Datum: 30 april 2021

OP WAARDEN GESCHAT

LIVING LAB DIGITALE PERIMETER

Inhoud

1. SAMENVATTING

In dit rapport, geschreven als onderdeel van mijn stage voor online burgerrechtenorganisatie Bits of Freedom, is uiteengezet welke waarden er meespelen voor de betrokken partijen bij het project Digitale Perimeter en de manier waarop daar in de praktijk invulling aan wordt gegeven. Dit project is een samenwerking tussen de gemeente Amsterdam, de landelijke politie, de Johan Cruijff ArenA en TNO, waarbij in en rondom de ArenA wordt geëxperimenteerd met technologische toepassingen op het gebied van veiligheid, mobiliteit en innovatie. Door de openbaar toegankelijke communicatie over het project onder de loep te nemen is onderzocht welke waarden door de betrokken partijen onderschreven worden in de uitvoer van het project. Met behulp van interviews met de betrokken partijen is vervolgens onderzocht op welke manier de onderschreven waarden invulling vinden in de experimenten en waar zich eventuele knelpunten bevinden of waarden overschreden worden. Op basis van de informatie die uit deze interviews naar voren is gekomen, is opgemerkt dat er sprake is van twee losse projecten: één gericht op mogelijke inzet van technologische toepassingen in en rondom de Johan Cruijff ArenA en de ander gericht op het experimenteren met gezichtsherkenning voor eventuele nationale inzet. Hoewel er in beide projecten veel aandacht wordt besteed aan gegevensbescherming, lijkt er op andere vlakken nog te weinig of helemaal geen invulling te worden gegeven aan de onderschreven waarden, waarbij ook andere ethische implicaties over het hoofd lijken te worden gezien. Om de experimenten binnen de Digitale Perimeter in overeenstemming te houden met (de onderschreven) publieke en mensenrechtelijke waarden zijn een aantal aandachtspunten uiteengezet in de vorm van ethische overwegingen, onderbouwd met relevante theorie. In de conclusie zijn er, op basis van deze aandachtspunten, aanbevelingen opgesteld voor de afzonderlijke projecten, maar ook voor de algehele samenwerking. Het is beoogd dat deze aandachtspunten ook generaliseerbaar zijn naar toekomstige, soortgelijke projecten.

2. INLEIDING

Steeds meer overheidsinstanties zien mogelijkheden (of zelfs noodzaak) om technologie in te zetten bij het oplossen van problemen. Wifi-trackers worden ingezet om verkeersstromen te analyseren en verbeteren, slimme sensoren moeten zorgen voor meer efficiëntie bij het ophalen van afval, en er worden camera's geïnstalleerd die onze straten veilig moeten houden. Er wordt hierbij regelmatig gesproken over "*living labs*" of "proeftuinen"; levende laboratoria waarin technologie wordt getest in realistische setting.[1] De heilige graal lijkt hier te zijn: een transformatie naar de Smart City, waarin alles zo gestroomlijnd, efficiënt, en veilig mogelijk is.

Een voorbeeld van zo'n levend laboratorium is de omgeving rondom de Johan Cruijff ArenA in Amsterdam. In dit gebied hebben de gemeente Amsterdam, de landelijke politie, de Johan Cruijff Arena, en onafhankelijk onderzoeksorgaan TNO de handen ineengeslagen. De brug tussen het private stadion en de publieke stad wordt hier gelegd met de Digitale Perimeter, een virtueel hek waarbij innovatie, mobiliteit en veiligheid centraal staan.[2] Dit wordt volgens de openbare berichtgeving over het project gerealiseerd door te experimenteren met onder andere gezichtsherkenning, slimme sensoren en bodycams.

Deze technologieën zijn niet oncontroversieel. Ze roepen niet alleen vragen op met betrekking tot privacy, ook kwesties omtrent transparantie, autonomie en eerlijkheid worden regelmatig ter tafel gebracht wanneer het om de inzet van deze toepassingen gaat. Dit betekent dat de partijen die betrokken zijn bij het project de moeilijke taak hebben om bij iedere stap in het proces afwegingen te maken met betrekking tot welke waarden het meeste gewicht in de schaal leggen. Het vraagstuk dat het project Digitale Perimeter dan ook onvermijdelijk oproept, is hoe de betrokken partijen omgaan met deze kwestie. Of, in andere woorden: *welke waarden zijn van belang voor de verschillende betrokken partijen bij het project Digitale Perimeter en op welke manier wordt hier invulling aan gegeven?*

Om een antwoord op deze vraag te formuleren, is in kaart gebracht welke waarden er voor de direct betrokken partijen meespelen binnen het project. Daarna is onderzocht of en hoe deze worden vertaald naar de praktijk. Hierbij is enerzijds gekeken naar de online communicatie over (de invulling van) deze waarden, anderzijds naar de technologieën waarmee wordt geëxperimenteerd en de context waarin dit plaatsvindt. Uiteindelijk zijn de uitkomsten hiervan geanalyseerd, waarin een aantal discrepanties en inconsistenties naar voren zijn gekomen. Op basis hiervan zijn er, onderbouwd met relevante theorie, ethische overwegingen uiteengezet die door de direct betrokken partijen beschouwd kunnen worden als aandachtspunten. Niet alleen voor het vervolg van de Digitale Perimeter, maar ook voor toekomstige projecten. Alleen wanneer er in iedere stap van het proces voldoende aandacht wordt besteed aan essentiële publieke waarden, dat wat we in de samenleving collectief als belangrijk en waardevol beschouwen, kan er op veilige, verantwoordelijke en rechtmatige wijze worden geëxperimenteerd met nieuwe technologieën.

THEORETISCH KADER EN RELEVANTIE De vraagstukken die in dit rapport worden behandeld, vinden hun basis in een sociaal maatschappelijke context. Vanuit dit perspectief wordt verondersteld dat technologie en maatschappij elkaar wederzijds beïnvloeden. Dit perspectief wordt ook wel *actor-network-theory* (ANT) genoemd.[3] Het uitgangspunt hierbij is dat technologie niet neutraal is en er altijd menselijke keuzes worden gemaakt bij het ontwikkelen en inzetten van de technologie. De inzet en uitkomsten van de technologie beïnvloeden vervolgens weer de maatschappij: "de ontwikkeling van een nieuwe technologie wordt beïnvloed door bestaande opvattingen, regelgeving, instituties en infrastructuur, maar de technologie beïnvloedt op haar beurt diezelfde opvattingen, regels, instituties en infrastructuur".[4] Om onvoorziene negatieve sociaal maatschappelijke effecten zoveel mogelijk te voorkomen of ondervangen, is het daarom van belang dat er bij een project als de Digitale Perimeter aandacht is voor publieke waarden. En vooral: dat deze waarden ook daadwerkelijk tot uiting komen in de technologieën en de context waarin deze worden geïmplementeerd.

Het is relevant om onderzoek te doen naar de manier waarop waarden een rol spelen in het project Digitale Perimeter, omdat het niet altijd even gemakkelijk of voordehandliggend is om een vertaalslag van waarden naar praktijk te maken. Onder anderen filosofe Helen Nissenbaum toont aan dat het lastig is om gewenste waarden te incorporeren in het ontwerp van technologie: "it is one thing to subscribe, generally, to these ideals, even to make a pragmatic commitment to them, but putting them into practice (…) in the design of technical systems is not straightforward".[5] Dat er bij het ontwerp van een technologie bepaalde waarden onderschreven worden, betekent dus niet automatisch dat deze waarden ook daadwerkelijk voldoende geïncorporeerd raken in het ontwerp en tot uiting komen bij het gebruik van de technologie. Het is echter niet alleen de technologie die het lastig maakt om aan

bepaalde waarden te blijven voldoen. Uit onderzoek van het Rathenau Instituut komt naar voren dat het voor smart city projecten in het algemeen moeilijk blijkt om stelselmatig in overeenstemming te blijven met onderschreven waarden. Dit onafhankelijke onderzoeksinstituut richt zich op de maatschappelijke impact van wetenschap, innovatie en technologie, en heeft reeds meerdere onderzoeken gedaan naar living labs en de transitie naar slimme steden in Nederland. In het meest recente rapport 'Voeten in de aarde: Datagestuurde innovatie in de stad' wordt uitgebreid stilgestaan bij de knelpunten die komen kijken bij smart city projecten.[6] Hierin wordt onder andere geconcludeerd dat het ook met duidelijk geformuleerde waarden en richtlijnen nog een beproeving kan zijn om dit soort projecten op de gewenste baan te houden.[7] Dit omdat bepaalde waarden in de uitvoering met elkaar kunnen conflicteren, maar ook doordat er niet altijd voldoende zicht lijkt te zijn op de manieren waarop publieke waarden in de praktijk en op de lange termijn eventueel zouden kunnen worden overschreden.[8] Dit onder zoek naar de manier waarop waarden een rol spelen in het project Digitale Perimeter sluit hierop aan; ook binnen dit project zijn er duidelijke publieke waarden geformuleerd. Gezien de ingrijpende aard van de technologieën waarmee wordt geëxperimenteerd, is het belangrijk om te onderzoeken of en hoe er aandacht wordt geschonken aan de relevante ethische overwegingen die bij (de inzet van) deze technologieën meespelen.

METHODE Om tot een sluitende conclusie te kunnen komen met betrekking tot de rol en de vertaling van waarden in het project Digitale Perimeter, is het onderzoek opgedeeld in twee componenten. Het eerste onderdeel is gericht op het verkrijgen van een volledig beeld van het project. Hierbij staan de waarden die onderschreven worden door de direct betrokken partijen en de invulling daarvan centraal. Om dit te bereiken, zijn er interviews afgenomen met de voor het project verantwoordelijke personen van de gemeente Amsterdam, de landelijke politie, en TNO. Ondanks herhaalde verzoeken is het helaas niet gelukt om ook met iemand van de Johan Cruijff ArenA over het project te spreken. De interviews zijn gestructureerd aan de hand van De Ethische Data Assistent (DEDA), een kader ontwikkeld door Utrecht Data School om data projecten te evalueren op basis van onder andere de ingebedde waarden in het project en de sociaal-maatschappelijke impact ervan.[9] DEDA helpt ethische knelpunten bloot te leggen en werpt een licht op waarden die worden overschreden.[10] Naast het afnemen van interviews, is ook de door de stakeholders openbaar gemaakte berichtgeving over de Digitale Perimeter onder de loep genomen. Met behulp van een discoursanalyse is onderzocht op welke manier (de onderschreven) waarden in de communicatie over het project naar voren komen en hoe deze worden omschreven.

De tweede fase van het onderzoek bestaat uit een literatuuronderzoek naar aanleiding van de ondervindingen die in de eerste onderzoeksfase naar voren zijn gekomen. Het doel hiervan is om relevante morele overwegingen, onderbouwd met ethische theorie, in kaart te brengen. Vervolgens zijn hieruit een aantal aandachtspunten gedestilleerd, gericht aan de direct betrokken partijen bij het project. Aangezien het onderzoek gericht is op de rol en invulling van waarden binnen een smart city project, is er beoogd dat deze aandachtspunten ook generaliseerbaar zijn naar toekomstige, soortgelijke projecten.

3. DOEL PROJECT DIGITALE PERIMETER

Voordat er gekeken kan worden naar welke waarden er binnen het project Digitale Perimeter meespelen en hoe hier invulling aan wordt gegeven, is het eerst belangrijk om dieper in te gaan op het project zelf. Wat is voor de betrokken partijen het beoogde resultaat dat dit project moet gaan bewerkstelligen en hoe wordt dit nagestreefd? Er is hierbij onderscheid gemaakt tussen de doelstellingen die worden genoemd in de openbare communicatie van betrokken partijen naar burgers en de doelstellingen die vanuit de interviews naar voren zijn gekomen.

Openbaar gecommuniceerd doel

De naam waaronder dit project is geïntroduceerd, wekt al een bepaalde suggestie met betrekking tot het doel van het project. Het woord 'perimeter' wordt doorgaans gebruikt om te refereren naar de omtrek van een afgebakend gebied,[11] waarbij de toevoeging 'digitaal' impliceert dat deze afbakening bewerkstelligd wordt door data te verwerken[12]. De naam 'Digitale Perimeter' in de context van de Johan Cruijff ArenA zou voor een buitenstaander logischerwijs geïnterpreteerd kunnen worden als de omtrek van een specifiek gebied rondom de ArenA, waarbij de afbakening van dit gebied gebeurt op basis van dataverwerking met behulp van technologie. De omschrijving op de website van de gemeente Amsterdam over het project, onderschrijft dit: "Het idee van de Digitale Perimeter is om te onderzoeken of een zogenaamd 'virtueel hek' het gebied in de gaten kan houden met behulp van o.a. camera's en sensoren".[13] Ook de teksten op de website van TNO en de Johan Cruijff ArenA zijn in overeenstemming met deze doelstelling.[14]

Door het afgebakende gebied, de perimeter, op deze digitale manier in de gaten te houden, wordt er geprobeerd om op innovatieve wijze aan de veiligheidseis van de UEFA te kunnen voldoen. Deze stelt namelijk dat er voor het EK voetbal dat in 2021 in Nederland gehouden zou worden fysieke hekken rondom alle stadions moeten worden geplaatst, waarvan de Johan Cruijff ArenA er één is.[15]

De digitale toepassingen die hier worden ingezet moeten de overlast die fysieke hekken zouden kunnen veroorzaken voor de omgeving zoveel mogelijk verkleinen. Tegelijkertijd willen de betrokken partijen de veiligheid en mobiliteit rondom en binnen de Johan Cruijff ArenA met deze innovatieve ideeën en technologieën vergroten.[16] Deze prominente rol voor innovatie is in lijn met de andere projecten die worden uitgevoerd onder de paraplu van het Innovation Lab, een samenwerking tussen de Johan Cruijff ArenA en verschillende partijen waarbij wordt geëxperimenteerd met technologie-gestuurde oplossingen.[17]. Volgens de huidige informatievoorziening over het project staan de volgende technologieën centraal:

"Gelaatsvergelijking Gelaatsvergelijking maakt het makkelijker ongewenst gedrag te detecteren. Ook zorgt het voor betere doorstroming, door onderscheid te maken tussen bezoekers en werknemers.

Blue-force tracking Met Blue-force tracking is het mogelijk om stewards te lokaliseren en hun welzijn te checken. De Blue-force tracker reageert bijvoorbeeld op vallende beweging of een plotselinge versnelling. Zo weet de organisatie sneller wanneer er iets mis is, en kan vervolgens gepast handelen.

Bodycams op 5G netwerk Bodycams via 5G maakt het mogelijk om live beelden te maken als zich een gevaarlijke situatie op evenementen voordoet. Zo kunnen operationele medewerkers ook op locaties filmen, waar dit normaal gesproken niet gebeurt. Dit kan leiden tot een afname in agressief gedrag naar werknemers bij bezoekers van de evenementen.

Slimme infrastructuur Slimme infrastructuur zijn technologieën die bijvoorbeeld bijhouden hoeveel mensen er op elk moment in en rondom het stadion zijn. Met deze gegevens kan de organisatie beter beslissen waar ze mensen heen kunnen sturen, of waar werknemers nodig zijn. Ze kunnen zo dus vaker een weloverwogen beslissing maken, en hier de bezoeker direct over inlichten.

Scan op wapens en vuurwerk Via een scan is beter te zien of bezoekers wapens of vuurwerk bij zich hebben. Zo'n scan versnelt de toegangscontrole en waarborgt de veiligheid van bezoekers en medewerkers."[18]

In de opvolgende paragrafen zal verder uiteen worden gezet wat deze toepassingen precies inhouden en of en hoe hiermee wordt geëxperimenteerd. Door de toepassingen van de verschillende technologieën die volgens de berichtgeving over de Digitale Perimeter worden onderzocht, lijkt de focus van het project voornamelijk te liggen op het identificeren en buiten de deur houden van ongewenste gasten en het verbeteren van publieksstromen. Wanneer de technologieën geschikt worden bevonden binnen het living lab, zouden deze ook bij andere evenementen ingezet kunnen worden.[19]

Doel in de praktijk

Ook in de gesprekken die gevoerd zijn met de gemeente Amsterdam, de landelijke politie en TNO is gevraagd naar het doel van het project Digitale Perimeter. Hier werd een ander beeld geschetst. Zo blijkt de perimeter niet uit een afgebakend gebied te bestaan, maar zijn er een aantal locaties in de omgeving van het stadion waar toepassingen worden ingezet. Daarnaast blijken het EK voetbal en de daaraan verwante veiligheidseisen van de UEFA geen einddoel op zich te zijn, maar enkel een termijn om een aantal van de toepassingen op hun plaats te hebben. De Digitale Perimeter moet dan ook niet gezien worden als project dat tot een kant en klaar product leidt, maar meer als een doorlopend proces van experimenten. Ook komt in de interviews naar voren dat het helemaal niet de bedoeling is om een hek na te bootsen waarmee ongewilde gasten buiten de deur gehouden kunnen worden, zoals de toepassingen op de website doen vermoeden.

Het meest opmerkelijke is dat, hoewel de Digitale Perimeter als een gezamenlijk project met één gezamenlijk doel naar buiten wordt gebracht, er eigenlijk gesproken kan worden van twee losse projecten. Hierbij nemen de gemeente Amsterdam en de Johan Cruijff ArenA de technologieën voor hun rekening die daadwerkelijk bedoeld zijn om ingezet te worden in en rondom de ArenA. De landelijke politie experimenteert onafhankelijk daarvan met gelaatsvergelijking, waarbij TNO het onderzoek naar de technologie heeft uitgevoerd. De reden waarom de twee projecten zijn samengevoegd, is zodat de betrokken partijen van elkaars experimenten kunnen leren, mochten de uitkomsten in de toekomst ook voor de andere partijen relevant worden. De specifieke doelstellingen voor de twee projecten zelf lopen echter uiteen.

In en rondom de Johan Cruijff ArenA

Uit het gesprek met de gemeente Amsterdam blijkt dat de afbakening van het gebied rondom de Johan Cruijff ArenA, de Digitale Perimeter zelf, voornamelijk gericht is op het innoveren met betrekking tot mobiliteit. Het gebied trekt doorgaans grote aantallen bezoekers vanwege de verschillende partijen die er gevestigd zijn, zoals evenementlocaties AFAS Live en Ziggo Dome, bioscoop Pathé, diverse winkels en de ArenA zelf. Deze grote bezoekersaantallen brengen uitdagingen met zich mee met betrekking tot veiligheid en efficiëntie, waardoor de betrokken partijen bij het project het belangrijk vinden om onderzoek doen naar innovatieve oplossingen. Daarnaast is het gebied volgens de gemeente representatief voor de stad Amsterdam en leent het zich goed om in het klein de verschillende elementen van innovaties te onderzoeken en testen. Zoals al eerder genoemd, is het doel hierbij niet om een hek na te bootsen. Er wordt vooral gekeken naar hoe mensenstromen op innovatieve wijze in goede banen kunnen worden geleid. Dit wordt gedaan met behulp van het *crowd monitoring* systeem genaamd "*Public Eye*", dat bestaat uit een algoritme dat op basis van beelden van camera's berekent hoeveel mensen zich in het gebied bevinden. Vervolgens bepalen medewerkers van het operationeel mobiliteitscentrum dat in het gebied gevestigd zit om de doorloop van publieksstromen in de gaten te houden hoe hier effectief op ingespeeld kan worden. De basisfunctie is reeds op verschillende locaties in Amsterdam geïnstalleerd en in gebruik genomen,[20] waarbij de toepassing enkel nog wordt geëvalueerd en verbeterd.

Er wordt door de Johan Cruijff ArenA zelf onderzoek gedaan naar Blue-force tracking en bodycams op 5G. Dit is volgens de gemeente Amsterdam om medewerkers te ondersteunen en de veiligheid rondom de ingangen en in de arena zelf te vergroten. Blue-force tracking bestaat uit een sensorband die om de borst gedragen wordt en detecteert wanneer een medewerker valt of de hartslag verhoogt. Vervolgens wordt er een signaal doorgestuurd naar het videomanagementsysteem, waardoor beveiligers automatisch zicht krijgen op de situatie. Met bodycams op 5G zou live kunnen worden meegekeken met medewerkers wanneer dit nodig wordt geacht.

Gezichtsherkenning

Het onderzoek naar gelaatsvergelijking lijkt in dit project een vreemde eend in de bijt te zijn. Het eerste dat opvalt is het gebruik van de term gelaatsvergelijking in plaats van het meer gangbare gezichtsherkenning. In de *explainer* van de Volkskrant over de stand van deze technologie in Nederland, wordt opgemerkt dat er vaak voor de term 'gelaatsvergelijking' wordt gekozen omdat deze term minder negatieve connotaties oproept. Echter, een noemenswaardig verschil tussen gelaatsvergelijking en gezichtsherkenning lijkt er volgens experts niet te bestaan.[21] Het gaat in beide gevallen om het herkennen van mensen op basis van hun gezicht. In de context van de Digitale Perimeter gaat het specifiek om geautomatiseerde gezichtsherkenning, waarbij met behulp van kunstmatige intelligentie een gezicht wordt gedetecteerd in een foto of camerabeeld. Dit gezicht wordt omgezet naar een gezichtstemplate, wat bestaat uit een verzameling punten die uniek zijn voor het gezicht. Dit template kan vervolgens afhankelijk van de toepassing worden vergeleken met andere gezichtstemplates die zijn opgeslagen in een

database,[22] of worden gebruikt om naar een match te zoeken in live camerabeelden. In het laatste geval, ook wel real time gezichtsherkenning genoemd, worden alle andere gezichten in de beelden ook automatisch omgezet naar templates om de vergelijking te kunnen voltrekken. In het vervolg van dit rapport wordt er, ten behoeve van de begrijpelijkheid, uitsluitend nog gesproken over gezichtsherkenning, waarmee real time geautomatiseerde gezichtsherkenning wordt bedoeld.

Ten tweede, willen de betrokken partijen bij elkaars experimenten meekijken om hiervan te leren, mochten de technologieën in de toekomst ook voor hen relevant worden. Dat de politie geïnteresseerd is in het crowd monitoring systeem of de experimenten met bodycams is niet merkwaardig. Wel is het opmerkelijk dat de gemeente Amsterdam en de Johan Cruijff ArenA geïnteresseerd zijn in het onderzoek naar gezichtsherkenning. De gemeente geeft namelijk aan geen ambitie te hebben om dergelijke technologie ooit in te gaan zetten. Wat de Johan Cruijff ArenA betreft, verklaren zowel de landelijke politie als de gemeente Amsterdam het niet proportioneel te vinden om de toepassing in te zetten bij toegangscontrole voor de arena, waarbij het, zoals de Autoriteit Persoonsgegevens aangeeft, ook nog eens in strijd zou zijn met de Algemene verordening gegevensbescherming (AVG).[23]

Uit de gesprekken blijkt dan ook dat het doel van de experimenten met gezichtsherkenning weinig te maken heeft met het gecommuniceerde doel van de Digitale Perimeter, namelijk het vergroten van de mobiliteit en veiligheid in en rondom de Johan Cruijff ArenA. Er wordt niet beoogd om de technologie daadwerkelijk in of rondom de arena te implementeren; de landelijke politie onderzoekt samen met TNO hoe de technologie werkt en hoe het aangepast kan worden om de aanverwante privacy dreigingen te minimaliseren. Hierbij wordt geprobeerd een beeld te vormen van de situaties waarin gezichtsherkenningstechnologie nuttig zou kunnen zijn, onder welke condities dit zou kunnen plaatsvinden en welke maatregelen hiervoor genomen zouden moeten worden. De ruimte binnenin de Johan Cruijff ArenA leent zich in dit geval enkel als testlocatie waar de technologie op gecontroleerde wijze en in geïsoleerde setting ingezet kan worden en er kan worden geëxperimenteerd met aanpassingen. De reden hiervoor is een door de landelijke politie geanticipeerde maatschappelijke druk om de technologie te gaan gebruiken, mede doordat gezichtsherkenningstechnologie reeds een plek in de maatschappij heeft veroverd. Het wordt door bedrijven en particulieren ten slotte al voor verschillende toepassingen gebruikt. Dit vormt voor de landelijke politie een drijfveer om te onderzoeken of er een meer wenselijke vorm van gezichtsherkenning ontworpen kan worden.

4. WAARDENVOLLE COMMUNICATIE

Wat vrijwel in alle communicatie naar voren komt, is een focus op innovatie. Het living lab van de Johan Cruijff ArenA wordt door henzelf niet voor niets *Innovation Lab genoemd*.[24] Het op innovatieve wijze verbeteren of vergroten van service, veiligheid en mobiliteit staat hierbij centraal. Met het oog op het digitale aspect van de Digitale Perimeter en de toepassingen die daarbij gebruikt worden, lijkt innovatie in veel gevallen te worden nagestreefd met toepassingen die data van burgers verzamelen en verwerken.

Om te waarborgen dat er bij deze verzameling en verwerking van data geen andere essentiële waarden verloren gaan, beschrijft de website van de gemeente Amsterdam dat alles wat er binnen het project Digitale Perimeter wordt gedaan, in overeenstemming is met het Tada-manifest.[25] Op deze manier zou er moeten worden gewaarborgd dat het innoveren en experimenteren op verantwoorde wijze plaatsvindt. Het Tada-manifest komt voort uit een samenwerking van lokale ondernemers, onderwijsinstellingen en burgers, die zich op uitnodiging van het Amsterdam Economic Board hebben gebogen over de vraag welke uitgangspunten er centraal zouden moeten staan om op een verantwoorde manier vorm te kunnen geven aan de Digitale Stad.[26] Deze uitgangspunten hebben zich vertaald naar een set waarden met bijbehorende principes die ervoor moeten zorgen dat er binnen datagedreven projecten meer bekwaamheid ontstaat om ethische afwegingen te maken, waarbij de centrale waarden consequent terugkomen.[27] De Tada-principes luiden als volgt:

”1. Inclusief. Onze digitale stad is inclusief. We houden rekening met de verschillen tussen individuen en groepen, zonder gelijkwaardigheid uit het oog te te verliezen

2. Zeggenschap. Data en technologie moeten bijdragen aan vrijheid van bewoners. Data zijn dienend. Om het leven vorm te geven naar eigen inzicht, zelf informatie te verzamelen, kennis te ontwikkelen, ruimte te vinden om jezelf te organiseren.
3. Menselijke maat. Data en algoritmen hebben niet het laatste woord, menselijkheid gaat altijd voor. We laten ruimte voor onvoorspelbaarheid. Mensen hebben het recht om digitaal vergeten te worden. Zo blijft er altijd ruimte voor een nieuwe, schone start.
4. Open en transparant. Welke data worden verzameld? Waarvoor? En met welke uitkomsten en resultaten? Daarover zijn we altijd transparant.
5. Legitiem en gecontroleerd. Bewoners en gebruikers hebben zeggenschap over de vormgeving van onze digitale stad. De overheid, maatschappelijke organisaties en bedrijven faciliteren dit. Zij monitoren de ontwikkeling en de maatschappelijke gevolgen.
6. Van iedereen – voor iedereen. Data die overheden, bedrijven en andere organisaties uit de stad genereren en over de stad verzamelen zijn gemeenschappelijk bezit. Iedereen kan ze gebruiken. Iedereen kan er voordeel van hebben. Hier maken we gezamenlijk afspraken over.”[28]

Zie ook deze presentatie-slide van de Tada Toolkit. [29]

De gemeente Amsterdam werkt nauw samen met de initiatiefnemers van het manifest om al haar dataprojecten in lijn te houden met deze principes.[30] Een andere manier waarop er door de gemeente aandacht wordt besteed aan publieke waarden in deze projecten, is door haar deelname aan de Coalitie van steden voor Digitale Rechten. Deze coalitie bestaat uit 26 steden verspreid over de wereld, waarmee wordt geprobeerd digitale rechten van burgers beter te beschermen. Mensenrechten – zoals privacy en vrijheid van meningsuiting – zijn hierbij het uitgangspunt en moeten volgens de coalitie per definitie in technologische toepassingen van steden worden geïntegreerd.[31] Dit geldt dus ook voor de toepassingen binnen de Digitale Perimeter.

5. WAAR ZIJN DE WAARDEN IN DE PRAKTIJK

Aangezien het project met betrekking tot de (omgeving van de) Johan Cruijff ArenA en het project omtrent gezichtsherkenning onder één noemer naar buiten zijn gebracht, wordt voor buitenstaanders de indruk gewekt dat beide projecten in overeenstemming met deze waarden te werk gaan. Van de vier betrokken partijen bij het project Digitale Perimeter, is de gemeente Amsterdam echter de enige die het Tada-manifest heeft ondertekend. Desondanks stelt de gemeente dat alles dat binnen het project gedaan wordt in overeenstemming is met de Tada-principes.[32] Uit de interviews blijkt niet alleen dat dit in de praktijk niet altijd het geval is, maar ook dat wanneer wél geprobeerd wordt deze waarden te vertalen naar de praktijk, dit nog niet altijd leidt tot het gewenste resultaat.

In en rondom de Johan Cruijff ArenA

De gemeente Amsterdam buigt zich binnen het project voornamelijk over de toepassingen in de publieke ruimte rondom de arena, terwijl de Johan Cruijff ArenA zich focust op technologieën die interessant zijn om binnen de arena en bij de ingangen in te zetten. Door dieper in te gaan op de technologieën waarmee wordt geëxperimenteerd en de manier waarop dit wordt gedaan, kan worden onderzocht of en hoe er voldoende aandacht wordt besteed aan de onderschreven waarden.

In de gesprekken met de gemeente Amsterdam werd benadrukt dat de toepassingen waarmee geëxperimenteerd wordt, volgens de ontwerpstrategie van *privacy by design* zijn ingericht. Deze strategie heeft als uitgangspunt dat privacybescherming vanaf het eerste moment wordt meegenomen in het ontwerp.[33] Privacy by design, ofwel 'gegevensbescherming door ontwerp' is opgenomen in de AVG – het aanhouden van deze strategie bij dataprojecten kan dus gezien worden als een plicht.[34] Ook het crowd monitoring systeem Public Eye is volgens de gemeente in lijn met deze strategie. Dit systeem brengt de drukte in het gebied in kaart met behulp van telcamera's. Deze camera's sturen real time beelden, beveiligd met *end-to-end* encryptie naar een server van de gemeente. Een algoritme getraind om hoofden van mensen te detecteren, berekent vervolgens hoeveel personen er op de beelden te zien zijn. Op dit moment probeert de gemeente het systeem te verbeteren door te kijken of het ook mogelijk is om de telling lokaal, dus dichter bij de telcamera's, plaats te laten vinden in plaats van op de server van de gemeente. Hierdoor hoeft er minder data naar deze servers verstuurd te worden en is de responstijd sneller. Het berekende aantal wordt namelijk doorgestuurd naar het operationeel mobiliteitscentrum, waar medewerkers de informatie inzetten om verkeersstromen te reguleren. Om de gegevens van personen in het gebied te beschermen, zijn de beelden niet zichtbaar voor medewerkers en worden direct automatisch gewist nadat de telling heeft plaatsgevonden. Wel is met behulp van vier camera' in het gebied een dataset gecreëerd van ongeveer 300 beelden per camera, waarin handmatig is aangegeven waar in de beelden (geanonimiseerde) hoofden van mensen aanwezig zijn. Daarnaast zijn er als trainingsdata beelden gebruikt uit twee online vrij beschikbare datasets.[35] De kwaliteit en nauwkeurigheid van het algoritme wordt periodiek handmatig geëvalueerd door medewerkers van de gemeente Amsterdam.[36] Op dit moment worden bezoekers van het gebied enkel geïnformeerd over de telcamera's door stickers op de palen waaraan de camera's bevestigd zijn, waarop een link staat naar een website met meer informatie over de functie van de camera. Uit een reportage van Amsterdamse nieuwszender AT5 blijkt echter dat deze informatievoorziening nog niet altijd even duidelijk of kloppend is.[37] Daarnaast zijn de camera's opgenomen in het algoritmeregister van de gemeente.[38] Het is uiteindelijk de bedoeling dat bewoners en bezoekers ook live drukte-informatie in kunnen zien door middel van informatieschermen op locatie en live online informatievoorziening.

Vanwege het feit dat de Johan Cruijff ArenA uiteindelijk moeilijk te bereiken bleek te zijn voor een interview, is er helaas geen aanvullende informatie verkregen over de technologieën die zij van plan zijn te implementeren. Zoals eerder beschreven zou het hierbij gaan om Blue-force tracking en bodycams op 5G.

Ethische overwegingen

TRANSPARANTIE EN VERANTWOORDING Eerder in dit rapport is al te lezen dat de communicatie over het project niet overeenkomt met de daadwerkelijke vormgeving van het project. Hierdoor wordt er aan burgers onvoldoende transparantie geboden over wat er nu precies gebeurt en kunnen zij dus niet beoordelen of hetgeen dat er gedaan wordt op rechtmatige wijze gebeurt. Zoals Tsamados en Turilli stellen, moet transparantie dan ook niet gezien worden als een ethisch principe op zichzelf "but a pro-ethical condition for enabling or impairing other ethical practices or principles".[39] Zo kan voldoende transparantie vanuit een organisatie ervoor zorgen dat er meer mogelijkheid ontstaat om deze organisatie

verantwoordelijk te houden, terwijl een gebrek aan transparantie dit juist tegenhoudt. Gedeeltelijke transparantie kan zelfs ten gevolge hebben dat men zich tevreden of veilig waant, terwijl dit in werkelijkheid misschien niet het geval is.[40] Met het oog op de Tada-waarden die de gemeente Amsterdam zegt te onderschrijven, is voldoende transparantie essentieel. In de eerste plaats omdat alleen dan burgers zeggenschap kunnen hebben over de vormgeving van de Digitale Stad én de data dan ook echt 'van iedereen - voor iedereen' kan zijn. Daarnaast is het verschaffen van informatie over de manier waarop persoonsgegevens verzameld, verwerkt, opgeslagen of op een andere manier gebruikt worden vastgelegd in de AVG.[41] Het is zonder deze informatie voor burgers niet mogelijk om de betrokken partijen verantwoordelijk te houden voor hun acties.

Hoewel de communicatie over de Digitale Perimeter in haar geheel te wensen overlaat, heeft de gemeente Amsterdam wel gedetailleerde en toegankelijke informatie vrijgegeven over het geïmplementeerde Public Eye systeem. Dit is een stap in de goede richting waar veel andere steden in Nederland nog iets van kunnen leren. Echter, deze informatie is pas vrijgegeven nadat het systeem al was geïmplementeerd. Ook valt er op de pagina te lezen dat burgers op dit moment enkel de druktemetingen voor één locatie in kunnen zien, terwijl het systeem al op meerdere locaties hangt. Als de gemeente Amsterdam in overeenstemming met het Tada-manifest wil opereren, is het raadzaam om een toepassing pas in te zetten wanneer ook de communicatie hierover gereed is. Daarnaast biedt de momenteel beschikbare informatie over Public Eye enkel gedeeltelijke transparantie. Zo wordt de indruk gewekt dat het systeem open-source is,[42] wat inhoudt dat de broncode van het systeem vrij toegankelijk is. Dit lijkt echter niet het geval te zijn; de gemeente geeft aan dit nog te onderzoeken. Ook is er geen inzicht in de herkomst van de technologie en de infrastructuur waarmee het wordt verbonden. Hierdoor is het voor buitenstaanders niet mogelijk om te beoordelen of de toepassingen rechtvaardig en veilig zijn. Dit laatste punt is ook relevant voor de toepassingen waar de Johan Cruijff ArenA mee aan de slag is gegaan, namelijk Blue-force tracking en bodycams op 5G. Hierover is namelijk nog minder informatie beschikbaar.

Een gebrek aan transparantie over de herkomst en infrastructuur is problematisch, omdat het voor buitenstaanders hierdoor niet mogelijk is om te bepalen of dat wat er gebeurt in en rondom de Johan Cruijff ArenA ook echt veilig en verantwoord gebeurt. Dit terwijl er een hoop dreigingen, kwetsbaarheden en ethische overwegingen verbonden kunnen zijn aan de herkomst van technologie en de infrastructuur waaraan het verbonden wordt. Wanneer er bijvoorbeeld door overheidsinstanties en private partijen steeds meer technologie wordt afgenomen van één specifiek techbedrijf, raakt onze nationale digitale infrastructuur hier steeds meer mee vervlochten en worden wij daardoor afhankelijker van deze bedrijven.[43] Techbedrijven krijgen op deze manier steeds meer macht over de invulling van ons dagelijks leven.[44] Wanneer overheidsinstanties en private partijen dan ook nog eens geen inzicht bieden in de herkomst van de technologie die zij inzetten, wordt de inspraak van burgers over deze inzet beperkt. Dit terwijl sommige bedrijven, zoals bijvoorbeeld het Chinese Huawei, niet bepaald bekend staan om hun aandacht voor essentiële publieke waarden en mensenrechten.[45] Daarnaast kan een onveilige infrastructuur van de geïmplementeerde technologie de deur voor spionage openzetten. Ongeautoriseerd zicht op een drukbezochte locatie als de (omgeving van de) Johan Cruijff ArenA brengt voor kwaadwillende actoren een hoop voordelen met zich mee. De oplossingen waarmee de veiligheid in het gebied vergroot zou moeten worden, zou dan zomaar juist het middel kunnen worden om die veiligheid te schaden.

De bewering dat de experimenten binnen de Digitale Perimeter in overeenstemming zijn met het Tada-manifest kan ter discussie worden gesteld door dit gebrek aan transparantie. Het beperkt niet alleen de mogelijkheid om te beoordelen of de betrokken partijen binnen het project daadwerkelijk doen wat ze beweren te doen, het maakt het voor de partijen ook lastiger om aan een aantal van de andere onderschreven waarden te voldoen. Zo kan er moeilijk worden gesteld dat burgers zeggenschap hebben over de vormgeving van hun digitale stad als er niet voldoende inzicht wordt gegeven in de plannen die er zijn of reeds geïmplementeerd zijn. Daarnaast is het ook moeilijk voor te stellen dat iedereen voordeel kan hebben van de verzamelde data, aangezien er maar beperkte informatie beschikbaar is over de data die wordt verzameld en de manier waarop dit gebeurt.

ZEGGENSCHAP EN INCLUSIVITEIT Dit betekent niet dat er helemaal niets wordt gedaan om burgers te betrekken bij de vormgeving van de Digitale Perimeter. Om het gesprek aan te gaan, is het project Catalyst in de arm genomen. Dit is een samenwerking tussen de Vrije Universiteit Amsterdam en NEMO Kennislink, waarbij bijeenkomsten worden georganiseerd om "bewoners een stem te geven in de ontwikkeling van nieuwe digitale technologie voor de stad".[46] Dit soort bijeenkomsten, waar burgers in kleinschalige setting

mee kunnen denken en inspraak kunnen hebben op bepaalde beslissingen, wordt ook wel *micro deliberative democracy* genoemd.[47] Het voordeel hiervan is dat er op kleine schaal en toegankelijke wijze kan worden geïnformeerd naar de mening van burgers. Echter, deze kleine schaal is ook direct de valkuil voor de methodologie. Uit het interview met de landelijke politie blijkt dat er maar weinig 'gewone' burgers aanwezig waren bij de sessies en er vooral belanghebbenden zoals vertegenwoordigers van bedrijven of werknemers van de gemeente deelnamen aan het gesprek. Door het organiseren van de sessies wordt de indruk gewekt dat er inspraak van burgers is geweest, terwijl de zeggenschap van burgers in werkelijkheid niet noemenswaardig is vergroot. Hierdoor kan ook de inclusiviteit niet goed worden gewaarborgd. Aangezien de innovaties niet enkel voor de Johan Cruijff ArenA worden ontworpen, maar ook op andere locaties en evenementen kunnen worden ingezet, is het raadzaam om ook op macro level naar de verschillende zienswijzen die er kunnen bestaan te kijken. Door aandacht te besteden en deel te nemen aan de publieke discours die over de vormgeving van digitale steden wordt gevormd door burgers, activisten, overheidsinstanties en de media, kan een representatiever en diverser beeld worden gevormd over wenselijke vooruitgang.[48]

WAARDEN EN EXPERIMENTEN Dat er binnen het project specifieke publieke waarden onderschreven worden, wijst erop dat de betrokken partijen zich ervan bewust zijn dat een living lab niet beschouwd moet worden als een plek waar los van morele en wettelijke regels geëxperimenteerd kan worden. Zoals voorgaande alinea's ook aantonen, gaat dit in de praktijk nog niet helemaal vlekkeloos. Dit komt nog sterker naar voren in het feit dat er binnen het project Digitale Perimeter regelrecht ingegaan lijkt te worden tegen de richting van één van de uitgangspunten van de gemeente: "(…) dat Amsterdammers zich onbespied en anoniem kunnen bewegen in de openbare ruimte".[49] Het is onduidelijk hoe uitbreiding van de inzet van crowd monitoring camera's in de publieke ruimte en de interesse in experimenten met bodycams en gezichtsherkenningstechnologie zich tot dit uitgangspunt verhouden. Dat er in sommige toepassingen binnen de Digitale Perimeter sprake is van technische aanpassingen die de beveiliging van de persoonsgegevens verbeteren zoals encryptie of beelden die ergens in de keten gepseudonimiseerd worden lossen dit probleem niet op. Immers, een vrije stad kan alleen worden gewaarborgd wanneer mensen zich ook daadwerkelijk vrij voelen. De aanwezigheid van steeds meer camera's en sensoren kan dit gevoel verstoren.

Daarnaast kunnen de experimenten de machtsverhoudingen tussen verschillende partijen op scherp zetten. Zoals eerder al beschreven, kan de inzet van technologie en infrastructuren de machtspositie van bepaalde techbedrijven versterken, maar ook de verhoudingen tussen burger en overheid en werknemer en werkgever komen in het project onder druk te staan. Zo kunnen burgers de inzet van digitale toepassingen door de gemeente Amsterdam in de publieke ruimte enkel ontduiken door deze ruimte niet meer te betreden. Dit terwijl openbare ruimtes juist voor iedereen toegankelijk zouden moeten zijn. Daarnaast is het onduidelijk hoe de experimenten met Blue-force tracking door de Johan Cruijff ArenA in overeenstemming kan worden gebracht met de AVG. Volgens de gemeente Amsterdam wordt deze toepassing namelijk direct getest op een selecte groep werknemers die hiervoor toestemming heeft gegeven. Dit terwijl de sensoren biometrische persoonsgegevens, namelijk de hartslag, van werknemers meten. Er is hiervoor uitdrukkelijke *in vrijheid gegeven* toestemming nodig. Werknemers hebben een afhankelijkheidspositie ten opzichte van de Johan Cruijff ArenA, waardoor zij niet in de positie staan deze toestemming daadwerkelijk in vrijheid te kunnen geven.[50] Het is hier echter nogmaals belangrijk om te benoemen dat de Johan Cruijff ArenA hier niet over gesproken is.

Dat er ook in de experimenteerfase rekening moet worden gehouden met morele en wettelijke regels komt niet alleen voort uit de directe invloed van de experimenten. Deze experimenten kunnen namelijk ook lange-termijn consequenties met zich meebrengen. Het experimenteren met een technologie brengt de daadwerkelijke inzet ervan dichterbij. In de eerste plaats omdat een experimenteerfase al tot een bepaalde mate van normalisering van de technologie leidt, zowel bij degene die ermee experimenteert als bij burgers die eraan onderworpen worden. Dit is vooral het geval bij experimenten waarbij de technologie direct in een publieke setting ingezet of getest wordt. Daarnaast is het living lab ook opgezet om bij elkaar mee te kijken. Dit zou technologisch solutionisme in de hand kunnen werken, wat inhoudt dat er al dan niet bewust een probleem wordt gezocht waarvoor de technologie ingezet kan worden.[51] Immers, wanneer je weet hoe iets werkt en de technologie toch al in huis hebt, zou het verleidelijker kunnen worden om de technologie ook daadwerkelijk in te zetten. Voornamelijk omdat de technologie bij de experimenten zo is aangepast dat de inzet ervan aantrekkelijker wordt. Wanneer essentiële publieke waarden vanaf het begin worden meegenomen in iedere stap van het proces, is de kans groter dat deze

ook in andere toepassingen en contexten zullen doorsijpelen.

Gezichtsherkenning

Het belang van aandacht voor publieke waarden geldt ook voor de experimenten met gezichtsherkenning, ook al vinden deze plaats in geïsoleerde setting. Ook hier kan worden onderzocht of en hoe er voldoende aandacht wordt besteed aan de onderschreven waarden door dieper in te gaan op de technologie waarmee wordt geëxperimenteerd en de manier waarop dit wordt gedaan.

Zoals eerder beschreven, werken de landelijke politie en TNO samen binnen dit project. TNO heeft hierbij de opdracht gekregen inzicht te geven in welke mogelijkheden er zouden kunnen bestaan om de technologie in te zetten in de publieke ruimte, met inachtneming van juridische, sociale en ethische kaders.[52] Het gaat hierbij uitsluitend om niet-coöperatieve gezichtsherkenning, wat inhoudt dat er geen expliciete consent of medewerking is verkregen van de persoon die aan de technologie wordt blootgesteld.[53] Uiteindelijk heeft dit geleid tot een rapport waarin de mogelijke werking en verwante privacy dreigingen van de technologie uiteen worden gezet, en tot slot een specifieke vorm van gezichtsherkenning wordt gepresenteerd die zich leent om een aantal gegevensbeschermende maatregelen te incorporeren. Het gaat hierbij om *multi-party computation* (MPC), wat in het geval van gezichtsherkenningstechnologie inhoudt dat de ene partij enkel toegang heeft tot de versleutelde gezichtstemplates die afkomstig zijn uit de live beelden, terwijl de andere partij de sleutel voor de dataset met vooraf geregistreerde gezichtstemplates in haar bezit heeft. De vergelijking tussen de gezichtstemplates en de vooraf geregistreerde gezichten vindt plaats met de versleutelde data en enkel de uitkomst (identificatie of geen identificatie) is voor de belanghebbende partij toegankelijk.[54] Dit zou een minder grote inbreuk maken op de persoonlijke levenssfeer van mensen, omdat de partijen enkel toegang hebben tot (een deel van de) onherkenbare gezichtstemplates in plaats van daadwerkelijke gezichten. Enkel wanneer er een identificatie plaatsvindt, worden de gezichtstemplates gekoppeld aan de identiteit van een persoon. Deze specifieke toepassing is op dit moment nog niet op het niveau om daadwerkelijk te kunnen worden ingezet, maar er kan volgens TNO al wel worden aangenomen dat het op korte termijn in bepaalde contexten tot een vermindering van een aantal privacy dreigingen kan leiden. D it heeft betrekking op het risico dat de verzamelde gegevens voor andere doeleinden gebruikt worden dan waarvoor ze zijn verzameld (secundair gebruik, of function creep), dat de gegevens door ongeautoriseerde partijen gebruikt worden, door bijvoorbeeld hacking (onveiligheid), en dat het gebruik van de gegevens zorgt voor een inbreuk op de vertrouwelijkheid, aangezien de vergelijking plaatsvindt met versleutelde data.[55] Het is met deze MPC vorm van gezichtsherkenning dat TNO samen met de landelijke politie aan de slag is gegaan binnen de Johan Cruijff ArenA. De experimenten moeten inzicht geven in hoe de technologie kan worden ingezet in de praktijk.

Uit het rapport van TNO en de daaropvolgende experimenten blijkt dat er veel aandacht is voor het vergroten van gegevensbescherming van mensen, waarbij geprobeerd wordt de daaraan verwante risico's die aan gezichtsherkenning kleven, te mitigeren. Vooral op het gebied van beveiliging en dataminimalisatie lijken grote stappen te worden gezet. In het rapport wordt een brede opvatting van privacy aangenomen, waarbij ook bedreigingen voor grondrechten als het recht op gelijke behandeling (in de vorm van uitsluiting en vervorming) en het recht op vrijheid van meningsuiting (in de vorm van beslissingsinferentie) worden beschreven. De vorm van gezichtsherkenning waarmee wordt geëxperimenteerd (MPC) in de Johan Cruijff ArenA biedt echter geen oplossing voor deze dreigingen. Er lijkt in dit project dus alsnog meer een focus te liggen op het beschermen van privacy in de nauwe zin, waarbij gegevensbescherming centraal staat.

Het is onduidelijk of, en zo ja, hoe, met betrekking tot het onderdeel gezichtsherkenning uiting wordt gegeven aan de Tada-waarden. Uit het interview met TNO blijkt dat zij bij de aansturing van het project geen opdracht heeft gekregen van de landelijke politie of de gemeente Amsterdam om de Tada-principes in acht te nemen. TNO heeft daarbij zelf de keuze gemaakt om zich in plaats daarvan te richten op meer fundamentele theorieën wanneer het op privacybescherming aankomt, waarbij ook privacy by design wordt aangehouden.[56] Reflecterend op de Tada-principes, stelde TNO dat die meer geaard zijn in het leggen van een verbinding met de burger, terwijl het onderzoek van TNO gericht is op het schetsen van de afweging tussen privacy en vrijheid enerzijds, en veiligheid anderzijds. Daarnaast wordt als reden genoemd dat Tada een Amsterdams initiatief is, terwijl het vraagstuk omtrent gezichtsherkenning van nationale aard is. De landelijke politie noemt echter wel dat er meerdere keren gesproken is met de initiatiefnemers achter het manifest, maar erkent ook dat het voornamelijk de gemeente Amsterdam is die

zich bezighoudt met de Tada-principes.

Ethische overwegingen

Hoewel er, zoals eerder beschreven, risico's optreden wanneer de communicatie over een project niet overeenkomt met de daadwerkelijke uitwerking, hoeft het niet problematisch te zijn dat er bij de experimenten met gezichtsherkenning niet in overeenstemming met het Tada-manifest wordt gewerkt. Zolang publieke waarden en mensenrechten voldoende worden meegenomen, kan er alsnog gesproken worden van een verantwoorde werkwijze. Echter, zoals eerder genoemd, heeft de landelijke politie ervoor gekozen om te experimenten met een toepassing die voornamelijk privacyrisico's met betrekking tot gegevensbescherming vermindert. Andere dreigingen en ethische bezwaren lijken niet als zodanig zwaar te worden gewogen dat deze ook in het vervolg van de experimenten worden meegenomen, ondanks dat ze wel in het rapport van TNO worden genoemd.

VOOROORDELEN EN GELIJKE BEHANDELING Een voorbeeld van een publieke waarde die door de toepassing alsnog in het geding zou kunnen komen, is gelijkwaardigheid, vastgelegd in de grondwet als het recht op gelijke behandeling. Het is inmiddels bekend dat gezichtsherkenningstechnologie geregeld een vertekend beeld geeft van de werkelijkheid.[57] Structurele vooroordelen en institutioneel racisme sijpelen door in de datasets waarop algoritmes worden getraind, waardoor bepaalde groepen over- en ondergerepresenteerd raken. Wanneer dit algoritme vervolgens wordt ingezet in de praktijk, blijft het categoriseren aan de hand van de lessen die het heeft getrokken uit de vertekende data. Hierdoor ontstaat er een ongelijke verdeling van de risico's op foutieve positieve en negatieve identificaties. In het geval van een foutieve positieve identificatie wordt er door het algoritme een foutieve match gemaakt tussen twee gezichtstemplates, terwijl het algoritme bij een foutieve negatieve identificatie juist een match over het hoofd ziet die er wel zou moeten zijn. Onderzoek toont aan dat foutieve identificatie vaker voorkomt bij etnische minderheden en vrouwen.[58] Wanneer het algoritme in de praktijk wordt ingezet, kunnen de foutieve identificaties tot gevolg hebben dat de impliciete structurele vooroordelen en het racisme die ten grondslag liggen aan de foutieve werking van het algoritme worden versterkt. De landelijke politie geeft aan te worstelen met dit gebrek in trainingsdata, maar heeft hier vooralsnog geen antwoord op gevonden en lijkt daar binnen het project Digitale Perimeter ook niet specifiek naar op zoek te zijn. Het feit dat er geëxperimenteerd wordt met een toepassingen die hier ook geen oplossing voor gaat bieden aangevuld met het gegeven dat er op dit moment wereldwijd geworsteld wordt met de risico's van impliciete vooroordelen in algoritmes, wordt door de landelijke politie echter niet als doorslaggevend gezien om de technologie af te wijzen en de tijd en middelen te investeren in experimenten met an dere, mogelijk eerlijkere oplossingen. Dit is problematisch, omdat de politie hiermee onbewust het signaal zou kunnen afgeven dat deze risico's niet belangrijk genoeg zijn, waarmee het grondrecht op gelijke behandeling wordt ondermijnd.

GECONTROLEERD EN GEÏSOLEERD Ook wanneer het wel mogelijk zou zijn om de impliciete vooroordelen in algoritmes te ondervangen, liggen nog steeds dezelfde risico's op de loer. De uiteindelijke specifieke keuzes met betrekking tot waar en met welk doel de technologie ingezet zou kunnen worden, kunnen dan alsnog grote schadelijke gevolgen met zich meebrengen.[59] Dit onderschrijft waarom het belangrijk is om niet enkel naar de werking van een technologie zelf te kijken, maar ook de context waarin het mogelijk geplaatst wordt mee te nemen in het proces. De overschrijding van een publieke waarde als gelijkwaardigheid wordt namelijk alleen dan zichtbaar én voelbaar. Vooralsnog kunnen en mogen de landelijke politie en TNO de experimenten alleen uitvoeren in een gecontroleerde, geïsoleerde setting, namelijk binnen de muren van de Johan Cruijff ArenA. Het wordt pas mogelijk om een volledig beeld te krijgen van de werking en sociaal-maatschappelijke invloed van de technologie wanneer gezichtsherkenning zou worden geplaatst in het sociale en technische netwerk waarin het uiteindelijk ingebed zal worden.[60] Dit houdt in dat er zowel rekening gehouden moet worden met eventuele wederzijdse invloeden die voortvloeien uit de sociale context waarin de technologie geïmplementeerd wordt, maar ook het netwerk van al bestaande technologieën waar de technologie mee vervlochten zal raken. Een experiment in de Johan Cruijff ArenA zal geen inzicht geven in de manier waarop gezichtsherkenning een plaats zal innemen tussen de andere toepassingen en praktijken waar de politie toegang toe heeft. Er zal bijvoorbeeld een dataset moeten worden gecreëerd, die vervolgens in verband staat met andere praktijken van de politie. Daarnaast zal de technologie gekoppeld moeten worden aan de infrastructuur van al bestaande camera's. Een volledig beeld van de mogelijke uitwerking en risico's van deze al bestaande structuren waar de technologie mee verbonden zal raken, zal de politie in de gecontroleerde setting niet krijgen – de mees te effecten worden pas zichtbaar wanneer de technologie in de praktijk wordt ingezet.

Zoals ook genoemd in het rapport van TNO, kan de inzet van gezichtsherkenningstechnologie een dreiging vormen voor bepaalde grondrechten, zoals het recht op privacy, het recht op gelijke behandeling en de vrijheid van meningsuiting. Ondanks dat het niet zeker is hoe en of real time gezichtsherkenning daadwerkelijk ingezet gaat worden, kan het voorzorgsprincipe in dit geval wel morele sturing bieden met betrekking tot het experimenteren met bepaalde technologieën. Dit principe behelst dat wanneer een bepaalde actie mogelijk, maar wel reëel gezien, tot ernstige schade kan leiden aan milieu of maatschappij, er voor een andere actie zou moeten worden gekozen indien dit mogelijk is. Het uitvoeren van experimenten met gezichtsherkenning maakt de inzet ervan reëler doordat de technologie met betrekking tot bepaalde aspecten aantrekkelijker wordt gemaakt. Echter, de inzet ervan kan alsnog schade aanrichten aan de maatschappij. Om deze reden is het raadzaam om de middelen en tijd juist in te zetten om te onderzoeken of er geen andere beveiligingsmogelijkheden zijn die een mindere bedreiging vormen voor essentiële grondrechten. Het reeds wijd verspreide gebruik van gezichtsherkenningstechnologie en de daardoor mogelijk oplopende druk op de politie om de inzet ervan ook te overwegen vormt in deze zin niet voldoende rechtvaardiging voor de experimenten.[61] De experimenten die worden uitgevoerd zullen ten eerste namelijk niet leiden tot een vermindering van de ingrijpende verwante dreigingen, behalve de genoemde dreigingen die betrekking hebben op persoonsgegevens.Daarnaast geeft het geen voldoende beeld van mogelijke andere schadelijke lange termijn effecten. Dit terwijl tegelijkertijd de drempel om gezichtsherkenning in te zetten wel wordt verlaagd door bepaalde aspecten van de technologie aantrekkelijker te maken.

TRANSPARANTIE EN VERANTWOODING Het willen formuleren van een antwoord op de vraag waarom de politie wel of geen gebruikmaakt van real time gezichtsherkenning kan worden beschouwd als een vorm van het willen afleggen van verantwoording naar burgers. Dit is een goede koers. Echter, het is raadzaam om ook verantwoording af te leggen met betrekking tot de manier waarop deze vraag tot stand komt en de hoe er geprobeerd wordt hier een antwoord op te formuleren. De landelijke politie noemt dat zij al haar rapporten over het project openbaar maakt, zo ook het rapport van TNO. Daarnaast probeert zij het debat actief op te zoeken door bijvoorbeeld in te gaan op spreekverzoeken, aanwezig te zijn bij workshops en pers en onderzoekers te woord te staan. Echter, de ervaring binnen dit onderzoek heeft geleerd dat burgers in eerste plaats erg gericht moeten zoeken om meer informatie over dit specifieke onderdeel van de Digitale Perimeter te verkrijgen. Daarnaast is het rapport van TNO niet geschreven voor het algemene publiek, maar voor lezers die deskundig zijn op het gebied van gezichtsherkenning. Hierbij komt ook dat de technologie waarmee geëxperimenteerd wordt moeilijk uitlegbaar is. De distinctie tussen verantwoording als deugd en verantwoording als mechanisme van Bovens is in dit geval illustratief.[62] Volgens Bovens staat bij verantwoording als deugd het daadwerkelijke gedrag van het subject centraal, waarbij wordt beoordeeld of dit gedrag in lijn is met een set standaarden die we in het algemeen als ‘goed’ ervaren. Dit is nauw verbonden met verantwoording als mechanisme, waarbij Bovens refereert naar de gevestigde processen van politieke en sociale controle. Een subject kan voldoende verantwoordelijk worden gehouden wanneer er door het mechanisme een verplichting ontstaat om het gedrag uit te leggen en te verantwoorden, en ook daadwerkelijk aansprakelijk kan worden gesteld wanneer dit gedrag niet overeenkomt met de verantwoordelijkheid als deugd.[63] Door het rapport van TNO openbaar te maken en in te gaan op spreekverzoeken, zou er kunnen worden gesteld dat de landelijke politie zich houdt aan de plichten die worden gesteld door het mechanisme. Er wordt echter nog steeds weinig verantwoording afgelegd als deugd, aangezien dit rapport niet bedoeld is voor het algemene publiek en verdere informatie enkel lijkt te worden verschaft wanneer hier actief naar gevraagd wordt. Dit bemoeilijkt de beoordeling van het handelen van de politie door burgers. Het is goed mogelijk dat er in een later stadium van het project openlijker en toegankelijker wordt gecommuniceerd over de keuzes die zijn gemaakt. Burgers hebben dan echter niet meer de mogelijkheid om die keuzes te beïnvloeden.

Tot slot trekken de bevindingen van dit rapport de mate waarin de politie zich daadwerkelijk houdt aan de plichten die worden gesteld door het mechanisme in twijfel. Op 16 april 2020 is er namelijk een reactie op een verzoek op grond van de Wet openbaarheid van bestuur (Wob) openbaar gemaakt, waarin wordt gereageerd op “het verzoek tot openbaarmaking van alle documenten die betrekking hebben op onderzoek naar een bredere inzet van gezichtsherkenning bij de uitvoering van de politietaak”.[64] In de reactie wordt expliciet gesteld dat er van een specifiek onderzoek naar een bredere inzet van gezichtsherkenning binnen de politie geen sprake blijkt te zijn. Daarbij wordt genoemd dat er wel een oriëntatie op gezichtsherkenning bezig is. De dunne lijn tussen oriëntatie en onderzoek is in dit geval interessant, aangezien uit het interview met de landelijke politie

blijkt dat er ruim voor 16 april 2020 al experimenten met acteurs zijn uitgevoerd in de Johan Cruijff ArenA.

6. AANBEVELINGEN LIVING LAB DIGITALE PERIMETER

In de voorgaande paragrafen zijn een aantal ethische overwegingen uiteengezet. Er kunnen hieruit een aantal algemene punten worden gedestilleerd die in beide projecten terugkomen en een rode lijn vormen in het project.

Ethics bluewashing

In zowel de openbare communicatie over het project als het interview met de gemeente Amsterdam wordt benadrukt dat er aan de principes van het Tada-manifest wordt voldaan. Zoals is aangetoond, blijkt dit in de praktijk enkel op oppervlakkige wijze of helemaal niet het geval te zijn. Er kan dan worden gesproken over *ethics bluewashing*, een term afgeleid van wat binnen milieu ethiek wordt aangeduid als *greenwashing*, waarbij organisaties of bedrijven zich 'groener' voordoen dan ze in werkelijkheid zijn. Met betrekking tot digitale ethiek, wordt deze praktijk als volgt beschreven: "implementing superficial measures in favour of the ethical values and benefits of digital processes, products, services, or other solutions to appear more digitally ethical than one is".[65] Dit is binnen het project Digitale Perimeter terug te zien in het feit dat er oppervlakkige, onvolledige, of onjuiste informatie over het project zelf en de te implementeren technologieën naar buiten wordt gebracht, waardoor maar gebrekkig of helemaal niet aan de onderschreven Tada-waarden kan worden voldaan. Hierdoor bestaat het gevaar dat het voor de burger onduidelijk is welke betekenis zij kunnen toekennen aan een vermelding van de Tada-waarden of de ambities van de gemeente met betrekking tot de invulling van deze waarden. Om dit te voorkomen, zijn er twee strategieën aan te bevelen: transparantie en kennisvergroting.[66] Toegankelijke, verklaarbare en op bewijs gebaseerde informatie over wat er binnen het project gebeurt, toont welwillendheid aan om verantwoording af te leggen voor de manier van werken en daadwerkelijk in overeenstemming te blijven met de onderschreven waarden. Deze welwillendheid wordt versterkt door zelf actief informatie in te winnen over de ethische bezwaren die er kunnen bestaan en deze ook daadwerkelijk te laten meewegen in de besluitvorming. Op deze manier ontstaat er een volledige beeld van de technologieën waarmee wordt geëxperimenteerd, kan er op grondigere manier v erantwoording worden afgelegd over wat er binnen het project gebeurt en is de kans uiteindelijk groter dat ieder component binnen het project daadwerkelijk in overeenstemming blijft met essentiële publieke waarden.

Van privacy by design naar value sensitive design

Nu kan er worden gesteld dat het bij experimenten niet altijd mogelijk is om direct voldoende zicht te hebben op de risico's die eraan verbonden zijn of welke waarden er overschreden zouden kunnen worden. Experimenten zijn ten slotte bedoeld om ruimte te bieden voor fouten en het onderzoeken van verschillende scenario's. Echter, wanneer het experimenten in de publieke ruimte betreft, kan de onderzoeker zich minder fouten of flexibiliteit met betrekking tot het maken van een inbreuk op de rechten en vrijheden van (onwetende) participanten veroorloven. Ook de experimenten met gezichtsherkenning zijn geen vrije speelplaats om zonder voldoende inachtneming van ethische overwegingen aan de slag te gaan. Zoals eerder benoemd, wordt de kans dat een technologie ingezet wordt groter wanneer de werking ervan aantrekkelijker wordt gemaakt. Wanneer er in het experiment voornamelijk wordt gekeken naar verbetering op één specifiek vlak, in dit geval gegevensbescherming, blijven andere publieke waarden onderbelicht en blijft de kans bestaan dat deze bij implementatie alsnog worden geschonden.

Zoals eerder benoemd, zeggen zowel de gemeente Amsterdam als de landelijke politie en TNO de ontwerpstrategie privacy by design te incorporeren in hun projecten. Hiermee wordt vanaf het begin af aan een zorgvuldige omgang met persoonsgegevens afgedwongen.[67] Dit is een positieve werkwijze, en onmisbaar om in overeenstemming met de AVG te blijven. Echter, als aanvulling hierop is het raadzaam om ook *value sensitive design* als strategie te incorporeren. Deze strategie wordt gedefinieerd als een theoretisch geaarde benadering waarin menselijke waarden op principiële en omvangrijke manier worden meegenomen gedurende het hele ontwerpproces.[68] Dit kan worden gedaan door middel van drie iteratieve stadia, namelijk conceptueel, empirisch en technisch.[69] In het conceptuele stadium worden de directe en indirecte stakeholders en de voor hen belangrijke waarden geïdentificeerd. De empirische component bestaat uit kwantitatief en kwalitatief onderzoek naar de menselijke context waarin de technologie mogelijk wordt geïmplementeerd waarbij kan worden onderzocht welke waarden er op het spel zouden kunnen komen te staan. Het technische aspect behelst een onderzoek naar de mate waarin de technologie in kwestie het toelaat om de bevindingen uit de twee eerdere fases te incorporeren in het ontwerp. Wat hierbij van belang is, is dat deze drie stadia bij iedere nieuwe stap van het proces doorlopen worden.

Op deze manier wordt een oppervlakkige of eenzijdige invulling van onderschreven waarden voorkomen en kan er gewaarborgd worden dat er in iedere stap van het proces voldoende aandacht aan deze waarden wordt geschonken.

7. CONCLUSIE

In dit rapport is uiteengezet welke waarden er meespelen voor de betrokken partijen bij het project Digitale Perimeter en de manier waarop daar in de praktijk invulling aan wordt gegeven. Door de openbaar toegankelijke communicatie over het project onder de loep te nemen, is naar voren gekomen dat waarden als innovatie, veiligheid en mobiliteit volgens de betrokken partijen stelselmatig worden aangevuld met de waarden en principes beschreven in het Tada-manifest. Daarnaast brengt het feit dat de gemeente Amsterdam onderdeel uitmaakt van de Coalitie van steden voor Digitale Rechten ook plichten op het gebied van mensenrechtelijke waarden met zich mee. Met behulp van interviews met de betrokken partijen, gestructureerd volgens De Ethische Data Assistent (DEDA), is vervolgens onderzocht op welke manier de onderschreven waarden invulling vinden in de uitvoer van de experimenten binnen het project en waar zich eventuele knelpunten bevinden of waarden overschreden worden. Op basis van de informatie die uit deze interviews naar voren is gekomen, is opgemerkt dat er sprake is van twee losse projecten: één gericht op mogelijke inzet van technologische toepassingen in en rondom de Johan Cruijff ArenA en de ander gericht op het experimenteren met gezichtsherkenning voor eventuele nationale inzet. Hoewel er in beide projecten veel aandacht wordt besteed aan gegevensbescherming, lijkt er op andere vlakken nog te weinig of helemaal geen invulling te worden gegeven aan de onderschreven waarden, waarbij ook andere ethische implicaties over het hoofd lijken te worden gezien. Om de experimenten binnen de Digitale Perimeter in overeenstemming te houden met (de onderschreven) publieke waarden en mensenrechten zijn een aantal aandachtspunten uiteengezet in de vorm van ethische overwegingen, onderbouwd met relevante theorie. Op basis hiervan zijn onderstaand per afzonderlijk project aanbevelingen opgesteld. Daarna zijn de twee algemene aanbevelingen, zoals uiteengezet in h oofdstuk 5, nogmaals kort herhaald.

Gemeente Amsterdam (en Johan Cruijff ArenA)

1. Breng openbare communicatie op orde
De openbare communicatie vanuit de gemeente Amsterdam over Digitale Perimeter komt niet overeen met wat er daadwerkelijk binnen het project gebeurt. Daarnaast is de informatie over Public Eye in het algoritmeregister pas na implementatie van de toepassing in de publieke ruimte openbaar gemaakt en biedt het maar gedeeltelijke transparantie. Dit bemoeilijkt de mogelijkheid om de gemeente verantwoordelijk te houden voor haar acties en kan tot gevolg hebben dat burgers zich tevredener en veiliger wanen dan wellicht zou moeten. Zorg ervoor dat de communicatie over dit soort projecten actueel en volledig is en zich op één gemakkelijk vindbare plek bevindt.

2. Vergroot inspraak burgers De informatieavonden van Catalyst zijn niet voldoende. Het is te kleinschalig en er zijn te weinig burgers aanwezig. Hierdoor kan niet aan de Tada-principes ‘legitiem en gecontroleerd’ en ‘inclusief’ worden voldaan, terwijl de indruk wordt gewekt dat dit wel het geval is. Zoek het debat actief breder op: neem deel aan de discours die door burgers, activisten, overheidsinstanties en media wordt gevormd om een representatiever en diverser beeld te vormen van wenselijke vooruitgang.

3. Beweeg richting je uitgangspunten Door de implementatie van Public Eye en de interesse in experimenten met bodycams en gezichtsherkenning lijkt de gemeente Amsterdam zich niet in de richting te bewegen van het door henzelf geformuleerde uitgangspunt waarin gesteld wordt dat de Amsterdamse burger zich onbespied en anoniem door de stad moet kunnen bewegen. Evalueer of de projecten en keuzes en de daarvan mogelijke lange termijn gevolgen ook in bredere context in lijn zijn met waar de stad voor wil staan.

4. Experimenteer in afgebakende ruimte De ruimte waarin wordt geëxperimenteerd met Public Eye is niet afgebakend en het wordt op verschillende locaties gebruikt. Het is aan te raden om niet in het wilde weg te gaan experimenteren, maar hier een duidelijk afgebakende locatie voor te kiezen. Op deze manier is het voor burgers duidelijk waar het experiment begint en eindigt en kunnen zij ervoor kiezen dit gebied niet te betreden.

5. Blijf ook bij experimenten in overeenstemming met de AVG Het Blue-force tracking systeem kan vanwege de machtsverhouding tussen werkgever en werknemer niet als wettelijk toelaatbaar worden beschouwd op basis van de AVG. Dit geldt ook voor experimenten met de toepassing.

Landelijke politie (en TNO)

1. Neem in iedere stap grondrechten in acht In het rapport van TNO zijn de mogelijke dreigingen voor grondrechten uiteengezet, maar in het vervolg van de experimenten is de focus gelegd op het vergroten van gegevensbescherming. Aangezien de politie stelt dat zij wil onderzoeken of er ook een meer verantwoorde vorm van gezichtsherkenning bestaat, zou hiermee

onbewust het signaal kunnen worden afgegeven dat de overige ingrijpende risico's minder zwaarwegend zijn.

2. Erken de gebreken van de geïsoleerde setting De experimenten met gezichtsherkenning kunnen en mogen alleen worden uitgevoerd in gecontroleerde en geïsoleerde setting. Een volledig beeld van de werking en de sociaal-maatschappelijke invloed kan pas worden gevormd wanneer de technologie in het sociale en technische netwerk waarin het ingebed zou worden wordt geplaatst. Wel zijn er al reële maatschappelijke risico's bekend die met behulp van de huidige experimenten niet kunnen worden gemitigeerd. Door dit te erkennen zou de politie wellicht al tot de morele overweging kunnen komen om de tijd en middelen in onderzoek naar eventuele andere, minder schadelijke, beveiligingsmogelijkheden te investeren.

3. Wees welwillend(er) in het afleggen van verantwoording De transparantie over het project is op dit moment nog niet voldoende. Om daadwerkelijk het publieke debat op te zoeken en verantwoording af te leggen naar burgers, is het raadzaam om het debat actiever en breder op te zoeken en de openbare communicatie over het project toegankelijker te maken.

Algemene aanbevelingen

1. Vergroot transparantie en kennis Toegankelijke, verklaarbare en op bewijs gebaseerde informatie over wat er binnen het project gebeurt, toont welwillendheid aan om verantwoording af te leggen voor de manier van werken en daadwerkelijk in overeenstemming te blijven met de onderschreven waarden. Deze welwillendheid wordt versterkt door zelf actief informatie in te winnen over de ethische bezwaren die er kunnen bestaan en deze ook daadwerkelijk te laten meewegen in de besluitvorming.

2. Implementeer value sensitive design Het is raadzaam om value sensitive design als strategie te incorporeren. Deze strategie wordt gedefinieerd als een theoretisch geaarde benadering waarin menselijke waarden op principiële en omvangrijke manier worden meegenomen gedurende het hele ontwerpproces. Op deze manier wordt een oppervlakkige of eenzijdige invulling van onderschreven waarden voorkomen en kan er gewaarborgd worden dat er in iedere stap van het proces voldoende aandacht aan deze waarden wordt geschonken.

Noten

1. Lees hier wat Bits of Freedom eerder schreef over living lab Stratumseind in Eindhoven: https://www.bitsoffreedom.nl/2019/06/05/experimentele-manipulatie-burger-steeds-vaker-onwetend-proefdier/.
2. ``Digitale Perimeter,'' Gemeente Amsterdam, bezocht op 9 april, 2021, https://web.archive.org/web/20210422093634
3. Bruno Latour, Reassembling the Social: An Introduction to Actor-Network-Theory (Oxford: Oxford University Press, 2005).
4. Annelli Janssen, Linda Kool, en Jelte Timmer, Dicht op de huid - Gezichts- en emotieherkenning in Nederland (Den Haag: Rathenau Instituut 2015), 10.
5. Mary Flanagan, Daniel C. Howe, and Helen Nissenbaum, ``Embodying Values in Technology: Theory and Practice,'' in Information Technology and Moral Philosophy, ed. Jeroen van den Hoven en John Weckert (Cambridge: Cambridge University Press, 2008): 323.
6. Bart Karstens, Linda Kool, en Rinie van Est, Voeten in de aarde - Datagestuurde innovatie in de stad (Den Haag: Rathenau Instituut, 2020).
7. Karstens, Kool, en van Est, Voeten in de aarde, 6
8. Kastens, Kool, en van Est, Voeten in de aarde, 6-7.
9. Aline Shakti Franzke, Iris Muis, en Mirko Tobias Schäfer, ``Data Ethics Decision Aid (DEDA): a dialogical framework for ethical inquiry of AI and data projects in the Netherlands,'' Ethics and Information Technology 22, no. 4 (January 2021). https://doi.org/10.1007/s10676-020-09577-5.
10. Utrecht Data School, De Ethische Data Assistent - Handleiding, Utrecht Data School, Universiteit Utrecht 2019, 6.
11. ``Perimeter definities,'' Encyclo.nl, bezocht op 9 april, 2021, https://www.encyclo.nl/begrip/perimeter.
12. ``Digitaal definities,'' encyclo.nl, bezocht op 9 april, 2021, https://www.encyclo.nl/begrip/Digitaal.
13. Gemeente Amsterdam, ``Digitale Perimeter.''
14. ``TNO neemt deel aan nieuwe samenwerking rondom digitale beveiliging Johan Cruijff ArenA,'' TNO, bezocht op 9 april, 2021, https://www.tno.nl/nl/over-tno/nieuws/2019/9/nieuwe-samenwerking-rondom-digitale-beve
15. Gemeente Amsterdam, ``Digitale Perimeter.''
16. Gemeente Amsterdam, ``Digitale Perimeter.''
17. ``Innovation lab,'' Johan Cruijff ArenA, bezocht op 9 april, 2021, https://www.johancruijffarena.nl/innovationl
18. Gemeente Amsterdam, ``Digitale Perimeter.''
19. ``Digital Perimeter,'' Amsterdam Smart City, bezocht op 9 april, 2021, https://amsterdamsmartcity.com/updates/p
20. ``Public Eye,'' Amsterdam Algoritmeregister Beta, gemeente Amsterdam, bezocht op 28 april, 2021, https://algoritmeregister.amsterdam.nl/public-eye/.
21. Niels Waarlo en Laurens Verhagen, ``De stand van gezichtsherkenning in Nederland,'' de Volkskrant, 27 maart, 2020, https://www.volkskrant.nl/kijkverder/v/2020/de-stand-van-gezichtsherkenning-in-nederland~v91028/.
22. Lees hier wat Bits of Freedom eerder schreef over CATCH, de gezichtsherkenningssoftware die de landelijke politie op dit moment gebruikt: https://www.bitsoffreedom.nl/2019/09/11/minister-komt-met-zorgwekken
23. ``AP: Pas op met camera's met gezichtsherkenning,'' Autoriteit Persoonsgegevens, 29 oktober, 2020, .https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-pas-op-met-camera%E2%80%99s-met-gezichtsherkenning.
24. Johan Cruijff ArenA, ``Innovation Lab.''
25. Gemeente Amsterdam, ``Digitale Perimeter.''
26. ``Over ons,'' Tada, bezocht op 9 april, 2021, https://tada.city/over-ons/.
27. Tada, ``over ons.''
28. ``Tada Toolkit,'' Tada, bezocht op 9 april, 2021, https://tada.city/tada-toolkit/.
29. Tada, ``Tada toolkit.''
30. Tessel Renzenbrink, ``Tada en de Gemeente Amsterdam. Het verslag van de eerste zes maanden,'' Tada, 1 maart, 2019, https://tada.city/nieuws/tada-in-de-praktijk/.
31. De Coalitie van steden voor Digitale Rechten, ``Coalitie van steden voor Digitale Rechten,'' voorjaar 2020, 3.
32. Gemeente Amsterdam, ``Digitale Perimeter.''
33. Jaap-Henk Hoepman, Privacyontwerpstrategieën (Het Blauwe Boekje), 27 januari, 2020.
34. Bart W. Schermer, Dominique Hagenauw, en Nathalie Falot, ``Handleiding Algemene verordening gegevensbescherming,'' Ministerie van Justitie en Veiligheid, 50.
35. ``Public Eye,'' Amsterdam Algoritmeregister Beta, gemeente Amsterdam, bezocht op 28 april, 2021, https://algoritmeregister.amsterdam.nl/public-eye/.
36. Gemeente Amsterdam, ¨Public Eye.''
37. AT5, ``AT5-panel: weinig zorgen om privacy, maar onduidelijk waar camera's precies hangen,'' laatst aangepast op 17 februari, 2021.
38. Gemeente Amsterdam, ``Public Eye.''
39. Matteo Turilli en Luciano Floridi, ``The ethics of information transparency,'' Ethics of Information Technology 11 (maart 2019), 105. DOI 10.1007/s10676-009-9187-9.
40. Turilli en Floridi, ``The ethics of information transparency,'' 107.
41. NLdigital, ``De Avg uitgelegd deel 2: transparantie en het recht op informatie,'' 8 maart 2017, https://www.nldigital.nl/news/de-avg-uitgelegd-deel-2-transparantie-en-het-recht-op-informatie/.
42. Gemeente Amsterdam, ``Public Eye.''

43. Linnet Taylor, ``Public Actors Without Public Values: Legitimacy, Domination and the Regulation of the Technology Sector,'' Philosophy & Technology (januari 2021), 1. https://doi.org/10.1007/s13347-020-00441-4.
44. Lees hier wat Bits of Freedom eerder schreef over de risico's van de toenemende invloed van techbedrijven in de openbare ruimte: https://www.bitsoffreedom.nl/2016/02/11/blog-of-things-smart-cities-en-de-
45. Marije Vlaskamp, ``Onderzoeksbureau: Chinese techbedrijven bezig met etnisch profileren: Oeigoeren zijn doelwit,'' de Volkskrant, 13 januari 2021, https://www.volkskrant.nl/nieuws-achtergrond/onderzoeksbureau-c
46. ``Hoe ziet de toekomst van de stad eruit?'' VU, NEMO Kennislink, bezocht op 16 april, 2021. https://sites.google.com/view/catalystamsterdam.
47. Ricardo Fabrino Mendonça, Selen Ercan, en Hans Asenbaum, ``More Than Words: A Multidimensional Approach to Deliberative Democracy,'' Political Studies (September 2020), 2. https://doi.org/10.1177/0032321720
48. Mendonça, Ercan, en Asenbaum, ``More Than Words,'' 2.
49. Gemeente Amsterdam, ``Datastrategie Gemeente Amsterdam: Amsterdamse zelfbeschikking over Data - 2021-2022,'' januari 2021, 5.
50. Autoriteit Persoonsgegevens, ``Vragen over de grondslag toestemming,'' bezocht op 16 april, 2021. https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/mag-u-persoonsgegevens-verwerken#w
51. Evgeny Morozov, To Save Everything, Click Here: Technology, Solutionism and the Urge to Fix Problems That Don't Exist (London: Penguin Books Ltd. 2014).
52. J.H.C. van Rest, T. Attema, T. Timan, R.J.M. den Hollander, en G.P. van Voorthuijsen, Privacy bescherming bij niet-coöperatieve gezichtsherkenning, (Den Haag: TNO, 2021), 2.
53. Van Rest, Attema, Timan, den Hollander, en van Voorthuijsen, Privacy bescherming, 2.
54. Van Rest, Attema, Timan, den Hollander, en van Voorthuijsen, Privacy bescherming, 38.
55. Van Rest, Attema, Timan, den Hollander, en van Voorthuijsen, Privacy bescherming, 61.
56. Daniel Solove, ``A Taxonomy of Privacy,'' University of Pennsylvania Law Review 154, no. 3 (February 2005), DOI:10.2307/40041279; Hoepman, Privacyontwerpstrategieën.
57. Patrick Grother, Mei Ngan, en Kayee Hanaoka, ``Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects,'' National Institute of Standards and Technology (December 2019), 2-3. Https://doi.org/10.6028/NIST.IR.8280.
58. Grother, Ngan, Hanaoka, ``Face Recognition Vendor Test,'' 2.
59. Lees hier wat Bits of Freedom eerder schreef over de risico's van gezichtsherkenning in de publieke ruimte: https://www.bitsoffreedom.nl/2019/07/01/volg-san-francisco-verbied-gezichtsherkennings-softwar
60. Lucas D. Introna, and David Wood, ``Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems,'' Surveillance & Society CCTV Special 2, no. ⅔ (2004): 195. https://doi.org/10.24908/ss.v2i2/3.3373.
61. Lees hier wat Bits of Freedom eerder schreef over waarom normalisering van gezichtsherkenning problematisch is: https://www.bitsoffreedom.nl/2020/01/29/facial-recognition-a-convenient-and-efficient-solution
62. Mark Bovens, ``Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism,'' West European Politics 33, no. 5 (September 2010): 946--67, https://doi.org/10.1080/01402382.2010.486119.
63. Bovens, ``Two Concepts of Accountability,'' 961.
64. Politie, ``(2020) Bredere inzet gezichtsherkenning,'' 16 april, 2020. https://www.politie.nl/wob/korpsstaf/2020
65. Luciano Floridi, ``Translating Principles into Practices of Digital Ethics: Five Risks of Being Unethical,'' Philosophy and Technology 32 (2019), 187. https://doi.org/10.1007/s13347-019-00354-x.
66. Floridi, ``Translating Principles,'' 188.
67. Hoepman, Privacyontwerpstrategieën (Het Blauwe Boekje), 1.
68. Batya Friedman, Peter H. Kahn Jr., Alan Borning, and Alina Huldtgren, ``Value Sensitive Design and Information Systems,'' Early Engagement and New Technologies: Opening up the Laboratory. Philosophy of Engineering and Technology 16, edited by N. Doorn, D. Schuurbies, I. van de Poel, and M. Gorman (Dordrecht: Springer, 2013): 56.
69. Friedman, Kahn Jr., Borning, en Huldtgren, ``Value Sensitive Design,'' 72-73.

Bits of Freedom komt op voor jouw vrijheid en privacy op internet.
Deze grondrechten zijn onmisbaar voor je ontwikkeling, voor technologische innovatie en voor de rechtsstaat. Maar die vrijheid is niet vanzelfsprekend. Je gegevens worden opgeslagen en geanalyseerd. Je internetverkeer wordt afgeknepen en geblokkeerd.

Bits of Freedom zorgt ervoor dat jouw internet jouw zaak blijft.

Bits of Freedom
www.bitsoffreedom.nl
@bitsoffreedom
Prinseneiland 97HS
1013 LN Amsterdam

Contactpersoon:
Bér Engels
+31 6 5881 5392
ber@bitsoffreedom.nl

C78C 306E 7F6D C3EF 7F1B
B77A 0CD1 8909 823C 8585
(bitsoffreedom.nl/openpgp)

BITS OF FREEDOM

Voor jouw internetvrijheid