Meervoudig gebruik van camera's: het mag, maar willen we het ook?

Thijs Turèl en Sander Flight[1]

4 april 2024

Stel: u werkt bij een gemeente die elke dag een scanauto door de straten laat rijden om te controleren of voor alle geparkeerde auto's is betaald. Dan is het natuurlijk heel handig om die camerabeelden ook te gebruiken om te zien of er afval op straat ligt. Of om te zien of alle verkeersborden nog recht staan. Dat heet 'meervoudig gebruik' van camera's. Onder bepaalde voorwaarden is het juridisch toegestaan een camera voor meerdere doelen te gebruiken: "Ja, mits…".[2] Maar er is meer dan de juridische afweging: het moet ook technisch en organisatorisch goed worden geregeld. En daar wringt de schoen in veel gemeenten. In dit artikel houden wij daarom een pleidooi om te blijven werken met een "Nee, tenzij…" benadering.

Welke zorgen hebben we over meervoudig cameragebruik?

Ambtelijk overenthousiasme

Als je een apart camerasysteem moet bouwen kost dat vaak veel tijd, geld en moeite. Dat zet een rem op het aantal nieuwe camerasystemen. Meervoudig cameragebruik is sneller, goedkoper en makkelijker. Je hoeft alleen maar een paar kabels aan elkaar te knopen *et voila*! Door het weghalen van de drie genoemde barrières lopen we een risico op ambtelijk overenthousiasme. Je kunt met camera's immers prima sigarettenpeukjes en verkeerd geparkeerde fietsen tellen. Je kunt ook zien of er hangjongeren of zwervers zijn. Daar zou je normaal gesproken waarschijnlijk geen zelfstandig camerasysteem voor bouwen, maar als er toch al camera's staan…

Het politieke debat overslaan

Niet alleen de proportionaliteit (je mag niet met een kanon op een mug schieten) komt in gevaar, maar ook de democratische legitimering. Bij een nieuw camerasysteem vindt vaak een politieke toets plaats. Die toets zou bij hergebruik van een bestaand camerasysteem tussen wal en schip kunnen verdwijnen. Maar zo'n toets is hard nodig: deze voorkomt namelijk dat we over tien jaar ineens ontdekken dat we een werkelijkheid hebben gebouwd waar we nooit bewust voor hebben gekozen.

Meer kwetsbaarheden in de datastroom

Als een camera voor meerdere doelen wordt gebruikt, zal *iets* de beelden moeten doorsluizen van afdeling A naar afdeling B. Zo'n

---

Noot 1 Thijs Turèl is programma-manager bij AMS waar hij zich bezighoudt met verantwoorde digitalisering. Sander Flight is onafhankelijk onderzoeker en adviseur op het gebied cameratoezicht. De auteurs willen graag de gemeentelijke medewerkers, privacy-experts en wetenschappers bedanken die een reactie hebben gegeven op een conceptversie van dit verhaal.
Noot 2 Het advies is afkomstig van Pels Rijcken en Verdonck, Klooster & Associates. Dit team wordt de *Adviesfunctie verantwoord datagebruik* genoemd en is opgericht in het kader van de Interbestuurlijke Datastrategie.

datadeelplatform is een systeem met een beheerder en verschillende gebruikersgroepen. Dat levert nieuwe kwetsbaarheden op: het wordt moeilijker te overzien wie er aan de data heeft gezeten. En na een datalek is het veel moeilijker om te "dweilen". Ook het toezicht wordt moeilijker. Want welke functionaris voor gegevensbescherming moet hier toezicht op houden: die van doel A of van doel B? Of gaan ze er vanuit dat de ander het wel heeft geregeld?

Meer delen dan nodig

Bij meervoudig gebruik van een camera is het makkelijker om de ruwe beelden door te sturen dan om een selectie te maken of de gegevens anoniem te maken. Maar zijn die ruwe beelden nodig voor doel B? Om te zien of ergens afval op straat ligt, heb je geen bewegende beelden met mensen en kentekens nodig. Maar de kans is groot dat de taak om de gegevens netjes te anonimiseren aan de ontvangende partij wordt overgelaten. Eigenlijk moet je dat niet willen. Want wie de gegevens anonimiseert, kan ze ook weer ontanonimiseren. De Autoriteit Persoonsgegevens is terecht heel streng: alleen als het anonimiseren niet kan worden ongekeerd door de ontvangende partij is het anoniem. Een goed voorbeeld is blurring as a service. Bij dit door Amsterdam ontwikkelde algoritme worden panoramabeelden zorgvuldig ontdaan van alle persoonsdata (hele personen worden geblurd, niet alleen hun gezichten) voordat de data door andere afdelingen mogen worden gebruikt.

Verwarring over toezicht

De spaghetti van verantwoordelijkheden is voor toezichthouders net zo ingewikkeld als het aantal kabels tussen de camera's en het aantal gebruikers van het camerasysteem. Toezichthouders kunnen elkaar voor de voeten gaan lopen, maar – nog erger – het kan ook dat de toezichthouder voor doel A denkt dat de ander van doel B het wel geregeld zal hebben. Juridisch is dat ook best ingewikkeld. In de AVG staat dat degene die doel en middelen van een verwerking vaststelt de verantwoordelijke is. Is de afdeling die de camerabeelden voor doel B ontvangt dan een verwerker voor de afdeling die met doel A bezig is? Nee, niet volgens de AVG – dan zou afdeling B namelijk 'ten behoeve van' afdeling A moeten werken. Een ontvanger dan? Ook niet, want de ontvanger is in dit geval zelf verantwoordelijk voor het kiezen en onderbouwen van het doel van de verwerking. Is het dan een 'derde'? Of een gezamenlijke verwerkingsverantwoordelijke? Dat lijkt wellicht juridische haarkloverij, maar het zal de eerste vraag zijn die elke toezichthouder stelt: wie is waar verantwoordelijk voor?

Tekort aan toezicht, controles en audits

Voor veel camerasystemen wordt netjes een Data Protection Impact Assessment (DPIA) uitgevoerd. Maar daar blijft het helaas vaak bij: een papieren tijger. De afspraken over jaarlijkse audits, controles en managementrapportages worden in de praktijk helaas niet altijd uitgevoerd als afgesproken. Door een tekort aan ervaren privacyexperts, bijvoorbeeld: veel vacatures kunnen niet worden vervuld. Of omdat het maken van nieuwe DPIA's en verwerkersovereenkomsten meer prioriteit krijgt dan het controleren en updaten van de huidige. Dat wordt allemaal nog veel ingewikkelder als de camerabeelden door iemand anders voor een ander doel worden gebruikt. Ook voor anderen die 'van buitenaf' toezicht willen houden (betrokken burgers, bijvoorbeeld) is het heel moeilijk om te zien wat er in dit soort verwerkingen precies gebeurt met de gegevens. Dat geldt al voor enkelvoudig gebruik en des te sterker voor meervoudig gebruik. Probeer maar eens een goed informatiebordje te maken als er drie verschillende partijen gebruikmaken van een camera.

De macht van de markt

Het is niet eenvoudig om te doorgronden hoe camerasystemen precies werken. Zelfs voor de leveranciers van dat soort systemen is dat soms moeilijk. Er zijn bedrijven die beweren dat de AVG niet van toepassing is omdat hun camera's geen camera's zijn, maar 'sensoren'. Maar vaak zijn die sensoren in eerste instantie toch gewoon camera's. De beelden worden door software anoniem gemaakt. Het probleem is dat die software vaak niet feilloos is. En zoals we al eerder schreven kan degene die de software 'aan' moet zetten, die ook 'uit' zetten – per ongeluk of met opzet.

Dus niet doen, tenzij…

We hebben inmiddels flink wat beren op de weg gezet. Het is soms echt wel een goed idee om een camera meervoudig te gebruiken. Maar dan moeten de hierboven gesignaleerde valkuilen worden vermeden. We trappen hier voor een deel open deuren in, maar dat doen we bewust: dit zijn de punten waar het vaak mis gaat.

Zorg voor genoeg mensen, geld en tijd

Hoe meer camera's, hoe meer risico's. Dat vereist niet alleen informatiebeveiligers, maar ook juristen met verstand van zaken en techneuten die gekoppelde camerasystemen in hun geheel kunnen overzien. Die zijn niet makkelijk te vinden, zoals elke gemeente inmiddels heeft ontdekt. Zorg ook voor genoeg budget om alle risico's te mitigeren: meervoudig cameragebruik kan kostenbesparend werken, maar in het begin kost het toch gewoon extra geld om de koppeling goed en veilig te bouwen. En neem de tijd: het is altijd een goed idee om een DPIA op te stellen, maar dat doe je niet in een maandje.

Tem de techniek

Verantwoordelijkheid dragen voor een technisch systeem impliceert dat je dat systeem tot op zekere hoogte moet begrijpen. Je hebt mensen nodig die kunnen checken of de glossy folder van een marktpartij *waar* is. En die de specs kunnen lezen en – waar nodig – extra waarborgen kunnen inbouwen. Die expertise wil je niet inhuren bij de leverancier, maar in eigen huis hebben. Hou ook rekening met het feit dat camerasystemen wel iets weg hebben van een levend organisme: ze ontwikkelen zich continu door updates, reparaties, back-ups en aanpassingen. Werk dus niet alleen aan een goeie opleverign, maar reserveer mensen, geld en tijd voor de *life-cycle*.

Delete by default

Zorg dat riskante koppelingen zichzelf automatisch uitschakelen, bijvoorbeeld elke 24 uur. Dat klinkt lekker makkelijk, maar is best complex. Want de meeste systemen zijn hier niet op gebouwd: de default is meestal om alles altijd te bewaren en het kost moeite om *privacy by design* te implementeren. En te bewaken, zodat alle vinkjes na een update nog steeds goed staan.

Doe de politieke volwassenheidscheck

Veel gemeenteraadsleden en bestuurders zijn nog onvoldoende bekwaam in digitale zaken. Dat is langzaam aan het veranderen: we zien steeds vaker colleges met een wethouder 'digitale zaken' die meer doet dan de gemeentelijke website. Een wethouder die antwoord kan geven op de vraag: "Wat voor gemeente willen wij zijn op digitaal gebied?" Maar het is een uitzondering: de meeste gemeenten zijn nog niet zo ver. Het is daarom interessant om alle raadsleden en collegeleden te vragen een korte toets te maken over digitalisering in de gemeente. Halen ze een onvoldoende? Dan allemaal op bijscholing. En in de tussentijd niet beginnen aan digitale projecten waar men de risico's nog niet van kan overzien.

Luister naar de techneuten

Feitelijk komt het delen van camerabeelden vaak neer op het aan- of uitvinken van een checkbox in de software. Of het uploaden van een lijstje mailadressen die vanaf dat moment ook toegang krijgen. Degenen die dat soort vinkjes mogen zetten en gebruikers kunnen toevoegen, moeten zich realiseren hoe belangrijk ze zijn. En ze moeten niet alleen verstand hebben van de bits en bytes, maar ook van juridische details en ethische dilemma's. Zij moeten de goeie vragen kunnen en durven stellen. Hun leidinggevende moet ze daarin steunen, want het zijn vaak lastige vragen.

Zorg voor de drie B's: beheer, beheer en beheer

Bestuurders van Nederland: pas op voor onderbegroting van het beheer van technische projecten. Een mooi nieuw meervoudig cameraproject bouwen is knap. Maar nog veel knapper en belangrijker is goed beheer. Daar zijn mensen, geld en tijd voor nodig. Dat is een open deur, dus is uw logische vraag: "Wat nou als me dat niet lukt door personeelstekorten, hoge doorloopsnelheid en te weinig budget om een concurrerend salaris te bieden aan de toppers die ik nodig heb?" Zorg dan in elk geval dat belangrijke keuzes altijd langs uw bureau komen en voorkom *function creep* die als innovatie wordt verkocht (zie Koops). Zorg dat het toezicht op orde is en vraag naar de resultaten van controles en audits. Trek preventief de stekker uit elk camerasysteem totdat aantoonbaar wordt

voldaan aan de gemeentelijke eisen en standaarden.

Maak het zichtbaar

Een gaslek kun je ruiken. Gelukkig maar, anders zouden er veel vaker keukens exploderen. Maar een datalek kan je niet ruiken. Het zou goed zijn als meer mensen kunnen zien wat elke camera eigenlijk doet. Dat kan door informatie op straat aan te bieden, met de mogelijkheid om online verder te lezen. Bij meervoudig cameragebruik moet je dan dus ook de achterliggende datastromen laten zien. Zo krijgt een grotere groep mensen de kans om te controleren of het allemaal goed gaat. Het zal de meeste mensen niet interesseren, maar de “informed minority theory” leert ons dat een beperkte groep geïnteresseerden uit het grotere publiek succesvol onze gemeenschappelijke belangen kan behartigen.

Dat dus. En nu?

We kunnen ons goed voorstellen dat u niet vrolijk bent geworden van dit verhaal. Al die risico’s! Al die maatregelen die we moeten treffen! Dat is dan precies de reactie waar wij op hoopten. Want het is allemaal een stuk ingewikkelder dan je bij eerste beschouwing zou denken. Daarom is het raadzaam altijd eerst de vraag te stellen: “Willen we dit echt?”

Zoals gezegd zijn wij niet tegen meervoudig gebruik van camera’s: er zijn kansen en die moeten worden gegrepen. Maar we maken ons wel zorgen en we hopen dat deze tekst helpt om te bezinnen voordat u gaat beginnen.

Let’s talk!

Wij willen heel graag doorpraten over dit onderwerp. We kunnen ons voorstellen dat er gemeenten zijn die nu met dit thema aan de slag zijn en wel wat structuur in de discussie kunnen gebruiken. Werkt u bij een gemeente en wilt u met ons doorpraten? Daar zijn we zeker voor in. We zijn goed bereikbaar via email.

info@sanderflight.nl

thijs.turel@ams-institute.org.