Welke privacyvraagstukken bestaan er bij slimme cameratoepassingen? Er is meer dan alleen gegegevensbescherming. Het raakt ook ons gedrag. Een interview met Dr. Rianne Dekker van de Universiteit van Utrecht.

Kansen Pakken en Verantwoordelijkheid Tonen

"Sensing is het digitaal waarnemen of verzamelen van informatie met betrekking tot een object of persoon met een technisch hulpmiddel (de sensor), met de intentie tot opvolging." Sensingtoepassingen zijn niet meer weg te denken uit ons dagelijks leven. Je auto zit er vol mee, je telefoon heeft meer sensoren dan je zou verwachten en probeer maar eens naar je werk te gaan zonder ergens door een sensor te zijn opgemerkt. Sensingtoepassingen vergemakkelijken taken, waardoor werk ook verschuift of verandert. Dat geldt ook voor het werk van de politie.

Vanwege de rol van het programma komen we regelmatig in aanraking met gevallen waar nog niet duidelijk is hoe we die kansen en de daarbij behorende zorgvuldigheid nu beide moeten invullen. Daar leren we van.

Ik zal voor deze nieuwsbrief regelmatig een casus uitwerken, niet met de bedoeling om volledig te zijn, wel om u deelgenoot te maken van de afwegingen waarmee ook u te maken gaat krijgen.

Niet alleen vanuit de politie wordt aandacht besteed aan deze onderwerpen, ook de Tweede Kamer buigt zich over de vraag op welke wijze zij hun rol moeten spelen in een snel digitaliserende samenleving. Dr. Rianne Dekker van de Universiteit van Utrecht werd gevraagd hierover te adviseren. Wij kwamen met haar in gesprek omdat zij hierin ook de ervaringen van de politie met sensingtoepassingen wilde betrekken.

Ook zij ontdekte in dit proces verwonderpunten. We hebben haar gevraagd zo'n verwonderpunt voor deze community toe te lichten, en zijn zeer vereerd dat ze daartoe bereid is.

Dit verwonderpunt gaat over het verschil tussen informationele privacy en gedragsmatige privacy. Ik denk dat dit onderscheid helpt om de dialoog rond privacy, het grondrecht op eerbiediging van de persoonlijke levenssfeer, op een meer volledige wijze te voeren. Ik denk ook dat het ons helpt om juist onze aandacht te richten op het effect van ons handelen op de relatie tussen overheid –de politie in het bijzonder- en burgers. Ik geef haar graag het podium:

Privacy en slimme camera's: kennis van gisteren voor toepassingen van morgen

Slimme camera's worden steeds slimmer. Automatische kentekenplaatherkenning (ANPR) is een vroege en inmiddels ingeburgerde vorm van deze technologie die kentekens optisch kan herkennen in beeldmateriaal. De techniek heeft zich ontwikkeld naar het herkennen van gedragingen en gezichten. Dit kan steeds accurater, onder moeilijke hoeken en lichtomstandigheden.

Deze vormen van waarneming op afstand bieden een scala aan mogelijkheden voor de politie. Slimme camera's worden bijvoorbeeld ingezet om bellen en appen in het verkeer te bekeuren. CATCH gebruikt gelaatsvergelijking om beelden uit politieonderzoek te vergelijken met referentielijsten met verdachten en vreemdelingen. Verdere toepassingen van gezichtsherkenning stuiten op privacybezwaren met China als schrikbeeld.

Welke privacyvraagstukken bestaan er bij slimme cameratoepassingen? Eerder dit jaar deed ik met collega's van de Universiteit Utrecht onderzoek naar hoe de Tweede Kamer het debat voert over digitale technologieën. De Tweede Kamer is dé plek waar onze volksvertegenwoordiging afwegingen van maatschappelijke waarden en belangen zoals veiligheid en privacy maakt.

In het debat over ANPR – één van de cases in ons onderzoek – gebeurde iets opmerkelijks.

Na kritische evaluaties van het College Bescherming Persoonsgegevens en de daarop volgende wetswijziging van WvS artikel 126jj vernauwde het debat over privacy tot de bewaartermijn van kentekens die niet in referentielijsten staan. Privacy werd opgevat als gegevensbescherming, ofwel informationele privacy. Ook rond gezichtsherkenning lijkt dit te gebeuren: Kamervragen over dit thema gingen voornamelijk over het verkrijgen en bewaren van gezichten op referentielijsten en dit specifiek door het bedrijf Clearview AI.

Privacy bij slim cameratoezicht omvat echter meer dan dat. Toen ANPR nog in de kinderschoenen stond, verscheen een interessant artikel van filosoof Jeffrey Reiman getiteld 'Driving to the panopticon'. Hij betoogt dat observatie in het publieke domein, ook wanneer deze rechtmatig is en voor de juiste bedoelingen wordt ingezet, privacy ook op andere manieren beperkt. Hij beargumenteert dat de aanwezigheid van slimme camera's voor surveillance de vrijheid van burgers beperkt. Het leidt tot 'chilling effecten': het vermijden van bepaald gedrag ook wanneer het niet illegaal is, maar slechts onconventioneel. Daarnaast gaat er volgens Reiman een onwenselijke symbolische boodschap uit van de aanwezigheid van grootschalig en permanent cameratoezicht: het is een motie van wantrouwen naar de burger.

Slim cameratoezicht raakt daarmee ook aan gedragsmatige privacy: dit zijn privacybelangen die een persoon heeft bij openlijk zichtbare activiteiten. Jezelf kunnen uiten, zonder dat alles geregistreerd wordt en waarbij onconventioneel gedrag verdacht is, is ook onderdeel van privacy. Dit vraagt om een verbreding van het politieke en maatschappelijke debat over privacy wanneer nieuwe slimme cameratoepassingen worden overwogen.

We moeten niet alleen waarborgen inbouwen om overmatige en onrechtmatige verzameling van slimme camera-data tegen te gaan. Ook is het belangrijk om rekening te houden met ongewenste neveneffecten op gedrag van burgers. Het gunnen van een zekere mate van anonimiteit, ook in de publieke ruimte, is een belangrijke basis voor gezond vertrouwen tussen overheid en burgers. Een les voor de Tweede Kamer, maar ook voor de politie wanneer nieuwe slimme cameratoepassingen worden overwogen.