TEKST: TSEARD ZOETHOUT

Privacy in de slimme stad

De slimme stad heeft ons veel gebracht. Burgers kunnen sneller een parkeerplaats vinden of gepersonaliseerde aanbiedingen van bedrijven krijgen en de overheid brengt eenvoudiger verkeersstromen of emissies in kaart. Aan zoveel technologie zit wel een keerzijde: privacy komt in het gedrang. Waar, wanneer en hoe worden burgers gecontroleerd en wat zijn daarvan de risico's? Een virtuele tocht door smart Amsterdam.

Maria Genova pikt me op bij Utrecht Centraal. De journalist en spreker heeft een dozijn boeken op haar naam staan, waaronder het succesvolle boek over identiteitsfraude, getiteld *Komt een vrouw bij de h@cker*. In haar elektrische Hyundai Kona rijden we naar Amsterdam om bij te praten met een ict-expert en een juridisch adviseur. Is onze privacy nog wel goed geregeld in de publieke ruimte: daarover willen we het gaan hebben.

Als we de ring rond Amsterdam binnenrijden, leggen niet alleen diverse verkeerscamera's maar ook milieuzonecamera's het kenteken van Genova's Hyundai vast. De stad heeft die laatste maatregel genomen om oude dieselauto's uit het centrum te kunnen weren. 'Goede zaak', zegt Genova lachend. Zij heeft sinds kort een elektrische auto en kan zonder problemen doorrijden. Camera's langs de hoofd- en snelwegen verbeteren de doorstroming van het autoverkeer van, naar en binnen Amsterdam. Volgens de richtlijn van de Wet Bescherming Persoonsgegevens mogen zulke gegevens niet langer dan 28 dagen worden bewaard.

Pinpas

'Als er geen overtreding of ongeluk heeft plaatsgevonden is de noodzaak om die data zo lang te bewaren, niet aanwezig', stelt ict-specialist Matthijs Pontier. 'In februari dit jaar is gebleken dat de politie onrechtmatig toegang tot de milieuzonecamera's kreeg om van misdaden verdachte personen op te sporen. Je zou die data ook direct kunnen wissen op het moment dat de auto de milieuzone in mag.'

De website van Park & Ride geeft aan dat parkeerplaatsen in Zuid vol staan, stelt Genova vast terwijl ze bij knooppunt Amstel de Ringweg A10 pakt. 'Toch fijn dat die digitale mogelijkheden er zijn, anders hadden we uren moeten zoeken naar een parkeerplaats', zegt ze dan vrolijk. We besluiten om door te rijden naar de Prins Hendrikkade, vlakbij het Scheepvaartmuseum. Dat ligt niet alleen centraler maar er zijn ook voldoende laadpalen.

Wat zou er qua privacy zijn gebeurd als we toch een overdekte plek hadden gevonden? Pontier antwoordt: 'Je betaalt met je pinpas en voert je kenteken in. Die gegevens mogen 48 uur worden bewaard. Zo val je als persoon te traceren. Het kan anders. In plaats van dat je op je kenteken reserveert, zou je per parkeervak kunnen betalen, en voor jou of voor iemand anders inboeken. Dat waarborgt anonimiteit. Helaas wordt het in Amsterdam steeds moeilijker om cash af te rekenen.'

De lampen van de Hyundai lichten op: met haar sleutel heeft Genova de auto afgesloten. 'Een moderne auto is niets anders dan een computer op wielen. Dat heeft

FOTO: DEPOSITPHOTOS

FOTO: DEPOSITPHOTOS

voordelen bij remmen, passeren en parkeren. Waar ik minder blij van word, is dat de meeste moderne auto's simpel zijn te stelen door het signaal van de sleutel te onderscheppen. Dat geeft problemen bij de verzekering.'

Via de Gelderse Kade lopen we naar de Nieuwmarkt. Tussen vertrek en aankomst zetten gemeentelijke scanauto's geparkeerde voertuigen op film, zo ook Genova's Hyundai. Met scanauto's wordt gecontroleerd wie er fout staat geparkeerd. Parkeerwachten kunnen overtreders op die wijze eenvoudig en snel beboeten. Dat moet de doorstroming in de steeds drukkere stad bevorderen.

Trackers en beacons

Op de hoek van de Nieuwmarkt en de Keizerstraat komen we aan op onze bestemming, café Fonteyn. Op het terras zit Pontier, die veelvuldig over privacy en de slimme stad publiceert, zowel in wetenschappelijke tijdschriften als in publieksbladen en op websites, en voor de Piratenpartij heeft hij zitting in het waterschap Amstel, Gooi en Vechtstreek. Op zijn laptop laat hij twee kaarten zien waarop de locatie van veel slimme apparaten staat aangegeven: camera's van de gemeente, sensoren, wifi-trackers en beacons. Wifi-trackers worden ingezet voor het volgen van grote groepen mensen, met beacons hengelen commerciële partijen via het bluetooth-signaal van de smartphone de locatiegegevens en het tijdstip van voorbijgangers en winkelbezoekers binnen.

Plotseling ontvang ik een push-bericht: een winkel in de buurt vraagt me toestemming om gepersonaliseerde aanbiedingen te doen. Van schrik zet ik mijn smartphone uit. 'Die winkel is nog transparant', reageert Pontier lachend. 'Die vraagt om je toestemming. Bij het merendeel is onduidelijk of men je volgt of niet. Het is al voorgekomen dat een winkel, met behulp van *beacons*, zijn prijskaartjes heeft aangepast toen men in de gaten kreeg dat op een bepaalde plek mensen meer of minder kochten. Dat is verboden. Eigenlijk zou een bedrijf expliciet toestemming moeten vragen om potentiële klanten op deze manier te volgen.'

'Overheid en bedrijven kunnen dankzij trackers en beacons precies zien welke route een individu neemt', gaat hij door. 'Weliswaar wordt het unieke identificatieadres van je smartphone versleuteld opgeslagen en dagelijks gewist, maar door data te koppelen aan andere ict-systemen valt toch te herleiden van wie de smartphone is. Eens in de acht dagen heeft Amsterdam een datalek en meer dan eens per dag een beveiligingsincident, bijvoorbeeld als iemand ongeautoriseerd meekijkt.'

Een alternatief zou volgens de ict-expert een tel- of een warmtecamera zijn: dat levert namelijk geen ▶

privacyproblemen op. ‘Overigens,’ en hij wijst op de eerste kaart op zijn laptop, ‘is dit kaartje onvolledig. Hier, in het centrum, staat bijvoorbeeld niet aangegeven waar camera’s hangen, alleen een indicatie van het gebied.’

Genova kijkt op. Aan de rand van de Nieuwmarkt verstoort een groepje dronken mannen de vrijdag. Agenten met bodycams zetten iedereen op film, ook toevallige passanten. Pontier: ‘Volgens officiële cijfers beschikt de politie landelijk nu over circa tweeduizend bodycams, privé-camera’s van de agenten niet meegerekend. Er zijn al voorbeelden bekend waarin die films worden gemanipuleerd, bijvoorbeeld door de camera op gezette momenten aan of uit te zetten waardoor de context verdwijnt. Passanten die niets met het incident te maken hebben, kunnen op die wijze worden gearresteerd. Een dergelijke vorm van profileren is echter bij wet verboden.’

> ‘Ethische hackers drongen al door tot de bedienkamers van waterwerken.’

Openbaar vervoer

We staan op, rekenen af en nemen metrolijn 51 naar de Zuidas, het zakendistrict. Een camera legt ons weer vast. Genova wijst ernaar, Pontier vervolgt al lopend zijn verhaal: ‘De publieke perceptie is dat camera’s bijdragen aan veiligheid. Eén camera kost al snel veertigduizend euro, terwijl uit onderzoek blijkt dat ze niet effectief zijn. Met andere woorden: er is geen verschil in het aantal geregistreerde misdaden tussen plekken met of zonder camera. Slimme burgers hebben al snel door waar die camera’s zich bevinden en gaan dan buiten het bereik staan. Beter is om te investeren in recherche of agenten op straat die bij calamiteiten direct kunnen ingrijpen.’

Genova plaatst er wel een kanttekening bij. ‘Negen van de tien keer is een agent te laat ter plekke en is de dader gevlogen. Een camera kan heel wat jaren blijven hangen. Bovendien worden die steeds slimmer, bijvoorbeeld door gericht agressie te registreren. Dan kunnen agenten ook sneller ter plekke zijn als een camera zoiets oppikt.’

Kon je bovengronds de gemeentelijke camera’s ontwijken, in de metro is dat uitgesloten. Pontier, Genova en ik checken in met onze persoonlijke ov-chipkaart. Andere mogelijkheden zijn er niet. Of wel? De anonieme 1-rit-kaartjes zijn bijna twee keer zo duur. Dat hebben we er niet voor over. Bovendien, een chipkaart gaat sneller. Translink Systems, eigenaar van de ov-chipkaart, houdt onze persoonsgegevens intussen wel anderhalf jaar vast, met mogelijke aantasting van privacy.

Terwijl we op de metro wachten, vertelt Pontier over gezichtsherkenning. ‘De stad Amsterdam doet dat niet, maar Rotterdam voert al wel experimenten uit met gezichtsherkenning in het openbaar vervoer. Dat levert een stevige discussie op omdat zoiets op gespannen voet met privacy staat. Niet zonder reden heeft San Francisco een totaalverbod op gezichtsherkenning ingevoerd.’ Bij station Spaklerweg zegt hij ons gedag. Volgens afspraak zullen we hem later terugzien bij Waternet aan de Amstel.

FOTO: DEPOSITPHOTOS

Gegevensbescherming

Een advocatenkantoor bij de Zuidas: bij de receptie zijn Genova en ik verplicht ons te registreren. En daar beginnen de privacyproblemen al: volgens de Algemene Verordening Gegevensbescherming (AVG), van kracht sinds 2018, dienen onze persoonsgegevens op zodanige wijze te worden verwerkt dat die ‘rechtmatig, behoorlijk en transparant’ is. Verder moet er een wettelijke grondslag tot opslag van onze persoonsgegevens zijn, bijvoorbeeld via toestemming, overeenkomst, wettelijke plicht of gerechtvaardigd belang. Omdat we geen werknemer van het kantoor zijn, valt een overeenkomst als juridische grondslag af. Wettelijke plicht is er niet, gerechtvaardigd belang valt te betwijfelen en bovendien hoe lang worden de lijsten bewaard? Er is een recht op vergeten.

‘In feite zou er een bordje moeten staan dat jullie ook toestemming voor opslag van persoonsgegevens verlenen, inclusief van eventuele camerabeelden, en hoe lang jullie gegevens worden opgeslagen’, zegt Ben Baldwin, zelfstandig juridisch adviseur voor bedrijven. Regelmatig komt hij hier nog op het advocatenkantoor, zijn vroegere werkplek. Als *certified information privacy manager* ziet hij de huidige ontwikkelingen met lede ogen aan. ‘Bedrijven en overheden komen pas in actie als het te laat is. Voldoen aan de AVG kost alleen geld en levert niets op.’

‘Elke overheid is verplicht een functionaris gegevensbescherming aan te stellen die onafhankelijk handelt en direct aan het hoogste orgaan binnen die overheid rapporteert’, vertelt hij. ‘In het geval van Amsterdam is dat de burgemeester. Onafhankelijkheid vereist wel senioriteit, een zekere rijpheid om ook onwelgevallige zaken naar voren te brengen. Wat je nu ziet, is dat veel functionarissen relatief jong en laag betaald zijn, en dat ze die functies met andere taken moeten combineren.’

Democratische controle

Hoewel Amsterdam zorgvuldig met de uitbesteding van slimme diensten omgaat, kan het niet anders dan dat de stad met een handvol partijen – multinationale technondernemingen, vooral uit de VS – zaken doet die de uitvoering vervolgens aan een groot aantal onderaannemers overlaten. De controlerende instantie is de Autoriteit Persoonsgegevens (AP). Daar treden de verschillen goed aan het licht: een onderbemande AP met onvoldoende kennis versus goedbetaalde ict-professionals.

‘*Smart cities* zijn stedelijke gebieden die met technologie oplossingen vinden voor bijvoorbeeld mobiliteit, energie, veiligheid of huisvesting. Gemeenten zoeken in toenemende mate naar datagedreven oplossingen. Daarbij gaat het vaak om verwerking van persoonsgegevens. Ze willen bewoners bewegen tot betere keuzes, de openbare ruimte optimaliseren en die inrichten volgens inzichten uit de verzamelde data (…). Wij juichen innovatief gebruik van data voor meerwaarde in de openbare ruimte toe, mits de privacy van burgers voldoende is gewaarborgd.’

‘Nee, dat zeg ik niet, maar zo staat het op de website van de Autoriteit Persoonsgegevens, in een vrij recent bericht over de ontwikkeling van slimme steden’, vervolgt Baldwin. ‘Het bestuur gaat er blijkbaar van uit dat slimme systemen de stad veiliger, efficiënter en democratischer maken.’ Op dat statement valt het nodige af te dingen. Het is sterk technologisch gedreven. “‘Bewoners bewegen tot betere keuzes” is politiek bedrijven met big data: wie bepaalt wat goed is? Waar blijft de democratische controle? Ook wordt met geen woord over bewaartermijnen gerept, noch wie toegang tot die slimme systemen heeft.’

Op de site van de gemeente Amsterdam staan alle camera’s, sensoren en beacons in de openbare ruimte aangegeven.
ILLUSTRATIE: GEMEENTE AMSTERDAM

Volgens de privacyjurist is dat vragen om problemen. ‘De waarborg tegen lakse leveranciers, misbruik en mogelijke schadeclaims is een zo goed mogelijk doordacht contract. Helaas schort het hier vaak aan doordat vrijwel alleen naar de koppeling van data wordt gekeken zonder voldoende inzicht in de systemen zelf te hebben. In plaats van sterk op efficiëntie in te zetten, zou de overheid de burger centraal kunnen stellen middels *privacy by design* en dataminimalisatie, bijvoorbeeld door de gemeenten een eigen cloud te laten opzetten die zowel fysiek (gebouw en locatie) als digitaal veilig is.’

Vitale infrastructuur

Na anderhalf uur verlaten we het gebouw zodat we, net op tijd, Pontier nog een keer kunnen spreken. Per sms laat hij ons weten dat de locatie niet Waternet wordt maar café Dauphine, vlakbij het Amstelstation.

‘Vorig najaar hebben hackers het internetnetwerk van de Universiteit Maastricht platgelegd’, zegt Pontier. ‘Een succesvolle digitale aanval op Medisch Centrum Leeuwarden is dit voorjaar ternauwernood voorkomen. Hetzelfde kan gebeuren bij onze waterinfrastructuur die op afstand wordt geregeld. Een klein deel is volgens de Rekenkamer onvoldoende beveiligd. Ethische hackers hebben al toegang gekregen tot de bedienkamer van de waterwerken. Als kwaadwillenden via hacking de sluizen van de Hollandse Waterkering kunnen openen, is niet alleen Leiden in last maar stroomt ook het zuidelijk deel van de Randstad onder.’

Waar de datacenters voor water en energie zijn gelokaliseerd, wil hij niet zeggen. Wel is duidelijk dat veel datacenters zich beneden het maaiveld bevinden. Het is de meest sprekende aansporing om slimme netwerken niet langer aan elkaar te koppelen maar juist te ontkoppelen, niet alleen in het belang van onze veiligheid maar ook – en vooral – om onze privacy beter te borgen. ●