijken het *digitaliseren van het lichaam* mogelijk te maken door steeds meer informatie te vergaren over de gezondheid en het gedrag van individuen. Vooral als indicatie van status en machtsverhoudingen, is het interessant en nuttig om deze informatie te vergaren. *Body data* omvatten dus niet alleen biologische gegevens maar ook de gegevens die inzicht geven in het sociale en politieke gedrag van een individu. *Body data* kan *bijzonder* zijn, zoals geïdentificeerd in de wet, maar kan ook *gevoelig* zijn, waar geen juridische bepaling voor is.

Bijzondere gegevens

De Algemene verordening gegevensbescherming identificeert een categorie van 'bijzondere' persoonsgegevens.[43] De bijzondere gegevens betreffen gegevens waaruit onder andere de "*verwerking van genetische gegevens, biometrische gegevens*[44] *met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid*."[45][46]

In principe is de verwerking van bijzondere gegevens verboden omdat deze gegevens zeer gevoelige informatie betreffen, waarbij verwerking en openbaarmaking schadelijke gevolgen kunnen hebben op onder meer de integriteit van de betrokkenen. Er is wel een uitzondering op het verbod, namelijk wanneer er aan de in artikel 9 lid 2 AVG genoemde voorwaarden is voldaan.[47]

Gevoelige gegevens

43 Algemene verordening gegevensbescherming, Artikel 9 lid 1.
44 Biometrische gegevens worden in Algemene verordening gegevensbescherming Artikel 4 lid 14 gedefinieerd als "persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukken."
45 Gegevens over de gezondheid worden in Algemene verordening gegevensbescherming Artikel 4 lid 15 gedefinieerd als de "persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven."
46 Algemene verordening gegevensbescherming, Artikel 9 lid 1.
47 Algemene verordening gegevensbescherming, Artikel 9 lid 2.

Niet alle gegevens die in de corona-maatregelen worden verwerkt zijn volgens de AVG te categoriseren als bijzondere gegevens. Naast de meer biologische interpretatie *van body data* is er ook sprake van *body data* die informatie geven over het sociale en politieke gedrag van een betrokkene. Deze gegevens zijn niet per se fysiek, fysiologisch of biometrisch. Hier gaat het meer om gedragsgerelateerde kenmerken en meer om het idee van het lichaam zoals omschreven binnen het kader van *body politics*. Verder kan hier vooral gedacht worden aan gegevens die invloed hebben op het ontwikkelen van de individuele autonomie.

Gegevens van gevoelige aard worden door toezichthouders gehanteerd als een categorie van gegevens waarvoor extra waarborgen noodzakelijk zijn. Denk bijvoorbeeld aan locatiegegevens. Locatiegegevens kunnen iets vertellen over iemands gezondheid, zonder dat hij dat expliciet heeft gedeeld, door bijvoorbeeld te laten zien dat hij een x aantal keer naar het ziekenhuis is geweest. Het kan iets vertellen over iemands religie, door bijvoorbeeld te laten zien dat hij een x aantal keer naar een religieuze instelling is geweest. Met deze voorbeelden wordt duidelijk zichtbaar dat locatiegegevens alsnog bijzondere gegevens kunnen openbaren, waardoor ze het verwerkingsverbod van de AVG tot op zekere hoogte schenden.

4.2. CoronaMelder

In Artikel 6d lid 2 van de *Tijdelijke wet notificatieapplicatie Covid-19* (3 september 2020) staan de gegevens die worden verwerkt vermeld. Deze gegevens, ook al worden ze net anders genoemd, staan ook vermeld in de privacyverklaring van de CoronaMelder. Naast de gegevensverwerking die in de wet staat, is er ook onderzoek verricht naar verwerking die niet (expliciet) in de wet staat. Het volgende overzicht illustreert welke gegevens er worden verzameld:

Er is in dit overzicht een selectie gemaakt van de gegevens die betrekking hebben op *body surveillance*, oftewel het surveilleren van het lichaam. Er worden echter meer gegevens verwerkt, maar die zijn binnen dit kader niet van belang.

Wat zeggen deze gegevens over jou?

De CoronaMelder verwerkt gevoelige gegevens over jouw gezondheid en sociale netwerk, maar wat zeggen deze gegevens precies?

1. Contactduur en nabijheid?

Via Bluetooth Low Energy wordt volgens CoronaMelder de contactduur en nabijheid van gebruikers gemeten.

Dit wordt op grond van de signaalsterkte gemeten. De signaalsterkte van telefoons is niet betrouwbaar. Het signaal kan worden beïnvloed door het type toestel, andere objecten die in de weg staan en andere mensen in de omgeving. Dit leidt tot een toename van vals-positieven.[48] Google en Apple zijn hun API aan het ontwikkelen om deze signaalsterkte nauwkeuriger te identificeren en verwerken.[49]

2. Risico van besmetting?

Het risico van besmetting wordt uitgerekend op grond van de contactduur, de nabijheid en de eerste ziektedag. Is deze inschatting betrouwbaar of buitensporig? Door de grote aantallen vals-positieven krijgen veel mensen een melding zonder dat dat echt nodig zou zijn. Dit heeft grote gevolgen op de vrijheden van burgers. Door deze melding voelen veel burgers zich genoodzaakt om (onnodig) thuis te blijven, waardoor ze bijvoorbeeld niet naar hun werk, school, familie en vrienden kunnen gaan.

3. Pseudoniem ≠ surveillance?

Volgens David Lyon is herleidbaarheid van *body data* niet bepalend voor de vraag of er sprake is van *body surveillance*. Zelfs zonder herleidbaarheid, heeft de verwerking van deze gegevens namelijk een impact op de samenleving en individuele rechten. Het feit dat het gaat om pseudonieme gegevens betekent dus niet dat er geen sprake is van surveillance.

4.3. Wijziging Telecommunicatiewet

In de wijziging worden locatie- en verkeersgegevens gebruikt om mobiliteit en drukte te monitoren. Het gaat voornamelijk om twee soort gegevens, namelijk de tellingen van actieve verbindingen en de afgeleide herkomst van gebruikers.

Wat zeggen deze gegevens over jou?

Locatie- en verkeersgegevens zijn van *gevoelige aard*. Ze geven inzicht in de locatie en verplaatsingen van "abonnees en eindgebruikers van aanbieders van openbare telecommunicatienetwerken en diensten."[50] Wat zeggen deze gegevens nog meer?

1. Jouw gedrag

Ze geven inzicht in wanneer, met wie en hoe lang je ergens bent. Door deze gegevens te verwerken wordt een duidelijk beeld geschetst over jouw gedrag Op basis van deze informatie kunnen er conclusies worden

48 Tijdelijke wet notificatieapplicatie covid-19 Nr.2 [MvT].
49 De Jonge, H.M. (2020, 18 november) Stand van zakenbrief COVID-19 [Kamerbrief].
50 Gegevensbeschermingseffectbeoordeling (DPIA) COVID-19 notificatie-app, p. 6.

getrokken over bijvoorbeeld jouw routine, gezondheid en religie.

2. Elke actieve verbinding

Volgens de Tweede Nota van Wijziging worden de tellingen afgeleid uit door de telecomproviders bewaarde verkeersgegevens van *actieve verbindingen*. Dat wil zeggen, de verbinding die je maakt wanneer je belt, sms't of een dataverbinding maakt met het mobiele netwerk. Je maakt geen actieve verbinding als je verbinding maakt met WiFi. Ook al is dit zeker een verbetering ten opzichte van het eerste voorstel, het is alsnog vrij makkelijk om een actieve verbinding te maken. De meeste telefoongebruikers hebben meestal hun data aanstaan waardoor het realistisch gezien niet het aantal telefoons in de gegevensverwerking beperkt.

3. Locatie op een bepaald moment

Het voorstel verwerkt gegevens over waar jij op een bepaald moment bent. Het antennegebied waar jouw apparaat verbinding mee maakt geeft een indicatie van de gemeentegrenzen. Meerdere actieve verbindingen en dus locaties worden aan elkaar gekoppeld om een inschatting te krijgen van hoe mensen zich verplaatsen.

4. Afgeleide herkomst

De afgeleide herkomst wordt berekend op grond waar jij de laatste 30 dagen het vaakst een actieve verbinding hebt gemaakt.

5. Groepsherkenning

Als het aantal telefoons met dezelfde afgeleide herkomst kleiner is dan 15 worden de gegevens niet uitgewisseld. Dit beperkt in zekere mate de individuele herleidbaarheid, maar er is nog steeds een risico tot groepsherkenning.[51] Zo kunnen groepen in bijvoorbeeld sport of in religieuze instellingen worden geïdentificeerd.

Een voorbeeldje: Stel er is een demonstratie in Utrecht vaar vooral veel actiegroepen uit Den Helder naartoe komen. Uit de data van deze maatregel zie je dat er meer mensen uit Den Helder in Utrecht zijn geweest dan normaal. Deze informatie kan je combineren met de social media-pagina's van de actiegroep of het evenement. Vervolgens kan je vrij nauwkeurig personen identificeren die aanwezig waren bij de demonstratie.

Groepsherkenning gecombineerd met de afgeleide herkomst kan ervoor zorgen dat bepaalde groepen en individuen andere maatregelen of instructies ervaren. De data op zichzelf is misschien niet zo gevoelig of herleidbaar, maar als deze data wordt gecombineerd is het een ander geval. Dit is zorgelijk omdat dit een discriminerend effect kan hebben en een inbreuk kan maken op andere rechten zoals het recht op de vrijheid van vereniging.

Niet voldoende anoniem

Een belangrijk punt en grote zorg is dat het moeilijk is telecommunicatiegegevens volledig te

51 Keijzer, M.C.G. (2020, 2 oktober) Tijdelijke wet informatieverstrekking RIVM ivm COVID-19 (35 479) [Kamerbrief] p. 5.

anonimiseren. Zoals genoteerd door de AP, de “kans op herleidbaarheid van de gegevens tot (groepen van) individuele personen is aanwezig” waardoor deze gegevens “niet als anonieme gegevens kunnen worden beschouwd.”[52] Uit onderzoek van … over mobiliteitsdata blijkt dat er maar *vier* data punten (of verbindingen) nodig zijn om een individu met 95% nauwkeurigheid te identificeren.[53] Telecommunicatiegegevens geven veel inzicht in de persoonlijke levenssfeer van individuen, waardoor de verwerking hiervan extra aandacht benodigd.

4.4. Corona opt-in

Met de Corona opt-in worden de “belangrijkste”[54] huisartsgegevens toegankelijk gemaakt. Een medisch dossier bevat uitgebreide informatie over de gezondheid van een cliënt, zoals welke medicijnen hen/zij/hij gebruikt, informatie over hun/haar/zijn leefstijl en uitslagen van onderzoeken. Een overzicht van welke gegevens onderdeel zijn van de belangrijkste gegevens, ook wel de professionele samenvatting genoemd,[55] is hier te zien:

Wat zeggen deze gegevens over jou?

Zoals hierboven te zien gaat het hier om een grote hoeveelheid gegevens. Er zijn vier aspecten die vooral belangrijk zijn op grond van *body surveillance*:

1. Jouw fysieke en mentale staat

Deze maatregel verwerkt medische gegevens die als bijzondere gegevens worden beschouwd. De informatie die wordt verwerkt in onder meer jouw episodelijst en in de verslagen van jouw arts geven in jouw fysieke en mentale staat. Een episodelijst is een lijst van (hoofd)diagnosen die bij de patiënt genoteerd staan. Of jij bijvoorbeeld depressief bent geweest of een keer je arm hebt gebroken, ook al is dit jaren geleden en is het niet relevant, is te zien in deze samenvatting.

2. De laatste vier maanden of de laatste vijf consulten

De professionele samenvatting omvat de gegevens van de *laatste vier*

52 Autoriteit Persoonsgegevens (2020, 19 mei) AP beoordeelt tijdelijke wet telecomdata op waarborgen privacy. Geraadpleegd via https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-beoordeelt-tijdelijke-wet-telecomdata-op-waarborgen-privacy.

53 De Montjoye, YA., Hidalgo, C., Verleysen, M. et al. (2013) Unique in the Crowd: The privacy bounds of human mobility. Science Report 3, p. 1376.

54 Nieuwsbericht rijksoverheid (2020, 8 april) Belangrijkste huisartsinformatie tijdelijk te raadplegen. Geraadpleegd via https://www.rijksoverheid.nl/actueel/nieuws/2020/04/08/belangrijkste-huisartsinformatie-tijdelijk-te-raadplegen.

55 Nederlands Huisartsen Genootschap, Richtlijn Gegevensuitwisseling huisarts en Centrale Huisartsenpost (CHP). Geraadpleegd via https://www.nhg.org/sites/default/files/content/nhg_org/uploads/richtlijn_waarneming-v3-24jul081_0.pdf.

maanden of de *laatste vijf consulten*. Vooral in het geval van het laatste, en als jij niet vaak naar de (huis)arts gaat, is er toegang tot medische gegevens van een aanzienlijke tijdsperiode.

3. Medicatiegebruik

De samenvatting bevat een overzicht van alle medicatie die jij *de laatste vier maanden* heb besteld, ook al is dit overzicht niet per se relevant voor corona-gerelateerde vragen.

4. Sociale gegevens

Ook bevat de professionele samenvatting sociale gegevens. Dit zijn gegevens over bijvoorbeeld jouw wilsbeschikking, (geloofs)overtuiging, woon- en gezinssituatie, maar ook je huwelijkse staat. Deze gegevens bevatten zeer gevoelige details over jouw persoonlijke, en niet-medische, levenssfeer.

4.5. Gezondheidspaspoort

Het gebruik van een gezondheidspaspoort en/of sneltest vereist de verwerking van bijzondere en gevoelige gegevens. Het verwerken van gegevens over een coronatest is een logisch onderdeel van zo'n maatregel. Er is nog onvoldoende informatie over de welke gegevens er in een Nederlands gezondheidspaspoort zouden worden verwerkt. Wel wordt er al veel gediscussieerd over het mogelijke gebruik van zo'n paspoort. Het kan worden gebruikt als een digitaal medisch dossier of een vaccinboekje. Ook kan het worden gebruikt als toegangsbewijs voor bijvoorbeeld festivals, waar een paspoort een overzicht kan gegeven van jouw aankoopbewijs, gezondheid en legitimatie. Er wordt nog veel onderzoek gedaan naar welke gegevens er kunnen worden gebruikt. De discussie dat hier veel mogelijkheden voor zijn is zorgelijk. Het is niet wenselijk dat een gezondheidspaspoort zodanig wordt ingeschakeld of in onnodige gevallen wordt gebruikt. Hieronder staan wat voorbeelden vermeld die worden genoemd in de discussie rondom de ontwikkelingen.[56]

Wat zeggen deze gegevens over jou?

Gezien er nog geen gezondheidspaspoort is in Nederland, is het moeilijk om conclusies te trekken over wat deze gegevens over jou zeggen.

4.6. Transparantie en duidelijkheid

Er is onvoldoende transparantie en duidelijkheid over de

56 Schellevis, J. (2020, 25 november) Overheid overweegt speciale corona-app met 'test-paspoort'. Geraadpleegd via https://nos.nl/artikel/2358056-overheid-overweegt-speciale-corona-app-met-test-paspoort.html; TNO (2020, 14 april) Consortium bouwt corona-test applicatie met privacy-by-design. Geraadpleegd via https://www.tno.nl/nl/over-tno/nieuws/2020/4/consortium-bouwt-corona-test-applicatie-met-privacy-by-design/.

gegevensverwerking van de corona-maatregelen. Dit is te zien in 1) wetgeving en beleid, 2) met betrekking tot de rechten van betrokkenen en patiënten.

Wetgeving en beleid: wat wordt er nou echt verzameld?

Het is in de wetgeving en het beleid vaak onvoldoende duidelijk om welke gegevens het gaat. Ten eerste worden veel technische termen gebruikt waardoor de gegevensverwerking niet toegankelijk is. Vragen die belangrijk zijn voor burgers worden hierdoor onvoldoende beantwoord. Hoe worden de gegevens verwerkt? Wanneer is deze maatregel van toepassing? Waarom is deze maatregel belangrijk? Hoe wordt een risico bepaald? Een begrijpelijk overzicht van de gegevensverwerking is essentieel om de betrokken personen te informeren over het gebruik van hun data en de impact hiervan.

De onduidelijkheid van de gegevensverwerking is niet alleen een probleem voor betrokkenen maar ook voor beleidsmakers, wetgevers en politici. Zo worden er in de Tweede Kamer kamervragen gesteld, moties ingediend en discussies gevoerd over beleid, terwijl er niet altijd genoeg informatie is voor politici om geïnformeerde keuzes te maken. Zo werd een rapport van Radically Open Security 28 september gepubliceerd met een belangrijke risicoanalyse van de CoronaMelder terwijl er al was gestemd over de CoronaMelder in de Tweede Kamer.

Verder worden deze maatregelen vaak *per maatregel* behandeld en niet in zijn geheel. Door deze maatregelen niet in context/onderling verband te behandelen wordt er geen rekening gehouden met het totale plaatje.

Rechten van betrokkenen en patiënten

Naast dat betrokkenen vaak onvoldoende zijn geïnformeerd over de uitrol en inhoud van deze maatregelen, zijn zij ook vaak onvoldoende geïnformeerd over hun rechten. De Europese en Nederlandse wetgeving op gegevensbescherming is in 2018 gewijzigd met belangrijke gevolgen voor betrokkenen Zo heeft de AVG meerdere rechten vastgesteld die de autonomie en zeggenschap van betrokkenen versterkt.[57] Helaas zijn burgers hier onvoldoende van op de hoogte. Uit een onderzoek uit 2018 bleek dat van de Nederlanders die zeiden dat ze op de hoogte waren van de AVG maar 20% echt wist welke nieuwe rechten ze hadden gekregen. [58] Met ontoereikende belangstelling en begrip voor het privacyrecht, beschikken burgers niet altijd over hoe zij hun rechten kunnen uitoefenen. Door dit gebrek aan kennis over de rechten van betrokkenen ontstaat er een ongelijke machtsverhouding tussen diegene die gegevens verwerkt en diegene wiens gegevens worden verwerkt.

57 Algemene verordening gegevensbescherming, Hoofdstuk 3.
58 KPMG (2018, 9 november) Een beetje privacy graag: Hoe Nederlanders omgaan met hun privacy, vier maanden na de invoering van de AVG.

5. Waar komen de gegevens terecht en wie kan erbij?

Nu weten we om welke gegevens het gaat, maar wie kan hier allemaal bij? In dit hoofdstuk kijken we naar waar de gegevens terechtkomen. Wat mag volgens de wetgeving en het beleid en hoe werkt dit in de praktijk?

5.1. Basisprincipes: doelbinding en verantwoordelijkheid

De Europese wetgeving regelt een aantal vereisten voor toegang tot en bewaring van gegevens. Zo mogen gegevens niet langer dan noodzakelijk voor de doeleinden worden bewaard.[59] Verder moeten er voldoende garanties zijn tegen het risico van misbruik, onrechtmatige raadpleging, en onrechtmatig gebruik van gegevens.[60]

Daarnaast zijn er regels voor degenen die toegang krijgen tot jouw gegevens. Als een persoon of organisatie invloed heeft op hoe, waarom en wanneer jouw gegevens worden verwerkt, moet diegene verantwoordelijk met deze data omgaan.[61] Het is belangrijk om te kijken naar de betrouwbaarheid van deze (rechts)personen en/of organisaties en of het gewenst is dat deze partijen inzicht hebben in gevoelige informatie over jou.

5.2. CoronaMelder

De CoronaMelder verwerkt gevoelige gegevens over jouw gezondheid en interacties. De verwerking begint lokaal op jouw smartphone, maar waar komen deze gegevens uiteindelijk terecht?

De CoronaMelder heeft meerdere fases van gegevensverwerking waar steeds verschillende actoren toegang hebben tot de gegevens. Per fase leg ik kort uit wie bij welke gegevens kan komen.

1. Installatiefase: Apple en Google

Via de appwinkel van Apple of Google, installeer jij de CoronaMelder op je smartphone. Denk aan je naam, e-mailadres, factuuradres, telefoonnummer en betaalgegevens. Deze gegevens worden *niet* tijdens gebruik van de CoronaMelder gebruikt.[62]

2. Uitwisselingsfase: Andere gebruikers

Tijdens de uitwisselingsfase worden de signaalsterkte en de duur van de uitwisseling via Bluetooth Low Energy opgeslagen door andere gebruikers in jouw omgeving. Deze gegevens worden lokaal op het toestel van de andere gebruikers waar jij mee in contact komt 14

59 Algemene verordening gegevensbescherming, Artikel 5 lid 1 sub e.
60 HVJEU 8 april 2014, C-293/12 en C-594/12, ECLI:EU:C:2014:238 (Digital Rights Ireland) r.o. 54.
61 Zie bijvoorbeeld Algemene verordening gegevensbescherming, Artikel 24.

dagen bewaard. De gebruiker ziet niet dat jij deze gegevens hebt gedeeld want het gaat om gepseudonimiseerde gegevens.

3. Validatiefase: Backend server en de GGD

Tijdens de validatiefase worden er *bijzondere* gegevens verwerkt, waar een strenger regime van bescherming voor geldt. Deze gegevens betreffen namelijk informatie over jouw coronatest, oftewel gevoelige informatie over jouw gezondheid. De backend server wordt beheerd door een uitvoeringsorganisatie van het Ministerie van Volksgezondheid, Welzijn en Sport, de CIBG, en de KPN.

De gegevens over jouw coronatest worden geverifieerd bij de GGD. Hier komen de gegevens, waaronder de datum van de eerste ziektedag terecht in het GGD-portaal, toegankelijk voor bevoegde GGD-medewerkers.

4. Koppelingsfase: Backend server en andere gebruikers

Tijdens de koppelingsfase worden er weer *bijzondere* persoonsgegevens verwerkt, namelijk informatie over de contactduur met andere gebruikers en het risico van besmetting. Jouw apparaat haalt elke dag nieuwe sleutels op van geïnfecteerde gebruikers via een server, beheerd door CIBG en KPN. Als deze codes matchen met de codes in het geheugen van jouw apparaat, krijg jij een melding dat jij in contact bent gekomen met een besmet persoon. CIBG en KPN zien niet van wie deze sleutels zijn en dus niet wie geïnfecteerd is met het virus.

5. Notificatiefase: Gebruikers

Tijdens de notificatiefase krijgen gebruikers een notificatie als zij in contact zijn gekomen met een besmette gebruiker.

Niet voldoende anoniem: onbevoegde toegang tot jouw gegevens

Volgens privacyontwerper en technologiecriticus Tijmen Schep is de CoronaMelder niet voldoende anoniem. Het is namelijk mogelijk om te achterhalen wie die andere gebruikers zijn die bij jou in de buurt zijn geweest. Dit kan voornamelijk op twee manieren: 1) Als je al met weinig mensen in contact komt is het makkelijk om de andere gebruikers te identificeren. Als jij maar met een aantal personen hebt afgesproken en je later een melding krijgt dat je op een bepaalde dag in contact ben gekomen met een besmet persoon, is dit vrij makkelijk te achterhalen. 2) Het is mogelijk om software te ontwikkelen om de anonieme gebruikers te ontmaskeren. Zo ontwikkelde Schep een website genaamd Corona Detective, waar het mogelijk is om op afstand CoronaMelder gebruikers te identificeren. Sterker nog, het wordt geadverteerd als een manier om uit te zoeken wie jou heeft besmet met het coronavirus – “Find out exactly who gave you COVID-19”. Hier hoef je zelf niet de app voor te hebben gedownload om te kunnen monitoren en volgen wie de app wel gebruikt. Lees hier meer over de werking van de Corona Detective.

5.3. Wijziging Telecommunicatiewet

De wijziging van de Telecommunicatiewet gaat over jouw locatie- en verkeersgegevens. Met betrekking tot toegang tot deze gevoelige gegevens, gaat het vooral om vier partijen: de telecomproviders, het Centraal Bureau voor de Statistiek (CBS), het RIVM en de GGD.

Hoe jouw locatie- en verkeersdata bij deze partijen terechtkomen is als volgt:

1. Jouw **telecomprovider** verwerkt jouw locatie- en verkeersgegevens
2. Jouw **telecomprovider** maakt een overzicht van de totaalaantallen per Nederlandse gemeente en per uur van de mobiele eindapparaten die in dat uur in die gemeente een actieve verbinding maakte. Deze tellingen worden nadat ze zijn geanonimiseerd en geaggregeerd,[63] dagelijks doorgestuurd naar het **CBS.** Als gegevens geanonimiseerd zijn wordt de mogelijkheid tot identificatie van individuen niet uitgesloten. Deze uitsluitbaarheid is de intentie, maar is technisch niet mogelijk om te garanderen. Zijn er minder dan 15 eindapparaten geïdentificeerd? Dan worden de tellingen afgerond naar 0 en worden de gegevens dus niet doorgestuurd.
3. Het **CBS** combineert de door de aanbieders los van elkaar verstrekte informatie. Deze gegevens worden aangepast om meer representatief te zijn van de bevolking want niet iedereen heeft een telefoon of maakt regelmatig een actieve verbinding. Dit wil zeggen, telefoons worden omgezet naar mensen.
4. Het **CBS** maakt een matrix van deze tellingen per uur afgerond op vijftigtallen en stuurt die dagelijks naar het **RIVM.**
5. Het **RIVM** kan conclusies trekken uit deze informatie en dan uit zichzelf of op aanvraag deze informatie delen. Zo kan het RIVM bijvoorbeeld **GGDs** signaleren of waarschuwen op basis van de mobiliteitscijfers.

De *body data* worden tijdens de verschillende fases van verwerking aangepast. Zo zijn de herleidbare gegevens die door de telecomproviders worden verwerkt anders dan de gegevens die bij het RIVM, het CBS en de GGD terechtkomen.

Telecomproviders zeggen 'nee'

Telecomproviders zijn niet positief over het wetsvoorstel. Zij worden gevraagd om gevoelige informatie over hun klanten af te staan. Dit kost geld en tijd en hierdoor worden de telecomproviders gevraagd verantwoordelijkheid te nemen voor een belangrijk deel van de verwerking. Telecomproviders zijn niet overtuigd van de waarborgen in het voorstel en stellen dat de

63 Geaggregeerde gegevens zijn een verzameling van gegevens die wordt uitgedrukt in een beknopte vorm, vaak voor statistische doeleinden. Zie Autoriteit Persoonsgegevens (2020, April) Over de anonimiteit van geaggregeerde telecomlocatiedata. Geraadpleegd via https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/anonimiteit_en_geaggregeerde_telecomdata.pdf.

privacy van hun klanten van het grootste belang is en dat dit voorstel te veel risico's met zich meeneemt.[64] Verder vragen zij zich af of de inzet van telecommunicatiegegevens voldoende bijdraagt aan de bestrijding van het coronavirus.[65]

Wie kan er nog meer bij?

Volgens het wetsvoorstel en de Memorie van Toelichting gaat het om de telecomproviders, het RIVM, het CBS en de GGD. Maar bieden deze partijen voldoende waarborgen tegen datalekken en andere onrechtmatige toegang? Het CBS heeft bijvoorbeeld meerdere keren een datalek gehad waar onbevoegde derden toegang kregen tot de data in het systeem van het CBS.[66]

5.4. Corona opt-in

De huisartsenposten (HAP) en spoedeisende hulp (SEH) krijgen met deze opt-in makkelijker toegang tot jouw medische gegevens. Deze gegevens kunnen zij via het Landelijk Schakelpunt (LSP) opvragen. Artsen die een behandelmoment met jou als patiënt hebben gehad vallen hieronder. Dit kan zowel jouw huisarts zijn als een arts elders. Als er toestemming is verleend in het huisartssysteem is er geen beperking tot het aantal opvragers. Deze toestemming is vaak al vanzelfsprekend, gezien de corona-opt-in deze toestemming heeft vastgelegd tenzij er bezwaar is gemaakt. Het blijkt ook dat het technisch niet mogelijk is om de toegang alleen te beperken naar specifieke artsen, zoals op de huisartsenpost (HAP) of de spoedeisende hulp (SEH).[67]

5.5. Gezondheidspaspoort

Wat betreft het gezondheidspaspoort is er nog onvoldoende informatie over wie er toegang heeft tot de gegevens. Er is namelijk nog geen concreet voorstel. Tijdens de ontwikkeling van een zodanig paspoort wordt hopelijk voldoende aandacht besteed aan wie betrokken is bij de verwerking en of deze partijen voldoende bescherming bieden.

5.6. Onafhankelijkheid en meerdere toegangspoortjes

Veel verschillende instanties en actoren zijn betrokken bij de gegevensverwerking van de corona-maatregelen. Ze werken samen in de ontwikkeling, uitvoering en analyse van de maatregelen. Soms veroorzaakt dit onduidelijkheid en onzekerheden over wie waar toegang tot heeft.

64 Hoekstra, M. (2020, 12 oktober) Position paper T-Mobile Nederland i.v.m. rondetafel over het wetsvoorstel voor "Tijdelijke Wet Informatieverstrekking RIVM i.v.m. COVID-19".
65 Hoekstra, M. (2020, 12 oktober) Position paper T-Mobile Nederland i.v.m. rondetafel over het wetsvoorstel voor "Tijdelijke Wet Informatieverstrekking RIVM i.v.m. COVID-19"; Houwing, L (2020, 7 oktober) Schriftelijke inbreng Bits of Freedom Tijdelijke wet informatieverstrekking RIVM i.v.m. COVID-19.
66 Jongejan, W. J. (2020, 26 oktober) Voorganger AP permitteerde door overheid georganiseerd datalek bij CBS. Geraadpleegd via https://www.zorgictzorgen.nl/voorganger-ap-permitteerde-door-overheid-georganiseerd-datalek-bij-cbs/.
67 Jongejan, W. J. (2020 8 april) VWS en Autoriteit Persoonsgegevens vertellen maar halve verhaal over corona-opt-in. Geraadpleegd via https://www.zorgictzorgen.nl/vws-en-autoriteit-persoonsgegevens-vertellen-maar-halve-verhaal-over-corona-opt-in/.

Deze onzekerheid is deels het gevolg van onvoldoende transparantie.

Ook moet er kritisch gekeken worden naar de afhankelijkheid van buitenlandse of Big Tech bedrijven. De CoronaMelder wordt bijvoorbeeld deels ontwikkeld door Apple en Google, twee Amerikaanse tech-giganten. Apple en Google geven geen volledig inzicht in het onderliggende systeem voor de app die zij hebben ontwikkeld waardoor controle op veiligheid niet kan worden gewaarborgd. Ook al krijgen deze bedrijven geen toegang tot de persoonsgegevens die in de CoronaMelder worden verwerkt, er blijft onvoldoende duidelijkheid over wat zij wel en niet kunnen.[68] Zo hebben Apple en Google jouw gegevens nodig om de app te kunnen installeren. Denk aan je naam, e-mailadres, telefoonnummer, betaalgegevens en andere downloads. Apple en Google monitoren bijvoorbeeld wat voor andere apps je hebt gedownload en hoe je deze gebruikt om daardoor andere vergelijkbare producten te adverteren. Per definitie deelt de gebruiker mede hierdoor zijn/haar/hun (meta)data met dezen partijen. Ook al hebben Apple en Google geen toegang tot de gegevens in de CoronaMelder, dan alsnog is de afhankelijkheid aan Apple en Google voor de CoronaMelder zorgelijk. Ten eerste is de CoronaMelder alléén toegankelijk voor gebruikers die een smartphone hebben met de Apple Store of de Google Playstore. Hierdoor worden gebruikers uitgesloten die geen toegang hebben tot deze applicatiewinkels of geen diensten willen gebruiken van Google of Apple. Ten tweede is het ongewenst dat de overheid voor applicaties voor publieke belangen als de volksgezondheid afhankelijk is van Amerikaanse Big Tech-bedrijven.

68 Nota naar aanleiding van het verslag inzake Tijdelijke wet notificatieapplicatie covid-19. Geraadpleegd via https://www.rijksoverheid.nl/documenten/kamerstukken/2020/08/28/nota-naar-aanleiding-van-het-verslag, p.1.

6. Een overzicht van gegevensverwerking

7. De aandachtspunten: normalisering en noodzakelijkheid

7.1. Normalisering van het verwerken van body data

mHealth steeds populairder

De afgelopen jaren is het verwerken van *body data* steeds normaler geworden. Zo gebruiken we steeds vaker mobiele applicaties en smart tools zoals FitBit die onze gezondheid, slaap en productiviteit monitoren. Dit wordt ook wel *mobile health* of *mHealth* genoemd. Het is een gewoonte geworden om steeds meer data te delen in ruil voor tips om beter en gezonder te leven. Als gevolg gaan veel mensen steeds onachtzamer om met hun gevoelige gegevens. Hoe lang je hebt geslapen, waar je hebt gefietst, hoe jouw menstruatiecyclus eruitziet, wat je eet en hoe jij je voelt wordt snel gedeeld in ruil voor tips en tricks om jezelf te verbeteren. Het is zeker niet het geval dat iedereen hieraan meedoet, maar het enorme aantal van mobiele applicaties en tools die nu beschikbaar zijn geeft aan dat wij gemakzuchtiger met onze *body data* omgaan.

Corona-maatregelen en fitness trackers: wat is het verschil?

Door deze ontwikkeling wordt de gegevensverwerking van de corona-maatregelen soms als minder ingrijpend ervaren. Waarom zou je de verwerking van deze maatregelen anders beschouwen dan de verwerking van de mobiele applicaties die al jaren worden gebruikt? Maar dit is een glijdende schaal. Ten eerste moet er onderscheid tussen *mHealth* en de corona-maatregelen worden gemaakt. Deze maatregelen worden door andere partijen uitgevoerd en worden op een andere wijze gebruikt. Ten tweede is het belangrijk om na te denken over hoe wij überhaupt, ook buiten deze maatregelen, omgaan met onze *body data* en wat dit met ons doet. De normalisering zorgt ervoor dat we onszelf niet meer zien als mensen maar als kwantificeerbare data. Wat is onze persoonlijke verantwoordelijkheid rondom de normalisering van *body surveillance?* Er moet meer aandacht worden besteed aan de gevoelige aard van deze gegevens en waarom deze gegevens belangrijk zijn voor de fysieke, politieke en sociale autonomie. De verwerking van biometrische gegevens, inclusief gedrag, is verboden in de Europese wetgeving tenzij er uitdrukkelijk toestemming voor is gegeven.[69] Toch zien wij het verwerken van *body data* alsnog in ons dagelijks bestaan.

Individuele versus collectieve privacy

De Europese wetgeving op gegevensbescherming biedt een sterk kader voor bescherming van het individu. Als het gaat om de individuele privacy zijn er meerdere middelen en waarborgen om deze te beschermen. Maar er is nog onvoldoende aandacht besteed aan het belang van collectieve privacy en de effecten op het niveau van de samenleving. Misschien is alleen

69 Algemene verordening gegevensbescherming, Artikel 9 lid 2 sub a; Er zijn ook andere waarborgen, maar de meest gebruikelijke is toestemming.

jouw data *op zichzelf* niet heel relevant maar wel wanneer jouw data worden *gecombineerd met andere data*. Zo worden juist de collectieve data vaak gebruikt voor beslissingen over individuen. Hierdoor heb jij minder controle over je gegevens, en over wat daarmee wel of niet gedaan kan worden. Als jouw premie of waarde wordt berekend op basis van deze collectieve data, heeft deze data wel een degelijke impact op jou. Het is daarom belangrijk om aandacht te besteden aan zowel individuele als collectieve privacy belangen.

Niet het "nieuwe normaal"

De maatregelen die hier worden getroffen moeten niet gebagatelliseerd worden met het idee dat dit "het nieuwe normaal" is. Er is niks normaals aan *body surveillance* die grote gevolgen heeft voor de autonomie over onze gegevens, gezondheid en vrijheid. Het doel van het bestrijden van het coronavirus maakt de verwerking van bijzondere en gevoelige gegevens niet automatisch legitiem. Dit is vooral het geval als het doel niet overeenkomt met het resultaat.

Noodzakelijkheid

De maatregelen worden vaak gerechtvaardigd met het argument dat deze maatregelen *noodzakelijk* zijn voor het bestrijden van het coronavirus. Wat maakt iets noodzakelijk? Om te voldoen aan het beginsel van noodzakelijkheid moet niet alleen de doelstelling duidelijk zijn maar ook *hoe* de maatregel bijdraagt aan dit doel. Zo is het belangrijk om de beginselen van proportionaliteit, subsidiariteit en effectiviteit mee te nemen in de noodzakelijkheidsbeoordeling.

Proportionaliteit

Ten eerste moet de verwerking *proportioneel* zijn. Dit houdt in dat 1) de verwerking het gestelde doel kan bereiken en dat 2) dit doel in verhouding staat tot de inbreuk op de privacy van betrokkenen. Een duidelijke doelbinding en bewaartermijn zijn in dit kader belangrijk. De maatregelen in dit onderzoek verwerken bijzondere gegevens. Ze maken een zwaardere inbreuk op de privacy van betrokkenen en vereisen daarmee een sterke onderbouwing en doelbinding. De vraag die we hier moeten stellen is of deze maatregelen wel echt noodzakelijk zijn en of er geen minder ingrijpende middelen zijn die hetzelfde doel kunnen bereiken. Wat hoort thuis in een corona-maatregel?[70]

Subsidiariteit

Ten tweede moet de verwerking voldoen aan de eis van *subsidiariteit*. De vraag die we hier moeten stellen is of deze maatregelen wel echt noodzakelijk zijn en of er geen minder ingrijpende middelen zijn die hetzelfde doel kunnen bereiken. Een maatregel is niet legitiem als er minder ingrijpende alternatieven zijn. De privacy van betrokkenen moet zo min mogelijk worden geschaad.

[70] Zenger, R. (2020, 19 augustus) Wat hoort thuis in een CoronaMelder-wet? Geraadpleegd via https://www.bitsoffreedom.nl/2020/08/19/wat-hoort-thuis-in-een-coronamelder-wet/.

In dit kader moet de bescherming van de volksgezondheid niet systematisch gebruikt worden als rechtvaardigingsgrond voor een inmenging met onze digitale rechten en vrijheden.[71] De volksgezondheid is zo'n breed begrip dat elke (kleine) inmenging op privacy daardoor geaccepteerd kan worden. Dan lijkt het steeds makkelijker om privacy om op te offeren. Zoals beargumenteerd door Foucault kan zulk systematische rechtvaardiging ervoor zorgen dat individuen worden beïnvloed zonder dat zij dat doorhebben.[72] Individuen worden gecontroleerd en gemonitord om op een bepaalde manier te gedragen zonder dwangmaatregelen. Alleen omdat het geen dwangmaatregel is, betekent het niet dat het geen ingrijpende maatregel kan zijn.

De volksgezondheid en privacy sluiten elkaar niet uit. Het is geen kwestie van kiezen voor *of* privacy *of* gezondheid. Het is belangrijk om maatregelen uit te voeren die beide de privacy *en* de volksgezondheid waarborgen.

Effectiviteit

Zijn deze maatregelen effectief in het bestrijden van het coronavirus? Worden de *juiste* gegevens verwerkt? Vindt deze verwerking plaats door de *juiste* instanties?

Effectiviteit is een belangrijk beginsel voor de rechtvaardiging van een maatregel.
Als een corona-maatregel bijvoorbeeld het virus *effectief* kan bestrijden, is de inmenging op individuele rechten en vrijheden makkelijker te verdedigen. Maar dan is het belangrijk dat die maatregel dat doel ook echt kan bereiken. Experts twijfelen hierover.[73]

De effectiviteit van dit soort maatregelen is vaak afhankelijk van regelmatig gebruik van bijvoorbeeld een applicatie of een telefoon. Gezien veel van deze maatregelen vrijwillig zijn, is de effectiviteit moeilijk te waarborgen. Zo moet ten minste 60% van de bevolking de contact-tracing applicatie gebruiken om een positieve impact te hebben.[74] In de praktijk wordt de CoronaMelder veel minder gebruikt. Joran van Apeldoorn van het Instituut van Informatierecht schat op grond van zijn onderzoek dat het aantal actieve gebruikers van de app slechts 17% is, wat zelfs nog een ruime schatting is.[75]

---

[71] Houwing, L. (2020, 24 april) Opfrisser: Ook in tijden van corona willen wij geen massasurveillance. Geraadpleegd via https://www.bitsoffreedom.nl/2020/04/24/opfrisser-ook-in-tijden-van-corona-willen-wij-geen-massasurveillance/.
72 Foucault, M. 1977. *Discipline and Punish: The Birth of the Prison*. New York: Random House, p, 25-6.
73 Hoekstra, M. (2020, 12 oktober) Position paper T-Mobile Nederland i.v.m. rondetafel over het wetsvoorstel voor "Tijdelijke Wet Informatieverstrekking RIVM i.v.m. COVID-19"; Zenger, R. (2020, 5 oktober) Niemand zit te wachten op een CoronaMelder die niets toevoegt. Geraadpleegd via https://www.bitsoffreedom.nl/2020/10/05/niemand-zit-te-wachten-op-een-coronamelder-die-niets-toevoegt/.
74 University of Oxford (2020, 16 april) Digital contact tracing can slow or even stop coronavirus transmission and ease us out of lockdown. Geraadpleegd via https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown.
75 Uit een gesprek met Joran van Apeldoorn, https://www.ivir.nl/employee/joranvanapeldoorn/.

Het verwerken van gevoelige gegevens over onze lichamen moet kritisch worden beoordeeld. Gegevens over jouw gezondheid, locatie en gedrag schetsen een duidelijk beeld van wie jij bent. Deze informatie kan worden gebruikt om jou te identificeren, volgen en beïnvloeden. *Body surveillance* moet niet genormaliseerd worden, en zeker niet zonder voldoende onderbouwing van noodzakelijkheid, proportionaliteit, subsidiariteit en effectiviteit.

7. Conclusie

Tijdens de coronacrisis zijn er meerdere maatregelen ontwikkeld met invloed op individuele en collectieve rechten en vrijheden. De verwerking van gevoelige gegevens over jouw gezondheid, locatie en gedrag kan leiden tot *body surveillance*. Oftewel, het gericht, systematisch en routinematig aandacht geven aan gegevens met betrekking tot het lichaam, met het oog op beïnvloeding, controle, bescherming of richting. We moeten kritisch zijn op de neiging om onder de noemer van virusbestrijding zomaar alle verwerkingen toe te staan.

Dit onderzoek keek naar de CoronaMelder, de wijziging van de Telecommunicatiewet, de Corona opt-in en het gezondheidspaspoort en hoe zij jouw gegevens verwerken. Welke gegevens worden verwerkt en wie kan erbij? Meerdere gegevens worden verwerkt over zowel groepen als individuen. Dit betreft voornamelijk gevoelige informatie, namelijk informatie over jouw fysieke en mentale staat. Deze informatie wordt verwerkt om conclusies te trekken over hoe jij als individu en wij als samenleving ons gedragen en hoe dit gedrag kan worden beïnvloed. Het is niet wenselijk dat deze data worden gebruikt om belangrijke keuzes te maken over individuen met informatie die in eerste instantie privé hoort te zijn. Meerdere partijen hebben de sleutel tot deze gegevens waardoor het snel onoverzichtelijk wordt wie welke gegevens heeft. Onvoldoende doelbinding, transparantie en onafhankelijkheid veroorzaken onzekerheid over hoe en door wie jouw gegevens worden verwerkt. Verder is het nodig om alle maatregelen samen te behandelen. Een begrijpelijk overzicht van welke gegevens waar, wanneer en door wie worden verzameld geeft meer ruimte voor reflectie en evaluatie.

In de beantwoording van de hoofdvragen kwamen twee aandachtspunten aan licht. Ten eerste wordt het verwerken van *body data* steeds meer genormaliseerd met de toename van mobiele zorg-technologieën. Ten tweede is we onvoldoende aandacht besteed aan de noodzakelijkheid, of proportionaliteit, subsidiariteit en effectiviteit van de gegevensverwerking.

Om *body surveillance* te voorkomen, is het belangrijk om voldoende aandacht te besteden aan welke gegevens worden verwerkt, wie deze gegevens verwerkt en wat voor invloed deze verwerking heeft op ons als individuen en als samenleving.

Bits of Freedom komt op voor jouw vrijheden privacy op internet.
Deze grondrechten zijn onmisbaar voor je ontwikkeling, voor technologische innovatie en voor de rechtsstaat. Maar die vrijheid is niet vanzelfsprekend. Je gegevens worden opgeslagen en geanalyseerd. Je internetverkeer wordt afgeknepen en geblokkeerd.

Bits of Freedom zorgt ervoor dat jouw internet jouw zaak blijft.

Bits of Freedom
www.bitsoffreedom.nl
@bitsoffreedom
Prinseneiland 97HS
1013 LN Amsterdam

Contactpersoon:
Lotte Houwing
+31 6 8320 7546
lotte@bitsoffreedom.nl

PGP sleutel

BITS OF FREEDOM

Voor jouw internetvrijheid