

Een App als Digitaal Hulpmiddel

Achtergronden bij traceren en informeren¹

(Concept)

Bart Jacobs, Peter Boncz, Danny Mekić
2 juni 2020

Over de inzet van een of meerdere apps bij de beheersing van het Corona virus (Covid-19) bestaat veel onduidelijkheid. Dit document beoogt brede achtergrondinformatie te verschaffen over het gebruik van zulke apps in de ‘pre-medische’ fase, voordat sprake is van testen of behandelen. Het gaat hier dus niet om apps voor het monitoren van de eigen gezondheid of voor zelf-rapportage, maar wel om apps voor het bijhouden (traceren) van contacten en het notificeren (waarschuwen, informeren) van mensen die in contact zijn geweest met iemand die reeds door het virus besmet is. Dit document verkent met name de mogelijkheden om de gebruikte techniek (ICT) zo nauw mogelijk te laten aansluiten bij het (huidige) epidemiologische begrip van de verspreiding van het virus. Juist door zo’n nauwe aansluiting kan een app mogelijk meerwaarde hebben, naast het bestaande bron- en contact-onderzoek (BCO) van de GGDs dat, los van een eventuele app gewoon doorgaat.

Inhoudsopgave

1	Achtergrond over Corona / Covid-19	2
2	Notitie of notificatie?	3
2.1	Globale werking van een notificatie app	5
3	Doelen van een notificatie app	6
4	Het notificatie bericht	8
4.1	Maatschappelijke kontekst van notificatie	9
5	De rol van de GGD bij een notificatie app	10

¹Met dank aan Hester de Vries, Erik Buskens en Jan Kluytmans voor discussie en commentaar.

6	Evaluatie van een notificatie app	13
7	Wettelijke basis van een notificatie app	14
8	Technische realisaties van een app	16
9	Afsluitende opmerkingen	19

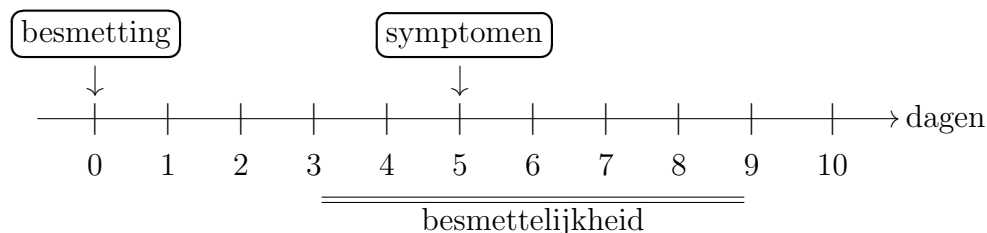
1 Achtergrond over Corona / Covid-19

Nauwe aansluiting van de werking van een (notificatie) app op de epidemiologische werkelijkheid is van groot belang voor de effectiviteit van een app als digitaal hulpmiddel bij de beheersing van het Corona virus. Daarom kan zo'n app niet goed beschreven en begrepen worden zonder enig epidemiologisch inzicht in het Corona virus.

- Van de personen die besmet raken met het virus vertoont een nog onbekend deel geen of heel weinig symptomen van de ziekte (waaronder koorts en droge hoest) en is dus *asymptomatisch*. Een schatting is dat het gaat om 10-20%. Deze personen kunnen het virus wel overdragen, maar waarschijnlijk in beperktere mate dan mensen die wel verschijnselen vertonen.
- Corona heeft naast een asymptomatische ook een *presymptomatische* besmettelijkheid. Dat wil zeggen dat besmette mensen het virus kunnen overdragen voordat verschijnselen van het virus zich bij hen zelf manifesteren.
- Ongeveer 40% van de besmettingen (transmissies) lijkt plaats te vinden in deze presymptomatische fase. Juist dit maakt de ziekte moeilijk te stoppen.
- Ongeveer 60% van de de besmette personen heeft milde symptomen. Van degenen met zware symptomen (20%) moet een kwart (5% van het totaal) naar het ziekenhuis. Ongeveer 1% overlijdt.

Als symptomen zich manifesteren, dan is dat gemiddeld 5 dagen na besmetting. Echter, besmettelijkheid begint vanaf de derde dag en duurt zo'n 6

dagen. Het volgende diagram geeft een overzicht. Het gaat vooral om de onderlinge verhouding, niet zozeer om de precisie.



De ‘gevaarlijke’ presymptomatische besmettelijkheid is ongeveer van dag 3 tot 6.

Aanwezigheid van het Corona virus wordt vastgesteld met de zogenaamde PCR-test. Die test kent nauwelijks vals-positieven, in de zin dat de test vertelt dat je drager bent van het virus, terwijl dat niet zo is.

De PCR-test werkt niet in de eerste dagen na de besmetting. De test heeft een hoog percentage van vals-negatieven: de test zegt dan onterecht dat je geen drager bent. Dat percentage hangt af van het aantal dagen na de besmetting. Volgens een recente (overzichts)studie² daalt dit percentage vals-negatieven tot zo’n 67% op dag 4 en tot zo’n 20% op dag 8. Dit geeft een lastig dilemma: vroeg testen geeft een onbetrouwbare (negatieve) uitslag, maar laat testen heeft als nadeel dat besmetting lang onbekend blijft waardoor de vereiste voorzichtigheid en/of maatregelen mogelijk niet toegepast worden.

Deze epidemiologische inzichten zijn zeer relevant voor het formuleren van het notificatie bericht dat gebruikers van de app kunnen ontvangen, zie § 4, na contact met een besmette persoon, en voor het vaststellen van eventueel nut van de app (zie § 6).

2 Notitie of notificatie?

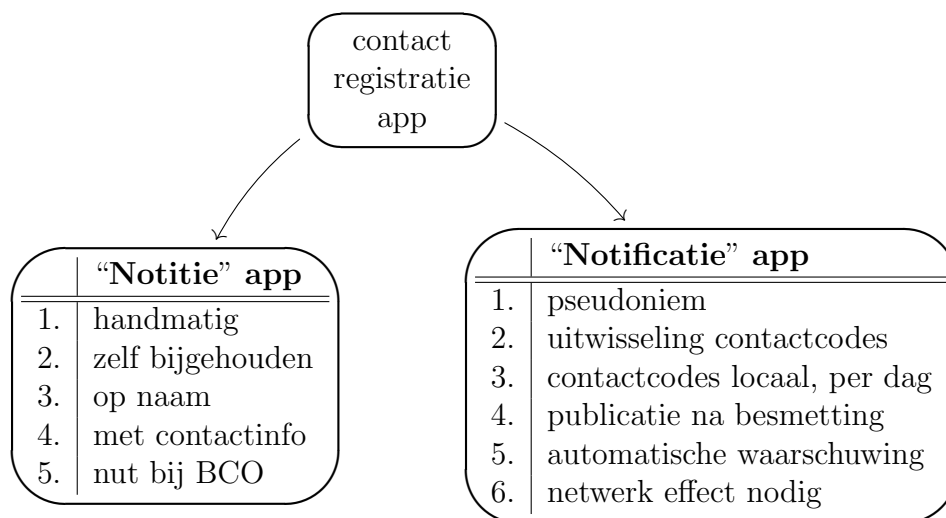
Bron- en contactonderzoek (BCO) is een belangrijke activiteit bij de beheersing van een epidemie, waarvoor de gemeenten (via hun GGDs) verantwoordelijk zijn. “Het doel van bron- en contactonderzoek is om contacten te identificeren, hen te informeren over de blootstelling en risico op besmetting, hen te wijzen op maatregelen die genomen moeten worden om verdere

²Zie: acpjournals.org/doi/10.7326/M20-1495.

verspreiding te voorkomen en hen hierin te begeleiden.”³

Twee belangrijke elementen uit dit citaat zijn: *identificeren* van contacten en *informer*en. Voor dat laatste worden ook de termen ‘notificeren’ en ‘waarschuwen’ gebruikt. Dit identificeren en informeren kan zowel handmatig (door een mens) als geautomatiseerd (via een app) plaatsvinden. Bij het identificeren via een app heeft het ministerie van VWS de eis gesteld dat dit anoniem⁴ en zonder locatie gegevens (van GPS of GSM) moet gebeuren. Dat kan gerealiseerd worden via de uitwisseling van zogenaamde contactcodes. De technische details daarvan zijn in dit stadium niet direct relevant maar komen later wel aan de orde (zie § 2.1 en § 8).

Om te beginnen kunnen twee type apps onderscheiden worden voor het registreren van contacten, aangeduid als *notitie* en *notificatie* app.



Een notitie app biedt de gebruiker enkel een speciaal notitieboekje op de telefoon waarin ‘relevante’ contacten van enige intensiteit (duur, relatieve nabijheid) door de gebruiker zelf worden genoteerd. Die registratie kan bestaan uit enkel de dag, tijd en persoon (“Hugo”), naar analogie van een agenda afspraak. Of zo’n registratie plaatsvindt wordt volledig door de gebruiker zelf bepaald — maar de app zou hiervoor wel algemene richtlijnen kunnen bieden.

³Citaat van de webpagina: lci.rivm.nl/COVID-19-bco, waar meer informatie te vinden is.

⁴De notificatie app zoals voorzien maakt echter geen gebruik van *anonieme* maar van *pseudonieme* gegevens: niet iedere mogelijkheid om een gegeven met een persoon in verband te brengen is uitgesloten, zie § 7. Op pseudonieme gegevens is de AVG van toepassing.

De registraties in de app kunnen nuttig zijn als geheugensteun bij het BCO-gesprek bij de GGD en kunnen ertoe leiden dat de GGD contact opneemt met de betreffende personen, op basis van de verschafte contactinformatie, en dat de GGD hen informeert en adviseert.

Zo'n notitie-app is een eenvoudig hulpmiddel dat nuttig kan zijn, vooral ook omdat de aanpak niet afhankelijk is van een netwerk effect: iedere persoon die de notitie-app gebruikt en besmet raakt levert voordeel op voor BCO, onafhankelijk van wat anderen doen. Natuurlijk kan men de vraag stellen of hier een aparte app voor nodig is. De autoriteiten zouden iedereen ook kunnen oproepen dagelijks in hun agenda te noteren met wie ze een 'relevant' contact hebben gehad. Men kan zich erover verbazen waarom dat nog niet gedaan is.

Voor GGDs is een notitie app in principe interessant omdat die direct aansluit bij hun bestaande BCO-activiteiten. In dit document zal echter niet verder ingegaan worden op zulke notitie apps. Het vervolg zal zich richten op een notificatie app. Zo'n notificatie app is voor GGDs echter niet of nauwelijks interessant: de app functioneert pseudoniem en levert geen contact informatie op die direct bruikbaar is in het bestaande proces. Een notificatie app functioneert dan ook (grotendeels) los van de activiteiten van GGDs: de app staat "ernaast" en dient een aanvulling te zijn. In § 5 wordt nader ingegaan op de GGD en de app; § 6 beschrijft hoe zo'n notificatie app zijn (aanvullende) nut zou kunnen bewijzen.

2.1 Globale werking van een notificatie app

Later in § 8 worden twee mogelijke technische realisaties beschreven van een notificatie app. Het kenmerkende verschil tussen deze twee realisaties zit in hoe een "relevant contact" bepaald wordt. Dat kan bijvoorbeeld automatisch vastgesteld worden via Bluetooth, of handmatig via het scannen van een QR-code. Van dit onderscheid wordt hier geabstraheerd: er wordt aangenomen dat op enigerlei wijze relevantie van een contact vastgesteld kan worden.

Bij zo'n relevant contact slaan de betrokken notificatie apps (allebei) een willekeurig groot getal op. Hoe dit getal tot stand komt is in dit stadium niet belangrijk. De app slaat niet het precieze tijdstip van de ontmoeting op, maar wel de dag waarop die ontmoeting plaatsvond. Deze getallen worden niet langer dan 14 dagen in de app bewaard. Ze worden alleen lokaal in de notificatie app zelf opgeslagen, en niet (ook) nog ergens anders, bijvoorbeeld in de cloud.

Bij vaststelling van een besmetting van een persoon die de notificatie app gebruikt worden de getallen uit diens app uitgelezen (door een bevoegde persoon, over een relevante periode) en via een (web)server publiek gemaakt.

Iedere app haalt regelmatig, bijvoorbeeld ieder uur, van deze server de gepubliceerde getallen op. Als zo'n app een van die getallen herkent, dan is er sprake geweest van contact met de besmette persoon, op een bepaalde dag, niet langer dan 14 dagen geleden. De app kan in dat geval een waarschuwing afgeven: op die-en-die dag heeft u contact gehad met iemand die besmet bleek te zijn. De app zal niet (kunnen) vertellen om welke persoon het ging. Op de verder inhoud van zo'n waarschuwingsbericht en op het bijbehorende handelingsperspectief wordt verder ingegaan in § 4.

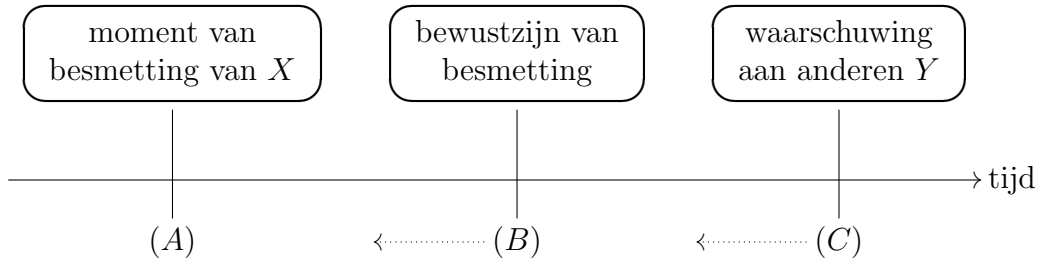
Het bovenstaande beschrijft zogenaamd *voorwaarts* waarschuwen: je waarschuwt de personen die *als gevolg van* een gekende besmetting mogelijk ook besmet zijn geraakt. Je zou in principe ook *achterwaarts* kunnen waarschuwen: je probeert dan de mensen te bereiken *als gevolg waarvan* de gekende persoon besmet is geraakt. Dat zou kunnen door contactcodes uit een andere periode (via een andere server) bekend te maken, zie het diagram in § 1. Dit is mogelijk zinvol bij Corona vanwege het asymptomatische en presymptomatische karakter. Er is echter nog weinig onderzoek gedaan naar achterwaarts waarschuwen. Het komt hier dan ook verder niet aan bod.

3 Doelen van een notificatie app

Het specifieke doel van een notificatie app bij de beheersing van de verspreiding van het Corona virus lijkt te zijn: snel, gericht en geautomatiseerd waarschuwen van mensen die in contact zijn geweest met een reeds besmette, positief geteste persoon. Indien de betrokkenen namelijk een app gebruiken om onderlinge contacten (min of meer) systematisch vast te leggen, dan kunnen die geregistreerde contacten de basis vormen voor gerichte waarschuwingen, see § 2.1.

Het volgende schema beschrijft drie opeenvolgende momenten voor een

individu X die besmet raakt.



Aan de hand van dit schema kunnen de volgende doelen van een notificatie app geïdentificeerd worden, los van de gebruikte techniek.

Doel 1 De tijdspanne tussen (A) en (B) wordt verkleind, door besmetting bij persoon X eerder vast te stellen. Hierbij kan een notificatie app van X helpen, als *ontvanger* van waarschuwingen: de app waarschuwt X over een eerder (risicovol) contact tussen X en een reeds besmette andere persoon, die de oorzaak is van de besmetting (A) van X .

Doel 2 De tijdspanne tussen (B) en (C) wordt verkleind, door alle personen Y die een (risicovol) contact met X hebben gehad snel te waarschuwen, om zo de risico's voor Y zelf en voor anderen met wie Y weer contact heeft te verkleinen (zie doel 1, met Y in de rol van X). Ook hier kan de notificatie app van X helpen, maar nu als *bron* van waarschuwingen. Wanneer die app van X een (min of meer) volledig overzicht verzameld heeft van zulke eerdere contacten die X met anderen Y gehad heeft kan Y een waarschuwing ontvangen. Bij de traditionele methode komt zo'n waarschuwing via de GGD, die zelf contact opneemt (via de telefoon of e-mail) met Y na een BCO-gesprek.

Doel 3 Personen Y worden bereikt (en gewaarschuwd) die nu niet via traditioneel bron- en contact-onderzoek (BCO) bereikt worden, zie § 6.

Doel 4 De beschikbare test-capaciteit wordt gericht ingezet. Een waarschuwing in een notificatie app kan een goede reden zijn om de gebruiker van de app een test te laten ondergaan, zie § 4.

Doel 5 Brandhaarden worden gedetecteerd.

4 Het notificatie bericht

Een notificatie app kan de gebruiker waarschuwen — wanneer de app zelf een gepubliceerde contactcode blijkt te bezitten, zie § 2.1, als gevolg van een eerdere ontmoeting met een besmette persoon. De vraag is dan: wat moet er in het waarschuwingsbericht staan, in het bijzonder, welk handelperspectief moet aan de zojuist gewaarschuwde gebruiker van de app geboden worden? Hieronder wordt eerst ingegaan op de persoonlijke aspecten van zo'n bericht. Vervolgens wordt ook kort aandacht besteed aan de sociale aspecten (in § 4.1).

Om te beginnen moet het bericht helder en begrijpelijk zijn. Het moet nuttige, feitelijke informatie bevatten en moet geen paniek zaaien. Dit aspect van de communicatie is een onderwerp op zich. Hier zal echter de nadruk liggen op de inhoud van het advies.

Omdat notificatie apps zo ontworpen zijn dat ze hun waarschuwing afgeven na een eerder 'gevaarlijk' contact dient het waarschuwingsbericht zich te richten op een adequate reactie op dat gevaar. De gebruiker van de app dient dan ook gewezen te worden op het risico dat hij/zij zelf besmet is geraakt. De twee meest logische adviezen zijn dan ook:

1. ga zelf onmiddellijk in quarantaine;
2. laat jezelf testen: bel dit nummer en maak een afspraak.

Het bieden van zo'n testmogelijkheid is redelijk, enerzijds omdat de persoon in kwestie een (gerechtvaardigde) behoefte aan zekerheid kan hebben, en anderzijds als onderbouwing om juist wel of niet de quarantaine voort te zetten.

Het moeilijke element hier bij is: hoeveel dagen na de waarschuwing in de app kan die test het beste plaatsvinden? Hierbij spelen twee aspecten een rol.

- Zoals beschreven in § 2.1 onthoudt de notificatie app van iedere contact de *dag* waarop de bijbehorende contactcodes zijn opgeslagen. Wanneer de app dus een gepubliceerde contactcode herkent, kan de app berekenen hoeveel dagen geleden dit 'gevaarlijke' contact heeft plaatsgevonden.
- Zoals beschreven in § 1 heeft een (PCR) test snel na besmetting geen enkele zin vanwege het hoge percentage vals-negatieven. Het kan dus

verstandig zijn een paar dagen te wachten met een test (maar dan wel in quarantaine).

Stel dat vanuit epidemiologisch perspectief een test pas n dagen na besmetting het meest zinvol is. En stel dat de app weet dat het gevaarlijke contact m dagen geleden plaatsgevonden heeft. De app dient dan zelf een verfijnd test-advies te formuleren:

- (a) als $m \geq n$, dan toont de app het advies: laat je zo snel mogelijk testen!
- (b) maar als $m < n$, dan is het advies: maak een afspraak voor een test over $n - m$ dagen.

Gezien het hoge percentage vals-negatieven van een PCR-test is het redelijk om bij een negatieve uitslag de mogelijkheid te bieden om een nieuwe test te ondergaan, een paar dagen later.

4.1 Maatschappelijke kontekst van notificatie

Hierboven is gesproken over het notificatie bericht in relatie tot de gebruiker van de app. Maar er is een bredere maatschappelijke kontekst die aandacht verdient. Ook daaraan zal bij introductie van de app aandacht besteed moeten worden zodat mensen weten waar ze aan toe zijn. Hieronder worden twee voorbeelden geschetst.

Om te beginnen dient zich de vraag aan: wordt er in het waarschuwingsbericht in de app ook op aangedrongen om de waarschuwing in de eigen omgeving bekend te maken? In een gezinssituatie zal de ontvanger van het bericht dat waarschijnlijk wel doen. Maar zal een zelfstandig ondernemer zijn klanten willen informeren en vervolgens ook zijn werkzaamheden (en dus inkomstenbron) willen stilleggen? Gaat de overheid daar compensatie voor bieden? Stel de persoon in kwestie kiest er voor om door te werken en besmet anderen. Als later op enig moment blijkt dat deze persoon een app-waarschuwing ontvangen heeft, is hij/zij dan aansprakelijk? Wordt in de waarschuwing uitgelegd welke rechtsgevolgen of compensatiemogelijkheden het bericht heeft?

De app is vooral bedoeld om te functioneren in een ‘nieuw normaal’ waarbij het maatschappelijke verkeer weer op gang gekomen is. Het volgende voorbeeld is dus realistisch. Werknemer X gebruikt een notificatie app en voert werk uit dat alleen op locatie kan plaatsvinden, samen met collega’s

en/of klanten. Op een goed moment krijgt X een waarschuwing in de app over een mogelijk gevaarlijk contact en krijgt het bovengenoemde advies om in quarantaine te gaan en zich te laten testen. Vermoedelijk zal X zich dan ziek melden op het werk. Biedt een bericht in de app daarvoor voldoende grond? Wordt van X verwacht dat hij/zij een screenshot van de waarschuwing naar de bedrijfsarts stuurt als onderbouwing van de ziekmelding? Zo'n screenshot biedt geen enkele zekerheid want het waarschuwingsbericht is niet aan de identiteit van de gebruiker van de app gebonden⁵. Of wil de bedrijfsarts meer zekerheid en bijvoorbeeld ook weten dat X de test ondergaan heeft en wat de uitslag is? Stel dat de waarschuwing vals-positief blijkt te zijn (zie ook § 6), dan lijden werkgever en werknemer schade. Is het ministerie van VWS daarvoor aansprakelijk?

5 De rol van de GGD bij een notificatie app

De notificatie app is bedoeld als *aanvullend* op het bestaande bron- en contact-onderzoek (BCO) van de GGD en zou daar geheel los van staan. Dat is een *onjuist* beeld. Voor deugdelijke werking en evaluatie van de app⁶ zal er sprake moeten zijn van brede integratie met GGD-werkzaamheden, met name in het kader van het testen en van de BCO-gesprekken, na vaststelling van een besmetting (via een positieve test). Het gaat dan om de volgende punten.

1. Als onderdeel van het afnemen van een PCR-test zal door de GGD gevraagd moeten gaan worden: “gebruikt u een notificatie app, en zo heeft die app u gewaarschuwd?” Als het antwoord “ja” is, is er sprake van een *true positive*: een terechte waarschuwing. Als het antwoord “nee” is, levert de app een vals-positieve waarschuwing. Deze gegevens zijn essentieel voor evaluatie van de app, zie § 6.
2. Bij een positieve uitkomst van de test volgt een BCO-gesprek met een GGD-medewerker. Voor het gemak wordt de persoon in kwestie aangeduid met X . Een belangrijk onderdeel van het BCO-gesprek is het

⁵Er zullen dan ook snel screenshots online verschijnen die gebruikt kunnen worden voor zulke ziekmeldingen.

⁶en van de instellingen van de app. Bij een op Bluetooth gebaseerde notificatie app zouden deze gegevens gebruikt kunnen worden om de gevoeligheid van de app aan te passen.

proberen te achterhalen wat het meest waarschijnlijke moment van besmetting van X is geweest — en ook op welke plaats. De GGD-medewerker zal ongetwijfeld aan X vragen of er besmette personen in dienst omgeving zijn met wie er contact is geweest. Maar de medewerker kan ook vragen: “Weet u of iemand in uw omgeving de app gebruikt en een waarschuwing ontvangen heeft? Zo ja, waar/wanneer heeft u met die persoon contact gehad?” Deze gewaarschuwde persoon zou namelijk zelf besmet kunnen zijn, en daarmee de bron van de besmetting van X kunnen zijn. De waarschuwingen uit de omgeving van X kunnen dus nuttig zijn bij het traceren van de bron.

3. De notificatie app van X kan mogelijk op nog een andere manier een bijdrage leveren in het BCO-gesprek, indien de app opslaat hoeveel relevante contacten van X er per dag gedurende de afgelopen 14 dagen hebben plaatsgevonden. Deze opgeslagen contactcodes zeggen niks over die contacten zelf, maar de aantallen contacten op een dag, indien zichtbaar, kunnen wel gebruikt worden door de GGD-medewerker als een geheugensteun voor X : “ik zie in de registratie van uw app dat u op die dag zoveel contacten had; kunt u zich herinneren, of kunt u opzoeken, met wie en waar dat was?”
4. Indien persoon X een notificatie app gebruikt is de (vermoedelijke) dag van besmetting zeer belangrijk, namelijk om te weten welke contactcodes⁷ uit de app van X publiek gemaakt moeten worden. Alleen de codes in de dagen 3-9 na die dag van besmetting van X doen ertoe, zie het plaatje in § 1, omdat er alleen in die dagen een besmettingsgevaar is. Het is belangrijk om zo min mogelijk contactcodes te publiceren om onnodige waarschuwingen te voorkomen (zie § 6). Het is belangrijk het tijdstip van publicatie goed te registreren want dit speelt een rol bij evaluatie van de app, zie onderstaand punt 7.
5. Na bepaling van deze (publicatie) periode moeten de contactcodes uit de notificatie app van X gelezen worden door een bevoegde persoon om vervolgens gepubliceerd te worden via een server. Deze extractie en publicatie handelingen dienen direct na het BCO-gesprek plaats te

⁷Om redenen van efficiëntie kan worden volstaan met het publiceren van de ‘dag’ sleutels die deze contactcodes genereren, maar dit aspect wordt hier bewust achterwege gelaten om de uiteenzetting niet nodeloos ingewikkeld te maken.

vinden — om anderen zo snel mogelijk te kunnen waarschuwen via hun app — en kunnen daarom het beste door de GGD verricht worden.

Terzijde: op deze wijze worden alleen van mensen die positief getest zijn de contactcodes gepubliceerd. In het licht van de hoge percentages vals-negatieven van de PCR-test kan men een aanvulling overwegen: indien iemand een waarschuwing in de eigen app ontvangen heeft en bovendien de huisarts verschijnselen van Corona constateert, zou ook tot publicatie van contactcodes overgegaan kunnen worden, zonder dat een test met positieve uitslag heeft plaatsgevonden.

6. De GGD is in de positie om gegevens te verzamelen voor evaluatie van de effectiviteit van de notificatie app (zie § 6), niet alleen bij het testen (zie punt 1), maar ook bij BCO-gesprekken en bij de opvolggesprekken, dat wil zeggen bij reguliere informeren door de GGD van de door X genoemde personen (zie het volgende punt 7). In het BCO-gesprek moet nogmaals gevraagd worden aan X : “Gebruikt u zelf een notificatie app en heeft die app u ook gewaarschuwd?”. Hiermee komen de vals-negatieven van de app beter in beeld. Deze vraag is een aanvulling op dezelfde vraag bij het uitvoeren van de test in punt 1 want er zit een tijdsverschil tussen het uitvoeren van de test en het BCO-gesprek, waardoor X inmiddels wel een waarschuwing ontvangen kan hebben.
7. Voor het verkrijgen van evaluatiegegevens over een notificatie app tijdens opvolggesprekken is de juiste volgorde van belang.
 - (a) BCO-gesprek met X ;
 - (b) publicatie van relevante contactcodes van X , zeg op tijdstip t ;
 - (c) opvolggesprekken van de GGD met door X genoemde personen Y .

Indien er minstens een uur tijd zit tussen (b) en (c) zijn de gepubliceerde contactcodes van X opgehaald door andere notificatie apps en hebben de gebruikers van die apps een waarschuwingsbericht ontvangen in hun app. Tijdens het opvolggesprek dienen de GGD-medewerkers dan ook te vragen: “gebruikt u een notificatie app en heeft u een waarschuwing ontvangen”. Sterker nog, er kan gevraagd worden: “heeft u die waarschuwing ergens in het uur na tijdstip t ontvangen?” Zo ja, dan is de waarschuwing met enige waarschijnlijkheid het gevolg van het

contact met X . Zulke informatie geeft de GGD zicht op de sporen van besmettingen. Als de app geen waarschuwing heeft gegeven aan Y kan dit gezien worden als een vals-negatief van de app.

6 Evaluatie van een notificatie app

Er is veel discussie over nut en noodzaak van een notificatie app. De houding die het ministerie van VWS in die discussie heeft aangenomen is: als het niet werkt stoppen we er gewoon weer mee. Maar hoe evalueer je of zo'n app werkt of niet? Zijn de doelen die genoemd zijn in § 3 meetbaar, en wel op zodanige wijze dat bepaalde effecten exclusief aan een notificatie app toe te wijzen zijn? Dat is geen eenvoudige zaak. Zoals hierboven in § 5 reeds beschreven — met name in punten 1, 6 en 7 — heeft de GGD een belangrijke rol bij het verzamelen van gegevens voor evaluatie van de werking van de app.

Een **eerste** criterium is het aantal gebruikers van de notificatie app — uitgedrukt bijvoorbeeld als percentage van de bevolking. Dit percentage is bij benadering af te leiden uit het aantal downloads van de app, dat gepubliceerd wordt in de appstores (van Google en Apple). Factoren die het percentage gebruikers beïnvloeden zijn, bijvoorbeeld: vertrouwen in de gebruikte techniek en in het proces, kwaliteit van de *user experience* (UX) inclusief perceptie van controle, beeldvorming in de media, privacy en security incidenten. De minister van VWS heeft een percentage van 60% genoemd als noodzakelijk voor effectieve werking. Als dit percentage niet gehaald (of benaderd) wordt zou dus meteen al gezegd kunnen worden: het werkt niet.

In het vervolg van deze sectie wordt er van uitgegaan dat een voldoende hoog percentage van gebruikers bereikt wordt.

Een **tweede** criterium is het percentage vals-positieven van de app. Het gaat daarbij om gebruikers van de app die een waarschuwing in hun app ontvangen maar die na een test niet besmet blijken te zijn. Zo'n vals alarm is misschien uiteindelijk een opluchting voor de gebruiker, maar deze gebruiker zal het de (verantwoordelijke voor de) app mogelijk kwalijk nemen onterecht paniek gezaaid te hebben, onnodige stress te hebben veroorzaakt, en tijd en geld (in quarantaine) en moeite (voor een test) verspild te hebben. Dit komt het draagvlak en de reputatie van de app niet ten goede. Zal aan de gebruiker ook uitgelegd worden dat een ogenschijnlijk vals-positieve waarschuwing het gevolg kan zijn van het hoge percentage vals-negatieven van de PCR-test? Dat is een communicatie-uitdaging. Zal bij een negatieve uitslag een tweede

test-mogelijkheid aangeraden/aangeboden worden?

Een hoog percentage vals-positieven betekent dat te veel contacten als relevant aangemerkt worden. Met name bij een Bluetooth implementatie kan dit een serieus probleem zijn, wanneer de app teveel contacten als relevant klassificeert. De gevoeligheid van de classificatie zal dan aangepast moeten worden.

Een **derde** criterium is het percentage vals-negatieven van de app. Daarbij raakt de gebruiker van de app besmet met het Corona virus zonder dat de app een waarschuwing gegeven heeft. Dat zal een begrijpelijke frustratie oproepen: “wat heb ik nou aan dat rotting?” Ook vals-negatieven tasten de reputatie en het draagvlak van de app ernstig aan.

Het zou de evaluatie van een notificatie app vergemakkelijken als van tevoren streef-limieten bekend gemaakt worden, zowel voor vals-positieven als voor vals-negatieven: om de app succesvol te laten zijn moeten de percentages beneden de x and y liggen.

Een grote verandering die een notificatie app te weeg zal brengen is de volgende. Traditioneel melden zich mensen bij (hun huisarts en) de GGD wanneer ze symptomen (denken te) hebben van het Corona virus. Met een notificatie app zal zich een nieuwe categorie mensen melden, namelijk degenen die een notificatie (waarschuwing) in hun app ontvangen hebben. Hoe gaan die percentages zich tot elkaar verhouden, in het bijzonder met betrekking tot de uitkomst van een test? Het is niet eenvoudig hier een meetbaar succes criterium uit te destilleren. Hier is aanvullend (denk)werk voor nodig.

Wel is er een belangrijk **vierde** criterium: wanneer een notificatie app er toe leidt dat personen zich melden, na een waarschuwing in hun app, met een asymptomatische of presymptomatische besmetting, dan is dat een echt winstpunt. Dit is misschien wel de meest positieve bijdrage die een notificatie app kan leveren. Zo'n eventuele bijdrage is objectief vast te stellen.

7 Wettelijke basis van een notificatie app

De minister van VWS heeft begin april 2020 de introductie van een Corona traceer app aangekondigd, gebaseerd op Bluetooth technologie. Sindsdien speelt zijn ministerie een actieve en leidende rol bij de ontwikkeling van zo'n app, eerst via een 'appathon' en nu via eigen ontwikkeling. Daarmee is VWS de partij die het doel en de middelen van deze app bepaalt. In de zin van de AVG is VWS aldus de *verwerkingsverantwoordelijke*. De GGD is verwerker

van de gegevens, indien de GGD de gegevens uit de notificatie app gebruikt, bijvoorbeeld zoals beschreven in § 5.

Een belangrijke vraag is of de contactcodes die door een notificatie app verzonden en verzameld worden persoonsgegevens zijn. Concreet spitst die vraag zich er op toe of die codes, onder omstandigheden, tot een persoon te herleiden zijn, dat wil zeggen of ze pseudoniem (en niet anoniem) zijn. Bij een Bluetooth implementatie zijn contactcodes pseudoniemen: iedereen kan een Bluetooth ontvanger opstellen die van iedere voorbijganger uitgezonden contactcodes verzamelt en koppelt aan het Bluetooth adres van de telefoon, mogelijk zelfs samen met een opname van de passerende app gebruiker⁸. Dit Bluetooth adres is zeker een persoonsgegeven, dat ook in allerlei andere situaties verzameld wordt, bijvoorbeeld om verkeersdrukke te meten. Wanneer zulke koppelingen eenmaal gelegd zijn kunnen later ook besmettingen, via gepubliceerde contactcodes, gekoppeld worden aan een Bluetooth adres. Daarmee raakt bekend dat de gebruiker van een bepaald Bluetooth adres besmet is geraakt.

Ook bij een op QRs gebaseerde realisatie van een notificatie app zal sprake zijn van verwerking van persoonsgegevens, bijvoorbeeld wanneer een contactcode die aan de app in de telefoon geleverd wordt vanuit een server (voor een QR op een locatie) gekoppeld wordt aan het IP-adres van de telefoon. Ook dit IP-adres is een persoonsgegeven.

De vraag is vervolgens: wat is de rechtsgrond voor de verwerking van deze contactcodes, als persoonsgegevens, in een notificatie app? Dat kan alleen maar *toestemming* zijn van de gebruiker. Direct na installatie van de app zal de gebruiker dus adequaat geïnformeerd moeten worden en gevraagd moeten worden om toestemming voor verwerking van persoonsgegevens voor een specifiek, wel-omschreven doel, door VWS, als verwerkingsverantwoordelijke van de app. De toestemming dient geheel vrijwillig gegeven te worden en kan niet het gevolg zijn van druk, bijvoorbeeld vanuit de overheid of vanuit andere partijen (zoals werkgevers of maatschappelijke dienstverleners).

Door VWS is steeds benadrukt dat het gebruik van een notificatie app vrijwillig⁹ en tijdelijk zal zijn. Het verdient daarom aanbeveling om in de toestemmingsvraag een expliciete einddatum op te nemen. Er zou bijvoorbeeld gevraagd kunnen worden om toestemming voor verwerking tot 31 december

⁸Sterker nog, een kwaadwillende zou de opgevangen contactcodes op een andere locatie weer kunnen gaan verspreiden en zo ‘ruis’ in het systeem te brengen, met mogelijk vals-positieve waarschuwingen tot gevolg.

⁹Zie ook de EDPB Guidelines 04/2020, punt 24.

2020. Dit geeft gebruikers duidelijkheid en vertrouwen. Mocht het nodig zijn om het gebruik van de app na die datum voort te zetten, dan kan alsnog, in de app, voor een beperkte extra periode toestemming gevraagd worden.

De eenmaal gegeven toestemming kan volgens de AVG op ieder moment weer ingetrokken worden, zonder opgaaf van reden. Alle verwerking moet dan onmiddellijk stoppen.

Het verdient aanbeveling om voor het daadwerkelijke gebruik van contactcodes door de GGD, zoals beschreven in § 5, als geheugensteun in BCO-gesprekken en ter publicatie, nogmaals expliciet toestemming te vragen.

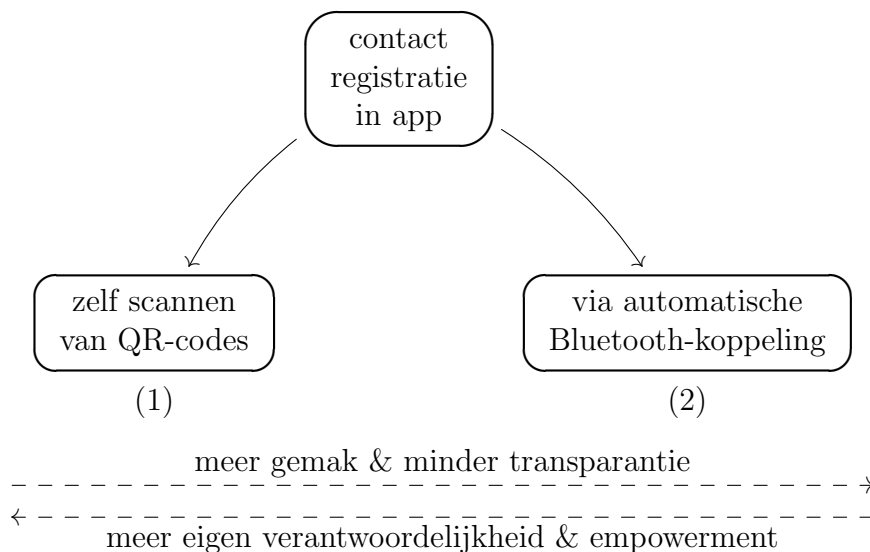
Tenslotte zal er voor ingebruikname van de app een *Data Protection Impact Assessment* (DPIA) uitgevoerd dienen te worden. Mogelijk moet de werkwijze van de app, op basis van de uitkomst van de PIA, nog aangepast moeten worden.

8 Technische realisaties van een app

Uit de talloze technische opties om een notificatie app te realiseren worden hieronder twee mogelijke versies in grote lijnen beschreven. Het onderscheidende kenmerk is wie bepaalt wat een ‘relevant contact’ is dat registratie vereist in de app: is dat de gebruiker zelf via het scannen van een QR, of is het de app via het meten van (de tijd en intensiteit¹⁰ van) een Bluetooth

¹⁰Technisch gezien gaat het om de *attenuation*, het sterkteverlies van het signaal

signaal¹¹.



De eerste versie (1) van de notificatie app stelt de gebruiker in staat om contacten te registreren via het scannen van een QR. Zulke QRs kunnen bijvoorbeeld op allerlei locaties opgehangen worden: in de supermarkt, op verdiepingen van gebouwen, in treinstellen, etc. Bij binnenkomst van zulke ruimten dienen gebruikers van de app die QRs te scannen en daarmee een registratie van hun aanwezigheid op die locatie en dat tijdstip vast te leggen. Ook kunnen individuele gebruikers QRs bij elkaar op de telefoon scannen, om een 1-op-1 contact te registreren. De vraag is of het maken van zulke scans bij (voldoende) veel mensen een systematische gewoonte kan gaan worden om een netwerk-effect te krijgen. Bij zulke QR-scans worden eenmalige, willekeurige getallen (*random* contactcodes) uitgewisseld — de details daarvan zijn in dit overzicht niet zo belangrijk. Varianten van de notificatie app (1) worden daadwerkelijk gebruikt, bijvoorbeeld in Nieuw Zeeland, als *NZ CO-*

¹¹Een van de auteurs (BJ) is meer betrokken bij de QR-variant, terwijl een andere auteur (PB) meer werk heeft gedaan aan de Bluetooth-variant. Een (kritisch) overzicht van het gebruik verschillende technieken in verschillende landen is te vinden in het artikel *Een snelle uitweg uit de lockdown? Niet met een app*, De Correspondent, 1/6/2020, zie: decorrespondent.nl/11291/een-snelle-uitweg-uit-de-lockdown-niet-met-een-app/1492115168313-d67078bc.

*VID Tracer app*¹², en worden internationaal ontwikkeld (bijvoorbeeld door zerobase) en in Nederland als zwaai.app.

De tweede versie van de notificatie app (2) op basis van Bluetooth heeft in Nederland de meeste aandacht gekregen. Daarbij versturen de telefoons van gebruikers voortdurend (*random*) berichtjes via Bluetooth, waarmee de notificatie apps de onderlinge afstand en duur van een contact met een zekere mate van nauwkeurigheid kunnen bepalen. Op basis daarvan — bijvoorbeeld bij minstens 15 minuten nabijheid op minder dan anderhalve meter — wordt een contact geregistreerd in de app van de gebruiker. De gebruiker hoeft hier dus niks voor te doen. Eerste toepassingen van deze realisatie, bijvoorbeeld in Singapore, zijn niet erg succesvol gebleken vanwege technische problemen en lage adoptie. Recentelijk hebben Apple en Google een gezamenlijk *exposure notification protocol* in de besturingssystemen van hun telefoons opgenomen die (internationale) compatibiliteit moet vergroten. Op basis daarvan wordt nu bijvoorbeeld in Zwitserland en in Nederland een notificatie app gebouwd. In deze benadering zijn de centrale rol van de ICT-giganten Apple en Google en de heimelijke werking van Bluetooth, mogelijk ook voor andere doeleinden, niet voor iedereen vertrouwenwekkend¹³. Dat kan een probleem zijn omdat ook deze versie van de notificatie app afhankelijk is van een netwerk-effect.

Een systematische vergelijking en afweging tussen versies (1) en (2), dat wil zeggen, tussen de QR en Bluetooth versie, heeft in Nederland niet plaatsgevonden. Dat wekt enige verbazing, al was het alleen maar omdat het in het algemeen onverstandig is om bij grote onzekerheden alle eieren meteen in één mandje te leggen. Experimenten met verschillende realisaties (1) en (2) kunnen goed parallel, op verschillende locaties, uitgevoerd worden, waarna resultaten vergeleken worden, bijvoorbeeld in termen van adoptie en vertrouwen van gebruikers, gebruikers-gemak/-ervaring, gedrag van gebruikers, vals-positieven, vals-negatieven, bruikbaarheid voor GGD, enz.

Daarbij zijn er ook aanzienlijke verschillen tussen de twee realisaties in termen van het vertrouwen dat gesteld wordt in burgers, de mate van roekeloosheid en/of voorzichtigheid die gebruik van de app met zich meebrengt

¹²Zie bijv. <https://www.health.govt.nz/our-work/diseases-and-conditions/covid-19-novel-coronavirus/covid-19-health-advice-general-public/contact-tracing-covid-19/nz-covid-tracer-app>

¹³Het zou kunnen helpen als de Nederlandse overheid het gebruik van Bluetooth voor het in kaart brengen van contacten van burgers op ondubbelzinnige wijze *tijdelijk* verklaart en *exclusief verbindt* aan het bestrijden van de huidige pandemie.

(actieve of passieve houding) enzovoort, die met sociaal-wetenschappelijk onderzoek verhelderd kunnen worden. Achter de twee versies (1) en (2) gaan immers verschillende mens- en maatschappij-visies schuil.

Verder kan men verwachten dat met de QR-aanpak het percentage vals-positieven laag zal zijn, maar mogelijk het aantal vals-negatieven hoger. Bij de Bluetooth-aanpak is dat waarschijnlijk andersom, omdat daarbij contacten makkelijker als relevant beoordeeld worden, juist omdat dat geen expliciete handeling vereist is. Het is op voorhand niet duidelijk welk ‘vals’ percentage prioriteit heeft om te minimaliseren.

In principe kunnen beide benaderingen (1) en (2) bijdragen aan het realiseren van de doelen in § 3, met uitzondering van het vijfde doel (detecteren van brandhaarden) waarvoor alleen de QR-gebaseerde aanpak lijkt te kunnen werken. De Bluetooth-aanpak is immers alleen gebaseerd op nabijheid tussen personen. De QR-aanpak maakt deels gebruik van nabijheid, wanneer twee personen de QR op elkaars telefoon scannen, maar zal voor een significanter deel gebaseerd zijn op locatie (winkel, werkvloer, etc.) waar gebruikers een QR scannen. Dat laatste maakt het mogelijk om brandhaarden met deze aanpak te herkennen.

Tenslotte is het bij een vergelijking belangrijk te kijken naar mogelijke fraude scenario’s. Er is al genoemd dat bij de Bluetooth-aanpak opgevangen contactcodes elders verspreid kunnen worden. De QR-benadering heeft als uitdaging om gecopieerde en verplaatste QRs te onderkennen. De Bluetooth-aanpak biedt nog een ander onbedoeld scenario: er zou een variant van de app kunnen verschijnen die alleen opvangt maar zelf geen Bluetooth signalen verspreidt. Gebruikers van zo’n app beschermen wel zichzelf, maar niet anderen. Bij al deze scenario’s zal men zich moeten afvragen: wat is de kans en wat is de impact. Niet alles is te voorzien. Daarom zal het gebruik nauwlettend gevolgd moeten worden en zullen snelle aanpassingsmogelijkheden nodig zijn.

9 Afsluitende opmerkingen

Het gebruik van een app bij het in kaart brengen en beheersen van een pandemie kan een interessante toevoeging zijn aan de bestaande epidemiologische gereedschapskist. De bestaande plannen van het ministerie van VWS met een op Bluetooth gebaseerde app zijn in feite een groot sociaal-medisch-technisch experiment. Dit experiment kent veel onzekerheden en open vragen

maar kan grote invloed hebben op gebruikers van de app die al of niet een waarschuwing krijgen. Men kan zich afvragen of een medisch-ethische commissie toestemming zou geven voor zo'n experiment — zelfs als de huidige uitzonderlijke toestand mee in overweging genomen wordt.

De volgende punten zijn in dit stadium urgent bij voortzetting van de voorbereiding.

1. De evaluatiecriteria moeten helder zijn, in relatie tot de beoogde doelen, en moeten omgezet zijn in procedures voor het verzamelen van relevante gegevens. Deze procedures moeten geïntegreerd zijn in de bestaande werkprocessen van de GGD en moeten landelijk verzameld worden.
2. De wijze van vaststelling van 'relevantie' van een contact moet afgewogen en onderbouwd zijn, via Bluetooth of via QR; voor Bluetooth dient een procedure ingericht te zijn voor bijstelling van de parameters, op basis van evaluatiegegevens.
3. Het handelingsperspectief bij een notificatie moet concreet en begrijpelijk uitgewerkt zijn, niet alleen in relatie tot de beoogde doelen, maar vooral ook vanuit de betrokkenen zelf: wat is het psychologische effect? Het moet duidelijk zijn hoe dit handelingsperspectief verandert wanneer de parameters voor relevantie van een contact wijzigen.
4. Bij het verdere ontwerp en ontwikkeling moet de mogelijkheid van moedwillige verstoring/fraude expliciet geadresseerd worden.

De opzet van het ministerie van VWS is in dit stadium onvoldoende uitgewerkt en rijp voor grootschalige, landelijk inzet. Wanneer de bovenstaande vier punten geadresseerd zijn is er hooguit ruimte voor een lokaal experiment (een pilot), met als doel om veel van te leren.