

Ontwikkeling en gebruik van zgn tracking apps bij beteugeling Covid-19

Min VWS verkent welke apps in de volgende fase kunnen worden ingezet. Internationaal zijn er tal van ontwikkelingen op het gebied van apps om het bron- en contactonderzoek door de GGD en het RIVM te ondersteunen. Min VWS toetst met deskundigen op toepasbaarheid en de borging van privacy. Uitwerking moet resulteren in besluitvorming door de MCCB in de week voor 28 april.

Het OMT heeft geadviseerd tot techniek die specifiek is ontwikkeld om te voldoen aan de AVG: Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT). Gegevens zijn geanonimiseerd, niet herleidbaar tot gebruiker en het zijn geen locatiegegevens maar gegevens over nabijheid.

Het gaat om twee apps: App 'traceren': de app houdt via bluetooth bij welke andere gebruikers van de app gedurende de afgelopen dagen dichtbij de besmette persoon zijn geweest, en kan deze personen een bericht sturen over het besmettingsrisico dat zij hebben gelopen. App 'thuisrapportage': de personen die een bericht krijgen vanuit het contactonderzoek kunnen op dat moment worden gevraagd een aanvullende app te installeren waarmee zij dagelijks hun gezondheidstoestand aan een arts in hun regio rapporteren.

Om succesvol te zijn, is gebruik door een groot deel van de Nederlanders (60 %) nodig.

We moeten over het onderstaande nu nadenken, moeten worden meegenomen bij de ontwikkeling van de app om te voorkomen dat app straks niet kan worden gebruikt als beoogd. De beslissing over beoogd gebruik moet ook zeer spoedig komen. Verplicht gebruik vergt andere juridische maatregelen dan vrijwillige deelname. Vrijwillige deelname is feitelijk onmogelijk als bv werkgevers gebruik van de app verplicht kunnen stellen om te komen werken. Ook de relatie overheid-ontwikkelaar behoeft nu aandacht. Want wie is straks eigenaar van app? Wie is beheerder, ook van de gegevens gegenereerd door de app? Wie is verantwoordelijk voor updates en beveiligingsniveau?

Ook moet je nu al nadenken over later. Wat gebeurt er met de (technologie van de) app als de medische noodzaak niet langer bestaat? En al die interessante locatie- en gezondheidsgegevens?

Enkele juridische vraagstukken

1. aansprakelijkheid/zorgplichten

- **Verantwoordelijkheid en aansprakelijkheid:** Als de Staat de app ontwikkelt en aanbeveelt, is de Staat verantwoordelijk voor de veiligheid van de app. De Staat is aansprakelijk voor schade die ontstaat als de app niet veilig is, bijvoorbeeld gehackt kan worden.
- **Hulpmiddel en behoud eigen verantwoordelijkheid burger:** Als de app slechts als hulpmiddel wordt aangeprezen, zijn de aansprakelijkheidsrisico's van de Staat waarschijnlijk beperkt. De Staat neemt dan met de app geen verantwoordelijkheid over van het individu. Van mensen wordt verwacht dat ze zelf verantwoordelijkheid nemen voor hun eigen gedrag.
- **Verwachtingenmanagement:**
 Voor beperking aansprakelijkheid is dan wel noodzakelijk dat de Staat heel duidelijk maakt:
 - dat de app geen garantie biedt op voorkomen Corona slachtoffers;
 - wat van burgers verwacht wordt in welke situatie, bijvoorbeeld:
 - Binnen blijven bij verkoudheidsklachten, ook al meldt de app niet dat je bij een Corona-patiënt in de buurt bent geweest.
 - Bij contact met een Corona-patiënt, overgaan tot twee weken quarantaine? Of advies om te laten testen?
- **Aansprakelijkheid dreigt als de app onnauwkeurig is:** Als de overheid verwacht dat je twee weken in quarantaine gaat zitten op basis van de app, moet dat wel gerechtvaardigd zijn. Als

een zzp-er thuis blijft, maar niet ziek wordt, lijdt hij schade. Dat kan hij verhalen op de overheid als deze een onnauwkeurige app aanbeveelt.

- **zorgplicht:** onder omstandigheden kan ook het *niet* inzetten van een app tot aansprakelijkheidstellingen leiden, gebaseerd op de zorgplichten van de overheid voor het leven van de burgers. Vgl. de redenering in Urgenda over de actieve zorgplicht. Dat Covid-19 gevaarzettend is, behoeft geen betoog.

2. Gebruik, privacy en handhaving

Verwerkingsverantwoordelijke en opslag van data

Wanneer wordt besloten tot het ontwikkelen van een 'traceerapp' op basis van bovengenoemde PEPP-PT raamwerk kan er worden gekozen voor zowel centrale als decentrale opslag van de persoonsgegevens. VWS lijkt vooralsnog uit te gaan van één traceerapp met centrale opslag. Dit is minder privacy vriendelijk dan decentrale opslag, waarbij gegevens op de verschillende mobiele telefoons worden opgeslagen, maar heeft als voordeel dat gegevens onder voorwaarden verder verwerkt kunnen worden voor andere doeleinden (zie: doelbinding).

Indien de overheid één app aanbiedt is de overheid de partij die het 'doel en de middelen' van de persoonsgegevensverwerking vaststelt en daarmee de 'verwerkingsverantwoordelijke' in de zin van de AVG. Dit betekent dat de verplichtingen onder de AVG in beginsel op de overheid zullen rusten. Alternatief model is dat de overheid marktpartijen onder bepaalde voorwaarden (bijv. dat alle apps met elkaar moeten kunnen communiceren) in staat stelt 'traceerapps' aan te bieden. In dat geval zijn deze private partijen de verwerkingsverantwoordelijke. Nadeel is dat het moeilijker zal zijn om te controleren of marktpartijen zich houden aan alle (privacy) regels.

Vanuit privacy perspectief geniet het dan ook de voorkeur om vanuit de overheid één app aan te bieden waarbij de data decentraal wordt opgeslagen.

Verder zijn er de volgende voorwaarden en aandachtspunten:

- **Rechtsgrondslag (artikel 6 AVG) en verbod verwerking bijzondere persoonsgegevens (artikel 9 AVG):** Er moet een rechtsgrondslag zijn om persoonsgegevens te verwerken (art. 6) en er moet een grondslag zijn om aan het verbod op verwerking van bijz. persoonsgegevens (gezondheidsgegevens) voorbij te gaan (art. 9).

Indien wordt gekozen voor een niet-verplichte applicatie kan er gebruik worden gemaakt van de rechtsgrondslag 'toestemming' en kan er tevens op basis van toestemming worden afgeweken van het verbod op verwerking bijzondere persoonsgegevens. Er zal dan uitdrukkelijk toestemming door de betrokkene moeten worden gegeven om voor een aantal specifieke doeleinden zijn/haar gegevens te verwerken. Dit kan mede omvatten dat de burger toestemming wordt gevraagd om deze informatie met bijvoorbeeld de GGD te delen.

Indien wordt gekozen voor een verplichte applicatie zien wij dat dit hoe dan ook een wettelijke grondslag vereist: een spoedwet of eventueel een spoed-AMvB indien er een geschikte delegatiebepaling bestaat in de wetgeving van VWS. Aanknopingspunten zijn om de gegevens uit een applicatie rechtmatig te verwerken op basis van de rechtsgrondslag 'noodzakelijk voor de vervulling van een taak van algemeen belang'. Het verbod op verwerking van bijzondere persoonsgegevens kan tevens worden opgeheven omdat de verwerking noodzakelijk is om 'redenen van algemeen belang op het gebied van volksgezondheid, zoals ter bescherming van grensoverschrijdende gevaren voor de volksgezondheid, (...) op grond van Unierecht of lidstatelijk recht waarin passende specifieke maatregelen zijn opgenomen ter bescherming van de rechten en vrijheden van betrokkenen'. De noodzakelijkheid staat niet op voorhand vast.

- **Noodzakelijk:** De vraag is of deze inbreuk op de persoonlijke levenssfeer noodzakelijk is teneinde de pandemie succesvol te bestrijden. In de beoordeling hiervan zal het al dan niet vrijwillige karakter van de app een bepalende rol spelen.
- **Subsidiariteit:** Aangetoond zal moeten worden dat er geen minder ingrijpende maatregelen denkbaar zijn, bijv. dat de inzet van locatiegegevens van telecomoperators kan werken ter handhaving van het samenscholingsverbod maar niet om besmette individuen te traceren. Indien wordt gedacht aan het delen van de gegevens met de GGD- en zal tevens moeten worden aangetoond dat die analyses niet op een minder ingrijpende manier kunnen worden verricht. Argument hierbij kan zijn dat een vrijwillige constructie relatief het minst ingrijpende instrument is, in tegenstelling tot instrumenten waarbij algemene surveillance plaatsvindt.
- **Proportionaliteit:** De app moet zo zijn ingericht dat die slechts tijdelijk bruikbaar is, namelijk zo lang dat in verband met de Coronacrisis nodig is.
- **Effectiviteit:** Uit de eis van noodzakelijkheid vloeit ook voort dat de verwerking van persoonsgegevens in de app effectief moet zijn. Met het oog op de vereiste kritische massa van het aantal gebruikers van de app (minimaal 60%) vergt dit inzet van de overheid om ervoor te zorgen dat voldoende mensen de app gaan installeren en gebruiken.
- **Dataminimalisatie:** De AVG bepaalt dat apps zo moeten zijn ingericht dat deze niet méér persoonsgegevens verwerken dan voor het doel van de app noodzakelijk zijn. Dit principe stelt ook grenzen aan de dataopslag in de app en het delen van data met anderen dan de gebruiker (bijv. niet melden bij wie het virus is vastgesteld, of waar iemand het virus heeft opgelopen).
- **Doelbinding:** de gegevens mogen in beginsel alleen verwerkt worden voor het doel dat is vastgesteld op het moment dat is gestart met de verwerking. Als het wenselijk is om de gegevens dus voor andere doeleinden (bijv. delen met de GGD, handhaving samenscholingsverbod) te gebruiken dan is daar een *aparte* rechtsgrondslag voor nodig. Zoals eerder genoemd kan gebruikers bijvoorbeeld om toestemming worden gevraagd voor gegevensdeling met de GGD.
- **Transparantie:** De werking van de app dient voor de burger volledig transparant en begrijpelijk te zijn.
- **Behoorlijkheid:** Er dienen voldoende waarborgen te zijn ingebouwd om ervoor te zorgen dat de meldingen van de app betrouwbaar zijn. Hierbij speelt bijvoorbeeld de vraag wie in gaat voeren dat een individu besmet is en of daar tevens bewijs voor moet worden geleverd.

Overigens heeft een coalitie van Bits of Freedom, de Waag en andere organisaties en personen (vergelijkbaar met de coalitie van destijds tegen de nieuwe Wet op de inlichtingen- en veiligheidsdiensten) gisteren een manifest uitgebracht waarin verzet wordt aangekondigd tegen introductie van een traceerapp door de overheid die niet aan tien door haar gestelde voorwaarden voldoet. De meeste voorwaarden komen grosso modo overeen met wat hiervóór aan voorwaarden en aandachtspunten naar voren is gebracht. Belangrijkste afwijking t.o.v. het concept dat door VWS lijkt te worden voorgestaan, is dat dat de coalitie tegenstander is van centraal opgeslagen persoonsgegevens. Met het oog op het noodzakelijke maatschappelijke draagvlak voor de te introduceren app en de daarbij vereiste kritische massa bij het gebruik, lijkt het wenselijk hiermee rekening te houden.

3. Informatiebeveiliging

Het uitlezen, verzamelen, verwerken van alle gegevens moet veilig gebeuren. Dat levert tal van vragen en risico's op. Waar opslaan? Wie is verantwoordelijk voor veilige opslag en wat gebeurt er bij een hack? Wie mag bij de informatie en waarom? Wie controleert dat? Moet de politie een telefoon kunnen vorderen en uitlezen? Maar ook: hoe voorkomen we connecties met facebook- en andere commerciële apps die door het besturingssysteem van de telefoon (iOS etc) worden afgedwongen? Gaat vaak via bestaande gebruikersvw, die niet altijd oneerlijke handelspraktijk-proof zijn.

Zie bijgevoegde analyse NCTV over cyber- en spyware aspecten:.

Statelijk en cyber-gerelateerd:

- Risico zit hem zowel in de schaal van het gebruik als in de personen die hem gebruiken:
 - Het **overgrote deel van de bevolking** zal de app gaan gebruiken;
 - **Hoogwaardigheidsbekleders** als ministers, CEO's, etc. kunnen vanwege de rol die zij vervullen een interessant doelwit vormen voor zowel statelijke als niet-statelijke (bijv. criminele) actoren;
 - Daaronder zullen ook **delen van de bevolking** vallen die **om politieke en ideologische redenen** reeds onder de aandacht van statelijke actoren/buitenlandse I&V-diensten staan.
- De datasets die gegenereerd zouden kunnen worden zijn interessant voor **digitale spionage door I&V-diensten**. De datasets die in de app gegenereerd worden en die spionage opleveren, alsmede de toegang tot die datasets, kan direct maar ook op lange termijn interessant zijn voor I&V diensten en criminelen;
 - **persoonsgegevens en andere gevoelige data zijn interessant voor I&V-diensten**. Een statelijke actor als China richt zich op het (clandestien) verzamelen van allerlei gegevens (ook in bulk), waarvan de verwachting is dat deze informatie hen op zeker moment op de een of andere manier voordeel kan opleveren. Voorstelbaar is dat de informatie zoals gedeeld in de betreffende apps ook aan die voorwaarden voldoen.
 - De apps zijn tevens uitnodigend voor **cyber criminelen**. **Betreffende telefoons bevatten persoonlijke profielen** waar namen, (email)adressen en telefoonnummers van afgeleid kunnen worden. Indien security van de apps onvoldoende is (de apps zijn 'hackbaar'), komen gegevens van besmette mensen op straat te liggen. Die kunnen vervolgens worden ingezet als **chantagemateriaal of worden doorverkocht**.
- Verstoring door statelijke actoren is pas voorstelbaar bij (sterk) oplopende conflicten.

NV-risico's ten aanzien van maatschappelijke onrust:

- Apps die gebruik maken proximity data en in casu aangeven of een telefoon in de buurt is geweest van een besmet persoon, betekent ook dat telefoons als 'besmet' moeten worden aangeduid in het systeem. Dat heeft potentiële gevolgen:
 - Dit kan leiden tot **verwarring**, bijvoorbeeld wanneer een telefoon in het raamkozijn ligt en een ander persoon loopt langs op straat;
 - In hoeverre kan een dergelijke app onderscheiden of je daadwerkelijk kans loopt op besmetting; als je een besmet persoon in de supermarkt tegenkomt is het natuurlijk wat anders dan dat je buurman het heeft die je niet fysiek hebt gezien; je telefoon geeft dan wel aan dat je dichtbij een besmet persoon bent geweest. Leidt dit tot onnodige angst onder de bevolking?
- Als deze **app niet verplicht wordt gesteld is de effectiviteit ervan beperkt**. Echter, het verplicht stellen van een app waarmee de overheid de **bewegingen van Nederlandse burgers volgt is een groot precedent waar niet te lichtvaardig over gedacht moet worden**. Enkele maanden geleden spraken we er nog allen schande van dat de Chinese overheid dit soort middelen gebruikte tegen de eigen bevolking;
- Hieruit volgt ook de vraag over **draagvlak voor deze apps**. Is de Nederlandse bevolking bereid tot het inleveren van **dit stukje privacy in ruil voor de belofte van een sneller einde aan de crisis?** De media-aandacht voor de app komt wellicht op een slecht moment, juist nu het RIVM steeds mededeelt dat de maatregelen lijken werken en de piek van besmettingen afzwakt. Dit vergroot het risico op het beeld van een opportunistische overheid dit de crisis aangrijpt als een excuus om data van de bevolking te verzamelen;

- Ter voorkoming van maatschappelijke rust is **duidelijke uitleg waarin de apps zich (in goede zin) onderscheiden van andere landen noodzakelijk**. Aandacht kan daarbij ook uitgaan naar de (goede) reputatie van de maker van de apps.
- **Wees alert op “nep apps”** die zichzelf voordoen als de correcte app, maar ondertussen gebruikt kunnen worden om onrust te stoken, malware te installeren, etc.;

4. *Te betrekken bij relatie ontwikkelaar-overheid*

aanbesteding/staatssteun/mededinging: juridische vragen afhankelijk van wijze van ontwikkeling.

- Denkbaar is dat de overheid niet aankoopt, maar dat app **‘om niet’** ter beschikking wordt gesteld. Dat betekent vrijwel altijd dat de ontwikkelaar zijn R&D elders dekt, bijvoorbeeld dat hij de gegevens mag gebruiken voor eigen commerciële doeleinden/koppelverkoop.
- Mededinging speelt als overheid een type **aanbeveelt** en een ander niet. Als overheid wel betaalt, is dat dan een R&D subsidie/ staatssteun?.
- Indien de overheid koopt van een private aanbieder, gelden **aanbestedingsregels**. Ook nu.
- **eigendomsverhoudingen** en intellectuele eigendom: wie is of blijft eigenaar van de app zelf, hoe zit het met updates, reverse engineering?