Tweede Kamer
DER STATEN-GENERAAL

Rondetafelgesprek

Corona-app

woensdag 22 april 2020 | 08.30-12.30 uur | Oude Zaal

VASTE COMMISSIE VOLKSGEZONDHEID, WELZIJN EN SPORT

VASTE COMMISSIE VOOR BINNENLANDSE ZAKEN | VASTE COMMISSIE ECONOMISCHE ZAKEN
VASTE COMMISSIE VEILIGHEID EN JUSTITIE

Tweede Kamer
DER STATEN-GENERAAL

Reader rondetafelgesprek Corona-app

datum 22 april 2020

Dienst Analyse en Onderzoek
Staf vaste commissie voor Volksgezondheid, Welzijn en Sport

Geachte Leden,

Hierbij treft u de definitieve versie aan van de reader voor het rondetafelgesprek 'Corona-app' van woensdag 22 april 2020.

In deze digitale reader kunt u via de inhoudsopgave doorklikken naar de onderliggende documenten. Via de grijze 'Terug' button (links bovenin elke pagina) gaat u terug naar de inhoudsopgave.

Op tablets kunt u de digitale reader onder andere openen met de Adobe Acrobat Reader App. U kunt dan via het 'opengeslagen boek' icoontje terug naar de inhoudsopgave.

Met vriendelijke groet,

De informatiespecialisten van de vaste commissie voor Volksgezondheid, Welzijn en Sport

Inhoudsopgave

I. Convocatie rondetafelgesprek Corona-app

II. Blok 1:
CV's deelnemers

Position Papers
Mw. N. Helberger
Mw. J. van Dijck
Dhr. M.R. van Steen

III. Blok 2:
CV's deelnemers

Position Papers
Dhr. N. Chavannes
Dhr. M.J. de Vries
Dhr. R. Creemers

IV. Blok 3:
CV's deelnemers

Position Papers
Dhr. B. Filippini
Mw. E. Austin (geen position paper bij het verschijnen van deze reader)
Mw. M. Stikker

V. Blok 4:
CV's deelnemers

Position Papers
Dhr. R. Prins
Dhr. S. Ruwhof
Dhr. J. Terstegge

VI. Position Papers niet-genodigden
Bijdrage Dhr. H. Sheikh, WRR
Bijdrage Mw. M. Koning, Amnesty International

VII. Selectie krantenartikelen 18-20 april 2020

VIII. Overige relevante documenten

Inhoudsopgave

Tweede Kamer
DER STATEN-GENERAAL

Den Haag, 20 april 2020

Voortouwcommissie:	**vaste commissie voor Volksgezondheid, Welzijn en Sport**
Volgcommissie(s):	vaste commissie voor Binnenlandse Zaken vaste commissie voor Economische Zaken en Klimaat vaste commissie voor Justitie en Veiligheid
Activiteit:	**Rondetafelgesprek**
Datum:	woensdag 22 april 2020
Tijd:	08.30 - 12.30 uur
Openbaar/besloten:	openbaar
Onderwerp:	Corona-app

Blok 1: 08:30 - 09:25 uur Wetenschap

1. Prof.dr. Natali Helberger, Universiteitsprofessor Recht en Digitale Technologie, Universiteit van Amsterdam
2. Prof. José van Dijck, Hoogleraar Media en Digitale Samenleving, Universiteit Utrecht
3. Prof.dr.ir. Maarten van Steen, Wetenschappelijk directeur, Digital Society Institute, Universiteit Twente

Blok 2: 09:30 - 10:25 uur Wetenschap

1. Prof. dr. Niels Chavannes, hoofd van de sectie Wetenschappelijk Onderzoek Eerstelijnsgeneeskunde, Initiatiefnemer National eHealth Living Lab, LUMC
2. Prof. dr. M.J. de Vries, Hoogleraar technische natuurwetenschappen TU Delft, expertise ethiek/filosofie van de technologie
3. Dr. R.J.E.H Creemers, University Lecturer Modern China Studies/Leiden University

Blok 3: 10:30 -11:25 uur (onderzoeks-) instellingen

1. Bas Filippini, voorzitter Privacy First
2. Evelyn Austin, directeur Bits of Freedom
3. Marleen Stikker, directeur Waag

Blok 4: 11:30 - 12:25 uur juridisch & bedrijfsleven

1. Ronald Prins, Lid Toetsingscommissie Inzet Bevoegdheden Inlichtingen- en Veiligheidsdiensten (TIB), Buitengewoon Raadslid OVV
2. Sijmen Ruwhof, Freelance IT Security Consultant/Ethisch Hacker
3. Jeroen Terstegge, partner bij Privacy Management Partners

Griffier:	M.Y. Israel
Activiteitnummer:	2020A01700

Inhoudsopgave

Inhoudsopgave

Tweede Kamer
DER STATEN-GENERAAL

Blok 1

CV’s en Position Papers

/

Rondetafelgesprek Corona-app woensdag 22 april 8.30 – 12.30 uur

Blok 1

Natali Helberger – Hoogleraar Law and Digital Technology, Universiteit van Amsterdam

- Natali Helberger bestudeert als hoogleraar Informatierecht de juridische, ethische en beleidsmatige uitdagingen die gepaard gaan met het gebruik van algoritmes en AI in de media, politieke reclame, commercie en de gezondheidssector en de implicaties voor gebruikers en de samenleving.
- Lid van het managementteam van het Instituut of Informatierecht van de UvA.
- Sinds 2019 leidt ze mede de Research Priority Area 'Human(e) AI' aan de UvA.
- Binnen de onderzoeksagenda 'De Digitale Samenleving' van de VSNU, leidt Helberger het onderdeel burgerschap en democratie.
- Ze zit in het expertcomité van de Raad van Europa voor AI en mensenrechten, de wetenschappelijke adviesraad van het Reuters Institute en van het Florence Institute for Regulation, en in de stuurgroep van het Zwitserse nationale onderzoeksprogramma over digitale transformatie.

José van Dijck – Hoogleraar Media en Digitale Samenleving, Universiteit Utrecht

- Sinds 1 januari 2017 is Van Dijck universiteitshoogleraar media en digitale samenleving aan de Universiteit Utrecht. Haar onderzoek gaat over media, sociale media en mediatechnologieën.
- 2001 tot en met 2016 hoogleraar vergelijkende mediawetenschappen aan de Universiteit van Amsterdam.
- Van 2015 tot 2018 was ze de eerste vrouwelijke president van de Koninklijke Nederlandse Akademie van Wetenschappen.
- Gasthoogleraar en -docent aan verschillende universiteiten in de Verenigde Staten, Canada en Australië zoals het Concordia University in Montreal (Canada), Massachusetts Institute of Technology (MIT) in Cambridge (USA), de University of Technology, Sydney (UTS) in Australie; Georgia Tech University in Atlanta (USA); de University of California, Santa Cruz (USCS); de Annenberg School of Communication van de University of Pennsylvania (Philadelphia); en Stockholm University.
- In mei 2019 ontving zij een eredoctoraat van de universiteit van Lund (Zweden).

Maarten R. van Steen – Wetenschappelijk directeur, Digital Society Institute, Universiteit Twente

- Maarten van Steen doet onderzoek naar genetwerkte computersystemen in het bijzonder draadloze systemen als ook meer traditionele gedistribueerde systemen.
- Expertises: Network Protocols, Communication, Servers, Scalability, Middleware, Experiments, Semantics, Internet.

- Sinds januari 2015 is Van Steen wetenschappelijk directeur van het digitaliseringsonderzoeksinstituut van de Universiteit Twente: The Digital Society Institute.
- Voorzitter van het ICT onderzoek Platform Nederland (IPN) waarin alle Nederlandse academische afdelingen en instituten vertegenwoordigd zijn.
- Voorzitter van de NWO Informatica adviesraad.

Inhoudsopgave

Ministerie van Algemene Zaken
T.a.v. minister-president Mark Rutte
Binnenhof 19
2513 AA Den Haag

Ministerie van Volksgezondheid, Welzijn en Sport
T.a.v. minister Hugo de Jonge, minister Martin van Rijn
en de heer F. Sijbesma
Parnassusplein 5
2511 VX Den Haag

Ministerie van Justitie en Rechtsbescherming
T.a.v. minister Ferdinand Grapperhaus
Turfmarkt 147
2511 DP Den Haag

Amsterdam, 13 april 2020

Inzake: COVID-19 tracking- en tracingapp en gezondheidsapp

Geachte minister-president Rutte, minister De Jonge, minister Van Rijn, minister Grapperhaus, heer Sijbesma,

"Surveillance is permanent in its effects, even if it is discontinuous in its action." - Michel Foucault

Tijdens de persconferentie over het Corona-virus van dinsdag 7 april jl. kondigde minister De Jonge aan dat het kabinet de inzet van twee apps overweegt. De eerste is een zogenaamde 'tracking- en tracingapp' om, zodra een of meerdere Corona-maatregelen gedeeltelijk kunnen worden opgeheven, beter in kaart te brengen wie contact heeft gehad met een met het Corona-virus besmette persoon (hierna: "Trackingapp"). De tweede is een gezondheidsapp waarbij de gezondheid en eventuele COVID-19 symptomen kunnen worden bijgehouden en gedeeld met medisch specialisten (de Gezondheidsapp), hierna gezamenlijk de "Apps".

De inzet van tracking- en tracingapps en gezondheidsapps is zeer ingrijpend. Belangrijk is daarom dat kritisch gekeken wordt naar het nut, de noodzaak en de effectiviteit van dergelijke apps, alsook naar de impact ervan op het brede sociale systeem inclusief onze fundamentele rechten en vrijheden. Of we het nu willen of niet, deze Apps zullen een precedent scheppen voor toekomstig gebruik van vergelijkbare invasieve technologieën, ook na deze crisis. Juist in crisistijd moet men zeer zorgvuldige maatschappelijke en juridische afwegingen maken om te bepalen of men een dergelijke zeer invasieve maatregel wil nemen.

Het lijkt er nu op dat de Nederlandse regering de pijlen bijna uitsluitend richt op inzet van de Apps (althans voor zover het de exit-strategie aangaat). De ondergetekenden van deze brief willen vooropstellen dat digitale technologie een bijdrage kan leveren aan het oplossen van maatschappelijke problemen, maar dat technologie zelden *de* oplossing is voor een bepaald probleem. Het is dan ook zaak om eerst goed inzichtelijk te krijgen welk probleem men exact wil adresseren en of de Apps überhaupt een oplossing bieden voor dat probleem.

Het besluit over of de Apps al dan niet zouden moeten worden ingezet, moet daarom worden begeleid door experts niet alleen op het gebied van app-ontwikkeling, maar juist ook op het gebied van recht, sociale wetenschappen, gedragswetenschappen, ethiek, het gezondheidsdomein en de systeemwetenschap. Dit temeer om techno-solutionisme te voorkomen en de mogelijkheid te behouden om te besluiten de Apps niet in te zetten.

Het gebruik van de Apps mag onze fundamentele rechten en vrijheden niet aantasten. Het gebruik van alle apps en technologieën in verband met de bestrijding van de Corona-crisis moet in ieder geval tijdelijk, strikt noodzakelijk, proportioneel, controleerbaar, transparant en toetsbaar zijn.

Hieronder lichten de ondergetekenden het voorgaande nader toe. De ondergetekenden zijn allen experts vanuit diverse disciplines, waaronder computerwetenschappen, datawetenschappen, artificiële intelligentie, recht, geneeskunde, gedragswetenschappen, sociale wetenschappen, ethiek, communicatiewetenschappen en beleid.

Samenvatting van de belangrijkste punten

- De inzet van de Apps is zeer ingrijpend. Belangrijk is daarom dat kritisch gekeken wordt naar het daadwerkelijke nut, de noodzaak en de effectiviteit van deze Apps , alsook de sociaal-maatschappelijke en juridische impact, naar voordat besloten wordt ze in te zetten.
- Technologie is zelden *de* oplossing voor een bepaald probleem. Gewaakt moet worden voor techno-solutionisme. De mogelijkheid moet blijven bestaan om te besluiten de Apps niet in te zetten. Minder invasieve oplossingen moeten de voorkeur krijgen.
- Effectiviteit en betrouwbaarheid van de Apps is van enorm belang, omdat *in*effectiviteit en *on*betrouwbaarheid juist kan leiden tot een groter risico op besmetting. Het creëert dan immers slechts 'schijnveiligheid'.
- De Apps hebben impact op meer dan (data)privacy alleen. Ze raken ook aan de vrijheid van vereniging, het recht op veiligheid, het recht op gezondheid en het recht op non-discriminatie.
- Fundamentele rechten en vrijheden kunnen niet zomaar opzij gezet worden. Daarvoor moet een gerechtvaardigd belang zijn, het moet strikt noodzakelijk zijn, evenredig en bovenal beperkt in de tijd.
- Van het gebruik van de Apps moet worden afgezien indien: (i) 'contact tracering' of gezondheidsmonitoring via de Apps niet (langer) doeltreffend, effectief of betrouwbaar is; (ii) er minder invasieve oplossingen mogelijk zijn; (iii) de sociale implicaties te zwaar wegen; (iv) er geen geen breed gedragen verantwoorde afweging gemaakt kan worden tussen conflicterende (fundamentele) rechten en vrijheden.
- Het gebruik van de Apps mag niet worden bereikt door middel van enige vorm van verplichting of dwang.
- Bij de besluitvorming en de eventuele ontwikkeling en inzet van de Apps moet een breed team van experts uit diverse disciplines worden betrokken, waaronder computerwetenschappers, datawetenschappers, epidemiologen, intensivisten en longartsen, rechtswetenschappers (privacy en databescherming, mensenrechten en bestuursrecht,) gedragswetenschappers, communicatiewetenschappers en ethici.
- De eventuele inzet van de Apps moet naast tijdelijk (en dus omkeerbaar), strikt noodzakelijk en proportioneel ook controleerbaar, transparant en toetsbaar zijn.
- Alleen het uitrollen van de Apps, zonder dat gekeken is naar de invloed op de (sociale) systemen en gedragspatronen, en zonder dat de achterliggende infrastructuur (GGD's, testlabs, etc.) daarop is ingesteld, is onvoldoende.

Sociaal-maatschappelijke impact - de noodzaak tot systeemdenken

Alleen het uitrollen van de Apps, zonder dat gekeken is naar de invloed op de (sociale) systemen en gedragspatronen, en zonder dat de achterliggende infrastructuur daarop is ingesteld, is onvoldoende.

De consequenties die worden verbonden aan 'signalering' door de App (zoals bijvoorbeeld verplicht isoleren, geen toegang tot werk of winkels, etc.) zullen van invloed zijn op het (juiste) gebruik van de Apps. Net zo goed als sommige mensen zich nu niet aan bepaalde maatregelen houden, zullen sommige mensen de App niet of (bewust) niet juist gebruiken, bijvoorbeeld om isolatie te voorkomen. Dit zal de effectiviteit en betrouwbaarheid van de Apps ondermijnen. De WHO heeft al gewaarschuwd voor stigmatisering als gevolg van het gebruik van tracking- en tracingapps en de geschiedenis leert ons dat het samenspel van surveillance en epidemiologie helaas ook kan leiden tot bedreiging en geweld jegens bepaalde groepen. Ook potentiële stigmatisering van zorgprofessionals, die immers continue contact met COVID-19 patienten hebben, is een punt van zorg. Als bovendien na enige tijd blijkt dat het gebruik van de Apps niet voldoende is om een nieuwe uitbraak van het virus te voorkomen, zal het maatschappelijke verzet om weer onder sociale afstand regels te gaan leven groot zijn.

Expertise uit de gedragswetenschappen en ervaring met vergelijkbare apps uit andere landen of bij eerdere epidemieën is cruciaal om goed te kunnen beoordelen of het gebruik ervan überhaupt het gewenste effect zal hebben. Andere, minder invasieve oplossingen verband houdende met contactonderzoek moeten actief worden onderzocht en geprioriteerd, zoals bijvoorbeeld het (tijdelijk) aannemen van meer personeel voor het uitvoeren van of ondersteunen bij contactonderzoek.

Ook moet worden onderzocht wat de impact van de invoering van de voorgestelde Apps zou kunnen zijn 'achterliggende' infrastructuur, en of deze voldoende is ingericht op het gebruik van de Apps. Als een 'App-signaal' bijvoorbeeld leidt tot uitgebreid contactonderzoek door de GGD of een advies tot testen, is de capaciteit daar dan op berekend?

Fundamentele rechten en vrijheden

Fundamentele rechten en vrijheden kunnen niet zomaar opzij gezet worden. Er moet een gerechtvaardigd belang zijn, het moet strikt noodzakelijk zijn, evenredig en bovenal beperkt in de tijd. Deze Apps leiden ertoe dat diverse fundamentele rechten en vrijheden opzij worden gezet, en dat vraagt dus om een gedegen afweging.

Minister de Jonge liet weten dat de Apps privacyvriendelijk zullen zijn en op basis van anonimiteit zullen werken. Van belang is echter om zich te realiseren dat naast impact op het fundamentele recht op privacy, tracking- en tracingapps en gezondheidsapps ook impact hebben op andere mensenrechten zoals de vrijheid van vergadering en vereniging, het recht op veiligheid en gezondheid en het recht op non-discriminatie. Al deze rechten worden hieronder toegelicht (te beginnen met privacy).

<u>Privacy - meer dan gegevensbescherming alleen</u>

De privacydiscussies rond de aangekondigde Apps richten zich momenteel voornamelijk op gegevensbescherming van (bijzondere) persoonsgegevens en op anonimiteit. De impact van de Apps op onze privacy gaat echter veel verder dan alleen onze data en anonimiteit.

Art. 8 van het EVRM (recht op een privéleven) omvat de bescherming van een breed scala aan elementen van ons privéleven waaronder (i) iemands (algemene) privacy, (ii) iemands fysieke,

psychologische of morele integriteit en (iii) iemands identiteit en autonomie. De Trackingapp creëert een situatie waarin we (constant) worden bekeken, gevolgd en (mogelijk) geïdentificeerd. Het is aangetoond dat zodra mensen weten dat ze worden gecontroleerd, ze zich anders gaan gedragen. Als psychologisch ‘chilling’ effect kunnen mensen geneigd raken om hun gedrag aan te passen, met mogelijk ongewenste gevolgen voor de doeltreffendheid en betrouwbaarheid van de Trackingapp. Zelfs als de data volledig wordt versleuteld en onmiddellijk wordt verwijderd na het vastleggen, dringt de technologie nog steeds ons privéleven en onze psychologische en morele integriteit binnen. Het enkel garanderen van anonimiteit is derhalve onvoldoende om ook de (brede) privacy te garanderen.

Terug naar dataprivacy, zullen beide Apps aan de strengste gegevensbeschermingsvereisten moeten voldoen. Beide Apps verzamelen in meer of mindere mate bijzondere persoonsgegevens, de verwerking waarvan slechts in uitzonderlijke gevallen en onder strenge voorwaarden is toegestaan. Het risico bestaat bovendien dat de verzamelde data (nu of in de toekomst) niet alleen gebruikt zullen worden ter ondersteuning van contactonderzoek en monitoring van de gezondheid door een medisch specialist, maar ook om mensen te profileren, categoriseren en scoren voor verschillende doeleinden. Met een langere horizon kan men zich zelfs voorstellen dat 'function creep' zal kunnen leiden tot ongewenste vormen van profilering bij toezicht en surveillance, acceptatie voor verzekeringen of sociale uitkeringen, aanname of ontslag, etc. De data die met de Apps wordt verzameld mag daarom onder geen beding worden gebruikt voor profilering, risico-scoring, classificatie of predictie.

Overige fundamentele rechten en vrijheden - meer dan privacy alleen

De Apps hebben daarnaast bredere implicaties voor een aantal andere fundamentele rechten en vrijheden. De vrijheid van vergadering en vereniging, vooral van degenen die geïnfecteerd zijn en degenen die met geïnfecteerden in 'contact' zijn gekomen, wordt aangetast. Genoemde stigmatisering van personen die bepaalde kenmerken of relaties vertonen die volgens de Trackingapp verband houden met COVID-19, kan leiden tot discriminatie op grond van (vermoedelijke) ziekte. Hoewel de Apps mogelijk zouden kunnen bijdragen aan het recht op veiligheid en gezondheid, geldt dat de veiligheid en bescherming van de gezondheid die met de Apps wordt geoogd afhangt van de doeltreffendheid, effectiviteit en betrouwbaarheid van de Apps (zie hieronder).

Verplicht of vrijwillig gebruik

Op een vraag van een van de aanwezige journalisten of het gebruik van de Apps verplicht zou worden gesteld antwoordde Minister De Jonge tijdens de persconferentie dat hij 'alle opties open hield'. Ten eerste, vrijwilligheid alleen is onvoldoende om de vele implicaties van het gebruik van de Apps adequaat te adresseren. De sociaal-maatschapplijke impact en de impact op fundamentele rechten en vrijheden alsook de vereisten van tijdelijkheid, strikte noodzakelijkheid, proportionaliteit, controleerbaarheid, transparantie en toetsbaarheid gelden evengoed als de Apps op vrijwillige basis worden gebruikt.

Als het gebruik van de Apps verplicht wordt gesteld zou dat betekenen dat niemand zich meer zonder (goed opgelade) compatibele mobiele telefoon mag verplaatsen. Dit is redelijkerwijs niet haalbaar en al zeker niet handhaafbaar. De ondergetekenden zijn dan ook tegenstander van verplicht gebruik van de Apps, maar merken op dat ook vrijwillig gebruik onder bepaalde omstandigheden feitelijk niet vrijwillig zal zijn. Wanneer de Apps worden ingezet om bijvoorbeeld toegang te verschaffen tot bepaalde plaatsen of als controle-instrument voor handhaving, is er geen sprake van echte vrijwilligheid. De Apps mogen derhalve ook niet als zodanig worden ingezet.

Doel, effectiviteit en betrouwbaarheid van de Trackingapp

Er dienen zich inmiddels diverse organisaties aan en er worden diverse initiatieven ontplooid voor de ontwikkeling van COVID-19 tracking- en tracing apps en het Ministerie van VWS heeft een tender opgengezet. Van belang echter is om eerst vast te stellen of de Apps überhaupt nuttig, effectief en betrouwbaar genoeg kunnen zijn om het gewenste doel te bereiken.

Effectiviteit en betrouwbaarheid van de Trackingapp is van enorm belang, omdat *in*effectiviteit en *on*betrouwbaarheid juist kan leiden tot een groter risico op besmetting. Het creëert dan immers slechts 'schijnveiligheid', waarbij mensen denken 'ik kan wel weer naar buiten, naar het werk of naar het park, want ik krijg toch wel een bericht van de app als ik in de buurt van een besmet persoon ben', terwijl deze informatie niet betrouwbaar is. Deze schijnveiligheid kan bovendien leiden tot onjuiste beleidsmaatregelen, met als risico dat de verspreiding van het virus juist weer toeneemt. Bovendien zullen de grote aantallen foute positieven en foute negatieven, een inherent gevolg van inefficiëntie en onbetrouwbaarheid van de Trackingapp, de druk op de 'achterliggende' infastructuur onnodig opvoeren.

Vragen rondom effectiviteit en betrouwbaarheid van de Trackingapp spelen bijvoorbeeld in het licht van: (i) het nog altijd relatief beperkte COVID-19 testbeleid in Nederland en de invloed van asymptomatische besmetting of besmetting via oppervlakten; (ii) instabiliteit en inaccuratesse van de mogelijke technologieën (Bluetooth, GPS); (iii) de haalbaarheid van het percentage van de bevolking dat de Trackingapp moet gebruiken voor betrouwbaar resultaat; en (iv) resultaten van het gebruik van tracking- en tracingapps in andere delen van de wereld zoals Singapore, waar recent een stijging van het aantal besmettingen is.

Kaders en proces - aanbevelingen

Hieronder vindt u een overzicht van de kaders en de aanpak die de ondertekenaars voorstellen tijdens de besluitvorming over, en de mogelijke ontwikkeling en inzet van de Apps.

<u>Algemene kaders ("0-vragen"):</u>

- De Apps moeten bewezen doeltreffend, effectief en betrouwbaar zijn (onderzocht tijdens de pilotfase, zie onder 'Aanpak') en blijven (tijdens eventueel gebruik) om het gewenste doel te bereiken en daadwerkelijk en beter dan andere minder invasieve maatregelen, helpen om het aantal COVID-19 infecties significant en aantoonbaar te verminderen.
- Minder invasieve oplossingen voor contactonderzoek en gezondheidsmonitoring moeten actief worden onderzocht en de voorkeur krijgen boven het gebruik van de Apps.
- De sociale implicaties van het gebruik van de Apps moeten bij het besluit tot het al dan niet inzetten van de Apps moet worden meegewogen.
- Het gebruik van de Apps respecteert alle relevante wet- en regelgeving, inclusief fundamentele rechten en vrijheden.
- Van het gebruik van de Apps moet worden afgezien indien: (i) 'contact tracering' of gezondheidsmonitoring via de Apps niet (langer) doeltreffend, effectief of betrouwbaar is; (ii) er minder invasieve oplossingen mogelijk zijn; (iii) de sociale implicaties te zwaar wegen; of (iv) er geen breed gedragen verantwoorde afweging gemaakt kan worden tussen conflicterende (fundamentele) rechten en vrijheden.

<u>Kaders voor besluitvorming:</u>

- Het gebruik van de Apps heeft een wettelijke basis, is tijdelijk, strikt noodzakelijk, proportioneel, controleerbaar, transparant en toetsbaar.
- De Apps mogen uitsluitend gebruikt worden om het gewenste doel te bereiken, inhoudende dat de Apps en alle daarmee verzamelde gegevens alleen mogen worden gebruikt ter ondersteuning van COVID-19 contactonderzoek (Trackingapp) en gezonheidsmonitoring

door een medisch specialist uitsluitend in verband met COVID-19 (Gezondheidsapp). Elk ander gebruik moet zoveel mogelijk technisch worden voorkomen en niet worden toegestaan.

- De duur van het gebruik van de Apps is beperkt in de tijd en het gebruik is volledig omkeerbaar. De met de Apps verzamelde en/of gegenereerde data zal na ontmanteling van de Apps permanent worden verwijderd.
- Het gebruik van de Apps mag niet worden bereikt door middel van enige vorm van verplichting of dwang. Het in rekening brengen van gebruiksvergoedingen of het aanbieden van financiële prikkels moet niet worden toegestaan. Mensen die weigeren een of beide Apps te gebruiken, mogen geen negatieve gevolgen ondervinden.
- De Trackingapp vervangt het contactonderzoek zoals dat nu door de GGD's wordt verricht niet, maar is daar uitsluitend ondersteunend aan.
- Het 'achterliggende' systeem (GGD, testcapaciteit, etc.) is berekend op het gebruik van de Apps.
- Er is een systeem ingericht voor monitoring van de maatschappelijke gevolgen van het gebruik van de Apps, inclusief de mogelijkheid om in te grijpen als zich misstanden voordoen.

Kaders voor de ontwikkeling en het gebruik:

- Verifieerbare technische maatregelen zoals cryptografie en anonimisering moeten de privacy van gebruikers waarborgen en de-anonimisering moet onmogelijk zijn. Enkel beleidsmaatregelen of -beloften zijn hiertoe onvoldoende. Een decentraal protocol waarbij geen gegevensuitwisseling hoeft plaats te vinden met een centrale autoriteit (zoals bijvoorbeeld het DP3T-protocol) dient te worden onderzocht.
- Alleen minimale gegevens en metagegevens die nodig zijn voor de werking van de Apps kunnen worden tijdelijk en zo kort mogelijk opgeslagen. Voor de Trackingapp betekent dit dat het verzamelen van gegevens die verder gaan dan een contact tussen mensen en de duur daarvan niet toegestaan is. Voor beide Apps geldt dat gegevens die niet langer nodig zijn, moeten worden verwijderd.
- Gevoelige gegevens waaronder, maar niet beperkt tot, bijzondere persoonsgegevens, moeten lokaal en veilig op de telefoon worden opgeslagen en versleuteld. Een koppeling van de gegevens met andere (openbare of niet-openbare) gegevens mag niet worden toegestaan. Delen van de gegevens met derden mag niet worden toegestaan.
- De Apps zelf moeten de gebruiker regelmatig herinneren aan het feit dat deze 'aan staan', moeten eenvoudig door de gebruiker tijdelijk kunnen worden gedeactiveerd en eenvoudig door de gebruiker definitief kunnen worden verwijderd.

Proces:

- De effectiviteit, betrouwbaarheid en doeltreffendheid van de Apps moet vooraf worden onderzocht en getest (pilotfase) om te beoordelen of de inzet van de Apps überhaupt zinvol is. Zo niet, dan moet van het gebruik van de Apps worden afgezien.
- Over het verloop en de uitkomsten van de pilotfase moet volledige transparantie worden gegeven.
- Tijdens deze pilotfase moeten procedures worden ontwikkeld voor het doorlopend controleren van het functioneren van de Apps, het signaleren en afhandelen van foute positieven en foute negatieven en de gevolgen voor de samenleving en het gedrag van mensen.
- Bij de besluitvorming over het al dan niet inzetten van de Apps, de pilotfase en het eventuele inzetten van de Apps, dienen niet alleen de experts op het gebied van app-ontwikkeling betrokken te zijn, maar ook computerwetenschappers, datawetenschappers, epidemiologen, intensivisten en longartsen, deskundigen op het gebied van recht, inclusief privacy en

databescherming, mensenrechten en bestuursrecht, gedragsdeskundigen, ethici, communicatiedeskundigen en systeemdeskundigen.
- Deze experts moeten tijdens het eventuele gebruik van de Apps betrokken blijven bij de monitoring van de uitkomsten en gevolgen van het gebruik van de Apps.
- Uit het oogpunt van democratische controle en verantwoording moet er volledige transparentie over de aanbieder(s)/ontwikkelaar(s) van de Apps en de selectie-procedure zijn.
- De relevante autoriteiten zoals het College voor Bescherming van de Rechten van de Mens, de Autoriteit Persoonsgegevens, de Federatie Medisch Specialisten, de NVIC en de Patiëntenfederatie moeten bij de pilotfase en tijdens het mogelijke gebruik van de Apps worden betrokken.
- De Tweede Kamer der Staten Generaal moet volledig geïnformeerd worden over en betrokken worden bij (de besluitvorming over) de ontwikkeling en inzet van de Apps, zowel gedurende de pilotfase als gedurende het eventuele gebruik ervan.

Conclusie

Bijzondere tijden vragen om bijzondere maatregelen. En dit zijn bijzondere tijden. Onze democratie en rechtstaat vereisen om ook in bijzondere tijden bijzondere maatregelen zoals deze kritisch tegen het licht te houden. Alleen dan kunnen weloverwogen en volledig geïnformeerde besluiten worden genomen. Wij hopen u met deze bijdrage een breed inzicht te hebben gegeven in de vele implicaties van de inzet van de Apps en u zo te hebben kunnen helpen bij uw besluitvorming.

Hoogachtend,

(Zie volgende pagina's voor ondertekenaars)

Cc:

Fractievoorzitters Tweede Kamer
Tijdelijke Tweede Kamercommissie Digitale Toekomst
Outbreak Mangement Team
College voor de Rechten van de Mens
Autoriteit Persoonsgegevens
Federatie Medisch Specialisten
Nederlandse Vereniging voor Intensive Care
Patiëntenfederatie

Catelijne Muller
Voorzitter ALLAI, Lid EU High Level Expert Group on AI
Natali Helberger
Universiteitsprofessor Recht en Digitale Technologie met speciale focus op AI
Universiteit van Amsterdam
Virginia Dignum
Professor of Social and Ethical AI
Umeå University Zweden en verbonden aan TU Delft Lid High Level Expert Group on AI, Bestuurslid ALLAI
Frank Dignum
Professor of Socially Aware AI
Umeå University Zweden en verbonden aan TU Delft
Claes de Vreese
Universiteitsprofessor Political Communication & Journalism
Universiteit van Amsterdam
Aimee van Wynsberghe
Associate Professor Ethics & Robotics TU Delft, Lid High Level Expert Group on AI
Bestuurslid ALLAI & Responsible Robotics
Valerie Frissen
Hoogleraar Digital Technologies & Social Change, Universiteit Leiden
Mireille Hildebrandt
Research Professor of Interfacing Law & Technology, Vrije Universiteit Brussel
Peter-Paul Verbeek
Universiteitshoogleraar Filosofie van Mens en Techniek, Universiteit Twente
Voorzitter UNESCO World Commission for the Ethics of Science and Technology
Iris de Rooij
Associate Professor Computational Cognitive Science, Radboud Universiteit
Lambèr Royakkers
Associate Professor Ethics and Technology
TU Eindhoven
Ronald Leenes
Head of the Department of Law, Technology, Markets, and Society
Tilburg University
Maxim Februari
Schrijver, jurist, filosoof
Rineke Verbrugge
Professor Artificial Intelligence, Logic and Cognition, Multi-agent systems
Rijksuniversiteit Groningen

Mark Coeckelbergh
Professor of Philosophy of Media and Technology, Universität Wien
Gabriëlle Speijer
Radiotherapeut-Oncoloog Haga Ziekenhuis
Founder CatalyzIT
Beate Roesler
Chair of the Department of Philosophy
Universiteit van Amsterdam
Holger Hoos
Professor Machine Learning
Universiteit Leiden
Michael Veale
Lecturer in Digital Rights and Regulation
Faculty of Laws, University College London
José van Dijk
Universiteitsprofessor Media en Digitale Samenleving, Universiteit Utrecht
Pinar Yolum
Universitair hoofddocent Informatica
Universiteit Utrecht
Jeroen van den Hoven
Universiteitshoogleraar Ethiek en Techniek
TU Delft
Carlo van de Weijer
General Manager
Eindhoven AI Systems Institute
Carina Weijma
Co-Chair Maatschappelijke acceptatie, Inclusie, Ethics Nationale AI Coalitie
Veronika Cheplygina
Assistant Professor TU Eindhoven
Moniek Buijzen
Professor of Communication Science
Radboud Universiteit
Martijntje Smits
Senior onderzoeker en Techniekfilosoof
Bureau Innovatie & Reflectie
Antal van den Bosch
Directeur Meertens Instituut
Davide Grossi
Adjunct Hoogleraar Science and Engineering
Rijksuniversiteit Groningen en UvA
Tom van Engers
Professor in Legal Knowledge Management
Universiteit van Amsterdam
Niels van Dijk
Assistant Professor Legal Philosophy & Sociology, Vrije Universiteit Brussel
Marijn Sax
Ethicus, Universiteit van Amsterdam

(vervolg ondertekenaars op volgende pagina)

Julia van Weert
Hoogleraar Gezondheidscommunicatie
Universiteit van Amsterdam
Margot van Herwaarden
Gastro-enteroloog
Deventer Ziekenhuis
Gerhard Weiss
Professor of Computer Science and AI
Universiteit Maastricht
Ralph Peters
Full Professor of Mathematics in Knowledge Engineering Universiteit Maastricht
Frank Thuijsman
Professor on Strategic Optimization and Data Science, Universiteit Maastricht
Mark Winands
Hoogleraar Machine Reasoning
Universiteit Maastricht
Andre Dekker
Hoogleraar Radiotherapy
Universiteit Maastricht
Sally Wyatt
Hoogleraar Technology & Society Studies
Universiteit Maastricht
Hans Radder
Emeritus Professor Department of Philosophy, VU
Vanessa Evers
Hoogleraar Human Media Interaction
Universiteit Twente
Janneke Gerards
Hoogleraar Fundamentele Rechten
Universiteit Utrecht
Tom van Engers
Hoogleraar Legal Knowledge Management
Universiteit van Amsterdam
Albert Meijer
Hoogleraar Publieke innovatie
Universiteit Utrecht
Bert Slagter
Expert complexiteit en onzekerheid,
Founder LekkerCryptisch.nl
Anna Gerbrandy
Hoogleraar Mededingingsrecht
Universiteit Utrecht
Marleen Huysman
Professor in the Department of Information Systems, Marketing and Logistics, VU
Linnet Taylor
Associate Professor Tilburg Institute for Law, Technology and Society

Edith Smit
Hoogleraar Communicatiewetenschapen
directeur Graduate School of Communication
Universiteit van Amsterdam
Simone van der Hof
Professor Law and Digital Technology
Universiteit Leiden
Tobias Blanke
Professor in Social and Cultural Informatics
Universiteit van Amsterdam
Maranke Wieringa
Universiteit Utrecht
Utrecht Data School
Guda van Noort
Professor Persuasion & New Media Technologies, Universiteit van Amsterdam
Johan Pouwelse
Associate Professor Computer Science
TU Delft
Aviva de Groot
Doctoral Researcher
Tilburg University
Frederik Zuiderveen Borgesius
Hoogleraar ICT en Recht
Radboud Universiteit
Merel Noorman
Assistant Professor
TILT/LTMS
Tilburg University
Mirko Tobias Schäfer
Associate Professor
Project lead Utrecht Data School
Universiteit Utrecht
Ivana Isgum
Universiteitshoogleraar AI
en Medical Imaging
Universiteit van Amsterdam
Francien Dechesne
Assistant Professor Law and Digital Technologies, Universiteit Leiden

Inhoudsopgave

Rondetafelgesprek Corona apps
Tweede Kamer, 22 april 2020
Bijdrage van prof. dr. José van Dijck, universiteitshoogleraar media en digitale samenleving, Universiteit Utrecht, onderzoeksgroep Governing the Digital Society.

Geachte leden van de Tweede Kamer,

Hartelijk dank dat u mij in de gelegenheid stelt mijn visie onder de aandacht te brengen; dit paper is geschreven in consultatie met een aantal collega's uit verschillende vakgebieden. Wij hebben met belangstelling het proces van de afgelopen weken gevolgd, inclusief de appathon van afgelopen weekend. Complimenten aan VWS voor een proces waarbij de input van velen gevraagd wordt, ook al verloopt het onder grote druk en in (te) grote haast. Het probleem is echter het veel te smalle doel van deze exercitie: een goed werkende, veilige, privacy- en gebruiksvriendelijke app die de GGD ondersteunt bij het contactonderzoek. Niet meer, niet minder. Zoiets als een goed werkende thermometer in een dokterstas van de GGD. Waar het eigenlijk om zou moeten gaan is het *geheel aan interventies* en het *overheidsbeleid* (op korte en lange termijn) waarvan dit ene instrument eventueel deel gaat uitmaken. Graag vraag ik uw aandacht voor het bredere kader waarin we het beleid, gebruik, de experimenteerstatus, de monitoring en het (Europese) rechtskader moeten beoordelen.

1. **Beleid**: Deze discussie rond de corona-app gaat nu alleen om een technische oplossing voor een medisch probleem met privacy, veiligheid en gebruikersgemak als belangrijkste aandachtspunten. De bredere vraag is echter op welke manier we in onze samenleving om willen gaan met het verzamelen en verwerken van informatie die nodig is om deze (en misschien volgende) gezondheidscrisis te bestrijden. Een app kan daar wellicht onder strikte condities een rol in spelen, maar zonder uitgekiend beleid valt die in los zand. Als dit een instrument wordt in de dokterstas van de GGD, heeft de GGD dan voldoende middelen, expertise en bevoegdheden om haar werk, waarvan de app een onderdeel kan worden, uit te voeren? We moeten het daarom ook hebben over **een *preventie-infrastructuur* die voor de langere termijn gaat werken** en waarin verschillende opties in samenhang worden afgewogen, waaronder technologische oplossingen.

2. **Gebruik:** in de discussie tot nu toe stond vooral gebruikersgemak en -ervaring centraal: is de app handig in het gebruik (bv voor ouderen)? En hoe bereik je dat een meerderheid van de mensen de app gaat gebruiken? Dit is vooral een toegepaste vraag over specifieke apps op de korte termijn. Gebruikersparticipatie draait echter niet alleen om het creëren van draagvlak waardoor participatiegraad hoger wordt. Draagvlak hangt samen met het vertrouwen van burgers in de effectiviteit, betrouwbaarheid en zinvolheid van de toegepaste technologie waarop zij hun gedrag afstemmen. Om dat te bereiken moet vooral duidelijk zijn **hoe en waarom een technische oplossing deel uitmaakt van een totaalpakket aan maatregelen,** bijvoorbeeld ten aanzien van testen en quarantainevoorschriften.

3. **Experimenteerstatus:** in deze fase van het bestrijden van de pandemie grijpen we naar middelen die uitzonderlijk en dus experimenteel zijn**.** Dat betekent dat er moet worden gekeken naar de vraag welke lessen dit experiment moet opleveren, hoe we dit

experiment in een aantal fasen gaan bijsturen, wie er betrokken wordt bij de leerprocessen en hoe we omgaan met tegenstrijdige waarden. We kunnen er niet van uit gaan dat het gebruik van welke app dan ook direct goed verloopt. Daarom moet het **experimenteren ingebed worden in een *democratische en ethische assessment*** zodat de juiste lessen kunnen worden getrokken.

4. **Monitoring:** een app is geen losstaande technische oplossing die door een bedrijf of consortium 'klaar' gemaakt wordt voor de samenleving. Een technische oplossing wekt pas vertrouwen als die deel uitmaakt van een breder systeem van institutionele *checks and balances*, waarin burgers en overheden een duidelijke rol spelen. Dat kan bijvoorbeeld betekenen dat de GGD kijkt naar vormen van inspraak, klachtenprocedures, periodieke review, bijvoorbeeld door een soort 'burgerraad'. We kunnen goed gebruik maken van principes van participatief bestuur om die aanpak democratisch te legitimeren en het proces kritisch te blijven volgen. Immers, er kan een groot verschil zijn tussen de manier waarop beleid is bedoeld en de wijze waarop het wordt uitgevoerd. Immers, bij grote beleidsschandalen van de laatste jaren – denk aan de Belastingdienst, SyRI – ging het om problemen in de uitvoering. Behalve mee te kijken naar de condities voor ontwikkeling van de app, kunnen we experts en burgers ook laten meekijken naar de wijze waarop de uitvoering vorm krijgt. **Het is van groot belang om deze uitvoering te blijven monitoren en hierin voldoende *checks and balances* aan te brengen**.

5. **Rechtskader:** De ontwikkeling van een corona-app kan niet los gezien worden van het bredere rechtskader en de handhaving daarvan. Uiteindelijk gaat het erom dat welke app dan ook – als vergaand en ingrijpend instrument – goed is ingebed in de controlemechanismen van de democratische rechtstaat. Die discussie gaat over de balans tussen grondrechten en gezondheid en over de proportionaliteit van bepaalde maatregelen. Die discussie gaat ook over macht. Bij wie leggen we bijvoorbeeld de macht over de sturing van gebruikersgedrag: bij de overheid, de GGD of bij de (al dan niet commerciële) ontwikkelaars van deze apps? Wat gebeurt er als er een andere/betere app op de markt komt die in andere landen veel meer gebruikt wordt? En hoe houden we toezicht over de macht van grote app-distributeurs (bv. Google, Apple)? De **overheid zal met alle partijen afspraken moeten kunnen maken over transparantie en publieke waarden**. Dat rechtskader is niet alleen Nederlands maar vooral ook Europees. Afgelopen week heeft de EU een aantal voorwaarden opgesteld waaraan digitale oplossingen zoals een app moeten voldoen wat betreft de ontwikkeling, implementatie en toetsing. Een strikt Nederlandse app is geen remedie tegen een pandemie. Voor deze samenwerking is **uiteraard afstemming binnen de Europese Commissie nodig**.

Kortom, wij hopen dat deze discussie niet blijft steken bij een eenmalige vlootschouw van corona-apps—een dubbel experiment in deze uitzonderlijke tijden. Dat de overheid de inzichten van experts en niet-experts betrekken bij het zoeken naar een oplossing, is prijzenswaardig. Hopelijk krijgt dit eenmalige experiment een vervolg in de vorm van een zorgvuldig, goed geïnformeerd democratisch afwegingsproces als basis voor effectief en verantwoord overheidsbeleid. Een goed werkende thermometer in de dokterstas van de GGD heeft geen nut als de regering niet zorgt voor een goed werkende GGD in een goed functionerende rechtsstaat. Het is aan het parlement om beide experimenten bij te sturen.

Inhoudsopgave

Technische kanttekeningen bij een contact-tracing app

Maarten van Steen
Hoogleraar Grootschalige Gedistribueerde Computersystemen
Wetenschappelijk Directeur Digital Society Institute, Universiteit Twente

In dit position paper stel ik dat er meer geprioriteerd moet worden op een aantal hardnekkige en wellicht onoplosbare technische problemen die eerst opgelost moeten worden willen we smartphones inzetten voor nabijheidsmetingen. In het bijzonder stel ik dat nu vooral gekeken moet worden naar de inzet van smartphones voor het detecteren van het feit of een besmet persoon in iemands buurt is geweest. Problemen rondom privacy lijken oplosbaar, maar verdienen nu wellicht meer specifieke aandacht.

Er is in de aanloop naar mogelijke apps die helpen bij het bestrijden van de verspreiding van het COVID-19 virus al veel gezegd en geroepen. Een probleem hierbij is dat de inzet van een dergelijke app veel verschillende kennisgebieden bestrijkt: sociale wetenschappen, recht, psychologie, epidemiologie, beveiliging, informatietechnologie, om maar eens een aantal te noemen. Deze multidisciplinariteit bemoeilijkt doorgaans besluitvorming: er zijn gewoon veel aspecten waar rekening mee gehouden dient te worden.

Het helpt hierbij om te prioriteren op die deelproblemen die niet evident oplosbaar lijken te zijn, maar waarbij die oplossing wel onvoorwaardelijk nodig is voor de effectieve inzet van een app. Daarbij is het essentieel dat het specifieke probleem, hoe ingewikkeld het ook lijkt, klip en klaar uitgelegd wordt, als ook een eventuele oplossing, en wel zo dat ook niet-deskundigen op het specifieke probleemgebied, maar die uiteindelijk wel besluiten moeten nemen, inderdaad goed geïnformeerd zijn.

Informatietechnologische toepassingen, en vooral de apps op smartphones, zijn tegenwoordig dikwijls verbluffend eenvoudig te bedienen en bieden bovendien ook nog eens een enorme krachtige functionaliteit. Zo ook verschillende beoogde COVID-19 apps. Echter, juist voor dergelijke apps waar veel verschillende meningen over zijn is het essentieel te begrijpen wat er zich onder de motorkap bevindt.

Er spelen hierbij minstens drie aspecten:

1. De inzet van een smartphone als meetinstrument.
2. Het technische protocol voor detectie, registratie en disseminatie van informatie over besmettingen.
3. De implementatie van dat protocol in de vorm van een app.

De smartphone als meetinstrument

Voor contact tracing is het belangrijk dat we kunnen vaststellen of iemand gedurende enige tijd in de fysieke nabijheid is geweest van een geïnfecteerde persoon. Doordat veel mensen een smartphone bij zich dragen, is het idee om deze in te zetten als instrument om te bepalen of mensen bij elkaar in de buurt zijn geweest. Om technische, maar ook niet-technische redenen vallen inmiddels technieken af die gebaseerd zijn op locatiebepaling. Er wordt daarom nu door veel ontwikkelaars gekeken naar directe detectie door middel van Bluetooth. De essentie is dat smartphones met Bluetooth met een bepaalde regelmaat signalen uitzenden, maar ook dat die signalen een beperkte reikwijdte hebben van enkele tientallen meters. Het ontvangen van een signaal betekent dat er een smartphone in de buurt is. De sterkte van het ontvangen signaal kan door de ontvanger gemeten worden en zou indicatief kunnen zijn voor de feitelijke afstand.

Het probleem is dat het uiterst lastig is, wellicht zelfs praktisch onmogelijk, om met een gewenste nauwkeurigheid te bepalen hoe dicht een smartphone in de buurt is. Bluetooth signalen zijn, net zoals alle radiosignalen, (dikwijls zeer) gevoelig voor omgevingsinvloeden. Daarom maakt het uit of het bijvoorbeeld regent, of waar een smartphone op het lichaam gedragen wordt. Ook maakt het uit of men op een open plein loopt, zich in een kamer bevindt, op een gang loopt, etc. De kwaliteit van de gebruikte antennes, en die per telefoon kunnen verschillen, zijn ook van invloed op de kwaliteit van het Bluetooth signaal. Signalen correct interpreteren zal nauwkeuriger kunnen plaatsvinden op basis van eerdere calibratiemetingen, metingen die bovendien omgevingsinvloeden zullen moeten meenemen. Vervolgens zal een smartphone ook nog automatisch moeten kunnen detecteren in welke soort omgeving het zich bevindt. Daarbij komt dat het feitelijk onmogelijk is om op basis van een ontvangen signaal vast te stellen of een detectie zelfs relevant is: Bluetooth signalen gaan door muren en andere COVID-19 beschermende barrières.

Kortom, er is voldoende reden om te twijfelen aan de effectieve inzet van een smartphone als instrument om te meten of iemand binnen het gebied van een geïnfecteerde persoon is geweest waar overdracht van het virus zou kunnen plaatsvinden. Wordt een smartphone toch ingezet, dan dient rekening gehouden met enerzijds veel onterechte detecties (omdat de ontvanger buiten het overdrachtsgebied was), maar ook veel gemiste detecties (binnen het overdrachtsgebied, maar het signaal is niet overgekomen). Het is vooralsnog onduidelijk hoe groot deze onnauwkeurigheid is, of die nauwkeurigheid op een gewenst niveau te krijgen is, maar ook in hoeverre die nauwkeurigheid van belang is.

Ik acht momenteel dit probleem een serieus obstakel voor de effectieve inzet van een COVID-19 app voor nabijheidsmetingen. Het probleem zal eerst op bevredigende wijze opgelost moeten worden.

Het technische protocol

Er is al veel gezegd over de eisen waaraan een technisch protocol voor detectie, registratie en disseminatie van besmettingen moet voldoen.[1] Privacy en beveiliging staan hierbij voorop. Er lijkt hiervoor een oplossing te zijn. De kern ervan kan als volgt samengevat worden:

- Een COVID-19 app genereert een nieuwe en voor de smartphone wereldwijde unieke ID waaruit op geen enkele wijze persoonsgevoelige informatie valt te destilleren.
- De COVID-19 app zendt via Bluetooth een ID uit, en ontvangt de IDs van andere apparaten. Het slaat lokaal, op de telefoon, de ontvangen IDs op.
- Wanneer iemand besmet is, meldt hij/zij dit via de app, en de app geeft de ID door aan de centrale server. De melding gaat samen met een autorisatiecode (zoals de wellicht nog bekende TAN codes bij bankverkeer) van een BIG-geregistreerde zorgverlener voor validatie dat de persoon inderdaad positief getest is.
- De app gaat ook regelmatig (zeg 1 of 2 keer per dag) naar de server en haalt alle IDs op waarvan men weet dat die horen bij geïnfecteerde personen, om vervolgens lokaal deze lijst te vergelijken met ontvangen IDs om vast te stellen of er een besmetting plaatsgevonden zou kunnen hebben.

Dit is een korte samenvatting van het zogeheten Decentralized Privacy-Preserving Proximty Tracing protocol (DP3T).[2] Ik laat belangrijke details weg die nodig zijn om de privacy en beveiliging beter te borgen dan hierboven geschetst. Echter, het belangrijke is dat het protocol uit te leggen is aan niet deskundigen (de ontwerpers hebben zelfs een waarheidsgetrouwe strip opgetekend), maar ook dat aannames expliciet gemaakt zijn, zoveel mogelijk ontwerpkeuzes toegelicht zijn, en ook zoveel mogelijk bekeken is waar eventuele zwakheden zitten die extra bescherming vereisen. Kortom: het protocol is openbaar en vooral transparant. Het kan dus door partijen met verschillende achtergronden op voorhand geïnspecteerd worden.

Vanuit mijn eigen expertise (met een focus op grootschalige gedistribueerde en dikwijls draadloze computersystemen) stel ik vast dat we hier met een schaalbaar ontwerp te maken hebben waarin minimale informatie op centrale plekken ligt. Vanuit diezelfde expertise heb ik het sterke vermoeden dat het protocol privacy volledig bewaakt en bovendien veilig is, maar weet dat er andere experts zijn (met een focus op technische privacy en beveiliging) met jarenlange training en onderzoek die hier een scherper oog voor hebben dan ikzelf.

Daarmee concludeer ik (voorlopig) dat een technisch protocol voor detectie, registratie en disseminatie van informatie over besmettingen niet in de weg staat voor de effectieve inzet van een COVID-19 app voor nabijheidsmetingen. Echter, het is essentieel dat juist technische privacy- en beveiligingsexperts het protocol inspecteren.

De feitelijke implementatie

Een protocol is een specificatie, uiteindelijk komt het aan op de realisatie daarvan in de vorm van een app. Laten we uitgaan van het feit dat het DP3T protocol aan de gewenste eisen voldoet. Wie garandeert mij dat een app ook daadwerkelijk het DP3T protocol geïmplementeerd heeft? Of dat die implementatie correct is, dat er geen extra "features" bedoeld of onbedoeld in de implementatie beland zijn, en vooral, dat de implementatie ook beveiligd is? Welke app we ook zullen inzetten, de broncode zal geïnspecteerd moeten kunnen worden door onafhankelijke specialisten. Zonder de transparantie zoals bij DP3T zullen gebruikers moeten vertrouwen op de ontwikkelaars. Voor COVID-19 apps acht ik dit laatste volstrekt onwenselijk.

De keuze om de broncode van een app openbaar te maken is terecht en essentieel. Van die keuze mag niet afgeweken worden. Wel is het van belang dat ook hier experts daadwerkelijk aan het werk gezet worden om die broncode te inspecteren en te valideren.

Credits

Dit paper was niet tot stand gekomen zonder de inzet van veel collega's, maar in het bijzonder die van Prof.dr.ir. Bart Nieuwenhuis, hoogleraar Telematica Services, die de drijvende kracht is bij de Universiteit Twente als het gaat om corona contact tracing. Prof.dr.ing. Paul Havinga, expert o.a. op het gebied van draadloze communicatie en sensornetwerken, heeft bijgedragen aan de articulatie van een aantal belangrijke technische aspecten, vooral met betrekking tot de inzet van smartphones als meetinstrument.

---

[1] Zie bijvoorbeeld het EU rapport "Mobile applications to support contact tracing in the EU's fight against COVID-19", dd. 15 april 2020.

[2] Zie https://github.com/DP-3T/.

Tweede Kamer
DER STATEN-GENERAAL

Blok 2

CV’s en Position Papers

Rondetafelgesprek Corona-app woensdag 22 april 8.30 – 12.30 uur

Blok 2

Niels Chavannes – hoofd van de sectie Wetenschappelijk Onderzoek Eerstelijnsgeneeskunde, Initiatiefnemer National eHealth Living Lab, LUMC

- Hoofd van de sectie Wetenschappelijk Onderzoek Eerstelijnsgeneeskunde
- Initiatiefnemer National eHealth Living Lab, LUMC. Het in 2018 geopende eHealth Living Lab is een patiëntgericht multidisciplinair Open Science0instituut om eHealth-initiatieven op een evidence-based manier op te schalen, m.b.v. innovatieve eHealth-methodologie en het stimuleren van publiek-private samenwerking.
- Adviseur nationaal actieprogramma chronische longziekten (Long alliantie Nederland)
- Vicevoorzitter CAHAG - Nederlands Huisartsengenootschap (NHG)

M.J. de Vries – Hoogleraar technische natuurwetenschappen TU Delft, expertise ethiek/filosofie van de technologie

- Hoogleraar christelijke filosofie van de techniek, TU Delft.
- Hoogleraar Science Education, TU Delft
- Affiliate hoogleraar filosofie en pedagogie van technologie en technisch onderwijs, KTH Royal Institute of Technology, Stockholm-Zweden.

Rogier Creemers – Universitair docent Modern China Studies verbonden aan de Universiteit van Leiden.

- Rogier Creemers heeft een Master in China Studies en Internationale Betrekkingen en een doctoraat in rechten. Zijn onderzoek bestudeert het binnenlandse technologiebeleid van China en de deelname van China aan wereldwijde cyberaangelegenheden. Zijn werk is onder meer gepubliceerd in The China Journal en het Journal of Contemporary China.
- Rogier is een van de oprichters van DigiChina, een project dat wordt uitgevoerd in samenwerking met New America, en levert regelmatig bijdragen aan de media.

Onderwerp: track & trace app COVID-19

Doel track & trace app: het verkorten van de tijd tussen isolatie case en de quarantaine van zijn/haar contactpersonen door het sneller opsporen en gericht informeren van contacten en bijdragen aan het traceren van minstens 60% van alle relevante contactpersonen van een bevestigde case.

Basis kwaliteitsprincipes ontwikkeling & implementatie track & trace apps
De volgende basis kwaliteitsprincipes zijn naar voren gekomen in discussies:

Aansluiting op de eindgebruiker

- Empowerment van de burger: de app helpt de burger sneller te achterhalen of hij/zij contact heeft gehad met iemand met COVID-19. In het geval dat de burger zelf hoort besmet te zijn, helpt de app de burger om zo snel mogelijk zijn/haar contacten te waarschuwen.
- Aansluiting op de burger met lage digitale vaardigheden/ de laaggeletterde burger: hier dient rekening mee gehouden te worden in het design.

Wetenschappelijke validatie

- Technologisch: in hoeverre zijn de afstandsmetingen met Bluetooth signaal betrouwbaar & precies?
- Hoe gaan we het effect op de COVID-19 besmettingsgraad precies meten, in een pilot en gedurende landelijke uitrol?

Implementatie & opschaling

- Aansluiting op de workflow van de GGD & RIVM, en interactie met de reguliere contactopsporing van de GGD
- IT infrastructuur moet schaalbaar zijn

Privacy/ juridische kaders

- Privacy/ data veiligheid: decentraal model m.b.t. data opslag, dus níét op een centrale server maar alleen op toestellen zelf wordt opgeslagen of er contact is geweest met een besmette burger.

Inventarisatie kwaliteit track & trace app
Zoals al uit bovenstaande basis kwaliteitsprincipes blijkt, is kwaliteit vereist op veel verschillende fronten. Vóór landelijke uitrol van de app dient dan ook een complete assessment van kwaliteit gedaan te worden. NeLL werkt in de kern mee aan de totstandkoming van de internationale ISO-norm voor e-health. Met deze norm – of een versie hiervan die is toegespitst op deze specifieke situatie – kunnen we een zo objectief en compleet mogelijke assessment maken van kwaliteit van de app als geheel. In aanvulling op de algemene ISO-norm kan gebruik gemaakt worden van de recent gepubliceerde EU Toolbox voor contact tracing apps (https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf).

Hoe komen we erachter of de app werkt?

Allereerst door een pilot met juist gedefinieerde uitkomstmaten:

1. Werking app i.h.k.v. infectieziektenbestrijding: hoe komen we erachter dat deze targets worden behaald door het nieuwe systeem/ app? Vaststellen van basale epidemiologische karakteristieken zoals sensitiviteit & specificiteit is een belangrijke stap.

2. Adoptie:
    - Dekkingsgraad: app gedownload bij welk % van doelgroep
    - Gebruik: staat de app (specifiek het Bluetooth signaal) ‘aan’ op de juiste momenten/?

3. Tijdswinst/ vergroting bereik GGD personeel
    - Tijdswinst m.b.t. informatievoorziening
    - Vergroting bereik contactonderzoek: burgers die géén bekenden zijn van een positief geteste burger worden momenteel niet bereikt door de GGD

Inhoudsopgave

Position paper voor de Vaste commissie voor Volksgezondheid, Welzijn en Sport van de Tweede Kamer der Staten-Generaal, t.b.v. de hoorzitting m.b.t. de zogenaamde Corona-app (22-04-2020)

Marc J. de Vries, Technische Universiteit Delft

Onderstaande overwegingen zijn vooral gebaseerd op inzichten uit de filosofie van de techniek en niet op technisch-inhoudelijke expertise van apps.

1. Gewicht van privacy in de afwegingen

De huidige overwegingen spitsen zich vooral toe op privacy-gerelateerde vragen. De aandacht voor privacy is terecht omdat dit een waarde is die bescherming verdient. Tegelijkertijd is een zekere nuancering op zijn plaats. In de afweging tussen privacy en een persoonlijk belang (zoals bij kopen via internet of reclameacties waarbij persoonsgegevens ingevoerd moeten worden) geven velen hun gegevens prijs ter wille van persoonlijke belangen. Gaat de afweging echter tussen privacy en een maatschappelijk belang (zoals volksgezondheid of bescherming tegen terrorisme), dan is privacy plotseling veel belangrijker. De overheid mag op dit punt van de bevolking vragen om ook maatschappelijk belang zwaar te laten wegen, en niet alleen persoonlijk belang.

2. Vertrouwen in technologie

Succesvolle inzet van technologie staat of valt met het vertrouwen van (onder meer) de gebruikers. Dat geldt zeker voor ICT-applicaties. Een toepassing waarvan het gedrag voor de gebruiker grillig en onnavolgbaar is (zoals in China waar de kleurcode die de gezondheidstoestand aangeeft, soms op voor de gebruiker onverklaarbare wijze kan veranderen) zal gebruik sterk ontmoedigen. De werking van de app zal dus in hoge mate consistent en stabiel moeten zijn. Normaal vraagt dit een lange ontwikkeltijd. Overhaaste implementatie zal zich later wreken in wantrouwen van de gebruikers en een falende toepassing.

3. Verschuiving van verantwoordelijkheid van mens naar technologie

Het beleid tot nu toe heeft vooral ingezet op de eigen verantwoordelijkheid van de bevolking. De inzet van technologie is nog nauwelijks aan de orde geweest. Dit is een goede zaak. Een technologie kan geen morele verantwoordelijkheid dragen, laat staan juridisch aansprakelijk gehouden worden. Het gedrag van de bevolking tot nu toe leeft laten zien dat het vertrouwen in het eigen verantwoordelijkheidsbesef van de bevolking terecht was. Het zou inconsistent en onverstandig zijn om zonder duidelijke aanleiding deze eigen verantwoordelijkheid te ontzeggen door de beslissingsbevoegdheid aan de technologie over te laten. Inzet van een app zal dus primair gericht moeten zijn op de ondersteuning van het beoefenen van de eigen verantwoordelijkheid van de burgers. Wanneer de bevolking ook maar het gevoel krijgt dat ze niet meer door de overheid vertrouwd wordt, dan zal het eigen verantwoordelijkheidsbesef snel weg-eroderen niet gemakkelijk terug te winnen zijn. Verplichting van het gebruik van de app (op dit moment nog niet aan de orde, maar mogelijk een latere overweging) zal onverantwoordelijk gedrag of het verhullen van gedrag stimuleren omdat de burger meent dat hij niet vertrouwd wordt.

3. Beperkingen van data

De grootschalige inzet van een app is een zeer ingrijpend proces, zoals terecht door de 70 deskundigen is aangegeven. De inzet van de technologie moet dus gerechtvaardigd worden door een hoge mate van

effectiviteit en efficiëntie. Data zijn echter altijd een reductie van de werkelijkheid. Wat in data uitgedrukt kan worden is altijd beperkt. De afstand van 1,5 meter is een reductie van een veelheid aan situaties (wel of geen glas ertussen, wel of geen geventileerde ruimte, enzovoorts). Hoe beperkter de data vanwege de privacy-gevoeligheid, hoe geringer de informatieve waarde en de effectiviteit van de app. Bovendien zit er een wetenschappelijke onzekerheid in de data (er kan niet 100% nauwkeurig worden vastgesteld wanneer iemand covid heeft, inzichten in de overdrachtsmechanismen veranderen nog steeds, enzovoorts). Ten aanzien van de wetenschappelijke claims sluit ik graag aan bij de oproep van de heer Van der Staaij in een eerder debat, waarin hij opriep om ook naar de stem van het gezonde verstand te gebruiken, naast die van de wetenschappelijke experts.

4. Langetermijn impact (Onomkeerbaarheid van technologische ontwikkelingen)

In bepaalde opzichten lijkt de Corona app op bestaande toepassingen maar ze is fundamenteel anders. Velen hebben op hun smartphone apps die hen informeren over de omgeving (dichtstbijzijnde supermarkt of boekhandel). De inkomende informatie van de omgeving betreft echter geen persoonsgegevens. Dat zal bij de Corona app bijna onvermijdelijk wel het geval zijn (als de informatie al niet direct persoonlijk is, zal er in veel gevallen persoonlijke informatie uit afgeleid kunnen worden, of door de gebruiker zelf of door anderen). Dit is mede vanwege de grootschaligheid een ingrijpende vernieuwing ten opzichte van de huidige apps. Elke technologische vernieuwing is in principe een weg met eenrichtingsverkeer. De app kan na de crisis verwijderd worden, maar de impact op de bevolking niet. De mogelijkheid van andere toepassingen zal snel worden onderzocht, niet in het minst voor commerciële doeleinden. De vraag moet gesteld worden of dit lange-termijn effect wordt gerechtvaardigd door de korte-termijn opbrengsten van de Corona app. Het is buitengewoon moeilijk om in dit vroege stadium in te schatten op welke wijze het gebruik van dit type toepassing zich gaat voortzetten. Zoals bij elke technologie kan het twee kanten op, een goede en een onwenselijke. Het is sowieso de vraag hoe we als gebruikers van media uit deze crisis tevoorschijn gaan komen. Voor een aantal mensen zullen de huidige ervaringen de waardering voor fysieke ontmoetingen terugbrengen na een periode waarin zij steeds meer door technologie gemedieerde contacten gekregen hebben. Voor anderen zal deze beweging naar meer indirecte contacten zich versterken omdat de voordelen ervan sterker dan voorheen beleefd zijn. De problemen van een gebrek aan fysieke contacten en activiteiten zijn al op vele wijzen aangetoond. Ook hier is een weg terug nauwelijks realistisch.

5. Functie van de app

Bovenstaande overwegingen hangen sterk samen met de functie van de app. Hier lijkt geen eenduidigheid te zijn bij de gekozen 7 apps, ondanks de richtlijnen. Het registreren van de aanwezigheid van anderen die al besmet zijn, lijkt een ongewenste functie. Daarvan zou immers het signaal uitgaan dat het acceptabel is dat covid-19 besmette burgers zich in de openbaarheid begeven. Vanwege de beperktheid van de data (zie boven) zou deze toepassing bovendien een vals gevoel van veiligheid stimuleren. Gaat hat alleen om de herkenning achteraf dat er contact geweest is met iemand die op dat moment nog niet als Corona-besmette geregistreerd stond, dan is de vraag welke gegevens over die ‘ontmoeting’ opgeslagen moeten worden (afgezien van de vraag of dat centraal of lokaal gebeurt). Is alleen het gegeven ‘dat’ er een ontmoeting was voldoende om het doel van bronondezoek te dienen? Als de locatie van de ontmoeting voor dit doel noodzakelijk is om te weten, doet zich al het probleem voor dat de gebruiker mogelijk op een plaats was waarvan z/hij liever niet heeft dat anderen dit te weten komen. Hetzelfde kan gelden voor het tijdstip van de ontmoeting.

LEIDEN ASIA CENTRE
Partners in Research and Knowledge

How Asia Confronts COVID-19 through Technology

The LeidenAsiaCentre | April 21, 2020

Introduction

With societies around the world tackling the Coronavirus pandemic, the role of digital technology has come into focus as a means of augmenting efforts to manage disease and its impacts. What can apps, big data, and digital analytics contribute to such efforts, and what risks do they pose?

Asia provides important lessons. Not only have societies in the region long been at the forefront of technological development, but they have also proactively adopted digital solutions as they confront COVID-19. Importantly, Asia has a history of managing highly contagious diseases, and outbreaks like SARS in 2002 or H1N1 in 2009 have provided experiences in risk management and health provision that now powerfully inform both digital and non-digital responses to the current pandemic. The result is a diverse range of different approaches that can teach us much about the advantages and disadvantages of designing tech solutions to fight pandemics.

The Leiden Asia Centre (LAC) has asked social science and area studies researchers knowledgeable about tech developments in Asia to survey current practices and results in five different settings: mainland China, Japan, Singapore, South Korea, and Taiwan. This preliminary report makes the most important results available to policymakers in a short, accessible format.*

In what follows, we provide an overview of app-based approaches in each setting. Our study shows how technology and its uses are never neutral. They instead heavily depend on the decisions that stakeholders make in specific contexts. The following are our five main lessons from the Asian cases:

LEIDEN ASIA CENTRE
Partners in Research and Knowledge

1. Tech is embedded in society: apps and other digital solutions are only ever as effective as the measures 'on the ground'. They do not exist in a vacuum; instead, they flank, augment, and amplify policy decisions in ways that are highly contingent on broader societal efforts. Across Asia, digital solutions interact with generally high-quality healthcare systems, strong border controls, strict social distancing measures, aggressive testing and re-testing, pro-active tracking, and a widespread use of masks and disinfectants throughout society. Any digital measures have to be understood in those contexts.

2. Tech is political: digital tools are designed by someone, for someone, and for specific purposes. They reflect the experiences and assumptions of designers and of the people commissioning such apps. This means that they can contain biases, sometimes invisibly so.

3. Tech relies on data: digital tools are only ever as good as the data they use. Garbage in, garbage out. If data is incomplete, or compromised, or unreliable, then so is the app. The result can be highly detrimental, leading to a false sense of security, policies that target the wrong issues, or discrimination of vulnerable groups.

4. Tech solutions require choices: governing a pandemic requires trade-offs, and this is also true for digital responses. In the case of apps, a prominent trade-off is between efficiency and privacy/freedom. Societal and political actors who wish to enhance their governance through apps will have to make choices on how to balance this trade-off; there is no single best-practice solution to this dilemma.

5. Tech is 'sticky': technological solutions are powerful because they can quickly, and seemingly comprehensively, shape behaviours, establish new habits, and form specific practices. They become institutions, and this means they can become 'entrenched' and suffer 'mission creep', making it hard to phase them out once they've fulfilled their purpose.

* The work presented here is based on a first round of desk-research, and it omits detailed references in the interest of brevity. More detailed and fully-sourced studies will follow: in late April, the LAC will publish the full regional surveys on its website; at a later stage, it will publish an in-depth report that will incorporate detailed policy analyses. All of these outputs are written in English, reflecting the international backgrounds of our contributors.

LEIDEN ASIA CENTRE
Partners in Research and Knowledge

Japan

Failing to adjust to new developments in the pandemic, a lack of information and impediments in structures of governance have undermined Japanese efforts to contain the spread of the virus, despite the implementation of several risk management strategies. The government has employed public surveys for data collection, using an existing and widely used application, LINE, in order to get a grasp on the magnitude of the spread. However, the Japanese case also highlights how apps are only effective if they are part of a concerted general effort to counter the disease. The current failure to contain the virus will have significant effects on healthcare, public trust, and the national economy.

To understand the limitations of Japan's app usage to combat COVID-19, it is important to highlight several impacts that Japan's current trajectory in crisis management has had more generally:

- The decentralised nature of governance and constitutional limitations have delayed the national strategy for containment.
- A failure to respond adequately to this pandemic continues to exacerbate problems with an already collapsing health care infrastructure.
- The perceived failures of the current administration have heavily eroded public trust in the government's capability to handle future pandemics.
- The failure to adapt is lengthening the negative impact on the national economy.

The main objective of the first stage of the national COVID-19 response was to contain the spread via a cluster-based approach based on identifying patients and any persons with whom this patient has come into contact. However, as of 4 April, over 40 per cent of cases could no longer be traced. The opaque origin of a large number of new cases has led to a clear switch to risk mitigation strategies in Japan's national response.

In accordance with the revised Act on Special Measures for Pandemic Influenza and New Infectious Diseases Preparedness and Response, a state of emergency was declared for large parts of the country from 7 April to 6 May. The declaration allows prefectural governors to close public facilities and request businesses where people gather to temporarily suspend operations. The government has also requested business operators to switch to teleworking unless they provide essential services and to restrict access to facilities where people gather to reduce personal contact. An initial lack of financial support for those affected has impeded grassroots cooperation, and constitutional restrictions form an impediment to limiting movement in the form of a lockdown. Moreover, there is no national control mechanism in place and the

government is forced to rely on prefectural governors. Accordingly, the response among different regions has been varied.

The government is focusing on creating awareness of the 'three C's': avoid 1) closed spaces, 2) crowded places, and 3) close-contact settings; and of the need for hand washing and avoiding face contact. In addition, the incumbent administration will provide two washable cotton masks to each household in a bid to reduce risk of spreading. In order to promote closures and to limit the economic impact, 100,000 yen (860 EUR) will be provided to each resident. However, due to initial delays in establishing policy for financial compensation, businesses have stayed open for extended periods despite the growing infection rates, and public support has been diminishing steadily in the face of a flailing government.

In order to gather information on the spread of the virus and the level of public cooperation, the Ministry of Health, Labour and Welfare (MHLW) has used LINE, a text-based social media application similar to WhatsApp, to send out nation-wide surveys. With an 87 per cent smartphone user rate and an 82.3 per cent total penetration rate in Japan, LINE is the most widely used online application in the country. 24.5 million Japanese residents responded to the initial survey, a total of 19.05 per cent of the population. Although using a private company to collect personal information requires flexibility in the processing of data, LINE's high user rate has the advantage of allowing the survey to reach a wide audience. The survey does not contain information about the use of the provided information other than that the data is collected for the MHLW. The results of the initial survey were published online, with the main conclusion that current efforts need to be strengthened and personal contact needs to decrease by at least 70-80 per cent.

Data on individual patients is collected through medical institutions and local governments. This data is sorted differently on the MHLW and individual prefectures' websites, with significant variation in the information that is made public. The MHLW's national data includes, a concise timeline of symptoms and test result, age range (in 10-year segments), sex, nationality, and prefecture and city. In contrast, in Osaka Prefecture, case information includes case number, age range (in 10-year segments), sex, date of test, prefecture and city, household structure, occupation, symptoms and an indication of severity, and current working situation. Identifiable personal information, such as precise location data and address, are excluded in all data sets. All official information is published in the form of total numbers or lists of new cases, available as links to pdf files on official websites. This is not user-friendly, and commercial enterprises, the media, and grassroots initiatives have had to fill the gap of providing accessible information to the public through open access media coverage and online maps of infection rates and high-risk areas.

LEIDEN ASIA CENTRE
Partners in Research and Knowledge

While the high response rate of the national survey suggests high levels of cooperation with the government's risk mitigation strategies, cooperation has nevertheless moved forward piecemeal. Many companies still require employees to come to the office as remote working has failed to take hold at levels necessary for containment. In addition, the two-mask policy has been highly criticised as unscientific, ineffective, and unnecessarily expensive. There are increasing reports of refusals to test possible infections, a collapsing health care infrastructure, shortages of masks and protective gear, and inaccessible phone numbers for medical consults. Because of the state's failure to adequately respond to the pandemic, containing the spread will have to rely on the population's willingness to either endure longer shutdowns or endure high infection rates. Travel restrictions will have to stay in place, also affecting Japan's major tourism industries. In either case, public trust has eroded, economic consequences are severe, and the health care sector will remain critically burdened for an indefinite amount of time.

Mainland China

In February 2020, the Chinese government started working together with Chinese technological giants Alibaba and Tencent to develop apps that could be used in the fight against the COVID-19 epidemic. After introducing initial apps, collectively referred to as "health code" apps, in early February, many provincial governments followed suit and unveiled their own software. "Health code" applications work independently or as mini programs embedded into other popular apps (WeChat, Alipay).

New users are required to answer questions pertaining to their recent travel history, body temperature, contact with infected persons, as well as personal information such as name, ID number, and phone number. Some apps (Beijing) require an ID scans, while others (Shanghai) require photos.

The user is assigned a QR code of varying colours: green (safe), yellow (requires 7-day isolation), or red (requires 14-day isolation). Whenever an app user enters publicly-used establishments, they go through a checkpoint, first scanning their QR code to prove their identity and their status as "safe", then going through temperature screening. In case of fever, the QR code changes colour to either yellow or red. "Health code" apps use governmental data, location-based information, travel routes of infected people and other means to assess whether a person was in contact with the disease. The QR

code changes colour to yellow or red depending on those factors. However, provincial governments and companies involved in creating those apps are not transparent and do not disclose which data is used specifically to assess the risk, or how personal data are gathered, stored, or used.

There is no single unified system across China yet, although there are plans to unify scattered and incompatible programs used by different cities and provinces within one application. Lack of a homogenous system, and of inter-app QR code recognition, impedes travel and is one of the main points of criticism. Unreliability, lack of information, lack of case-to-case solutions, and possible data breaches are other issues. Nevertheless, overall, the introduction of "health code" apps was welcome by the citizens. The Chinese government responded to some domestic criticism, apparently in a fashion that convinced the public at large.

The New York Times reported that Hangzhou's "health code" app contained a tracking program, allowing the user's location to be sent to law enforcement agencies. The Chinese government has not responded to those allegations. Law enforcement authorities were also involved in developing said app.

Drawing on previous experience when China expanded its surveillance system due to major events (2008 Beijing Olympics, Expo 2010), "health code" apps are likely to further escalate citizen control.

Singapore

The Singaporean government started taking precautionary measures in response to COVID-19 relatively early, at the beginning of January. The first case in Singapore was confirmed on January 23rd. On March 20th, the government launched TraceTogether, one of the first apps developed to counter COVID-19. On that day, Singapore had only 385 confirmed cases and zero deaths. The government had not implemented a lockdown, although social distancing measures were in place. Around that time, the approach of the Singaporean government was internationally regarded as exemplary. At the end of March, about 1 million (1 in 6) Singaporeans had downloaded the app.

In April, however, the situation in the city-state has worsened, and the government implemented a lockdown on April 7th after all. April 20th saw a record 22% (1,426 persons) increase in confirmed cases to a total of 8,014. Of the newly confirmed cases, 1,369 are permit holders residing in dormitories, a group which is currently more extensively tested than before. All confirmed cases in Singapore are hospitalised, as has been the approach from the start; 23 patients are in intensive care. In total, 59,737 persons had been tested by April 14th.

TraceTogether works as follows. Individuals can choose to download the app, after which they submit their mo-

bile phone number. The app then attaches a randomly generated ID to this number. Via Bluetooth, the app detects the random IDs of other nearby users and records these. If a user tests positively for COVID-19, he or she can choose to share the app's logs with the Ministry of Health, who will encrypt the IDs of other users found in these logs. This opens up the phone numbers of the infectee's 'close contacts' (users who have been within 2 meters for at least 30 minutes), who will receive a message that they are at high risk of infection, so that they can take steps to prevent further spreading. The app supplements manual contact tracing efforts and is not the only technology relied upon to fight COVID-19, as Singaporeans also receive government updates via WatsApp, while quarantined citizens are being monitored via video calls and have to share their phone locations with officials.

The Singaporean government has stated that it is committed to safeguarding the privacy of TraceTogether's users, emphasising that using the app is voluntary. Furthermore, the data, which is stored securely on non-public servers, only include the user's phone number and random ID. No personal or location data are collected. The data will be deleted if a user chooses to revoke consent. The app solely stores the random IDs of other users, which only the Ministry of Health can decrypt. The personal identity of users will not be revealed on the phones of other users. Third parties are unable to track the identity of a user, since the random ID is refreshed at regular intervals. Finally, the collected data is solely used for tracing persons who might be exposed to COVID-19. If contact tracing ends, users will be prompted to disable the functionality of the app. If they do so, the connection data will be lost. Users could be requested to reinstall or enable permissions in case of a future outbreak.

On April 10, about one in five Singaporeans had downloaded TraceTogether, while authorities stated that 75% of the population should use the app for it to be effective. What could explain this low number is that only 41% of Singaporeans feel comfortable sharing a positive COVID-19 test result via this technology. Furthermore, the app has received negative reviews because of technical issues. Apart from problems deriving from a low adoption rate, a director of TraceTogether has warned against over-reliance on contact tracing apps and stated that these should not replace manual contact tracing efforts, which can take into account more factors in the process and increase accuracy.

Governments and developers from around the world, including from the Netherlands, have shown interest in TraceTogether, partly because the app allows for relatively little privacy intrusion compared to other tracing apps, although privacy concerns still remain. The app's code has been made open source by the Singaporean government.

LEIDEN ASIA CENTRE
Partners in Research and Knowledge

South Korea

South Korea's success in containing the spread of COVID-19 is due to its integration of big data with user-friendly applications, enforcement of quarantine guidelines, and regulations in terms of data sharing capabilities. The country will be among the first in the world to have an efficient long-term strategy for containing pandemics. However, the use of personal information in tracking patients, and flexible regulations with regard to data-sharing is expected to permanently affect individual privacy.

The main points and impacts discussed below are as follows:

- User-friendly and mandatory app usage, combined with enforced quarantine guidelines and quick information-gathering mechanisms have enabled a comprehensive approach to containing COVID-19.
- Flexibility in policymaking and the utilization of remote medicare has effectively decreased the burden on healthcare infrastructure.
- National lockdowns and large-scale restrictions of movement are unnecessary with successful containment strategies, limiting the negative economic impact of the pandemic.
- There are permanent impacts on the use of personal information and privacy, and the possibility of future pandemics ensure that information gathering mechanisms will remain in place.

Several apps in both the public and private sectors have been developed in South Korea with the purpose of containing the spread of COVID-19, in addition to national and local emergency systems that notify anyone in a certain radius of possible risks.

The government of South Korea has developed two apps available for public use, the "self-diagnosis app" and the "self-quarantine safety app". The "self-diagnosis app" can be downloaded on arrival into South Korea and is required for both foreigners and Korean nationals to pass through immigration. Users have to enter their "passport information, nationality, name, address, and other necessary information for quarantine" into the system. Refusal to cooperate will result in a denial to enter the country.

Users are required to report possible symptoms once a day during the mandatory 14-day quarantine on arrival. The data is collected through the Korea Centers for Disease Control and Prevention (KCDC) and shared with local governments and public health clinics if the user shows symptoms for more than 2 consecutive days. Local governments are then prompted to have users tested. In order to assure users keep reporting, notifications are sent out whenever a user fails to do so. They are subsequently contacted via phone. If the user refuses to use the application, the police track down the user and enforce compliance.

The app is user-friendly and accessible, and reporting symptoms is done through four yes or no questions asking the user if they have 1) a cough, 2) a fever, 3) a sore throat, or 4) difficulty breathing (dyspnea). This can be done in four languages (Korean, English, Chinese, and Japanese) on either an iOS or Android system. The app also provides information on nearby testing clinics. Testing facilities are widely available, making the process easy to understand and complete.

The "self-quarantine safety app" is available in the same languages and operating systems. The main feature/function of this app is to monitor symptoms and provide a tool for self-diagnosis. In addition, an alarm is set to go off once the user leaves the designated self-quarantine area. Everyone coming from outside of South Korea is obligated to download the app, including Korean nationals. According to the South Korean government, around 91.4 per cent of people in self-quarantine have installed the app, although the authorities do not clarify how this rate is calculated. The government states that: "The application largely has 3 key functions: a self-diagnosis for the users to conduct and submit the results with the assigned government officers; a GPS-based location tracking to prevent possible violation of self-quarantine orders; and providing necessary information including self-quarantine guidelines and the contact info of the assigned government case officers." Officials are tasked with checking the data received through the app and following up on possible non-response or violations of self-quarantine guidelines by tracking the movements of the patient using GPS.

Both systems are designed to control large populations of possibly infected users, and they require the collection and processing of big data, on top of vast human resources for enforcement. Ultimately, these apps function to reduce the risk of spreading the virus and govern the movement of (possibly) infected people using surveillance technology.

In the private sector, several apps have been released that utilise publicly available data published by the KCDC. For example, the "Now and Here app" determines the possible risks of a planned route using recorded movement data of confirmed COVID-19 patients. It also provides the locations of testing facilities. The "Cobaek app" tracks the movement of users and alerts them when they are within 100 meters of a confirmed patient, also listing the availability of masks at pharmacies based on public data provided by the National Information Society Agency (NIA).

Laws on data use have been revised in order to facilitate such broad use. Through the Infectious Disease Control and Prevention Act (IDPA) and the introduction of the Advancement of Smart Quarantine Information System, the state has made it possible to track individuals coming in from overseas, tracking their movements through ship or flight number, place of departure and destination, arrival time and personal passenger information, GPS data, card transactions, and CCTV recordings. Under the IDPA, any institution,

organization, or individual must share information on anyone who is infected or deemed "likely to be infected by an infectious disease." The KCDC shares information with the "National Police Agency, Credit Finance Association of Korea, 3 telecommunications companies and 22 credit card companies" for the purpose of tracking possible patients and to "quickly identify transmission routes and places". This includes current whereabouts and the total time spent in each location. Information collection is automated and can be done in 10 minutes from the moment a request is made. The use of big data thus extends beyond healthcare and far into the lives of private individuals.

Within the healthcare sector, the government has made temporary arrangements for allowing doctors and nurses to consult with patients through video calls and video conferencing, telemedicine, or "remote medicare". This is done to decrease the burden on hospital staff, and to provide technical knowledge between healthcare facilities. The app "Medihere" allows users to contact hospitals and make an appointment online. "Odoctor" gives patients the option to access general medical information and diagnosis, and it allows them to participate in remote treatment through the "Coronavirus 119" function. This app is also designed to screen patients before they visit clinics and hospitals, and to shorten the amount of time spent there, reducing possibility of transmission. In order to make use of these apps, patients are required to answer questions concerning their medical history. This information is shared with care providers.

Public and private apps have been widely used, with millions of downloads in South Korea. Combined with the emergency system from which receivers cannot opt out, South Korean residents are able to access critical information and avoid high-risk areas. There are signs of fatigue among residents from continuous notifications. However, the use of technology and information-sharing in South Korea has been highly effective in delaying the spread of COVID-19. As a result, the country has avoided severe lockdowns and restrictions of movement on a national scale. Economic impact has been limited by the swift response, and healthcare infrastructure remains intact and able to cope with current levels of infections.

In return, South Koreans and foreign visitors have been subject to invasive changes in terms of privacy protection, with the government able to access personal information if there are suspicions of a possible infection. South Korea has faced multiple pandemics in the past, and these experiences inform a policy approach in which recent changes could be made permanent, in anticipation of possible new pandemics. Although the government has stated it will remove any personal information after the pandemic is over, a clear line delineating the end of the pandemic has not been established. The measures allowing for the described response have become embedded in policy and law, meaning that these mechanisms can be started up quickly whenever a new pandemic arises. Moreover,

the government has stated it will pursue further investments in enhancing and innovating the current systems, enshrining current strategies as a benchmark of future policymaking.

Taiwan

Taiwan has been relatively successful in its fight against COVID-19, and there is no signs of domestic transmission so far. As a result, the most import measures to contain COVID-19 currently is still to effectively quarantine those who travel from outside of Taiwan. The Taiwanese government uses a system called 'digital fence' to help enforce the quarantine, as it monitors if the people under quarantine stay at their quarantine address; to this end, the app uses the location data generated by cellular signals every ten minutes.

To address privacy concerns, the 'digital fence' takes several measures. First, it uses cellular signals instead of GPS signals, which are able to generate more accurate location data to locate people under quarantine. According to the Taiwanese government, this infringes privacy to a lesser degree. Second, the app uses location data exclusively for the purpose of the quarantine, and people under quarantine will not be monitored anymore after the 14-days quarantine period. However, the location data will be stored until the end of the ongoing crisis. Third, the location data is not actually shared with the government, since it is the five major telecommunication companies in Taiwan that do the monitoring, and they only report to the local government authorities in case there are indications of non-compliance.

However, the 'digital fence' system also reported several common problems and has been challenged by civil society. First, the app created false alarms and serious annoyance for people under quarantine, due to various technical issues, such as telephones running out of battery, bad network connections, or simple failures to answer phone calls. Second, as MP Wu I-ding pointed out in her parliamentary inquiry, the government's Home Quarantine Notice fails to properly inform those who undergo quarantine that they will be monitored.

Furthermore, the Taiwanese government, in cooperation with the Taiwan AI Lab, has developed a contact-monitoring smartphone application for possible future scenarios. The usage of this application will be voluntary, and the personal data of the users will be anonymised and will only be stored locally on the user's smartphone. Also, as Taiwan's digital minister explained, there will be no need for this app unless there are signs of domestic transmission in Taiwan. Finally, Taiwan's digital minister has rolled out a well-received 'eMask' app that tracks and displays the inventories of local drugstores, to prevent shortages, panic buying, and price gauging of health-related goods.

The work presented here is based on a first round of desk-research, and it omits detailed references in the interest of brevity. More detailed and fully-sourced studies will follow: in late April, the LAC will publish the full regional surveys on its website; at a later stage, it will publish an in-depth report that will incorporate detailed policy analyses. All of these outputs are written in English, reflecting the international backgrounds of our contributors.

This preliminary report is the common effort of researchers from the LeidenAsiaCentre, led by **Dr. Florian Schneider** (Director) and **Dr. Rogier Creemers** (Head of the China's Role in Cyber Security project). Authors of the specific cases are (in order of appearance):

Introduction: **Dr. Florian Schneider** (LeidenAsiaCentre, Leiden University)
Japan: **Anoma van der Veere** (LeidenAsiaCentre, Osaka University)
Mainland China: **Emma Burgers** (LeidenAsiaCentre) & **Ryszard Sicinski** (LeidenAsiaCentre)
Singapore: **Jonas Lammertink** (LeidenAsiaCentre)
South Korea: **Anoma van der Veere** (LeidenAsiaCentre, Osaka University)
Taiwan: **Siyi (Eric) Zhang** (LeidenAsiaCentre)

LeidenAsiaCentre is an independent research centre affiliated with Leiden University and made possible by a grant from the Vaes Elias Fund. The centre focuses on academic research with direct application to society. All research projects are conducted in close cooperation with a wide variety of partners from Dutch society.

More information can be found on our website : www.leidenasiacentre.nl

For contact or orders: info@leidenasiacentre.nl M. de Vrieshof 3, 2311 BZ Leiden, The Netherlands

Inhoudsopgave

Tweede Kamer
DER STATEN-GENERAAL

Blok 3

CV’s en Position Papers

/

Inhoudsopgave

Rondetafelgesprek Corona-app woensdag 22 april 8.30 – 12.30 uur

Blok 3

Bas Filippini – Voorzitter stichting Privacy First

- Bas Filippini is voorzitter van de door hem in 2008 opgerichte Privacy First; een onafhankelijke stichting met als doel het behoud en de bevordering van het recht op privacy.
- Filippini heeft een ondernemende carrière achter de rug in het bedrijfsleven, als laatste bij KPN Telecom. In 1997 richtte hij zijn eigen bedrijf op, Tele'Train te Amsterdam. Op dit moment participeert hij als venture capitalist in diverse bedrijven en projecten. Vanuit persoonlijke interesse volgde hij diverse trainingen en opleidingen in zelfontwikkeling. Persoonlijke vrijheid en integriteit ziet hij als het meest kostbare wat een mens bezit en wat hem vanuit eigen ervaring heeft gevormd, zowel privé als zakelijk. Als persoonlijke bijdrage aan de samenleving heeft hij daarom het initiatief genomen voor het oprichten van de stichting Privacy First.

Evelyn Austin – Directeur van Bits of Freedom

- Evelyn Austin is directeur van Bits of Freedom, een onafhankelijke stichting die opkomt voor internetvrijheid in Nederland en zich richt op de grondrechten communicatievrijheid en privacy.
- Austin kwam via de kunsten, namelijk als programmamaker, redacteur en onderzoeker, in 2014 bij Bits of Freedom terecht. Als directeur is zij sinds 2019 verantwoordelijk voor de strategie, het personeel, en de operationele leiding. Daarvoor ondersteunde zij de vrijwilligersprojecten, droeg bij aan het verstevigen van het Europese netwerk en schreef ze over de dominantie van grote communicatieplatforms. Ze is mede-oprichter van The Hmm, platform voor hedendaagse beeldcultuur, en lid van de adviescommissie Digitale Cultuur van het Stimuleringsfonds Creatieve Industrie.

Marleen Stikker – Directeur van Waag

- Marleen Stikker (1962) is oprichter, directeur en bestuurder van Waag; een Europees onderzoeksinstituut voor technologie en maatschappij dat aanzet tot actief burgerschap door open, eerlijke en inclusieve technologie te ontwikkelen.
- In 1993 stond Marleen aan de wieg van het internet. Als bedenker en 'burgemeester' van De Digitale Stad ontwikkelde ze de eerste gratis toegangspoort tot een virtuele gemeenschap op het internet. In 1994 richtte ze samen met Caroline Nevejan Waag op. Vanuit Waag houdt Marleen zich bezig met vele projecten en initiatieven. Zo was ze nauw betrokken bij de oprichting van XS4ALL, PICNIC, Creative Commons Nederland en het eerste FabLab van Europa in de Waag. Marleen is tevens betrokken bij de Open Design-beweging. Ze neemt op dit moment zitting in de Europese Horizon2020 Commissie 'High-level Expert Group for SRIA on innovating Cities/DGResearch' en is lid van het executive board van Public Spaces, een coalitie die zich richt op het voorstellen van een nieuw internet dat niet gaat om politieke controle, maar om een nieuwe publieke ruimte. In 2019 kwam Marleens boek 'Het internet is stuk (maar we kunnen het repareren)' uit. Ook is ze winnaar van de Felipe Rodriguez Award 2019.

PRIVACY FIRST

Keizersgracht 127
1015 CJ Amsterdam
Tel. 020 - 8100279

Aan:
Tweede Kamer der Staten-Generaal
Vaste commissie voor Volksgezondheid, Welzijn en Sport
Per email: cie.vws@tweedekamer.nl

Uw ref.	:	
Onze ref.	:	SPF20200420
Datum	:	20 april 2020
Betreft	:	Position paper t.b.v. rondetafelbijeenkomst Corona-app 22 april 2020

Geachte Kamerleden,

Dank voor uw uitnodiging om deel te nemen aan de rondetafelbijeenkomst inzake de zogeheten Corona-app. In de optiek van Stichting Privacy First vormt een dergelijke app een bedreiging voor ieders privacy. Hieronder zullen wij dit kort toelichten.

Gebrek aan noodzaak en effectiviteit

Met grote zorg heeft Privacy First kennisgenomen van het voornemen van de Nederlandse overheid om een contact-traceerapp te gaan inzetten ter bestrijding van het Corona-virus. De maatschappelijke noodzaak van een dergelijke app is tot op heden niet aangetoond. Ervaringen vanuit het buitenland laten bovendien zien dat aan het nut en de effectiviteit ervan ernstig kan worden getwijfeld. Mogelijk werken deze apps zelfs contra-productief, aangezien de inzet ervan tot schijnveiligheid leidt. Daarnaast wordt de meest kwetsbare doelgroep (ouderen) met dit middel nauwelijks bereikt. Alleen al om deze redenen zou van de inzet van “Corona apps” moeten worden afgezien.

Surveillance maatschappij

Privacy First ziet het gebruik van dergelijke apps als een gevaarlijke ontwikkeling, aangezien dit kan leiden tot talloze onterechte verdenkingen, stigmatisering, onnodige onrust en paniek. Zelfs “geanonimiseerd” kunnen de gegevens uit dergelijke apps via koppeling alsnog tot individuele personen herleid worden. Bij grootschalig gebruik leidt dit tot een surveillance maatschappij waarin iedereen geobserveerd en geregistreerd wordt en men zich voortdurend gemonitord waant, met een maatschappelijk *chilling effect* tot gevolg.

Risico’s op misbruik

Groot risico is dat de verzamelde data voor meerdere doelen zullen worden gebruikt en misbruikt door bedrijven en overheden. Het risico van heimelijke toegang, hacking, datalekken en misbruik is met name groot bij centrale i.p.v. decentrale (persoonlijke) opslag en bij gebrek aan open source software. Tegelijkertijd biedt ook louter persoonlijke opslag geen enkele garantie tegen misbruik, afhankelijk van technische kwetsbaarheden of aanwezige malware en spyware. In handen van criminele

© 2020 STICHTING PRIVACY FIRST

organisaties vormen de verzamelde data bovendien een goudmijn voor criminele activiteiten.

Voor Privacy First wegen deze risico's van "Corona apps" niet op tegen de veronderstelde voordelen. Dus adviseert Privacy First uw Kamer om er bij het kabinet op aan te dringen niet tot de inzet van dergelijke apps over te gaan.

Testen i.p.v. appen

Vanuit de beginselen van proportionaliteit en subsidiariteit in de strijd tegen het Corona-virus bestaat volgens Privacy First een betere en effectievere oplossing, namelijk het grootschalig testen van de bevolking op het virus en op immuniteit. De benodigde testcapaciteit dient daartoe zo spoedig mogelijk beschikbaar te zijn.

Haastige spoed, zelden goed

Mocht ondanks bovenstaande bezwaren alsnog besloten worden tot de inzet van "Corona apps", dan kan dit pas gebeuren na een zorgvuldig maatschappelijk en democratisch proces met voldoende kritische, objectieve en onafhankelijke toetsing. Tot op heden is hier geen sprake van geweest, getuige de ontwikkelingen de afgelopen dagen. Privacy First adviseert uw Kamer in dit verband om het kabinet een pas op de plaats te laten maken en een moratorium op de inzet van "Corona apps" in te stellen.

Privacy by design

Het recht op anonimiteit in de openbare ruimte is een klassiek grondrecht en cruciaal voor het functioneren van onze democratische rechtsstaat. Een democratisch besluit tot opheffing hiervan is onacceptabel. Mocht alsnog besloten worden tot grootschalige inzet van "Corona apps", dan dient dit dus strikt anoniem, tijdelijk en op zuiver vrijwillige basis te gebeuren. Met individuele toestemming vooraf zonder enige vorm van druk, volledig geïnformeerd en voor een legitiem, specifiek doel. *Privacy by design* (het inbouwen van privacybescherming in de techniek) dient daarbij leidend te zijn. Voor Privacy First zijn dit harde juridische voorwaarden die niet onderhandelbaar zijn. Mocht hier niet aan voldaan worden, dan zal Privacy First dit bij de rechter aanvechten.

Voor nadere informatie of vragen met betrekking tot bovenstaande is Privacy First te allen tijde bereikbaar op telefoonnummer 020-8100279 of per email: info@privacyfirst.nl.

Hoogachtend,

Stichting Privacy First

mr. Vincent A. Böhre, CIPP/E
directeur

© 2020 STICHTING PRIVACY FIRST

Inhoudsopgave

Positioning paper ten behoeve van het rondetafelgesprek corona-app
Datum: woensdag 22 april 2020 Tijd: 8.30 – 12.30 uur
Locatie: Tweede Kamer der Staten-Generaal, Oude Zaal

Door: Marleen Stikker, Tom Demeyer, Sander van der Waal, Gijs Boerwinkel, (Waag) Roel Dobbe (AI Now Institute, New York University), Douwe Schmidt (Tada.city)

OPROEP TOT INTERDISCIPLINAIR PUBLIEK ONDERZOEK & ONTWERPPROCES

1. Proces

Afgelopen week heeft zich iets zeer bijzonders voltrokken: nooit eerder werden ICT ontwikkelaars zo in het openbaar gefileerd. De digitale anatomische les werd live naar onze huiskamers gestreamd. Het proces was chaotisch, de criteria onhelder, er was sprake van onbegrijpelijke haast, mensen vroegen zich vertwijfeld wat het ministerie bezielde. Toch wil ik ervoor pleiten dat we het publieke karakter van dit traject, zei het zorgvuldig, als leidraad nemen voor toekomstige ICT ontwikkeling en aanbestedingen In korte tijd werden bedrijfsbelangen, technologische grootspraak en fundamentele zelfoverschatting blootgelegd. En dat is goed.

Ook goed nieuws is dat de samenleving zich nadrukkelijk mengt in het debat: van burgerrechten- en culturele organisaties, wetenschappers uit alle disciplines, hackers, journalisten en ontwerpers tot talkshow hosts. Daar komt bij dat u als Tweede Kamer een grondig debat wil voeren over de wenselijkheid van een corona-app. U maakt zich terecht zorgen over het proces en stelt fundamentele vragen over de toetsing aan grondrechten en de mogelijkheid tot parlementaire controle.

Tot zover het goede nieuws. Wat deze week kraakhelder werd is dat er veel meer moet gebeuren om applicaties als deze in hun socio-technische en juridische context te ontwikkelen en te valideren. Dat experts hebben meegekeken op het gebied van privacy en security is mooi, maar daarmee is alleen de technologie in beeld gebracht, niet de onderliggende aannames of de implicaties van gebruik. Waar centraal had moeten staan zijn de maatschappelijke scenario's voor een exit strategie uit de intelligente lockdown en hoe technologie daaraan kan bijdragen. In plaats daarvan hebben we naar ontwikkelaars geluisterd die onbekend zijn met de complexiteit van contact onderzoek, de sociale-culturele processen die gedrag beïnvloeden en de wijze waarop technologie de rechtsorde kan ondermijnen. Het uit den treure herhalen dat 'privacy belangrijk is' en een twee uur durende spoedcursus van de GGD over contact onderzoek zijn volstrekt onvoldoende. Het ministerie heeft een podium gegeven voor fancy digitale verkooppraatjes en heeft met een start-up 'can do' mentaliteit gesuggereerd dat ze het varkentje wel even zouden wassen. Een probleem dat

omkleed is met zoveel onzekerheid (zowel technisch, sociaal en juridisch) vergt een fundamenteel andere aanpak.

Het feit dat er geen tijd aan de analyse en de probleemfase is besteed, spreekt boekdelen. De coalitie Veilig Tegen Corona was er vroeg bij om het gehele proces fundamenteel ter discussie te stellen en heeft scherpe uitgangspunten geformuleerd in een manifest. Voor zover er in de marktconsultatie uitgangspunten zijn meegenomen, zijn deze grotendeels hieruit overgenomen. Het ministerie had er zelf geen tijd voor ingeruimd.

Het geeft aan hoe naïef en techno-solutionistisch het Nederlandse bestuur nog is. Tijdens het weekend werd optimistisch verkondigd dat het ging om "een appathon en geen hackathon, we zijn de probleemfase voorbij." Een groot deel van de maatschappelijke opwinding werd gevoed doordat minister De Jonge de app presenteerde als een oplossing zonder dat duidelijk was waarvoor. Dat er tevens werd gekozen voor een turbo-proces, met als doel binnen drie weken tot een “productierijpe” oplossing te komen, wakkerde het wantrouwen verder aan. Het was als een bullet trein zonder duidelijke bestemming die allerlei cruciale stations oversloeg.

Het is niet verwonderlijk dat deze trein krakend en piepend tot stilstand is gekomen. Het heeft duidelijk gemaakt dat een open en interdisciplinair ontwerpproces noodzakelijk is waarbij vanuit diverse perspectieven meegedacht kan worden over wenselijke scenario’s om uit de intelligente lockdown te komen. Scenario's die rekening gehouden met de rechten, belangen en wensen van alle betrokkenen.

2. Criteria veilig tegen Corona

De coalitie Veilig tegen Corona heeft nadrukkelijk aangegeven dat de noodzaak tot een app nog nergens was aangetoond en beargumenteerd. De bredere eisen van doelmatigheid, effectiviteit en maatschappelijke impact uit deze lijst van criteria is pas in de loop van het weekend van de appathon breed opgepikt. De wetenschappelijke onderbouwing van de keuze voor het inzetten van een app met bijbehorende infrastructuur en de bijdrage daarvan aan het bron- en contactonderzoek van de GGD behoeft - nog steeds - veel meer aandacht. De vernauwing die ontstaat door het voortdurend gebruik van het woord app is ook gevaarlijk. Het wordt met deze term iets individueels, een keuze van het individu om in te zetten of niet. Vanuit het oogpunt van een digitale infrastructuur, waar we het in werkelijkheid over hebben, moeten we ons realiseren dat we het hebben over een veel ingrijpender maatschappelijk mechanisme met risico's op grotere surveillance en waar afbreuk van rechtsstaat en grondrechten in het geding kunnen zijn. Het woord "app" is een handig term om die dimensies niet zichtbaar te maken. Net zoals het begrip privacy, is het teveel gericht op het individu. Net zoals databescherming niet om persoonlijke privacy gaat, maar om algemeen belang, zoals Maxim Februari scherp verwoordde, zo draait bron- en contactopsporing niet om een app maar om een gedeelde infrastructuur ontwikkeld in een ecosysteem van mensen en organisaties. Een app is maar een klein onderdeel. De infrastructuur raakt aan het hart van de rechtsstaat.

3. Wat nu?

We staan voor een complexe opgave, daar is iedereen het over eens. We moeten dus een aanpak en methode inzetten die al deze complexiteit erkent in plaats van negeert, en toch inspeelt op de urgentie van het moment. Het eerste waar we in Nederland het gesprek gedegen over moeten voeren is welk *exit scenario* haalbaar is. Vragen moeten beantwoord worden als: wat is verantwoord, wat is wenselijk gedrag, wat weten we over het verloop van het virus, hoeveel testen zijn er beschikbaar en wie gaan we testen? Maar ook: hoe waarborgen we de fundamentele burgerrechten in de keuze voor de aanpak, en hoe zorgen we dat iedereen die het aangaat op de juiste manier betrokken is? Het is bij uitstek een ontwerpvraagstuk. Hiervoor het is cruciaal dat de verschillende disciplines gezamenlijk ontwerpend te werk gaan. Experts van virologie en epidemiologie, de medische wetenschap, zorgverleners, gedragswetenschappers, social designers, maatschappelijke en culturele organisaties, privacy experts, juristen, ze zijn allemaal essentieel.

Pas wanneer we gezamenlijk de probleemstelling helder geformuleerd hebben en grondig verkend hebben welke mogelijke scenario's er zijn, kunnen we een weloverwogen keuze maken voor welk exit scenario het meest passend is en hoe technologie daar een ondersteunende rol in speelt. Een groot voordeel van het traject de afgelopen weken is dat we veel helderder voor ogen hebben welke uitdagingen en problemen er kleven aan de mogelijke inzet van technologie hierbij.

We raden daarom aan de het proces van de afgelopen week niet als verloren te beschouwen, maar te zien als bijdragend aan een open consultatie over de criteria waaraan een eventuele app en infrastructuur, en de inzet daarvan, zouden moeten voldoen. Het zou een waardevolle stap kunnen zijn in aanloop naar een zorgvuldige open call, op basis van een gedegen en gedragen set aan eisen.

Het moet een opsteker zijn voor de Tijdelijke Commissie Digitale Toekomst dat dit brede debat over maatschappelijke impact van digitalisering plaatsvindt. Het geeft aan dat specifieke domeinkennis op tal van terreinen nodig is om tot een zorgvuldig afgewogen proces en resultaat te kunnen komen. Het is een debat dat een paar jaar geleden waarschijnlijk nog niet had plaatsgevonden, en het is een debat dat we in de toekomst nog veel vaker zullen moeten voeren. Dat is winst.

Inhoudsopgave

Tweede Kamer
DER STATEN-GENERAAL

Blok 4

CV’s en Position Papers

/

Rondetafelgesprek Corona-app woensdag 22 april 8.30 – 12.30 uur

Blok 4

Ronald Prins – Lid Toetsingscommissie Inzet Bevoegdheden Inlichtingen- en Veiligheidsdiensten (TIB)Functie

- Buitengewoon Raadslid Onderzoeksraad voor Veiligheid (OVV)
- Lid van Raad van Toezicht DIVD, DIVD is een platform voor beveiligingsonderzoekers om kwetsbaarheden te melden, ondersteund door vrijwilligers
- Lid van Adviescommissie Fintech & Innovatie Autoriteit Financiële Markten
- Mede-oprichter van cybersecuritybedrijf Fox-IT

Sijmen Ruwhof – Freelance IT Security Consultant / Ethisch Hacker

- Specialist in hacking, IT security onderzoeken en het uitvoeren van geavanceerde penetratietesten.
- Sinds 2005 voert hij professioneel beveiligingstesten uit en meer dan 700 beveiligings-onderzoeken afgerond. Heeft meer dan honderd websites ontwikkeld op een PHP, MySQL, Apache en Linux softwarestack.

Jeroen Terstegge – Partner bij Privacy Management Partners

- Ruim 25 jaar ervaring op privacygebied en was als Privacy Officer van Philips één van de geestelijke vaders van de Binding Corporate Rules (BCR's)
- Country Leader Netherlands bij IAPP - International Association of Privacy Professionals. Voorzitter van de Privacy Commissie van de Nederlandse Raad van Centrale Bedrijfsorganisaties (VNO-NCW / MKB Nederland).
- Als deskundige op het gebied van privacywetgeving en compagnon van Privacy Management Partners geraadpleegd bij het opstellen van de Algemene Verordening Gegevensbescherming (AVG).

Inhoudsopgave

Hoorzitting Corona app - Blok 4 - Ronald Prins

Goedemorgen,

dank voor de uitnodiging.

Hele kleine disclaimer vooraf. Ik ben ook lid van de onderzoeksraad voor veiligheid. Het zou zomaar kunnen dat er een evaluatie gaat plaatsvinden. Ik ga dus nu niet hier al zeggen of een Contact Tracing app een zinnige toevoeging is in het geheel van maatregelen.

Ik kan u wel meenemen in het ontwikkelproces van software waar het gaat om het beschermen van grote belangen.

Heel erg versimpeld valt het proces uiteen in vijf stappen:

Stap 1: GGD definieert helder wat ze nodig hebben en hoe hun contactonderzoek proces eruit ziet
Stap 2: Een ontwikkelteam onderzoekt hoe ze dat zouden kunnen maken met een minimaal privacy risico
Stap 3: Afweging of dat risico opweegt tegen de potentiële ‘opbrengst’ van het gebruik van de app. (proportionaliteit)
Stap 4: Security review van de oplossing (het totale systeem dus apps en backend) zal leiden tot issues die mogelijk opgelost kunnen worden door het ontwikkelteam of meegenomen moeten worden als restrisico
Stap 5: afweging of het nieuwe risico nog opweegt tegen de potentiële opbrengst.

In de praktijk blijkt vaak dat je met 1 keer doorlopen van dit proces het niet haalt, en je dan terug moet naar stap 1: Bijstellen van de wensen door GGD. Ik kan dit niet genoeg benadrukken, het lukt niet in 1 keer.

De GGD zal allicht zoveel mogelijk data willen verzamelen, en vanuit privacy oogpunt wil je dat zo min mogelijk. Alleen met een gedegen proces waarbij de GGD met de ontwikkelaars rond de tafel zit, kan je komen tot een punt waarbij je een acceptabel compromis kan bereiken. En dan nog moet je je afvragen (subsidiariteit) of wat je overhoudt aan functionaliteit niet kan oplossen met andere creatieve oplossingen. Misschien is de GGD al heel blij met een digitale export van het telefoonboekje uit de telefoon van een covid 19 patient.

Daarnaast wil ik eraan toevoegen dat het allemaal nieuw is, en veel empirisch zal moeten worden vastgesteld. We weten bijvoorbeeld helemaal niet hoe goed Bluetooth technologie gebruikt kan worden om afstanden en besmettelijkheid in te schatten, en we weten ook niet precies hoe we de eerder genoemde ‘opbrengst’ moeten kwantificeren. Er van uitgaand dat er geen tijd is voor laboratoriumonderzoek zal je dit in een live omgeving moeten uitvinden. Met de uitkomsten daarvan kunnen de parameters in de app in de loop der tijd aangepast worden.

Nog wat losse observaties:

- Er zijn contact tracing voorstellen gedaan (Google/Apple en DP-3T) die in staat zijn, om contacten vast te leggen zonder dat daar bij identificerende gegevens opgeslagen worden. Dit werkt heel goed en anoniem, en ik was dus ook zeer verbaasd dat er voorstellen waren waarbij bijvoorbeeld via sms en dus telefoonnummers gecommuniceerd wordt.
- Een app die van bluetooth gebruik maakt, zal altijd vereisen dat bluetooth aanstaat. Het is hackers regelmatig gelukt om misbruik van een telefoon te maken via bluetooth. De impact van dit risico moet zeker meegewogen worden. De app maker heeft hier geen invloed op.

Tenslotte

Zoals bekend hebben Google en Apple de handen ineen geslagen om op hun platforms een voorziening aan te brengen die app bouwers helpt om de bluetooth voorziening zo effectief mogelijk te kunnen gebruiken en ook te zorgen dat het contacten lijstje dat op de telefoon wordt opgeslagen geen identificerende gegevens bevat. Daarnaast houdt de gebruiker altijd zelf de keuze of je dit wilt of niet, en mogen alleen ‘relevante autoriteiten’ van een land een contact tracing app in de app store plaatsen.

De details zijn nog niet allemaal bekend, maar omdat zij ‘dieper’ in de telefoon aanpassingen kunnen maken dan app-bouwers is de verwachting dat dit tot een zowel veiligere als technisch betrouwbaardere oplossing kan leiden.

Ik kijk uit naar uw vragen

Inhoudsopgave

Position paper: Corona contact-tracing app

Door: Sijmen Ruwhof - IT Security Consultant / Ethisch Hacker **Datum:** 19 april 2020

Op 11 april 2020 heeft het ministerie van Volksgezondheid, Welzijn en Sport aan de markt een uitnodiging gedaan voor het indienen van voorstellen voor slimme digitale oplossingen voor bron- en contactonderzoek (app). De appathon die van het weekend plaatsvond heb ik aandachtig gevolgd. Het valt te prijzen dat dit selectieproces zo openbaar wordt uitgevoerd.

Selectieproces is afvalrace geweest
De onder hoge tijdsdruk uitgevoerde marktuitvraag mondde echter uit in een veel bekritiseerde competitie. In een paar dagen tijd zijn 660 projectvoorstellen door 65 experts in sneltreinvaart beoordeeld, zonder duidelijke criteria en structuur. Een deel (9) van de experts heeft publiekelijk afstand genomen van de uiteindelijke selectie. Afgelopen weekend zijn de 7 overgebleven apps gepresenteerd aan het publiek.

Privacy en security in apps niet gewaarborgd
Geen enkele van deze apps blijkt enigszins in de buurt te komen van de door de ministerie gestelde privacy en security randvoorwaarden. De apps zijn allen nog in een zeer prematuur prototype stadium. KPMG beoordeelt de apps als onveilig en volgens de landsadvocaat is de anonimiteit in geen van de apps gewaarborgd. Sommige apps die waren afgewezen bleken technisch veel beter te zijn uitgewerkt.

Het selectieproces heeft niet gewerkt
Het experimentele en overhaaste selectieproces heeft een duidelijke conclusie opgeleverd die unaniem door experts wordt gedragen: het selectieproces heeft niet gewerkt. De enorme haast waarmee het proces werd ingestoken deed op allerlei manieren afbreuk aan een al wankel vertrouwen.

Terug naar de tekentafel
Het slim inzetten van moderne technologie is een heel goed idee. Daar moet echter wel eerst zorgvuldig over nagedacht worden. Expliciete eisen inzake functionaliteit en veiligheid/privacy zijn van het allergrootste belang!

Een app die een dermate grote impact gaat hebben op de Nederlandse samenleving, verdient een gedegen aanpak. De inspanningen die tot nu toe zijn gepleegd, zijn uitermate nuttig geweest om dit beeld helder te krijgen en daarmee zeer waardevol.

60% vrijwillige installatie is bijzonder ambitieus
De beoogde 60% vrijwillige installatie (meer dan 10 miljoen mensen) van de app is met het huidige proces en de voorgeselecteerde 7 apps bijzonder ambitieus. In Nederland heeft 80% van de bevolking een smartphone. Dat betekent dat 3-op-de-4 smartphone-gebruikers de app vrijwillig moet gaan installeren. Er zal daarom heel veel vertrouwen in de app moeten zijn om het een succes te laten worden. Tot dusver heeft het selectieproces weerstand van honderden experts opgeroepen. Hoe wil de overheid de burger overtuigen met deze aanpak terwijl experts zeggen dat het op deze manier niets gaat worden? Vertrouwen komt te voet en gaat te paard.

Experimentele technologie
Het is nog maar de vraag of de beoogde Bluetooth-technologie gaat werken. Daarvoor moet er nog te veel uitgezocht, getest en ontwikkeld worden. De potentie van een app die voldoet aan alle gestelde privacy en security eisen is er, maar om daar te komen dient toch een zorgvuldiger selectieproces gevolgd te worden.

Conclusie
Op basis van mijn observaties van het proces en de doorgenomen voorstellen adviseer ik de Kamer met klem om niet in te stemmen met de uitkomsten van het selectieproces.

Gebruik de verkregen inzichten van de afgelopen week om terug te gaan naar de tekentafel om te onderzoeken in welke mate een app effectief kan zijn bij de ondersteuning van contactonderzoek door regionale GGD's.

Inhoudsopgave

Memo

Van:	mr. drs. Jeroen Terstegge CIPP/E CIPP/US, partner
Aan:	De Vaste Commissie Volksgezondheid, Welzijn en Sport
Datum:	20-04-2020
Betreft:	Privacy en de Corona app

Geachte Commissieleden,

Dank voor de uitnodiging om deel te nemen aan het rondetafelgesprek over de corona-app. Afgelopen weekend was ik een van de privacyexperts die op uitnodiging van VWS deelnemen aan de appathon. Hoewel iedereen zonder meer zijn en haar best deed om er ondanks weinig voorbereiding, beperkte/ontbrekende documentatie en de zeer korte tijd per leverancier iets van te maken, werd mij al snel duidelijk dat **de app nog onvoldoende doordacht is om de privacyrisico's goed te kunnen inschatten**. Ik licht een en ander hieronder kort toe.

Valse tegenstelling
Laat ik voorop stellen dat het gebruik van een app geen tegenstelling is tussen gezondheid en privacy. Gezondheid is een *doel* (sociaal grondrecht), privacy is een *waarde* (klassiek grondrecht). Het is dus niet óf óf. Het is wél: bescherming van de volksgezondheid met inachtneming van de regels over inperking van privacy, zoals legitimiteit, noodzaak, proportionaliteit en transparantie. Als deze regels niet goed in acht worden genomen, bestaat het risico dat de app door de rechter ongeldig wordt verklaard, zoals onlangs gebeurde met SyRI.

Kaders onduidelijk
Ondertussen staat het grondrecht op databescherming (zoals uitgewerkt in de AVG) onverkort overeind, ook in deze crisis. De AVG gaat over meer dan privacy; ook non-discriminatie, non-stigmatisering, reputatiebescherming, autonomie, menselijke waardigheid en veiligheid van de betrokkene behoren tot de doeleinden van de AVG. De AVG vereist dat gegevensverwerking rechtmatig, behoorlijk en proportioneel is en een geldige juridische basis heeft. Betrokkenen hebben rechten zoals inzage, correctie, bezwaar en verwijdering. Er is een verwerkingsverantwoordelijke die accountable en aansprakelijk is en die maatregelen moet nemen zoals privacy by design en het uitvoeren van risicoanalyses om de gegevensverwerking in goede banen te leiden (privacymanagement).

Het is echter vooralsnog volstrekt onduidelijk onder wiens juridische verantwoordelijkheid de app straks wordt uitgerold. Door het ontbreken van die kaders kan nog geen serieus begin worden gemaakt met het inrichten van de juridische, technische en organisatorische waarborgen.

Een ander aandachtpunt is dat de AVG niet van toepassing is op alle gegevensverwerkingen. Zo is de AVG *niet* van toepassing op persoonlijke gebruik van de gebruiker van de app (art. 2 lid 2 AVG). Bij een volledig decentrale en dus privacyvriendelijke oplossing waarbij de gebruiker er zelf voor kiest om

zijn/haar gegevens door te geven aan de huisarts of de GGD, bestaat de kans dat de AVG niet van toepassing is op de gegevens in de telefoon en de communicatie tussen de telefoons (of dit inderdaad zo is, moet voor elk voorstel nader worden onderzocht). Dit zou grote gevolgen hebben voor de governance rondom de app. Zo zou de Autoriteit Persoonsgegevens bijvoorbeeld niet bevoegd zijn om toezicht te houden en kunnen de gebruikers zich niet beroepen op hun rechten in de AVG.

Duidelijkheid over het doel van de app nodig.
Elke gegevensverwerking vereist een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel (art. 5 AVG). Het doel van de app is vooralsnog gekoppeld aan het werk van de GGD. Het is echter de vraag of de gebruikers dit doel ook zo zullen ervaren. Als de app wordt ervaren als een middel om besmettingen te voorkomen, creëert de app schijnveiligheid. Het doel van de app moet dus glashelder binnen en buiten de app worden gecommuniceerd. Een zogeheten '*layered privacy notice*', waarin de informatie in gradaties van gedetailleerdheid wordt aangeboden, kan daarbij helpen.

Noodzaak nog niet aangetoond
Noodzakelijkheid valt juridisch (grondrechtelijk/AVG) uiteen in twee componenten:

1. De app draagt effectief bij aan een concreet doel (zie ook hieronder *datakwaliteit*).
2. Een minder vergaand, maar even effectief middel is niet voorhanden of realistisch (subsidiariteit).

De Minister zal de noodzaak van de app moeten aantonen. Een "verwachting van de GGD" (zie Kamerbrief van 16 april) is onvoldoende om de noodzaak te onderbouwen. Ook het enkele feit dat het normale contacttracingproces van de GGD het niet meer kan bijbenen als de lockdown wordt opgeheven, is onvoldoende om de noodzaak te rechtvaardigen als de app niet ook effectief bijdraagt aan de oplossing van het probleem van de GGD.

Datakwaliteit is belangrijk
Het succes van de app staat of valt met de kwaliteit van de gegevens (zie ook art. 5 AVG). Los van het feit dat onvoldoende testen op zich al leidt tot een lage datakwaliteit, moet een besmette persoon zijn/haar positieve status ook daadwerkelijk (willen) registreren in de app. Dit vereist dat zowel de app als het ecosysteem waarin de app functioneert volledig moeten kunnen worden vertrouwd door een besmette persoon. Niet alleen moet de app veilig zijn en alleen doen wat het zegt te doen, de partij onder wiens verantwoordelijkheid de app wordt uitgerold moet ook volstrekt betrouwbaar zijn, onder meer door aantoonbare en kwalitatief hoogstaande beheersmaatregelen, zoals privacy-by-design en default in de app en de organisatie, een openbare en periodiek bijgewerkte gegevenseffectbeoordeling (DPIA), een auditcyclus, en een kwalitatief goede functionaris gegevensbescherming (FG) die toezicht houdt en adviseert.

Daarnaast moet de app ook betrouwbaar een mogelijk risicocontact kunnen vaststellen. Dit stelt hoge eisen aan de gebruikte techniek. Veel loos alarm is immers funest voor de betrouwbaarheid en de acceptatie van de app. De eerste keer zullen de meeste mensen de adviezen wel opvolgen, de tweede keer misschien ook nog wel, maar de derde, vierde, vijfde of tiende keer? Er zit waarschijnlijk een grens aan hoeveel loos alarm mensen bereid zijn om te accepteren.

De app vereist wetgeving
De app kan op basis van ingebouwde beslisregels komen tot een signaal en mogelijk ook een advies aan de gebruiker die in contact is geweest met een besmette persoon. Dat signaal/advies kan grote gevolgen hebben voor zo'n gebruiker, zowel praktisch (isolatie) als emotioneel. De AVG verbiedt daarom categorisch dergelijke functionaliteit (art. 22 lid 1). Hoewel de AVG toelaat dat de betrokkene uitdrukkelijk toestemming geeft voor dergelijke functionaliteit (art. 22 lid 2 sub c AVG), raad ik het vragen van toestemming met klem af omdat mensen die gevolgen op voorhand niet of nauwelijks

goed kunnen overzien bij de installatie van de app. Logischer is dus om op basis van art. 22 lid 2 sub b AVG specifieke wetgeving te maken waarin ook voorschriften en waarborgen zijn opgenomen met betrekking tot die functionaliteit ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de gebruiker.

NB. Als de app het ook mogelijk maakt om een zelfdiagnose te stellen, is naast de AVG mogelijk ook de Verordening betreffende medische hulpmiddelen (MDR) van toepassing.

Flankerend privacybeleid is nodig
In de Kamerbrief van 16 april staan de eisen aan de app zelf. Maar de inzet van de app vereist ook beschermingsmaatregelen rondom het gebruik van de app in de maatschappij, zoals een verbod om het gebruik van de app verplicht te stellen voor toegang tot gebouwen of het openbaar vervoer, regels over wat werkgevers wel of niet mogen vragen aan hun werknemers, en een *sunset clause* in de wet waarmee de app wordt ingevoerd om te voorkomen dat de app langer wordt gebruikt dan nodig.

Verbod op nevengebruik
Gelet op de risico's van stigmatisering en uitsluiting van besmette personen en personen waarvan de app aangeeft dat zij een risicocontact hebben gehad, moet het gebruik van gegevens voor andere doeleinden zonder uitdrukkelijke toestemming van de gebruiker of voorafgaande wettelijke verplichting verboden worden. Dat betekent bijvoorbeeld ook dat de app zo min mogelijk additionele functies mag bevatten anders dan voorlichting of communicatie met de (huis)arts.

Digitale enkelband?
Terwijl wij in Nederland nadenken over een contacttracing app, werken Google en Apple aan hun Google Apple Contact Tracing (GACT) standaard, die het mogelijk maakt om contact tracing tussen iOS en Android telefoons via bluetooth mogelijk te maken. Daar zitten, ongeacht de privacykeuzes die Nederland maakt rondom de corona app, enorme risico's aan. GACT werkt op het operation system niveau, niet op app-niveau. Dit betekent dat contact tracing altijd beschikbaar is voor alle applicaties op de telefoon (dus niet alleen voor de corona app). Zelfs als je geen corona app op je telefoon hebt geïnstalleerd, zal je telefoon -zolang bluetooth aanstaat- voortdurend communiceren met andere telefoons in de buurt. In essentie creëren Apple en Google een systeem voor massa-surveillance, waarmee betrouwbaar kan worden nagegaan wie met wie in contact is geweest (en mogelijk ook wanneer, hoelang en waar).

Onze telefoon dreigt dus een digitale enkelband te worden die misschien wel nooit meer afgaat.

Privacy
Management
Partners
Coöperatie UA
adres
Vondellaan 58
3521 GH Utrecht
telefoon
+31 85 401 38 66
e-mail
info@pmpartners.nl
website
www.pmpartners.nl

Inhoudsopgave

Tweede Kamer
DER STATEN-GENERAAL

Position Papers
Niet-genodigden

/

WRR

WETENSCHAPPELIJKE RAAD VOOR HET REGERINGSBELEID

Tweede Kamer corona-app – position paper vanuit de WRR

Ter inleiding

De Wetenschappelijke Raad voor het Regeringsbeleid (WRR) werkt momenteel aan een rapport over kunstmatige intelligentie, ook wel AI, en publieke waarden. Daarnaast heeft de WRR de afgelopen jaren verschillende publicaties geschreven die (mede) over het gebruik van nieuwe technologieën gaan, zoals Voorbereiden op Digitale Ontwrichting (2019), Veiligheid in een wereld van verbindingen (2017), Big Data in een vrije en veilige samenleving (2016), iOverheid (2011) en Het betere werk (2020). Vanuit de WRR-expertise over nieuwe technologieën leveren wij in dit position paper een korte bijdrage aan het Tweede Kamerdebat over de introductie van een corona-app.

Als startpunt is het belangrijk op te merken dat nieuwe digitale technologieën de samenleving veel voordelen kunnen brengen. Ook tijdens de coronacrisis is de waarde daarvan gebleken. Voorbeelden zijn de snelle informatievoorziening, video-conferencing software, online leeromgevingen en bezorgdiensten. Dat de regering door middel van een app wil proberen digitale technologie verder in te zetten bij de bestrijding van de coronacrisis is op zichzelf dan ook heel begrijpelijk. Maar het is ook belangrijk daar kritisch naar te kijken.

Waken voor techno-optimisme

Cruciaal is dat een zorgvuldig proces in acht wordt genomen. In het bijzonder zijn er twee grote gevaren. Ten eerste is er het risico dat gehaast beslissingen worden genomen die op de lange termijn gevolgen hebben die dan moeilijker te verhelpen zijn dan wanneer ze aan het begin zorgvuldig overwogen worden, en die geen ruimte meer laat voor een alternatieve aanpak. Het tweede probleem is dat onvoldoende aandacht wordt besteed aan de inbedding in de sociale en technologische context. Wij lichten beide punten toe.

Risico 1: Langetermijngevolgen van gehaaste beslissingen

In een vroeg stadium wordt een nieuwe technologie vaak onvoldoende gereguleerd, omdat er veel optimisme is en er nog veel onzekerheid is over de werking en gevolgen ervan. In een later stadium is het echter moeilijk om het te reguleren, omdat belangrijke beslissingen al zijn

genomen en er vaak machtsstructuren zijn ontstaan die verandering moeilijk maken (het Collingridge-dilemma).

Het is bij een ingrijpende technologie dan ook van het grootste belang om vroegtijdig zoveel mogelijk valkuilen te identificeren, zoals:

- *Afhankelijkheid van de ontwikkelaar*. Bekend is dat grote technologiebedrijven ook aan een corona app werken (denk aan de samenwerking tussen Google en Apple). Rondom veel hedendaagse technologie speelt nu al de vraag naar afhankelijkheid van sterke buitenlandse spelers. Met deze gezondheidsdata is dit vraagstuk nog nijpender.
- *De relatie publiek-private belangen*. Naast de geografische dimensie speelt ook de vraag naar het type ontwikkelaar. Omdat het een publiek vraagstuk betreft is het belangrijk om vroeg stil te staan bij de vraag wat de effecten kunnen zijn van een vermenging met een commerciële logica, en daar heldere begrenzingen aan te stellen.
- *Mission creep*. Veel technologieën worden ontwikkeld voor een bepaald doel, maar ontwikkelen nieuwe toepassingen wanneer zij eenmaal geïnstalleerd zijn. Het betreft in dit geval een app voor een specifieke crisissituatie en het doel van de app, van de gegenereerde data en de duur van het gebruik ervan moet daarmee helder afgebakend zijn. Het lijkt erop dat coronamaatregelen voor de langere duur zijn in de anderhalve-metersamenleving. Het gevaar dreigt dan van gewenning, en vervolgens ook van verschuiving van doelen. Daarom is het van belang vooraf te definiëren waar de app niet dan wel nooit voor bedoeld kan zijn.
- *Democratische controle*. Een te gehaast proces kan dergelijke controle, ook achteraf, moeilijk maken. Onvoldoende zorg voor randvoorwaarden wat betreft de applicatie, het ontwikkeltraject en de broncode kan in een later stadium een obstakel zijn voor een geïnformeerd parlementaire debat.
- *Voortijding negeren van alternatieven*. Door snel te kiezen voor een app kunnen ook alternatieven die mogelijk beter zijn voortijdig worden genegeerd. De premier van Nieuw-Zeeland, bijvoorbeeld, heeft alle burgers gevraagd een dagboek bij te houden met de contacten die ze elke dag onderhouden, om te kunnen gebruiken bij contactonderzoek. En Massachusetts, schreef The New York Times, 'is the first state to invest in an ambitious contact-tracing program, budgeting $44 million to hire 1,000 people' (16 april 2020). We kunnen niet beoordelen of dit ook voor ons land goede ideeën zijn en weten niet of dit soort varianten in het OMT of de regering overwogen zijn.

Risicovol aan gehaaste beslissingen is, tot slot, ook dat zij verkeerde verwachtingen wekken. Alhoewel een appathon een veelgebruikte methode is om ideeën te genereren, is het slechts een rudimentaire stap in een groter proces. De uitkomst van veel appathons/hackatons wordt

dan ook vaak voorgesteld als ‘vaporware’: grote aankondigingen van technologieën die nooit ontwikkeld zullen worden of vooralsnog technisch niet haalbaar zijn.

Een andere verkeerde verwachting die door een gehaast proces kan ontstaan is het idee dat er een keuze gemaakt moet worden tussen langer thuis zitten en weer de straat op kunnen onder voorwaarde dat burgers hun data prijsgeven. Dit is een vals dilemma.

Risico 2: Onvoldoende aandacht voor inbedding
Een tweede vaak voorkomend probleem is dat technologieën in isolatie als oplossing worden beschouwd zonder voldoende rekening te houden met de context waarin zij geplaatst moeten worden. Zonder die contextualisering kunnen grote problemen ontstaan.

Het gaat ten eerste over de technologische context. Een app is afhankelijk van een set aan ondersteunende technologieën om goed te kunnen functioneren. In dit geval is een breed verspreid gebruik van smartphones vereist, en dat is – zeker bij oudere en minder vermogende doelgroepen – niet vanzelfsprekend. Er zijn voldoende gebruikers van de app nodig om netwerkeffecten te generen. Een goed-dekkend communicatienetwerk is ook van belang, wat juist in drukbezochte gebouwen een probleem kan zijn. Bluetooth is een veelgenoemde ondersteunende technologie voor de geplande app, en daar speelt o.a. de vraag of nabijheid een adequate representatie is van besmettingsgevaar (denk aan het voorbeeld van een buur die achter een muur minder dan een meter afstand kan hebben). Zelfs als een app naar behoren functioneert, kan onvoldoende aandacht voor deze technologische context het functioneren daarvan ondermijnen.

Naast de technologische is ook de maatschappelijke inbedding in de sociale context van groot belang wat verschillende dimensies kent:

- *Juridisch*. Het gaat o.a. om de juridische context. In verschillende fora is aandacht gevraagd voor privacy, keuzevrijheid en de gevaren van profilering van burgers. Wanneer de App bovendien niet voldoende nuttig blijkt is het mogelijk dat een gerechtvaardigd belang van het willen opsporen van besmettingsgevallen zich niet verhoudt tot de inbreuk die daarmee wordt gemaakt op de privacy van burgers
- *Vertrouwen*. Een gevaar is dat mensen blind gaan vertrouwen op de werking van een technologie, waardoor burgers zich roekelozer gaan gedragen. Een bekend voorbeeld hiervan is Tesla’s zogenaamde Autopilot-functie. In de gebruiksaanwijzing staat dat de bestuurder hierbij verantwoordelijk blijft voor het besturen, maar veel bestuurders handelen daar niet naar, met verschillende ongelukken tot gevolg. Ook de corona app

waar nu sprake van is, mag geen vervanging worden van gezond verstand, en juiste communicatie is van het grootste belang.

- *Bedrog*. Rekening houden met de context van menselijk gedrag houdt ook in dat de mogelijkheid van bedrog serieus wordt genomen: mensen die elkaars telefoon gebruiken, de telefoon bewust thuis laten liggen, of de grenzen van de app willen verkennen.
- *Macht*. Hoewel gecommuniceerd is dat de overheid de app niet verplicht, bestaat het risico dat partijen als werkgevers of vervoersorganisaties installatie van de app als voorwaarde voor toegang gaan inzetten, waarmee de weg geopend wordt naar 'zachte dwang', misbruik van machtsposities en ongelijkheid van mogelijkheden.

Conclusie

Samenvattend zijn grote voorzichtigheid en zorgvuldigheid geboden bij de eventuele introductie van een ingrijpende nieuwe technologie. Gewaakt dient te worden voor wat wel 'techno-optimisme', 'techno-chauvinisme' of 'techno-solutionisme' genoemd wordt: het idee dat de introductie van een nieuwe technologie op zichzelf een oplossing kan bieden voor complexe weerbarstige maatschappelijke vraagstukken. Er zijn veel voorbeelden van projecten waarbij dit tot zeer problematische gevolgen heeft geleid.

Inhoudsopgave

AMNESTY INTERNATIONAL

Afdeling Nederland
Keizersgracht 177
Postbus 1968
1000 BZ Amsterdam

T 020 626 44 36
F 020 624 08 89
E amnesty@amnesty.nl
I www.amnesty.nl

Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA Den Haag

Datum
20 april 2020

Onderwerp
Position paper Amnesty International t.b.v. hoorzitting corona-app

Ons kenmerk

Uw kenmerk

Geachte Kamerleden,

Amnesty International wil graag waardering uitspreken voor de actieve controlerende rol die uw Kamer op zich neemt waar het gaat om de inzet van technologie in de bestrijding van het coronavirus. Technologie kan een belangrijke rol spelen in deze bestrijding. Maar dat mag niet ten koste gaan van mensenrechten. Amnesty International wil benadrukken dat er meer mensenrechtenrisico's verbonden zijn aan de inzet van apps in de virusbestrijding dan alleen de privacy, namelijk discriminatie. Deze risico's worden alleen maar versterkt door het hoge tempo waarmee dit proces doorlopen wordt. Amnesty heeft dit proces op afstand kritisch gevolgd.

Met deze *position paper* wil Amnesty International uw Kamer enkele voorwaarden meegeven voor het gebruik van apps. Graag wijzen wij u erop dat het moment van indienen van deze *position paper* maandag 20 april 15.00 uur is, dus nog voordat het kabinet een besluit neemt over een volgende stap voor de inzet van apps.

Apps mogen niet leiden tot ongelijke behandeling
Zoals gezegd hebben dergelijke apps naast de terecht grote zorgen over privacy potentieel meer risico's op mensenrechtenschendingen. Het gebruik van de app moet vrijwillig zijn en mag dus nooit verplicht worden gesteld door de overheid. Ook moet er een verbod komen op het verplicht stellen van de app door derden.

Vrijwillig betekent ook dat niemand behalve zorgverleners mogen vragen naar de risicoscore van de app. De risicoscore van de app is niets meer dan een inschatting en geeft een vertekend beeld buiten de context van *contact tracing*. Bijvoorbeeld in wijken met een lage sociaal-economische status wonen mensen veel dichter op elkaar in kleine rijtjeswoningen of flats. Hierdoor zullen bewoners meer signalen ontvangen van personen met wie zij nog nooit in contact zijn geweest, zogeheten *false-positives* die hun risicoscore omhoog krikken. Indien de risicoscore mag leiden tot een andere behandeling van een individu door niet-zorgverleners kan dit al snel leiden tot ongelijke behandeling en discriminatie op basis van economische positie.

Amnesty International werkt voor mensenrechten. Die waarborgen vrijheid, gelijkheid en rechtvaardigheid. Amnesty doet onderzoek, voert actie en steunt verdedigers van mensenrechten wereldwijd.

Vrijwilligheid betekent daarnaast dat het belonen of straffen van appgebruik moet worden verboden. Dit belonen zou bijvoorbeeld kunnen door het geven van korting op producten of diensten, het straffen door een hogere prijs te vragen bij geen appgebruik. Mensen die in armoede leven moeten dan noodgedwongen voor appgebruik kiezen. Dat is geen vrije keuze.

Apps mogen niet leiden tot surveillance

Contact tracing leidt gemakkelijk tot massa-surveillance omdat contact- en bewegingspatronen van individuen worden gemonitord door de overheid of door bedrijven. Dit is ontoelaatbaar. Te meer nu er privacy-vriendelijke opties bestaan. Echter, ook *contact tracing* met apps die aan de eisen voldoet van Veilig Tegen Corona openen de deur voor massa-surveillance. Deze risico's kunnen niet door de technologie worden opgelost en worden ook niet afgevangen door het naleven van de privacywetgeving, zoals de Avg. Voordat *contact tracing* wordt ingevoerd in Nederland moeten de volgende gevaren van surveillance en voor ongelijkheid zijn uitgesloten.

Ook moet er een verbod komen op *contact tracing* door anderen dan de overheid. De kans is reëel dat een eventuele *contact tracing*-app gebruik gaat maken van de Google en Apple API. Deze bedrijven zijn nu bezig met de ontwikkeling van die tool. Amnesty roept de overheid op om deze bedrijven deze tool zo te laten ontwerpen dat gebruikers het bijhouden van databases en het uitzenden van signalen altijd zelf aan of uit kunnen zetten. *Privacy by design* en *privacy by default* moeten ook in deze tool het uitgangspunt zijn.

Contact tracing infrastructuur mag niet voor een ander doel dan virusbestrijding gebruikt worden. Door *contact tracing* te promoten als overheid, spoor je mensen aan om de hele tijd signalen uit te zenden. Die uitgezonden signalen kunnen ook voor andere doeleinden worden gebruikt dan *contact tracing*. Bijvoorbeeld door werkgevers die willen weten of hun werknemers een hoog risico hebben, door Google die afluistert via "smart" home producten of door winkels om mensen te volgen en te analyseren en die gegevens eventueel te combineren met online profielen. Dit moet verboden worden. De *contact tracing*-infrastructuur mag niet worden hergebruikt voor andere doeleinden. De AVG regelt het hergebruik van data en kan dus niet het hergebruik van infrastructuur reguleren. Hier moet een apart verbod op komen.

Apps mogen niet werken op oncontroleerbare kunstmatige intelligentie

Een van de geselecteerde apps die gepresenteerd werd op de 'appathon' stelde een platform voor waarbij gebruikers zelf data kunnen doorsturen die gebruikt kunnen worden voor analyse met behulp van (zelflerende) algoritmes. Overheidshandelen moet controleerbaar en voorspelbaar zijn, zeker wanneer hier rechtsgevolgen aan verbonden zijn, het individuen in aanmerkelijke mate treft, of een grote impact heeft op mens of maatschappij, zoals een besluit over coronamaatregelen. Het gebruik van zelflerende algoritmes impliceert verminderde controle op het overheidshandelen. Hierdoor passen zelflerende algoritmes niet bij de uitvoering van dit type overheidstaak. Daarnaast biedt het huidige wettelijk kader te weinig mensenrechtenbescherming voor het gebruik van algoritmes in de uitvoering van de overheidstaken. Zie voor het verdere standpunt van Amnesty International over AI, algoritmes en mensenrechten deze *position paper* aan Kamercommissie Digitale Toekomst.

Middels dit schrijven willen we u vragen er bij het kabinet op aan te dringen zich te bezinnen voordat er verdere stappen genomen in dit proces. Welk probleem lost een dergelijk app op? Wat is de bewezen effectiviteit? En wat is de impact op mensenrechten in brede zin? Hierbij roepen we u op om bovengenoemde mensenrechtenwaarborgen mee te nemen in dit proces.

Hoogachtend,

Merel Koning
Senior Medewerker Tech & Mensenrechten Amnesty International

Inhoudsopgave

Tweede Kamer
DER STATEN-GENERAAL

Selectie krantenartikelen

/

Ministerie kleunt mis met appathon

NRC.NEXT

20 april 2020

Byline: Rik Wassens

Analyse Corona-app

Zeven partijen mochten dit weekend een corona-app presenteren, die onder grote druk was ontwikkeld. Geen enkele was goed genoeg.

VOLLEDIGE TEKST:

Een kritisch rapport van KPMG over de informatieveiligheid van de voorstellen, de landsadvocaat die zegt dat niet kan worden vastgesteld of een van de voorgestelde apps voldoet aan de privacywetgeving, halve of geen gedeelde broncode en negen geconsulteerde experts die inmiddels hun handen van het selectieproces aftrokken; te gehaast, te chaotisch, te veel fundamentele vragen.

Er is veel aan te merken op de zoektocht van het ministerie van Volksgezondheid naar slimme technologie die moet helpen bij de bestrijding van het coronavirus - die dit weekend eindigde in een tweedaagse 'appathon', waarbij de overgebleven voorstellen onder hoog tempo verbeterd moesten worden. De afvalrace begon ruim een week geleden in hoog tempo; 750 ondernemers reageerden in het paasweekend op de oproep van het ministerie om ,,slimme digitale oplossingen" aan te leveren. Drie dagen later waren er zeven over. De voorkeur is duidelijk: slechts één voorstel bevatte niet direct een contact- en traceerapp gebaseerd op bluetooth, waarmee vrijwel elke telefoon uitgerust is.

Het is de hoop van de overheid dat zo'n app in de volgende fase van de bestrijding van het coronavirus een wezenlijke bijdrage kan leveren aan het bronnen- en contactonderzoek van de GGD. Door de wijde verspreiding van Covid-19 is het reguliere GGD-onderzoek ontoereikend. Een app kan een belangrijke rol spelen om dit onderzoek ,,in ere te herstellen", zei minister Hugo de Jonge (Volksgezondheid, CDA) zaterdag tegen NRC. Zonder app blijft Nederland mogelijk langer op slot. Haast is geboden. Bewegingsvrijheid inperken is óók een rigoureuze maatregel, zei de bewindsman.

Die haast zette een belangrijke voorwaarde voor het slagen van een contact- en traceerapp op het spel: draagvlak. Zonder de medewerking (dwang sloot De Jonge dit weekend uit) van het merendeel van de Nederlanders zijn er te veel zwarte plekken en blijft het coronavirus ongrijpbaar voor iedere app - hoe goed of slecht die ook werkt.

Privacyorganisatie Bits of Freedom beëindigde in een vroeg stadium de samenwerking met het ministerie vanwege ,,het moordende tempo", ook omdat er veel op het spel staat.

De haast wreekte zich tijdens de appathon, toen zondag een datalek bij één van de voorstellen opgemerkt werd door RTL Nieuws. ,,Binnen een half uur werd ons gevraagd onze broncode te uploaden", zegt ontwikkelaar Sander de Vries. Er kwam per ongeluk ook een interne database mee.

'Extreem onder druk'

Het is makkelijk de appathon te bekritiseren door de gemaakte fouten. Filmpjes die niet goed starten, beeldverbindingen die niet werken. En de opgelegde tijdslimieten, bewaakt door een belletje, steken schril af tegen de potentiële impact die een corona-app op het dagelijkse leven kan hebben. ,,Dit is de professionaliteit die je krijgt als je mensen extreem onder druk zet", zegt de geconsulteerde en kritische IT-expert Brenno de Winter.

Tegelijk heeft de overheid zich nog nooit zo publiekelijk via livestreams in de kaart laten kijken bij een groot IT-project. Nederlandse softwareontwikkelaars, verenigd in Code For NL, spraken zondag in een verklaring van ,,een uniek

moment". ,,We denken dat dit een aanzet is tot een model dat in de toekomst, zij het onder minder hoge druk" kan leiden ,,tot een optimale samenwerking tussen overheid en maatschappij".

Alleen had de appathon met de voorkeur voor een bluetooth-app het verkeerde vertrekpunt, zegt appathon-deelnemer De Vries. Die techniek is eigenlijk te onnauwkeurig. Ook de landsadvocaat concludeerde dat het risico op vals-positieven bij geen van de voorstellen voldoende wordt ondervangen. Voor halverwege mei hebben Apple en Google verbeteringen aangekondigd die bluetooth betrouwbaarder moeten maken voor contact- en traceerapps.

Negen experts trokken zich terug uit het selectieproces: te chaotisch en te veel fundamentele vragen

Nog geen geschikt ontwerp voor corona-app

Trouw

20 april 2020 maandag

Byline: WENDELMOET BOERSEMA, REDACTIE POLITIEK
Highlight: data - Er is nog geen kandidaat voor de corona-app die aan alle eisen voldoet, erkende de overheid gisteren.
Experts hadden al kritiek op de haast waarmee het ministerie een corona-app wil ontwikkelen. Ze kregen dit weekend tijdens een 'appathon' gelijk: de zeven geselecteerde ontwerpen vertonen nog te veel gebreken. Het kabinet had graag morgen al een keus willen maken.

Na twee dagen livesessies met vragen, pitches en technische verbeteringen moest ook het ministerie van volksgezondheid erkennen: zo snel gaat het niet met de corona-app. Het ministerie had er dit weekend een heuse appathon voor georganiseerd, waarbij iedere bezoeker vragen kon stellen en oplossingen aandragen. Duizenden mensen deden mee. Daarmee zou de app deze week al gereed moeten zijn, maar dat lukt dus niet.

Er werd flink ingehakt op de zeven geselecteerde ontwerpen. Een van de spaanders die daarbij in het rond vloog, was een datalek bij een van de kandidaten, de Covid19 Alert. In de grote haast om de broncode (het ontwerp van de software) openbaar te maken, was korte tijd een bestandje met zo'n tweehonderd persoonsgegevens zichtbaar dat eigenlijk verwijderd had moeten worden. Een open broncode is een eis van het kabinet, maar twee van de zeven apps konden daar nog niet aan voldoen.

Het tekent de grote haast waarmee coronaminister Hugo de Jonge een corona-app wil introduceren. Zo'n app voor mobieltjes is een onmisbaar onderdeel van de kabinetsstrategie om het coronavirus onder controle te krijgen. Vooral als straks de kinderen weer naar school gaan en mensen weer voorzichtig aan het werk mogen. De app helpt GGD-medewerkers na te gaan met wie een besmet iemand contact heeft gehad. Dat werk is straks onmogelijk allemaal handmatig uit te voeren.

Ter voorbereiding op het weekend bracht De Jonges ministerie van volksgezondheid donderdag in één dag het aantal van 63 serieuze inzendingen voor ontwerpen van de app terug tot zeven. De it- en privacy-experts die bij deze selectie meehielpen, uitten vrijdag in een openbare brief al hun twijfels. Volgens hen was volstrekt onduidelijk wat de selectiecriteria zijn. Onder de zeven kandidaten zijn enkele die de experts afkeurden, terwijl betere ontwerpen ontbreken, stellen ze. Ook privacy-organisaties als Bits of Freedom en Platform Burgerrechten roepen de minister op terug te gaan naar de tekentafel.

De ontwerpen die bij de appathon onder het vergrootglas lagen, zijn afkomstig van grote bedrijven als Accenture, DTACT en SIA. Zo stopte SIA de app uit Singapore in een nieuw jastje. De app Covid19 Alert is een Europees non-

profit-initiatief. Sommige apps zijn in elders al in gebruik, zoals die van Accenture. Hun ontwerp, in opdracht van het Rode Kruis in Oostenrijk, ging als eerste live in Europa.

Tijdens de sessies stelden de deelnemers vooral vragen over de privacy. Wie voert de gegevens in en hoe is dat proces beveiligd? Kan een hacker chaos voorzaken met een valse melding? Hoe nauwkeurig is de afstelling van de app? De meeste ontwerpen werken met bluetooth, waarbij afstand en duur van het contact met een ander mobieltje worden opgeslagen, maar de locatiedata niet. Zorgen zijn er over de nauwkeurigheid van bluetooth. Dat kan namelijk zorgen voor een hoop onrust doordat er bij te ruime criteria te veel meldingen komen. Bij alle ontwerpen zullen zorgmedewerkers de data over besmettingen invoeren, met beveiligingscodes.

"De ontwerpen moeten nog van een zeven naar een tien", gaf minister De Jonge zaterdagavond al toe. De conclusie is nu dat in alle apps nog beveiligingsproblemen zitten en zelfs beginnersfouten.

De Autoriteit Persoonsgegevens zou vandaag nog met een oordeel over de zeven geselecteerde apps komen, maar de vraag is of dat al zin heeft. Het kabinet stelt het doorhakken van de knoop nu uit. Na de keus begint nog de grootste klus: hoe overtuigt het kabinet burgers de app ook daadwerkelijk op hun telefoon te installeren? Meedoen blijft vrijwillig, heeft premier Rutte beloofd. Ook is nog onduidelijk hoeveel mensen er nodig zijn om alle gegevens in te voeren en te verwerken.

Corona-app lijkt verder weg na weekendje pitchen

Het Financieele Dagblad

20 april 2020

Byline: Hella Hueck, Martijn Pols en Stijn van Gils

Het hele weekend hebben zeven bedrijven hun voorstellen gepresenteerd en aangescherpt om een privacy-veilige corona-app voor de overheid te mogen ontwikkelen. Maar een winnaar is er voorlopig nog niet.

Alle vergaderkamertjes op het ministerie van Volksgezondheid zijn zaterdagmiddag bezet. Experts houden video-interviews met ondernemers die stellen dé ultieme corona-app te kunnen maken. In de gangen is het te druk. Anderhalve meter afstand houden van elkaar is niet te doen.

Heel Nederland kan met de bijeenkomst meekijken via YouTube, een paar duizend mensen doen dat ook echt.

Ron Roozendaal, directeur Informatiebeleid bij het ministerie is de organisator van de 'appathon', zoals de tweedaagse is genoemd. Hij probeert tussen alle interviews door nog even broodje te eten. De grote vraag: gaat zo'n app echt helpen? 'Het echte antwoord is: dat weten we niet precies', vertelt hij.

Als Nederland dadelijk weer van het slot gaat en de winkelstraten, terrasjes en parken weer volstromen, is de kans aanwezig dat het coronavirus weer de kop opsteekt. Dan zou een app kunnen helpen bij bron- en contactopsporing, legt Sjaak de Gouw, directeur publieke gezondheid van GGD Nederland uit.

'Het is voor ons veel uitzoekwerk wie er allemaal op een bepaald tijdstip in een café stonden.' Een anoniem berichtje naar iedereen die met een coronapatiënt in aanraking is geweest, moet 'de werkdruk van de GGD ontlasten'.

Om de verspreiding van het virus in te dammen, is volgens de De Gouw meer nodig. 'Om de besmettingshaard te vinden moeten we weten wáár precies in Nederland de besmetting heeft plaatsgevonden. Daarvoor moeten we weten waar de patiënt precies is geweest.' Het verzamelen van locatiegegevens zal op veel maatschappelijke weerstand stuiten.

Eerste corona-apps 'slordig haastwerk'

De appathon is vooraf al overladen met kritiek, en dat hield afgelopen weekend aan. Het lijkt wel het tv-programma Dragon's Den, met pitches, jury's en panels, in plaats van een zorgvuldig proces te volgen, zeggen critici. Zo'n snel in elkaar getimmerde beautycontest moet wel onzorgvuldigheid in de hand werken, vinden Platform Burgerrechten en Bits of Freedom. 'Het evenement had meer weg van een spelshow waar bedrijven met elkaar strijden dan een serieuze aanbesteding ...', schrijft digitale burgerrechtenvereniging Bits of Freedom op zijn site.

Vrijdag trokken negen experts die betrokken waren bij het beoordelen van de ruim 700 ideeën zich terug omdat ze de maatstaven waar de app aan moet voldoen onduidelijk vinden. Gisterochtend vond RTL Nieuws bij een van de deelnemers, Covid19-Alert, zelfs een datalek. De ontwikkelaars publiceerden per abuis een bestand met zo'n tweehonderd namen, e-mailadressen en versleutelde wachtwoorden, terwijl juist privacy en beveiliging bij de apps zo gevoelig liggen.

De kritiek dat de overheid via YouTube een soort songfestival met stemmen en likes organiseert om een gezondheidscrisis op te lossen, werpt ambtenaar Roozendaal verre van zich: 'De enige manier om dit goed te doen is om heel transparant te zijn. Dat betekent ook harde kritiek krijgen. Het is juist belangrijk dat mensen kunnen meekijken.'

Ook minister Hugo de Jonge is aanwezig. Hij benadrukt nog maar een keer dat de app technisch volledig veilig moet zijn, ook voor de privacy. Lukt dat niet, dan komt er geen app, zegt hij. Serieuze alternatieven zijn er volgens hem niet. En de overheid had vorige week wel degelijk breed uitgevraagd, stelt hij. Het hoefde geen app te zijn, andere technische oplossingen konden ook.

Het beursgenoteerde CM.com uit Breda kwam bijvoorbeeld met een voorstel om met een soort chatbot het contactonderzoek grotendeels te automatiseren. Maar een dergelijke oplossing viel af bij de voorselectie. Hiermee is het niet mogelijk om vluchtig contact met onbekenden in kaart te brengen, vertelt minister De Jonge.

Het gebruik van de app zal sowieso vrijwillig zijn. Daarin is De Jonge naar eigen zeggen 'opgeschoven'. Eerder sloot hij niet uit het te verplichten, bij een te lage dekking. 'Maar als we dit niet hebben, dan zijn we minder effectief (in het tegengaan van het virus, red.) en zullen we langer dan noodzakelijk allemaal ingrijpende maatregelen moeten nemen.'

Hoe toezichthouder Autoriteit Persoonsgegevens oordeelt over de apps wordt vandaag duidelijk, morgen houdt de Tweede Kamer een hoorzitting met experts op dit terrein.

Minister de Jonge mikte op een werkende app eind deze maand. Gisteren aan het einde van de middag tempert secretaris-generaal Erik Gerritsen de verwachtingen. 'Ik heb nog geen expert horen zeggen: we hebben al voldoende informatie om te kiezen. Als je dat al zou willen.'

Harm Erbe van Capgemini is op een scherm te zien in de 'regiekamer' op het ministerie van Volksgezondheid tijdens het corona-app-voorstelweekend.

Kritiek op selectieprocedure corona-app

NRC.NEXT

18 april 2020

Byline: Rik Wassens

Technologie

Er zijn nog zeven kandidaten voor het maken van een corona-app. Experts zijn bezorgd over de privacy bij sommige ontwerpen.

Eerste corona-apps 'slordig haastwerk'

VOLLEDIGE TEKST:

Er komt steeds meer kritiek op de gehaaste zoektocht van het ministerie van Volksgezondheid naar een corona-app voor Nederland. Vrijdag werden zeven kandidaten bekend, na een afvalrace die een week geleden met 750 voorstellen begon.

Na de bekendmaking van de shortlist keerden meerdere privacy- en ICT-experts zich tegen het selectieproces van het ministerie van Volksgezondheid, dat in hun ogen te haastig en chaotisch verloopt. IT-specialist en privacy-expert Brenno de Winter, een van de 67 experts die het ministerie gaandeweg consulteerde, is teleurgesteld. ,,Ik vond de sfeer positief. De teleurstelling kwam aan het einde van de dag, bij de afsluitende sessie. Toen realiseerde ik me, o mijn god, jullie gaan doen waar je zin in hebt."

De shortlist bevat volgens acht betrokken experts voorstellen die zij expliciet hadden afgekeurd. Terwijl apps die zij inschatten als kansrijk nu ontbreken, om onduidelijke redenen. De 'gelegenheidscoalitie' Veilig Tegen Corona - waar onder meer privacyorganisatie Bits of Freedom deel van uitmaakt - roept het ministerie ,,dwingend" op om terug naar de tekentafel te gaan. De Winter: ,,Het begint te rieken naar onbehoorlijk bestuur."

De zeven geselecteerde voorstellen zijn ingediend door gevestigde IT-consultants (Accenture, Capgemini), of het zijn bestaande apps uit Singapore en België. Ook is er een initiatief uit Duitsland. Twee Nederlandse bedrijven dingen nu nog mee: het Amsterdamse softwarebedrijf DEUS - gespecialiseerd in kunstmatige intelligentie - en databedrijf DTACT.

'Slechts twee apps veilig'

Volgens geraadpleegd expert Tom Demeyer van Waag, een onderzoeksinstiuut voor kunst, technologie en samenleving, keurden diverse experts het voorstel uit Singapore af. ,,Het voorstel van SIA-group bood geen enkele privacygaranties." Slechts twee van de zeven voorstellen voldoen volgens hem aan de eisen van Veilig Tegen Corona. ,,Nog niet volledig. Maar die wil je dan een kans geven."

Het ministerie maakte zelf de eerste schifting en legde uiteindelijk 63 voorstellen voor aan de experts, waarvan vooral de privacy-experts en informatici zich nu publiekelijk roeren. Ook epidemiologen en experts uit de gezondheidszorg zaten in de panels.

Onder de afvallers zaten veelbelovende inzendingen, zegt Demeyer en het is niet duidelijk waarom die niet geselecteerd werden. Bert Hubert van PowerDNS stuurde ook een concreet voorstel in en is teleurgesteld. ,,Ik wil ook niet al te veel zeuren, maar een inzending van Fox-IT en Intermax - de grootste medische hoster in Nederland - negeren, is ook wel bruut. Ik kreeg alleen maar een automatische ontvangstsbevestiging."

Hoewel niet van alle zeven geselecteerde voorstellen duidelijk is waar het precies om gaat, lijken veel partijen Bluetooth te willen gebruiken om een logboek van recente contacten aan te leggen. Als een van die contacten besmet blijkt met het virus, ontvangen anderen die recent contact hebben gehad een waarschuwing.

Dat kan met een hoge mate van privacy, maar er zijn ook twijfels of de techniek goed genoeg werkt om de besmettingen na te trekken. Volgens De Winter was er weinig ,,ruimte of appreciatie" voor het temperen van de ,,hooggespannen verwachtingen" rond Bluetooth. ,,Het leek de hoogmis van het techno-optimsime."

De belangrijkste vraag, over de noodzaak en de potentiële effectiviteit van de apps, stond volgens Demeyer niet ter discussie. ,,De hele wereld bouwt op Bluetooth, waarvan de effectiviteit onbewezen is. Singapore stelt dat de app in feite geen oplossing is. En toch gaan wij hier met zijn allen Bluetooth-apps beoordelen."

Rejo Zenger van Bits of Freedom noemde het selectieproces in een blogpost ,,gehaast en chaotisch". ,,De vooraf bepaalde agenda was onbespreekbaar en procesvragen werden niet beantwoord. Heldere criteria ontbraken, en er was geen tijd om deze af te stemmen waardoor de beoordelingen sterk uiteenliepen."

Appathon gaat door

Eerste corona-apps 'slordig haastwerk'

Het ministerie van Volksgezondheid lijkt ondanks de kritiek op de selectie het proces door te zetten. Dit weekend moeten de zeven voorstellen zich presenteren tijdens een 'appathon' die zaterdag begint met elevator pitches.

Tijdens de appathon worden prototypen van de voorstellen digitaal aan het publiek voorgelegd, dat commentaar kan geven en vragen kan stellen. De broncode van de voorstellen wordt ook gecontroleerd. Experts van binnen en buiten de overheid kijken mee en stellen vragen. Maar een aantal van hen hebben inmiddels bedankt, zegt Demeyer: ,,Je wordt bijna als excuus gebruikt en daar passen we voor." Zondag om 16.00 uur is de laatste demonstratie.

De hoop van de regering is dat de apps meer grip geven op de verspreiding van het virus, als de maatregelen na 28 april - eventueel - verlicht worden. Verbeterd, versneld contactonderzoek met een grotere capaciteit moet nieuwe uitbraken van Covid-19 in kaart brengen en isoleren, om zo te voorkomen dat de ziekenhuizen opnieuw overbezet dreigen te raken.

Hoewel haast geboden is, mag snelheid de zorgvuldigheid niet in de weg staan, schreef minister Hugo de Jonge (Volksgezondheid, CDA) eerder deze week in een brief aan de Tweede Kamer. ,,En net zo belangrijk: de inzet van digitale oplossingen moet noodzakelijk en zinvol zijn in de bestrijding van het Covid-19 virus." Het ministerie van Volksgezondheid vulde vrijdagavond in een reactie aan dat niet iedere expert dezelfde voorstellen heeft gezien. ,,Het is dus mogelijk dat er initiatieven meedoen aan de appathon waar sommige experts niet achter staan. Zaterdag en zondag zal moeten blijken of deze initiatieven inderdaad niet voldoen en dus zullen afvallen."

Ook de Tweede Kamer is kritisch over de corona-apps. Woensdag organiseert de kamer een hoorzitting over de corona-app en worden deskundigen naar hun mening gevraagd.

De Autoriteit Persoonsgegevens onderzoekt de zeven voorstellen om te zien of ze zich aan de privacywet houden. Maandag wordt het oordeel van de toezichthouder verwacht. De Winter verwacht dat het ,,niet heel erg feestelijk zal zijn".

Een dag later, dinsdag 21 april, neemt het kabinet een besluit over hoe en óf er verder gegaan wordt met de apps. Demeyer hoopt dat de regering meer tijd neemt. ,,Probeer het niet in twee dagen dit helemaal uit de grond te stampen. Dat is veel te snel."

Onder de afvallers zaten volgens de experts juist veelbelovende inzendingen

'Straks leiden we zo'n corona-app massaal om de tuin'

de Volkskrant

18 april 2020

Byline: TONIE MUDDE
Highlight: Hoogleraar Lokke Moerel - specialisatie: tech en privacy - is kritisch op de kabinetsplannen met corona-apps. Privacy is nog een van de minst prangende problemen.

Interview Lokke moerel

Telefoon uit Brabant voor de echtgenoot van Lokke Moerel. Herinnert u zich die workshop die u gaf? Twee deelnemers hebben coronaverschijnselen.

Het gebeurde begin maart, de dag dat minister Rutte op televisie aan Nederlanders vraagt geen handen meer te schudden. Lokke Moerel en haar echtgenoot overleggen met elkaar. Zo'n workshop van een hele dag in één ruimte, handen schudden, samen lunchen; het risico op een infectie lijkt hun aanzienlijk. Ze besluiten zichzelf thuis in Amsterdam op te sluiten. Ze worden allebei ziek. Benauwdheid, knallende koppijn, wekenlang.

Eerste corona-apps 'slordig haastwerk'

De echtgenoot van Moerel vult elke dag temperatuur en symptomen in op de OLVG corona check, een app met ruim 100 duizend downloads. Medisch personeel beoordeelt de scores en biedt hulp op afstand. 'Nuttige app', vindt Moerel, hoogleraar aan de Universiteit van Tilburg, advocaat en door overheden en multinationals veelgevraagd expert op het gebied van ict en privacy. 'De app geeft inzicht in het verloop van klachten en het is een prettig idee dat artsen contact opnemen als je toestand verslechtert. Medisch experts kunnen deze data gebruiken om meer inzicht te krijgen in het ziekteverloop en de verspreiding van het virus. De privacy is bovendien goed gewaarborgd.'

Bij een ander type corona-app - die in de gaten houdt met wie je contact hebt en alarm slaat als je in de buurt bent geweest van iemand met een corona-infectie - heeft Moerel meer bedenkingen. En laat dit nou precies het type tracing app zijn waar minister Hugo de Jonge zijn zinnen op heeft gezet. Dit weekend organiseert zijn ministerie een zogeheten appathon, om dit soort apps te testen. Volgende week beslist hij of en hoe de apps kunnen helpen om het virus in te dammen.

Waarom maakt u zich zorgen over zo'n tracing app?

'Kijk naar Singapore, dat nu in lockdown is ondanks het gebruik van zo'n app. Hier beoordeelt de app of je gedurende dertig minuten op minder dan 2 meter afstand van iemand bent geweest die later corona blijkt te hebben. Zo ja, dan krijg je een signaal dat je mogelijk zelf ook bent besmet. Privacy kun je inbouwen, maar hoe betrouwbaar is zo'n app? Als ik één minuut met een coronageïnfecteerde zoen, raak ik vast besmet, maar slaat de app geen alarm. En bluetooth (een draadloze verbinding die nabijheid tot andere telefoons kan bepalen, red.) werkt door glas heen. Daardoor kan de app een signaal afgeven, terwijl mijn oma al die tijd achter het raam stond. Zo'n app biedt vooral schijnveiligheid. Bovendien zou de meerderheid van de bevolking haar moeten installeren en goed gebruiken. Twijfelachtig of dat lukt.'

Idee: heel Nederland installeert verplicht die corona-apps. Ben je gezond en met niemand in contact geweest met een coronabesmetting, dan mag je weer naar je werk en het café. En anders moet je twee weken thuiszitten tot de kust weer veilig is. Zo kunnen we het land tenminste weer op gang krijgen.

'Je schetst het als een positief scenario, maar dit is precies het gevaar van zo'n app. Ook als de app vrijwillig is, zullen werkgevers een 'groene code' eisen voor je naar kantoor mag. Dat zijn zeer ingrijpende gevolgen op basis van een extreem foutgevoelig systeem. Nu moet iedereen afstand houden, maar als sommigen wel naar het café mogen en anderen niet, dan gaan mensen massaal in hun eigen voordeel zo'n app om de tuin leiden. Even je telefoon of bluetooth uitzetten als je anderen ontmoet. Andermans mobiel meenemen als je de trein wil nemen. De monitoring die nodig is als je zulk gedrag wil bestrijden, door te controleren of mensen hun mobiel bij zich hebben, loopt snel uit de hand.'

U bent zelf besmet geweest met het coronavirus. Had u anders gehandeld met zo'n tracing app op uw telefoon?

'Het had bij mij eerder averechts gewerkt. Stel, we hadden zonder context een anonieme melding gekregen: 'U bent in de buurt geweest van een coronageïnfecteerde', terwijl we goed afstand hadden gehouden. Waren we dan ineens in quarantaine gegaan? Nu kregen we een telefoontje van een bekende, waardoor we precies snapten hoe sterk de mate van contact was. Dan ga je handelen. Ik zie meer in een app die fungeert als een geheugensteun voor jezelf als je besmet blijkt. Waar ben je de afgelopen weken allemaal geweest en met wie heb je nauw contact gehad? Dan kun je al die mensen zelf informeren, waarna zij zelf ook weer eerder hun verantwoordelijkheid zullen nemen. Technologie is vaak vervreemdend, je kan je er makkelijker achter verschuilen.

'De app is niet de oplossing, maar kan alleen een hulpmiddel zijn. Je kunt hem ook niet los zien van allerlei maatregelen om de app heen. Wordt toegang tot openbaar vervoer afhankelijk van je score op de app? Komen er extra coronatestfaciliteiten om te voorkomen dat mensen onnodig twee weken thuis moeten zitten omdat hun telefoon

een valse melding geeft? Hoe mensen en organisaties in de dagelijkse praktijk reageren op zo'n app is complex, dat ontdek je niet in één testweekend waarin je je blindstaart op de app zelf.'

Ik zie meer in een app die fungeert als een geheugensteun voor jezelf

Negentig seconden voor een pitch

NRC.NEXT

20 april 2020

Byline: Kees Rottinghuis

Rik Wassens

Reportage Appathon

De zoektocht naar een app tegen het coronavirus moet vooral snel resultaat opleveren. De kritiek op het selectieproces groeit.

VOLLEDIGE TEKST:

Negentig seconden, langer mag de elevatorpitch van IT-bedrijf Accenture over hun corona-app niet duren. Maar de bel hoeft er zaterdag tijdens de 'appathon' niet aan te pas te komen. ,,Complimenten, dan kunnen we goed vaart maken vandaag", klinkt het dankwoord van de dagvoorzitter.

Tempo is dit weekend op het ministerie van Volksgezondheid het sleutelwoord in de zoektocht naar de app die kan helpen om de maatregelen van de 'intelligente lockdown' te verlichten. Centraal in bijna alle zeven ideeën staan bronnen- en contactonderzoek via een app, die via bluetooth recente contacten in kaart brengt.

In de hallen van het ministerie van Volksgezondheid in Den Haag zijn zaterdag tientallen ambtenaren, app-ontwikkelaars en experts druk in de weer en trekken ze van vergaderzaal naar vergaderzaal. Media en cameratechnici lopen in de smalle gangetjes af en aan over internet- en stroomkabels. In glazen hokjes en op afstand bevragen experts gegroepeerd in de panels 'veiligheid', 'privacy' en 'doelmatigheid' de voorstellen. Via een livestream konden geïnteresseerden meekijken en feedback geven. Zeker dertienhonderd vragen kwamen via e-mail binnen. De appathon werd zaterdag door zo'n 90.000 mensen bekeken, 24.000 lieten hun mening over de voorstellen achter via een speciale website van de Rijksoverheid.

Experts trekken zich terug

Intussen groeit de kritiek op het selectieproces, dat zeven dagen geleden begon met zo'n 750 voorstellen. Met als strikte voorwaarde: kan de app op 28 april klaar zijn voor gebruik? Sinds de bekendmaking van de selectie op vrijdag hebben negen betrokken experts - veelal informatici en privacydeskundigen - hun handen van het proces getrokken. Er was te weinig informatie en tijd om de voorstellen goed te toetsen, schreven zij vrijdag in een verklaring. Ze roepen minister Hugo de Jonge (Volksgezondheid, CDA) ,,dwingend" op om terug naar de tekentafel te gaan.

Voor een maatschappelijk debat is eigenlijk geen tijd, zei minister De Jonge zaterdag na afloop van de eerste dag van de appathon in gesprek met NRC. ,,Natuurlijk is het goed om debat te hebben, me dunkt dat er een behoorlijk levendig debat plaatsvindt. Maar de verspreiding van het virus wacht daar niet op." Snelheid is van belang, zegt hij. ,,Daarom hebben we gezocht naar apps die dicht tegen een livegang aan zitten." 67 experts keken tijdens de selectie mee, benadrukt De Jonge. Hij zit er niet zo mee dat er negen vertrokken. ,,Ieder bepaalt zelf de bijdrage die hij wil leveren."

Eerste corona-apps 'slordig haastwerk'

De vraag of een app wel noodzakelijk is in de strijd tegen het coronavirus stond niet ter discussie, zeiden betrokken experts eerder. Apps daarom helemaal terzijde schuiven, gaat De Jonge te ver. ,,Als je te snel zegt: zo'n app moet je dat wel willen, moet je bedenken wat daar de consequenties van zijn. Waarschijnlijk zul je langer in deze rigoureuze maatregelen blijven zitten."

Zondag zit de druk er nog steeds op, net als de hectiek. Een video van de verkeerde app wordt gestart, het telefoonnummer van een ontwikkelaar komt in beeld, die vervolgens gelijk gebeld wordt. Wat wel veranderd is, is de toon. De noodzaak van de app wordt afgezwakt. De nadruk ligt op het mógelijk gebruik van de app. Secretaris-generaal van het ministerie van Volksgezondheid Erik Gerritsen: ,,Als mogelijk onderdeel van een exitstrategie." Als hij de appathon afsluit zegt hij: ,,De hectiek en tijdsdruk hebben de nodige onrust veroorzaakt. Mensen denken: ze willen in één week tak, tak, tak en dan woensdag een app invoeren." Hij snapt dat beeld, ontstaan door ,,de pressurecooker-methode" van zo'n weekend.

Contactonderzoek herstellen

De bedoeling is dat de app het bronnen- en contactonderzoek van de GGD ondersteunt. Dat onderzoek moet ,,in ere hersteld worden", zei De Jonge. De vraag is alleen hoe, en of daarbij aan de strenge eisen op het gebied van privacy, informatieveiligheid en gebruiksgemak kan worden voldaan.

Er zijn nog grote verschillen tussen de zeven voorstellen, zegt Sjaak de Gouw, portefeuillehouder infectieziekten binnen GGD Nederland en aanwezig bij de appathon. Waar de gegevens opgeslagen worden, wat gedeeld kan worden, hoe de privacy gewaarborgd wordt. Welke gegevens de app überhaupt moet verzamelen. ,,Dat is minimaal een identificatienummer, de afstand tot andere telefoons en het tijdstip van het contact."

De Gouw heeft de voorkeur voor alle informatie die de GGD normaliter ook zou verzamelen. ,,Dat zou ons het meest helpen. Maar we moeten hier kiezen tussen de hoeveelheid gegevens en acceptatie van de app. Als het aan ons ligt, zo snel mogelijk en zo veel mogelijk data." De GGD weet hoe hiermee om te gaan, stelt hij. ,,Met soa's beschikken wij ook over data die niet zomaar op straat mogen komen te liggen."

Naast privacy, informatieveiligheid en toepasbaarheid binnen het werk van de GGD, is ook vrijwilligheid van de app van belang, zegt De Jonge. ,,Juist als je hard uitspreekt dat iets vrijwillig is, heeft de samenleving er meer vertrouwen in." Eerder wilde De Jonge het verplicht stellen van de app niet uitsluiten. ,,Dat is voor mij ook voortschrijdend inzicht geweest."

Het kabinet beslist dinsdag hoe en of er verder gegaan wordt, waarna de Tweede Kamer woensdag debatteert over de plannen. Ook de Autoriteit Persoonsgegevens onderzoekt de zeven voorstellen en zal deze maandag met een oordeel komen. Alleen als de app voldoet aan álle voorwaarden, zal het ministerie het gebruik overwegen. ,,We doen geen concessies", zei De Jonge. Het kan zijn dat het ministerie na de appathon met lege handen komt te staan. De Jonge: ,,Een echt goed alternatief is er in ieder geval niet. Je wilt hem juist gebruiken. Je hebt hem nodig."

Eerste corona-apps 'slordig haastwerk'

de Volkskrant

20 april

Byline: HASSAN BAHARA

Highlight: Publiek en deskundigen kregen afgelopen weekend zeven mogelijke corona-apps gepresenteerd. Er mankeerde nogal wat aan. 'Ik denk dat we nog geen winnaar hebben.'

Reportage presentatie apps

Het klonk veelbelovend: een zogenoemde 'appathon', uitgesmeerd over twee dagen, waarin zeven app-bouwers met strakke pitches het Nederlandse publiek ervan mochten overtuigen dat hun app het meest geschikte hulpmiddel is om het coronavirus in te dammen. Een onverdeeld succes werd het niet. Zondag eindigde de onderneming met een pijnlijk datalek, onduidelijkheid over privacywaarborgen, en onbeantwoorde vragen over het algehele nut van het project.

De appathon was de eindspurt van een traject dat vorige week was ingezet door het ministerie van Volksgezondheid, Welzijn en Sport (VWS). Die had techneuten opgeroepen een voorstel in te dienen voor een app die de GGD kan helpen bij het doen van contact- en bronondezoek naar het coronavirus.

Het evenement werd gehouden op het ministerie van VWS en was live te volgen via YouTube. De deelnemers kregen ieder negentig seconden om hun waar aan te prijzen. Wie de tijdslimiet overschreed, werd met een schelle pieptoon aangespoord snel af te ronden.

Van de meer dan zeshonderd ingediende voorstellen kregen uiteindelijk alleen it-bedrijven en (universitaire) samenwerkingsverbanden zoals CapGemini, Deus BV, Accenture, Sia Partners, Covid19, ITO en DDT Consortium de kans om hun werk nader toe te lichten.

Bluetooth

Veel apps bleken met bluetooth-technologie te werken. Met deze techniek krijg je een seintje op je telefoon wanneer je in contact bent geweest met iemand die is besmet. Er wordt dan gevraagd in zelfquarantaine te gaan. Ook privacyzorgen werden geadresseerd. Stuk voor stuk benadrukten de app-bouwers dat de persoonlijke gezondheidsinformatie bij hen in veilige handen is. Technische termen als 'toestemmingsinfrastructuren' en 'DP-3T-protocollen' moesten de leek ervan verzekeren dat hij niets heeft te vrezen.

Daarna mochten experts, van privacywatchers tot epidemiologen, gaten schieten in de voorstellen en de app-bouwers aansporen nog wat aan de privacywaarborgen en gebruikersvriendelijkheid te sleutelen. Zondag presenteerden de app-bouwers hun verbeterde apps en hoorden zij het eindoordeel van de experts. Dat was hooguit gematigd positief. Wat betreft de gebruikersvriendelijkheid leken de apps 'op de goede weg'. Maar wat betreft de privacywaarborgen was er nog 'werk aan de winkel'.

Of het grote publiek op dat verbeterwerk zal vertrouwen, is de vraag. Zondag meldde RTL Nieuws dat het een datalek had achterhaald in een van de zeven apps, Covid19Alert. In de broncode waren oude bestanden te vinden die namen, e-mailadressen en versleutelde wachtwoorden bevatten van een andere app.

Chaos bij selectie corona-apps, adviseurs trekken zich terug

Het lek illustreerde voor veel privacy-experts het slordige haastwerk rondom het project. Afgelopen vrijdag noemden zij in de Volkskrant de selectie van de zeven app-bouwers ondeugdelijk. Met name over Sia Partners - dat kwam met een voorstel voor een kopie van de corona-app uit Singapore - was veel onvrede wat betreft privacywaarborgen.

'Ik denk dat we na dit weekeinde kunnen concluderen dat we nog geen winnaar hebben', zegt expert Jelle Prins, die apps maakte voor onder meer Booking.com en Uber. 'Alle partijen zitten absoluut nog in de beginfase. Het zou dapper zijn van de overheid als ze dit erkennen. Ik denk dat we een stap terug moeten doen, dat we nogmaals naar de 600 inzendingen moeten kijken, met de experts, en dan een nieuw plan opstellen.'

Prins heeft ook zorgen over de beperkte effectiviteit van de apps op iPhones. Op deze toestellen werken apps die gebruikmaken van bluetooth alleen als ze op de voorgrond draaien. Dan ontvangen en verzenden ze informatie. Worden ze weggedrukt op de iPhone, dan ontvangen ze nog wel informatie maar verzenden ze zelf niks.

'Apple en Google hebben aangekondigd samen te werken om deze beperking op te lossen. Maar geen van de zeven partijen heeft het over deze beperkingen gehad, of de nieuwe mogelijkheden die Apple en Google bieden genoemd', zegt Prins.

Los van alle technische kwesties en privacy-gevoeligheid ziet Prins ook de distributie van de app als een onderbelicht probleem. Alleen als een overgrote meerderheid van Nederlanders de app gebruikt, zou die wellicht enig effect kunnen sorteren.

Meerderheid bevolking

'Helaas is geen van de partijen dieper ingegaan op het vraagstuk hoe we met deze app de meerderheid van de bevolking zullen bereiken', zegt Prins. 'Niet alleen moeten mensen weten van het bestaan van de app, ze moeten hem ook begrijpen en vertrouwen alvorens ze hem zullen installeren. Accenture meldde trots dat in Oostenrijk 3 procent van de bevolking hun app had geïnstalleerd. Feitelijk betekent dit dat van de dertig mensen die je op een dag tegenkomt, er maar eentje de app zal hebben. Als een van de andere 29 ziek wordt, zul je dat nooit weten.'

Een winnaar werd zondag niet aangewezen. Hoewel het publiek via een internetpoll liet weten positief te zijn over de apps, was Erik Gerritsen, secretaris-generaal bij het ministerie van VWS, na afloop van de appathon veel voorzichtiger. Volgens hem is een app weliswaar 'een mogelijk onderdeel van de strategie naar het nieuwe normaal', maar in beton gegoten is het nog niet. 'Ik heb nog geen expert horen zeggen: we hebben al voldoende informatie om te kiezen. Als je dat al zou willen.'

Chaos bij selectie corona-apps, adviseurs trekken zich terug

de Volkskrant

18 april

Byline: LAURENS VERHAGEN
Highlight: Onder enorme tijdsdruk heeft het kabinet zeven corona-apps uitgekozen die kans maken binnenkort in appwinkels te verschijnen. Adviserende experts voelen zich in hun hemd gezet en nemen afstand van de lijst.
Vrijdag kwam het kabinet met zeven gegadigden voor het leveren van één of meerdere officiële corona-apps, waaronder Covid19 (een bestaande app), Sia Partners en grote ict-dienstverleners Capgemini en Accenture. 'De apps van deze zeven teams sluiten volgens experts het best aan bij het werkproces van de GGD voor het doen van bron- en contactonderzoek en voldoen tegelijkertijd aan eisen die zijn gesteld op onder andere het gebied van privacy, data- en informatieveiligheid en gebruikersgemak', meldt het kabinet.

Chaos bij selectie corona-apps, adviseurs trekken zich terug

67 experts op het gebied van epidemiologie, gezondheidszorg, privacy, informatiebeveiliging en ict beoordeelden donderdag in kleine teams 63 voorgestelde apps. De lijst met 7 deelnemers komt voort uit hun advies.

Een flink deel van die experts voelt zich echter gepasseerd, blijkt uit een rondgang onder hen door de Volkskrant. Van de criteria tot de haast: eigenlijk ging niets goed, volgens hen. 'We hebben geen flauw idee hoe deze lijst tot stand is gekomen', zegt een van hen. Zo wezen meerdere expertgroepen Sia Partners - dat een kopie van de app uit Singapore voorstelt - af op privacygronden. 'Dat juist Sia nu op de lijst staat, is onbegrijpelijk. Hugo de Jonge heeft altijd gezegd dat privacy het uitgangspunt is', aldus een bron.

Door organisatorische chaos en technische problemen hadden de experts vaak niet meer dan een half uur per voorstel. 'De doelen waren niet helder en er waren geen duidelijke objectieve criteria op basis waarvan we moesten toetsen', luidt de kritiek verder.

De meest fundamentele vraag, of een tracing app wel bijdraagt, mocht niet worden gesteld, zeggen de experts: 'De app moet en zal er komen.' Volgens privacy-expert Brenno de Winter, een van de 67 beoordelaars, heeft het proces de kenmerken van een mislukt ict-project. 'Het techoptimisme en gebrek aan ervaring bij het ministerie in combinatie met vage plannen van de ict-bedrijven zijn een dodelijke cocktail.' Zeven van de experts hebben zich inmiddels teruggetrokken uit het proces.

Niet de technische mogelijkheden, maar maatschappelijk nut en noodzaak moeten volgens hen voorop staan. Een groep wetenschappers liet deze week eenzelfde geluid horen. Een van hen, computerwetenschapper Frank Dignum van de Universiteit Utrecht, stelt op basis van computersimulaties dat de voordelen van dit soort apps beperkt zijn, zelfs al gebruikt 60 procent van de bevolking ze. Het willekeurig testen van een deel van de bevolking levert volgens Dignum ongeveer evenveel op.

De Autoriteit Persoonsgegevens (niet betrokken bij de selectie) buigt zich dit weekend over de privacyvoorwaarden van de zeven voorstellen. Het ministerie organiseert dit weekend een 'appathon', waarbij de zeven teams hun ideeën presenteren aan - weer andere - experts. Op basis van het expert- en publieksadvies en het advies van de Autoriteit Persoonsgegevens wordt volgende week bekend of en hoe apps kunnen bijdragen aan het werk van de GGD.

Tweede Kamer
DER STATEN-GENERAAL

Overige relevante documenten

Overige bronnen en documenten

In aanvulling op de in deze reader opgenomen position papers en mediaberichten, in dit slothoofdstuk nog enkele andere informatiebronnen:

I. Informatie over de zeven voorstellen voor apps bron- en contactopsporing
II. Informatie over de Europese richtlijnen voor mobiele corona apps
III. Onderzoeksrapportage Autoriteit Persoonsgegevens apps (20 april 2020)
IV. Samenvatting privacy-analyse Landsadvocaat apps (19 april 2020)
V. 'Bericht aan het parlement' van het Rathenau Instituut (17 april 2020)

I. Zeven voorstellen voor apps bron- en contactopsporing

Website 'Publieke beproeving'
https://www.publiekebeproeving.nl/
Een overzicht van de oplossingen die de zeven geselecteerde ontwikkelaars van de apps tot dusver hebben uitgewerkt.

Website Rijksoverheid, onderdeel coronavirus-app:
https://www.rijksoverheid.nl/onderwerpen/coronavirus-app
Overige informatie over de apps en de dit weekend georganiseerde appathon op het ministerie van VWS.

Onderzoeksrapportage van de apps van de Autoriteit Persoonsgegevens
https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-privacy-corona-apps-niet-aangetoond
De tekst van deze onderzoeksrapportage is hierna integraal opgenomen in deze reader.

Privacy-analyse van de apps van de Landsadvocaat
https://www.rijksoverheid.nl/onderwerpen/coronavirus-app/documenten/publicaties/2020/04/19/samenvatting-privacy-analyse-contactonderzoeksapps
De tekst van de samenvatting van deze privacy-analyse is hierna integraal opgenomen in deze reader.

II. Europese richtlijnen voor mobiele corona apps

Op 8 april heeft de Europese Commissie **een aanbeveling ter ondersteuning van exit strategieën via mobiele data en apps** uitgebracht. Goed gecoördineerde en in overeenstemming met de EU-regels zijnde digitale tools kunnen volgens de Commissie een belangrijke rol spelen bij de geleidelijke opheffing van isoleringsmaatregelen zodra de tijd daarvoor aanbreekt. Door middel van het proces in de aanbeveling kan samen met de lidstaten een toolbox worden vastgesteld, waarbij de nadruk wordt gelegd op twee dimensies:

- een gecoördineerde pan-Europese aanpak voor het gebruik van mobiele applicaties, om burgers in staat te stellen doeltreffende en meer doelgerichte sociale onthoudingsmaatregelen te treffen, en om te waarschuwen, te voorkomen en contacten te traceren; en
- een gemeenschappelijke aanpak voor het modelleren en voorspellen van de ontwikkeling van het virus door middel van geanonimiseerde en geaggregeerde mobiele locatiegegevens.

In de aanbevelingen gaat de Commissie onder andere in op het belang van interoperabiliteit tussen de IT-oplossingen van de lidstaten om grensoverschrijdende samenwerking mogelijk te maken en ervoor te zorgen dat contacten tussen gebruikers van verschillende apps worden opgespoord.
Het eHealth netwerk van de Europese Commissie heeft vervolgens op 16 april een eerste versie van de **toolbox voor *contact-tracing* apps** gemaakt. De toolbox schetst onder andere de essentiële voorwaarden waar een *contact-tracing* app aan moet voldoen:

- vrijwillige deelname;
- goedkeuring door de nationale gezondheidsautoriteit;
- privacy en bescherming van persoonsgegevens; en

- directe ontmanteling op het moment dat de app niet langer nodig is.

Volgens het eHealth netwerk kan digitale technologie, mits correct ingezet, inhoudelijk bijdragen aan het inperken van de verspreiding van het virus. Indien het zonder de juiste waarborgen wordt ingezet, kan het echter een aanzienlijk negatief effect hebben op privacy en individuele rechten. De toolbox is er daarom op gericht om te komen tot een zoveel mogelijk gemeenschappelijke benadering van apps voor contactopsporing. Een ongecoördineerde aanpak zou, volgens het eHealth netwerk, kunnen leiden tot belemmeringen in de doeltreffendheid van de maatregelen en het functioneren van de interne markt. De toolbox gaat in op verschillende aspecten van de ontwikkeling van apps zoals het epidemiologische kader, technische vereisten, waarborging van interoperabiliteit in de EU, toegankelijkheid, governance en informatie-uitwisseling tussen lidstaten.

Op 17 april heeft de Europese Commissie vervolgens **richtsnoeren betreffende gegevensbescherming voor vrijwillige apps ter ondersteuning van de bestrijding voor de COVID-19 pandemie** gepresenteerd. Volgens de Commissie is vertrouwen een belangrijke voorwaarde voor de ontwikkeling van deze apps en de aanvaarding ervan door de mensen. Mensen moeten de zekerheid hebben dat de naleving van de grondrechten wordt gewaarborgd en dat de apps alleen voor de specifiek omschreven doelstellingen zullen worden gebruikt, dat zij niet voor grootschalig toezicht zullen worden gebruikt en dat mensen zeggenschap over hun gegevens houden. De richtsnoeren gaan in op de kenmerken en vereisten waaraan vrijwillige apps volgens de Commissie zouden moeten voldoen met het oog op de naleving van de EU-wetgeving inzake privacy en gegevensbescherming. Het gaat hierbij onder andere om de volgende kenmerken/vereisten:

- De nationale gezondheidsautoriteit aanwijzen als verwerkingsverantwoordelijke voor de gegevensverwerking.
- Ervoor zorgen dat de gebruikers zeggenschap houden over hun persoonsgegevens. Vrijwilligheid en expliciete toestemming voor appfunctionaliteiten zijn hierbij essentieel.
- Gegevensminimalisatie; gebruik alleen die gegevens die echt nodig zijn. Afhankelijk van de doelstelling van de app, moet zorgvuldig worden beoordeeld welke gegevens nodig zijn.
- Beperking van openbaarmaking van gegevens.
- Strikte beperkingen voor gegevensopslag.
- Beveiliging van gegevens waarborgen.
- Juistheid van gegevens waarborgen.
- Gegevensbeschermingsautoriteiten betrekken bij de ontwikkeling van de app.

Hierna treft u de integrale teksten aan van:

III. Onderzoeksrapportage Autoriteit Persoonsgegevens apps (20 april 2020)

IV. Samenvatting privacy-analyse Landsadvocaat apps (19 april 2020)

V. ‘Bericht aan het parlement’ van het Rathenau Instituut (17 april 2020)

Inhoudsopgave

AUTORITEIT
PERSOONSGEGEVENS

20 april 2020

Onderzoeksrapportage bron- en contactopsporingsapps

AUTORITEIT
PERSOONSGEGEVENS

Inhoudsopgave

1. Aanleiding 3

2. Opzet onderzoeksrapportage 3

3. Bevindingen AP 4

4. Onderzoek 5
4.1 Opzet onderzoek 5
4.2 Opzet juridisch onderzoek 6
4.3 Opzet technisch onderzoek 6

5. Bevindingen op hoofdlijnen 7
5.1 De noodzakelijkheid van apps niet aangetoond 7
5.2 Kaders apps onduidelijk 7
5.3 Doelen onscherp geformuleerd 8
5.4 Juridische grondslagen onvoldoende onderbouwd 8
5.5 Welke gegevens zijn minimaal nodig? 8
5.6 AVG rechten onvoldoende gewaarborgd 9

6. Technische bevindingen 9
6.1 Ten aanzien van de voorgelegde apps 9
6.2 Focus niet alleen op de front-end maar ook de back-end 9
6.3 Ten aanzien van het gebruiken van contact tracing apps 9
6.4 Gebruik van unieke identificatienummers 10
6.5 Vragen over de effectieve inzet van bluetooth-technologie 10

AUTORITEIT
PERSOONSGEGEVENS

1. Aanleiding

Het Outbreak Management Team (OMT), het Nederlands adviesorgaan dat de minister van Volksgezondheid, Welzijn en Sport (VWS) en de Ministeriële Commissie Crisisbeheersing (MCCb) adviseert bij de bestrijding van een epidemie, heeft op 6 april 2020 gevraagd om digitale oplossingen die kunnen worden ingezet voor de bestrijding van het coronavirus in Nederland.

Op 11 april 2020 heeft het ministerie van VWS bedrijven en deskundigen uitgenodigd om voorstellen in te dienen voor slimme digitale oplossingen, zoals apps, die kunnen bijdragen aan bron- en contactopsporing, waarbij stringente eisen worden gesteld aan onder meer snelle beschikbaarheid, privacy en informatiebeveiliging. Voorstellen konden worden aangeleverd tot 14 april 2020.[1] Na de uitnodiging zijn meer dan 700 reacties ontvangen, waarvan 660 daadwerkelijk een voorstel bevatten.[2] Het ministerie heeft na advies van diverse deskundigen zeven inzendingen geselecteerd, die hun voorstel nader konden toelichten op 18 en 19 april 2020. Het ministerie van VWS heeft ook de Autoriteit Persoonsgegevens (AP) gevraagd om te beoordelen of de opzet van elk van de zeven apps in Nederland in overeenstemming zou zijn met de AVG.[3] Hiertoe heeft de AP op 17 april 2020 via het ministerie van VWS documentatie ontvangen over de zeven door het ministerie geselecteerde voorstellen. De documentatie die op 17 april was ontvangen was voor vrijwel alle voorstellen niet in één keer compleet. Om die reden heeft de AP ook op 18 en 19 april 2020 nog documenten ontvangen via het ministerie van VWS.

Enkele uitgangspunten zijn volgens de minister dat de inzet van digitale hulpmiddelen noodzakelijk, effectief en proportioneel is en voldoet aan bestaande wetgeving, zoals de Algemene verordening gegevensbescherming (AVG). De minister heeft aan de Tweede Kamer gemeld dat de AP als toezichthouder betrokken wordt.

Hierbij komt de AP tegemoet aan het verzoek van het ministerie van VWS. De AP benadrukt dat het aan VWS en de leveranciers is om aan te tonen dat de apps voldoen aan de geldende wet- en regelgeving omtrent gegevensbescherming. Dit volgt uit de AVG ('verantwoordingsplicht', artikel 5, lid 2, AVG). De AP toetst of dat het geval is.

2. Opzet onderzoeksrapportage

In deze onderzoeksrapportage beschrijft de AP de wijze waarop zij de opzet van de apps heeft beoordeeld. Hierbij wordt niet verwezen naar afzonderlijke apps. Enerzijds omdat de AP tot de slotsom is gekomen dat op grond van de beschikbare informatie geen oordeel kan worden geformuleerd over de vraag of de apps voldoen aan de kaders die de privacywetgeving stelt. Anderzijds omdat een deel van de informatie die aan de AP is verstrekt bedrijfsvertrouwelijk is.

[1] https://www.rijksoverheid.nl/onderwerpen/coronavirus-app/nieuws/2020/04/11/oproep-om-mee-te-denken-over-apps
[2] https://www.rijksoverheid.nl/onderwerpen/coronavirus-app/nieuws/2020/04/17/zeven-apps-doen-mee-aan-publieke-test-komend-weekend
[3] https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-toetst-opzet-corona-apps. De werking van de app of apps zal later worden onderzocht, áls het kabinet daadwerkelijk kiest voor de inzet van een corona app.

AUTORITEIT
PERSOONSGEGEVENS

3. Bevindingen AP

De AP spreekt haar waardering uit voor het innovatief vermogen van app-ontwikkelaars waarvan de AP een voorstel heeft ontvangen. Tegelijkertijd constateert de AP dat de voorstellen qua opzet nog onvoldoende uitgekristalliseerd zijn. Ook was een deel van de documenten met informatie waarop de AP zou moeten toetsen niet aanwezig, gefragmenteerd, onvolledig, laat ingediend en in verschillende talen opgesteld. Daarom komt de AP tot de volgende bevindingen:

De AP kan geen oordeel geven over de opzet van de zeven 'corona-apps' die het ministerie van VWS heeft geselecteerd. De AP vindt dat het ministerie van VWS de kaders niet duidelijk genoeg heeft gesteld. Daardoor zijn de zeven app-voorstellen onvoldoende uitgewerkt om te kunnen beoordelen of de bescherming van gevoelige gegevens van Nederlanders voldoende is gewaarborgd.

Kaders apps onduidelijk
Uit de analyse van de AP blijkt dat de kaders die de overheid stelt voor de corona-app onduidelijk zijn: in het programma van eisen voor de app is een aantal fundamentele vragen onvoldoende beantwoord.

Zo is niet duidelijk omschreven wat het doel is van de app en wie verantwoordelijk is voor de verwerking van de gegevens. Is dat een private partij, een zorgpartij of een overheid? Ook staat in het programma van eisen niet genoemd of de app een onderdeel is van een pakket aan maatregelen en welke maatregelen dat dan zijn. Terwijl het ontwerp en de werking van een app zeer afhankelijk zijn van die overige maatregelen.

Bij een ingrijpend middel als zo'n corona-app moet de AP bovendien kunnen toetsen of de inzet ervan in verhouding staat tot de mogelijke privacyschendingen. Het moet duidelijk zijn waarom alternatieven die minder ingrijpend zijn dan een app minder effectief zijn om het virus in te dammen. Dat is nu onvoldoende duidelijk. De AP kan de proportionaliteit van de inzet van de corona-apps daardoor niet beoordelen.

Te weinig informatie over apps
Het feit dat de kaders onvoldoende duidelijk zijn, maakt dat veel app-ontwikkelaars nog zoekende zijn en zij hun plannen onvoldoende hebben kunnen uitwerken, zowel op technisch als op juridisch vlak. De AP heeft van de app-ontwikkelaars te weinig informatie ontvangen om een goed beeld te krijgen van de opzet van hun apps.

Zo leverden sommige app-ontwikkelaars alleen informatie over hoe de app eruit ziet voor gebruikers, en laten ze informatie over hoe de app 'aan de achterkant' werkt achterwege. Daardoor is door de app-ontwikkelaars onvoldoende aangetoond dat de privacy technisch maar ook organisatorisch gezien gewaarborgd is.

Daarnaast onderbouwen de ontwikkelaars van de apps in hun voorstellen niet of onvoldoende waarom ze een bepaalde techniek inzetten en wat de beperkingen van die techniek zijn. Bijvoorbeeld de inzet van Bluetooth in een app die contact tussen mensen bijhoudt. Het gebruik van deze techniek kan betekenen dat er veel vals positieven zijn. De onderbouwing van dit soort keuzes is nodig voordat de AP een oordeel kan vellen.

Wanneer de noodzaak, de kaders, de plannen en de apps beter uitgewerkt zijn, kan de AP pas een afgewogen oordeel vellen.

AUTORITEIT
PERSOONSGEGEVENS

4. Onderzoek

4.1 Opzet onderzoek

Het onderzoek naar waarborgen van de apps op het punt van gegevensbescherming, vond plaats op vrijdag 17, zaterdag 18 en zondag 19 april. De AP heeft voor de beoordeling een multidisciplinair team ingezet, bestaande uit technologen, sociaal wetenschappers en juristen. Het team heeft de voorstellen en de bijbehorende documentatie over voorgelegde apps onderzocht op zowel technische als juridische aspecten van het gegevensbeschermingsrecht. De apps zelf en de softwarecode zijn slechts zijdelings bij het onderzoek betrokken. Voor een beoordeling hiervan verwijst de AP naar het KPMG onderzoek.[4]

De AP heeft via het ministerie van VWS bij de app-ontwikkelaars de volgende documentatie opgevraagd:

1. Het verwerkingenregister*
2. De DPIA*
3. Technische documentatie over opzet en werking van de app, opslag van data en informatiebeveiliging.
4. Eventuele expertrapportages (oordelen van deskundigen, contra-expertise rapportages, evaluaties, technische testrapporten, et cetera)
5. De duidelijke handleiding en instructie*
6. Beschreven aandacht voor vertrouwelijkheid en integriteit*
7. Beschrijving van controleerbaarheid van daadwerkelijk gebruikte oplossing*
8. Omschreven doel en doelgroep*
9. Eventueel uitgevoerde audits*
10. Documentatie waaruit volgt dat wordt voldaan aan de ISO-normen*
11. Alle overige documentatie waarvan de ontwikkelaar / aanbieder denkt dat die relevant is in het kader van de vraag welke gegevensbeschermingsrisico's gepaard gaan met het gebruik van de app.
12. Contactgegevens voor aanvullende (technische en juridische gegevensbeschermingsgerelateerde) vragen.
13. Een overzicht per app van de bij die app aangeleverde documenten.

* Deze documenten maakten ook onderdeel uit van de uitvraag van het ministerie van VWS[5]

Ook heeft het ministerie van VWS een samenvatting van de opmerkingen van de door hen ingeschakelde experts aan de AP verstrekt. Eventueel online beschikbare informatie over de apps is door de AP niet meegenomen of slechts zijdelings bij de technische beoordeling betrokken. Wel heeft de AP kennis genomen van de pitches die door de app-ontwikkelaars zijn gegeven op 18 en 19 april tijdens de door het ministerie van VWS georganiseerde appathon. Ook volgden enkele AP-medewerkers is de appathon via de livestream.
Ten slotte heeft de AP twee documenten van het ministerie van VWS ontvangen over de juridische inbedding van de apps, te weten de notitie 'Uitwerking grondslag en juridische inbedding apps VWS/WJZ/ Landsadvocaat 17 april 2020' en het 'Aanbouwdocument juridische verantwoording corona-apps' van de landsadvocaat van 18 april 2020.

[4] https://www.rijksoverheid.nl/onderwerpen/coronavirus-app/documenten/publicaties/2020/04/19/rapportage-veiligheidstest-potentiele-corona-apps
[5] Document "Uitnodiging slimme digitale oplossingen Corona" via https://www.tenderned.nl/tenderned-tap/aankondigingen/192421;section=2

4.2 Opzet juridisch onderzoek

Voor de vraag of de verwerkingen van persoonsgegevens middels de voorgestelde app binnen de kaders van de AVG zouden kunnen plaatsvinden heeft de AP allereerst per app in kaart gebracht welke gegevens binnen de app zelf zouden worden verzameld, en welke gegevens vanuit de app via een centrale server met andere partijen (bijvoorbeeld de GGD) worden uitgewisseld. Hieruit bleek dat alle apps – in ieder geval in potentie – persoonsgegevens verwerken en uitwisselen. Daarnaast worden in veel gevallen ook gezondheidsgegevens verwerkt. De AVG is derhalve van toepassing op alle aan de AP voorgelegde corona-apps.
Op basis van de aangeleverde informatie heeft de AP vervolgens – voor zover mogelijk op basis van de aangeleverde informatie – een inschatting gemaakt of en hoe per app aangetoond ('aantoonplicht') wordt of aan de beginselen van rechtmatigheid, behoorlijkheid, transparantie en minimale gegevensverwerking wordt voldaan.

Opvallend genoeg ontbrak een (adequaat) verwerkingenregister in alle gevallen. Bij sommige voorstellen was door de leverancier van de app een gegevensbeschermingseffectbeoordeling[6] (op hoofdlijnen) toegevoegd. Echter door de vele nog openliggende keuzes met betrekking tot het doel van de apps, de wijze waarop de apps organisatorisch worden ingezet, de precieze functionaliteit die daaruit volgt en de te nemen beveiligingsmaatregelen van de corona-app in Nederland, waren deze DPIA's – voor zover aanwezig - weinig concreet en daarmee onvoldoende bruikbaar voor de AP om haar beoordeling op te baseren. De beschrijving van de functionele en technische werking van de verschillende apps verschilde in kwaliteit. Sommige apps waren gebaseerd op apps die al in andere landen in gebruik zijn (bijvoorbeeld in Tsjechië en in Oostenrijk) en sommige apps zijn nog in de ontwikkel- en testfase.

4.3 Opzet technisch onderzoek

Het technisch onderzoek door de AP bestond uit het analyseren van de technische documentatie.

Beschikbare gegevens
In de aan de AP aangeleverde documentatie ging het veelal om mock-ups en andere documenten met ideeën ten aanzien van te ontwikkelen apps. Bij sommige was duidelijk welke onderliggende techniek men voor de betreffende app wilde gaan gebruiken en hoe deze techniek zou moeten worden geïmplementeerd maar bij andere voorstellen was dit niet het geval. Aan de AP zijn ook geen demo's, films of ander materiaal ter beschikking gesteld. De –in een later stadium door een aantal partijen ter beschikking gestelde –broncodes zijn niet door de AP getoetst.

Appathon
Enkele AP-technologen hebben de gevolgd via de livestream. Opvallend was dat er via de appathon op beide dagen aanvullende informatie werd verstrekt die niet was opgenomen in de door de AP ontvangen documentatie. Zo kon de bij de appathon getoonde nieuwe informatie bij een aantal apps meer helderheid geven over de slechts in beperkte mate beschikbaar gestelde informatie, bijvoorbeeld informatie over onder de app ten grondslag liggende technologie of brachten zij risico's aan het licht ten aanzien van bijvoorbeeld het gebruik van telefoonnummers. In een enkel geval leek de app-ontwikkelaar gedurende de appathon te wisselen van de onderliggende techniek, dit zorgde voor verwarring ten aanzien van de analyse van de door de app-ontwikkelaar gebruikte techniek.

Inhoudelijke analyse
De AP heeft voor de technische analyse gebruik gemaakt van een vaste werkwijze, die voor elk van de apps is doorlopen. Daarbij is gekeken naar de volgende onderwerpen:

[6] Ook wel bekend als Data Protection Impact Assessment (DPIA).

- **Algehele indruk**: hierbij is globaal gekeken in hoeverre is voldaan aan AVG-principes zoals privacy by design en privacy by default.
- **De aard van de gekozen oplossing**: de gekozen oplossing; op welke wijze is de betreffende app ontworpen om het bron- en contactonderzoek uit te voeren. Bijvoorbeeld door middel van het gebruik van bluetooth of locatiegegevens, de door de app vereiste app-machtigingen, het gebruik van unieke identifiers, maar ook het gebruik van een centrale of decentrale server.
- **De software:** de door de app-ontwikkelaars gekozen software. Bijvoorbeeld of de software open-source is, of deze afhankelijk is van Software Development Kits van derden, het gebruik van privacy enhancing technologies, de distributiewijze van de app, maar ook de documentatie bij de software.
- **De beveiliging van de app**: de beveiliging van de app en de met de app verkregen gegevens. Bijvoorbeeld op welke wijze de data zelf opgeslagen en beveiligd worden en wie vervolgens bij die data kan. Speciale aandacht is besteed aan vragen die zien op het voorkomen van fraude; welke maatregelen hebben de leveranciers genomen tegen het spoofen van unieke identificatienummers, het de-anomiseren daarvan of het aanpassen van de status van een gebruiker indien iemand besmet is.

Zoals eerder aangegeven was niet alle informatie beschikbaar en konden hierdoor vragen in voorkomende gevallen niet beantwoord worden. Daar waar mogelijk is geprobeerd verder te kijken dan de door de app-ontwikkelaars aangeleverde stukken, bijvoorbeeld door het bestuderen van de onderliggende techniek. Dit kon alleen in die gevallen waar geen enkel misverstand bestond over welke onderliggende techniek het ging.

Steekproefsgewijs en in duo's hebben de betrokken onderzoekers elkaars bevindingen getoetst.

5. Bevindingen op hoofdlijnen

5.1 De noodzakelijkheid van apps niet aangetoond

Voorop staat dat de inzet van contact tracing apps een vergaande en zeer ingrijpende inbreuk oplevert op het grondrecht op privéleven van burgers. Daar komt bij dat het hier gaat om de verwerking van gegevens over gezondheid. Dat zijn zeer gevoelige (bijzondere) persoonsgegevens, waarop soms ook het medisch beroepsgeheim van artsen rust. De AP is zich overigens bewust van het algemene belang van de bescherming van de volksgezondheid en de bestrijding van infectieziekten. Dat raakt ook aan andere grondrechten van burgers, zoals het recht op leven. Idealiter zijn grondrechten met elkaar in balans. Er moet onderbouwd worden hoe de verschillende grondrechten tegen elkaar zijn afgewogen. Kernvraag vanuit het gezichtspunt van de AP is wat de noodzaak is voor een vergaande en ingrijpende inbreuk op het grondrecht op privéleven van burgers. Op het punt van de noodzaak en de effectiviteit heeft de AP in het onderzoek geen documentatie aangetroffen.
Voor de volledigheid merkt de AP op dat die noodzakelijkheid er ook moet zijn indien de app op basis van vrijwillige toestemming van betrokkenen wordt gebruikt.

5.2 Kaders apps onduidelijk

Uit de aangeleverde documenten blijkt dat er kaders ontbreken over de verantwoordelijkheden in het proces nu, en in een situatie waarin de apps in gebruik zouden zijn, terwijl dit voor gebruikers van de app volkomen helder moet zijn. De doelstellingen van de apps zijn niet altijd helder gedefinieerd. Deze dienen

te worden gedefinieerd door de verwerkingsverantwoordelijke; dit kan niet louter aan een app-ontwikkelaar worden overgelaten nu hij de beoogde situationele inzet van de apps onvoldoende kent.

Ten aanzien van de aangeleverde documenten geldt dat deze korte analyses van deskundigen bevatten, maar dat een verdere beschouwing van het ministerie van VWS daarover, ontbreekt. Het ministerie heeft voorts geen afweging aangeleverd waarin de noodzaak van bron- en contactopsporingsapps is aangetoond. Denk hierbij aan de afweging van alternatieven en het aantonen van de proportionaliteit. Ook is van belang dat helder wordt gemaakt waarvoor de app wordt ingezet. De sociaal-maatschappelijke gevolgen kunnen immers groot zijn. Het mag niet zo zijn dat wanneer iemand geen gebruik kan of wil maken van een app, toegang tot werk, school of bijvoorbeeld een supermarkt wordt geweigerd. Dit betekent dat het ministerie van VWS helder moet zijn over de kaders waarbinnen de app gebruikt mag worden.
Voor zover de app-voorstellen verder uitgewerkt zijn, stelt de AP vast dat een beoordeling van gegevensbeschermingsrechtelijke aspecten in deze fase van het proces moeilijk is. De reden hiervoor is dat fundamentele keuzes - een juridisch raamwerk - over onder andere de verwerkingsverantwoordelijkheid, het precieze doel van de verwerking en de grondslag voor de verwerking, nog niet gemaakt zijn. Als logisch gevolg daarvan kon daarmee bij het ontwikkelen van de apps geen rekening worden gehouden. Die keuzes zullen naar het oordeel van de AP van grote invloed zijn op de inrichting van de te ontwikkelen app. Pas als die keuzes zijn gemaakt, kan een beoordeling van de rechtmatigheid van de verwerking van persoonsgegevens met de te ontwikkelen app plaatsvinden, waarbij fundamentele vragen over bijvoorbeeld noodzakelijkheid, doelbinding, dataminimalisatie en de rechten van betrokkenen kunnen worden beantwoord.

5.3 Doelen onscherp geformuleerd

Het doel van de verwerking van persoonsgegevens die de app meebrengt, in sommige gevallen meerdere doelen, zijn kritisch bekeken met het oog op de eis van doelbinding. Dat is een van de principes van de AVG. Het feit dat sommige apps meerdere doelen nastreven ziet de AP als een risico voor de gegevensbescherming. De beoordeling van de vraag of de verwerking van persoonsgegevens als gevolg van het gebruik van de corona-app noodzakelijk is gelet op de daarmee nagestreefde doeleinden, kon door de AP niet worden gemaakt. Enerzijds omdat de doeleinden nog niet scherp zijn geformuleerd en anderzijds omdat geen van de voorstellen informatie bevatte over de (bewezen) effectiviteit van de contact tracing app of een afweging van alternatieven.

5.4 Juridische grondslagen onvoldoende onderbouwd

Het ministerie van VWS heeft een juridische onderbouwing voor de toepassing van een corona-app in Nederland aan de AP verstrekt. Die onderbouwing is weergegeven in twee documenten: de notitie 'Uitwerking grondslag en juridische inbedding apps VWS/WJZ/ Landsadvocaat 17 april 2020' en het 'Aanbouwdocument juridische verantwoording corona-apps van de landsadvocaat van 18 april 2020'. Deze documenten bieden naar de mening van de AP zinvolle aanknopingspunten voor een nadere doordenking van de juridische aspecten en mogelijkheden van de inzet van apps voor bron- en contactopsporing ter bestrijding van het coronavirus.
Tegelijk maakt de AP uit alle ter beschikking gestelde documenten op dat er op het moment van beoordeling tussen het ministerie en de geselecteerde app-ontwikkelaars geen eenduidig beeld lijkt te bestaan van hoe de grondslagen invulling zouden moeten krijgen.

5.5 Welke gegevens zijn minimaal nodig?

De AP constateert dat de verschillende app-ontwikkelaars veel documentatie binnen korte tijd hebben kunnen aanleveren en dat dit een aanzienlijke inspanning heeft gekost bij de app-ontwikkelaars. De AP

constateert dat app-ontwikkelaars soms aannames hebben moeten doen omdat nog niet alle uitgangspunten rondom de app duidelijk zijn geformuleerd. Deze aannames zorgen ervoor dat een beoordeling complex wordt omdat er daarmee geen zekerheid is over de vraag of de aannames van de app-ontwikkelaars overeenstemmen met de uitgangspunten zoals deze later ook door VWS worden gedefinieerd. De vraag welke gegevens noodzakelijk zijn, valt tegen deze achtergrond eveneens niet goed te beantwoorden. Een beoordeling van het beginsel van dataminimalisatie uit de AVG was daarom niet mogelijk.

5.6 AVG rechten onvoldoende gewaarborgd

Het is voor burgers cruciaal dat voldoende helder is bij wie zij kunnen aankloppen met vragen over de verwerking van hun persoonsgegevens. Omdat op dit moment onduidelijk is wie de verwerkingsverantwoordelijke zal zijn en wie de verwerker, is niet helder wie nu let op de AVG-rechten van burger en daar verantwoordelijkheid voor neemt. Noch de app-ontwikkelaars noch het ministerie kon hier uitsluitsel over geven.

6. Technische bevindingen

6.1 Ten aanzien van de voorgelegde apps

De kwaliteit van de door de verschillende app-ontwikkelaars aangeleverde stukken was sterk wisselend, sommige voorgestelde apps waren in een veel verder gevorderd stadium dan andere voorstellen. Dat wil niet altijd zeggen dat de onderliggende uitgangspunten van de betreffende app incorrect waren. Vanuit het perspectief van de AP kan in het algemeen kan gesteld worden dat de apps ten behoeve van contact tracing die gebruik maken van een decentrale oplossing zonder het gebruik van (aanvullende) persoonsgegevens de grootste potentie hebben om een bijdrage te kunnen leveren aan het ondersteunen van de GGD bij het uitvoeren van contactonderzoek. De door verschillende partijen genoemde onderliggende privacy-vriendelijke oplossingen zijn op dit moment nog niet uitontwikkeld en dat maakt mede dat vragen over de daadwerkelijke werking in de praktijk nog beantwoord moeten worden.

6.2 Focus niet alleen op de front-end maar ook de back-end

De AP heeft in haar technische beoordeling gebruik gemaakt van de door de app-ontwikkelaars aangeleverde documentatie. Deze documentatie was voor een goede beoordeling op technisch vlak niet voldoende. De aangeleverde documenten zagen bijvoorbeeld alleen op een front-end, zonder de back-end in ogenschouw te nemen. Een dergelijke back-end kan een zwakke schakel vormen in de keten, het is bijvoorbeeld van groot belang dat een eventuele terugkoppeling van registraties met het coronavirus ‘besmette’ identificatienummers samen met de overige communicatie goed beveiligd is.

6.3 Ten aanzien van het gebruiken van contact tracing apps

Het is niet aan de AP om te oordelen of een app een effectieve oplossing is voor het ondersteunen van de GGD bij het uitvoeren van contactonderzoek of het voorzien van informatie met betrekking tot de pandemie. Mogelijk zijn hier nader door het ministerie te onderzoeken alternatieven voor. Het is wel nodig om helder te maken wat de afweging is voor de inzet van bepaalde technologieën; in hoeverre is de inzet van een contact tracing app die mogelijk een inbreuk maakt op de persoonlijke levenssfeer van de gebruiker de oplossing? Is er een andere oplossing denkbaar die minder inbreuk maakt op de persoonlijke levenssfeer? Het inzetten van een app kent immers tal van nadelen en onzekerheden, die niet technisch weggenomen kunnen worden.

De aan de AP voorgelegde apps zagen voornamelijk op het bijhouden van interpersoonlijk contact. Op basis hiervan ziet zij twee problemen terugkomen: het gebruik van (herleidbare) identificatienummers en tevens een mogelijke overschatting van de betrouwbaarheid van bluetooth.

6.4 Gebruik van unieke identificatienummers

De AP constateert dat de app-ontwikkelaars over het algemeen kiezen voor de uitwisseling van unieke identificatienummers om bij te houden wie met wie in contact is geweest. Deze unieke identificatienummers kunnen persoonsgegevens zijn waardoor de AVG van toepassing is. Bij een aantal van de gekozen oplossingen zijn deze identificatienummers gemakkelijk te herleiden tot de individuele gebruiker van de apps. Maatregelen tegen de-anomisering ontbreken.

6.5 Vragen over de effectieve inzet van bluetooth-technologie

De voorgelegde apps wisselen de unieke identificatienummers veelal uit door middel van het bluetooth-protocol. Bluetooth kan ingezet worden voor contact-tracing. In de ingediende voorstellen kwam echter niet duidelijk naar voren hoe betrouwbaar het gebruik van bluetooth is, en hoe eventuele tekortkoming zijn op te vangen. Zo is de door de overheid gebruikte richtlijn van anderhalve meter afstand vele malen kleiner dan het gemiddelde bereik van bluetooth. Daarnaast is het bereik afhankelijk van allerlei externe factoren (bijvoorbeeld de signaalsterkte van verschillende apparatuur en de aanwezigheid van fysieke objecten tussen gebruikers).[7] Het is lastig om vervolgens op basis van bijvoorbeeld signaalsterkte in combinatie met contactduur te kunnen bepalen in hoeverre verschillende app-gebruikers met elkaar in contact zijn geweest en wat de kans is dat het coronavirus op die manier verspreid is. Mogelijk kunnen deze nadelen worden gemitigeerd, of zijn de resulterende valse positieven geen belemmering in de praktijk. Een onderbouwing daarvoor, eventueel op basis van simulaties, ontbreekt

[7] Voor meer informatie over het bereik van Bluetooth in verschillende omstandigheden zie https://www.bluetooth.com/learn-about-bluetooth/bluetooth-technology/range/#estimator

AUTORITEIT
PERSOONSGEGEVENS

Vragen over de Algemene verordening gegevensbescherming

Op onze website autoriteitpersoonsgegevens.nl vindt u informatie en antwoorden op vragen over de Algemene verordening gegevensbescherming (AVG). Heeft u op deze website geen antwoord op uw vraag gevonden? Dan kunt u contact opnemen met het Informatie- en Meldpunt Privacy van de Autoriteit Persoonsgegevens op 088-1805 250.

AUTORITEIT
PERSOONSGEGEVENS

Contactgegevens

Bezoekadres
(alleen volgens afspraak)
Prins Clauslaan 60
2595 AJ DEN HAAG

Let op: bij bezoek aan de Autoriteit Persoonsgegevens moet u een geldig identiteitsbewijs laten zien.

Postadres
Postbus 93374
2509 AJ DEN HAAG

Telefonisch spreekuur
Op onze website autoriteitpersoonsgegevens.nl vindt u informatie en antwoorden op vragen over de bescherming van persoonsgegevens. Heeft u op deze website geen antwoord op uw vraag gevonden? Dan kunt u contact opnemen met de publieksvoorlichters van de Autoriteit Persoonsgegevens tijdens het telefonisch spreekuur via telefoonnummer **0900-2001 201**. De publieksvoorlichters zijn bereikbaar op werkdagen van 09.30 tot 12.30 uur. (5 cent per minuut, plus de kosten voor het gebruik van uw mobiele of vaste telefoon).

Persvoorlichting
Journalisten en redacteuren kunnen met vragen terecht bij de woordvoerders van de Autoriteit Persoonsgegevens. Zie de contactgegevens van de woordvoerders van de AP op deze pagina.

Zakelijke relaties
Bent u een zakelijke relatie van de Autoriteit Persoonsgegevens, zoals een leverancier, dan kunt u ons telefonisch bereiken via telefoonnummer **070-8888 500**.

Over de Autoriteit Persoonsgegevens
Iedereen heeft recht op een zorgvuldige omgang met zijn persoonsgegevens. De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en adviseert over nieuwe regelgeving.

Inhoudsopgave

PELS RIJCKEN

Openbare samenvatting privacyanalyses bron- en contactonderzoekapps

19 april 2020
Gerrit-Jan Zwenne en Marte van Graafeiland

Alle werkzaamheden worden verricht op grond van een overeenkomst van opdracht met de naamloze vennootschap Pels Rijcken & Droogleever Fortuijn N.V. gevestigd te Den Haag en ingeschreven in het Handelsregister onder nr. 27283716. Op de overeenkomst zijn de algemene voorwaarden van toepassing, die zijn gedeponeerd ter griffie rechtbank Den Haag onder nr. 19/2015. Daarin is een aansprakelijkheidsbeperking opgenomen. De algemene voorwaarden worden op verzoek toegezonden of zijn te raadplegen op www.pelsrijcken.nl. Kwaliteitsrekening notariaat 21.30.13.495

1 INLEIDING

1.1 Op zaterdag 11 april 2020 heeft het ministerie van Volksgezondheid, Welzijn en Sport ('**VWS**') aan de markt een uitnodiging gedaan voor het indienen van voorstellen voor slimme digitale oplossingen voor – voor zover van belang – bron- en contactopsporing (hierna: de bron- en contactonderzoekapp of kort gezegd app).

1.2 Doel van de uitnodiging is om VWS mede op basis van de opgehaalde informatie in staat te stellen naar beste inzicht een stap te zetten in de besluitvorming over de mogelijke inzet van een bron- en contactonderzoekapp bij de bestrijding van COVID-19 en de volgende fase uit de intelligente lockdown.[1] In de uitnodiging zijn verschillende uitgangspunten genoemd waaraan de voorstellen moeten voldoen, waaronder:

- De gegevens die worden verwerkt zijn en blijven niet tot individuen herleidbaar (anonimiteit);
- Valse positieven moeten zoveel mogelijk beperkt worden door de oplossing (juistheid);
- Gegevens worden zo min en zo kort mogelijk opgeslagen (dataminimalisatie);
- Gegevens mogen uitsluitend uitgelezen of gedeeld worden als er sprake is van a) contact- of brononderzoek als bedoeld in art. 6 Wpg of b) toestemming van de gebruiker (grondslag);
- Het huidige proces van bron- en contactopsporing is uitgangspunt ter ondersteuning. Het gebruik moet gericht zijn op het vereenvoudigen van contactonderzoek (doelbinding);
- Er is voorzien in een informatieportal voor de gebruikers waarin fouten en kwetsbaarheden kunnen worden gemeld (transparantie);
- Gangbare beveiligingsstandaarden;
- Als de app niet meer effectief of noodzakelijk is, moet de uitrol kunnen worden teruggedraaid en data kunnen worden verwijderd (verwijdering).

Overkoepelend geldt dat (voor zover van toepassing) wordt voldaan aan de Algemene Verordening Gegevensbescherming ('**AVG**').

1.3 Tegen deze achtergrond heeft VWS ons gevraagd een privacyanalyse te verrichten op zeven van de ingediende voorstellen. Dit document betreft een samenvatting van onze bevindingen.

---

[1] Zie: 'Uitnodiging slimme digitale oplossingen Corona'.

2 OPMERKINGEN VOORAF

Bij onze analyse hebben wij ons zoveel mogelijk gebaseerd op de documentatie die aan ons ter beschikking is gesteld.[2] De hoeveelheid stukken, het detailniveau en de kwaliteit daarvan verschilde per inschrijver. Daarnaast is van belang dat wij, gelet op de beperkte tijd die beschikbaar was, de inschrijvers bij het uitvoeren van onze analyse niet op de gebruikelijke wijze hebben kunnen bevragen op (onder andere) de voorgestelde techniek, de precieze inrichting van de app en andere relevante aspecten. Het voorgaande maakt dat deze samenvatting is beperkt tot een overzicht van onze bevindingen op hoofdlijnen.

Wij hebben de voorstellen beoordeeld aan de hand van zes fasen: de installatiefase, uitwisselingsfase, validatiefase, waarschuwingsfase, koppelingsfase en notificatiefase. Per fase hebben wij op basis van de beschikbaar gestelde documentatie beoordeeld of aan de hiervoor genoemde uitgangspunten en AVG is voldaan.

3 BEVINDINGEN

Hoofdconclusie

Wij hebben op basis van de beoordeelde stukken bij geen van de voorstellen kunnen vaststellen dat ze volledig voldoen aan de zojuist geformuleerde uitgangspunten. Evenmin hebben wij op basis van de stukken kunnen vaststellen dat wordt voldaan aan alle eisen van de AVG. Daarmee is echter niet gezegd dat niet alsnog aan de AVG kan worden voldaan. Dat vergt enerzijds een doorontwikkeling en anderzijds een meer gedetailleerde uitwerking van de voorstellen.

Deelbevindingen

Wij hebben op basis van de beoordeelde stukken bij geen van de voorstellen kunnen vaststellen dat volledige anonimiteit gegarandeerd.

Op basis van de beoordeelde stukken kan bij geen van de voorstellen worden vastgesteld dat volledige anonimiteit is gegarandeerd.

Vals positieven moeten zoveel mogelijk worden beperkt

Alle voorstellen werken met Bluetooth. Bepaalde risico’s zijn daaraan inherent. Zo bestaat bij het gebruik van Bluetooth het risico dat niet-risicovolle connecties ook worden geregistreerd, bijvoorbeeld wanneer een Bluetoothconnectie wordt gelegd met devices die zich op voldoende afstand bevinden, of bijv. achter een muur, raam, of plexiglas. Ook is denkbaar dat iemand in de buurt is geweest van een device op een moment dat deze zich niet in de nabijheid van de gebruiker bevond.

---

[2] Een groot aantal partijen heeft gedurende dit weekend van 18 en 19 april 2020 nog aanvullende stukken toegestuurd.

Sommige inschrijvers hebben (door middel van instellingen) getracht dit probleem te ondervangen. Daarmee is het risico op vals positieven kleiner, maar ten aanzien van geen enkel voorstel hebben wij op basis van de aan ons ter beschikking gestelde stukken kunnen vaststellen dat dit inherente risico volledig wordt ondervangen.

Bij sommige voorstellen wordt de besmetting van de gebruiker gevalideerd door een arts. Het aantal vals positieven kan hiermee verder worden teruggebracht.

Er worden zo min en zo kort mogelijk gegevens opgeslagen (dataminimalisatie)

Alle voorstellen kennen enige vorm van centrale opslag. In het gros van de voorstellen betreft dat alleen ID's en/of keys. In bepaalde gevallen worden ook contactgegevens centraal opgeslagen. Dat laatste is behulpzaam voor de bron- en contactopsporing door de GGD en in zoverre lijken de genoemde contactgegevens toereikend, ter zake dienend en niet bovenmatig te zijn voor het doel waarvoor de app zal worden gebruikt.

Een ander belangrijk aspect van dataminimalisatie is het moment waarop de risicoanalyse plaatsvindt en door wie. Bij een volledig gedecentraliseerde opzet vindt de risicoanalyse plaats in de app zelf. Dat doet het meeste recht aan het beginsel van dataminimalisatie.

Wij zijn ook apps tegengekomen waarbij de risicoanalyse centraal plaatsvindt. Bij een dergelijke centrale opzet krijgt de beheerder van de server gedetailleerde inzichten in de contactmomenten en de risico's die de mogelijk besmette gebruiker heeft gelopen. Ook de wijze waarop gebruikers worden gewaarschuwd dat zij in contact zijn geweest met een besmette gebruiker, is van invloed op de omvang en de aard van de (gepseudonimiseerde) persoonsgegevens die worden verwerkt. Kort en goed zijn wij bij de centrale opzet twee varianten tegengekomen. Bij de eerste variant worden meldingen gericht verzonden naar de mogelijk besmette gebruikers. Bij deze variant bestaat een risico dat de mogelijk besmette gebruiker kan worden geïdentificeerd. In de tweede variant wordt een melding op een centrale server opgeslagen, waarna deze ongericht wordt 'gebroadcast' naar gebruikers. Bij de tweede variant lijkt dat risico kleiner. Tot slot zien wij verschillen in wie toegang heeft tot de vastgelegde contacten.

Onderling kennen de oplossingen verschillen in de gegevens die door middel van Bluetooth worden verwerkt (o.a.: de (gepseudonimiseerde) ID van de tegengekomen gebruiker, datum en tijd(sbestek) van het contact, duur van het contact en signaalsterkte) en in welke fase ze worden gepseudonimiseerd. Ook verschilt of contacten alleen zichtbaar worden bij een match dan wel dat gebruikers real time inzage hebben in alle signalen die de app heeft geregistreerd.

Gegevens mogen uitsluitend worden uitgelezen of gedeeld als er sprake is van a) contact- of bronnonderzoek als bedoeld in art. 6 Wpg of b) toestemming van de gebruiker (grondslag)

In de installatie- en uitwisselingsfase van ieder van de voorstellen kan een grondslag worden gevonden in de toestemming van de gebruiker. Het merendeel van de verwerkingen in de validatiefase, waarschuwingsfase en koppelingsfase en notificatiefase binnen de voorstellen vindt plaats om de GGD te ondersteunen bij het bron- en contactonderzoek inzake de bestrijding van COVID-19. Een deel van het contactonderzoek wordt geautomatiseerd in de zin dat een gebruiker zelfstandig met zijn smartphone (via de server) gewaarschuwd kan worden dat hij mogelijk een risico op besmetting heeft gelopen. Voor zover een app in die fases (gepseudonimiseerde) persoonsgegevens verwerkt, bestaan goede argumenten dat de overheidsinstelling (de GGD) de verwerking kan baseren op artikel 9, tweede lid, aanhef en onder i, AVG jo. artikel 6, eerste lid, aanhef en onder e, AVG jo. artikel 6, eerste lid, aanhef en onder c, Wet publieke gezondheid (Wpg). Zekerheid op dit punt vergt nadere analyse en/of een nieuwe specifieke wettelijke grondslag.

Het huidige proces van bron- en contactopsporing is uitgangspunt ter ondersteuning. Het gebruik moet gericht zijn op het vereenvoudigen van contactonderzoek (doelbinding)

Bijna alle apps zijn gericht op het ondersteunen van bron- en contactopsporing. Enkele voorstellen bieden een platform aan waarop een dergelijke applicatie zou kunnen aansluiten.

In alle voorstellen lijkt te worden uitgegaan van enige vorm van centrale opslag van gegevens. In het gros van de voorstellen betreft dat alleen ID’s en/of keys. In bepaalde gevallen worden ook contactgegevens centraal opgeslagen. Dat laatste is behulpzaam voor de bron- en contactopsporing door de GGD. In die zin lijken de genoemde contactgegevens toereikend, ter zake dienend en niet bovenmatig te zijn voor het doel waarvoor de app zal worden gebruikt.

Er is voorzien in een informatieportal voor de gebruikers waarin fouten en kwetsbaarheden kunnen worden gemeld (transparantie)

Wij concluderen dat alle voorstellen in potentie aan dit uitgangspunt voldoen.

Gangbare beveiligingsstandaarden (beveiliging)

De beveiligingsexperts van KPMG hebben op 19 april 2020 een eerste securitytest verricht op de deelnemende apps. KMPG heeft daarbij onder meer gekeken naar specifieke beveiligingseisen en risico’s (Randvoorwaarde 4, Uitnodigingseis 22 en 23). Voor de vraag of de voorstellen voldoen aan de geldende beveiligingseisen, verwijzen wij naar de door KPMG uitgevoerde securitytest.

Als de app niet meer effectief of noodzakelijk is, moet de uitrol kunnen worden teruggedraaid en data kunnen worden verwijderd (verwijdering)

Wij concluderen dat alle voorstellen in potentie aan dit uitgangspunt kunnen voldoen en dat kan worden aangesloten bij de guidelines van het European Centre for Disease Prevention and Control.

4 Disclaimer

Deze samenvatting en onderliggende privacy-analyses zijn in opdracht van het Ministerie van VWS opgesteld om inzicht te geven in de privacy aspecten van de 7 apps die publiekelijk zijn gepresenteerd tijdens de zogenaamde Appathon. De samenvatting en privacy-analyses zijn uitsluitend bestemd voor het Ministerie van VWS. Derden kunnen daaraan geen rechten ontlenen; reeds omdat zij geen kennis dragen van de onderliggende adviesrapporten en die ook niet voor hen zijn bestemd. De in deze samenvatting en privacy-analyses opgenomen informatie is met zorg samengesteld. Toch kan Pels Rijcken – gelet op de aard van de werkzaamheden en de tijdsdruk – niet instaan voor de juistheid en volledigheid van de informatie. Zo is veel informatie over de 7 apps niet tijdig aan ons beschikbaar gesteld. Er is – gelet op de tijdsdruk – ook beperkt navraag gedaan of de documentatie compleet was en alles tijdig was aangeleverd. Daarnaast zijn er mogelijk na het verkrijgen van de initiële documentatie aanpassingen gedaan. Deze aanpassingen zijn niet door ons in deze samenvatting en privacy-analyses betrokken. Ten behoeve van deze samenvatting en privacy-analyses is tevens gebruik gemaakt van informatie van het Ministerie van VWS, van derden en van links naar externe websites.

De bevindingen in deze samenvatting en privacy-analyses zijn – gelet op de tijdsdruk en gelet op de opdrachtverlening van het Ministerie van VWS – niet op voorhand met de leveranciers van de 7 apps besproken en/of aan de leveranciers van de 7 apps ter beschikking gesteld.

Aan de samenvatting en privacy-analyses kunnen geen rechten worden ontleend. Voor onjuistheden of onvolledigheden op deze samenvatting aanvaardt Pels Rijcken geen aansprakelijkheid. Op de samenvatting en privacy-analyses zijn de algemene voorwaarden van Pels Rijcken & Droogleever Fortuijn N.V. van toepassing, te raadplegen via https://www.pelsrijcken.nl/algemene-voorwaarden.
Op de samenvatting en privacy-analyses van Pels Rijcken rust tot slot auteursrecht. Niets uit deze samenvatting en privacy-analyses mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand of openbaar worden gemaakt, in enigerlei vorm of wijze, hetzij elektronisch, mechanisch, door fotokopieën, opname of enige andere manier. Dit is alleen toegestaan na voorafgaande schriftelijke toestemming van Pels Rijcken.

Rathenau Instituut

De Corona-crisis vraagt om zorgvuldig handelen en democratisch debat

Bericht aan het Parlement

Het Coronavirus eist mensenlevens, brengt ernstige gezondheidsschade toe en legt de maatschappij momenteel grotendeels stil. Om de lock-down te versoepelen overweegt de regering de mogelijke inzet van twee soorten apps. Met een 'gezondheidsapp' kunnen burgers hun symptomen monitoren en op afstand begeleid worden. Een 'tracking- en tracing-app' draagt bij aan bron- en contactopsporing, zoals de GGD dat normaal gesproken uitvoert.

Maatschappelijke partijen en experts hebben hun zorgen geuit over de betrouwbaarheid en de doelmatigheid van dergelijke Corona-apps. Bovendien stuit de ontwikkeling en inzet van deze apps op ernstige principiële bezwaren met betrekking tot publieke waarden en mensenrechten. Deze bezwaren vragen om politieke deliberatie. Het Rathenau Instituut heeft de afgelopen jaren onderzoek gedaan naar de verantwoorde inzet van AI en apps, waaronder in het medische domein. Op basis daarvan geeft het Instituut de Tweede Kamer voor de hoorzitting over de Corona-apps vijf overwegingen mee.

Het Coronavirus eist een ingrijpende tol van de Nederlandse samenleving – in mensenlevens, in gezondheidsschade, in welvaart en in sociaal contact. De crisis stelt Nederland, en andere landen, voor de uitdaging om de publieke gezondheid te beschermen, de economische schade te beperken en de samenleving als geheel weerbaar te maken: hoe kan de Nederlandse samenleving snel en adequaat reageren op deze virusuitbraak? En hoe kunnen we veilig, en met inachtneming van publieke waarden en mensenrechten, de samenleving weer op gang brengen?

Het kabinet verkent als onderdeel van de aanpak de ontwikkeling van twee Corona-apps om, tenminste gedeeltelijk, de lock-down af te bouwen en naar een nieuwe normale situatie te gaan. In die situatie moeten nieuwe uitbraken van het coronavirus voorkomen worden. De vraag die tijdens de hoorzitting voorligt is of, en in hoeverre, de voorgestelde apps hieraan een bijdrage kunnen leveren.

Bij de beantwoording van deze vraag moet bijzondere aandacht uitgaan naar de voorwaarden die gelden in het medische domein, publieke waarden en mensenrechten en het behouden van het vertrouwen en de medewerking van burgers. Dit blijkt uit onderzoeken van het Rathenau Instituut. Ook diverse maatschappelijke organisaties en experts roepen op om deze aspecten helder voor ogen te houden. De regering heeft kenbaar gemaakt bij de ontwikkeling van deze Corona-apps de privacy te beschermen.

Het Rathenau Instituut geeft de Tweede Kamer vijf overwegingen mee om de parlementaire discussie te informeren:

1. Versterk de publieke gezondheidsinfrastructuur.
2. Beoordeel de inzet van Corona-apps in het kader van publieke gezondheid: niet als de kern van de oplossing, maar als één beleidsoptie.
3. Neem de tijd om de Corona-apps zorgvuldig, met aandacht voor alle relevante aspecten, te onderzoeken.
4. Bouw kennis op over de Corona-apps, en andere beleidsopties, om richting te geven aan de internationale en Europese beleidsontwikkeling.
5. Handel zodanig dat burgers vertrouwen houden in de aanpak van de Corona-crisis.

1. Versterk de publieke gezondheidsinfrastructuur

Om het Coronavirus effectief het hoofd te bieden, zal een structurele versterking van de publieke gezondheidsinfrastructuur nodig zijn. We zullen ook over een half jaar, over een jaar, en misschien wel over twee jaar moeten beschikken over de middelen om zowel het Coronavirus te bestrijden als de reguliere zorg te organiseren. Dit betekent dat er, onder andere, structureel meer IC-bedden, IC-personeel, beschermingsmiddelen, testcapaciteit en GGD-capaciteit nodig zullen zijn. Deze versterkte infrastructuur vormt het fundament van een weerbare samenleving, en

verdient prioriteit. Het is cruciaal om te voorkomen dat deze infrastructuur bij een toekomstige uitbraak tekort schiet, en met spoed weer opgebouwd moet worden. Het is van belang dat de Tweede Kamer de inspanningen van het kabinet nauwlettend volgt.

2. Beoordeel de inzet van Corona-apps in het kader van publieke gezondheid: niet als de kern van de oplossing, maar als één beleidsoptie

Om het virus terug te dringen en de samenleving weer op gang te brengen, is het belangrijk de publieke gezondheidsinfrastructuur aan te vullen met een combinatie van innovaties en maatregelen. Denk aan innovaties zoals nieuwe medische behandelingen, en maatregelen zoals verfijnde social distancing-normen, en uitgewerkte bevoegdheden van burgermeesters.

Apps kunnen een onderdeel vormen van dit pakket – maar dat is geen onvermijdelijke keuze. Apps vormen niet de kern van de oplossing, maar zijn een beleidsoptie die naast en in samenhang met andere beleidsopties overwogen kan worden. Het gaat erom de combinatie van innovaties en maatregelen te kiezen die effectief is met betrekking tot de publieke gezondheid, en tegelijkertijd mensenrechten en grondrechten niet onder druk zet, en het vertrouwen van de burger behoudt. Het pakket moet proportioneel zijn. Het is gezien de bezwaren die ten aanzien van de apps geuit zijn, de vraag of deze apps aan de eis van proportionaliteit voldoen. Ook de Tweede Kamer kan het kabinet vragen naar de proportionaliteit van de uiteindelijke aanpak.

3. Neem de tijd om de Corona-apps zorgvuldig, met aandacht voor alle relevante aspecten, te onderzoeken

Omdat de mogelijkheid bestaat dat apps het contactenonderzoek en de monitoring van patiënten vereenvoudigen en verbeteren, is het belangrijk deze apps te onderzoeken. Het is zaak voor dat onderzoek de tijd te nemen, om recht te doen aan de relevante technische, maatschappelijke, ethische en juridische aspecten. De geschiedenis van digitale innovaties leert dat zorgvuldigheid geboden is en dat er altijd lastige kwesties boven komen drijven. Hoe ga je om met werkgevers die de apps van werknemers in willen zien? Hoe zorg je ervoor dat de dataverzameling daadwerkelijk anoniem is? Bovendien kampen nieuwe digitale toepassingen vrijwel altijd met praktische uitvoeringsproblemen – dit zal ook voor de Corona-apps gelden.

Onderzoek van het Rathenau Instituut laat zien dat AI-innovaties vaak technisch onvolkomen zijn, en door onbetrouwbare metingen of beperkte algoritmes geen goed oordeelsvermogen hebben. In het geval van de te ontwikkelen Corona-app werd al gewezen op de beperkingen van het bluetooth-signaal. Realisme is op zijn plaats: een betrouwbare en veilige app is niet eenvoudig te ontwikkelen.

Bovendien blijkt uit ons onderzoek dat succesvolle e-health apps voldoen aan specifieke voorwaarden. Bijvoorbeeld dat er sprake is van een behandelrelatie tussen

een patiënt en een arts. Ook voor Corona-apps moet uitgezocht worden onder welke voorwaarden burgers de apps vertrouwen en gebruiken. Er zijn kaders nodig voor het uitvoeren en beoordelen van experimenten met de apps. Wie gaan de data verzamelen en analyseren? Wie bepaalt of de werking van de apps voldoende is? Het beantwoorden van al deze vragen zal tijd kosten. Het is te midden van een zeer ingrijpende crisis onverminderd nodig om zorgvuldig na te denken en te handelen, en daarbij burgers, experts en volksvertegenwoordigers te betrekken. De Tweede Kamer kan het kabinet vragen naar de kaders voor de ontwikkeling van de apps, en vragen om bij de evaluatie van de apps betrokken te worden.

4. Bouw kennis op over de Corona-apps, en andere beleidsopties, om richting te geven aan de internationale en Europese beleidsontwikkeling

Ook op Europees niveau wordt overwogen apps te ontwikkelen, of die ontwikkeling te coördineren. Het is van belang dat het kabinet, door de apps te laten onderzoeken, voldoende expertise opbouwt om aan deze Europese coördinatie richting te geven. Ook over de betekenis van immuniteit en vaccinatie moeten internationale afspraken gemaakt worden. Wanneer kunnen personen zich weer vrij verplaatsen?

Maar er speelt ook een ander belang. Juist in de Corona-crisis staan democratische en autocratische denkbeelden en oplossingen tegenover elkaar. Het kabinet is gecommitteerd aan publieke waarden en zet het belang van mensenrechten en democratische rechten van burgers centraal. Het is cruciaal dat Europa erin slaagt om een proportioneel en democratisch antwoord te geven op dit virus, dat onze gedeelde publieke waarden versterkt. De Tweede Kamer kan het kabinet vragen om inzicht te geven in de ontwikkelingen op internationaal en Europees niveau.

5. Handel zodanig dat burgers vertrouwen houden in de aanpak van de Corona-crisis

Bij het bestrijden van een epidemie staat menselijk gedrag centraal, en speelt de burger een belangrijke rol. Van burgers wordt bijvoorbeeld verwacht dat ze afstand houden, regelmatig hun handen wassen, in de elleboog hoesten en alleen boodschappen doen. Dit vraagt veel van burgers, en de onderlinge solidariteit in de samenleving. Daarom is het essentieel dat burgers vertrouwen houden in de overheid, de kennis en het advies van experts, en technologie.

Ondermijning van dat vertrouwen zet het succes van iedere aanpak op het spel. De afgelopen weken is veel geleerd en nog meer afgeleerd. Burgers vormen het sociaal kapitaal waarmee Nederland de Coronacrisis aanpakt. Net als onze gezondheid is ook dat sociaal kapitaal kwetsbaar. Apps hebben alleen zin als ze burgers echt helpen, hun goede gewoontes ondersteunen en geen schijnveiligheid creëren.

Onderliggende publicaties van het Rathenau Instituut

Waardevol digitaliseren - Hoe lokale bestuurders vanuit publiek perspectief mee kunnen doen aan het 'technologiespel'

Doelgericht digitaliseren – Hoe Nederland werkt aan een digitale transitie waarin mensen en waarden centraal staan

Gezondheid centraal – Zorgvuldig data delen in de digitale samenleving

Zo brengen we AI in de praktijk vanuit Europese waarden

Rathenau.nl

© Rathenau Instituut