Punten rond Rathenau Instituut

Het Rathenau Instituut geeft een in aantal punten in hun document “Overwegingen naar aanleiding van de Kamerbrief introductie "CoronaMelder"[1]” zorgen weer. In het begeleidend artikel wordt er verder gesproken op een inbreuk op de rechten van de burgers[2]. Er wordt verder niet geduid waar de inbreuk volgens hen uit bestaat. De opinie is volgens het Rathenau Instituut gevormd op basis van de informatie in de Kamerbrief. Uit navraag blijkt dat voor zover is na te gaan er geen vragen gesteld zijn aan het ministerie. Het Rathenau Instituut heeft niet duidelijk gemaakt welke inbreuk op de rechten van de burgers zij zien.

Algemene opmerkingen
CoronaMelder is een hulpmiddel om de bron- contactopsporing van de GGD-en aan te vullen. De app waarschuwt gebruikers waarschuwt als zij een risicovol contact hebben gehad met een op COVID-19 positief getest persoon. Hierdoor neemt de kans toe dat potentieel geïnfecteerde personen eerder in beeld komen en – daarmee – dat een exponentiële uitbraak van het virus sneller wordt afgeremd. Het is geen panacee tegen COVID-19. Maar uit onderzoek van de Universiteit van Oxford wordt duidelijk dat het wel een invloed op de verspreiding van het virus kan hebben.

Er zijn een aantal punten relevant om mee te wegen:

- Het systeem is zo ingericht dat op ieder moment het herleiden naar gebruikers extreem moeilijk of zelfs onmogelijk is.
- Het gebruik van de app is vrijwillig en mag niet worden verplicht. Er is wetgeving gemaakt om dwang voor gebruik strafbaar te stellen.
- De inzet van de app is tijdelijk en er is voorzien dat deze ook weer stopt, wanneer de Corona-pandemie is ingedamd.

Belangrijk is ook de context van de COVID-19 pandemie niet over het hoofd te zien. Het voorkomen van aanvullende besmettingen of het eerder behandelen kan een behoorlijk verschil maken in het verloop van de ziekte. Zo kunnen patiënten ernstige vormen van COPD ontwikkelen, hartproblemen oplopen of langdurig last houden van chronische vermoeidheid met een fors lagere productiviteit en verdiencapaciteit tot gevolg. Het kan en mag niet worden gezien als een griep.

[1] https://www.rathenau.nl/sites/default/files/2020-08/Overwegingen%20naar%20aanleiding%20van%20Kamerbrief%20introductie%20Coronamelder.pdf – geverifieerd op 12 augustus 2020.
[2] https://www.rathenau.nl/nl/digitale-samenleving/plannen-voor-coronamelder-vragen-om-verduidelijking - geverifieerd op 12 augustus 2020.

Gefragmenteerde informatievoorziening

De informatievoorziening aan de Kamer is zeer gefragmenteerd. De brief van de minister en de vele adviezen zijn puzzelstukjes van een onvolledige puzzel. De Tweede Kamer kan het kabinet vragen om het politieke en maatschappelijke debat te helpen door te beginnen met een toelichting vanuit de bestaande wetgeving en de huidige bevoegdheden van de minister en de GGD en vervolgens aan te geven hoe CoronaMelder hieraan bijdraagt.

CoronaMelder is een lopend ICT-project. Gaandeweg het project komen er meer documenten beschikbaar. Deze worden met de eerstvolgende Kamerbrief ter beschikking van de Kamer gesteld juist met het doel hen maximaal mee te nemen in de ontwikkelingen en niet te wachten tot CoronaMelder af is. Dit biedt de mogelijkheid tot het stellen van inhoudelijke vragen, het organiseren van een technische briefing of andere stuurelementen in te zetten. Zo is ook door de Tweede Kamer gevraagd in de motie Jetten.

Nadeel van deze aanpak is een meer fragmentarische manier van informatie beschikbaar maken. Anderzijds moet CoronaMelder een rol spelen in een pandemie, waardoor op zeer hoge snelheid gewerkt moet worden.

Het punt van fragmentarische informatie met daarbij een heldere duiding is in een vroeg stadium onderkend. Daarom is in mei al besloten tot het maken van een eindrapportage, waarin de werking van CoronaMelder, de privacy, het privacyrecht, de informatiebeveiliging, de onderzoeken worden geduid. Hierdoor ontstaat een zeer gedetailleerd totaalbeeld.

Rechtvaardiging en proportionaliteit

Gezien de betrouwbaarheid van 70-75% van CoronaMelder in combinatie met de betrouwbaarheid van coronatests en het risico op onzorgvuldigheden in het meldingsproces is het de vraag of de introductie van de app voldoende effectief en daarmee proportioneel is. Vanwege het gebrek aan een duidelijke toelichting op de proportionaliteit is het nu tevens onduidelijk wanneer de inzet niet meer proportioneel is en wanneer het gebruik van de app wordt beëindigd.

Zoals CoronaMelder geen panacee is, is bluetooth dat ook niet. Het is niet geschikt om afstanden te meten. Dat is een van de leerpunten van de appathon geweest. Om duidelijk te krijgen waar de sterke en minder sterke kanten van bluetooth liggen, is het onderzoek dat door het Rathenau Instituut is aangehaald uitgevoerd. Dat onderzoek ging uit van de situatie dat er blind wordt vertrouwd op bluetooth af tool om afstanden te meten. Dat leidt inderdaad tot het beeld dat er 70-75 procent betrouwbaarheid is. Het betreft echter niet de situatie, zoals deze in CoronaMelder gerealiseerd wordt.

Als gevolg van dit onderzoek is duidelijk geworden dat bluetooth signalen in drie groepen kunnen worden verdeeld:

1. Wanneer signalen sterk zijn, zijn telefoons in elkaars nabijheid. Deze signalen zijn betrouwbaar en bruikbaar. Ze worden dan ook gebruik voor de meting in CoronaMelder.
2. Wanneer signalen minder sterk zijn, zijn telefoons verder uit elkaar. De signalen zijn dan minder betrouwbaar. Deze signalen gebruiken we alleen als twee telefoons meer dan een kwartier onafgebroken in elkaars nabijheid zijn geweest. Dat geeft een hoge mate van zekerheid dat mensen daadwerkelijk bij elkaar in de buurt zijn geweest en dat een waarschuwing nuttig is.
3. Zwakke signalen blijken onbetrouwbaar en deze worden dan ook door CoronaMelder genegeerd.

Dit is op basis van info 5.1.2e 5.1.2e net in concept brief TK opgenomen:

Daarbij wijst KIVI op de uitkomst dat in 27% van de gevallen een contact dat er wel was niet registreert en ook in 27% van de gevallen een contact dat niet voldoende langdurig was wél registreert. Dat zou bij een acceptatiegraad van 60% leiden tot melding van maximaal 42% van de risico-contacten. Deze percentages hangen samen met de strikte grens van 1,5 meter. Wanneer bijvoorbeeld de grens van 3 meter wordt gehanteerd, stijgt de sensitiviteit met deze instellingen tot boven de 90%. Ofwel: de meeste gevallen die bij de huidige instellingen een onterecht een notificatie zullen krijgen omdat ze niet binnen 1,5 meter van elkaar waren, bevonden zich wél binnen 3 meter van elkaar.

De kans om geïnfecteerd te worden met COVID-19 neemt af door afstand te houden. Des te groter de afstand is des te kleiner de kans op infectie. De grenzen die landen trekken zijn altijd arbitrair en een evenwicht tussen het verkleinen van risico's en alsnog de samenleving te laten functioneren. Omdat de schaal van besmetting logaritmisch afneemt. Dat betekent dat iemand op meer dan anderhalve meter afstand geen risico op besmetting meer loopt. In uitzonderlijke gevallen kan een besmetting over grotere afstand plaatsvinden. Door anderhalve meter kiezen neemt het risico op besmetting zeer fors. Een melding van CoronaMelder boven de anderhalve meter is dan in de juiste context nog altijd zinvol.

De metingen hebben dan ook geleid tot een verbetering van de betrouwbaarheid. Daarnaast zijn de bevindingen in internationaal verband besproken in het eHealth netwerk, zodat andere landen er hun voordeel mee kunnen doen. Ook hebben Apple en Google verbeteringen aan de API doorgevoerd om tot betere resultaten te komen. Alles bij elkaar betekent dat de nulmeting net te vergelijken is met de realiteit binnen CoronaMelder.

Er zijn altijd onnauwkeurigheden in het gebruik van technologie. De situatie is echter dat CoronaMelder mensen kan waarschuwen op verhoogde risico's op een infectie met COVID-19 zelfs al zijn er nog geen ziekteverschijnselen, waardoor eerder medisch ingrijpen mogelijk is. Dat is – zeker met de kennis van nu – een grote pre ten opzichte van een situatie waar mensen niet de mogelijkheid krijgen te worden gewaarschuwd.

Er is nog weinig wetenschappelijk bewijs over het gebruik van apps. Dat is niet vreemd, omdat bij eerdere pandemieën dergelijke mogelijkheden er niet of nauwelijks waren. Er is wel een studie, die suggereert da teen app effect kan sorteren. Dat blijkt uit het onderzoek[3] "COVID-19 incidence and R decreased on the Isle of Wight after the launch of the Test,

[3] Dit betreft de studie: COVID-19 incidence and R decreased on the Isle of Wight after the launch of the Test,

Trace, Isolate programme" van [redacted]. De adoptie van de Britse app bleek op de Isle of Wright hoger dan in de rest van het Verenigd Koninkrijk, waarbij duidelijk werd dat er een invloed op de R0 bleek.

Uit het Europese Verdrag van de Rechten van de Mens (EVRM) volgt dat geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van rechten van burgers zoals hun privacy rechten, dan voor zover bij wet is voorzien. Daarnaast moet de inmenging in een democratische samenleving noodzakelijk zijn en in het belang van bijvoorbeeld de bescherming van de gezondheid of voor de bescherming van de rechten en vrijheden van anderen.

Dit punt onderschrijven wij volledig. Daarom is er juist gekozen voor een benadering, waarbij gebruik van CoronaMelder vrijwillig is en het kabinet het dwingen van het gebruik van de app strafbaar wil stellen. Wie kiest voor het gebruik van de app moet kunnen vertrouwen dat over privacy goed is nagedacht en dat deugdelijk is geborgd. Het hele stelsel van CoronaMelder leunt op DP3T (Decentralised Privacy Preserving Proximity Tracing) dat – zoals de naam al aangeeft – decentraal werkt op een manier dat de privacy beschermd is. Zo is het systeem zo opgetuigd en heeft het ministerie zulke maatregelen getroffen dat het niet mogelijk is mensen te volgen of te identificeren.

Daarnaast speelt dat er meer fundamentele rechten zijn, die een druk uitoefenen maatregelen te nemen om deze pandemie te bestrijden. Die vloeien deels voort uit het EVRM, maar nadrukkelijk uit het Europees Sociaal Handvest[4]. Daarin staat een plicht om maatregelen te nemen in artikel 11, aanhef en derde lid[5]. Of hieruit meteen voortvloeit dat het aanbieden van de app verplicht is, zal waarschijnlijk pas na procederen zeker zijn. Maar dat er een druk is om mensen een kans te bieden een waarschuwing te krijgen bij een verhoogd op een besmetting met COVID-19 mag duidelijk zijn. CoronaMelder zou dan gelden als een zogenaamde 'non pharmaceutical intervention'. Zeker als er meer wetenschappelijk bewijs zou komen dat er enige mate van effectiviteit blijkt te zijn. Dat hier een spanning is, mag duidelijk zijn. Juist de vrijwillige benadering op een privacy vriendelijke manier kleurt dit in ieder geval goed in.

De Tweede Kamer kan het kabinet vragen hoe de aangekondigde wetgeving rondom de corona-app voldoet aan de kwaliteitseisen die (inter)nationale wetgeving, zoals het EVRM, daaraan stelt.

Trace, Isolate programme. Michelle Kendall, Luke Milsom, Lucie Abeler-Dorner, Chris Wymant, Luca Ferretti, Mark Briers, Chris Holmes, David Bonsall, Johannes Abeler, [redacted] - https://www.medrxiv.org/content/10.1101/2020.07.12.20151753v1 - link geverifieerd 8 augustus 2020.

[4] https://wetten.overheid.nl/BWBV0001800/2006-07-01#Verdrag_2 – geverifieerd 8 augustus 2020.

[5] Aanhef: Teneinde de doeltreffende uitoefening van het recht op bescherming van de gezondheid te waarborgen, verbinden de Partijen zich, hetzij rechtstreeks, hetzij in samenwerking met openbare of particuliere instanties, passende maatregelen te nemen onder andere met het oogmerk:

Derde lid: epidemische, endemische en andere ziekten, alsmede ongevallen, zoveel mogelijk te voorkomen.

Het EVRM, de AVG en andere internationale wetgeving geven algemene kaders. Het ontbreekt echter aan kwaliteitseisen. Er zijn wel verplichtingen, zoals het maken van een DPIA. Uiteraard is die uitgevoerd net als andere risicoinschattingen. Het ministerie heeft dit in een vroeg stadium erkent en daarom aansluiting gezocht bij de regulier geldende normen. Een voorbeeld daarvan is het zoveel mogelijk werken volgens de Baseline Informatiebeveiliging Overheid of het toetsen tegen internationale standaarden tijdens de penetratietest.

De Tweede Kamer kan het kabinet vragen de datum vast te leggen waarop het gebruik van de app wordt beëindigd, of de criteria kenbaar te maken die tot beëindiging zullen leiden.

[CYBER]
Uit brief: (bij doorlopen evaluatie van werking)
De doorlopende evaluatie kan zo nodig leiden tot aanpassingen en bijstellingen van de app, het werkproces of de informatievoorziening over de app. De indicatoren zullen ook gebruikt worden als input bij het bepalen wanneer de app niet meer noodzakelijk is. Ik zal hierover te zijner tijd op advies van onder anderen de begeleidingscommissie en de taskforces besluiten. Uiteraard houd ik uw Kamer op de hoogte van de uitkomsten van de doorlopende evaluatie.

Met de eventuele introductie van CoronaMelder gaat de regering in haar publieke gezondheidsinfrastructuur een verregaande afhankelijkheidsrelatie aan met de private partijen Google en Apple. Zoals de begeleidingscommissie Digitale ondersteuning bestrijding Covid-19 reeds formuleerde (Advies 2: Gebruik Google en Apple API) zijn heldere en bindende afspraken met hen noodzakelijk.

Er zijn bindende afspraken met Apple en Google gemaakt. De software (de API) is onderhevig aan een licentie, waarin duidelijke afspraken zijn gemaakt. Uit de afspraken en de vragen blijkt duidelijk dat beide organisaties geen toegang krijgen tot de verwerkte gegevens. Dit is technisch ook uitgesloten. Zij zijn in deze louter een leverancier van software.

Google en Apple bieden nu bijvoorbeeld geen volledig inzicht in de broncode van de door hen aangeboden API en het is onzeker of de deels geopenbaarde broncode wel dezelfde is als de code die in werkelijkheid op de telefoons van gebruikers staat. Onafhankelijke controle op veiligheidsaspecten en controle op oneigenlijke verwerking van persoonsgegevens zijn daardoor onmogelijk.

Het is juist dat technisch niet is vast te stelen dat de broncode van Apple en Google deze dezelfde is als de broncode die in gebruik is. Alleen binnen het stelsel van samenwerking is er geen aanleiding aan te nemen dat dit anders is. Binnen Nederlands recht zou er sprake

zijn van een onrechtmatige daad als beide bedrijven andere functionaliteit zouden toevoegen aan de API.

Daar waar het verwerking van gegevens zou betreffen bij verborgen functionaliteit zou er sprake zijn van verwerking waar dat nu niet het geval is. Dat betekent dat in zo'n geval de AVG zou worden overtreden. Kijkend naar de informatie die ze zouden kunnen afleiden zou deze omslachtige methode vragen oproepen. Beide bedrijven hebben langs legitieme weg toegang tot gegevens die veel meer informatie opleveren.

Verder bepalen Google en Apple nu eenzijdig de voorwaarden voor gebruik en het staat hen vrij om in de toekomst die gebruiksvoorwaarden of het gedrag van de API te wijzigen. Nu zijn bijvoorbeeld voor het gebruik van CoronaMelder op Android-systemen de Play Store en het registreren van een Google-account voorwaardelijk gesteld, terwijl dit vanuit technisch oogpunt niet noodzakelijk is. Gebruikers met andere Android-systemen of bijvoorbeeld diverse Huawei-telefoons waarop geen Play Store beschikbaar is, worden daardoor uitgesloten.

Dat is een correct vaststelling, waarvan het ministerie zich bewust is. De groep gebruikers die hier wordt aangegeven is dermate klein (iets boven de 5.000 gebruikers) dat omwille van de voortgang niet direct een oplossing kan worden geboden. Het aanbieden van een oplossing voor alle platformen is dermate arbeidsintensief dat dit enorm vertragend zal zijn. Er wordt gekeken of gebruikers van de nieuwste Huawei telefoons op een later moment alsnog bediend kunnen worden.

Kortom, Google en Apple worden door de keuze van het kabinet bevoordeeld in hun concurrentiepositie en het is niet vast te stellen of hun API een Trojaans paard betreft.

Het is niet duidelijk waarom de app als een trojaans paard zou worden ingezet, terwijl beide bedrijven reeds toegang hebben tot deze mobiele telefoons. Wij achten het onwaarschijnlijk dat wanneer die behoefte zou bestaan er wordt meegelift op een app van een vreemde mogendheid. Deze app wordt immers door een deel van de gebruikers geïnstalleerd. Het besturingssysteem wordt door alle gebruikers van deze telefoons ingezet en zou een betere plaats zijn om in te zetten omdat daar verborgen functionaliteit lastiger te ontdekken is. De kans van ontdekking bij de API is groter, omdat er veel door beveiligingsbedrijven op wordt getest.

In Nederland wordt zeer zorgvuldig omgegaan met de introductie van het elektronisch patiëntendossier en de toepassing van AI in de zorg. Tot op heden wordt gewerkt aan de haken en ogen die dit met zich meebrengt. De Tweede Kamer moet ervoor waken dat deze private partijen via deze app toegang krijgen tot medische of andere gevoelige gegevens, zonder zorgvuldige garanties.

CoronaMelder heeft op geen enkele wijze toegang tot medische dossiers. Het wordt louter en alleen ingezet om mensen te waarschuwen voor een verhoogd risico op een besmetting met COVID-19 als gevolg van een contact met een positief getest persoon. Er is geen andere functionaliteit.

De Tweede Kamer kan het kabinet vragen hoe het de risico's die voortvloeien uit de afhankelijkheden van Google en Apple zal beheersen.

Hoe de risico's worden beheerst wordt hiervoor en in de DPIA aangegeven.

Medische gegevens

In de Data & Privacy Impact Assessment (DPIA) wordt opgemerkt dat bij constatering door de GGD van een (mogelijke) infectie sprake is van een behandelrelatie tussen een geïnfecteerde burger en de GGD. Als die gegevens eenmaal onderdeel uitmaken van de behandelrelatie, dan worden ze beschermd door het medisch beroepsgeheim. De betreffende gegevens zijn dan onderdeel van het medisch dossier. Hierop is de huidige wet- en regelgeving van toepassing. Bijvoorbeeld in gevallen waarin de infectiegegevens worden gebruikt voor onderzoeken omwille van (inzichten in) de volksgezondheid.

Dat is correct, maar dit betreft niet direct de inzet van CoronaMelder.

Ook hebben app-gebruikers, in de hoedanigheid van patiënten, verschillende rechten met betrekking tot de gegevens in hun medisch dossier. Zo moet de patiënt in de regel toestemming geven voor verder gegevensgebruik door anderen dan de behandelend GGD-hulpverlener. Het is nu onduidelijk hoe de app waarborgt dat het medisch beroepsgeheim wordt gerespecteerd en dat de gebruikers hierover worden geïnformeerd. In de tot nog toe verstrekte stukken is er nauwelijks aandacht uitgegaan naar deze aard van de gegevens en de daarbij geldende regels.

In de app worden geen andere gegevens verwerkt. De sleutels die na positief melden worden gedeeld met andere gebruikers, zijn niet meer tot de persoon te herleiden. Na het beschikbaar stellen van de sleutels door de gebruiker, worden deze op het toestel verwijderd. Ze zijn dan ook niet meer te vinden. De GGD heeft geen toegang tot de beschikbaar gestelde sleutels, waardoor zij geen link tussen de verificatiecode en de beschikbaar gestelde sleutels kunnen leggen. Omdat er niet meer gegevens worden verwerkt, is het ook onmogelijk om verdere wettelijke kaders toe te passen. Er wordt niet behandeld op basis van CoronaMelder. Het is slechts een waarschuwingstool.

De Tweede Kamer kan het kabinet vragen of de app voldoet aan alle eisen die gesteld worden aan het verwerken van medische gegevens.

Er is geen indicatie dat waar dan ook niet wordt voldaan aan de regels.

Risico op profilering en stigmatisering

In de DPIA wordt alleen aandacht besteed aan de AVG-aspecten van de app zelf en de data die daarin worden verwerkt. In een DPIA horen de risico's op profilering te worden beoordeeld, maar die zijn ditmaal buiten beschouwing gelaten.

Het is niet correct dat deze risico's buiten beschouwing zijn gelaten. Ze zijn echter niet aangetroffen. Het is inherent aan een DPIA dat wordt gekeken naar de privacyaspecten voor de verwerking van gegevens waarvoor er verantwoordelijkheid is. Dat is niet een miskenning van risico's maar de werking van de AVG. Juist hierom wordt in de uiteindelijke duidingsrapportage niet alleen gekeken naar privacyrecht, maar ook naar privacy.

De app functioneert bijvoorbeeld binnen de besturingssystemen van Google en Apple. Het is voor hen mogelijk om de (telemetrische) gegevens van gebruikers te combineren met andere gegevens over gebruikers die reeds bij hen bekend zijn en zo profielen op te bouwen.

Het Ministerie zou graag de afhankelijkheid van besturingssystemen willen oplossen, maar dit is inderdaad de realiteit. Hier is niet de app de oorzaak, maar de manier de markt is samengesteld. Alleen anders dan de onderzoekers van het Rathenau Instituut stellen, worden er geen telemetrische gegevens die naar de persoon herleidbaar zijn. Zou dat wel het geval zijn dan zou er alsnog een verwerking van persoonsgegevens worden gestart. Daarvan is nadrukkelijk geen sprake.

Gebruikers en niet-gebruikers van de app kunnen ook worden gestigmatiseerd. Mensen kunnen worden gevraagd of zij de app gebruiken en dit kan zonder hun medeweten worden bepaald door een scanner. Zo bestaat er in allerlei situaties het risico op stigmatisering, discriminatie en uitsluiting, waardoor gebruikers schade kunnen ondervinden, hun keuzes kunnen worden beïnvloed of hen bijvoorbeeld de toegang kan worden ontzegd tot belangrijke plaatsen, producten, diensten of behandelingen.

Er wordt een actief beleid gevoerd op de vrijwilligheid. Een strafbepaling in voorgenomen wetgeving stelt ieder die de app verplicht probeert te stellen. De straffen zijn fors: maximaal

8.000 euro boete of een half jaar cel per overtreding, waarbij er daadwerkelijk handhavend zal worden opgetreden.

De dreiging die uitgaat van profilering en stigmatisering kan langdurig van aard zijn. Profielen kunnen immers lang blijven bestaan, ook al zijn de app en de daarin gebruikte data tijdelijk.

Deze stelling is in het algemeen ontegenzeggelijk juist. Alleen wordt uit het onderzoek niet echt duidelijk aan welke stigma's in het kader van CoronaMelder moet worden gedacht. De risicoanalyse in de DPIA – waar stigmatisering in de voorbereiding nadrukkelijk is besproken – maakt duidelijk dat dit probleem moeilijk praktisch voorstelbaar is.

Ook in de 'Ethische analyse van de COVID-19 notificatie-app ter aanvulling op bron- en contactonderzoek GGD' wordt aanbevolen om oneigenlijk gebruik te voorkomen, waaronder het stigmatiseren van gebruikers en niet-gebruikers. De ethische analyse heeft echter nog geen aandacht voor profilering.

Er wordt een breed beleid gevoerd op oneigenlijk gebruik varierend van de eerder genoemde strafbepaling tot het bijstaan van mensen die het slachtoffer zijn van oneigenlijk gebruik. De AVG biedt mogelijkheden tot schadevergoeding bij misbruik. Hierop zal een actief beleid worden gevoerd om betrokkenen van oneigenlijk gebruik op te wijzen.

Het is onduidelijk of burgers wordt gevraagd om toestemming om gegevens geanonimiseerd te mogen gebruiken. Bij de bestaande Corona Check-app vraagt de app-bouwer (een private partij) bijvoorbeeld om data te mogen gebruiken, om zo bepaalde 'services' te verbeteren. Anonimiseren betekent echter niet dat er geen profilering mogelijk is. Ook als de data worden vernietigd of geanonimiseerd, kan persoonsgevoelige informatie blijven bestaan en kunnen (groepen) burgers hiervan nadeel of schade ondervinden. Op basis van de COVID Radar communiceert bijvoorbeeld het LUMC in welk postcodegebied meer risico bestaat op besmetting. Dit kan een bepaalde wijk stigmatiseren.

Anders dan de genoemde apps verwerkt CoronaMelder geen ziekteverschijnselen. Het is een app gericht op het waarschuwen van gebruikers. Er worden geen locatiegegevens bij gewerkt. De functionaliteit verschilt dan fundamenteel. Wat de functionaliteit is, valt op te maken uit de DPIA.

De Tweede Kamer kan het kabinet vragen of er naast de partijen die worden genoemd in de DPIA andere partijen toegang vragen tot gegevens, en zo ja, met welk doel.

In de DPIA worden alle partijen genoemd die toegang hebben tot persoonsgegevens en waarom dat noodzakelijk is. Andere partijen toegang verlenen zou betekenen dat het Ministerie de AVG bewust zou gaan overtreden.

De Tweede Kamer kan het kabinet vragen welke maatregelen het neemt om de dreiging die uitgaat van profilering en stigmatisering tegen te gaan, en daarbij niet alleen te kijken naar de app, maar de gehele brede context van het gebruik of niet-gebruik ervan.

Welke maatregelen zijn genomen, is hiervoor benoemd.

Klachten, bezwaren, wederhoor, schade en verhaalmogelijkheden

De stukken die aan de Tweede Kamer zijn gestuurd gaan alleen in op de rechten van betrokkenen voor zover er sprake is van persoonsgegevens. Er zijn echter situaties denkbaar waarin er geen persoonsgegevens worden verwerkt, maar een burger toch een klacht of bezwaar wil indienen, wederhoor wil toepassen of schade heeft ondervonden. Deels valt dit binnen het domein van de GGD, in het kader van de behandelrelatie, maar in andere situaties is dat onduidelijk. Bijvoorbeeld met klachten over de app.

De Tweede Kamer kan het kabinet vragen hoe invulling wordt gegeven aan rechten die niet voortvloeien uit de AVG.

Het is niet duidelijk op welke rechten het Rathenau Instituut hier precies doelt, omdat dit niet nader is uitgewerkt. Voor de gevallen die hier zijn genoemd is er een servicedesk om mensen bij te staan en informatie te geven. Indien deze het antwoord op een vraag niet direct weet, is er een mogelijkheid om de vraag door te geleiden.