Digitale democratie:

Lessen uit een gezondheidscrisis

Florimond Houssiau, **Mark Hunyadi**, **Steve Tumson**
Leden van het collectief AlterNumeris
https://www.alternumeris.org/

Vertaling : Matthijs Driesen, Evelien De Pauw

Florimond Houssiau *is burgerlijke ingenieur en toegepast wiskundige. Bovendien is hij doctorandus binnen het departement 'Computational Privacy ' van Imperial College London.*
Mark Hunyadi *is professor in de filosofie, moraal en politiek (UCLouvain), en lid van de onderzoeksgroep medicinale robotica in Leuven. Ook is hij auteur van verschillende artikels over het thema digitalisering.*
Steve Tumson *is burgerlijk ingenieur gespecialiseerd in robotica. Ook is hij consultant, spreker en docent.*

Samenvatting

De door Covid-19 veroorzaakte volksgezondheidscrisis heeft in verschillende delen van de Belgische samenleving, maar ook in de rest van de wereld, voor een schokgolf gezorgd. Op het gebied van technologie heeft het de aandacht gevestigd op het gebruik van digitale hulpmiddelen om de verspreiding van het virus tegen te gaan. Dit dossier brengt verslag uit over de problematiek rond het gebruik van deze technologieën in het huidige Belgische debat. Het trekt drie lessen uit deze crisis, dat als symptomatisch wordt beschouwd voor het huidige digitale beleid: (1) het digitale tijdperk kan geen tijd van urgentie zijn, (2) bij het ontwerp en het gebruik van nieuwe digitale technologieën moeten fundamentele beginselen in acht worden genomen en (3) een sterke interface tussen technologie en samenleving is van essentieel belang. Uit deze lessen blijkt de noodzaak om de institutionele capaciteit op te bouwen om de basis te leggen voor een echte digitale democratie.

I. Gezondheidscrisis en digitale instrumenten: waar hebben we het over?

Sinds midden maart, heeft de epidemie die door Covid19 werd veroorzaakt, in België, en nog eerder in andere landen, een ongekende impact op ons persoonlijk en beroepsleven, onze economie en onze maatschappij als geheel. Velen van ons werden onderworpen aan inperkingsmaatregelen die toen onvoorstelbaar leken, terwijl het hele land aan het wachten was tot het aantal besmettingsgevallen afnam.

In de loop van die weken en nu nog steeds kwam de rol van digitale technologieën in het crisismanagement plotseling naar voren als een instrument om de verspreiding van het virus te meten en te beperken. Dit omvat het gebruik van systemen die de te testen personen identificeren als gevolg van nauw contact met geïnfecteerde personen, of die het mogelijk maken dat personen die geïnfecteerd kunnen zijn, blijven communiceren of medisch worden gemonitord terwijl ze geïsoleerd zijn. Deze systemen kunnen automatische systemen zijn (toepassing op onze smart phones) of semi-automatisch (callcenters), en er is een enorme dataverzameling nodig om ze te voeden. Meer in het algemeen wordt verwacht dat de gegevens die met behulp van deze instrumenten worden verzameld, een analyse van de trends en ontwikkelingen van de pandemie op een breder niveau mogelijk zullen maken.

BELANGRIJKSTE GEBEURTENISSEN INZAKE DE CONSTRUCTIE VAN HET KADER VOOR TRACERINGSINSTRUMENTEN (TOT 16/09/20)

⇒ **4 februari 2020** : Eerste geval van COVID-19 in België

⇒ **10 maart** : Twee Big Data ondernemers schrijven een 'carte blanche' om de overheid aan te sporen de door telecomoperatoren verzamelde bevolkingsgegevens te gebruiken voor het algemeen belang[1]

⇒ **15 maart** : Het Ministerie van Volksgezondheid en het Ministerie Digitale Agenda richten de werkgroep "Data Against Corona" op, die deze gegevens zal analyseren om de fasen van (de)inperking van de bevolking te begeleiden[2], wat gedurende 2 maanden zal gebeuren [3].

⇒ **8 april** : De werkgroep "Data Against Corona" onderzoekt een smartphone tracking applicatie[4].

⇒ **22 april** : Ontwerpresolutie ingediend om de ontwikkeling van een traceerapplicatie op smartphones te kaderen.

⇒ **23 april** : Federaal minister De Backer kondigt aan dat een traceringsaanvraag niet nodig is en geeft aan dat de Gewesten elk hun strategie zullen moeten bepalen [5].

⇒ **25 april** : Op de officiële persconferentie kondigt de federale regering aan dat het traceren zal gebeuren via callcenters[6].

⇒ **30 april :** De Gegevensbeschermingsautoriteit (GBA) brengt een negatief advies uit over twee ontwerpen van koninklijke besluiten betreffende respectievelijk het gebruik van traceringstoepassingen en het opzetten van een databank om de verspreiding van het coronavirus te voorkomen[7]. Niemand was op de hoogte van deze twee projecten, zelfs het Parlement lijkt verbaasd [8], vooral omdat het systeem van tracering via een applicatie niet meer up-to-date leek te zijn.

⇒ **04 mei** : Publicatie in het Belgisch Staatsblad van het Koninklijk Besluit nr. 18 tot oprichting van een databank op Sciensano in het kader van de strijd tegen de verspreiding van het coronavirus COVID-19. Een nieuw Koninklijk Besluit nr. 25 van 28 mei 2020 zal de gevolgen en de bewaartermijn van de gegevens verlengen tot respectievelijk 30 juni en 5 juli;

⇒ **05 mei** : Inwerkingtreding van het Besluit van de Waalse regering nr. 35 tot organisatie van de sociale en sanitaire opsporing in het kader van de strijd tegen de COVID-19-epidemie. De tekst heeft tot doel om het verzamelen van informatie te organiseren over mensen die positief getest zijn en over degenen met wie zij in contact zijn geweest;

⇒ **13-14 mei** : Twee wetsvoorstellen worden in de Kamer ingediend om de verspreiding van VIDOC-19 tegen te gaan. Het ene is voor het opzetten van een database op Sciensano

(voor het manueel traceren) en het andere voor het gebruik van digitale contactopsporingsapplicaties ter voorkoming van de verdere verspreiding van het coronavirus COVID-19 onder de bevolking (voor het digitaal traceren).

⇒ **26 mei** : De pers kondigt aan dat er vanaf juli een trackingtoepassing in gebruik zou zijn, ontwikkeld door een nieuwe interfederale werkgroep[9], ondanks de zeer geringe activiteit van de manuele tracking callcenters. Bovendien vermeldt het advies van de Raad van State dat de federale overheid bevoegd is om algemene regels te bepalen inzake de beperking van het recht op eerbiediging van het privéleven maar dat de opsporing ook kan gebeuren door de gemeenschappen en gewesten als men een samenwerkingsakkoord afsluit.

⇒ **2 juni :** Publicatie in het Staatsblad van het Vlaams decreet betreffende de organisatie van de meldingsplicht en de opvolging van de contacten in het kader van COVID-19. De tekst voorziet in de oprichting van een contactcentrum dat verantwoordelijk is voor het opsporen en begeleiden van personen die gediagnosticeerd zijn met COVID-19 en van risicocontacten.

⇒ **12 juni:** De Vlaamse regering beslist dat er een contactopsporingsapp komt na de zomer[10].

⇒ **18 juni** : De federale regering en de deelregeringen verwerpen het basisakkoord inzake de samenwerking in de manuele en digitale contactopsporing[11].

⇒ **26 juni** : Aangezien het niet lukt om vóór 30 juni een samenwerkingsakkoord met alle parlementen te sluiten en te bekrachtigen, wordt Koninklijk Besluit van Bijzondere Bevoegdheden nr. 44 gepubliceerd in het Belgisch Staatsblad om een juridisch vacuüm te vermijden. Het verlengt de geldigheidsduur van de database die voor tracering wordt gebruikt tot 15 oktober en legt ook de rechtsgrondslagen vast voor het gebruik van een digitale applicatie.

⇒ **juli** : Er werd een openbare aanbesteding uitgeschreven om de digitale volgapplicatie te ontwikkelen en men ontving slechts twee aanvragen. Het Brusselse DevSide wordt uiteindelijk geselecteerd. Het wordt steeds duidelijker en we kennen de naam van de trackingapplicatie: 'Coronalert'.

⇒ **5 augustus**: Zoals vereist door de Algemene Verordening Gegevensbescherming (RDPD), wordt een openbare raadpleging geopend door de interfederale werkgroep die verantwoordelijk is voor de ontwikkeling van Coronalert. Het sluit op 31 augustus.

⇒ 10 september: De Interfederale Werkgroep maakt bekend dat de applicatie in de week van 28 september beschikbaar zal zijn, terwijl het wettelijk kader nog onduidelijk is.

Gedurende deze hele periode heeft de gegevensbeschermingsautoriteit en de Raad van State hun rol ten volle gespeeld door een reeks adviezen te publiceren over voorgestelde wetgeving voor het reguleren van traceringsinstrumenten. Hun werk, dat soms hard is voor de ingediende teksten, herinnert aan het belang ervan in het wetgevingsproces om te werken aan de naleving van de fundamentele beginselen die ten grondslag liggen aan het gebruik van gegevensverzameling in het algemeen en het gebruik van digitale instrumenten in het bijzonder. Hoewel deze episode de complexe verwevenheid van de verschillende bevoegdheidsniveaus om met het betreffende materiaal om te gaan aantoont, zijn de aarzelingen met betrekking tot de implementatie van een digitale traceringstoepassing bijzonder opmerkelijk. Eerst aangekondigd, vervolgens vervangen door callcenters, werd het uiteindelijk eind mei opnieuw aangekondigd en voorzien eind september zonder een effectief wettelijk kader.

Hoe werken trackingapplicaties?

Telefonische metagegevens bevatten informatie over onze (onnauwkeurige) locatie. Dit is informatie die door telefoonoperatoren wordt verzameld wanneer een gebruiker een SMS of een oproep ontvangt/verzendt. Meestal worden de gegevens samengesteld uit de data van de twee gebruikers, de tijd en de locatie van elke gebruiker. Deze gegevens zijn zeer identificeerbaar: het kennen van een paar punten (plaats + tijd) is vaak genoeg om slechts één persoon te identificeren.

Dit zijn zeer gevoelige gegevens, omdat ze veel informatie over ons privéleven kunnen onthullen. Ze worden op een geaggregeerde manier gebruikt om te proberen de verplaatsingen van de bevolking te meten en de doeltreffendheid van de inperkingsmaatregelen te beoordelen. Zo heeft Google bijvoorbeeld geaggregeerde rapporten gepubliceerd waarin de afname van de mobiliteit als gevolg van overheidsmaatregelen over de hele wereld wordt gemeten, om te helpen bij de besluitvorming. De telefoonmaatschappijen hebben er ook mee ingestemd hun anonieme geaggregeerde gegevens met de overheid te delen, met (mogelijk) een grotere mate van gedetailleerdheid. Dit maakt het bijvoorbeeld mogelijk om te detecteren welke openbare plaatsen (winkelstraat, park, …) te druk bezocht zijn en gesloten moeten worden.

Proximity tracing: wanneer een persoon positief wordt gediagnosticeerd, worden alle mensen die hij/zij in de afgelopen twee weken hebben ontmoet (en mogelijks heeft geïnfecteerd), op de hoogte gebracht en in quarantaine geplaatst. Proximity tracing is een standaard techniek om de verspreiding te beperken en werd bijvoorbeeld gebruikt bij de controle van Ebola. Zolang deze tracering efficiënt gebeurt door middel van een applicatie die door veel mensen wordt geïnstalleerd, kan het land opnieuw worden geopend zonder het risico te lopen dat het aantal geïnfecteerden explodeert. Deze

"contacttracing" kan worden uitgevoerd door een directe interventie van bevoegde personen (via een callcenter), of door gebruik te maken van digitale toepassingen die automatisch de nabijheid van twee smartphones die door twee personen moeten worden gedragen, detecteren en onthouden, of door de twee benaderingen te combineren.

II. Vraagstukken en spanningsvelden

De invoering van dit soort systemen kan moeilijk zonder spanningen te creëren binnen de samenlevingen, fricties waar we op moeten letten, niet alleen om de mogelijke excessen gelinkt aan de invoering van digitale technologieën te voorkomen, maar ook om ervoor te zorgen dat **de burgers zich deze toe-eigenen** en dat ze op de lange termijn echt effectief zijn. Een analyse van de recente debatten brengt verschillende soorten wrijvingen aan het licht.

1. Vanuit het oogpunt van privacy

Beschermt **de algemene verordening inzake gegevensbescherming (GDPR)** van Europa zijn burgers niet tegen het gebruik van gegevens voor het meten en controleren van de gevolgen van het virus te belemmeren? Nee. De AVG staat een uitzondering toe in het geval van een pandemie, mits het gebruik van de gegevens in het algemeen belang gebeurt. Het is daarom belangrijk dat dit concept voldoende kan worden gedefinieerd, zodat in geval van een noodsituatie zoals voorzien in de AVG een duidelijke en operationele definitie van wat aanvaardbaar is, ter beschikking kan worden gesteld van de betrokken actoren.

In overeenstemming met deze verplichting heeft het European Data Privacy Board (EDPB) in een publicatie uiteengezet dat een dergelijke **uitzondering** alleen gerechtvaardigd is als deze in een democratische samenleving noodzakelijk, passend en proportioneel is. Zo moet bijvoorbeeld het delen van telefonische metagegevens met de overheid om de mobiliteit van mensen te beoordelen anoniem gebeuren of met de uitdrukkelijke toestemming van de bevolking. In België heeft het Agentschap voor gegevensbescherming (ADP) onlangs een verslag gepubliceerd waarin het belang wordt benadrukt van het aantonen van de noodzaak en de proportionaliteit van het traceren van toepassingen.

2. Vanuit een technisch oogpunt

Er vond een technisch debat plaats over het ontwerpen van een traceerapplicatie: gecentraliseerde oplossingen (*à la Française*), waarbij een centrale autoriteit zorgt voor het contact met personen, en gedecentraliseerde oplossingen (zoals DP3T ondersteund door Google en Apple), waarbij elke telefoon via versleutelde informatie leert of hij in contact is geweest met een geïnfecteerde persoon. Beide brengen verschillende risico's en trade-offs met zich mee, en de keuze tussen beide moet op een **transparante en democratische** manier worden gemaakt. Dit geldt ook voor handmatige tracering: welke gegevens vinden wij acceptabel om te delen met instellingen en bedrijven (rekening houdend met het feit dat anonieme gegevens vaak niet zo 'anoniem' zijn).

In deze fase weet niemand of een traceringstoepassing echt effectief is om de epidemie in te dammen. Volgens een studie van de Universiteit van Oxford zou, als de toepassing door ten minste 60% van de bevolking wordt gebruikt, de overdracht van het virus kunnen worden geëlimineerd, mits er uitgebreide tests worden uitgevoerd en een strikte quarantaine wordt ingesteld. De resultaten van de studie tonen aan dat een nog minder wijdverspreid gebruik van de applicatie het mogelijk zou maken om de verspreiding van het virus tegen te gaan, maar het is nog niet duidelijk in hoeverre deze resultaten van toepassing zijn op de realiteit. Ook kunnen vals-positieven en vals-negatieven ernstige gevolgen hebben. Aan de ene kant kan de applicatie een gevoel van overdreven vertrouwen geven en kunnen geïnfecteerde maar niet gedetecteerde mensen het virus gemakkelijker verspreiden. Aan de andere kant kunnen mensen die als potentieel risicodrager zijn aangemerkt, worden gedwongen om hun mobiliteit en sociale contacten te beperken zonder dat daar een echte reden voor is, wat een echte ramp kan zijn...

Ook al is het verzamelen van gegevens (door een applicatie of callcenter) goed ontworpen vanuit een privacy perspectief, toch vormt het een belangrijk probleem voor het lekken van gegevens. Of het nu gaat om georganiseerde hackers, of om menselijke fouten, gegevens die door een applicatie worden verzameld kunnen gaan lekken. De ervaring leert dat dit risico niet over het hoofd mag worden gezien.

3. Vanuit een ethisch oogpunt

De toestemming van mensen voor het gebruik van hun persoonlijke gegevens is een belangrijk punt. Contact tracing applicaties zijn een goed voorbeeld: de installatie van een

dergelijke applicatie moet aan de wil van iedereen worden overgelaten. De toestemming voor het gebruik moet worden gegarandeerd, tegen elke vorm van verplichting om het te installeren of tegen discriminatie van mensen die ervoor kiezen om het niet te installeren

De verzamelde gegevens zijn van gevoelige aard en kunnen voor discriminerende doeleinden worden gebruikt. Zo kan een werkzoekende die last heeft gehad van het coronavirus meer moeite hebben om een baan te vinden (door de werkgever "de schuld te geven aan het slachtoffer"). Deze mogelijke misbruiken moeten vermeden kunnen worden om ervoor te zorgen dat de gegevensverwerking niet leidt tot discriminerende maatregelen in de verschillende aspecten ervan. De Wereldgezondheidsorganisatie waarschuwt met name voor de stigmatisering die zou kunnen ontstaan ten aanzien van mensen die door het virus worden getroffen.

4. Vanuit een politiek oogpunt

De wijze waarop de gegevens worden gebruikt, de inhoud van de toepassingen en de omvang van de gebruikte technologieën moeten duidelijk en op **transparante wijze** worden gecommuniceerd, **zodat ze openstaan door het publiek en door deskundigen kunnen worden gecontroleerd**. Gezien de vele onzekerheden over de doeltreffendheid van de technologieën en het belang van het waarborgen van de beginselen die eraan ten grondslag liggen, is het ook belangrijk dat deze nauwlettend worden gevolgd door multidisciplinaire instanties die in staat zijn de gevolgen ervan op verschillende niveaus te beoordelen.

Uitzonderlijke maatregelen voor het gebruik van gegevens door de overheid (of een particulier bedrijf) houden **het risico in dat de bewakingsmaatregelen worden gebagatelliseerd**. Polen heeft bijvoorbeeld het gebruik van een opdringerige toepassing opgelegd aan mensen in quarantaine (GPS permanent geactiveerd, en de noodzaak om af en toe een selfie te sturen op straffe van een politiebezoek). Dit is al gebeurd in de Verenigde Staten, en in Europa, als reactie op de aanslagen. Zonder bewustzijn kan de publieke acceptatie van bewakingstechnologieën, zoals een toepassing voor het traceren van contacten of het gebruik van drones, een negatieve invloed hebben op onze vrijheid en vrije meningsuiting.

III. De visie van AlterNumeris

De Coronavirus-crisis heeft een dringend karakter meegekregen: het is een gezondheids-, economische, sociale en politieke noodsituatie. Deze urgentie zet de autoriteiten ertoe aan krachtige maatregelen te nemen, die ook buiten de crisis zelf kunnen overleven (ontwikkeling van een databank van besmette personen en hun contacten of andere toepassingen voor het opsporen van populaties en personen[12], bewakingsdrones[13], gezichtsherkenning[14], enz.) Het is belangrijk om de voorzichtigheid van de autoriteiten[15] en de massale deelname van deskundigen en academici aan het publieke debat over deze complexe en gevoelige kwesties te erkennen. Met betrekking tot het opsporen van personen hebben verschillende groepen van deskundigen een reeks technische aanbevelingen gepubliceerd om het ontwerp en het gebruik van dergelijke systemen te sturen[16] (toestemming, termijnen, architectuur van de databank, enz.).

Hoewel wij deze voorstellen steunen en het eens zijn met de waarborgen waarop zij zijn gebaseerd, **achten wij het van essentieel belang om op het niveau van het digitale beleid te komen om na te denken over de wijze waarop het gebruik van digitale middelen de organisatie van het sociale leven kan beïnvloeden**. De gezondheidscrisis is een groot klankbord voor onze relatie met het digitale De reacties op het Coronavirus zijn symptomatisch voor de manier waarop digitale technologie in alle gebieden van ons individuele en collectieve leven sluipt; gevangen in de urgentie, zijn we niet altijd in staat om de impact ervan op ons leven en onze samenlevingen te begrijpen. **Bij gebrek aan een echt beleid dat zich bewust is van de ingrijpende gevolgen van de digitale technologie, zet de crisis ons tegen de stroom in en dwingt ons om met de rug tegen de muur te handelen**. Het risico bestaat dat de politieke dimensie van de gemaakte keuzes uit het oog wordt verloren, dat de tijd voor overleg wordt weggehaald, dat de belangen van een paar industriële groepen in het gedrang komen of dat de politiek wordt overgeleverd aan een technicistisch solutionisme dat gerechtvaardigd wordt door de hoogdringendheid van de situatie.

Wij zijn van mening dat uit deze crisis drie belangrijke lessen moeten worden getrokken om te voorkomen dat we in deze valkuilen terechtkomen. Deze drie lessen zullen waarschijnlijk de basis vormen voor een echt digitaal beleid dat ons niet alleen beter moet voorbereiden op toekomstige crises, maar ook de democratische legitimiteit van de keuzes die op dit gebied worden gemaakt, moet versterken.

1. Digitale tijd kan niet de tijd van urgentie zijn

In tijden van gezondheidscrisis is het argument voor alle technologische ontwikkelingen het argument van de veiligheid. Het lijdt geen twijfel dat deze prioriteit belangrijk is in de richting van onze beleidsmakers. Maar het argument kan niet rechtvaardigen dat er niet wordt nagedacht over de vraagstukken in verband met de invoering van een technologie en de beschikbare alternatieven. Veel commentatoren en burgers vrezen dat de autoriteiten, net als bij terroristische aanslagen [17], het voorwendsel van urgentie zullen gebruiken om maatregelen te nemen die veel langer duren dan de noodsituatie. Deze urgentie, in termen van digitale technologie, is ook in tijden van stabiliteit een schandaal; het is dan de economische urgentie en de eisen van de internationale concurrentie die worden ingeroepen (de digital wave die niet mag worden gemist...).

In de Coronavirus-crisis **lijkt de kwestie van de verschillende tijdsperiodes die op het spel staan ons van essentieel belang**. Het gaat inderdaad om verschillende tijdsregimes. Het ontvouwen van de verschillende niveaus van temporaliteit maakt het dus mogelijk om telkens de vraag te stellen: welke maatregelen zijn in de tijd geschikt voor de situatie? Een algemeen onderscheid kan als volgt worden gemaakt.

- **De temporaliteit van de korte termijn** als het gaat om het nemen van onmiddellijke uitvoeringsmaatregelen (inperking, sluiting van winkels, restaurants, scholen; het bestellen van apparatuur, tests, compenserende economische maatregelen, etc.) ;
- **De temporaliteit van de middellange termijn** als het gaat om het voorspellen en organiseren van deconfiniëring, met alle bijbehorende gezondheids-, sociale en economische maatregelen;
- **De temporaliteit van de lange termijn** als het gaat om het nemen van structurele maatregelen tegen de cyclische terugkeer van het virus, en meer in het algemeen tegen toekomstige pandemieën (hervorming van de gezondheidssystemen, logistieke reorganisatie, verplaatsing van de productie, etc.) ;
- **De temporaliteit van de zeer lange termijn,** wanneer het, afgezien van specifieke gezondheidskwesties, gaat om de maatschappelijke en zelfs antropologische gevolgen van de systemen die tijdens de pandemie zijn opgezet (gezichtsherkenning, gegevenscentralisatie, enz.).

Op digitaal gebied moet elke beslissing worden genomen met behulp van een dubbele focusbril: een voor de onmiddellijke oplossing van de problemen die zich voordoen, en een

andere voor de impact op lange termijn van de beoogde oplossingen. Geen van beide kan en mag afzonderlijk worden beschouwd, temeer daar we het onderlinge verband kennen tussen technische oplossingen die, eenmaal toegepast, in feite onomkeerbaar zijn. De focus op de lange termijn vereist een verschuiving naar de limiet: Wat zou er gebeuren als een dergelijke oplossing veralgemeend zou worden of als zo'n uitzonderlijk apparaat de norm zou worden? Dit langetermijnperspectief vereist dat we de technologie herintegreren in een fundamentele politieke vraag, de vraag die betekenis geeft aan alle andere: in **wat voor digitale samenleving willen we leven?** De technologie kan deze vraag niet voor ons beantwoorden; de technici van de technologie alleen kunnen de toekomst van onze samenlevingen niet sturen.

2. De principes voor het ontwerp en het gebruik van een technologie aannemen ... en zich daaraan houden!

Het gebruik van digitaal in deze crisis mag niet binair zijn. Het gaat er niet om nee te zeggen tegen digitaal, dat zou absoluut absurd zijn. Het is echter belangrijk om principes te kunnen ontwikkelen om het ontwerp en het gebruik ervan te sturen. Principes die, zowel in tijden van crisis als in tijden van stabiliteit, op vele manieren kunnen worden ondermijnd:

• Noodzakelijkheid

De noodzakelijkheid houdt in dat **de techniek niet het automatische antwoord moet zijn op alle problemen** die zich voordoen. Meer in het algemeen vullen digitale technologieën immers in toenemende mate de moderne behoefte van publieke en private krachten voor controle, calculatie en voorspelbaarheid aan. Vandaar een schijnbaar onverzadigbare behoefte aan alle continue dataverzamelingstechnologieën van sensoren, tracers en persoonlijke gegevens die de zachte onderbuik van Big Data zelfgenoegzaam worden aangeboden. Dus besluit na besluit, crisis na crisis, is technologie het standaardkader voor al het verwachte gedrag en de enige mogelijke oplossing. Deze schijnbaar neutrale houding is in werkelijkheid zeer ideologisch, want het ziet alleen redding in de technologie, ten koste van andere mogelijkheden die niet eens in overweging worden genomen.

Laten we ons systematisch de vraag stellen of het nodig is een technologie in te voeren door de winst en het verlies op korte en lange termijn tegen elkaar afwegen. De verleiding om

automatisch een digitaal middel te gebruiken om al onze problemen op te lossen, vooral in tijden van instabiliteit, moet in bedwang worden gehouden en aan reflectie worden onderworpen.

• Voorafgaande en voortdurende evaluatie

De voorafgaande en voortdurende evaluatie van het gebruikte digitale systeem lijkt ons essentieel om de voorwaarden van het experiment te voorzien alvorens een gebruik te veralgemenen naar een hele populatie. Evenzo is het belangrijk om het gebruik ervan te kunnen controleren en de langetermijneffecten ervan te kunnen evalueren.

VOORBEELD 1 : De noodzaakelijkheid van en de evaluatie van een applicatie voor het traceren van de populatie.

Het traceren van de bevolking via een applicatie die op onze 'smart' phone is geïnstalleerd, is in verschillende landen ingezet, waardoor België voldoende inzicht heeft om de effecten van dit systeem op voorhand te evalueren. De lage participatiegraad van de bevolking[18], het grote risico op vals-positieven[19] en de lage toegevoegde waarde van de applicatie[20] kunnen de noodzakelijkheid van een dergelijk systeem terecht in twijfel trekken. Het zou zelfs contraproductief zijn als het de bevolking een vals gevoel van veiligheid zou geven[21]. Als dit systeem echter zou worden ingevoerd, zou de permanente evaluatie ervan van essentieel belang zijn. Aangezien dit systeem echter snel lijkt te worden ingevoerd in België, is de voortdurende evaluatie van de doeltreffendheid en de meerwaarde ervan (via gekwantificeerde resultaten) essentieel. Merk op dat een dergelijke evaluatie niet is voorzien, aangezien alleen de evaluatie van de werking van de applicatie in de huidige juridische teksten is voorzien om de problemen op te lossen die in de loop van de tijd zullen worden ontdekt (veiligheid, privacy of functionaliteit) en die inherent zijn aan de ontwikkeling van een dergelijke applicatie, zoals in het bijzonder is opgemerkt bij onze Franse[22] of Duitse buren[23].

• Proportionaliteit

Proportionaliteit, d.w.z. de mate waarin de genomen maatregelen geschikt zijn voor het nagestreefde doel, het volume van de verzamelde gegevens tot een minimum beperken en de anonimiteit garanderen. De Belgische en Franse privacy-autoriteiten specificeren ook - in het specifieke geval van tracering - dat moet worden aangetoond dat de gebruikte oplossing

(al dan niet technologisch) het minst indringende middel is om het nagestreefde doel te bereiken.

Er is reden tot ongerustheid wanneer bedrijven de bewakingsmaatregelen willen afdwingen door het installeren van elektronische armbanden[24] of gezichtsherkenningstoestellen aan de deur onder het voorwendsel van gezondheidsbescherming[25,26]! Zo werd onder meer aan de Belgische kust een netwerk van 250 slimme camera's voorzien om de toestroom van toeristen op te vangen en in kaart te brengen[27]. De urgentie gaat hier verder dan de tijdelijkheid van de wet. Is al deze digitale ontplooiing gepast, proportioneel? Wordt de schijnbare onmiddellijke winst niet tenietgedaan door de langetermijneffecten?

VOORBEELD 2 : Regelen van de klantenstroom in winkels via gezichtsherkenning

In België stelt een startend bedrijf voor om camera's te installeren bij de ingang van winkels om mensen te tellen en zo te zorgen dat de gezondheidsregels worden nageleefd (aantal mensen per m^2), maar ook om klanten te filteren bij de ingang door hun temperatuur te meten[28]. Ten eerste kan men de noodzaak van temperatuurmeting in twijfel trekken [29] De gegevensbeschermingsautoriteit stelt duidelijk dat dergelijke praktijken vooralsnog niet zijn toegestaan en herinnert ook aan de gedeeltelijke ondoeltreffendheid van een dergelijk systeem in de strijd tegen de verspreiding van de COVID 19[30] Dan kan men de proportionaliteit van het camerasysteem dat hier gebruikt wordt om klanten te tellen in vraag stellen, wetende dat andere eenvoudige systemen (bewakingsagent bij de ingang, laserteller,...) dezelfde lens op een veel minder opdringerige manier kunnen vullen. In de pers kondigt deze startup aan dat zijn monitoringsysteem in de loop van de tijd zal evolueren en verrijkt zal worden met andere opties[31] (klantprofiel en -gedrag, enz.), wat ook vragen oproept over de tijdelijkheid en het werkelijke doel van een dergelijk system.

VOORBEELD 3 : Databank om de verspreiding van COVID-19 tegen te gaan

Eind mei wordt een wetsvoorstel ingediend voor de oprichting van een door Sciensano beheerde databank. Bij twee gelegenheden heeft de gegevensbeschermingsautoriteit het voorstel in het kader van de AVG onwettig bevonden - uit de tekst blijkt niet dat de vereiste verzameling en registratie van alle gegevens noodzakelijk en evenredig is[32]. Een andere grote grief in dit advies is de schending van het medisch beroepsgeheim.

• Technische transparantie

Technische transparantie betreft het ontwerp en de code van de applicatie, inclusief de auteurs, het doel van de applicatie en het gebruik van de gegevens die ze verzamelt, zodat iedereen er zeker van kan zijn dat ze alleen doet wat ze moet doen.

VOORBEELD 4 : Technische transparantie en broncode

In de computerwetenschappen is de broncode een tekst die de instructies waaruit een programma bestaat in een leesbare vorm presenteert, zoals die in een programmeertaal is geschreven. De publicatie van de broncode van de traceringsapplicaties is dus een elementaire voorwaarde voor transparantie. Sommige landen zoals Frankrijk[33], Groot-Brittannië[34] en India[35] hebben al stappen in die richting gezet. Hoewel deze praktijk op het juiste spoor lijkt te zitten, moet worden opgemerkt dat dit bij lange na niet het geval is voor andere applicaties van het type 'gezichtsherkenning' - waar de broncode grotendeels in handen is van de bedrijven die deze ontwikkelen.

• Politieke transparantie

Politieke transparantie heeft betrekking op de randvoorwaarden voor het nemen van beslissingen over digitaal beleid.

VOORBEELD 5 : Politieke transparantie van de Task Force "Gegevens tegen Corona".

Na een carte blanche [36] van *tech* ondernemers in de Franstalige pers werd door het Ministerie van Volksgezondheid en het Ministerie van Digitale Zaken een werkgroep "Data & Technologie tegen Corona" opgericht om de overheid te helpen bij het nemen van goede beslissingen over het gebruik van data en technologie[37]. De werking van deze werkgroep blijft ondoorzichtig, aangezien de lijst van de leden en de verslagen van de uitgevoerde werkzaamheden nergens officieel worden gepubliceerd [38].

3. Een digitaal beleid: technologie en maatschappij verbinden

Om de mechaniek van een voldongen feit te vermijden, verdedigen wij de noodzaak van een gemeenschappelijke en transparante reflectie over het gebruik, de implicaties en de mogelijkheden van de digitale instrumenten. Alleen een dergelijke bezinning zal het mogelijk maken deze crisis en de daarop volgende crises het hoofd te bieden in een vorm van democratische maturiteit, die vandaag de dag lijkt te ontbreken. **Een sterk digitaal beleid moet kunnen profiteren van alle stemmen die tellen in het publieke debat en van de bestaande democratische mechanismen.**

Alleen door de digitale instrumenten en het systeem dat eraan ten grondslag ligt democratisch en structureel te herbestemmen, kunnen we ons de betekenis van de technologische vooruitgang met vertrouwen toe-eigenen. Deze toe-eigening betekent dat we politieke onderwerpen van de digitale wereld kunnen worden, om er op een andere manier in te leven dan in de modus van een fait accompli, in tijden van crisis als in elke andere tijd. Wij pleiten voor een digitaal beleid door het ontwikkelen van het interface tussen technologie en de maatschappij.

Concreet, wat moet er gedaan worden?

Opbouw van institutionele capaciteit

Tijdens deze crisis zijn er voorstellen gedaan voor een grotere aanwezigheid van de burgers in de comités van deskundigen of, in het kader van het specifieke project voor het opzetten van een traceringsapplicatie, voor de oprichting van een toezichtcomité om ervoor te zorgen dat alle beginselen die ten grondslag liggen aan een verantwoordelijk digitaal gebruik kunnen worden nageleefd.

In het licht van deze lessen dringen wij aan op de structurele kenmerken die een echt democratisch digitaal beleid moeten sturen. Om de burgers bewust te maken van de problemen die op het spel staan en actief deel te nemen aan de te nemen beslissingen, hebben we adequate en duurzame democratische instrumenten en passende institutionele vormen nodig. Daarom hebben wij onder meer voorgesteld een **multidisciplinair en onafhankelijk instituut op te richten** dat belast is met het faciliteren van het publieke debat over deze kwesties, het informeren van het publiek over beslissingen en het ondersteunen van processen van burgerparticipatie in technologische zaken. Dit houdt in dat er nieuwe interfaces tussen technologie en samenleving moeten worden ontwikkeld, dat er nieuwe processen van democratisch debat moeten worden uitgevonden en dat de technologische vooruitgang moet worden gekoppeld aan de eisen van een wenselijke samenleving.

Werken met AlterNumeris

AlterNumeris staat ter beschikking van zowel de politieke besluitvormers als het maatschappelijke middenveld, om elk initiatief dat gericht is op de ontwikkeling van de digitale democratie of op het cultiveren van digitaal burgerschap te helpen, te begeleiden en te adviseren.

https://www.alternumeris.org/

CONTACT: EVELIEN DE PAUW · 0486 23 30 09 · INFO@ALTERNUMERIS.ORG

Referenties

1 Knack, Telenet, Proximus en Orange willen corona indijken met data

2 Numerikare, De Block en De Backer richten data against corrona taskforce op.

3 RTBF, L'analyse des déplacements, via GSM, a influencé les décisions du Conseil National de Sécurité

4 VRT, Privacy Corona App en privacy

5 De Standaard, De Backer: 'Voor contactonderzoek is eigenlijk geen app nodig'

6 VRT, hoe verloopt de contactopsporing?

7 GBA, KB's moeten herzien worden.

8 L'Avenir, Application anti-coronavirus: un travail dans le désordre

9 RTBF, Coronavirus : la Belgique mise sur l'application de tracing début juillet

10 De Morgen, Dan toch een app voor contactopsporing?

11 RTBF, Lutte contre le coronavirus en Belgique : que prévoit l'accord de coopération sur le traçage?

12 RTBF, "Coronavirus en Belgique : le parlement veut encadrer une future application de tracking"

13 De Morgen, politie zet drones in om corona maatregelen te handhaven

14 RTL Nieuws, AI helpt supermarkt met deurbeleid

15 Gegevensbeschermingsautoriteit (GBA), Opsporingsapplicaties en COVID-19 databanken: voor de GBA moeten de voorontwerpen van koninklijke besluit worden herzien

16 >Collectief van 600 internationale wetenschappers : Déclaration commune sur le traçage des contacts ; Collectief van 123 Belgische wetenschappers (p59-62) : Stratégie de déconfinement ; Leden van de Koninklijke Academie van Wetenschappen van België, «Tracing: attention aux exploitations non désirables de nos données!»

17 CREDOF-onderzoeksrapport, Ce qui reste(ra) toujours de l'urgence

18 MIT Tech Review initiative, Covid Tracing Tracker

19 Dossier van CNRS, Risques et limites des applications de traçage

20 Technology Review, Nearly 40% of Icelanders are using a covid app—and it hasn't helped much

21 La Tribune Toulouse, "StopCovid risque de donner un faux sentiment de sécurité" (Baptiste Robert)

22 CNIL, « Application StopCovid : la CNIL tire les cons equences de ses contrôles. »

23 Er zijn 77 bugs gevonden in de Android app (12/9/20) : https://github.com/corona-warn-app/cwa-app-android/issues

24 HLN, Slimme armband moet coronabesmettingen voorkomen in Antwerpse haven

25 Nouvel Observateur, Des caméras intelligentes pour surveiller le port du masque dans le métro parisien font polémique

26 Libération, A Cannes, des caméras scrutent les habitants non masqués

27 De Standaard, camera's brengen drukte aan kust in kaart

28 Le Soir, Une startup automatise le comptage des clients dans les magasins

29 Knack, Controverciële start-up levert ook aan België

30 Adives GBA, Koorts meten in de strijd tegen covid19

31 UCM Magazine, La créativité et le rebond des PME

32 Advies GBA, Adviesaanvraag betreffende oprichting databank Sciencano

33 Toms Guide, StopCovid : le gouvernement met à disposition le code source de l'application

34 BBC, Coronavirus: NHS reveals source code behind contact-tracing app

35 Tech Crunch, India's contact-tracing app is going open-source

36 Knack, Telenet, Proximus en Orange willen corona indijken met data

37 Numerikare, Ministers richten data against corona taskforce op

38 E-health.gov.be, De rol van de task force data technologie against corona