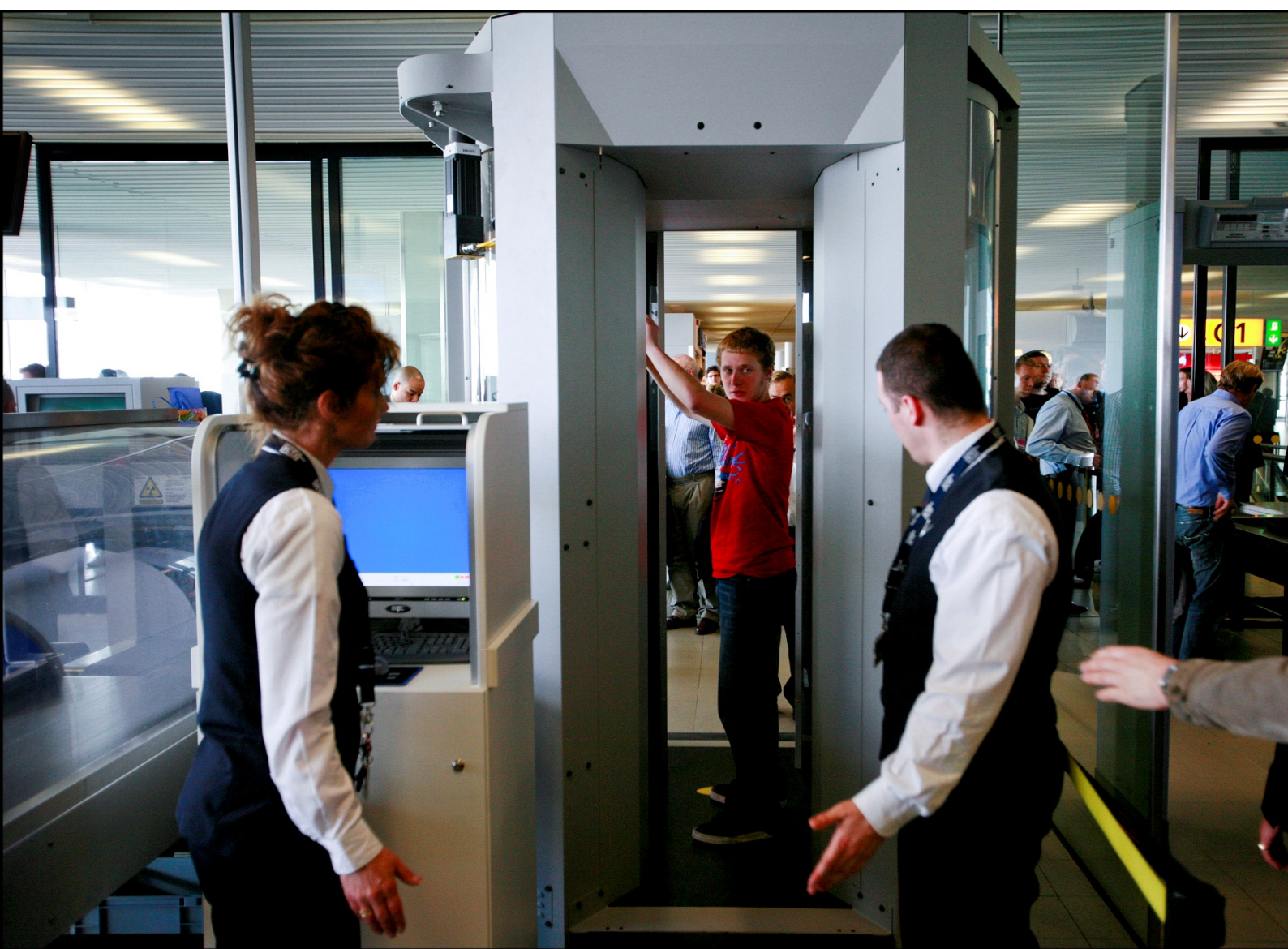


Hoe kijken burgers naar het gebruik van sensordata voor leefbaarheid en veiligheid?

Begrippenkader om met burgers in gesprek te gaan



Artikel

Auteurs

Marijn Biesiot, Erik de Bakker, Tim Jacquemard & Rinie van Est

Redactie

Frank Steverink

Illustraties en foto's

Rikkers Infographics

Foto omslag

Nederland, Schiphol, 15-05-2007, Introductie / wereldprimeur van de Security Scan. Een oppervlakte scanner die, voor het lichaam onschadelijke, straling uitzendt en zo lichaamsvreemde objecten op het lichaam kan waarnemen. Handmatig fouilleren wordt daarmee overbodig. Foto Michael Kooren / Hollandse Hoogte

Bij voorkeur citeren als:

Biesiot, M., E. de Bakker, T. Jacquemard & R. van Est (2018). Hoe kijken burgers naar het gebruik van sensordata voor leefbaarheid en veiligheid? – *Begrippenkader om met burgers in gesprek te gaan*. Den Haag: Rathenau Instituut

Het Rathenau Instituut onderzoekt op verzoek van de Nationale Politie hoe burgers aankijken tegen het gebruik van sensordata om leefbaarheid en veiligheid te verbeteren. Om daar goed zicht op te krijgen organiseren we zes focusgroepen met Nederlandse burgers. In de focusgroepen brengen we burgers met behulp van een aantal scenario's met elkaar in gesprek. De focusgroepen moeten zicht bieden op de percepties van diverse burgers en de motivaties achter hun meningen.

Ons doel is dat er in de focusgroepen zoveel mogelijk aspecten met betrekking tot de percepties van burgers besproken worden. We maken daarvoor gebruik van inzichten uit eerdere onderzoeken. Dit artikel zet op een rij wat wetenschappelijke literatuur zegt over de percepties van burgers met betrekking tot het gebruik van sensoren en sensordata. We introduceren een begrippenkader dat ons helpt de focusgroepen volgens bovengenoemde doelstelling voor te bereiden en vorm te geven.

Meer informatie over het onderzoek staat op onze website:

<https://www.rathenau.nl/nl/digitale-samenleving/nieuw-onderzoek-sensordata-voor-veiligheid-en-leefbaarheid>

Eerder verscheen in het kader van dit onderzoek: Overal ogen en oren – *De inzet van sensordata voor leefbaarheid en veiligheid*.

<https://www.rathenau.nl/nl/digitale-samenleving/inzet-van-sensordata-voor-leefbaarheid-en-veiligheid>

Inleiding

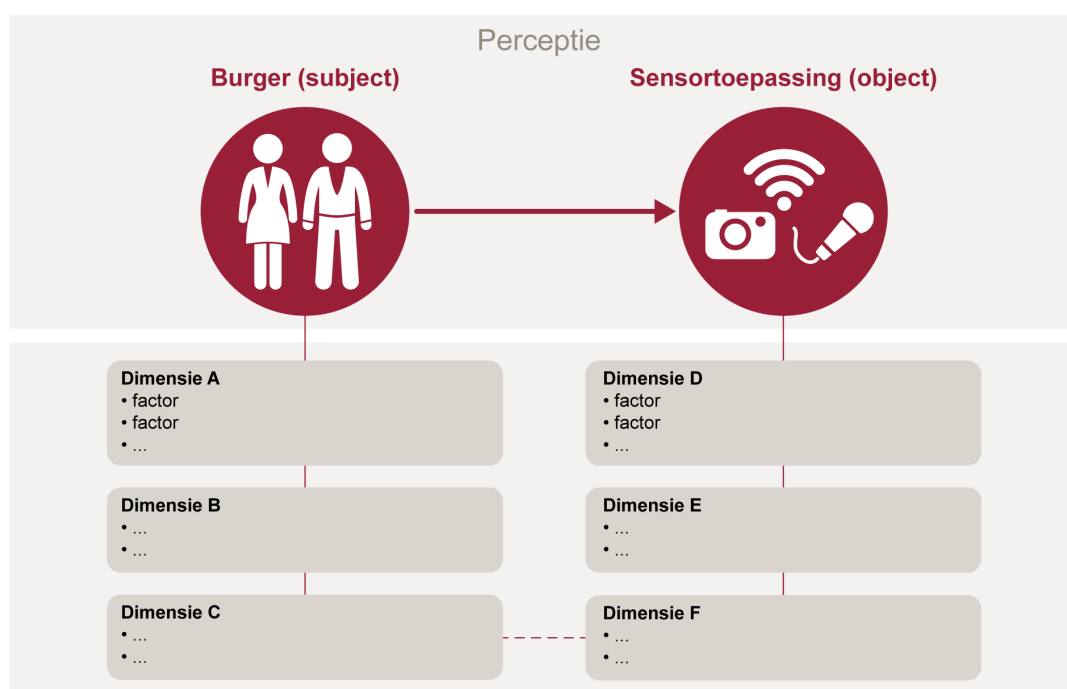
Toen de securityscanners tien jaar geleden op Schiphol werden geïntroduceerd ontstond er ophef over deze 'naaktscanners'. Opiniemakers en media stelden vragen. Ging de manier waarop reizigers zich moesten 'blootgeven' in de scanner niet te ver? Konden mensen erop vertrouwen dat de beveiliging zorgvuldig omging met de data? Was het zeker dat er geen negatieve gezondheidseffecten waren? Waren de scanners wel het juiste middel in de strijd tegen terrorisme?

Deze vragen wijzen op factoren die invloed kunnen hebben op de mate waarin burgers een sensortoepassing wel of niet acceptabel vinden, zoals het omgaan met persoonlijke gegevens en gezondheidsveiligheid. In dit artikel zoeken we naar meer van dit soort factoren. Inzicht in wat er al bekend is over de percepties van burgers helpt ons bij het voorbereiden van de focusgroepen. In de focusgroepen gaan gewone Nederlanders in kleine groepen met elkaar in gesprek over verschillende

situaties waarin sensoren¹ en sensordata worden gebruikt om de leefbaarheid en veiligheid² te verbeteren. Wat vinden ze van die situaties, welke afwegingen maken ze en welke onderliggende redenen hebben hun meningen?

In dit artikel introduceren we een begrippenkader voor de percepties van burgers over het gebruik van sensoren en sensordata. Ons uitgangspunt is: *iemand* (een subject) heeft een perceptie van *iets* (een object). Oftewel, *een burger vindt een sensortoepassing* acceptabel of niet. Het subject en het object van perceptie vormen het eerste niveau van ons begrippenkader.

Figuur 1 Introductie begrippenkader



Bron: Rathenau Instituut

Of een burger een sensortoepassing acceptabel vindt (of niet), kan te maken hebben met kenmerken van de burger zelf (staat iemand open voor het delen van informatie?) en van de sensortoepassing (wat voor soort informatie wordt verzameld?). Het begrippenkader is een handvat om naar relevante factoren te zoeken in praktijkvoorbeelden en wetenschappelijke literatuur, en om de factoren

-
- 1 Met 'sensoren' bedoelen we digitale meetinstrumenten die data verzamelen over de fysieke en sociale omgeving. Voorbeelden van digitale sensoren zijn de camera en gps op een smartphone.
 - 2 Het onderzoek 'Burgerperspectief op inzet sensordata voor leefbaarheid en veiligheid' richt zich op een breed spectrum van leefbaarheid en veiligheid. Onder *leefbaarheid* verstaan we lichte overtredingen, zoals afval op straat gooien. Aan de andere kant van het spectrum staan zwaardere misdrijven die voor een groot gevoel van *onveiligheid* zorgen, zoals straatroof, bedreigingen, mishandeling en zware vormen van criminaliteit zoals drugs- en mensenhandel. Dit onderzoek blijft daarmee dicht bij de taak van de politie, die zich in de kern richt op handhaving van de rechtsorde en hulpverlening bij nood. Bij een keuze om een praktijkvoorbeeld te bespreken stellen we ons daarom altijd de vraag: is dit een situatie waarvoor je de politie zou kunnen bellen?

vervolgens op een logische manier te ordenen in dimensies die betrekking hebben op het subject of object.

We leggen eerst uit waarom we ons in dit artikel vooral richten op surveillance en niet op de andere vormen van sensortoezicht die we in het vorige artikel ‘Overall ogen en oren’ identificeerden. Vervolgens bestuderen we twee praktijkvoorbeelden van surveillance met sensoren en identificeren drie belangrijke dimensies van sensortoepassingen. Vervolgens zoeken we in wetenschappelijke studies naar factoren die kunnen beïnvloeden in welke mate burgers een sensortoepassing wel of niet aanvaardbaar vinden. Met die inzichten vullen we ons begrippenkader verder in. Tot slot komen we terug op de verschillende vormen van sensortoezicht en formuleren we op basis van de inzichten uit dit artikel een aantal handvatten voor de focusgroepen.

Surveillance met sensoren

De securityscanners op de luchthaven Schiphol zijn een voorbeeld van surveillance met sensoren om de veiligheid te vergroten. Bij surveillance wordt ‘gericht, systematisch en routinematig’ naar persoonlijke details gezocht.³ In dit geval zoeken de scanners op de luchthaven naar voorwerpen op het lichaam, maar sensoren kunnen allerlei soorten data verzamelen (zoals locaties, vingerafdrukken, geluiden en beelden).

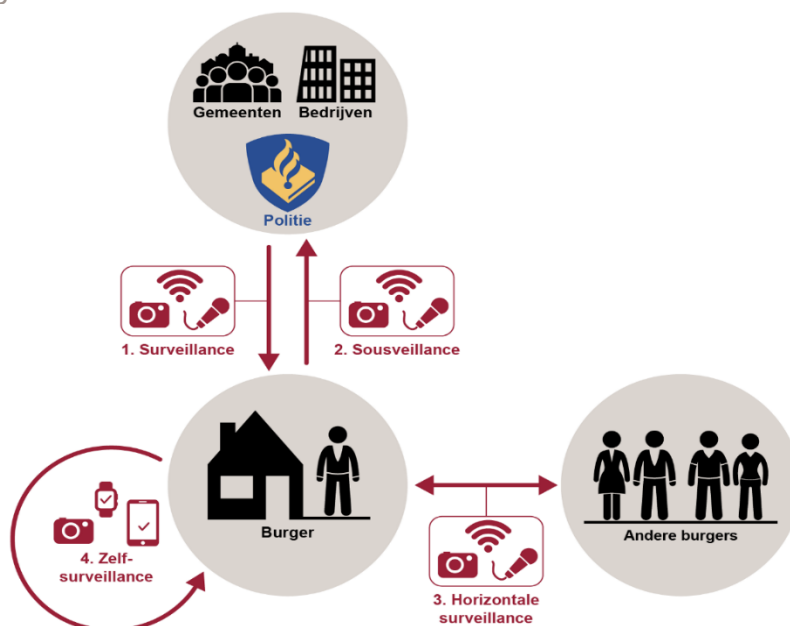
In het vorige artikel zagen we dat ‘sensoretoezicht’ een dynamisch en interactief proces is. Het gebeurt niet vanuit één centraal punt.⁴ Burgers, overheidsinstanties en bedrijven bekijken elkaar én worden bekeken. Naast het toezicht van overheidsinstanties en bedrijven op burgers (*surveillance*), houden burgers omgekeerd ook met sensoren organisaties (*sousveillance*) en andere burgers (*horizontale surveillance*) in de gaten. Daarnaast zetten burgers sensoren in om zichzelf aan regels voor leefbaarheid en veiligheid te houden (*zelf-surveillance*). Figuur 2 illustreert deze vier vormen van sensortoezicht.

In dit artikel richten we ons op surveillance. Er is namelijk meer bekend over wat burgers vinden van surveillance met sensoren, dan van de andere vormen van sensortoezicht. De factoren die we vanuit dit perspectief vinden kunnen ook bij de andere vormen van sensortoezicht een rol spelen. Hier komen we aan het einde van dit artikel op terug.

3 Boutellier, H. (2015). *Het seculiere experiment. Hoe we van God los gingen samenleven*. Amsterdam: Uitgeverij Boom, hoofdstuk 4

4 Idem

Figuur 2 Vier vormen van sensortoezicht



Bron: Rathenau Instituut

Vragen over surveillance in de praktijk

We gaan dieper in op twee praktijkvoorbeelden waarin sensoren en sensordata worden ingezet om leefbaarheid en veiligheid te vergroten: securityscanners op de luchthaven Schiphol en een proef met sensordata in Roermond. We benoemen enkele maatschappelijke vragen die opiniemakers opwerpen.

Securityscanners op Schiphol

Op de luchthaven Schiphol controleren securityscanners of reizigers geen verboden voorwerpen op hun lichaam dragen. In 2009 mislukte de poging van een Nigeriaan man om een vliegtuig van Schiphol naar Detroit op te blazen met een bom. Sindsdien zijn steeds meer securityscanners in gebruik genomen om zulke aanslagen te voorkomen.⁵ Op Schiphol maken deze sensoren gebruik van millimetergolven die door kleding gaan, maar door de huid en andere materialen gereflecteerd worden.⁶ Zo worden verdachte voorwerpen gedetecteerd.

In 2007 werden passagiers op Schiphol voor het eerst op kleine schaal gecontroleerd door een securityscanner.⁷ Deze scanners toonden verboden materialen die onder kleding zijn verborgen, maar ook een driedimensionaal zwart-

5 'Hirsch Ballin wil bodyscan invoeren'. *Het Parool*, 29 december 2009. <https://www.parool.nl/binnenland/hirsch-ballin-wil-bodyscan-invoeren~a273592/>

6 'Security check'. Schiphol, geraadpleegd op 22 oktober 2018. <https://www.schiphol.nl/nl/security-check/>

7 Kamerstukken II 2006/2007, 24 804, nr.44

wit beeld van het lichaam van de reiziger. Daardoor werden de scanners in de volksmond al snel bekend als 'naaktscanners'.⁸ Om privacy te waarborgen beoordeelde een beveiligingsmedewerker het beeld in een aparte ruimte. Daarbij werd het gezicht van de reiziger afgeschermd en het beeld werd na beoordeling gewist. Het gebruik van de securityscanners op Schiphol is aangepast na kritiek op de 'naaktbeelden' van reizigers.

De securityscanners op Schiphol geven nu de plek van verdenking aan op een getekend poppetje. Dit plaatje van de scan is ter plekke zichtbaar voor zowel de reiziger als de beveiligingsmedewerker.⁹ Zo zijn de resultaten van het scanningsproces transparant gemaakt voor de reiziger. Schiphol zegt daarover: 'De scan wordt geanalyseerd door een computer en niet door een beveiligingsmedewerker. De scan kan niet door je lijf heen kijken en ziet je ook niet naakt. Daarmee is je privacy gewaarborgd.'¹⁰

Maatschappelijke organisaties en opiniemakers brengen verschillende kritische vragen naar voren over de securityscanners op luchthaven Schiphol. In 2009 uitte burgerrechtenorganisatie Bits of Freedom zorgen over de inbreuk van de 'naaktscanners' op privacy en lichamelijke integriteit.¹¹ In hun ogen worden reizigers 'digitaal uitgekleeft'. Hoe weet je zeker dat beveiligingspersoneel wel integer omgaat met het beeldmateriaal?¹² Daarnaast wees Bits of Freedom erop dat de scanners niet foutloos zijn, hoge kosten met zich meebrengen en het risico van aanslagen slechts deels kunnen beperken.¹³ Ancilla van de Leest, destijds lijsttrekker van de Piratenpartij die zich sterk maakt voor digitale burgerrechten, kaartte in de zomer van 2015 de regels en procedures aan die bij deze scans gelden voor zwangere vrouwen.¹⁴

In de ogen van Bits of Freedom en Van de Leest hebben securityscanners dus ook minder wenselijke kanten. Ze stellen de vraag of de inzet van security scanners een effectief middel is in de strijd tegen terrorisme. Zijn aanslagen wel te voorkomen met een maatregel als de securityscan? Aan de andere kant, wat vinden burgers

8 Zie bijvoorbeeld: 'Naaktscan of bodyscan?', *de Volkskrant*, 18 november 2010.

<https://www.volkskrant.nl/nieuws-achtergrond/naaktscan-of-bodyscan-~q1dd14d9/>

9 'Wat ik zie als jij in de securityscan staat'. Schiphol, 14 juli 2017. <https://nieuws.schiphol.nl/wat-ik-zie-als-jij-in-de-securityscan-staat/>

10 'Security check' (veelgestelde vragen). Schiphol, geraadpleegd op 22 oktober 2018. <https://www.schiphol.nl/nl/security-check/>

11 Van Daalen, O. Persbericht: 'Bits of Freedom: Naaktscanners niet introduceren'. Bits of Freedom, 30 december 2009. <https://www.bitsoffreedom.nl/2009/12/30/persbericht-bits-of-freedom-naaktscanners-niet-introduceren/>

12 'Open brief aan de Minister van Justitie'. Bits of Freedom, 30 december 2009. <https://www.bitsoffreedom.nl/2009/12/30/persbericht-bits-of-freedom-naaktscanners-niet-introduceren/>

13 'Open brief aan de Minister van Justitie'. Bits of Freedom, 30 december 2009. <https://www.bitsoffreedom.nl/2009/12/30/persbericht-bits-of-freedom-naaktscanners-niet-introduceren/>

14 Van de Leest, A. 'Schiphol dwingt je onterecht in de naaktscanner'. Joop, 1 juni 2015. <https://joop.bnnvara.nl/opinies/schiphol-dwingt-je-onterecht-in-de-naaktscanner>

ervan als een aanslag voorkómen had kunnen worden met een securityscanner en deze technologie niet is ingezet?

Sensoren als puntentellers in Roermond

De stad Roermond heeft veel last van winkeldieven en zakkenrollers die vooral uit Oost-Europese landen komen. In 2017 werd 456 keer aangifte gedaan van zakkenrollerij en 383 keer van winkeldiefstal.¹⁵ Roermond is een aantrekkelijke locatie voor deze vorm van criminaliteit. Dat komt mede door het grote aantal buitenlandse bezoekers uit Azië en Rusland dat (vaak met contant geld) naar het grootste outletcentrum van Europa trekt. Jaarlijks komen ongeveer acht miljoen bezoekers op het Designer Outlet Roermond af.¹⁶ Samen met de andere voorzieningen trekt Roermond jaarlijks totaal ongeveer veertien miljoen bezoekers, op een bevolking van nog geen zestigduizend.

Ondanks de inzet van private beveiligers, samenwerkingen met de Duitse en Roemeense politie en aanpassingen in de plaatselijke verordening, is het aantal incidenten de afgelopen drie jaar niet significant gedaald.¹⁷ De politie test in een zogenaamde 'proeftuin' of een nieuwe aanpak met sensortechnologie hier verandering in kan brengen.¹⁸ In juli 2018 startte de politie samen met de gemeente Roermond, TU Eindhoven en het Openbaar Ministerie een proef waarin sensordata worden gekoppeld om mogelijke bendes rondreizende criminelen al zo vroeg mogelijk op te sporen.

De proeftuin in Roermond werkt met slimme sensortoepassingen die patronen herkennen en een bijbehorend puntensysteem.¹⁹ Uit de analyse van de gekoppelde gegevens kan een 'verdacht profiel' rollen. Niet alle sensoren en sensordata worden nu al gebruikt, maar het idee voor het eerste profiel is als volgt: ANPR camera's boven de toegangswegen naar het Designer Outlet Roermond registreren de kentekens van en het aantal passagiers in alle auto's. Wanneer er een auto met een Roemeens kenteken langsrijdt, dan krijgt deze bijvoorbeeld tien punten. Zitten er vier personen in een witte huurauto, dan komen er extra punten bij. Wifi-trackers analyseren telefoongegevens en volgen verdere bewegingspatronen.²⁰ Wanneer er genoeg punten zijn toegekend aan (een groep) mensen, komt de politie in actie. Bijvoorbeeld door meer aandacht als het voertuig in de komende week nog een keer opvalt, het vragen om extra toezicht door de beveiliging of, bij herkende auto's uit eerdere incidenten, een opvolgactie door de politie zelf, zoals het aanspreken

15 Driessen, G. 'Jacht op de zakkenroller'. In: *de Limburger* 12 juli 2018.

16 'Bijna 4000 Chinezen komen shoppen in Designer Outlet Roermond'. Website Roermond Nieuws, 1 mei 2018. <https://roermond.nieuws.nl/nieuws/81749/bijna-4000-chinezen-komen-shoppen-designer-outlet-roermond/>

17 Driessen, G. 'Jacht op de zakkenroller'. In: *de Limburger* 12 juli 2018.

18 'Zakkenrollers herkennen dankzij data-koppeling'. Website Politie, 11 juli 2018. <https://www.politie.nl/nieuws/2018/juli/11/00-zakkenrollers-herkennen-dankzij-data-koppeling.html>

19 Andringa, R. 'Politie wil zakkenrollers en plofkrakers vangen met data'. NOS, 17 september 2018. <https://nos.nl/artikel/2250767-politie-wil-zakkenrollers-en-plofkrakers-vangen-met-data.html>

20 Van Teeffelen, K. 'Met camera's en sensors is een winkeldief straks op grote afstand te herkennen'. *Trouw* 17 september 2018. <https://www.trouw.nl/samenleving/met-camera-s-en-sensors-is-een-winkeldief-straks-op-grote-afstand-te-herkennen~acdee79e/>

van de bestuurder. Een dergelijk gezamenlijk optreden op basis van sensordata zou ook een afschrikwekkende werking moeten hebben.

Begin 2019 worden bovenstaande koppeling van sensordata en het gezamenlijke optreden naar aanleiding van verdachte profielen nog niet volledig uitgevoerd. Op dat moment worden bijvoorbeeld al wel de kentekens geregistreerd, maar nog niet het aantal inzittenden. Ook vindt het volgen van bewegingspatronen nog niet plaats.

In de lokale politiek is draagvlak voor deze proeftuin. Uit de samenleving klinkt wel een waarschuwend geluid. Digitale burgerrechtenorganisatie Bits of Freedom spreekt in september 2018 de zorg uit dat burgers bij voorbaat verdacht zijn wanneer ze zich afwijkend gedragen of aan bepaalde criteria voldoen. Wanneer vergelijkbare systemen in de toekomst vaker ingezet gaan worden, aldus Bits of Freedom, is er in potentie niets meer dat aan het oog van de toezichthouders kan ontsnappen. Elke vorm van verkeerd gedrag kan op geautomatiseerde wijze bestraft worden.²¹ Maar wat gebeurt er wanneer er onschuldige mensen onterecht als verdacht worden aangemerkt (*false positives*)? Wie is er verantwoordelijk voor eventuele negatieve gevolgen? Een algoritme? Bij de proeftuin in Roermond is geen sprake van automatisering van bestrafning, maar Bits of Freedom ziet hier het gevaar van een hellend vlak.

Lokke Moerel, hoogleraar Global ICT Law aan de Universiteit van Tilburg, vraagt zich af of er geen minder ingrijpende manieren bestaan om de zakkenrollers op te sporen dan data verzamelen over iedere voorbijganger.²² De kwestie die zij aanroert is of het verzamelen van informatie over grote aantallen burgers wel in verhouding staat tot het aanhouden van een mogelijk klein aantal zakkenrollers.

De Autoriteit Persoonsgegevens (AP) wees er in november 2018 op dat het digitaal volgen van mensen op straat, in winkelcentra en (semi-)openbare plekken alleen onder strikte voorwaarden is toegestaan. Wifi-tracking valt onder persoonsgegevens en dus onder privacyregels. AP-bestuursvoorzitter Aleid Wolfsen: 'Er zijn vrijwel geen redenen die het volgen van winkelend publiek of reizigers rechtmatig maakt. Bovendien zijn er minder ingrijpende methoden om hetzelfde doel te bereiken, zonder schending van de privacy.'²³

21 Zenger, R. 'Experimenteren zonder visie is onverantwoord en gokken met onze toekomst'. Bits of Freedom, 18 september 2018. <https://www.bitsoffreedom.nl/2018/09/18/experimenteren-zonder-visie-onverantwoord-en-gokken-met-onze-toekomst/>

22 Hendriks, J. 'Boeven vangen met big data, mag dat?'. Univers, 26 september 2018. <https://universonline.nl/2018/09/26/boeven-vangen-met-big-data-mag-dat>

23 'Bedrijven mogen mensen alleen bij hoge uitzondering met wifitracking volgen'. Autoriteit Persoonsgegevens, 30 november 2018. <https://autoriteitpersoonsgegevens.nl/nl/nieuws/bedrijven-mogen-mensen-alleen-bij-hoge-uitzondering-met-wifitracking-volgen>

Drie dimensies van sensortoepassingen

Bovenstaande twee praktijkvoorbeelden raken aan diverse maatschappelijke vraagstukken over surveillance. Deze vragen hebben betrekking op drie belangrijke dimensies van de sensortoepassingen:

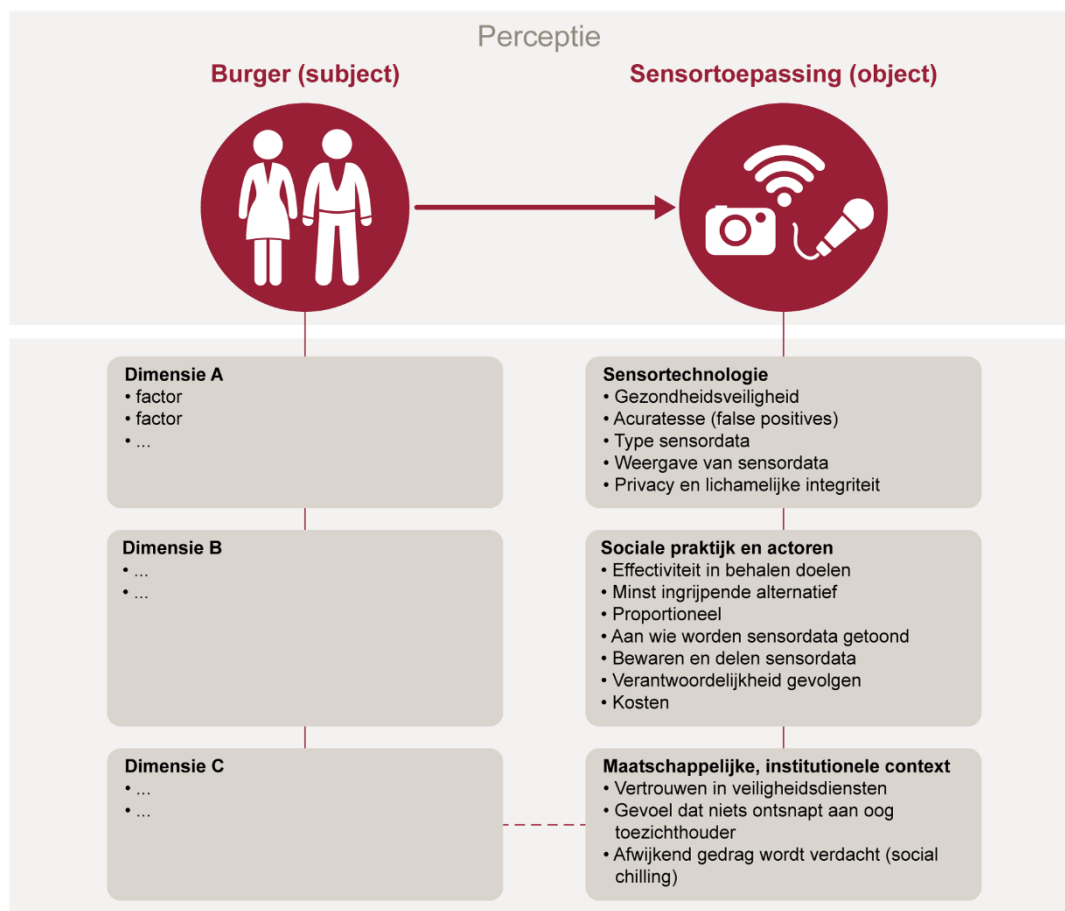
1. de werking van de sensortechnologie;
2. de sociale praktijk waarin de technologie wordt toegepast en de actoren die daarbinnen een rol spelen;
3. de bredere maatschappelijke, culturele en institutionele context waarbinnen de genoemde praktijk is vormgegeven.

Percepties van burgers kunnen over al deze dimensies van een sensortoepassing gaan. De factoren die deze percepties kunnen beïnvloeden dus ook. In figuur 3 hebben we relevante factoren uit de praktijkvoorbeelden opgenomen in het begrippenkader. Zorgen om gezondheidsrisico's van securityscanners, bijvoorbeeld, richten zich op de werking van de technologie zelf. De wens van reizigers om ter plekke te kunnen zien hoe de scanner de data over hun lichaam afbeeldt, gaat over de toepassing in de praktijk van luchthaven Schiphol. Vertrouwen in veiligheidsdiensten gaat over de maatschappelijke en institutionele context waarin de toepassing plaatsvindt. In de praktijk staan de drie dimensies niet los van elkaar. De mate waarin een sensortoepassing inbreuk maakt op de privésfeer van mensen, kan bijvoorbeeld samenhangen met het ontwerp van de technologie zelf, maar ook met de procedures in de specifieke praktijk waarin de technologie wordt gebruikt.

In de tweede dimensie (sociale praktijk) is 'actoren', een verzamelterm voor alle partijen die betrokken zijn bij de sensortoepassing. Dat zijn bijvoorbeeld de persoon of organisatie die sensordata verzamelt, de analist die aan de slag gaat met de resultaten van de computerprogramma's die alle sensordata koppelen en analyseren, de agent op straat of de beveiliging in de winkel die in actie komt. Daarnaast kunnen sensordata worden verzameld over verschillende (groepen) mensen. Bijvoorbeeld iedereen die door een winkelstraat loopt of met de auto langs een ANPR-camera rijdt.

In de besproken praktijkvoorbeelden worden sensordata automatisch verzameld en geanalyseerd door computerprogramma's, maar is er altijd een agent of beveiligingsmedewerker die de informatie bestudeert en een besluit neemt over wat voor actie nodig is. Binnen het systeem van verzamelen, analyseren en toepassen van sensordata speelt de mens dus nog steeds een beslissende rol.

Figuur 3 Inventarisatie van factoren uit praktijkvoorbeelden



Bron: Rathenau Instituut

Verderop in het artikel vullen we het begrippenkader verder in met factoren die betrekking hebben op het subject. Daarvoor kijken we eerst naar Nederlandse studies.

Factoren uit Nederlands onderzoek

Ieder jaar onderzoekt Capgemini hoe burgers in Nederland aankijken tegen ontwikkelingen in het veiligheidsdomein. Uit cijfers van *Trends in veiligheid 2018* blijkt dat 23 procent van de burgers in Nederland zich zeer vertrouwd en veilig voelt met het groeiend aantal camera's in de openbare ruimte, terwijl negen procent het tegenovergestelde zegt te ervaren.²⁴ Capgemini vraagt burgers ook hoe ze staan tegenover het gebruik van sensoren om veiligheid te vergroten. 78% van de ondervraagden staat bijvoorbeeld (zeer) positief tegenover het gebruik van

24 Hoorweg, E. et al. (2018). Vertrouwen en wantrouwen in de digitale samenleving. Trends in veiligheid 2018. Utrecht: Capgemini, p.4. <https://www.capgemini.com/nl-nl/bronnen/visierapport-trends-in-veiligheid-2018/>

bodycams door de politie en zes% (zeer) negatief.²⁵ Het onderzoek geeft geen inzicht in de argumenten en afwegingen achter de meningen van de burgers.

In Nederland is weinig (recent) empirisch wetenschappelijk onderzoek gedaan naar de wensen, zorgen en overwegingen van burgers over het gebruik van sensordata om leefbaarheid en veiligheid te verbeteren. Onderzoek uit de jaren '00 laat zien dat burgers eerder geneigd zijn privacygevoeligere ingrepen toe te staan als het gaat om de oplossing van zware misdrijven, en dat burgers positiever staan tegenover het natrekken van camerabeelden dan het af luisteren van telefoons of huiszoekingen.²⁶ Burgers vinden het ook belangrijk om te weten wat er met hun informatie gebeurt, voor welk doel hun informatie wordt ingezet. Zij hebben meer vertrouwen in de politie dan in particuliere beveiligingsbedrijven.²⁷

Verder komt naar voren dat burgers die meer openstaan voor het delen van informatie, positiever zijn over de inzet van sensoren voor surveillance doeleinden dan burgers die minder geneigd zijn om informatie te delen.²⁸ Ook blijkt uit een onderzoek dat sekse (gender) van invloed kan zijn op percepties: mannen vinden de partij die de sensor inzet (zoals de politie of een beveiligingsbedrijf) vaker belangrijker, terwijl vrouwen meer waarde hechten aan het doel van de opsporing.²⁹ Een factor als effectiviteit van de sensortoepassing komt als nauwelijks relevant naar voren³⁰: burgers wegen de mate van persoonlijke informatie en het doel waarvoor sensordata worden ingezet mee, maar voor de afweging lijkt het minder van belang of het middel ook echt werkt.

Drie persoonlijke dimensies

Bovenstaande studies laten zien dat ook persoonlijke kenmerken (zoals sekse) en algemene houdingen van mensen (zoals openstaan voor het delen van informatie) een rol kunnen spelen bij de afwegingen die mensen maken over sensortoepassingen. Hoe burgers naar een sensortoepassing kijken kan worden beïnvloed door drie belangrijke dimensies van de sensortoepassing, maar ook door persoonlijke dimensies die de 'bril' kleuren waardoor iemand naar een

25 Idem, p.38

26 Koops, E.J. & A. Vedder (2001). *Opsporing versus privacy: de beleving van burgers*. Den Haag: Sdu Uitgevers; Dinev, T. et al. (2005). 'Internet Users, Privacy Concerns and Attitudes towards Government Surveillance - An Exploratory Study of Cross-Cultural Differences between Italy and the United States'. *BLED 2005 Proceedings* 30.

27 Schildmeijer, R., C. Samson & H. Koot (2005). *Burgers en hun privacy: opinie onder burgers*. Amsterdam: TNS NIPO Consult.

28 Dinev, T. et al. (2005). 'Internet Users, Privacy Concerns and Attitudes towards Government Surveillance - An Exploratory Study of Cross-Cultural Differences between Italy and the United States'. *BLED 2005 Proceedings* 30.

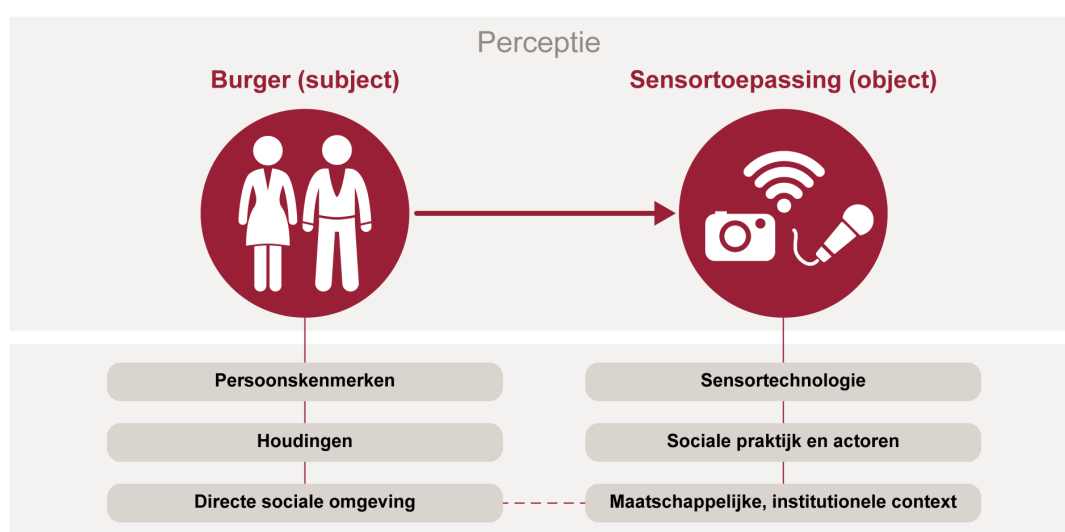
29 Koops, E.J. & A. Vedder (2001). *Opsporing versus privacy: de beleving van burgers*. Den Haag: Sdu Uitgevers.

30 Idem

sensortoepassing kijkt. Figuur 4 illustreert deze dimensies van het subject en object van perceptie.

Daarbij speelt de maatschappelijke, culturele en institutionele context op verschillende manieren een rol. In brede zin kan deze dimensie gaan over wettelijke regels voor cameratoezicht en over een algemeen maatschappelijke vertrouwen of wantrouwen in autoriteiten. Op kleinere schaal worden opvattingen van mensen beïnvloed door hun directe sociale omgeving, zoals de wijk waarin ze wonen en hun werkomgeving.

Figuur 4 Begrippenkader: dimensies van subject en object



Bron: Rathenau Instituut

Factoren uit Europees onderzoek

Internationaal is er wel een aantal actuele studies te vinden over hoe burgers naar sensortoepassingen kijken.³¹ Vanuit het perspectief van ons onderzoek is een beperking van deze studies dat ze sterk focussen op privacy en dat het vaak studies binnen de Amerikaanse context zijn. Met name de Europese studie 'SurPRISE' is interessant voor de vraag die wij onderzoeken. Deze studie biedt een overzicht van factoren die een rol kunnen spelen in de mate waarin burgers een sensortoepassing wel of niet acceptabel vinden.

31 Zie bijvoorbeeld: Potoglou, D. et al. (2017) 'Public preferences for internet surveillance, data retention and privacyenhancing services: Evidence from a pan-European study'. *Computers in Human Behaviour* 75, p.811-825; Rainie, L. M. Duggan. (2016). 'Privacy and information sharing'. <http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/>; Madden, M. L. Rainie. 'Americans' Attitudes About Privacy, Security and Surveillance'. <http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>

SurPRISE in het kort

SurPRISE is een recente en grootschalige studie naar de publieke acceptatie van op surveillance georiënteerde sensortechnologieën.³² Het onderzoek is in negen Europese landen uitgevoerd. In 2012-2015 werd in Denemarken, Duitsland, Hongarije, Italië, Noorwegen, Oostenrijk, Spanje, Verenigd Koninkrijk en Zwitserland de acceptatie van burgers zowel kwantitatief als kwalitatief in kaart gebracht. De onderwerpen waren onder meer: (slimme) camera's, biometrische identificatiemiddelen, drones, *smartphone location tracking* en *deep packet inspection* (een verregerende controle van elektronisch dataverkeer). Tweeduizend burgers (circa tweehonderd per land) werden ondervraagd en namen deel aan participatieve workshops. Op basis van een uitgebreide literatuurstudie komt SurPRISE tot dertig factoren die de percepties van burgers rond surveillance georiënteerde sensortechnologieën mogelijk beïnvloeden.³³ Deze diverse invloedfactoren zijn vervolgens empirisch getoetst.

Factoren die acceptatie van surveillance met sensoren beïnvloeden

Uit het kwalitatieve SurPRISE onderzoek komt naar voren dat zeven factoren, nuances terzijde gelaten, significante invloed hebben op de opvattingen van mensen over sensortechnologieën die voor surveillance worden gebruikt:

- **Algemene houding ten aanzien van technologie:** een positieve houding ten aanzien van de mogelijkheden van technologieën om veiligheid te vergroten, werkt door in een grotere acceptatie van sensortechnologieën. Andersom geldt dat een kritische of sceptische houding de publieke acceptatie hiervan vermindert.
- **Betrouwbaarheid van instituties:** vertrouwen in de betrokken autoriteiten draagt bij aan de publieke acceptatie van sensortechnologieën. Het gebruik van meer acceptabele technologieën helpt veiligheidsinstanties ook om betrouwbaarder over te komen.
- **Sociale 'nabijheid':** zodra de technologieën op specifieke doelgroepen worden gericht, zoals verdachten en criminelen, zijn ze meer acceptabel dan technologieën waarbij de inzet zonder onderscheid des persoons is.
- **Gevoel van inbreuk:** hoe meer mensen het gevoel hebben dat een technologie indringt in het persoonlijke of alledaagse leven, hoe minder aanvaardbaar deze is.
- **Waargenomen effectiviteit:** naarmate mensen er meer van overtuigd zijn dat een sensortechnologie effectief is, wordt deze meer aanvaardbaar.

32 Pavone, V., E. Santiago & S. Degli-Esposti (2015). *SurPRISE. Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe*. <http://surprise-project.eu/wp-content/uploads/2015/02/SurPRISE-D24-Key-Factors-affecting-public-acceptance-and-acceptability-of-SOSTs-c.pdf>

33 Pavone, V., E. Santiago & S. Degli-Esposti (2015). *SurPRISE. Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe*, p.77

- **Substantiële privacyzorgen:** hoe hoger de zorgen over persoonlijke gegevens en (lichamelijke) integriteit, hoe lager de publieke acceptatie.
- **Leeftijd:** oudere mensen zijn meer geneigd sensortechnologieën te accepteren dan jongere mensen.

Voor al deze factoren geldt dat mensen zich niet altijd bewust hoeven te zijn dat deze factoren hun meningen, gevoelens en afwegingen beïnvloeden.³⁴ Uit het onderzoek blijkt dat zeven andere factoren, nuances terzijde gelaten, weinig of indirecte invloed hebben op de publieke acceptatie van sensortechnologieën.³⁵ De onderzoekers vonden dat ‘gevoelens van veiligheidsdreiging’ en ‘de mate van vertrouwdheid met sensortechnologieën’ geen significante invloed hadden. Hetzelfde gold voor ‘inkomen’, ‘opleiding’, de ‘fysieke nabijheid van de technologie’, ‘de verwachting dat de technologie in de toekomst van grote invloed zou zijn’, en de ‘voorstelling dat veiligheid en privacy een uitruil zijn’.

‘Spelregels’ voor surveillance met sensoren

SurPRISE maakt ook inzichtelijk aan welke voorwaarden of ‘spelregels’ volgens burgers moet worden voldaan om een sensortoepassing meer acceptabel te maken.³⁶ Deze spelregels geven aan wat burgers belangrijk vinden bij surveillance met sensoren. In de participatieve sessies binnen SurPRISE hebben burgers criteria en argumenten aangedragen om hun meningen en gevoelens over sensortechnologieën te onderbouwen.³⁷ Burgers vinden de op surveillance georiënteerde sensortechnologieën uit het SurPRISE onderzoek acceptabeler als:

- deze vallen onder een Europees raamwerk van regels en onder de controle van een Europese instantie;
- de uitvoering ervan is ingebed in transparante procedures voor gegevensbescherming en aansprakelijkheid;
- de uitvoering daarvan in handen is van overheidsinstellingen en dat ze alleen voor publieke doelen worden ingezet. Mochten er ook private partijen betrokken zijn, dan moet dit strikt worden gereguleerd;
- de voordelen ervan ruimschoots opwegen tegen de kosten, in het bijzonder in vergelijking met niet-technische alternatieven die minder inbreuk maken;
- de uitvoering te reguleren is via instemming van de betrokkenen (*opt-in approach*);
- betrokken personen toegang hebben tot de data die over hen gaan en de mogelijkheid hebben deze aan te passen of te verwijderen;

34 Idem, p.80

35 Pavone, V., E. Santiago & S. Degli-Esposti (2015). *SurPRISE. Surveillance, Privacy and Security: Final publishable summary report*, p.6

36 Pavone, V., E. Santiago & S. Degli-Esposti (2015). *SurPRISE. Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe*

37 Pavone, V., E. Santiago & S. Degli-Esposti (2015). *SurPRISE. Surveillance, Privacy and Security: Final publishable summary report*, p.7

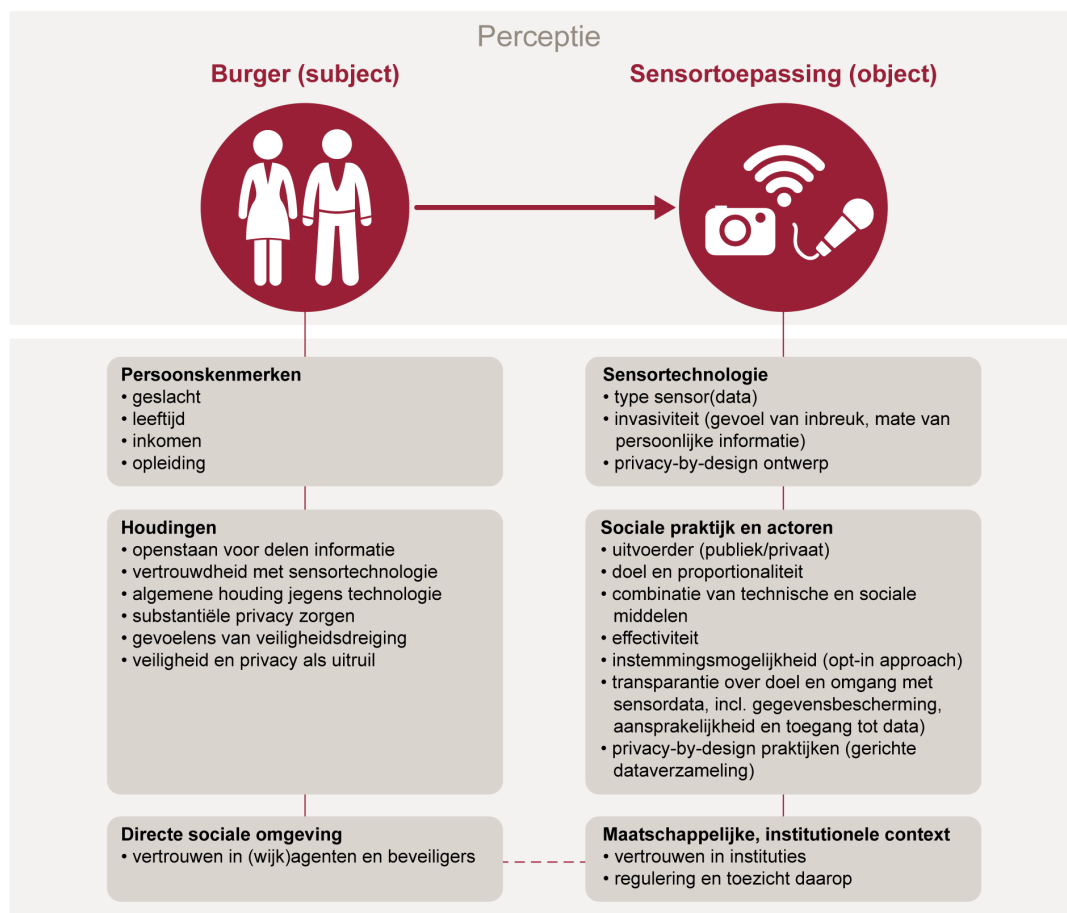
- deze zoveel mogelijk gericht zijn op minder gevoelige data en ruimtes, volgens criteria en doelen die publiekelijk bekend zijn;
- deze niet in alomvattende zin worden ingezet, maar gebonden zijn aan specifieke doelen, tijden en plaatsen;
- deze op basis van *privacy-by-design* zijn ontworpen;
- deze in combinatie met niet-technische maatregelen en sociale strategieën worden ingezet die zich richten op de sociale en economische oorzaken van onveiligheid.

Als we kijken naar ons begrippenkader, dan gaan deze spelregels vooral over de dimensie van praktijken en actoren: de manier waarop sensoren in de praktijk worden toegepast, door wie dat gebeurt en voor welke doelen. Toch stellen burgers ook eisen aan de technologie zelf en de institutionele context. Burgers vinden het belangrijk dat een sensortechnologie zo is ontworpen dat privacyproblemen worden voorkomen, door bijvoorbeeld de gegevensopslag te minimaliseren, te kiezen voor anonimiseren en alle informatie te beveiligen met encryptie. '*Privacy by design*'-principes kunnen onderdeel uitmaken van de procedures rond het gebruik van sensortechnologie, zoals de afspraak om zo min mogelijk mensen toegang te geven tot de gegevens. Burgers vinden tevens de bredere institutionele context belangrijk: voldoen aan het raamwerk van Europese regels en het toezicht daarop. Dit veronderstelt ook een vertrouwen van burgers dat de Europese regels de juiste zijn en dat het toezicht daarop goed plaatsvindt. Deze regels worden in praktijk weer vertaald naar een specifieke sociale context.

Inventarisatie van factoren uit wetenschappelijke studies

We hebben de factoren uit de Nederlandse studies en het Europese SurPRISE-onderzoek geordend in ons begrippenkader. Figuur 4 geeft een overzicht van factoren uit wetenschappelijk onderzoek die mogelijk de perceptie van burgers van surveillance met sensoren beïnvloeden.

Figuur 5 Inventarisatie van factoren uit wetenschappelijke literatuur



Bron: Rathenau Instituut

Reflectie op andere vormen van sensortoezicht

We hebben in dit artikel een begrippenkader ontwikkeld waarmee we inzicht bieden in de manier waarop mensen tot een oordeel komen over (de aanvaardbaarheid van) de toepassing van sensortechnologie om leefbaarheid en veiligheid te verbeteren. Er zijn drie persoonlijke dimensies en drie dimensies van sensortoepassingen die een rol kunnen spelen in hun afwegingen. Op basis van praktijkvoorbeelden en wetenschappelijk onderzoek naar de percepties van burgers hebben we ook andere factoren gevonden die mogelijk een rol spelen bij wat mensen vinden van surveillance met sensoren. Die factoren kunnen geplaatst worden binnen het ontwikkelde begrippenkader. Ze ondersteunen daarmee dat kader en geven er invulling aan. Hoewel dit kader is ontwikkeld door *surveillance* te bestuderen, is het ook een zinvol raamwerk om naar de percepties van andere vormen van sensortoezicht (*sousveillance*, *horizontale surveillance* en *zelf-surveillance*) te kijken. We bespreken hier kort een aantal relevante

overeenkomsten en verschillen tussen de vormen van sensortoezicht. Hierbij nemen we de drie dimensies van sensortoepassingen als uitgangspunt.

Sensortechnologie

Bij diverse vormen van toezicht met sensoren is de technologie veelal hetzelfde. Videocamera's kunnen bijvoorbeeld worden ingezet voor surveillance (CCTV), sousveillance (camera's op mobiele telefoons) en horizontale surveillance (beveiligingscamera's bij de voordeur). Er zijn ook verschillen. De politie kan bijvoorbeeld gebruik maken van andere type sensortechnologieën dan burgers.

Sociale praktijk en actoren

In de dimensie 'sociale praktijk en actoren' zitten belangrijke verschillen tussen vormen van sensortoezicht. Bij *surveillance* worden burgers met camera's en andere sensoren in de gaten gehouden door overheidsinstanties en bedrijven. We hebben in eerdere studies gezien dat het voor mensen uit kan maken wie precies de sensordata verzamelen en gebruiken. Worden persoonlijke gegevens gebruikt door publieke of private partijen, en voor publieke of voor commerciële doelen? Aan welke regels zijn deze partijen gebonden?

Bij *sousveillance* gebeurt er iets interessants. Hier wordt de 'kijkrichting' van het gebruik van sensoren namelijk omgedraaid: burgers hanteren zelf de camera om toezicht te houden op overheidsinstanties en bedrijven. Bijvoorbeeld bij het filmen van politieagenten of hulpdiensten die aan het werk zijn. In het geval van *horizontale surveillance* verandert de kijkrichting van het gebruik van sensoren ook. Bij horizontale surveillance kunnen burgers namelijk gefilmd worden door andere burgers én zelf andere burgers filmen. Bij *zelf-surveillance* gebruiken mensen sensoren om zichzelf te monitoren en te controleren (zie figuur 2).

Deze verschillende kijkrichtingen veranderen niet alleen de uitvoerder (wie de sensordata verzamelt en gebruikt), maar ook over wie de sensordata worden verzameld. En er liggen andere doelen en motivaties aan ten grondslag om persoonlijke gegevens te verzamelen. Volgens het SurPRISE-onderzoek zijn dit allemaal factoren die kunnen beïnvloeden of burgers een sensortoepassing wel of niet aanvaardbaar vinden.

Maatschappelijke, culturele en institutionele context

Bij surveillance gaat het om vertrouwen in bijvoorbeeld de politie of bedrijven. Bij horizontale surveillance en sousveillance gaat het om vertrouwen in medeburgers, ook met betrekking tot de vraag of ze zich aan bijvoorbeeld privacywetgeving houden. Daarbij geldt dat de politie en gemeenten aan andere regels zijn gebonden dan bedrijven en burgers.

Tot slot: handvatten voor de focusgroepen

In de focusgroepen willen we diverse opvattingen en afwegingen verzamelen. Dat doen we door aan kleine groepen gewone Nederlanders scenario's voor te leggen waarin sensoren en sensordata worden gebruikt om leefbaarheid en veiligheid te verbeteren. In welke mate vinden gewone Nederlanders deze sensortoepassingen aanvaardbaar, en waarom? Wanneer verwachten burgers dat sensoren worden gebruikt om leefbaarheid en veiligheid te verbeteren? Welke redenen, ervaringen en gevoelens zitten achter hun meningen? Welke voordelen en nadelen zien mensen? We willen dat er in de focusgroepen zoveel mogelijk aspecten met betrekking tot de percepties van gewone Nederlanders worden besproken. Op basis van ons begrippenkader en de inventarisatie van mogelijke factoren, formuleren we twee handvatten die ons helpen bij het vormgeven van de focusgroepen. Deze handvatten verwijzen naar de twee centrale uitgangspunten van ons begrippenkader: iemand (het subject) heeft een mening over iets (het object). Bij de perceptie van mensen spelen zodoende zowel eigenschappen van de betreffende persoon als van de sensortoepassing een rol:

- Zorg voor diversiteit in de groep en heb oog voor het individu**
 Wij zijn geïnteresseerd in 'percepties van burgers'. Dat klinkt abstract, maar het gaat in de kern om meningen en ervaringen van gewone Nederlanders 'van vlees en bloed'. We hebben gezien dat persoonskenmerken, algemene houdingen en de directe sociale omgeving van mensen invloed kunnen hebben op hoe iemand naar sensortoepassingen kijkt. Factoren als leeftijd, sekse, opleiding en de buurt waarin iemand woont kunnen een rol spelen. Dit zijn aspecten waar we bij het werven van een diverse groep deelnemers rekening mee kunnen houden. Daarnaast kan het zinvol zijn om meer zicht te krijgen op de houdingen van mensen voordat we met ze gaan praten over specifieke sensortoepassingen, bijvoorbeeld of iemand in het algemeen vertrouwen heeft in de politie.
- Vraag deelnemers naar de belangrijke dimensies van sensortoepassingen**
 We zorgen voor diversiteit in de scenario's door variaties te maken binnen de drie belangrijke dimensies van sensortoepassingen. Percepties van burgers kunnen immers gaan over de sensortechnologie die wordt gebruikt, de specifieke praktijk en partijen die daarbinnen een rol spelen, en de maatschappelijke, culturele en institutionele context. Speelt het voor iemand mee wat voor type sensordata worden verzameld? Maakt het uit of de data worden verzameld door de politie of private beveiligingsbedrijven? Maakt het uit over wie de data worden verzameld? In hoeverre speelt vertrouwen van mensen in de wijkagent of in de politie als instituut een rol? En welke rol speelt 'gefilmd worden' en 'zelf filmen' in de mate waarin mensen een sensortoepassing aanvaardbaar vinden?

Met deze handvatten werken we de aanpak voor de focusgroepen uit. De politie kan deze handvatten ook gebruiken bij het voeren van gesprekken binnen en buiten de organisatie over het maatschappelijk verantwoord gebruik van sensoren en sensordata.

Het volgende artikel gaat in op de scenario's en vragen die we aan burgers in de focusgroepen willen voorleggen. Een onderwerp waar we in dit artikel nog niet bij hebben stilgestaan is *kennis*. In de praktijk hebben mensen vaak geen zicht op alle details van alle dimensies van een sensortoepassing. In de scenario's kunnen we deelnemers gericht informatie geven over een situatie en kijken wat het effect daarvan is op hun verwachtingen van het gebruik van sensordata en op de mate waarin ze de toepassing wel of niet aanvaardbaar vinden. Daarover meer in het volgende artikel.

Het Rathenau Instituut stimuleert de publieke en politieke meningsvorming over de maatschappelijke aspecten van wetenschap en technologie. We doen onderzoek en organiseren het debat over wetenschap, innovatie en nieuwe technologieën.

Rathenau Instituut