Veiligheid en privacy in de smart city

Uitkomsten van het onderzoeksproject 'Managing Privacy in the Smart City'

CENTRE FOR BOLD CITIES

URBAN BIG DATA ROTTERDAM

Universiteit Leiden The Netherlands

TU Delft Delft University of Technology

Erasmus University Rotterdam

Veiligheid en privacy in de smart city

Auteurs
Vivien Butot, Freek de Haan, Liesbet van Zoonen, Gabriele Jacobs, Petra Saskia Bayerl en Luuk Schokker

Productie en ontwerp
Leiden-Delft-Erasmus Centre for BOLD Cities

Veiligheid en privacy in de smart city

Uitkomsten van het onderzoeksproject
'Managing Privacy in the Smart City'

Inleiding

Hoe ga je om met veiligheid en privacy in de smart city?

Hoe ga je om met veiligheid en privacy in de 'smart city'? Als steden slimme digitale technologieën zoals beveiligingscamera's, telefoontracking of gezichtsherkenning inzetten om de veiligheid van burgers te vergroten, wat vinden die burgers daar dan van? Welke kansen zien ze en welke zorgen hebben ze; hoe komt privacy daarin naar voren?

In het project Managing Privacy in the Smart City van de Erasmus Universiteit Rotterdam en de Gemeente Rotterdam hebben we deze vragen onderzocht; het gaat om de gevolgen van het zogenaamde 'datagedreven veiligheidsbeleid' voor privacy.

Achtergrond van het onderzoek

Steden zijn steeds meer bezig met het inzetten van moderne technologieën. In een 'smart city' worden digitale technologie en grote datasets gebruikt om bijvoorbeeld mobiliteit en duurzaamheid te verbeteren, maar ook om veiligheid en leefbaarheid te vergroten. Dat laatste doel verdient meer aandacht omdat zowel het

> Het vraagstuk over stedelijke veiligheid in de smart city is vaak nog onderbelicht

In ons onderzoek analyseerden we drie hedendaagse digitale veiligheidstoepassingen en keken we naar toekomstverwachtingen van burgers op dit gebied. De belangrijkste uitkomsten van het onderzoek wijzen op de noodzaak van bredere bewustwording en grotere transparantie over slimme stedelijke veiligheidstechnologie; van intensiever debat over wat stedelijke veiligheid eigenlijk betekent; en van open, democratisch ontwerp van slimme veiligheidstechnologie.

wetenschappelijk onderzoek als het publieke debat over smart cities het vraagstuk van stedelijke veiligheid nog vaak onderbelicht laat[1]. Dat is opmerkelijk, omdat stedelijke veiligheid in het algemeen een controversieel onderwerp is, waarover maatschappelijke groeperingen en politieke partijen zeer uiteenlopende opvattingen hebben.

Centrale begrippen in het onderzoek

Smart city	De slimme stad of smart city is een plek waar een grote verscheidenheid aan informatietechnologie en data wordt gebruikt om het leven in de stad te monitoren en verbeteren.
Veiligheid	In dit onderzoek richten we ons op de veiligheid van de openbare ruimte: straten, parken, pleinen, etc.
Privacy	In dit onderzoek verwijst privacy naar: 1) de controle van burgers over hun eigen zichtbaarheid in de openbare ruimte, 2) persoonlijke gegevens, 3) de analyse en het gebruik van gegevens over personen in de stedelijke publieke ruimte.

Veiligheidsdebatten worden ook vaak in heftige en verwijtende termen gevoerd[2]: de ene groep voelt zich bedreigd, de andere gestigmatiseerd, een derde vreest de uitdijende macht van de staat.

De betekenis van digitale veiligheids-technologieën en de steeds uitgebreidere inzet van data is in die gesprekken nog maar mondjesmaat aanwezig. Maar hoe meer gegevens een stad verzamelt en hoe meer activiteiten van burgers in de openbare ruimte ter wille van de veiligheid 'gedataficeerd' kunnen worden, hoe meer vragen er ontstaan over de privacy en de positie van burgers in de stad. Die vragen ontstaan niet alleen bij burgers zelf, maar ook bij beleidsmakers en uitvoerders die verantwoordelijk zijn voor digitale technologie, data en veiligheid. Over dat soort vragen gaat ons onderzoek.

We bespreken eerst op basis van interviews en observaties het huidige gebruik en de aanwezige privacydilemma's bij drie hedendaagse Rotterdamse toepassingen voor, respectievelijk, burgers (*WhatsApp-buurtpreventie*), handhavers (*Digitale Assistent Spitter*) en beleidsmakers (*Dataplattegrond*). In het tweede deel van ons onderzoek duiken we in de toekomstmogelijkheden van deze technologieën en vragen we burgers welke mogelijkheden ze zien en welke zorgen ze hebben. Op basis van de gecombineerde resultaten formuleren we in het derde deel aanbevelingen voor gemeenten die digitale technologie en data voor de stedelijke veiligheid inzetten.

1: Actualiteit

Veiligheids-technologieën voor burgers, handhavers en bestuurders

In Rotterdam bestaan diverse digitale veiligheidstoepassingen, die elk als doel hebben om de openbare orde en veiligheid in de wijken te optimaliseren. We spraken met burgers, handhavers en beleidsambtenaren die deze toepassingen gebruiken over de mogelijkheden en de risico's die ze bij deze toepassingen zien. Daarnaast keken we mee met het gebruik van die toepassingen in de praktijk om na te gaan hoe ze daadwerkelijk gebruikt worden. Het gaat om *WhatsApp-buurtpreventie* voor burgers, *Spitter* voor handhavers en de *Dataplattegrond* voor beleidsmakers.

Voor burgers: WhatsApp-buurtpreventie

WhatsApp-buurtpreventiegroepen zijn een digitale variant op vroegere burgerpatrouilles. In deze chatgroepen, die in Rotterdamse buurten veel voorkomen, informeren buurtbewoners elkaar en politie of handhavers over verdachte situaties in hun wijk. (Wijk)agenten zijn vaak lid van de groepen. De WhatsApp-buurtpreventiegroepen worden door veel gemeenten aangemoedigd en worden inmiddels gezien als volwaardige burgerinitiatieven.

De preventiegroepen bestaan vaak naast gewone 'buurt-apps', waarin over veel meer onderwerpen wordt gesproken. Het is in WhatsApp-buurtpreventiegroepen de bedoeling dat er uitsluitend berichten over veiligheidskwesties worden verstuurd, vaak volgens het specifieke SAAR-protocol (waarbij de letters SAAR staan voor *signaleren, alarmeren, appen, reageren*). De strenge regels rondom het naleven van zo'n protocol blijken continu voor discussie binnen de groep zorgen, met name over de vraag of men zich wel aan de regels houdt. Daar is een duidelijke rol voor de moderator weggelegd die kan zorgen dat deze toepassing optimaal functioneert. Bij goed gebruik zijn burgers dan de ogen en oren van de handhavers. Ze kunnen via de groep snel en efficiënt hun observaties noteren en delen, zeker als het protocol goed wordt nageleefd.

Er zijn duidelijke privacyrisico's te vinden bij het gebruik van WhatsApp-buurtpreventiegroepen, zoals gebruikers zelf ook aangeven.

WhatsApp-buurtpreventiegroepen worden inmiddels gezien als volwaardige burgerinitiatieven

"Iedereen staat er nog wat schichtig tegenover in verband met de privacy. Van de wet op de privacy word je helemaal gek. Als je iets wil, dan krijg je gelijk: 'maar privacy.'" (Moderator van een Whatsapp-buurtpreventiegroep)

Het is moeilijk te voorkomen dat er persoonsgegevens, zoals signalementen en foto's van verdachte personen, worden gedeeld in de groepen. Een goede, verantwoordelijke moderator kan dit in de hand houden en materiaal verwijderen dat niet in de groep gedeeld hoort te worden. Maar dat is nog geen garantie: de maker van de beelden heeft deze immers op haar/zijn eigen telefoon staan.

Ook kan het voorkomen dat privacygevoelig materiaal per ongeluk naar een verkeerde groep wordt doorgestuurd, zoals een algemene buurtgroep. Zo maakten we mee dat een agent per ongeluk een foto van een verdacht busje deelde in een Whatsapp-buurtpreventiegroep, terwijl die foto bedoeld was voor collega-agenten, niet voor burgers.

Volgens het SAAR-protocol moet een melding '112-waardig' zijn. In de praktijk is dat niet altijd het geval, en ook dat zorgt voor privacyrisico's. Groepsleden delen regelmatig onnodige of overdreven verdacht-makingen, die discriminerend van aard kunnen zijn. Vaak worden foto's of video's gemaakt en gedeeld op basis van heel algemene kenmerken of observaties. Daarbij is er een serieus risico dat deelnemers voor eigen rechter gaan spelen.

"Men denkt te snel dat hij politie, handhaver of beveiliger is. Je bent alleen maar de ogen en de oren van de buurt. Je kijkt, je ziet en je meldt. Dat is het enige. Je moet ook hoofdzakelijk naar de buitenruimte kijken." (Moderator van een WhatsApp-buurtpreventiegroep)

Als de buurtpreventiegroep te ijverig te werk gaat kan de publieke ruimte overdreven veel worden gecontroleerd. Niet-crimineel gedrag, zoals rondhangen, kan dan als verdacht worden aangemerkt en uitgebannen, waarmee de vrije rol van de publieke omgeving wordt ingeperkt.

Figuur 1: Fragment uit een melding in een WhatsApp-buurtpreventiegroep

Figuur 2: Een handhaver noteert zijn observaties in de Spitter-app

Voor handhavers: Spitter

Spitter is een soort digitaal notitieboekje dat dienst doet als 'surveillance-assistent'. De app wordt gedeeld door straathandhavers en andere medewerkers van de gemeente. Via Spitter kunnen zij snel hun observaties delen. Daarnaast werkt de app als archief voor de gedeelde observaties.

Spitter was op het moment van ons onderzoek in Rotterdam (midden 2019) alleen nog in gebruik bij jeugdhandhavers, maar in principe zou de app gebruikt kunnen worden door elke gemeenteambtenaar. Mede daarom is afgesproken om geen persoonsgegevens te registreren in de app.

> *"Mijn einddroom is dat niet alleen mensen van stadsbeheer, of mensen van team ondermijning, of mensen van directie veiligheid dat ding op hun telefoon hebben staan, maar ook mensen van woningtoezicht, ook sociale inspecteurs, ook mensen van het sociale wijkteam. En dat die allemaal met elkaar, met name in het wijkgerichte werken, van elkaar weten dat ze bezig zijn en wat ze doen."* (*Stadsmarinier NPRZ/Ondermijning*)

Omdat de observaties binnen Spitter in een archief worden opgeslagen en worden voorzien van een locatietag, leveren de verzamelde observaties ook algemenere data over wijken op die door een gemeente geanalyseerd kunnen worden. Jeugdhandhavers doen met Spitter in feite niets anders dan wat zij al deden met een portofoon en notitieboekje. Ze zijn aanwezig in de wijk, spreken jongeren aan, en waarschuwen, beboeten of arresteren hen als dat nodig is. Het belangrijkste verschil: de informatie van alle collega's is nu altijd en overal toegankelijk.

Evenals WhatsApp-buurtpreventie is Spitter niet vrij van risico's. Ondanks de afspraak om geen persoonsgegevens te registreren in de app, gebeurt dit af en toe toch. Zo kunnen er per ongeluk persoonsgegevens in de registratie sluipen of worden de gegevens buiten Spitter om gedeeld, bijvoorbeeld via WhatsApp.

Figuur 3: Voorbeeld van een melding in de Spitter-app

Figuur 4: Observaties tijdens een surveillance op deze locatie werden geregistreerd in de Spitter-app

Maar er is ook een ander risico: als persoonskenmerken niet worden genoteerd, registreren gebruikers vaker groepskenmerken die niet ter zake doen. Er ontstaan zo onnodig etnisch gekleurde profielen. Er hoeven echter helemaal geen fysieke signalementen in de app te belanden om nuttige observaties te doen, zoals onderstaande melding laat zien:

> *"Tijdens onze surveillance troffen wij ongeveer 22 jongeren aan. Wij zagen dat zij met zeven voertuigen waren. Het waren zowel jongens en meiden. Wij gingen met de jongeren in gesprek. Zij gaven aan snel te gaan vertrekken. De bedoeling was om hier snel elkaar te ontmoeten en vervolgens weer verder te gaan. Na enkele minuten vertrokken de groep jongeren in de diverse voertuigen."* (*Spitter-registratie*)

Daarnaast zagen we ook dat gebruikers situaties registreren die geen overlast geven. Op die manier komen ook jongeren die feitelijk niets verkeerd doen in de observaties en het archief terecht. Dat kan vervelende gevolgen hebben: mensen die (onterecht) intensief gesurveilleerd worden, kunnen zich in het ergste geval gaan gedragen als doelwit, of ze kunnen uit voorzorg bepaalde gebieden of handhavers gaan mijden[3]. Omdat deze gedragingen óók weer geregistreerd kunnen worden, kan een onnodige vicieuze cirkel ontstaan.

Als persoons-kenmerken niet worden genoteerd, registreren gebruikers vaker groepskenmerken die niet ter zake doen

Voor beleidsmakers: Dataplattegrond

De Dataplattegrond is een zogenaamd digitaal dashboard waarmee beleidsmedewerkers snel en flexibel veiligheidsanalyses van buurten kunnen maken. Elke gebruiker van de Dataplattegrond kan gegevens over buurten 'over elkaar leggen'. Op die manier kan een beleidsmaker een lokale situatie analyseren en bijdragen aan maatwerk voor een wijkgerichte aanpak. Het is goed om hier te benoemen dat de Dataplattegrond nog in ontwikkeling is. Er zijn dus weinig concrete voorbeelden van hoe de tool wordt gebruikt. Wel hebben we in dit onderzoek uitgebreid gesproken met initiatiefnemers en betrokkenen. Zo hebben we een goed idee gekregen van het beoogde gebruik.

"Deze cijfers geven aan, eventjes grofweg gezegd: het zit in heel de wijk, overal gebeurt wat. Dus dat is jammer, want dan kan je niet heel erg met scherp schieten. Dus ik ging op zoek naar andere cijfers. [...] *Uiteindelijk heb ik ook deze kaart erbij gepakt, dit zijn heatmaps, vlekkenkaarten, die op een nauwkeurigheid van 50x50 meter aangeven hoe de mensen geantwoord hebben op die grootschalige enquête. Dit is goud waard. De enquête kan je geografisch scherper maken* [...] *Ja, de hele wijk heeft aandacht nodig. Maar als we echt met scherp willen schieten moeten we in die hoek zijn. Dat is geweldig."* (*Stadsmarinier Informatiegestuurd werken*)

De Dataplattegrond is bedoeld om up-to-date en locatiegebonden data te verschaffen over zaken als criminaliteit en overlastmeldingen. Deze informatie wordt in het dashboard gevisualiseerd. Omdat verschillende informatie-bronnen gecombineerd worden, kunnen beleidsmedewerkers met de Dataplattegrond samenhang tussen problemen inzichtelijk maken. Dat kan leiden tot suggesties voor aandachtsgebieden in het (veiligheids-)beleid. Ook kunnen gemeenteprofessionals zodoende beter samenwerken, zowel op beleids- als uitvoeringsniveau. Hierbij kun je denken aan het gezamenlijk ontwikkelen en uitvoeren van surveillance- en handhavingsstrategieën.

Er is goed nagedacht over wanneer het wenselijk is om persoonsgegevens te gebruiken, maar toch kleven er privacyrisico's aan het dashboard

Bij de ontwikkeling van de Dataplattegrond is goed nagedacht over of/wanneer het wenselijk is om in het dashboard persoonsgegevens weer te geven. Dat is ook te merken aan hoe betrokkenen over het (beoogde) gebruik spreken. Desondanks gaat ook de Dataplattegrond gepaard met privacyrisico's.

"Kijk, ik heb een postcode 6, dat klinkt als redelijk geaggregeerd. Alleen, ja, hoe ga je nou ermee om als je maar twee adressen op zo'n postcode hebt." (*Projectmanager Dataplattegrond*)

"Als je gegevens op elkaar legt [...], *en je hebt een persoon met een rollator, en een uitkering, en nog iets, dat je eigenlijk...* [*dat*] *degenen in de wijk dan wel weten wie dat is."* (*Externe consultant Dataplattegrond*)

Daarnaast zijn de redenen voor het wel of niet gebruiken van specifieke indicatoren voor veiligheid in de Dataplattegrond niet openbaar, terwijl indicatoren nooit neutrale gegevens zijn, maar altijd een bepaalde visie op de werkelijkheid inhouden. Zo werd 'welvaart' vroeger uitsluitend economisch gedefinieerd op basis van het Bruto Nationaal Product. Nieuwe maatschappelijke inzichten hebben ertoe geleid dat tegenwoordig ook ecologische en sociale indicatoren meegerekend worden. Een indicator is wat dat betreft net een foto: sommige dingen staan erop, andere niet. Juist daarom is het zaak om zo transparant mogelijk te zijn over de indicatoren die in de Dataplattegrond wel en niet gebruikt worden en de manier waarop ze met elkaar gecombineerd worden. Anders wordt het een algoritmische 'blackbox' waar geen mogelijkheid voor gesprek, oordeel of verzet in zit.

De Dataplattegrond kan daarnaast de relatie tussen burger en ambtenaar veranderen. De 'harde data' van het systeem kunnen aanleiding vormen voor ongerichte fouilleeracties of huisbezoeken. Net als in de Spitter-app geldt ook hier dat een sterke aandacht op specifieke gebieden of groepen tot een vorm van tunnelvisie kan leiden; de focus op deze plekken of groepen leidt tot meer meldingen, waardoor er meer aandacht aan wordt gegeven, die weer tot meer meldingen kan leiden, enzovoort.

We constateren op basis van onze gesprekken en observaties dat veel gebruikers van deze drie technologieën kanttekeningen plaatsen over hun risico's, vooral over privacy en, in mindere mate, over verkeerd gebruik. Maar veel meer hebben ze grote verwachtingen over het nut van deze apps en de hoop dat ze op grotere schaal en met grotere impact uitgerold kunnen worden. De technologische verleiding rond deze apps is veel sterker dan de zorgen over mogelijke risico's.

Figuur 5: Weergave van hoe de Dataplattegrond op een tablet zou kunnen functioneren (bron: dcmr.nl)

2: Toekomst

Hoe denken burgers over nieuwe mogelijkheden?

Buiten de in het vorige hoofdstuk besproken WhatsApp-buurtpreventie-groepen zijn de meeste stads-bewoners niet bekend met de veiligheidstechnologieën die hun stad gebruikt. Om in het onderzoek een goed gesprek met hen te kunnen voeren, niet alleen over de huidige situatie maar ook over toekomstige ontwikkelingen, is het dus allereerst nodig om dit goed uit te leggen. In dit onderzoek hebben we daarom een aantal kleine toekomstscenario's gemaakt (zogenaamde 'vignetten') waarin nieuwe gedigitaliseerde en gedataficeerde veiligheids-technologieën werden voorgesteld.

We legden deze vignetten aan een diverse groep van 31 Rotterdammers voor en gingen met hen over de scenario's in gesprek. We vonden onze onderzoeksdeelnemers onder andere via de Erasmus Academie voor een Leven Lang Leren, via wijknetwerkers van de gemeente en via buurtorganisatie Dock. We hebben in de rekrutering specifiek gelet op een spreiding in leeftijd en herkomstbuurten in de stad; uiteindelijk hebben we daarbij wel relatief veel hogeropgeleiden gesproken[4].

De gesprekken hebben we opgenomen en geanalyseerd. Hierbij zochten we vooral naar terug-kerende onderwerpen en woord-combinaties. Vanuit die onderwerpen en combinaties reconstrueerden we vijf zogenaamde 'repertoires': samenhangende verzamelingen van kennis en ideeën waaruit mensen putten om hun eigen mening over veiligheidstechnologieën te formuleren.

De meeste bewoners zijn nauwelijks bekend met de veiligheids-technologieën in hun stad

De analogie met een orkest is hier verhelderend: op basis van het repertoire 'jazz' kunnen steeds verschillende uitvoeringen worden gegeven. Belangrijker nog is dat verschillende repertoires in één uitvoering kunnen worden gecombineerd. Datzelfde geldt voor de repertoires over de smart city.

In het vervolg van dit hoofdstuk laten we per repertoire in meer detail zien op welke kennis en ideeën het is gebaseerd. Het is daarbij belangrijk om in de gaten te houden dat onze gespreksdeelnemers in de regel verschillende repertoires combineerden om tot hun individuele oordeel over de vignetten te komen. Zo gebruikten ze bijvoorbeeld

De vijf repertoires

Systeemkenmerken	Kennis (of gebrek daaraan) van het digitale technieken in de smart city.
Pragmatiek	Beschrijvingen van de opkomst van computertechnologieën en de acceptatie of onvermijdelijkheid ervan.
Nut	Overpeinzingen over het nut en de waarde van smart city-technologie.
Risico's	Zorgen over de gevaren van digitale technologieen voor het gebied van privacy, veiligheid en rechtvaardigheid in de stad.
Burgerschap	Bespreking van de eigen rol, en algemene rechten en verantwoordelijkheden in de smart city.

systeemkenmerken in combinatie met nut om een concreet toekomstscenario te beoordelen. Of wezen ze op de risico's van de nieuwe veiligheidstechnologieen om te pleiten voor meer controle en transparantie. Met dat laatste putten ze dan uit het repertoire van de verantwoordelijke burger. We bespreken de afzonderlijke repertoires en laten aan de hand van voorbeelden uit onze gesprekken zien hoe onze deelnemers voor hun een concrete beoordeling van een specifiek toekomstscenario verschillende repertoires combineerden.

Systeemkenmerken

> ***"De computer doet alles op, ja, basis van cijfers of iets wat er is ingevoerd. Die kunnen misschien wel*** [...] ***een bepaalde afwijking d'r uit halen, maar, ja, als het gaat*** [...] ***automaten die auto's flitsen, dan is het heel duidelijk: het is goed of fout, want als je door rood rijdt dan ben je gewoon fout bezig, dan is het heel duidelijk om dat te digitaliseren*** [...]. ***Maar ik denk dat*** [...] ***het wat lastiger kan zijn bij andere soorten onderwerpen of andere soorten problemen."*** [*vrouw, 22 jaar oud*]

Als onze onderzoeksdeelnemers over systeemkenmerken praten, gaat het meestal over de manier waarop gegevens verzameld kunnen worden, en hoe systemen goede beslissingen kunnen nemen. Ze maken vaak onderscheid tussen duidelijke en onduidelijke manieren om gegevens te verzamelen en analyseren.

Zoals het gespreksfragment hierboven laat zien, vinden ze ook dat systemen soms te ingewikkelde beslissingen moeten nemen. Ze betwijfelen of dat wel goed kan en vinden wat er nu aan technologie en data gebruikt wordt weinig doorzichtig. Toch geven deelnemers soms ook aan dat transparantie en het geven van een stem aan burgers tijdens de ontwerpfase van systemen tot meer acceptatie zou kunnen leiden. We zien hier dat het repertoire van burgerschap ook gebruikt wordt om over systeemkenmerken te praten.

Onze gesprekspartners ervaren echter een algemeen gebrek aan transparantie.[5] Ze hebben bovendien het gevoel te weinig van de systemen in de slimme stad te weten om er goed over mee te kunnen praten. Dit gesprek over kennisachterstand en onduidelijke systemen voerden we met al onze deelnemers en daarom concluderen we dat systeemkenmerken een basisrepertoire is dat in alle oordeelsvorming terugkomt.

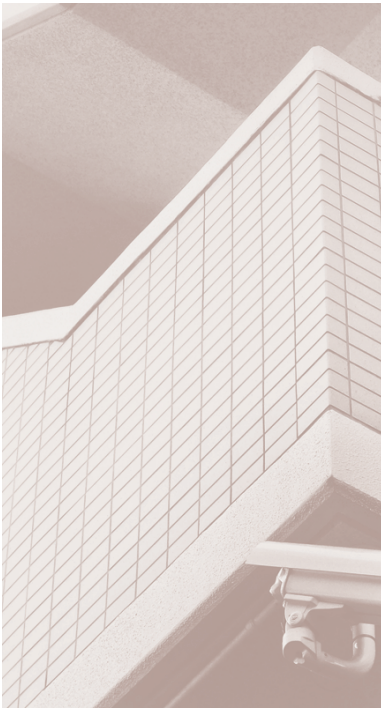
Pragmatiek

> *" [...] ik bedoel ik ben zélden pragmatisch, maar in dit soort dingen denk ik pragmatisch na. Je weet toch nooit hoe de toekomst verder loopt, en je hebt je altíjd aangepast [...] Ik bedoel... een mens gaat altijd overleven, dus je gaat je aanpassen, en je probeert slim te zijn. Nou, zo doe ik het ook altijd. Dus ik denk van, ik réd me wel [...] in wat voor systeem dan ook, ik réd me wel."* [*man, 72 jaar oud*]

Onder pragmatiek vallen reacties van deelnemers waarin de opkomst en het gebruik van digitale technologieën staan. Het gaat dan vooral om de manier waarop dat soort technologieen en toepassingen in het dagelijks leven opgenomen worden. In de wetenschappelijke literatuur staat dat verschijnsel bekend als 'domesticatie'; de technologie wordt 'getemd' en binnen het erf van de eigenaars gebracht[6].

Dat is niet altijd een heel actief proces; sommige digitale technologieën zoals de smartphone zijn zonder veel ophef het dagelijks leven in geslopen. Het gesprek over de nieuwe veiligheidstechnologieën van de slimme stad, wordt soms op dezelfde manier gevoerd. Wat nu nog vreemd of onacceptabel lijkt, is morgen gewoon geworden; daar valt niet echt aan te ontkomen, dat gaat toch wel gebeuren.

Er spreekt uit het pragmatisch repertoire een gevoel van machteloosheid tegenover de technologische ontwikkelingen en dat gaat gepaard met termen als 'groei' en 'aanpassing'.



Figuur 6: Voorbeeld van een surveilla

Noch het burgerschapsrepertoire, noch het risicorepertoire sluit hier makkelijk bij aan, omdat er een zekere mate van gelatenheid in de pragmatiek zit. Zowel de slechte kanten van de technologie, als de mogelijkheid om bij te sturen worden genegeerd ten faveure van de pragmatische en weinig vergende aanpassing.[7]

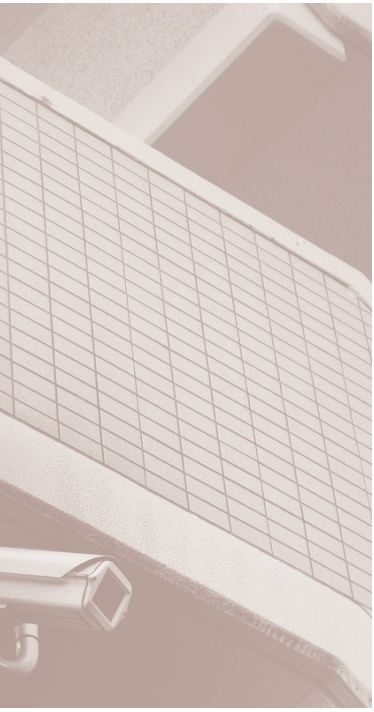
Nut

"Je kan natuurlijk zo'n hele stad min of meer beheersen [...] ***ik bedoel straks ook het hele grote vraagstuk van klimaatbeheersing, wat ga je nou doen met koude en warmte? Dat je dat veel meer zou kunnen volgen, zou kunnen uitwisselen.*** [...] ***Ik denk zelfs dat het hele klimaatbeheersing, dat het ons moet gaan redden daarin."*** [*vrouw, 66 jaar oud*]

Onze gesprekken gingen ook vaak over de voordelen van smart city-technologie. Onze deelnemers overwegen de informatieve en communicatieve mogelijkheden van technologie, en de efficiëntie die de smart city kan opleveren voor de organisatie van hun stad. Vaak zien ze ook grote voordelen van de technologie voor hun eigen leven en gemak in de stad. Ze illustreren hun gedachten dan ook vaak met voorbeelden uit hun werkende leven.

Wanneer het maatschappelijk belang van deze technologieën aan de orde komt, zoals in het citaat hierboven, spreken deelnemers eerder in termen van noodzaak dan van gemak. Het nuttigheidsrepertoire maakt een zeker optimisme en hoop over de smart city mogelijk. Sommige deelnemers speculeerden daarom enthousiast verder en verkenden bijvoorbeeld het idee van cameratoezicht met software die de goede en kwade intenties van mensen kan onderscheiden en daarmee kan bepalen wie toegang krijgt tot publieke gebouwen.

Andere deelnemers putten echter uit het risico- en burgerschapsrepertoire door het nut van de technologieën tegenover de inbreuk op privacy af te wegen, en de manier waarop burgers controle over de nieuwe technologieën kunnen krijgen te bespreken.



surveillancecamera in de binnenstad

"Dan heb je dus altijd vooraf data nodig van allerlei mensen, of je verzamelt heel veel data van mensen, gaandeweg dat systeem. En dat is mijn vraag wel, van, hoe veilig blijft dat, voor de persoon?"

(Deelnemer over de risico's van digitale technologieën)

Risico's

> ***"Maar dan heb je dus altijd of al vooraf data nodig van allerlei mensen, of je verzamelt heel veel data van mensen, gaandeweg dat systeem. En dat is mijn vraag wel, van, hoe veilig blijft dat, voor de persoon an sich? He, zoals ik denk aan Big Brother is Watching You, hoe ver gaan wij dan, dat is een beetje mijn vraag."*** [*vrouw, 66 jaar oud*]

In het 'risicorepertoire' draait het om implicaties van de slimme stad op het gebied van privacy, veiligheid en rechtvaardigheid. De bezorgdheid van onze gesprekspartners komt op drie manieren naar voren. Allereerst gaat het vaak over de surveillance in de slimme stad. Zoals in het citaat naar voren komt, grijpen mensen vaak terug op bekende populaire beelden, in het bijzonder 'Big Brother' (uit het boek *1984* van George Orwell).

Ten tweede hebben mensen het vaak over privacy. Hier onderscheiden we twee soorten privacy. In het eerste geval praten mensen dan over datalekken en -misbruiken die in de media zijn uitgelicht en doelen ze op zaken als wetgeving en regulering. In het tweede geval gaat het meer over een gevoel van ongemak over de aanwezigheid van eigen, persoonlijke gegevens in digitale systemen.

Tot slot uiten deelnemers vaak de zorg dat de riskante gevolgen van veiligheidsmanagement in de slimme

stad vaak vooral zouden voorkomen in bepaalde wijken of bij bepaalde minderheden. Tegelijkertijd verloopt het gesprek over deze zorgen vaak in termen van "aan de ene kant, aan de andere kant". Bijvoorbeeld: aan de ene kant is het nuttig om dit soort technologieen te hebben (nut-repertoire), maar aan de andere kant loop je het risico dat je privacy verliest of groepen stigmatiseert. Of: we raken wel heel veel gegevens kwijt aan de stad of gemeente, maar ja daar moeten we mee leren leven (pragmatiekrepertoire).

Burgerschap

Naar aanleiding van een vignet over het automatisch registreren van je alcoholpromillage wanneer je in de auto stapt, zegt een van onze respondenten:

> *"*[...] *wat je nu zegt* [*die techniek*], ***daar zouden we dan mee worden opgevoed*** [...] ***Ik heb een kleindochter, die is 20, en die heeft haar rijbewijs en*** [...] ***laatst*** [...] ***zit ze daar, en ze drinkt niks. Ze zegt núl procent mag ik drinken, núl procent! En dat zegt ze heel overtuigd*** [...] ***En dan is het iets van, ze doet het uit zichzelf, ze vindt het ook*** [...] ***ze stemt ermee in En zij hoeft ook zo een ding niet te hebben want ze zou altijd glansrijk slagen.***" [*vrouw, 76 jaar oud*]

Zoals de uitspraak van onze deelnemer laat zien, komt in onze gesprekken ook de persoonlijke verantwoordelijkheid van burgers naar voren. Men zegt bijvoorbeeld dat je zelf onveilige plekken en situaties moet vermijden. Maar je moet elkaar ook in de gaten houden, en daarmee claimen onze gespreksdeelnemers gezamenlijke verantwoordelijkheid. Dergelijk goed individueel en collectief burgerschap is in sterk contrast met het schrikbeeld van onze respondenten dat de smart city burgers in de positie van marionetten manoeuvreert, die alleen reageren op technologische sturing. Zo zou hun autonomie en vrijheid ondermijnd worden. Tegelijkertijd geven deelnemers ook aan dat je niet van iedereen kan verwachten dat ze zich ten behoeve van hun eigen en andermans veiligheid verantwoordelijk gedragen. In die gevallen kunnen de nieuwe veiligheidstechnologieën toch hun nut hebben, vinden ze; maar hoe en wanneer die keuze dan gemaakt moet worden, blijft in het midden.

Reflectie op de gesprekken

Onze deelnemers gebruikten de verschillende repertoires vaak in combinatie met elkaar om te reageren op een specifiek toekomstbeeld. Onze gesprekken maakten ook duidelijk dat mensen zoeken naar hun oordeel over de nieuwe veiligheidstechnologieën en permanente afweging maken tussen nut en risico's, tussen bedreigingen en kansen, tussen eigen verantwoordelijkheid en technologische sturing. Een vaststaand en blijvend oordeel heeft nog vrijwel niemand, al is het gevoel dat er weinig te doen is tegen deze nieuwe technologieën wel wijdverbreid.

3: Conclusies en aanbevelingen

Welke stappen kunnen gemeenten zetten?

In ons onderzoek zochten we naar beleidsrelevante inzichten over veiligheid en privacy in de smart city aan de hand van belangrijke hedendaagse toepassingen van digitale veiligheidstechnologieën en een aantal toekomstscenario's. We ontdekten dat burgers, handhavers en beleidsambtenaren nog veel vragen hebben over hoe deze technologieën precies werken, en op welke manier ze privacy en sociale verhoudingen beïnvloeden. Daarnaast hoorden we in ons onderzoek zowel van handhavers, als van burgers en beleidsmakers dat veel technologische ontwikkelingen gepaard gaan met ongewenste effecten voor bijvoorbeeld surveillance en privacy.

Hun verwachtingen en gevoelens over de nieuwe technologieën lijken echter tegenovergesteld. Diverse handhavers en beleidsambtenaren spreken met verlangen over alle mogelijkheden die deze technologieën bieden voor monitoring en controle. Iemand vindt het jammer dat we nog niet kunnen 'scherpschieten' met de data omdat ze te algemeen zijn; een ander vindt de privacywetgeving een sta-in-de-weg om tot betere resultaten te komen; een derde wil graag dat de veiligheidsdata door het gehele ambtelijk apparaat gebruikt gaan worden. Voor deze mensen betekenen de nieuwe veiligheidstechnologieën een uitbreiding van hun handelingsruimte en een potentiële vereenvoudiging en efficiëntieslag van hun werk.

Uit de gesprekken met de burgers bleek het tegenovergestelde; zij voelen zich vaak machteloos tegenover technologische ontwikkelingen en verkiezen op het gebied van veiligheid de eigen verantwoordelijkheid van mensen vaak boven digitale beheersing. Tegelijkertijd hebben ze het gevoel dat deze "niet te vermijden" zijn. Sommigen koppelden daar een somber toekomstbeeld aan vast, over een smart city die indruist tegen huidige publieke waarden. Dergelijk defaitisme en pessimisme illustreren een gevoel van machteloosheid en een gebrek aan handelingsperspectief.

Diverse handhavers en ambtenaren spreken met verlangen over de mogelijkheden van technologie; burgers voelen zich vaak machteloos tegenover de ontwikkelingen

Wat betekenen deze resultaten voor burgers, bestuurders en veiligheidsorganisaties van de smart city? Wat kunnen steden doen om op het snijvlak van technologie, veiligheid en privacy te werken naar een werkelijk slimme, of liever gezegd *wijze* toekomst voor onze steden? Wat zijn de handelingsperspectieven van de diverse partijen? En bij wie liggen de grootste verantwoordelijkheden?

We identificeren de noodzaak tot transparantie, bewustzijn en inspraak of co-creatie. Dat lijkt voor de hand te liggen, maar is in het veiligheidsdomein lang niet vanzelfsprekend. Om het veiligheidsdomein hangt een waas van geheimzinnigheid die sommige actoren wenselijk vinden omdat dit de effectiviteit ten goede zou komen. Specifiek is het inderdaad zo dat sommige meldingen anoniem gedaan moeten kunnen worden, en soms zijn geheime operaties bij zware criminaliteit of maatschappelijke bedreiging noodzakelijk. Maar als het gaat om de beheersing van individueel en collectief gedrag in de openbare ruimte, waar dit onderzoek in het bijzonder over gaat, dan is er voldoende reden om bewustzijn, transparantie en co-creatie ook voor de veiligheidstechnologieën in de slimme stad te laten gelden.

Transparantie

Hoewel burgers in onze gesprekken soms sceptisch tegenover digitale technologie en data staan, is hun weerstand zelden definitief. Meer transparantie over wie, wat, hoe, waarom van nieuwe veiligheidstechnologieën zou een positief effect kunnen hebben: waar en door wie worden veiligheidstechnologieën gebruikt; wat wordt er precies gemonitord en gecontroleerd; wat gebeurt er met de verzamelde gegevens, van wie zijn ze en kan je er inzage in krijgen; waarom is het eigenlijk nodig om de stad op deze digitale en gedataficeerde manier veiliger te maken? Het gesprek over dergelijke vragen zal de bewustwording over deze technologieën vereenvoudigen; over wat je niet weet of niet ziet, kun je immers moeilijk een mening vormen.

Bewustwording

Als we het hebben over bewustwording, is er nog veel winst te behalen. Wanneer gemeenten en veiligheidsorganisaties (politie, stadstoezichthouders) digitale en data-innovaties ontwikkelen, dienen burgers om te beginnen actief geïnformeerd te worden. Burgers blijken namelijk sterke gevoelens over het onderwerp hebben. Deelnemers aan ons onderzoek bleken dankbaar dat

Stadsbewoners hebben sterke gevoelens over digitale veiligheids-technologieën en leggen doorgaans de verbinding met hun eigen leefomgeving

ze over sociale en technologische kwesties konden praten en legden daarbij doorgaans de verbinding met hun directe leefomgeving. De inhoud van dergelijke gesprekken is van waarde voor de gemeente en publieke veiligheidsinstanties, die de last dragen om democratische legitimiteit voor haar beleid te waarborgen. Voor burgers zijn dergelijke reflecties van belang omdat ze hun kennis vergroten en leiden tot de datawijsheid die nodig is om inspraak te hebben in, en mee te doen aan het ontwerp van veiligheidstechnologieën voor de openbare ruimte[8].

Inspraak en co-creatie

Wij adviseren ten slotte dat burgers ook daadwerkelijk betrokken worden via een duurzame vorm van inspraak in het veiligheidsbeleid en de flankerende technologieën in de stad. Daar zijn inmiddels buiten het veiligheidsbeleid talloze voorbeelden van in de vorm van burgerpanels, buurtplatforms of bewonersbudgetten.

Het gaat dan niet alleen over de efficiëntie van de techniek, maar juist over de fundamentele aspecten, zoals de vraag wat veiligheid is, hoe het werkt, en welke stedelingen de meeste last kunnen hebben van mogelijke technologische instrumenten. Alleen zo komen deze discussies tot de kern van wat burgers belangrijk vinden.

Hierbij moet erkend worden dat een roep om meer veiligheid niet altijd geïnterpreteerd moet worden als een roep om meer technologische oplossingen[9]. Veel deelnemers aan dit onderzoek gaven namelijk te kennen dat de stad niet altijd veilig is, maar dat zij de voorkeur geven aan meer eigen en collectieve verantwoordelijkheid, niet aan technologische oplossingen.

4: Colofon en noten

Colofon

Dit onderzoek is voorgesteld en uitgevoerd door onderzoekers van het Centre of Excellence in Public Safety Management (CESAM) van de Erasmus Universiteit Rotterdam, met hulp en ondersteuning van het Leiden-Delft-Erasmus Centre for BOLD Cities en de Kenniswerkplaats Urban Big Data van de Erasmus Universiteit en de gemeente Rotterdam.

Freek de Haan is postdoctoraal onderzoeker aan de Erasmus Universiteit en verbonden aan CESAM en het Centre for BOLD Cities. Hij houdt zich bezig met stedelijk beleid op het gebied van de smart city.

Vivien Butot is promovendus aan de Erasmus Universiteit en verbonden aan CESAM en het Centre for BOLD Cities. In zijn onderzoek richt hij zich op de verbinding tussen smart city-ontwikkelingen en privacykwesties.

Liesbet van Zoonen is wetenschappelijk directeur van het Centre for BOLD Cities. Haar huidige onderzoek betreft de privacy van burgers in smart cities en de diverse gevoeligheden die hierbij een rol spelen. Van Zoonen is medeoprichter van de Kenniswerkplaats Urban Big Data in Rotterdam.

Gabriele Jacobs is decaan van het Erasmus University College en werkte voorheen als wetenschappelijk directeur van CESAM.

Petra Saskia Bayerl is hoogleraar digitale communicatie en veiligheid aan Sheffield Hallam University (Verenigd Koninkrijk). Voorheen werkte Bayerl aan de Erasmus Universiteit en was zij verbonden aan CESAM.

Luuk Schokker is programmacoördinator van het Leiden-Delft-Erasmus Centre for BOLD Cities. In die rol houdt hij zich o.a. bezig met het vertalen van het onderzoek naar maatschappelijke programma's, activiteiten en samenwerkingen.

Noten

1. de Haan, F. & Butot, V. (2020) *Finding safety in the Smart City: A discourse analysis with strategic implications,* in *International Security Management - New Solutions to Complexity.* Basel: Springer.

2. Huysmans, J. (2014). *Security Unbound: Enacting Democratic Limits.* Abingdon: Routledge.

3. Een uitgebreidere bespreking van deze effecten ('labelling' en 'chilling') is te vinden in bijvoorbeeld: Bernburg, J. G. (2009) *Labeling Theory. in Handbook on Crime and Deviance* (eds. Krohn, M. D., Lizotte, A. J. & Hall, G. P.) 187–207 (Springer, 2009) en Penney, J. W. (2016) *Chilling Effects: Online Surveillance and Wikipedia Use.* Berkeley Technological Law Journal. 31, 117–182.

4. Zie voor meer informatie over de opzet van deze interviews het eindrapport van dit onderzoek. Het eindrapport is op te vragen via het LDE Centre for BOLD Cities of bij onderzoeker Vivien Butot (butot@essb.eur.nl).

5. Jameson, S., Richter, C. & Taylor, L. (2019) *People's strategies for perceived surveillance in Amsterdam Smart City*. Urban Geography 40, 1467–1484.

6. Berker, T., Hartmann, M., Punie, Y. & Ward, K (2006). *Domestication of media and technology*. Londen: Open University Press.

7. Morozov, E. *To save everything click here: Technology, solutionism and the urge to fix problems that don't exist.* Londen: Penguin.

8. Meer over het betrekken van burgers en het vergroten van databewustzijn is te lezen in de publiekspublicatie *Jouw buurt, jouw data: Uitkomsten van de onderzoeksgame over kennis, houding en gedrag van burgers in de slimme stad* (2019) van collega's van het LDE Centre for BOLD Cities.

9. Pavone, V., Ball, K., Degli Esposti, S., Dibb, S. & Santiago-Gómez, E (2018). *Beyond the security paradox: Ten criteria for a socially informed security policy.* Public Understanding of Science Journal 27, 638–654.

Hoe ga je om met veiligheid en privacy in de 'smart city'? Als steden slimme digitale technologieën zoals beveiligingscamera's, telefoontracking of gezichtsherkenning inzetten om de veiligheid van burgers te vergroten, wat vinden die burgers daar dan van? Welke kansen zien ze en welke zorgen hebben ze; hoe komt privacy daarin naar voren?

In het project *Managing Privacy in the Smart City* hebben we deze vragen onderzocht; het gaat om de gevolgen van het zogenaamde 'datagedreven veiligheidsbeleid' voor privacy in de stad. We keken hierbij naar zowel bestaande technologieën als mogelijke toepassingen in de toekomst.

CENTRE FOR BOLD CITIES

URBAN BIG DATA ROTTERDAM

Universiteit Leiden The Netherlands

TU Delft Delft University of Technology

Erasmus University Rotterdam