Gemeentelijke grip op private sensorgegevens

Juridisch kader voor het gemeentelijke handelingsperspectief bij de verwerking van private sensorgegevens in de openbare ruimte

Onderzoek in opdracht van de gemeente Amsterdam

UNIVERSITEIT VAN AMSTERDAM

Gemeentelijke grip op private sensoren

Juridisch kader voor het gemeentelijke handelingsperspectief bij de verwerking van private sensorgegevens in de openbare ruimte

Onderzoek in opdracht van de gemeente Amsterdam

December 2022

Mr. dr. H.L. Janssen
Mr. L.W. Verboeket
Mr. A. Meiring
Mr. dr. J.V.J. van Hoboken
Prof. mr. M.M.M. van Eechoud
Prof. mr. J.E. van den Brink
Prof. mr. R. Ortlep
Dr. B. Bodó

Universiteit van Amsterdam
Instituut voor Informatierecht
Afdeling Publiekrecht, sectie Staats- en bestuursrecht

Dit rapport valt onder een Creative Commons Naamsvermelding 4.0 Internationaal-licentie.

Managementsamenvatting

Context van het onderzoek

Private partijen verzamelen informatie met behulp van sensoren over het gedrag van personen in de openbare ruimte. Bij sensoren gaat het niet alleen om camera's, maar ook bijvoorbeeld om sensoren die verkeersbewegingen tellen, intelligente reclameborden of wifi-trackers. Bedrijven winnen gegevens in de openbare ruimte doorgaans in voor commerciële doeleinden, zoals reclamedoeleinden of wifi-tracking in winkelgebieden om het aantal passanten te tellen. Er zijn ook private partijen die sensoren inzetten voor onderzoeksdoeleinden, zoals het Centraal Bureau voor de Statistiek (hierna: CBS).

Wanneer private partijen voortdurend en op grote schaal informatie verzamelen kan dit gevolgen hebben voor fundamentele rechten en vrijheden, zoals het recht op privacy, het recht op bescherming van persoonsgegevens en het recht niet zonder toestemming geprofileerd te worden. Dit kan problematisch zijn, omdat private sensoren in de openbare ruimte voor burgers niet altijd zichtbaar zijn en omdat vaak niet duidelijk is hoe lang of met welk doel gegevens worden verzameld en met wie ze verder worden gedeeld. Het Amsterdamse college van burgemeester en wethouders heeft daarom in zijn stedelijke beleidskader aangegeven vast te willen houden aan zijn uitgangspunt dat iedereen in Amsterdam het recht heeft op respect voor zijn of haar privéleven en dat iedereen zich onbespied in de openbare ruimte moet kunnen bewegen.

Dezelfde private sensorgegevens kunnen tegelijkertijd echter ook informatief zijn voor de gemeente en dienstbaar zijn bij de uitvoering van publieke taken, zoals bij de bevordering van de bereikbaarheid, fysieke veiligheid en leefbaarheid in de stad. Bedrijven stellen deze gegevens echter niet zomaar beschikbaar, omdat ze bijvoorbeeld vrezen dat de gemeente met deze zogenoemde *business-to-government* gegevensdeling (hierna: B2G-gegevensdeling) een inbreuk zou kunnen maken op het gegevensbeschermingsrecht of hun eigen bedrijfsgeheimen en intellectuele eigendomsrechten. Er kunnen ook andere redenen aan een weigering ten grondslag liggen, zoals het verlies van controle en zeggenschap over wat er gebeurt met de gegevens of economische overwegingen. Een specifiek wettelijk kader dat B2G-gegevensdeling reguleert is op dit moment niet voorhanden. Dit creëert rechtsonzekerheid over de toelaatbaarheid en voorwaarden bij B2G-gegevensdeling. De EU-wetgever bereidt een Dataverordening voor die ruimte laat voor nationale regulering rondom B2G-gegevensdeling, maar een meer specifiek materieel-normatief kader met heldere voorwaarden voor B2G-gegevensdeling lijkt daarin nog niet te zijn uitgekristalliseerd.

De gemeente vroeg de Universiteit van Amsterdam om een inventariserend advies over hoe zij bestaande juridische instrumenten (zoals overeenkomsten, subsidies, vergunningen, maar bijvoorbeeld ook gemeentelijke verordeningen) zou kunnen inzetten om de fundamentele rechten van burgers in de openbare ruimte beter te kunnen beschermen. Daarnaast verzocht de gemeente de Universiteit van Amsterdam om een inventariserend advies over de vraag of en hoe de gemeente de eerdergenoemde juridische instrumenten kan inzetten om, indien en voor zover dat nodig is, B2G-gegevensdeling te kunnen laten plaatsvinden ten behoeve van een betere vervulling van de gemeentelijke publieke taak en voor verdere deling ten behoeve van innovatiedoeleinden van andere professionele partijen die actief zijn binnen de gemeente.

In dit onderzoeksrapport analyseren we het toepasselijke juridisch kader bij verwerkingen van sensorgegevens door private partijen over het gedrag van mensen in de openbare ruimte en adviseren we de gemeente over de wijze waarop zij de gemeentelijke juridische instrumenten zou kunnen inzetten om de naleving van de fundamentele rechten te verbeteren. Daarnaast analyseren we het juridisch kader rondom B2G-gegevensdeling en adviseren we hoe de gemeente de eerdergenoemde juridische instrumenten zou kunnen toepassen om, waar dat nodig is, vaker B2G-gegevensdeling te kunnen laten plaatsvinden ten behoeve van een betere vervulling van de gemeentelijke publieke taak en ten behoeve van innovatiedoeleinden van andere professionele partijen die actief zijn binnen de gemeente. De adviezen

steunen op juridisch onderzoek en op semigestructureerde interviews met medewerkers van de gemeente Amsterdam en van bedrijven die actief zijn in de gemeente Amsterdam.

Bevindingen en adviezen voor een betere bescherming van fundamentele rechten

- *Beperkte regelgevende rol voor de gemeente*
  Uit de analyse van de Grondwet, het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (hierna: EVRM) en het Handvest van de grondrechten van de Europese Unie (hierna: EU-Handvest), alsook de Algemene Verordening Gegevensbescherming (hierna: AVG) komt naar voren dat de gemeente in beginsel geen rol toekomt bij de aanpassing van het wetgevend kader met betrekking tot de naleving van de fundamentele rechten door private partijen in de openbare ruimte; die rol is weggelegd voor de formele wetgever. Dat wil niet zeggen dat de gemeente in het geheel geen rol toekomt. Zo geeft de gemeentelijke Verordening meldingsplicht sensoren een eigentijdse invulling aan de AVG. Wij geven hierna een aantal inventariserende adviezen die gemeente zouden kunnen helpen bij een betere naleving van deze rechten door private partijen die sensoren in de openbare ruimte plaatsen en beheren.

- *De Verordening meldingsplicht sensoren biedt een beperkte verbetering van de bescherming van fundamentele rechten*
  Beter geïnformeerde burgers kunnen op basis van registraties in het sensorenregister bij de betreffende partij nagaan of, waar en welke persoonsgegevens over hen worden verwerkt en zich daartegen zo nodig verzetten bij de Autoriteit Persoonsgegevens (hierna: AP) die (hoge) boetes kan uitdelen. Als middel tot verbetering van de naleving van de fundamentele rechten kan het sensorenregister een beperkte verbetering voor de naleving van de fundamentele rechten met zich meebrengen. De doeltreffendheid van het register hangt immers niet alleen samen met de handhaving en het onderhoud ervan; de effectiviteit ervan lijkt ook af te hangen van de bereidheid van burgers zelf tot het uitoefenen van hun betrokkenenrechten. In dat verband verdient het overwegen van steun (subsidiëring) aan initiatieven die collectieve actie initiëren op basis van de Wet afwikkeling massaschade in collectieve actie (hierna: WAMCA) aanbeveling. Belangenorganisaties kunnen dergelijke acties voor individuen op touw zetten; gemeenten kunnen overwegen belangenorganisaties die zich toeleggen op kwesties die zich voordoen in gemeentelijke context steunen.

- *Breng de Verordening meldingsplicht sensoren, de meldingsplicht en het meldformulier actief onder de aandacht*
  Voor de naleving van de verplichtingen die de Verordening meldingsplicht sensoren oplegt is het van belang dat de Verordening, de meldingsplicht en de link naar het meldingsformulier gemakkelijk toegankelijk en vindbaar zijn voor private partijen, zodat zij precies weten wat van hen wordt verwacht. Actief beleid voor bewustwording en het wijzen op reeds bestaande wettelijke verplichtingen (zoals de AVG die geldt indien en voor zover de sensor persoonsgegevens verwerkt) kan bijdragen aan de naleving.

- *Ondersteun organisaties die collectieve uitoefening van de AVG-betrokkenenverzoeken mogelijk willen maken*
  Individuele betrokkenenverzoeken, ook indien gebaseerd op het sensorenregister, kosten vaak tijd en vereisen kennis en aandacht, maar leggen doorgaans niet de meer precieze verwerkingspraktijk van organisaties bloot. De individuele verzoeken en de antwoorden van verwerkingsverantwoordelijken daarop leiden in de praktijk nauwelijks tot bruikbare inzichten of tot betere naleving van het gegevensbeschermingsrecht. Gelet hierop zou de gemeente kunnen overwegen subsidies te verstrekken aan NGO's of organisaties in het maatschappelijk middenveld met expertise op het terrein van de AVG, die betrokkenenverzoeken vanuit een collectief perspectief kunnen coördineren. Recente ervaringen tonen aan dat betrokkenenrechten effectiever kunnen zijn als ze op collectieve schaal worden uitgeoefend. Indien een NGO (of een andere *ad hoc* ingerichte organisatie die dat op een

legitieme wijze kan coördineren) een groot aantal betrokkenenverzoeken en antwoorden van verwerkingsverantwoordelijken kan analyseren, kan zij de werkelijke omgang met persoonsgegevens door een bepaalde verwerkingsverantwoordelijke blootleggen. Vervolgens kan zij gebleken niet-naleving van de AVG (of van andere wetgeving) door de betreffende verwerkingsverantwoordelijke aan de kaak stellen. Betrokkenenverzoeken kunnen uiteraard ook worden gericht aan publiekrechtelijke verwerkingsverantwoordelijken, maar in dit rapport staan private verwerkingsverantwoordelijken centraal.

- *Laat onderzoeken hoe de naleving en handhaving van sensorenregisters kan worden verbeterd*
  Op dit moment kan de gemeente Amsterdam de verplichtingen die voortvloeien uit de Verordening meldingsplicht sensoren bestuursrechtelijk handhaven door middel van het opleggen van een last onder bestuursdwang of onder dwangsom. Naast Amsterdam zijn meer gemeenten bezig met het opzetten van een sensorenregister. Aandacht voor de naleving en handhaving op nationaal niveau kan helpen bij de bewustwording van 'meldingsplichtige' partijen. De gemeente Amsterdam kan, samen met andere gemeenten die waarschijnlijk met vergelijkbare vragen en onzekerheden rondom de naleving en handhaving zullen moeten omgaan, door wetenschappers en/of de regering en haar adviesorganen laten onderzoeken of naleving en handhaving op landelijk niveau zou kunnen bijdragen aan de verbetering van de naleving.

- *Zoek binnen het bestaande wettelijk kader ruimte om te experimenteren*
  De inzet van vrijwel alle bestuurlijke instrumenten vereist proportionaliteit van de eisen met betrekking tot de naleving van de mensenrechten, indien de gemeente dergelijke eisen wil opnemen als voorwaarde voor bijvoorbeeld het verkrijgen van een vergunning. Daarnaast vereist de inzet van die instrumenten een duidelijk en nauw verband tussen die eisen en het achterliggende doel van de inzet van het instrument (connexiteit). Daarbij geldt meer algemeen dat de drempels voor het opleggen van eisen met betrekking tot de naleving van de fundamentele rechten lager zijn dan voor het opleggen van eisen met betrekking tot B2G-gegevensdeling. De gemeente dient het opleggen van eventuele eisen met betrekking tot het naleven van de fundamentele rechten op weloverwogen wijze te doen. Zij zou daarbij niet bang moeten zijn om te experimenteren. Hier kan '*regulatory sandboxing*' wellicht mogelijkheden bieden om te verkennen welke ruimte bestaat. Of en welke experimenteerruimte bestaat is niet op voorhand te zeggen, aangezien deze ruimte sterk context-gebonden is.

Bevindingen en adviezen voor B2G-gegevensdeling en het delen van gegevens met derden

- *B2G-gegevensverwerking die raakt aan fundamentele rechten moet op een specifieke wettelijke grondslag berusten*
  B2G-gegevensdelingen en gemeentelijke verwerking van de uit die B2G-deling verkregen gegevens die kunnen raken aan de fundamentele rechten (waaronder gegevens-beschermingsrechten) van burgers of rechten van bedrijven, kunnen alleen plaatsvinden als voor de gegevensverwerking een specifieke wettelijke grondslag bestaat. Daarnaast laat de analyse van de Awb en de algemene beginselen van behoorlijk bestuur zien dat de gemeente weinig ruimte toekomt om zonder wettelijke grondslag bedrijven tot een B2G-gegevensdeling te verplichten op basis van een publiekrechtelijk instrument, zoals een vergunning of subsidie. Privaatrechtelijke overeenkomsten kunnen een basis voor B2G-gegevensdeling bieden indien bij de deling geen persoonsgegevens of andere fundamentele rechten betrokken zijn en de B2G-gegevensdeling proportioneel is ten opzichte van het onderwerp van de overeenkomst. Hier geldt dat publiekrechtelijke wegen naar een B2G-gegevensdeling niet onaanvaardbaar mogen worden doorkruist door een privaatrechtelijke overeenkomst. Voor zover de gemeente op basis van een wettelijke grondslag een private partij de opdracht geeft een gegevensbestand op te maken waarin zich geen persoonsgegevens bevinden, maar waarbij wel

persoonsgegevens werden gebruikt om het bestand te creëren, treedt de gemeente voor het betreffende bestand op als verwerkingsverantwoordelijke in de zin van de AVG. In alle andere gevallen moet de gemeente op basis van de gemeentelijke bevoegdheid en de specifieke feiten en omstandigheden nagaan of zij verwerkingsverantwoordelijke is ten aanzien van het betreffende gegevensbestand.

- *Bij het verder delen van gegevens moeten rechten en belangen die gemoeid zijn met de gegevens worden gerespecteerd*
  Gemeenten lijken soms de overtuiging te hebben dat gegevens verzameld in de openbare ruimte het karakter van een publiek goed hebben en daarmee "van ons allemaal" zijn, mits het geen persoonsgegevens betreft. Vanuit die optiek bestaat dan soms de wens om zoveel mogelijk gegevens open te stellen, bijvoorbeeld met het oog op het aanjagen van innovatie bij bedrijven en ondernemers binnen de eigen gemeente. Gemeenten moeten bij het openstellen van gegevens echter steeds rekening houden met de intellectuele eigendomsrechten en de handelsgeheimen die op de gegevens kunnen rusten. Bij B2G-gegevensdeling is een palet aan wetten relevant, waaronder de Databankenwet, de Wet bescherming bedrijfsgeheimen, de Wet open overheid, de Richtlijn open data en de Wet hergebruik van overheidsinformatie. In het algemeen komt naar voren dat B2G-gegevensdeling en het verder delen van de gegevens met derden in beginsel niet onmogelijk is, maar dat telkens na moet worden gegaan of de bescherming van de betrokken rechten en belangen op passende wijze worden gerespecteerd. Dit kan erg complex zijn voor de gemeente, omdat niet zeker is of zij de relevante wetten op juiste wijze toepast en specialistische kennis daarvoor nodig kan zijn.

- *Onderzoek of en waar nieuwe wettelijke grondslagen voor B2G-gegevensdeling noodzakelijk zijn*
  Zonder specifieke wettelijke grondslag bieden de besproken (concept-)wetgeving en bestuurlijke instrumenten de gemeente een beperkt handelingsperspectief voor het verplichten tot B2G-gegevensdeling. Vrijwillige B2G-gegevensdeling is eveneens aan beperkingen onderworpen zodra bij een B2G-gegevensdeling fundamentele rechten kunnen worden geraakt of wanneer bij de deling persoonsgegevens worden verwerkt. Wanneer de gemeente het aantal situaties waarin zij bedrijven kan verplichten tot B2G-gegevensdeling zou willen uitbreiden, dan kan zij zowel de Europese als de nationale wetgever aansporen wetgeving tot stand te brengen. De gemeente kan onderzoek (laten) verrichten naar wetgeving die op dit moment al mogelijkheden biedt voor B2G-gegevensdeling. Zo bevat bijvoorbeeld artikel 30c van de Wet personenvervoer 2000 (hierna: Wp) een opening voor het mogelijk maken van een specifieke B2G-gegevensdeling. De gemeente zou bij de minister van Infrastructuur en Waterstaat kunnen aandringen op uitvoering van deze bepaling. Daarnaast kan de gemeente (laten) onderzoeken of dergelijke openingen in andere wettelijke bepalingen voorhanden zijn of (laten) onderzoeken bij welke wettelijke bepalingen een dergelijke opening noodzakelijk zou zijn. De wetgever zou, indien hij die handschoen oppakt, zoveel mogelijk moeten voorkomen dat een gefragmenteerd beeld ontstaat van situaties waarin B2G-gegevensdeling wel of niet is toegestaan. Voor zover de huidige wetgeving geen eenduidig antwoord geeft op de vraag of B2G-gegevensdeling in een bepaald geval wel of niet toelaatbaar is, kan de gemeente overwegen over te gaan tot 'regulatory sandboxing', waarbij zij een gecontroleerde testomgeving creëert om te onderzoeken of een bepaalde wet voor een specifieke B2G-gegevensdeling openingen biedt (of zou moeten bieden) en op welke wijze de betrokken rechten en belangen kunnen worden geborgd.

- *Dring gezamenlijk aan op verduidelijking van het wetgevend kader voor B2G-gegevensdeling in de Dataverordening*
  Meer rechtszekerheid rondom B2G-gegevensdeling is, gelet op enerzijds de groeiende belangstelling voor B2G-gegevensdeling en anderzijds de rechten, belangen en machtsverhoudingen die met B2G-gegevensdeling gemoeid kunnen zijn, urgent en noodzakelijk. De concept-Dataverordening laat ruimte voor de nationale wetgever om wetgeving tot stand te brengen waarmee private partijen kunnen worden verplicht tot het delen van gegevens, maar legt in de huidige versie (nog) geen kader met materiële

normen en beginselen vast voor een wetsconforme, maatschappelijk aanvaardbare en succesvolle B2G-gegevensdeling, dat de machtsverschillen tussen de publieke sector en globaal opererende bedrijven zoveel mogelijk mitigeert. De gemeente Amsterdam zou in samenwerking met andere gemeenten (in Nederland en met gelijkgestemde gemeenten in de EU) kunnen overwegen de namens Nederland onderhandelende departementen en leden van het Europees Parlement te wijzen op de noodzaak van een meer uitgewerkt juridisch-normatief kader dat meer rechtszekerheid kan bieden. Uit de publieksconsultatie van de concept-Dataverordening kwam overigens naar voren dat de industrie geen voorstander is van bindende regels rond het delen van B2G-gegevens en dat het standpunt van de Nederlandse regering over verplichte B2G-gegevensdeling dat in Brussel wordt uitgedragen, tot nu toe terughoudend is. Ook op rijksniveau constateren we terughoudendheid als het gaat om de regierol van de minister van Infrastructuur en Waterstaat op het gebied van B2G-gegevensdeling.

- *Zoek binnen het bestaande wettelijk kader ruimte om te experimenteren*
  De inzet van vrijwel alle bestuurlijke instrumenten vereist zoals gezegd proportionaliteit van de eisen met betrekking tot het verzamelen en/of delen van private sensorgegevens, indien de gemeente dergelijke eisen wil opnemen als voorwaarde voor bijvoorbeeld het verlenen van een vergunning. Daarnaast vereist de inzet van de instrumenten een duidelijk en nauw verband tussen die eisen en het achterliggende doel van de inzet van het instrument (connexiteit). Bij de inzet van publiekrechtelijke instrumenten om private organisaties te verplichten tot B2G-gegevensdeling is, zoals eerder aangegeven, een wettelijke grondslag noodzakelijk. De gemeente dient, gelet op de vereiste proportionaliteit, connexiteit en de noodzaak van een specifieke wettelijke grondslag, het opleggen van eventuele eisen met betrekking tot het verzamelen en/of delen van private sensorgegevens op weloverwogen wijze te doen, maar ook hier zou zij niet bang moeten zijn om te experimenteren. Ook bij deze experimenten kan 'regulatory sandboxing' wellicht mogelijkheden bieden. De interviews met bedrijfsmedewerkers wijzen immers uit dat niet alleen bilateraal, maar ook unilateraal ingrijpen tot positieve ervaringen voor zowel de gemeente als private partijen kan leiden.

- *Gebruik naast de DPIA het IAMA voor het inschatten van risico's bij B2G-gegevensdeling*
  Voor de beoordeling of zich risico's voor de fundamentele rechten voordoen bij een voorgenomen B2G-gegevensdeling waarin tevens persoonsgegevens worden verwerkt, zal de gemeente mogelijk een Data Protection Impact Assessment (hierna: DPIA) moeten verrichten. Zij zou daarnaast kunnen overwegen het Impact Assessment Mensenrechten en Algoritmes (hierna: IAMA) te gebruiken. Het IAMA sluit in opzet aan bij de DPIA. Het IAMA onderzoekt echter niet alleen risico's voor de verwerking van persoonsgegevens en privacy, maar biedt ook zicht op risico's voor andere grondrechten. Het IAMA is erop gericht overheden in staat te stellen in het ontwerp- en ontwikkelstadium van een voornemen tot B2G-gegevensdeling na te gaan of deze gegevens conform het fundamenteelrechtelijk kader kunnen worden verwerkt. Het IAMA beoogt een praktisch toepassingskader te bieden. Het legt uit hoe de gemeente kan nagaan of het gebruik van een bepaalde verwerking tegen de achtergrond van het fundamenteelrechtelijk kader noodzakelijk, evenredig en subsidiair is en geeft voorbeelden van maatregelen om restrisico's te mitigeren.

Municipal control over private sensor data

Summary

Context of this study

Private parties gather information about people's behaviour in public spaces by using several different types of sensors. Sensors include not only cameras, but also, for example, sensors that count traffic movements, intelligent billboards or wifi-trackers. Companies typically collect data in public spaces for marketing or commercial purposes, such as advertising purposes or wifi-tracking in shopping areas to count the number of pedestrians in these areas. There are also private parties that deploy sensors for research purposes, such as the Central Bureau of Statistics (hereinafter CBS).

Where private parties collect information continuously and at scale, fundamental rights and freedoms might be affected, such as one's right to privacy, the right to protection of one's personal data and the right not to be profiled without one's consent. The use of sensors in public spaces can be problematic because these sensors may not always be visible to citizens. Moreover, it may not be clear how long or for what purpose data is collected and stored, how this data may be processed, or with whom it is further shared. The municipality of Amsterdam has therefore indicated in its urban policy framework that it aims to stick to its basic principle that everyone in Amsterdam has the right to respect for their private life and that everyone should be able to move unobserved in public space.

Meanwhile, the same private sensor data can be informative for the municipality, and assist the municipality with better informed performances of its public tasks, such as in promoting accessibility of the municipality's public spaces, of people's physical safety, or citizens' liveability in the city. However, companies do not simply make this data available because they fear, for instance, that sharing their data might infringe data protection law, or risk infringements of their own trade secrets and intellectual property rights with this so-called *business-to-government* data sharing (hereinafter B2G data sharing). Also other reasons might underlie a refusal, such as loss of control over what happens to the data, or economic considerations. A specific legal framework regulating B2G data sharing is currently not in place. This might create legal uncertainty about the permissibility and conditions according to which B2G data sharing is legally compliant. The EU legislator is preparing a Data Act that may leave room for national regulation concerning B2G data sharing, but a more specific substantive-normative framework with clear conditions for B2G data sharing has so far not yet occurred in the forthcoming Data Act.

It is within this context that the municipality of Amsterdam has asked the University of Amsterdam for an inventory advice on how the municipality could use existing administrative instruments (such as agreements, subsidies, permits, but also municipal regulations) to better protect the fundamental rights of citizens in public spaces. In addition, the municipality asked the University of Amsterdam for an inventory advice on whether and how the municipality could deploy the aforementioned administrative instruments to allow B2G data sharing, if and to the extent necessary, for better performance of the municipal public task and for further sharing for innovation purposes of other professional parties active within the city of Amsterdam.

In this research report, we analyse the applicable legal framework for private parties that are processing sensor data about people's behaviour in public spaces, and advise the municipality on how it could use its administrative instruments to improve the protection of fundamental rights. In addition, we analyse the current and forthcoming legal framework surrounding B2G data sharing, and advise how the municipality could apply the aforementioned administrative instruments to allow, where the municipality deems this necessary, more frequent B2G data sharing, for the better performance of the municipal public

task and for innovation purposes of other professional parties operating within the municipality. The findings are based on legal research and semi-structured interviews with employees of the Amsterdam municipality and companies active in the Amsterdam municipality.

Findings and advice to improve fundamental rights protection in public spaces

- *Limited regulatory role for the municipality*
  From the analysis of the Dutch Constitution, the European Convention on Human Rights and Fundamental Freedoms (hereinafter: ECHR) and the Charter of Fundamental Rights of the European Union (hereinafter: EU Charter), as well as the General Data Protection Regulation (hereinafter: GDPR), it emerges that, in principle, the municipality is not entitled to any role in adapting the legislative framework regarding a private party's compliance with fundamental rights in public spaces; that role is reserved for the formal legislator (i.e., the parliament which passes an Act of Parliament). This does not mean that the municipality is not entitled to any role at all. Below, we provide some exemplar policy measures that could help municipalities with improving a private party's compliance with these rights whenever they capture data about huma behaviour by way of sensors in public spaces.

- *Sensor notification ordinance might potentially contribute to the protection of fundamental rights*
  As of October 2021, the municipality of Amsterdam obliges by way of its so-called sensor notification ordinance all organisations, including private parties deploying sensors in public spaces, to register their sensors in a publicly accessible sensor register. Citizens can access the register and check whether and where a party collects personal data about them. Where necessary, citizens can exercise their data rights under the GDPR against the data controller, or object to that processing of their personal data with the Data Protection Authority (hereinafter: DPA), which can issue (high) fines. As a means of improving compliance with fundamental rights, the sensor notification ordinance might bring about a limited improvement for fundamental rights compliance by private parties processing personal data via sensors. Indeed, the effectiveness of the register is not only dependent on being enforced and maintained by the municipality; its effectiveness also seems to be contingent on the willingness of citizens themselves to exercise their data subjects' rights. In that context, considering support (by way of subvention) for initiatives instigating collective actions based on the Dutch Mass Tort Claims Settlement Act in Collective Action (hereinafter: WAMCA) is a path we advise the municipality to consider supporting. Interest groups may initiate such actions for individuals; municipalities may consider supporting interest groups dedicated to issues arising in municipal contexts.

- *Bring the Amsterdam sensor notification ordinance and its obligations to the attention of private parties*
  Active awareness-raising policies can contribute to compliance. For compliance with the obligations imposed by the municipality's ordinance, it is important that the ordinance, the notification obligation and particularly the link to the notification form are easily found and made accessible to private parties, so that they know exactly what is expected of them.

- *Support organisations wishing to enable collective exercises of GDPR's data subjects' rights*
  Individual data subject requests, also those based on the sensor register, often take time and require knowledge and attention, but usually do not reveal the more precise data processing practices of private organisations that could inform data subjects more accurately about how 'their' personal data is dealt with. Moreover, in practice, individual requests and data controller responses to these requests hardly lead to useful insights or better compliance with data protection law. Here, the municipality could consider subsidising NGOs or civil society organisations with expertise in the field of the GDPR and data rights exercises. These organisations could coordinate data subjects' requests from a collective perspective. Recent experiences have shown that collective exercises of data rights can be more

effective. Whenever an organisation that can legitimately and reliably coordinate such collective rights exercises can analyse a large number of data subjects' requests and responses from data controllers, it might be able to uncover the handling of personal data by a specific controller more accurately. It can then bring any proven non-compliance with the GDPR (or other legislation) by the data controller to the attention of data subjects, the DPA and/or the public at large.

- *Commission or conduct research on improvement of compliance and enforcement of the sensor registration obligation*
  Currently, the municipality of Amsterdam can enforce the obligations arising from the ordinance under administrative law by imposing an administrative enforcement order or administrative fine. Besides Amsterdam, other municipalities are also establishing sensor registers. An effective approach regarding compliance and enforcement with the local registers at national regulatory level can further help raise awareness among those to whom the registration obligations apply. The municipality of Amsterdam, together with other municipalities that may have to answer similar questions and uncertainties around compliance with and enforcement of their sensor registers, could consider to commission researchers and/or request the government and its advisory bodies to investigate how compliance and enforcement with current and forthcoming sensor registries could be improved.

- *Try and experiment with the administrative instruments within the existing legal framework*
  The deployment of almost all administrative instruments requires conditions aiming at fostering fundamental rights compliance to be proportionate, if the municipality wants to include such requirements as a condition for obtaining, for instance, a permit. In addition, the deployment of the administrative instruments requires a clear and close link between those fundamental rights conditions on one hand, and the underlying purpose of the deployment of the instrument on the other. Note, however, that the thresholds for imposing conditions relating to compliance with fundamental rights are generally lower than for imposing requirements relating to B2G data sharing (see below). The municipality should impose any requirements regarding fundamental rights compliance as a condition in a careful manner. In doing so, the municipality should not be afraid to try and experiment; here, '*regulatory sandboxing*' might offer opportunities to explore what scope for such conditions would exist. Whether and what space for such experiments will exist cannot be said in advance, as such space usually depends on the specific context.

Findings and advice on B2G data sharing and sharing with third parties

- *B2G data sharing affecting fundamental rights must have a basis in a formal law*
  B2G data sharing that potentially affects fundamental rights, including data protection rights, can in principle only occur whenever a formal legal basis (i.e., an Act of Parliament) for that B2G data sharing exists. The analysis of the Dutch General Administrative Law Act and the general administrative law principles of good administration demonstrates that municipalities have little room to oblige businesses to share data in a B2G data sharing relationship whenever a formal legal basis is absent. Private law agreements (usually contract-based) can provide a basis for B2G data sharing, but this applies only under the conditions that the sharing does not involve the processing of personal data nor affects any other fundamental rights, and that the B2G data sharing is proportionate to the subject matter of the agreement. Here, it must be noted that public law arrangements for B2G data sharing cannot be unacceptably thwarted by a private law agreement. Moreover, insofar as the municipality instructs a private party, based on a law, to create a data file that does not contain personal data, but where personal data were processed to create that file, the municipality likely acts as a data controller within the meaning of the GDPR for the file in question. In other situations, the municipality must carefully determine whether it acts as a data controller with regard to the data files it receives from B2G data sharing –

which may be derived from the municipality's competence, and the specific facts and circumstances of the data sharing.

- *Any further sharing of data with third parties must respect the rights and interests pertaining to the data*
  Municipalities might be convinced that data collected in public space is a public good, and therefore belongs to "all of us" (provided it is not personal data). From this perspective, a municipality's desire might exist to open up and share as much data as possible, with a view to, for instance, boosting innovation among companies and entrepreneurs within the city. However, when opening up and sharing data that was received through B2G data sharing, municipalities should comply with intellectual property rights and trade secrets that may rest on that data. Several different laws apply to B2G data sharing and to onward sharing of that data with third parties. These laws include the Databases Act, the Trade Secrets Protection Act, the Open Government Act, the Open Data Directive and the Reuse of Public Sector Information Act. In general, it emerges that B2G data sharing and further sharing with third parties is in principle not impossible, but each sharing with third parties requires a municipality's careful checking of whether the protection of the rights and interests pertaining to the data are appropriately respected, in compliance with existing legal obligations. This can be very complex for the municipality, as the municipality might not be certain whether the relevant laws are correctly applied. A legal specialist's expertise may be necessary.

- *Explore whether and where new legal bases for B2G data sharing are deemed necessary*
  Without any basis in an Act of Parliament, legislation and the use of administrative instruments might offer municipalities a limited perspective for obligatory B2G data sharing. Voluntary B2G data sharing is also subject to restrictions whenever fundamental rights are affected in B2G data sharing, arrangements or where personal data is processed. If the municipality would like to expand the number of situations in which it can oblige companies to share B2G data, it may consider urging both European and national legislators to create legal bases fur such sharing. The municipality could examine whether currently existing legislation already provides opportunities for B2G data sharing. For example, section 30c of the Dutch Passenger Transport Act 2000 contains a provision for implementing specific B2G data sharing obligations. As this provision has so far not been implemented, the municipality could encourage the Minister of Infrastructure and Water Management to use that provision. In addition, the municipality could (commission research to) investigate whether such openings are available in other laws, or (commission research to) investigate in which legal provisions such an opening should be created. Whenever the legislator (by way of an Act of Parliament) indeed decides to create new legal bases, it should avoid creating a patchwork of situations in which B2G data sharing is (or is not) allowed. To the extent that current legislation does not provide an unambiguous answer to the question of whether B2G data sharing is or is not permissible in a particular situation, the municipality could consider regulatory sandboxing, whereby it creates a controlled test environment to investigate whether a particular law offers (or should offer) openings for a specific B2G data sharing and how the rights and interests involved can be safeguarded.

- *Jointly push for clarification of the legislative framework for B2G data sharing in the forthcoming EU Data Act*
  Greater legal certainty around B2G data sharing is urgent and necessary, given the growing interest in B2G data sharing on the one hand, and the rights, interests and power relations pertaining to B2G data sharing on the other. The forthcoming EU Data Act leaves space for national legislators to enact legislation that could oblige private parties to share data, but the current version this draft Act does not (yet) contain a framework of conditions, standards and principles for lawful, socially acceptable and successful B2G data sharing that mitigates, as much as possible, the power differences between the public sector and (globally operating) companies. The municipality of Amsterdam could, in cooperation

with other municipalities (in the Netherlands and with like-minded municipalities across the EU), consider drawing the attention of the ministry of Economic Affairs negotiating on behalf of the Netherlands and members of the European Parliament to the need for a more elaborate legal-normative framework, that can provide more legal certainty for B2G data sharing. Incidentally, the public consultation on the forthcoming Data Act revealed that the industry is not in favour of binding rules. with regard to B2G data sharing, and that the Dutch government's position on mandatory B2G data sharing expressed in Brussels has so far been reticent. At the national level, we also noted a reluctance when it comes to the steering role of the minister of Infrastructure and Water Management with regard to B2G data sharing.

- *Try and experiment with the administrative instruments within the existing legal framework*
  As mentioned, the deployment of almost all administrative legal instruments necessitates proportionality of a municipality's requirements relating to the collection and/or sharing of private sensor data, if the municipality wants to include such requirements as a condition for granting, for instance, a licence. In addition, the deployment of the instruments requires a clear and close relationship between those requirements and the underlying purpose of the deployment of the instrument. When deploying public law instruments to oblige private organisations to share B2G data, a legal basis is necessary. Considering the required proportionality, the presence of a close relationship and the need for a formal law (i.e., an Act of Parliament), the municipality should carefully consider imposing any requirement regarding the collection and/or sharing of private sensor data, but again, it should not be afraid to experiment. Regulatory sandboxing might also in B2G data sharing contexts offer opportunities for such experiments. Indeed, interviews with company officials indicate that not only bilateral, but also unilateral intervention can lead to positive experiences for both the municipality and private parties in B2G data sharing relations.

- *In addition to the DPIA, use the IAMA to assess risks in B2G data sharing*
  To assess whether risks to fundamental rights arise from a proposed B2G data sharing relation that also processes personal data, the municipality may have to conduct a Data Protection Impact Assessment (DPIA). We advise the municipality to additionally use the Dutch Fundamental Rights and Algorithms Impact Assessment (hereafter: FRAIA). The FRAIA is similar in concept to the DPIA. However, the FRAIA not only examines risks to the processing of personal data and privacy, but also provides insight into risks to other fundamental rights. The FRAIA aims to enable governments at the design and development stage of a B2G data-sharing intention, to assess whether such data can be processed in accordance with the fundamental rights framework. The FRAIA aims to provide a practical application framework. It explains how the municipality can verify whether the use of a given processing against the background of the fundamental rights framework is necessary, proportionate and subsidiary, and provides examples of measures to mitigate residual risks.

Inhoudsopgave

1 Inleiding

1.1 Context en probleemduiding

Het Amsterdams stedelijk beleidskader stelt dat "iedereen in Amsterdam het recht [heeft] op respect voor zijn of haar privéleven" en dat "voor iedereen in Amsterdam het uitgangspunt geldt dat zij zich onbespied en anoniem (moeten) kunnen bewegen in de openbare ruimte".[1] Dit uitgangspunt staat echter onder druk. Deze druk wordt in toenemende mate veroorzaakt door het feit dat naast de gemeente ook bedrijven, private onderzoeksinstellingen en andere private organisaties steeds meer, steeds grootschaliger en voor de burger veelal onopgemerkt gegevens inwinnen in en over de openbare ruimte.[2] Dit kan geschieden met behulp van diverse sensoren, zoals wifi-tracking, *automated number plate recognition* (hierna: ANPR),[3] drones of camera's die zich bijvoorbeeld in reclameschermen bevinden.[4]

Private partijen hebben informatierechten: binnen de geldende wettelijke kaders zijn zij vrij om informatie in de openbare ruimte te verzamelen. Informatieverzameling helpt hen bij het nastreven en vervullen van diverse legitieme doeleinden. Zij zijn om uiteenlopende redenen en afhankelijk van de sector waarin ze opereren gemotiveerd om gegevens over menselijk gedrag in de openbare ruimte te verzamelen en te gebruiken. Sommige private onderzoeksinstellingen, zoals het CBS, gebruiken sensoren in de openbare ruimte voor statistische onderzoeksdoeleinden. Bedrijven kunnen commerciële, economische of marktgeoriënteerde belangen hebben bij het gebruik van sensoren in de openbare ruimte. Zo kunnen sensoren in digitale reclameschermen die oogbewegingen van personen volgen die langs die reclameborden lopen, voor een bedrijf waardevolle feedback over een advertentie opleveren. Informatie verkregen met sensoren kan bedrijven informeren over het efficiënter en zuiniger gebruik van middelen en mensen bij het verlenen van diensten – eveneens een belangrijke drijfveer voor bedrijven, zeker als zij in een zeer competitieve markt opereren.[5] Wifi-trackers kunnen een bedrijf informeren over drukte op een bepaalde plaats of aangeven waar een persoon woont en werkt. Met die informatie kan het bedrijf dienstverlening of reclame nauwgezet afstemmen. Soms gebruiken private partijen sensoren om de (fysieke) veiligheid in en om het eigen gebouw te bewaken.

Wanneer de inzet van sensoren voortdurend, onopgemerkt, en/of op grote schaal plaatsvindt, kan dit gevolgen hebben voor de rechten en vrijheden van burgers en voor hun vertrouwen in publieke en private actoren in de openbare ruimte, temeer omdat private sensoren voor burgers vaak onopgemerkt worden verwerkt[6] en omdat er geen 'alternatieve' openbare ruimte beschikbaar is waar deze private monitoring niet plaatsvindt. Fundamentele rechten zoals privacy, menselijke waardigheid, de vrijheid van meningsuiting en het recht op gegevensbescherming kunnen met deze gegevensverwerkingen met behulp van sensoren in de openbare ruimte onder druk komen te staan. In antwoord hierop wil het college van

[1] Gemeente Amsterdam, *Stedelijk kader verwerken persoonsgegevens door de gemeente Amsterdam*, 25 september 2018.
[2] Wetenschappelijke Raad voor het Regeringsbeleid (hierna: WRR), *Opgave AI. De nieuwe systeemtechnologie* (2021) p. 428. De WRR spreekt over een 'wildgroei' van allerlei sensoren in de openbare ruimte.
[3] L. Fang, 'Debt collectors fight privacy advocates over limits for automated licence plate readers', *The Intercept* (8 mei 2015); T. Marsic en K. Bego, *When billboards stare back. How cities can reclaim the digital public space* (mei 2022), Nesta rapport; Marsic & Bego wijzen er in hun rapport op ook in de openbare ruimte van Amsterdam een incassobedrijf actief was dat ANPR gebruikte om wanbetalers met behulp van kentekens op te traceren.
[4] De gemeente Amsterdam heeft deze vorm van (heimelijk) cameragebruik in reclameschermen in 2017 verboden, zie Raadsbesluit van 18 december 2017 van de gemeente Amsterdam waarin Amendementen 1121 en 1122 bij het Programma van Eisen inzake reclame in het metronetwerk werden aangenomen en waarbij werd besloten dat de installatie en het gebruik van camera's, sensoren en andere apparaten die op enige wijze inbreuk kunnen maken op de privacy van reizigers bij reclame-uitingen niet is toegestaan.
[5] E. Baumer, 'Toward human-centred algorithm design' (2017) *Big Data & Society* 4(2), p. 1.
[6] Groep Gegevensbescherming Artikel 29, Advies 1/2015 over vraagstukken betreffende privacy en gegevensbescherming in verband met het gebruik van drones' (WP 231 van 16 juni 2015); M. Heezen, D. Louwers en E. Riestra, *Smart City? Graag. Maar dan wel met bewuste burgers!* Rapport Platform 31 (Den Haag, juni 2018); Marsic & Bego 2022.

burgemeester en wethouders van de gemeente Amsterdam de fundamentele rechten van personen op wie de private sensorgegevens betrekking hebben, beter beschermen.
Dezelfde verzameling van sensorgegevens door private partijen in de openbare ruimte moet volgens het Amsterdamse college van burgemeester en wethouders zoveel mogelijk dienstbaar zijn aan degenen op wie de gegevens betrekking hebben. Deze personen zouden volgens het college meer zeggenschap moeten krijgen over gegevensverzamelingen die op hen betrekking hebben.[7] In deze context ziet de gemeente[8] gegevensverwerking door private partijen met behulp van sensoren in de openbare ruimte dan ook niet enkel als een bedreiging. Private sensoren en de gegevens die daarmee worden gegenereerd kunnen volgens haar ook dienstbaar zijn aan de stad, omdat ze inzichten kunnen bieden die behulpzaam kunnen zijn bij de uitvoering van haar publieke taken. In de interviews met gemeentemedewerkers die in het kader van dit rapport werden afgenomen, werden concrete voorbeelden genoemd van situaties waarin B2G-gegevensdeling ten behoeve van publieke taken waarbij bereikbaarheid, fysieke veiligheid, leefbaarheid en comfort een rol spelen, erg nuttig zou kunnen zijn.

> Gemeentelijke crowdmanagers gaven aan dat een integraal beeld van bezoekersstromen essentieel is voor het treffen van adequate maatregelen om de (toenemende) drukte in de stad te kunnen monitoren en te beheersen. Naast informatie uit de eigen bronnen, waaronder het Crowd Monitoring Systeem Amsterdam is er ook een behoefte aan aanvullende informatie van bijvoorbeeld openbaar vervoerders (over de in- en uitstroom van en naar stations), digitale reis- en routeplanners en andere partijen die druktegegevens over de openbare ruimte verzamelen.[9] Medewerkers op het gebied van Smart Mobility wezen op hun beurt op de waarde van gebruikersgegevens van deelvervoerplatforms. Wanneer de gemeente immers weet waar veelvuldig gebruik wordt gemaakt van deelvervoer, kan zij strategische stallingsplaatsen bouwen en autoluwe straten creëren. Gegevensdeling kan volgens de gemeente ook meerdere kanten op werken: zo ontvangt de gemeentelijke verkeerscentrale gegevens van de navigatie-app Waze over verwachte files en ongelukken en wordt informatie van de verkeersleiding over weg- en tunnelafsluitingen weer gedeeld met Waze.[10] Ten slotte ziet de gemeente kansen in het delen van private sensorgegevens met andere (derde) private partijen die professioneel actief zijn binnen de gemeentegrenzen en die de sensorgegevens kunnen gebruiken ter verbetering van hun producten en/of diensten (innovatie).

Verder kunnen de met private sensoren gegenereerde gegevens de gemeente helpen bij het sneller bepalen welke schaarse publieke middelen op welke plaats moeten worden ingezet. Daarnaast kunnen deze gegevens volgens de gemeente, wanneer zij deze deelt met partijen die professioneel of commercieel actief zijn in de stad, dienstbaar zijn aan innovatie binnen de gemeente.[11]

Waardevolle gegevens over het gedrag van personen in de openbare ruimte zijn veelal in handen van commerciële bedrijven, die vaak meer weten over openbare ruimten dan de gemeente zelf. Google, TomTom, parkeergarages of winkeliers met camera's aan de buitenmuur die (deels) gericht zijn op de openbare ruimte weten bijvoorbeeld hoe druk het op bepaalde plaatsen is, terwijl vervoersbedrijven een indicatie kunnen geven van aantallen passagiers die onderweg zijn naar of in de stad.[12]

Informatie over de mate waarin en de wijze waarop bedrijven hun sensorgegevens over menselijk gedrag in de openbare ruimte verzamelen en verwerken, en/of hun informatie delen met de gemeente, is op dit moment beperkt. Dat kan problematisch zijn, omdat burgers belang hebben bij kennis over de redenen waarom de sensorgegevens met betrekking tot bijvoorbeeld hun gedrag worden verzameld of

[7] Tada-principes Gemeente Amsterdam, zie https://www.amsterdam.nl/innovatie/digitalisering-technologie/data/tada-waarden/ en zie *Datastrategie Gemeente Amsterdam. Amsterdamse zelfbeschikking over data 2021 – 2022* (januari 2021), p. 12.
[8] Met 'gemeente' bedoelen we, afhankelijk van de bevoegdheidstoebedeling, het college van burgemeester en wethouders, de gemeenteraad of de publiekrechtelijke rechtspersoon.
[9] Voor haar webapplicatie druktebeeld.amsterdam.nl koopt de gemeente geaggregeerde locatiegegevens in van Resono, een partij die mobiele locatiegegevens van verschillende apps ontvangt in het geval gebruikers van de apps toestemming hebben gegeven dat die gegevens met derden (Resono) worden gedeeld.
[10] https://smartmobilitymra.nl/gemeente-amsterdam-google-maps-waze/
[11] Datastrategie gemeente Amsterdam. Amsterdamse Zelfbeschikking over data 2021 – 2022, p. 18.
[12] Datastrategie Gemeente Amsterdam, p. 18.

omdat de gemeente met meer accurate informatie over de openbare ruimte beter geïnformeerde beleidskeuzes kan maken. Informatie verkregen uit gegevens vertegenwoordigt economische waarde. Kennis over gegevens geeft organisaties doorgaans macht en controle over die economische waarde, met name wanneer de gegevens en informatie daarover in exclusief bezit van een organisatie blijven. Daarnaast stelt kennis over en het (exclusieve) bezit van gegevens organisaties in staat het gedrag van personen en organisaties te beïnvloeden. Omdat het (exclusieve) bezit van en kennis over gegevens organisaties een machtspositie geven, lijken veel bedrijven tot op heden niet zomaar bereid hun gegevens ter beschikking te stellen voor (her)gebruik door de lokale overheid en/of voor verdere verwerking door andere (private) partijen.[13]

Gemeenten kunnen bedrijven en andere organisaties met hun bestuurlijke instrumentarium niet zonder meer dwingen tot het afstaan van gegevens. Vaak staan juridisch beschermde rechten van bedrijven en personen wier gegevens het betreft in de weg aan gegevensdeling met de gemeente. Zo kunnen persoonsgegevens of gegevens waar handelsgeheimen of intellectuele eigendomsrechten op rusten door private partijen niet zomaar worden gedeeld met anderen. Grotere gegevensbestanden zijn doorgaans kostbaar, omdat deze van grote economische waarde kunnen zijn en omdat er kosten verbonden zijn aan de verwerkingsslag die nodig is voordat de gegevens bruikbaar zijn voor de gemeente.[14] Het alternatief voor informatieverkrijging via B2G-gegevensdeling[15] zou zijn dat gemeenten meer eigen sensoren in de openbare ruimte installeren. Hiervoor is echter expertise en dure of specialistische apparatuur en kennis nodig.[16] De gemeente vraagt zich gelet op deze beperkingen af in hoeverre zij op basis van het bestaande, haar toebedeelde juridisch instrumentarium kan bewerkstelligen dat gegevens van private partijen via B2G-gegevensdeling[17] toegankelijk en bruikbaar kunnen worden gemaakt voor de gemeente (en voor andere professionele partijen die actief zijn in de gemeente). Daarbij plaatsen wij overigens uitdrukkelijk de kanttekening dat de gemeente niet uit is op toegang tot alle private sensorgegevens die in de openbare ruimte worden vergaard.

In dit rapport wordt geïnventariseerd welke juridische instrumenten (zoals overeenkomsten, subsidies, vergunningen en gemeentelijke verordeningen) de gemeente tot haar beschikking heeft om de fundamentele rechten van burgers meer effectief te beschermen tegen de verzameling van gegevens in en over openbare ruimten met behulp van sensoren, die worden beheerd en gecontroleerd door private actoren.[18] Daarnaast wordt geïnventariseerd welke juridische instrumenten de gemeente zou kunnen inzetten om toegang te verkrijgen tot en gebruik te kunnen maken van (informatie geëxtraheerd uit) private sensorgegevens, zodat de gemeente haar publieke taken meer *evidence-based* en efficiënter kan uitvoeren[19] of zodat zij die informatie kan delen met andere professionele partijen die actief zijn binnen de gemeente ten behoeve van het aanjagen van innovatie. Overigens moet worden afgewacht of de gemeente de verwachting van beter geïnformeerd beleid op basis van de verkregen informatie daadwerkelijk kan waarmaken.[20]

---

[13] Dit werd bevestigd in de interviews met diverse medewerkers bij bedrijven en bij de gemeente. Zie ook hoofdstuk 2.

[14] M. Heezen, D. Louwerse en E. Riedstra (Platform 31) *Smart city? Graag. Maar dan wel met bewuste burgers!* Rapport juni 2018, p. 22.

[15] High-Level Expert group on Business-to-Government Data Sharing. Europese Commissie Towards a European Strategy on Business-to Government Data Sharing for the Public Interest. Final report (2020), HEC Paris Research Paper, No. LAW-2020-1394.

[16] Idem, p. 17-18.

[17] High-Level Expert Group on Business-to-Government Data Sharing European Commission, *Towards a European Strategy on Business-To-Government Data Sharing for the Public Interest*. Final report (2020), HEC Paris Research Paper No. LAW-2020-1394.

[18] Zie voor typen sensoren §1.5.3.

[19] Geonovum. *Verkenning Publiek Gebruik Data van Derden* (rapport, 27 mei 2021).

[20] Dit rapport laat verder in het midden of de gemeente daarin slaagt of zal slagen. Over de legitimiteit van het sturen met gegevens door publieke actoren in het algemeen wordt thans veel discussie gevoerd, zie onder meer Raad voor het Openbaar Bestuur, *Sturen of gestuurd worden? Over de legitimiteit van sturen met data*, Adviesrapport (mei 2021); M. Bovens & S. Zouridis, 'From street-level to system-level bureaucracies: How information and communication technology is transforming administrative discretion and constitutional control' (2002) *Public Administration Review* 62(2) 174; M. Veale & I. Brass, Administration by algorithm? Public management meets public sector machine learning. In: M. Veale & I. Brass

1.2 Onderzoeksvraag

Teneinde de hiervoor geschetste problematiek te analyseren, hebben wij de volgende hoofdonderzoeksvraag en deelvragen geformuleerd:

> Wat zijn voor de gemeente Amsterdam de juridische mogelijkheden om ten aanzien van de verzameling en het gebruik van gegevens (waaronder persoonsgegevens) die worden vergaard met behulp van sensoren door private partijen in de openbare ruimte, aanvullende voorwaarden te stellen? Dit met het oog op:
>
> > deelvraag (i) het beter beschermen van de fundamentele rechten van personen op wie de private sensorgegevens betrekking hebben; en
> >
> > deelvraag (ii) het belang van de gemeente om ten behoeve van de uitvoering van haar publieke taken – en in het verlengde daarvan, het belang van andere in de stad opererende organisaties, zoals private onderzoeksinstellingen of ondernemers actief binnen de gemeente – toegang te verkrijgen tot (informatie over) sensorgegevens die door private partijen werden verkregen in de openbare ruimte, opdat zij die gegevens kunnen gebruiken voor de verwezenlijking van publieke doeleinden.

De deelvragen brengen een zeker spanningsveld met zich mee. Enerzijds wil de gemeente de fundamentele rechten van burgers beter beschermen tegen de verzameling van sensorgegevens door private partijen, terwijl de wens van de gemeente om in bepaalde gevallen toegang te krijgen tot private sensorgegevens de fundamentele rechten van burgers mogelijk kan raken. Gemeentelijke verwerking kan daarnaast mogelijk nadelige gevolgen hebben voor de rechten en belangen van private partijen wier sensorgegevens door de gemeente mogelijk zouden worden gedeeld met andere bedrijven en organisaties die actief zijn binnen de gemeente. Het verder delen kan immers risico's voor de bedrijfsgeheimen of intellectuele eigendomsrechten (die tevens worden aangemerkt als fundamentele rechten in het EU-Handvest) met zich meebrengen voor de partijen die deze gegevens bezitten.[21]

1.3 Doelstelling, opzet en reikwijdte

Het doel van het rapport is het inventariseren van het juridisch kader met betrekking tot (i) het handelingsperspectief van de gemeente voor een (betere) borging van fundamentele rechten in de openbare ruimte, en (ii) voor de gemeentelijke vraag om in voorkomende gevallen toegang te verkrijgen tot de door private partijen in de openbare ruimte verzamelde sensorgegevens. Dit rapport inventariseert welke juridische knelpunten en kansen zich voordoen bij beide gemeentelijke handelingsperspectieven. Tot slot voorziet het rapport in inventariserende adviezen, die de gemeente kan benutten bij verdere beleidsontwikkeling.

Voor de beantwoording van de tweeledige onderzoeksvraag hanteren wij de volgende opzet. We duiden in hoofdstuk 2 de politiek-economische achtergrond bij het handelingsperspectief van de gemeente in relatie tot de verwerking van sensorgegevens door private partijen in de openbare ruimte. Hierbij brengen we discussies in kaart over de rol van de gemeente als actor in de openbare ruimte en geven we een typologie van vaker voorkomende relaties waarbinnen de gemeente te maken kan krijgen met private partijen die sensorgegevens verzamelen in de openbare ruimte. In hoofdstuk 3 inventariseren we het relevante juridisch kader met het oog op de beantwoording van de tweeledige onderzoeksvraag. Hier behandelen wij

(Eds.), *Algorithmic regulation*. Oxford University Press: 2019; J. Cobbe, M. Seng Ah Lee, H. Janssen, J. Singh, 'Centering the rule of law in the digital state, (2020) IEEE *Computer* 53 (10); B. Bodo & H. Janssen, Maintaining trust in a technologized public sector (2022) *Policy & Society* 41(3).

[21] Art. 16 EU-Handvest, zie ook §3.2.1.

achtereenvolgens het juridisch kader dat geldt voor private partijen die met sensoren informatie over menselijk gedrag in de openbare ruimte verzamelen (§3.1), het juridisch kader dat de gemeentelijke bevoegdheden en verplichtingen reguleert (§3.2) en het kader dat het bestuurlijke instrumentarium voor de gemeente regelt (§3.3). In §3.2 bespreken we per wet wat deze betekent voor het handelingsperspectief van de gemeente met het oog op een betere borging van de fundamentele rechten (deelvraag 1) en wat deze betekent voor het verkrijgen van toegang tot private sensorgegevens en het verder delen van deze informatie met derden (deelvraag 2). In hoofdstuk 4 presenteren we op basis van de bevindingen in hoofdstuk 2 en 3 de mogelijkheden en de beperkingen die het huidige juridisch kader biedt bij de beantwoording van deelvragen 1 en 2.

Het wettelijk kader dat in dit rapport wordt behandeld, betreft een inventarisatie van de toepasselijke horizontale wetgeving, oftewel wetgeving die niet sectorspecifiek is. Wel zijn enkele voorbeelden uit specifieke wetgeving ter verduidelijking opgenomen. Wat betreft de reikwijdte ziet het onderzoek op gegevens over niet-identificeerbare personen en op persoonsgegevens zoals gedefinieerd in de AVG. Het onderzoek behelst niet de sensoren die door de gemeente zelf zijn geïnstalleerd.[22] Daarnaast valt het verkrijgen van toegang tot private sensorgegevens ten behoeve van gemeentelijke taken ter voorkoming, opsporing en vervolging van strafrechtelijk handelen buiten de reikwijdte van dit onderzoek. Ook bestrijkt het onderzoek niet de mogelijke commerciële activiteiten die de gemeente wil ontwikkelen of reeds uitvoert. Tot slot laten we de discussie over B2G-gegevensdeling in het kader van de naleving van de coronaregels, waarin wifi-tracking specifiek speelde, ook buiten beschouwing.

1.4 Methode

Het onderzoek is gebaseerd op een analyse van relevante wetgeving, rechtspraak en literatuur. Ten behoeve van het onderzoek werd een workshop georganiseerd, waarin de toetsing van de volledigheid en de juiste duiding van het juridisch kader centraal stond.[23] Voor de beantwoording van de vraag naar de inzet van gemeentelijke bevoegdheden en bestuurlijke instrumenten ten behoeve van B2G-gegevensdeling, is naast de analyse van juridische bronnen om meerdere redenen gekozen voor een empirische benadering. Allereerst is in de juridische academische literatuur een dergelijke empirische analyse met betrekking tot deze vragen bij ons beste weten niet eerder verricht.[24] Daarnaast wordt steeds vaker gewezen op de noodzaak van meer empirische analyses van bestuursmechanismen, institutionele regelingen en relaties tussen publieke en private actoren.[25] Tot slot is B2G-gegevensdeling een recent maar snel evoluerend fenomeen, waardoor kennis, informatie en ervaring uit de praktijk noodzakelijk zijn om de dynamiek van dit fenomeen beter te kunnen volgen en duiden. Deze empirische benadering helpt de juridische praktijk bij het – zo nodig – (adviseren over) de ontwikkeling van regulering.

In het licht van de empirische benadering zijn kwalitatieve semigestructureerde interviews afgenomen met gemeentemedewerkers en bedrijfsmedewerkers.[26] De geïnterviewden zijn (deels) actief op het terrein van mobiliteit in de gemeente Amsterdam. De keuze voor deze sector ligt voor de hand, omdat mobiliteit bij uitstek in de openbare ruimte plaatsvindt. Daarnaast gaf de gemeente vanwege haar verantwoordelijkheid voor de inrichting en het beheer van de openbare ruimte en de dynamiek in deze

[22] *Monitoring in de openbare ruimte* (20 juni 2019), onderzoeksrapport Price Waterhouse Coopers in opdracht van de Commissie Persoonsgegevens Amsterdam.
[23] Deze workshop vond plaats op 13 april 2022 bij het Instituut voor Informatierecht. Hiervoor werden juridische experts uit wetenschap en praktijk uitgenodigd van de gemeenten Amsterdam en Eindhoven, het ministerie van Justitie en Veiligheid, de AP en de Vereniging van Nederlandse Gemeenten (hierna: VNG).
[24] Recentelijk deden Marsic & Bego (2022, Nesta-rapoprt) hier onderzoek naar, maar dat onderzoek is niet gebaseerd op juridische onderzoeksmethoden.
[25] G. Nesti, 'Defining and assessing the transformational nature o smart city governance: insights from four European cases', (2020) *International Review of Administrative Sciences* 30; A. Voorwinden, Regulating the Smart city in European municipalities: a case study of Amsterdam' (2022) *European Public Law* p. 155 e.v.
[26] Zie de Bijlage bij dit rapport.

sector de voorkeur aan een focus op deze sector. Voor semigestructureerde interviews is gekozen zodat ruimte bestond voor de geïnterviewden om inzichten en knelpunten vanuit hun eigen ervaringen naar voren te brengen. De interviews zijn gecombineerd met wetgeving en bevindingen uit de literatuur, om te begrijpen hoe gemeente- en bedrijfsmedewerkers situaties waarin B2G-gegevensuitwisseling wordt onderzocht of uitgevoerd waarderen en waar zij eventuele (juridische) knelpunten en/of kansen voor B2G-gegevensdeling zien. Zowel de gemeentemedewerkers als de bedrijfsmedewerkers werden elk vanuit hun eigen rol en taak bevraagd over een of beide deelvragen en over de geldende juridische randvoorwaarden.[27]

Dit onderzoek geeft een momentopname weer van de juridische mogelijkheden en beperkingen met betrekking tot het delen van private sensorgegevens in B2G-verhoudingen. We verschaffen met de interviews inzicht in een gebied waar de kennis over de toepassing van het bestaande juridisch kader op dit moment nog beperkt is. De keuze voor een specifieke sector hangt samen met het inventariserend karakter van het onderzoek, al tekenen wij hierbij aan dat de problematiek die in dit onderzoek centraal staat, ook kan spelen in andere sectoren. De mobiliteitssector fungeert in dit onderzoek als voorbeeld en als vehikel om het algemene juridisch kader bij B2G-gegevensdeling nader te illustreren. Aangezien de geïnterviewden mede zijn geselecteerd door de opdrachtgever is een selectiebias aanwezig. Desalniettemin beschouwen we de bevindingen van deze interviews als actueel, relevant en indicatief voor de uitdagingen waarmee de gemeente bij B2G-gegevensdeling te maken zal krijgen.

Het onderzoek werd afgesloten op 30 december 2022.

1.5 Termen

In dit onderzoek gebruiken we een aantal termen die we hier toelichten en die verderop in het rapport waar nodig nader worden uitgediept.

1.5.1 Openbare ruimte

Het op juiste wijze duiden van een 'ruimte' of 'plaats' is van belang, omdat de duiding gevolgen heeft voor de gemeentelijke bevoegdheden de betreffende plaatsen te reguleren. Bij de duiding van een openbare ruimte of plaats wordt uitgegaan van de feitelijke omstandigheden. Gemeenten zijn verantwoordelijk voor de inrichting en het beheer van *openbare plaatsen*.[28] Dit komt onder meer tot uitdrukking in de Gemeentewet,[29] in sectorale wetgeving[30] en in de rechtspraak.[31] De definitie van openbare plaats volgens de Wet openbare manifestaties (Wom) luidt: een plaats die krachtens bestemming of vast gebruik openstaat voor het publiek.[32]

---

[27] De ervaringen die uit de interviews naar voren kwamen, zijn op basis van anonimiteit verwerkt in het juridisch kader en in de aanbevelingen. De onderliggende, uitgewerkte interviews worden in geanonimiseerde vorm bewaard binnen de Universiteit van Amsterdam.

[28] 'Plaats' wordt ruim geïnterpreteerd en omvat ook buitenruimten, gebouwen, bijbehorende erven, afzonderlijke ruimten in gebouwen: zie A.E. van Rooij, *Orde in het semi-publieke domein: particuliere en publiek-private orderegulering in juridisch perspectief* (diss. Amsterdam VU), Den Haag: Boom juridisch 2017, p. 55.

[29] Zie bijvoorbeeld artt. 151c (gemeente kan camera's inzetten in openbare ruimte en bij verordening aan te wijzen plaatsen die voor eenieder toegankelijk zijn); 154b lid 1 (boetes voor overlast in de openbare ruimte); 160 lid 1 (algemene bevoegdheden van het college); 172 (bevoegdheden burgemeester); 174 lid 1 (De burgemeester is belast met het toezicht op de openbare samenkomsten en vermakelijkheden, alsmede op de voor het publiek openstaande gebouwen en daarbij behorende erven) Gemeentewet.

[30] Zie bijvoorbeeld de Wegenwet 1930, de Woningwet 1991 en art. 6:174 lid 1, 2 en 6 BW, die de gemeente Amsterdam aanwijzen als verantwoordelijke voor de gemeentelijke bruggen op haar grondgebied (Beheer en onderhoud bruggen, Rapport Rekenkamer Amsterdam (oktober 2015), p. 9).

[31] Bijv. Gerechtshof 's-Hertogenbosch 28 maart 2017, ECLI:NL:GHSHE:2017:1534, r.o. 5.3.5.

[32] Hierbij valt te denken aan wegen en pleinen die voor eenieder vrij toegankelijk zijn en aan plaatsen die een met de weg vergelijkbare functie vervullen zoals "openbare plantsoenen, speelweiden, parken, en de voor eenieder vrij toegankelijke gedeelten van overdekte passages, winkelgalerijen, stationshallen en van vliegvelden", zie *Kamerstukken II* 1985/86, 19427, nr. 3, 15-16. Deze definitie sluit ook aan bij de definitie in art. 1 sub j Wet basisregistratie adressen en gebouwen.

Naast openbare plaatsen wordt in de Gemeentewet gewezen op *voor het publiek toegankelijke plaatsen*. Dit zijn ruimten of gebouwen met een bepaalde bestemming of functie waarvan de toegang openstaat voor eenieder die er conform de bestemming (of functie) gebruik van wil maken.[33] De beheerder van een voor het publiek toegankelijke plaats kan voorwaarden aan de toegang of het gebruik van de plaats verbinden, zoals het geval is bij voetbalstadions, musea, winkels, ziekenhuizen, bibliotheken en trein- en metrostations.[34] Het beheer van de voor het publiek toegankelijke plaats kan in handen zijn van een publieke actor (zoals bij een universiteitsgebouw of het stadhuis) of een private partij (zoals bij horeca, winkels of voetbalstadions).[35] In eerste instantie is de beheerder van de voor het publiek toegankelijke plaats verantwoordelijk voor de handhaving van de orde. Daarmee is de burgemeester niet verantwoordelijk voor de handhaving van de openbare orde, maar is hij wel belast met het toezicht op die plaats.[36] Wordt de openbare orde op een dergelijke plaats verstoord, dan kan de burgemeester aldus bevelen geven met het oog op bijvoorbeeld het borgen van de fysieke veiligheid en/of de verkeersveiligheid en gezondheid van bezoekers.[37] Een bijzondere wet kan op de toezichthoudende bevoegdheid van de burgemeester echter een uitzonderingen maken, zoals met betrekking tot de aanpak van overlast in het openbaar vervoer, waar het toezicht op en handhaving van de openbare orde is neergelegd bij de vervoerder.[38]

De duiding van openbare plaatsen is overigens niet statisch. Soms kunnen feitelijk omstandigheden wijzigen, waardoor een plaats van karakter kan veranderen, zoals gebeurde bij de plaatsing van toegangspoortjes bij trein- en metrostations in 2015. Vanwege deze 'feitelijke beletselen' in de openbare ruimte vallen delen van trein- en metrostations nu binnen de categorie "voor het publiek toegankelijke plaatsen".[39]

De plaats als openbare ruimte of als een voor het publiek toegankelijke plaats kunnen in de praktijk niet altijd geheel los van elkaar worden gezien; soms vertonen deze plaatsen een logische verbondenheid. Gegevensverwerkingen met private sensoren in voor het publiek toegankelijke ruimte kunnen relevant zijn voor het gemeentelijk beheer en inrichting van de openbare ruimte. Kennis over aantallen voetbalfans en de wijze waarop zij een stadion gaan verlaten (een voor het publiek toegankelijk plaats, die wordt beheerd door een private partij), kan van grote betekenis zijn voor de inzet van gemeentelijke bevoegdheden in de openbare ruimte rondom het stadion. Kennis van reizigersaantallen op de perrons van ProRail – een voor het publiek toegankelijke ruimte – kunnen de gemeente informeren over aantallen die reizigers zich even later zullen bevinden in de openbare ruimte – het domein van de gemeente.[40] In dit rapport bespreken wij in beginsel de verwerking van sensorgegevens van private partijen in de openbare ruimte; in voorkomende gevallen zullen we vraagstukken rondom de verbondendheid van de twee typen plaatsen signaleren.

Van openbare plaatsen en voor het publiek toegankelijke plaatsen zijn tot slot *besloten plaatsen* te onderscheiden. Hier staan toegang en gebruik alleen open voor rechthebbenden en specifieke personen die toestemming hebben gekregen van rechthebbenden. Deze plaatsen zijn in het algemeen onder te verdelen

[33] In de zin van art. 174 lid 1 Gemeentewet, *Kamerstukken II* 2000/01, 27732, nr. 3, p. 4-5.
[34] Rechtbank Amsterdam 4 september 2014, ECLI:NL:RBAMS:2014:5688, r.o. 4.2.
[35] In die gevallen wordt toegang verkregen tegen betaling, vanaf een bepaalde leeftijd, het tonen van en identiteitsbewijs of toegangspas, of worden beperkte openingstijden of doelgebonden gebruik van de plaats door de beheerder opgelegd, zie W. Bantema, 'De locale Facebookpagina als café. Een discussie over het bestaan van publieke plaatsen op het internet en de regulering daarvan', (2020) *Bestuurswetenschappen* 74(2) p. 94.
[36] Art. 174 (1) Gemeentewet
[37] Zo wilde Greenpeace demonstreren in een voor het publiek toegankelijke plaats op Schiphol, hetgeen om veiligheidsredenen werd verboden door de burgemeester van Schiphol (onterecht, zo bleek later, zie Rechtbank Noord-Holland, ECLI:NL:RBNHO:2022:3696).
[38] Zie Wp en *Kamerstukken I* 2009/10, 31467, C, 14.
[39] *Kamerstukken II* 2014/15, 28642, nr. 65, p. 2–3; Van Rooij 2017, p. 179, 190.
[40] Perrons en trein- en metrostations werden in interviews met gemeentemedewerkers ook wel 'de toegangspoorten tot de stad en de openbare ruimte' genoemd. De perrons in de treinstations worden beheerd door ProRail, een private rechtspersoon, al is op dit moment wetgeving aanhangig waarin wordt voorgesteld ProRail de status van zelfstanding bestuursorgaan toe te kennen, waarmee het een bestuursorgaan wordt (zie Wijziging van de Spoorwegwet en enige andere wetten in verband met de omvorming van ProRail van een besloten vennootschap tot een publiekrechtelijk zelfstandig bestuursorgaan, Wet publiekrechtelijke omvorming ProRail, Kamerstukken II, 35 396, nrs 2 en 3).

in woningen en overige niet voor het publiek toegankelijke plaatsen,[41] zoals scholen of kantoren.[42] Een private sensor in een reclamescherm in een kantoorpand bevindt zich dus niet in de openbare ruimte of in een voor het publiek toegankelijke ruimte.

1.5.2 Gedigitaliseerde openbare ruimte

Bij de duiding van de openbare plaats is de wetgever uitgegaan van de fysieke openbare ruimte. Wet- en regelgeving garanderen bepaalde vrijheden en beperken bepaalde soorten activiteiten in die fysieke openbare ruimte. Tegelijkertijd zien we dat de term 'digitale openbare ruimte' in beleidsrapporten opduikt. Deze wordt daarin veelal opgevat als een fysieke plaats waarin digitale infrastructuren en technologieën (zoals sensoren, apps of glasvezelkabels) menselijk gedrag in die fysieke openbare ruimte waarnemen of beïnvloeden en waarin dat gedrag voortdurend worden teruggekoppeld naar digitale infrastructuren.[43]

In dit rapport gaan we uit van de aanname dat er niet zoiets als een met de fysieke openbare ruimte vergelijkbare digitale openbare ruimte bestaat, maar we aanvaarden wel dat fysieke openbare plaatsen een digitale component kunnen hebben.[44] De term 'digitale openbare ruimte' is immers niet wettelijk gedefinieerd. Onduidelijk is bijvoorbeeld of een dergelijke ruimte anders is dan de enkele fysieke ruimte, wat de fysieke begrenzingen van een digitale openbare ruimte zouden moeten zijn en of aan het digitale aspect specifieke juridische gevolgen zouden moeten worden verbonden.[45] Tegelijkertijd zien we dat in fysieke ruimten steeds vaker digitale middelen worden gebruikt die kunnen raken aan de rechten, belangen en bevoegdheden van eenieder die zich op die plaats bevindt.[46] Omdat we deze realiteit onderkennen, maar niet erkennen dat een met de juridische fysieke openbare ruimte vergelijkbare 'digitale openbare ruimte' bestaat, gebruiken we in dit rapport zo nodig de term *gedigitaliseerde openbare ruimte*. Met deze term bedoelen wij een fysieke ruimte waarin zich digitale componenten kunnen bevinden.

1.5.3 Sensoren

Sensoren maken veelal deel uit van het *Internet of Things* (hierna: IoT) – het verschijnsel waarbij 'gewone' objecten en apparaten, niet zijnde traditionele computers, worden aangesloten op het internet.[47] Een sensor detecteert fysieke prikkels zoals beweging, hitte, geluid, druk of de nabijheid van personen, die worden omgezet naar machineleesbare – en voor mensen interpreteerbare – informatie.[48] De gemeente Amsterdam definieert in haar recent ingevoerde meldingsplicht voor sensoren een sensor als "een kunstmatig zintuig dat wordt ingezet of kan worden ingezet om waarnemingen te doen en deze digitaal te verwerken of laten

[41] Bantema 2020, p. 94.
[42] Conclusie Procureur-Generaal 7 november 2017, ECLI:NL:PHR:2017:1407, r.o. 4.18-4.19.
[43] Kool et al. stellen dat "Steeds meer onderdelen uit de fysieke wereld krijgen een virtuele representatie. Daardoor ontstaat op steeds meer plekken een continue terugkoppeling tussen de fysieke en virtuele wereld, waarmee producten of diensten direct worden aangepast op basis van analyse van digitale gegevens", L. Kool, J. Timmer, L. Royakkers, R. Van Est. *Opwaarderen. Borgen van publieke belangen in de digitale samenleving*. Den Haag, Rathenau Instituut 2017, p. 8; zie ook VNG, *Principes voor de digitale samenleving*. Deel 1 De digitale openbare ruimte (2020) p. 7; Digitale Infrastructuur Amsterdam (DI020), zie https://openresearch.amsterdam/nl/page/34950/digitale-infrastructuur-amsterdam.di020, bezocht op 23 december 2022; Code Future Internet Lab, *Digitisation of the physical public space* (Waag Society 15 mei 2021).
[44] Zo ook S. van der Waal et al., *European Digital Spaces*. Waag Technology & Society 2020 https://culturalfoundation.eu/wp-content/uploads/2021/05/Waag-Report-on-European-Digital-Public-Spaces.pdf, bezocht op 27 juni 2022.
[45] Voor onderzoek naar de fysieke en de digitale componenten in de openbare ruimte en de verhouding tussen beide typeringen in het kader van strafvorderlijke taken van de gemeente, zie bijvoorbeeld onder meer G. Ritsema van Eck, *Privacy and participation in public data protection issues of crowdsourced surveillance*' (diss. RUG 2021).
[46] Dit sluit aan bij de VNG *Principes voor de digitale samenleving*, 2020, p. 7.
[47] Gartner IT Glossary, https://www.gartner.com/it-glossary/Internet-of-Things.
[48] International Telecommunication Union, pp. 20 – 27.

verwerken".[49] Sensoren verzamelen informatie en zijn veelal gericht op personen en/of zaken en verwerken daarover gegevens.[50]

Voorbeelden van sensoren die zich in de openbare ruimte (kunnen) bevinden zijn mobiele telefoons (als primaire digitale infrastructuur voor private partijen waarop zij in toenemende mate leunen om informatie in en over de openbare ruimte te verzamelen); wifi-signaalmeters (passantentellingen en loopstromen); optische sensoren, al dan niet met gezichtsherkenningstechnologie (camera's); sensoren in digitale reclameborden (camera's, bewegingssensoren, warmtesensoren, glasbreuksensoren); in het wegdek aangebrachte sensoren (voor het meten van verkeersstromen, gladheid, gewicht en snelheden van passerende voertuigen); sensoren die geluid, trillingen en meteorologische indicatoren meten; sensoren die luchtkwaliteit meten; en sensoren die het in- en uitchecken van reizigers in het openbaar vervoer registreren.

Sensoren kunnen vast verbonden zijn aan of in een object, zoals het geval is bij camera's in digitale reclameschermen en winkelpanden, bij in- en uitcheckpunten van de NS of camera's op metroperrons. Sensoren kunnen ook dynamisch oftewel mobiel zijn. Binnen het spectrum van mobiele sensoren kan een onderscheid worden gemaakt tussen (i) (bewegende) sensoren die (mede) tot doel hebben informatie te verzamelen in en over de openbare ruimte (zoals bij drones het geval is),[51] en (ii) sensoren die met behulp van apps op mobiele telefoons van gebruikers informatie verzamelen met een directe link en doel naar de openbare ruimte. Dit is bijvoorbeeld het geval bij Uber, Google Maps of sommige deelscooters (Felyx, Check), die via de mobiele telefoon van de gebruiker informatie verzamelen over de gebruiker en de openbare ruimte waarin de gebruiker zich bevindt. Daarnaast kunnen nog sensoren worden onderscheiden die met behulp van apps op mobiele telefoons informatie verzamelen over de gebruiker, zonder dat daarmee wordt beoogd informatie in of over de openbare ruimte te verzamelen (bijvoorbeeld Airbnb, Booking.com en wasmachines of koelkasten met ingebouwde IoT-toepassingen). Gelet op het ontbreken van de link met de openbare ruimte heeft deze laatste categorie niet onze primaire belangstelling. Voor mobiele sensoren geldt dat de regels die binnen de specifieke ruimte waar de sensor zich beweegt, van toepassing zijn. Wanneer de sensor van de openbare ruimte naar een voor het publiek toegankelijke plaats of een besloten ruimte wordt verplaatst (of omgekeerd) zullen bij het verzamelen van gegevens in de betreffende ruimte mogelijk andere regels gelden met betrekking tot de rechten, bevoegdheden en verantwoordelijkheden rondom die gegevens dan in de openbare ruimte.

In dit onderzoek staan sensoren met een vast en een mobiel karakter van private partijen centraal, waarbij de private gegevensverzameling een directe link heeft met de openbare ruimte.

[49] Zie Verordening van de raad van de gemeente Amsterdam tot wijziging van de Algemene Plaatselijke Verordening 2008 in verband met het invoeren van een meldingsplicht voor sensoren (Verordening meldingsplicht sensoren), Gemeenteblad 2021, 368183 (gepubliceerd op 20 oktober 2021, inwerking getreden op 1 december 2021).

[50] *Principes voor de digitale samenleving. Deel 1. De digitale openbare ruimte*, VNG 2019, p. 12. Voorbeelden van mobiele sensoren zijn sensoren die aan auto's zijn bevestigd, zoals de gemeentelijke scanauto's die controleren of parkeergelden zijn betaald; voorbeelden van vaste sensoren zijn camera's of geluidssensoren die op of aan gebouwen of constructies (bruggen) zijn bevestigd.

[51] Zo laat Apple laat de openbare ruimte scannen voor bepaalde doeleinden; de sensoren bevinden zich in dit geval in rugtassen van medewerkers die zich door de openbare ruimte bewegen. Zie https://maps.apple.com/imagecollection/.

2 De gemeente als kaderstellende partij in de openbare ruimte

In dit hoofdstuk bespreken we enkele in het oog springende ontwikkelingen die van invloed zijn op het gemeentelijk handelingsperspectief met betrekking tot het beheer en de inrichting van de (gedigitaliseerde) openbare ruimte. We bespreken dit handelingsperspectief tegen de achtergrond van de verwerking van sensorgegevens door private partijen in de openbare ruimte. Daarnaast brengen we discussies in kaart over de rol van de gemeente als kaderstellende partij in de gedigitaliseerde openbare ruimte in relatie tot private actoren en in haar regulerende rol in verhouding tot de nationale wetgever en de EU-wetgever. Tot slot geven we een typologie van relaties waarbinnen de gemeente te maken kan krijgen met de verwerking van sensorgegevens door private partijen.

2.1 De rol van de gemeente in de gedigitaliseerde openbare ruimte

Gemeenten zijn verantwoordelijk voor de inrichting en het beheer van openbare ruimten. Om passend beleid en regulering te ontwikkelen, heeft de gemeente informatie nodig over de openbare ruimte (en soms, zoals we zagen in §1.5.1, over aangrenzende ruimten). Met betrekking tot toegang tot en opslag van informatie over de openbare ruimte bestaan intoenemende mate verschillen tussen de gemeente en private partijen, waarbij met name grote (globaal opererende) private partijen een veel betere informatiepositie hebben weten op te bouwen dan de gemeente. Dit heeft geleid tot vragen over hoe gemeenten hun publieke taken in de openbare ruimte kunnen blijven vervullen, en meer in het algemeen, over wie de openbare ruimte nu eigenlijk beheert.[52]

2.1.1 Politiek-economische context

Allereerst zijn er diverse politiek-economische redenen de regierol van de gemeente in de openbare ruimte in het algemeen minder sterk lijkt te zijn geworden in vergelijking met de groeiende rol van private parten als het gaat om toegang tot gegevens in de openbare ruimte.[53] Gemeenten hebben in de afgelopen decennia over het algemeen een meer reactieve rol gespeeld bij het vormgeven van het beheer van gegevens en de digitale infrastructuren waarlangs gegevens worden verzameld, geanalyseerd, geaggregeerd en overgedragen.[54] Dit is onder meer een gevolg van de privatisering van diverse publieke diensten,[55] die traditioneel door de publieke sector werden vervuld.

De huidige, veelal op sensoren gebaseerde technologieën die worden ingezet in openbare ruimten worden doorgaans ontworpen en ontwikkeld door bedrijven en in mindere mate door gemeenten.[56] Daarmee definiëren en bepalen bedrijven vaak de praktische-, technische- en kennisvoorwaarden voor de gegevensverwerking en het beheer met betrekking tot waarnemingen in de openbare ruimte, hetgeen hen

[52] J. van Dijck, T. Poell en M. Janssen, *The Platform society - public values in a connected world* (Oxford University Press: 2018), p. 15.
[53] I. Susha, Å. Grönlund, en R. van Tulder, 'Data driven social partnerships: Exploring an emergent trend in search of research challenges and questions', (2019) *Government Information Quarterly* 36, 112.
[54] Met 'digitale infrastructuren' sluiten wij aan bij de invulling die de VNG geeft aan dit begrip. Volgens de VNG omvat de digitale infrastructuur die onderdelen die ter beschikking staan aan toepassingen van en voor burgers en publieke en private organisaties, inclusief de netwerkvoorzieningen, gegevensverzamelende apparaten en platformen voor toepassingen (VNG Realisatie, Principes voor de digitale samenleving. Deel 1 de Digitale openbare ruimte (oktober 2019), p. 2.
[55] J. Cobbe e.a.,. 'Centring the law in the digital state' (2020) *Computer* 48.
[56] In de gevallen waarin gemeenten zelf innoveren op dit soort technieken is dat vaak een reactie op technologieën ontworpen door bedrijven. De gemeente Amsterdam (en een aantal andere Europese steden) was eerder actief in het DECODE project dat beoogde burgers meer zeggenschap te geven over hun gegevens, zie https://decodeproject.eu, bezocht op 22 maart 2022. Zie ook C. Nevejan, City science for urban challenges, Pilot assessment and future potential of the City science Initiative 2019–2020, 46 https://ec.europa.eu/jrc/communities/en/community/city-science-initiative/document/city-science-urban-challenges-pilot-assessment-and-future bezocht op 9 augustus 2022.

feitelijke beslismacht geeft over welke gegevens worden vastgelegd, opgeslagen, geduid, geaggregeerd, overgedragen en gebruikt.[57] Het feit dat de gemeente soms een kant en klaar systeem van een private partij aankoopt en inzet in de openbare ruimte, doet daar niet aan af; deze systemen zijn doorgaans al ingericht volgens de door het bedrijf bepaalde voorwaarden.[58] Van gemeenten wordt tegelijkertijd verwacht dat zij ervoor zorgen dat ook de gedigitaliseerde openbare ruimte veilig en leefbaar blijft en dat zij de regie nemen over zorgvuldige gegevensverwerkingen in de openbare ruimte.[59]

Daarnaast heeft de structurele en grootschalige verzameling van gegevens, waaronder ook sensorgegevens, door private partijen gevolgen voor het machtsevenwicht tussen de gemeente en private partijen. Private partijen zijn zoals gezegd vaak beter dan de gemeente geïnformeerd over wat zich in de openbare ruimte afspeelt. Via netwerken, gegevensstromen en infrastructuren waarover zij veelal exclusief controle uitoefenen, hebben zij toegang tot zeer granulaire informatie over menselijk gedrag in de openbare ruimte. De gemeente heeft die informatie vaak niet, althans niet in die omvang en op dat detailniveau. De voorsprong van private partijen bij de toegang tot informatie beïnvloedt dan ook het handelingsperspectief van de gemeente; met hun sterkere informatiepositie zijn private partijen – vaker en sneller dan de gemeente – in staat te bepalen op welke manier mobiliteit vorm krijgt en/of verkeer zich beweegt maar en in de stad (Google Maps) of op welke manier een wijk wordt bewoond (AirBnB).[60]

Verder zijn private partijen vanwege hun sterke informatiepositie beter in staat eenzijdig voorwaarden te stellen aan de toegang van de gemeente tot (informatie over) gegevens die zij in hun bezit hebben.[61] Indien en voor zover bedrijven al gegevens delen, beschikken gemeenten lang niet altijd over de middelen (kennis, expertise, opslagcapaciteit, ervaring met het uitvoeren van analyses) om de ontvangen gegevens te verwerken en te gebruiken, waarvoor ze eveneens afhankelijk zijn (en blijven) van private actoren.[62]

B2G-gegevensdeling kan overigens ook gunstig uitpakken voor private partijen. Meewerken aan B2G-gegevensdeling kan bijdragen aan de kennisopbouw binnen een bedrijf over de informatiebehoeften van de gemeente, en daarnaast bijdragen aan het verwerven van zichtbaarheid en een goede reputatie bij de gemeente. Zoals gezegd geeft het bezit van gegevens private partijen exclusieve zeggenschap over wie toegang heeft tot die gegevens en over hoe de gegevens worden verwerkt, verrijkt, en/of gedeeld met derden. Andere partijen, waaronder de gemeente, hebben echter geen zicht op welke keuzes ten aanzien van de toegang of van deze gegevens en de verwerkingen ervan een private partij precies maakt. Private partijen kunnen aldus (deels) zelf beslissen welke gegevens in het kader van B2G-gegevensdeling wel en niet met de gemeente worden gedeeld. Het is voor de gemeente, die geen toegang heeft tot de gegevensopslag en het interne beheer ervan door de private partij, immers niet goed mogelijk om na te gaan of de private partij de voor de gemeente meest accurate gegevens deelt. Private partijen kunnen op deze wijze praktisch bepalen welke informatie de gemeente kan benutten voor de verwezenlijking van haar publieke taken.

---

[57] J. Mercille. Inclusive smart cities: beyond voluntary corporate data sharing (2021) *Sustainability* 8135, p. 1.

[58] Mogelijk ligt dit anders indien de gemeente een nog te bouwen systeem aankoopt en het bedrijf specifiek instrueert hoe een sensor dient te worden ontworpen en hoe deze moet functioneren. Een DPIA kan de gemeente meer zekerheid geven over de mate waarin het aan te kopen systeem de specifieke waarden herbergt die de gemeente in het systeem wil terugzien.

[59] Zie o.a. VNG-ledenbrief 1 november 2019, p. 4: "Inwoners verwachten van de overheid dat zij zelf zorgvuldig en veilig omgaat met data verzamelen en gebruik, maar ook dat zij ervoor zorgt dat anderen dit doen en daar afspraken over maakt en 'verkeersregels' voor hanteert." Zie ook de VNG *Principes voor de digitale samenleving*, p. 7.

[60] De Europese Commissie heeft recentelijk een voorstel voor een Verordening uitgebracht betreffende het verzamelen en delen van gegevens met betrekking tot kortetermijnverhuur van accommodatie en tot wijziging van Verordening (EU) 2018/1724, COM(2022) 571 final van 7 november 2022. Hiermee stelt de Commissie voor een specifieke B2G-gegevensdelingscontext te reguleren (kortetermijnverhuur) met het oog op buitensporige toeristenstromen en een gebrek aan betaalbare langetermijnhuisvesting.

[61] T. Scassa. Sharing data in the platform economy: a public-interest argument for access to platform data' (2017) *UBC Law Review* 50(4) pp. 1017 – 1071.

[62] Z. Allam, *Cities and the Digital Revolution: Aligning Technology and Humanity (*Palgrave Macmillan: London, UK, 2020).

In het verlengde hiervan kan vervolgens de vraag rijzen of een bepaalde B2G-gegevensdeling dan steeds in het belang van de burger is en of deze deling optimaal is voor de vormgeving en uitvoering van de gemeentelijke publieke taak, en of met de betreffende gegevensdeling niet ook of wellicht vooral een (commerciële) agenda van een private partij wordt gediend.[63]

Tot slot merken wij op dat waar B2G-gegevensdeling aan de orde is, in veel gevallen de aandacht met name zal uitgaan naar de economische en commerciële rechten en belangen van bedrijven[64] en de noden en bevoegdheden van de gemeente. Bij het zoeken naar de juiste balans tussen die rechten, belangen en bevoegdheden rijst echter ook de vraag welke plaats de rechten en belangen van burgers krijgen in de B2G-gegevensdeling.

2.1.2 Huidige gemeentelijke praktijk met B2G-gegevensdeling

Gemeenten willen in het algemeen meer 'datagedreven' beslissingen kunnen nemen ter onderbouwing en vervulling van hun publieke taken in de openbare ruimte, zoals steden groener en schoner maken, efficiënter gebruik van openbaar vervoer stimuleren en een eerlijker verdeling van sociale woningen bereiken. In een snel digitaliserende samenleving is empirisch onderbouwde gemeentelijke beleidsvorming in toenemende mate mede afhankelijk van toegang tot en het gebruik van gegevens, met name gegevens die worden verzameld en bewaard door bedrijven.[65] Thans wordt de gemeentelijke toegang tot gegevens in bezit van private partijen veelal vastgelegd in ad hoc publiek-private samenwerkingen. Zo kan gemeentelijke toegang tot gegevens in het bezit van private partijen soms een voorwaarde zijn voor deelname aan een aanbestedingsprocedure.[66] In andere gevallen kan de gemeente toegang verkrijgen door bestanden van private partijen aan te kopen.

Buiten dergelijke publiek-private overeenkomsten heeft de praktijk uitgewezen dat gemeentelijke toegang tot private sensorgegevens die in de openbare ruimte zijn verzameld (via bijvoorbeeld wifi-tracking of camera's) vaak verschillende juridische en praktische uitdagingen met zich meebrengt.[67] Gemeenten worden regelmatig geconfronteerd met belemmeringen bij de toegang tot private sensorgegevens. Soms gaat het om wereldwijd opererende bedrijven, die weinig bereid zijn (informatie verkregen uit) sensorgegevens te delen, al laat de mobiliteitssector in de praktijk zien dat lokale partijen ook niet altijd geneigd zijn gegevens met de gemeente te delen.[68] Deze bedrijven beroepen zich bij het delen van gegevens met gemeenten veelal op juridische en economische bezwaren. Wat betreft de juridische bezwaren worden onder meer de bescherming van persoonsgegevens (van reizigers of passanten) en handelsgeheimen of intellectuele eigendomsrechten (van het bedrijf) opgevoerd.[69] Deze bezwaren liggen regelmatig aan de basis van afwijzingen van verzoeken tot het delen van informatie met de gemeente. Wat betreft de meer economisch georiënteerde voorwaarden om de gemeente tot B2G-gegevensdeling te komen, komt het regelmatig voor dat bedrijven hoge prijzen vragen voor het beschikbaar maken van gegevensbestanden, zeker als die bestanden mogelijk met derden buiten de gemeente zullen worden gedeeld. Gegevens, met name wanneer het grote hoeveelheden of gecombineerde gegevensbestanden betreft, zijn doorgaans van (grote) financiële, commerciële en economische waarde. Aan het prepareren en aggregeren van de door de gemeente gewenste gegevensbestanden kunnen ook (hoge) kosten verbonden zijn.

---

[63] M. Micheli, Public bodies' access to private sector data: The perspectives of twelve European local administrations',(2022) *First Monday* 27(2).
[64] M. Micheli, Public bodies' access to private sector data: The perspectives of twelve European local administrations',(2022) *First Monday* 27(2).
[65] Van Dijck e.a. (2018), p. 15.
[66] D. van Barneveld, C. Corver en A. Yeh, *Sensoren en de rol van gemeenten*, VNG Realisatie Whitepaper (maart 2018).
[67] Dit werd bevestigd in interviews met gemeentemedewerkers.
[68] Uit interviews met een gemeentemedewerker bleek dat lokaal opererende bedrijven terughoudend kunnen zijn met het delen van gegevens over bijvoorbeeld de aanwezigheid van aantallen personen in een specifieke openbare ruimte of in een voor het publiek toegankelijke plaats.
[69] Dit werd door verschillende medewerkers van de gemeente bevestigd.

Deze bezwaren tegen B2G-gegevensdeling kunnen de gemeentelijke toegang tot gegevens van private partijen beperken, en daarmee aan een beter geïnformeerde beleidsvorming en prioritering van gemeentelijk beleid in de weg staan. In hoofdstuk 3 van dit onderzoek gaan we nader in op de houdbaarheid van de hierboven besproken juridische argumenten.

2.1.3 Onzichtbaar voor burgers

Problematisch vanuit fundamenteelrechtelijk perspectief is dat informatie over de precieze plaatsing en werking van private sensoren in openbare ruimten vaak ontbreekt.[70] Daardoor zijn het doel van de private gegevensverwerking, het type gegevens dat wordt verzameld en de organisaties met wie deze gegevens mogelijk worden gedeeld, vaak onbekend voor de betrokken personen. Daarentegen dienen bestuursorganen die sensoren in de openbare ruimte bevestigen verantwoording af te leggen over deze aspecten. Zo wordt democratisch en rechtsstatelijk geborgd dat bekend is welk doel een sensor op een specifieke plaats vervult en op welke wijze de naleving van fundamentele rechten wordt gegarandeerd, en eventuele beperkingen op deze rechten worden gerechtvaardigd en geadresseerd. Deze verantwoordingsprocessen spelen niet 'van nature' bij private partijen.Zij hebben, anders dan de overheid, geen geweldsmonopolie. Private partijen hebben informatierechten en mogen gegevens verwerken, tenzij een bepaalde gegevensverwerking bij wet wordt genormeerd of verboden. De EU-wetgever heeft onder meer met de AVG en de ePrivacyrichtlijn getracht de omgang met (persoons)gegevens door private partijen aan banden te leggen. Hier wordt in hoofdstuk 3 nader op ingegaan.

Daarnaast is het bereik van een sensor niet altijd bekend. Een sensor kan bijvoorbeeld bevestigd zijn aan een object in een voor het publiek toegankelijke plaats die wordt beheerd door de private partij, terwijl de sensor (ook) waarnemingen doet in de openbare ruimte, waar zoals hiervoor uitgelegd, de regels met betrekking tot de gemeentelijke inrichting en het beheer van die openbare ruimte gelden (en niet die van de private partij). Voor zover de aanwezigheid en de werking van een private sensor bekend zijn, zijn er vaak geen realistische alternatieven in de vorm van andere openbare ruimten zonder sensoren. De aanwezigheid van sensoren, of deze nu gekend worden of niet, kan daarmee worden ervaren als een voortdurende en onontkoombare private 'monitoring' van de openbare ruimte.

Wanneer de gemeente (grootschalig) gebruik gaat maken van gegevens die werden verkregen via B2G-gegevensdeling kan dat, gelet op de onzichtbaarheid van sensoren, al gauw vragen oproepen over het gebruik van private sensorgegevens over menselijk gedrag in de openbare ruimte. Wanneer B2G-gegevensdelingsafspraken voor burgers obscuur blijven, kan dat bijdragen aan gevoelens van achterdocht.[71] Het belang van transparantie vanuit de gemeente over het gebruik van private sensorgegevens ten behoeve van de onderbouwing van het gemeentelijk beleid kan daarmee niet worden overschat.

In de openbare ruimte in Amsterdam zijn op dit moment gemeentelijke en private sensoren actief; volgens het overzicht van het sensorenregister van de gemeente Amsterdam gaat het op 20 december 2022 om in totaal 1.889 sensoren. Van dit aantal zijn 38 sensoren van private partijen.[72] Volgens het register verwerken van deze 38 private sensoren 17 sensoren tevens persoonsgegevens. Alle 17 (optische) sensoren die persoonsgegevens verwerken, werden aangemeld door Artis. Blijkens het overzicht worden deze gegevens verwerkt op basis van het gerechtvaardigd belang (het veiligheidsbelang) van de verwerkingsverantwoordelijke. Het overzicht van de verwerkingsverantwoordelijke van Artis vermeldt ook een privacyverklaring en de gegevens van een contactpersoon.

[70] Nesta rapport 2022.

[71] L. Van Zoonen, Privacy concerns in smart cities (2016) *Government Information Quarterly* 33 (3) 472; European Data Protection Board (EDPB) *Guidelines 3/2019 on Processing of personal data through video devices* (9–10 juli 2019).

[72] Sensorenregister.amsterdam.nl. Het overzicht telt twee registratie van een stichting (Stichting NDSM werf) die persoonsgegevens verwerkt voor het verkeersmanagement op de grachten door de gemeente Amsterdam (zie https://www.amsterdam.nl/privacy/specifieke/privacyverklaring-parkeren-verkeer-bouw/verkeersmanagement-gracht-privacy/). Hoewel de stichting van privaatrechtelijke aard is, is de verwerkingsgrondslag publiekrechtelijk (publieke taak).

Voor wat betreft het type sensoren waren van de 1889 sensoren op 20 december 2022 1.235 optische sensoren, 106 druksensoren en 128 positie- of verplaatsingssensoren actief in de stad. Het grootste aantal sensoren doet waarnemingen met betrekking tot mobiliteit, waaronder de auto (1.162 sensoren), scheepvaart (589 sensoren), milieu (40 sensoren), fiets (236 sensoren) en voetgangers (38 sensoren). Of en op welke wijze mobiele sensoren, zoals de scanauto's van de gemeente of de Apple-medewerkers met scanapparatuur in een rugtas worden weergegeven is (nog) niet af te leiden uit het register. Waarschijnlijk zijn er meer dan de thans gemelde 38 private sensoren actief in de openbare ruimte, maar zijn die (nog) niet gemeld bij het sensorenregister (zie voor de uitwerking van het sensorenregister §3.2.2).

2.2 Gemeentelijke rollen bij sensoren in de openbare ruimte

Gemeenten verzamelen al langer sensorgegevens in en over de openbare ruimte, al dan niet in enige vorm van samenwerking met private partijen. Als het gaat om wie betrokken is bij het verzamelen van sensorgegevens en wat de onderlinge relaties zijn, kunnen, aansluitend bij een Whitepaper van de VNG, over het algemeen vijf situaties worden onderscheiden.[73] Elke situatie brengt meer of minder mogelijkheden met zich voor de gemeente om te sturen op de verzameling van sensorgegevens door private partijen:

1. De gemeente verzamelt zelfstandig gegevens met eigen sensoren geplaatst op, in of aan gemeentelijke objecten (en in sommige gevallen op of aan objecten van particulieren of private partijen).
2. De gemeente neemt een dienst af, waarbij zij een dienstverleningsovereenkomst afsluit met een commerciële dienstverlener die sensoren plaatst in of op gemeentelijke objecten (en in sommige gevallen op of aan objecten van private partijen).
3. De gemeente treedt op in een publiek-private samenwerking, waarbij zij een samenwerkingsverband vormt met andere overheden, bedrijven en/of onderzoeksinstellingen. Het samenwerkingsverband verzamelt zelfstandig sensorgegevens of verzamelt deze in samenwerking met een commerciële dienstverlener.
4. Een private partij neemt met behulp van een dienstverleningsovereenkomst een dienst af bij een andere private partij. De dienstverlener plaatst sensoren op, in of aan objecten van de opdrachtgever.
5. Een private partij verzamelt geheel zelfstandig sensorgegevens. Zij plaatst die op, in of aan haar eigen objecten.

In de eerste situatie zijn geen private partijen betrokken, dus hieraan besteden we in het kader van dit onderzoek beperkt aandacht. In de tweede en derde situatie heeft de gemeente doorgaans een handelingsperspectief, omdat zij door middel van contracten een relatie aangaat met de private partijen. In de vierde en vijfde situatie lijkt het sturend perspectief beperkt, omdat de gemeente geen partij is. De gemeente Amsterdam wenst echter ook te vernemen welke juridische mogelijkheden er zijn om in de vierde en vijfde situatie fundamentele rechten (beter) te beschermen en om toegang te kunnen krijgen tot private sensorgegevens die in de openbare ruimte werden verzameld.

[73] Deze typologie is ontleend aan VNG, *Sensoren en de rol van gemeenten*, VNG Realisatie Whitepaper, p. 22 e.v.

3 Juridisch kader

In dit hoofdstuk wordt allereerst in § 3.1 een beknopt overzicht gegeven van wetgeving die de verzameling van sensorgegevens door private partijen in de openbare ruimte normeert. Vervolgens geven we in § 3.2 een overzicht van nationale en Europese wetgeving die de ruimte bepaalt waarbinnen de gemeente de fundamentele rechten in de openbare ruimte (beter) kan borgen en die bepaalt welke ruimte bestaat voor de gemeente om via B2G-gegevensdeling toegang krijgen tot (informatie verkregen uit) private sensorgegevens.[74] Tot slot geven we in §3.3 een overzicht van het bestuurlijk instrumentarium dat de gemeente tot haar beschikking heeft met het oog op betere bescherming van de fundamentele rechten in de openbare ruimte en met het oog op het via B2G-gegevensdeling verkrijgen van toegang tot (informatie uit) private sensorgegevens.

3.1 Juridisch kader voor private partijen

Het juridisch kader voor private partijen die met behulp van sensoren gegevens over menselijk gedrag in de openbare ruimte verzamelen, wordt in belangrijke mate gevormd door de AVG en door de Europese Verordening betreffende het vrij verkeer van niet-persoonsgebonden gegevens. Deze worden achtereenvolgens besproken.

3.1.1 Algemene Verordening Gegevensbescherming (AVG)

Private partijen die met behulp van sensoren persoonsgegevens verzamelen in openbare ruimten en in voor het publiek toegankelijke plaatsen worden genormeerd door de AVG. In de AVG wordt de private partij – in de regel de bedrijfsleiding die beslist over het doel van de verwerking van de persoonsgegevens en over de middelen die daartoe worden ingezet – aangeduid als de verwerkingsverantwoordelijke.[75] Niet-naleving van de AVG door de verwerkingsverantwoordelijke kan niet alleen leiden tot schade voor betrokkenen en (hoge) boetes van de AP. Niet-naleving heeft in situaties waarin B2G-gegevensdeling aan de orde is, ook gevolgen voor de latere verwerking door de gemeente. In dat geval kan de gemeente de private sensorgegevens namelijk zelf niet rechtmatig verwerken. Gelet op de tweede deelvraag van dit onderzoek – B2G-gegevensdeling – is het van belang na te gaan onder welke voorwaarden private partijen met behulp van sensoren in de openbare ruimte persoonsgegevens kunnen verwerken.

Indien private partijen gegevens met behulp van sensoren in de openbare ruimte verzamelen en deze gegevens (direct of indirect) te herleiden zijn tot identificeerbare natuurlijke personen ('betrokkenen'[76]), worden deze gegevens aangemerkt als persoonsgegevens.[77] Voordat sensorgegevens die tevens persoonsgegeven zijn kunnen worden verzameld en verwerkt, dient de private partij het specifieke doel waarvoor de gegevens worden gebruikt vast te stellen. Persoonsgegevens mogen ingevolge de AVG alleen worden verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden.[78] Het komt soms voor dat eenzelfde private partij sensoren plaatst ten behoeve van een private (commerciële) doelstelling, alsook dat deze sensoren plaatst ten behoeve van een publieke taak die aan deze partij is opgedragen. In deze gevallen is het cruciaal dat de betreffende partij helder naar alle betrokkenen communiceert wat de specifieke doelstelling van de voorgenomen verwerking van de persoonsgegevens is en wat de grondslag van de betreffende verwerking is. Voor zover deze situatie wenselijk is zal de betreffende private partij intern (beveiligings- en autorisatie-) maatregelen moeten treffen om ervoor te

[74] Daarmee richten we ons op het algemeen, horizontaal toepasselijke juridisch kader, en gaan we in beginsel niet in op bepalingen in sectorspecifieke wetgeving die ziet op de verwerking van gegevens.
[75] Art. 4 lid 7 AVG.
[76] Art. 4 lid 1 AVG.
[77] Art. 4 lid 1 AVG.
[78] Art. 5 lid 1 sub b AVG; zie ook Article 29 Data Protection Working Party ('WP29'), Opinion 03/2013 on purpose limitation (WP 203 van 2 april 2013).

zorgen dat de persoonsgegevens die voor de private doelstelling werden verzameld, niet worden verwerkt voor de publiekrechtelijke doelstelling (of andersom). Daarnaast komt het voor dat een sensor voor meer private doeleinden wordt ingezet:

> Zo bleek bijvoorbeeld uit een interview dat een bedrijf met sensoren twee specifieke doelen nastreefde, namelijk het onderzoeken van een betere beveiliging van degenen die verblijven in de voor het publiek toegankelijke plaats (die onder het beheer van het bedrijf valt) en het verkrijgen van inzichten in de drukte, zodat op basis daarvan aanvullende maatregelen kunnen worden getroffen, zoals het inzetten van extra personeel bij een *crowd control*-operatie.

Ook hier schrijft de AVG voor dat de betrokkenen op juiste wijze worden ingelicht over de specifieke en expliciete doelstelling van de voorgenomen verwerking. Daarnaast dient de verzameling en de verwerking van persoonsgegevens door private verwerkingsverantwoordelijken steeds te berusten op een van de rechtsgrondslagen uit de AVG.[79] Zij mogen persoonsgegevens verwerken indien de betrokkene toestemming heeft gegeven voor die verwerking.[80] Deze toestemming moet altijd worden gegeven voordat enige vorm van verwerking van persoonsgegevens kan plaatsvinden.[81] Bijzondere persoonsgegevens – gegevens waaruit bijvoorbeeld iemands etniciteit, godsdienst, levensovertuiging, seksuele voorkeur, en/of gezondheid blijkt – mogen in beginsel niet worden verwerkt, tenzij de betrokkene uitdrukkelijke toestemming heeft verleend.[82] Toestemming kan te allen tijde ook weer worden ingetrokken. Verwerkingsverantwoordelijken dienen het intrekken even eenvoudig te maken als het geven ervan.[83]

> In interviews gaven de meeste bedrijfsmedewerkers aan dat hun bedrijf bij voorkeur geen persoonsgegevens verwerkt en dat zij proberen het ontwerp van hun sensortechnologie daarop af te stemmen. Zo telt een bedrijf het aantal personen dat een roltrap neemt, zodat duidelijk is hoeveel personen in een voor het publiek toegankelijke plaats kunnen worden verwacht. Bij de telling wordt omwille van de anonimiteit een ondergrens gehanteerd van minimaal 6 personen; bij minder dan 6 personen wordt niet het exacte aantal, maar 'minder dan 6 personen' geregistreerd. Een ander bedrijf gebruikt camera's die looproutes van personen anoniem vastleggen; de camera's nemen een beeld van bovenaf waar, dat wordt omgezet naar X- en Y-coördinaten en een unieke identificatiecode, waarbij een persoon als stipje wordt weergegeven op een kaart.

Ook dient te worden vermeld dat de e-Privacyrichtlijn (die voor Nederland is geïmplementeerd in de Telecommunicatiewet) in bepaalde gevallen specifieke eisen stelt. Private verwerkingsverantwoordelijken die informatie – dit is een breder begrip dan enkel persoonsgegevens – met behulp van wifi-tracking over een persoon verzamelen die zich op diens eindapparatuur (ofwel een fysiek apparaat, zoals een smartphone) bevindt, moeten erop bedacht zijn dat in dergelijke gevallen de Telecommunicatiewet van toepassing is,[84] en dat deze informatie enkel rechtmatig kan worden verkregen en verwerkt op grond van toestemming (en waar bijzonere categorieën van persoonsgegevens aan de orde zijn, uitdrukkelijke toestemming).[85]

---

[79] Art. 13 lid 1 sub c en d AVG. Worden de gegevens niet direct bij de betrokkene verzameld, dan informeert de private partij de betrokkene over de bron van de persoonsgegevens (art. 14 AVG). Daarnaast dient bij elke verwerking van persoonsgegevens te worden voldaan aan de beginselen inzake de verwerking van persoonsgegevens (art. 5 AVG).
[80] Art. 6 lid 1 sub a AVG.
[81] We hebben niet onderzocht in welke mate private partijen die met behulp van sensoren persoonsgegevens in de openbare ruimte verzamelen voldoen aan het toestemmingsvereiste van de AVG. Zie hierna §3.2 waarin wordt ingegaan op de Amsterdamse Verordening Meldingsplicht sensoren, die beoogt alle partijen die sensoren in de openbare ruimte exploiteren, te melden of zij persoonsgegevens verwerken.
[82] Art. 9 lid 1 AVG.
[83] Art. 7 lid 4 AVG.
[84] Art. 11.7a lid 1 Telecommunicatiewet; deze bepaling gaat voor de AVG als *lex specialis* (zie art. 95 ePrivacyrichtlijn en Overweging 173 AVG; EDPB, Opinion 5/2019 *on the interplay between the Privacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities*, paragrafen 35, 38 – 40.
[85] Art. 5 lid 3 ePrivacyrichtlijn.

Soms kunnen verwerkingsverantwoordelijken een verwerking van persoonsgegevens baseren op een *contract* met de betrokkene, indien de verwerking noodzakelijk is voor het aanbieden van een dienst.[86] En in sommige gevallen kan het *gerechtvaardigd belang* van de verwerkingsverantwoordelijke als verwerkingsgrondslag dienen, maar dan dient deze aan te kunnen tonen dat diens commerciële of andere belangen zwaarder wegen dan de fundamentele rechten van de betrokkenen,[87] hetgeen in veel gevallen niet zomaar voor de hand zal liggen waar het verzameling van persoonsgegevens met sensoren in de openbare of voor het publiek toegankelijke plaats betreft. Tot slot zijn sommige bedrijven op basis van de wet belast met de uitvoering van een publieke taak. Zo moeten bepaalde vervoersbedrijven er bijvoorbeeld voor zorgen dat het niet te druk wordt op stations en dat de fysieke veiligheid van personen op die plaatsen wordt gegarandeerd – taken die zij met inachtneming van het recht met behulp van sensoren kunnen uitvoeren.[88]

De verwerkingsverantwoordelijke[89] is gehouden technische en organisatorische maatregelen te treffen ter bescherming van de persoonsgegevens en de rechten van de betrokkenen.[90] Betrokkenen kunnen jegens de verwerkingsverantwoordelijke rechten uitoefenen; zo hebben zij onder meer het recht op inzage in de doeleinden van de verwerking van hun persoonsgegevens, het recht op gegevenswissing, het recht gegevens over te dragen naar een andere verwerkingsverantwoordelijke (een andere private partij) en het recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming (inclusief profilering), tenzij de verwerking noodzakelijk is voor de totstandkoming of uitvoering van een contract tussen betrokkene en verwerkingsverantwoordelijke of wanneer de verwerking berust op uitdrukkelijke toestemming.[91]

Een specifiek geval doet zich voor wanneer particulieren (consumenten) sensoren (zoals camera's in deurbellen) in de openbare ruimte gebruiken. Zij worden door de uitzondering voor 'huishoudelijke activiteiten' in de AVG beschermd tegen het van kracht worden van de verplichtingen die normaal gesproken op verwerkingsverantwoordelijken rusten, indien en voor zover de particuliere gegevensverwerkingen 'zuiver persoonlijke of huishoudelijke activiteiten' betreffen.[92] Particulieren die voor de veiligheid van hun directe leefomgeving deurbellen met camera's (inclusief gezichtsherkenningstechnieken) hebben geïnstalleerd en die zich (gedeeltelijk) uitstrekken over de openbare ruimte, vallen voor het deel van de gegevensverwerking dat de openbare ruimte bestrijkt onder de huishoudelijke activiteiten in de zin van de AVG.[93] Om te voorkomen dat een vacuüm ontstaat met betrekking tot de rechtsbescherming van betrokkenen die door de sensoren worden waargenomen, zijn de AVG-verplichtingen voor het deel dat persoonsgegevens in openbare ruimte worden verwerkt van toepassing op de verwerkingsverantwoordelijke die de particulier de middelen verschafte.[94]

Voorafgaand aan de daadwerkelijke verwerking van persoonsgegevens zijn private partijen, wanneer de verwerking mogelijk hoge risico's voor betrokkenen met zich meebrengt, gehouden een

[86] Art. 6 lid 1 sub b AVG.
[87] Art. 6 lid 1 sub f AVG; zie nader I. Kamara & P. de Hert, 'Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach', Brussels Privacy Hub, Vol. 4, No. 12, August 2018.
[88] In het geval van personenvervoer is de verwerking van persoonsgegevens gebaseerd op artt. 6(1)(e) AVG en 32 lid 2 aanhef en onder h, Wp.
[89] Art. 4 sub 7 AVG.
[90] Art. 24 lid 1 AVG. Andere verplichtingen die rusten op de verwerkingsverantwoordelijke zijn onder meer dat de verwerking aan *privacy by design* en *privacy by default* methoden moet voldoen (art. 25 AVG); dat een register van de verwerkingsactiviteiten wordt bijgehouden (art. 30 AVG); of dat beveiligingsmaatregelen moeten worden getroffen (art. 32 AVG).
[91] Achtereenvolgens artt. 15, 17, 20 en 22 AVG; zie ook B. Schermer, D. Hagenauw en N. Falot, *Handleiding Algemene Verordening Gegevensbeschermingen Uitvoeringswet Algemene Verordening Gegevensbescherming* 2018 (rapport opgesteld in opdracht van het Ministerie van Justitie en Veiligheid), met name hoofdstuk 7.
[92] Art. 2 lid 2 sub c en Overweging 18 AVG.
[93] Zie EU HvJ C-212/13 (11 december 2014) *František Ryneš v Úřad pro ochranu osobních údajů*, EU:C:2014:2428; H. Janssen, J. Cobbe, C. Norval en J. Singh, 'Decentralised dataprocessing. Personal data stores and the GDPR', (2020) *International Data privacy Law* 10(4), pp. 356.
[94] Overweging 18 AVG.

gegevensbeschermingseffectbeoordeling (DPIA) uit te voeren met het oog op het mitigeren van risico's voor de 'rechten en vrijheden van individuen' die zich bij de voorgenomen verwerking van persoonsgegevens kunnen voordoen.[95] De DPIA verplicht private partijen bij de toetsing van de voorgenomen gegevensverwerking niet alleen risico's voor rechten gerelateerd aan gegevensbescherming te beoordelen, maar ook risico's voor het bredere spectrum van fundamentele rechten te beoordelen.[96] Wanneer de verwerking hoge risico's oplevert die de verwerkingsverantwoordelijke niet kan adresseren, raadpleegt deze de AP.[97] De AVG kent geen publicatieplicht voor DPIA's.

3.1.2 Vrij verkeer van niet-persoonsgebonden gegevens

De Verordening voor het vrije verkeer van niet-persoonsgebonden gegevens heeft tot doel één markt tot stand te brengen voor diensten op het gebied van gegevensopslag en -verwerking. Niet-persoonsgebonden gegevens betreffen informatie die niet is gekoppeld aan een identificeerbare of geïdentificeerde persoon, oftewel andere gegevens dan persoonsgegevens als gedefinieerd de AVG.[98] Deze gegevens kunnen interessant zijn voor de gemeente, bijvoorbeeld als zij voor de borging van de fysieke veiligheid van personen in de openbare ruimte informatie wenst te verkrijgen over het aantal personen dat zich met een metro of trein naar het centrum van de stad beweegt.[99] Private partijen die hun niet-persoonsgebonden sensorgegevens buiten Nederland opslaan of verwerken, kunnen de gemeente bij een rechtmatig verzoek om B2G-gegevensdeling niet de toegang weigeren tot die gegevens met een beroep op nationale localisatierestricties.[100] Het 'wegsluizen' van gegevens naar het buitenland is voor private partijen daarmee geen manier om te ontkomen aan een (potentiële) verplichting tot het verstrekken van toegang tot gegevens.

3.2 Juridisch kader bij het gemeentelijk handelingsperspectief

In dit deel van het juridisch kader gaan we indachtig de twee deelvragen (ter opfrissing: (i) mogelijkheden voor de gemeente om met het bestaande bestuurlijk instrumentarium een betere bescherming van de fundamentele rechten in de openbare ruimte te bieden waar het de inzet en het gebruik van private sensoren betreft en (ii) mogelijkheden en beperkingen voor B2G-gegevensdeling met het oog op de gemeentelijke vervulling van de publieke taak en verdere deling van sensorgegevens door de gemeente), nader in op een aantal wetten dat van toepassing is op de verzameling en het delen van private sensorgegevens. Daartoe presenteren we per wet eerst een algemene introductie. Daarna gaan we in op wat de gemeente op basis van de betreffende wet kan doen om de bescherming van de fundamentele rechten te verbeteren in situaties waar gegevensverzameling door private sensoren in de openbare ruimte aan de orde is. Vervolgens geven we aan wat de gemeente op basis van dezelfde wet kan doen om toegang te verkrijgen tot de private sensorgegevens te verkrijgen. In hoofdstuk 4 volgen aanbevelingen voor de verbetering van het juridisch handelingsperspectief van de gemeente.

[95] Art. 35 lid 1 AVG.
[96] Art.35 lid 1 AVG spreekt over "een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen", hetgeen ook fundamentele rechten omvat. Zie ook H. Janssen, 'An approach for a fundamental rights impact assessment to automated decision-making' (2020) *Internatinonal Data Privacy Law* 10(1), p. 76.
[97] Art. 36 lid 1 AVG.
[98] Verordening 2018/1807 van het Europees Parlement en de Raad van 14 november 2018 inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie, Pb L 303/59; art. 3 lid 1 Verordening vrij verkeer niet-persoonsgebonden gegevens en art. 4 sub 1 AVG.
[99] Art. 5 lid 1 Verordening.
[100] Art. 5 lid 1 van de Verordening. Een uitzondering geldt uitsluitend voor verboden die evenredig en gerechtvaardigd zijn in het kader van openbare veiligheid.

3.2.1 Grondwet, EVRM en EU-Handvest van de grondrechten

Juridisch kader

Het wettelijk kader voor de fundamentele rechten is neergelegd in de Grondwet, het Europees Verdrag voor de Rechten van de Mens (EVRM) en het EU-Handvest van de Grondrechten (EU-Handvest). Dit kader, inclusief de bijbehorende beperkingssystematiek, normeert de gemeente in haar relaties met burgers en met private organisaties binnen de gemeente, die soms eveneens rechten kunnen ontlenen aan het fundamenteelrechtelijk kader.[101] Fundamentele rechten omvatten onder meer het recht op bescherming van de persoonlijke levenssfeer (privacy),[102] het recht niet te worden gediscrimineerd,[103] vrijheidsrechten,[104] eigendomsrechten[105] inclusief intellectuele eigendomsrechten,[106] het recht op toegang tot een onafhankelijke en onpartijdige rechter,[107] het recht je vrijelijk te verplaatsen en het recht op vrijheid van beroep en bedrijf, en ondernemerschap.[108] De kerngedachte achter fundamentele rechten is dat de burger moet worden beschermd tegen een almachtige overheid die een op de wet berustend geweldsmonopolie kan uitoefenen, en dat overheidsregulering die inbreuken (beperkingen) op de fundamentele rechten met zich kan meebrengen, beperkt blijft tot het hoogstnoodzakelijke.

In het licht van de huidige en opkomende sensortoepassingen in de openbare ruimte zijn in de rechtspraak al diverse fundamenteelrechtelijke risico's geduid ten aanzien van het recht op privacy. Het Europees Hof voor de Rechten van de Mens (hierna: EHRM) heeft in de afgelopen decennia de betekenis en de toepasselijkheid van het recht op privacy in de openbare ruimte meermaals bevestigd in het licht van de opkomst en een groeiend aantal toepassingen van nieuwe informatie- en communicatietechnologieën, die voortdurende verzameling, opslag, verspreiding, koppeling en hergebruik van persoonsgegevens mogelijk maken.[109] Deze toepassingen worden niet alleen benut door opsporings- en vervolgingsinstanties of inlichtingen- en veiligheidsdiensten, maar ook door private partijen. Onder meer in *Von Hannover t. Duitsland* (waarin het EHRM bepaalde dat publieke figuren zoals een lid van een koninklijk huis ook een recht op privéleven toekomt, en dat zij effectief beschermd moeten worden tegen de roddelpers) merkte het EHRM op dat effectieve bescherming van het recht op privacy van staatswege geboden is. Het EVRM is volgens het Hof immers niet bedoeld om rechten te garanderen die theoretisch of illusoir zijn, maar om rechten te beschermen die praktisch en effectief zijn – ook in verhoudingen tussen burgers en private partijen onderling.[110]

Voor de vraag naar de toepasselijkheid van het recht op privacy in openbare ruimten is tevens van belang dat het EHRM meermaals heeft bevestigd dat privacy in artikel 8 EVRM ook 'sociale' en 'openbare aspecten van iemands leven' omvat, alsook het 'recht op het ontwikkelen en vestigen van relaties met anderen en de buitenwereld', het recht op de bescherming van persoonsgegevens en het recht op het leiden van een sociaal privéleven in een meer publieke context.[111] Deze deelaspecten van het recht op privacy

[101] Respectievelijk de Grondwet, het EVRM (inclusief de bijbehorende Protocollen die door Nederland zijn ondertekend) en het EU-Handvest.
[102] Art. 8 EVRM, art. 10 Grondwet en art. 7 EU-Handvest.
[103] Art. 14 EVRM en Protocol 12 bij het EVRM, art. 1 Grondwet en artt. 21 en 23 EU-Handvest.
[104] Art. 10 en 11 EVRM, artt. 7, 8 en 9 Grondwet en artt. 11, 12 EU-Handvest.
[105] Art. 1 lid 1, eerste Protocol bij het EVRM, art. 14 Grondwet en art. 17 EU-Handvest.
[106] Art. 17 lid 2 EU-Handvest.
[107] Art. 6 EVRM, Art. 17 Grondwet en art. 47 EU-Handvest.
[108] Art. 19 lid 3 Grondwet en art. 16 EU-Handvest.
[109] Zie M. Galič, *Surveillance and privacy in smart cities and living labs: Conceptualising privacy for public space*. (Diss. UvT 2019), Optima Grafische Communicatie, Rotterdam: 2019).
[110] *Von Hannover t. Duitsland*, EHRM 24 juni 2004, nr. 59320/00, paragrafen 72 en 73; zie ook EHRM 24 juni2004 (*Caroline von Hannover t. Duitsland*) NJ 2005, 22 (m.nt. E.J. Dommering).
[111] *Niemietz t. Duitsland* (16 december 1992), nr. 13710/88, paragraaf 27; *Pretty t. Verenigd Koninkrijk* (29 april 2002) nr. 2346/02, paragraaf 61; *Peck t. het Verenigd Koninkrijk* (28 januari 2003), nr. 44647/98; *Von Hannover t. Duitsland* EHRM 24 juni 2004; *Gillan en Quinton t. Verenigd Koninkrijk*, (12 januari 2010) nr. 4158/05, paragraaf 6; *Vukota-Bojić v. Switzerland* (18 oktober 2016) nr. 61838/10, paragraaf 62; *Bărbulescu t. Roemenië* (5 september 2017) nr. 61496/08, paragraaf 70.

geven het recht ook betekenis buiten de enger gedefinieerde intieme of huiselijke persoonlijke levenssfeer. Het EHRM heeft de betekenis van het recht op privacy in horizontale verhoudingen (zoals tussen werkgever en werknemer, tussen verzekeraar en verzekerde, en tussen pers en persoon van wie afbeeldingen worden gemaakt en verspreid) inmiddels ook bevestigd – ook ten aanzien van de bescherming van persoonsgegevens.[112]

De kans is reëel dat iemand een sensor in de openbare ruimte niet opmerkt of zich er niet van bewust is dat informatie over haar of hem wordt verzameld, omdat sensoren niet altijd goed zichtbaar zijn.[113] Wanneer personen zich ervan bewust zijn dat een sensor in hun nabijheid is, is het voor de meesten lastig te bepalen welke gegevensverwerkende apparatuur een sensor bevat, met welk doel informatie wordt verzameld en door wie, hoe lang de gegevens worden opgeslagen, met welke andere bestanden de gegevens worden gekoppeld en of ze met derden worden gedeeld. Dit kan burgers het gevoel geven dat zij voortdurend worden bespied, waardoor zij mogelijk hun fundamentele rechten minder snel of met terughoudendheid uitoefenen (en er een zogenoemd verkillend effect op de uitoefening van de grondrechten optreedt).[114]

Het hoeft bij het vastleggen van gedrag met sensoren overigens niet steeds te gaan om specifiek gedrag.[115] Er kan al sprake zijn van een inmenging wanneer het gedrag of de daarop betrekking hebbende gegevens op zichzelf beschouwd niet bijzonder gevoelig zijn, zoals het vastleggen van de bewegingen van een persoon in het centrum van zijn woonplaats, of op straat lopen en een winkel binnengaan om boodschappen te doen. Dergelijke verwerkingen kunnen echter wel van belang worden bij systematische inzet en/of koppeling van private sensoren, bijvoorbeeld ten behoeve van de bewaking van een openbare ruimte, waar zulke gegevens meer stelselmatig worden vastgelegd, opgeslagen en geanalyseerd. In deze ogenschijnlijk onschadelijke situaties is belangrijk dat deze informatie met behulp van de huidige verwerkings-, koppelings- en aggregatietechnieken kan leiden tot allerlei soorten afgeleide informatie en/of profielen, waardoor vervolgens veel meer persoonlijke en bijzonder gevoelige informatie over een persoon kan worden onthuld.

Beperkingen op het recht op bescherming van de persoonlijke levenssfeer, bijvoorbeeld wanneer de gemeente met eigen sensoren (bijvoorbeeld camera's) toezicht houdt op een uitgaansgebied met als doel de fysieke veiligheid te bewaken, kunnen juridisch toelaatbaar zijn, mits deze inzet van sensoren voldoet aan de cumulatieve set van vereisten, zoals die is neergelegd in het eerdergenoemd wettelijk kader. Het gemeentelijk gebruik van de sensoren en de verwerking van gegevens die daarmee gepaard gaat, moeten een *legitiem doel* dienen[116] en berusten op een *formeel-wettelijke grondslag*.[117] De betreffende wet moet voor burgers *toegankelijk* en *voorzienbaar* zijn, zodat burgers weten wat de gemeente precies beoogt met de camera's en het gebruik van de gegevens, en daar zo nodig hun gedrag op kunnen afstemmen.

Ook moet de gemeentelijke verwerking van de gegevens *noodzakelijk* zijn in een democratische samenleving. 'Noodzakelijk' houdt in dat het gebruik van die gegevens ook echt noodzakelijk is voor het

---

[112] *Halford t. Vereningd Koninkrijk* (25 juni 1997), nr. 20605/92; *Vukota-Bojić v. Switzerland* (18 oktober 2016) nr. 61838/10, paragraaf 58 [in deze zaak werd de klager werd voortdurend gefilmd in de openbare ruimte door een professionele partij in opdracht van een verzekeraar]; *Reklos en Davourlis t. Griekenland* (15 januari 2009) nr. 1234/05, paragraaf 40; *Bărbulescu t. Roemenië* (5 september 2017) nr. 61496/08, paragraaf 80;

[113] Dit geldt bij bijvoorbeeld gezichtsherkenningstechnieken, zie E. Keymolen, M. Noorman, B. van der Sloot, C. Cuijpers en B-J. Koops, *Op het eerste gezicht. Een verkenning van gezichtsherkenning en privacyrisico's in horizontale relaties*. Studie verricht in opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum (2020) p. 122.

[114] Zie bijvoorbeeld R. L. Finn, D. Wright en A. Donovan, L. Jacques en P. de Hert, *Study on privacy, data protection and ethical risks in civil remotely piloted aircraft: final report*, Publications Office, 2015, https://data.europa.eu/doi/10.2769/756525; deze studie belicht in het bijzonder risico's bij het gebruik van drones.

[115] Zie hierover P. de Hert & S. Gutwirth, 'Data protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in action' in: Y. Poullet, S. Gutwith, C. De Terwanghe, & P. de Hert (Eds.), *Reinventing Data Protection?* Springer: Dordrecht 2009, p. 26.

[116] Art. 8 lid 2 EVRM; artt.7 en 8 EU-Handvest. Art. 8 EU-Handvest is nader uitgewerkt in de AVG.

[117] Art. 10 lid 1 en 2 Grondwet. Een verwijzing naar art. 6 lid 1 sub c of e AVG of naar bijvoorbeeld art. 160 Gemeentewet kan niet volstaan omdat deze bepaling onvoldoende specifiek is.

behalen van het doel (in voornoemd voorbeeld het bewaken van de fysieke veiligheid) en dus niet enkel 'wenselijk', 'handig' of 'efficiënt': die laatste redenen zijn op zichzelf genomen onvoldoende om een inbreuk op een fundamenteel recht te kunnen rechtvaardigen.[118] Noodzakelijk *in een democratische samenleving* betekent bovendien dat de gewenste verwerking van private sensorgegevens noodzakelijk is om een *dringend maatschappelijk probleem effectief te kunnen aanpakken.*[119] Het doel waarvoor de gemeente de private sensorgegevens verwerkt moet daarnaast *evenredig* zijn aan de grondrechtelijke inbreuk.[120] Zo kan het borgen van de fysieke veiligheid evenredig zijn aan de inbreuk op iemands recht op verplaatsingsvrijheid, wanneer de inbreuk kortdurend en effectief is en niet al te diep ingrijpt in het recht op iemands recht zich vrijelijk te verplaatsen.[121] Naast het bewaken van de evenredigheid moet de gemeente voor het bereiken van het doel kiezen voor de middelen die het minst ingrijpen in het grondrecht.

Deelvraag 1: handelingsperspectief bij betere naleving van de fundamentele rechten

Anders dan de overheid worden private partijen in beginsel niet genormeerd door de Grondwet of het EVRM, maar dat betekent niet dat zij zich geheel aan grondrechtelijke normen kunnen onttrekken. Het gedrag van private partijen wordt namelijk op diverse wijzen grondrechtelijk genormeerd. Zo is er wetgeving die de informatieverzameling van private partijen in de openbare ruimte kan beperken, zoals de AVG en de ePrivacy Verordening (zie §3.1.1). Dergelijke beperkingen worden tot stand gebracht door de formele wetgever. De grondwettelijk beschermde rechten op informatieverzameling, het recht op vrijheid van bedrijf en beroep en de vrijheid van ondernemerschap kunnen immers enkel worden ingeperkt wanneer die inperking is terug te voeren op een formele wet.[122]

Private partijen kunnen in hun gedrag ook op andere manieren worden genormeerd door fundamentele rechten. Wanneer het handelen van een bedrijf de fundamentele rechten van personen raakt, kunnen de fundamentele rechten helpen bij het invullen van civielrechtelijke 'vage' normen. Fundamentele rechten kunnen bijvoorbeeld een rol spelen bij de beoordeling of het handelen van een private partij maatschappelijk betamelijk is, of bij de beoordeling of sprake is van goed werkgeverschap zoals vastgelegd in het Burgerlijk Wetboek (hierna: BW).[123] Verder vloeit uit de rechtspraak van het EHRM voort dat nationale autoriteiten burgers actief dienen te beschermen tegen inbreuken door private partijen.[124] Het EHRM verplichtte nationale overheden eerder al regelgeving inzake de inzet van surveillancetechnieken binnen de arbeidsrelatie aan te nemen; werkgevers moeten bijvoorbeeld werknemers met voorafgaande communicatie inlichten over dergelijke monitoring, terwijl overheden voor eventuele conflicten hierover een toegankelijke en passende rechtsgang moeten bieden.[125] In navolging hiervan is in de literatuur geopperd dat uit artikel 8 EVRM een positieve verplichting voor de overheid zou kunnen voortvloeien om het gebruik van sensoren door private partijen nader te reguleren.[126] De bevoegdheid wettelijke regels vast

[118] *Handyside t. Verenigd Koninkrijk*, EHRM 7 december 1976, nr. 5493/72, paragraaf 48; EU HvJ C-293/12 en C-594/12 *Digital Rights Ireland,* paragraaf 54.
[119] *S. and Marper v the UK* (Grote Kamer), 4 december 2008, nrs. 30562/04 & 30566/04, paragraaf 101.
[120] *ECHR Leander v Sweden*, 26 maart 1987, nr. 9248/81, paragrafen 50 en 58. De indringendheid van de verwerking voor het grondrecht bepaalt de strengheid van de eisen die aan de toegang tot de private sensorgegevens worden gesteld: naarmate een beperking op het grondrecht indringender is, worden de eisen aan de toelaatbaarheid van de beperkende activiteit strenger.
[121] Art. 2, Protocol 4 bij het EVRM.
[122] Artt. 10 lid 2 en 19 lid 3 Grondwet; art. 10 EVRM; artt. 11 lid 1, 16 en 52 lid 1 EU-Handvest.
[123] Respectievelijk art. 6:162 BW en art. 7:611 BW.
[124] Zie bijvoorbeeld *Evans t. het Verenigd Koninkrijk,* EHRM 10 april 2007, nr. 6339/05, paragraaf 75; zie ook Zie M.J. Vetzo, J.H. Gerards en R. Nehmelman, *Algoritmes en fundamentele rechten*, Den Haag: Boom juridisch 2018, pp. 76 – 78 en 177 – 178. In art. 10 lid 2 en 3 Grondwet zijn daarnaast twee positieve verplichtingen gecodificeerd, namelijk tot het stellen van regels omtrent persoonsgegevens en omtrent kennisneming van vastgelegde gegevens, zie ook A.K. Koekkoek, *De Grondwet: een systematisch en artikelsgewijs commentaar,* derde druk, Deventer 2000, p. 4.
[125] EHRM 5 september 2017, app nr 61496 (*Bărbulescu t. Roemenië*).
[126] M.J. Vetzo e.a. 2018, pp. 126 – 127.

te stellen met het oog op normering van private partijen ligt kortom niet primair bij gemeenten, maar bij de formele wetgever[127] en in voorkomende gevallen bij de rechter.
Dat betekent niet dat er nu geen lokale wetgeving tot stand kan worden gebracht die meer specifiek de inzet van sensoren door private partijen in de openbare ruimte reguleert. Met het oog op de verbetering van de naleving van de fundamentele rechten vanwege het groeiend aantal sensoren in de openbare ruimte, nam de gemeente Amsterdam in 2021 de Verordening meldingsplicht sensoren aan. Deze verordening verplicht alle partijen die met een professioneel doel gegevens in de openbare ruimte inwinnen door middel van vaste of mobiele sensoren, daarover transparant te zijn.[128] Ook private partijen dienen melding te maken van sensoren die zij in de openbare ruimte plaatsen.[129] Aan de melding zelf worden door de gemeente nadere eisen gesteld; deze is dus niet vormvrij. In het digitale meldformulier moet worden aangegeven of met de sensor persoonsgegevens worden verwerkt en als dat het geval is, op basis van welke wettelijke grondslag dit gebeurt. Ook dient bij de verwerking van persoonsgegevens een link naar de privacyverklaring van de meldende partij te worden opgenomen.[130] Het meldingsformulier kan desgewenst met nieuwe informatievereisten worden uitgebreid.

De informatie in het meldingsformulier wordt in een openbaar register opgenomen, zodat gebruikers van openbare ruimten kunnen nagaan welke gegevens over hen worden ingewonnen. Zo nodig kunnen zij daarover contact opnemen met de partij die deze gegevens inwint of een klacht indienen bij de AP. Hoewel de verordening al in werking is getreden, laat het register vooralsnog overwegend gemeentelijke sensoren zien.[131] De gemeente Amsterdam is na een 'wenperiode' voornemens te verordening te gaan handhaven.

In aanvulling op de bescherming van de grondwettelijke persoonlijke levenssfeer verdient artikel 441b in het Wetboek van Strafrecht vermelding. Deze bepaling beoogt burgers te beschermen tegen inbreuken op dit grondrecht door onder meer private partijen.[132] Het verbiedt de structurele inzet van technische hulpmiddelen waarmee een afbeelding van een persoon wordt vervaardigd in openbare ruimten en in voor het publiek toegankelijke ruimten, waarvan de aanwezigheid niet op duidelijke wijze kenbaar is gemaakt. Voor de strafbaarstelling is bepalend of de afgebeelde persoon zich op een voor het publiek toegankelijke of openbare plaats bevond en niet of het technisch hulpmiddel op een voor het publiek toegankelijke of openbare plaats is aangebracht. Dit betekent dat ongeacht waar het hulpmiddel is aangebracht, sprake kan zijn van een strafbare gedraging, wanneer het hulpmiddel is *gericht* op een voor een voor het publiek toegankelijke plaats of openbare plaats. Private partijen die dergelijke hulpmiddelen ten behoeve van het maken van afbeeldingen inzetten, moeten passanten aldus op duidelijke wijze over het cameratoezicht informeren; het nalaten hiervan is strafbaar.

Deelvraag 2: normering B2G-gegevensdeling en deling met derde partijen

Waar private partijen en particulieren in beginsel vrij zijn om *binnen de grenzen van de wet* te handelen, kunnen overheden in het algemeen alleen *op basis van* en in overeenstemming met een wet handelen. Dit betekent dat de gemeente bij de verkrijging van private sensorgegevens door middel van B2G-gegevensdeling steeds moet nagaan of daarbij de fundamentele rechten en de bijbehorende wettelijke grenzen in acht worden genomen. We behandelen hier de eisen die voortvloeien uit het fundamenteelrechtelijk kader met betrekking tot B2G-gegevensdeling. In §3.2.2 gaan we in op de eisen die de AVG stelt aan de gemeentelijke verkrijging van toegang tot private sensorgegevens waarbij persoonsgegevens betrokken zijn.

[127] De formele wetgever kan voorts wetgeving tot stand brengen die voor private partijen nadere inkleuring geeft aan grondwetsnormen (zie bijvoorbeeld de Algemene wet gelijke behandeling).
[128] Verordening van de Raad van de gemeente Amsterdam tot wijziging van de Algemene Plaatselijke Verordening 2008 in verband met het invoeren van een meldingsplicht voor sensoren (inwerkingtreding 1 oktober 2021).
[129] Zie §3.2.2.
[130] https://formulier.amsterdam.nl/thema/privacy/sensorregistratie/sensorregistratie/.
[131] Zie Sensorenregister Amsterdam.
[132] Memorie van toelichting bij Wijziging van artt. 139f en 441b Wetboek van Strafrecht (uitbreiding strafbaarstelling heimelijk cameratoezicht), *Kamerstukken II* 2000-2001, 27732, nr. 3. Doel was het toepassingsbereik van de bepaling uit te breiden van winkels en horecagelegenheden naar voor het publiek toegankelijke plaatsen en openbare ruimten.

Voor zover een B2G-gegevensdeling een inbreuk maakt op (fundamentele) rechten van de delende private partij, zal steeds een formeelwettelijke grondslag vereist zijn. De gemeente zal aldus bij elke voorgenomen B2G-gegevensdeling moeten nagaan of zich bij de beoogde gegevensdeling inbreuken op deze rechten kunnen voordoen. In die gevallen is een formeelwettelijke basis vereist. Zo kunnen fundamentele rechten van private partijen, waaronder de eerdergenoemde informatierechten, het recht op eigendom, intellectuele eigendom en/of de rechten op de vrijheid van beroep en bedrijf of het ondernemerschap worden geraakt, indien de gemeente B2G-gegevensdeling afdwingt. Een verplichte B2G-gegevensdeling kan enkel worden gelegitimeerd, wanneer daarvoor een wettelijke grondslag bestaat. Indien private partijen *vrijwillig* tot B2G-gegevensdeling overgaan (bijvoorbeeld op basis van een overeenkomst), dan zal van een fundamenteelrechtelijke inbreuk op de rechten van de betreffende private partijen in beginsel geen sprake zijn.

B2G-gegevensdeling kan ook de fundamentele rechten van burgers raken. Indien met de gemeente een gegevensbestand wordt gedeeld waarin zich een bias ten aanzien van personen of groepen bevindt of waarin zich discriminerende profielen van personen bevinden, bestaat een risico dat het gebruik van het betreffende gegevensbestand door de gemeente discriminerend kan uitwerken. Een inbreuk op fundamentele rechten kan zich daarnaast voordoen wanneer de beoogde private sensorgegevens werden verzameld in een openbare ruimte waar bijvoorbeeld veel manifestaties plaatsvinden. B2G-gegevensdeling kan in die situatie een verkillend effect hebben op de betogings- en vergaderingsrechten, omdat burgers niet weten voor welk doel de gemeente de met behulp van B2G-gegevensdeling vergaarde informatie zal gebruiken. Zij kunnen hierdoor minder genegen zijn van deze rechten gebruik te maken op de plaats waar de private sensor zich bevindt. Een formeelwettelijke grondslag is in deze gevallen van B2G-gegevensdeling aangewezen. Deze wettelijke grondslag dient burgers adequaat te informeren over het doel, de noodzaak en de proportionaliteit van die specifieke B2G-gegevensdeling, alsook over de wijze waarop de risico's die met de B2G-gegevensdeling kunnen optreden, worden gemitigeerd. In navolging hiervan moet de gemeente voorafgaand aan elke specifieke B2G-gegevensdeling nagaan of zich bij de beoogde B2G-gegevensdeling inbreuken op fundamentele rechten van bedrijven kunnen voordoen.

Diverse geïnterviewden melden dat bij gemeentelijke verzoeken om B2G-gegevensdeling betreffende gegevens over menselijk gedrag in de openbare ruimte niet altijd duidelijk was of een dergelijke deling noodzakelijk was, en voor zover die nodig werd geacht, op welke wettelijke basis het verzoek om B2G-gegevensdeling werd gebaseerd. Ook gaven zij aan dat de noodzaak voor het delen niet altijd even helder was geformuleerd.[133] In een van de interviews gaf een gemeentemedewerker aan dat informatie over drukte op perrons (in dit geval informatie van vervoersbedrijven) de gemeente in specifieke gevallen zou kunnen helpen bij het beheer van de openbare ruimte, bijvoorbeeld na afloop van een voetbalwedstrijd.

> De gemeente wil de fysieke veiligheid in de openbare ruimte waarborgen, voorkomen dat mensen worden verdrukt door de massa en de doorstroom bevorderen. Als bijvoorbeeld een Ajax-wedstrijd of een ander grootschalig evenement is afgelopen, moet de gemeente *in real-time* op de hoogte zijn van de drukte en de hoeveelheid metro's en treinen die worden ingezet, zodat mensenmassa's niet ophopen in de stations, op de perrons en in de openbare ruimte grenzend aan de stations, die onder het beheer van de gemeente valt. Dan ontstaan immers onveilige situaties. De gemeente moet en wil daarom zicht houden op mensenmassa's tijdens grote evenementen.[134]

Of en op welke wijze in dit specifieke voorbeeld fundamentele rechten van private partijen en/of van burgers als gevolg van de B2G-gegevensdeling worden geraakt, hangt zoals hiervoor uiteengezet af van diverse factoren en vergt daarmee een context-specifieke beoordeling.

Verder kan B2G-gegevensdeling gebaseerd op sensorgegevens die werden verkregen uit voor burgers niet-waarneembare sensoren – zoals sensorgegevens die werden vergaard met camera's in

[133] Dit werd gemeld door medewerkers van zowel bedrijven als van de gemeente.
[134] Gemeentemedewerker.

reclamezuilen, in rugtassen van personen die de stedelijke omgeving voor een bedrijf in kaart brengen of in auto's van incassobedrijven die daarmee wanbetalers in de openbare ruimte proberen te traceren – meer algemeen leiden tot wantrouwen van burgers tegenover de gemeente.[135] Bovendien leidt een dergelijke gemeentelijke praktijk tot spanning met het uitgangspunt van de gemeente dat iedereen in Amsterdam het recht heeft op respect voor zijn of haar privéleven, en dat voor iedereen in Amsterdam het uitgangspunt geldt dat zij zich onbespied en anoniem moet kunnen bewegen in de openbare ruimte.[136] De gemeente zal voorafgaand aan de verwerking van gegevens die met B2G-gegevensdeling werden verkregen steeds moeten onderzoeken en verantwoorden of en waarom B2G-gegevensdeling in die situaties in overeenstemming is met de fundamentele rechten van burgers en private partijen. Bij de gemeentelijke beoordeling van de naleving van het fundamenteelrechtelijk kader bij een voorgenomen B2G-gegevensdeling zijn de AVG, de Awb en overige wetgeving die hierna worden behandeld van groot belang.

3.2.2 Algemene Verordening Gegevensbescherming

Juridisch kader

We behandelden in §3.1.1 de wijze waarop de AVG van toepassing is op de verwerking van persoonsgegevens door private partijen. In deze paragraaf gaan we in op de wijze waarop de AVG van toepassing is op verwerkingen van persoonsgegevens door de gemeente. De AVG stelt immers andere eisen aan publieke actoren dan aan private.

Wanneer de gemeente met behulp van B2G-gegevensdeling gegevens verzamelt en deze vervolgens verwerkt, en deze gegevens herleidbaar zijn tot specifieke personen, verwerkt zij persoonsgegevens in de zin van de AVG.[137] De gemeente treedt in die gevallen steeds op als verwerkingsverantwoordelijke voor zover zij het specifieke doel en middelen met betrekking tot de verwerking van die gegevens bepaalt.[138] Daarbij dient de gemeente zich als verwerkingsverantwoordelijke ervan te vergewissen dat de verwerking van private sensorgegevens die tevens persoonsgegeven zijn, in overeenstemming is met de beginselen inzake de verwerking van persoonsgegevens zoals die zijn vastgelegd in de AVG.[139] De gemeentelijke verwerking van deze persoonsgegevens dient daarnaast gebaseerd te zijn op een verplichting die is vastgelegd in de wet, en noodzakelijk te zijn voor de vervulling van een publieke taak of een taak in het kader van de uitoefening van openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen.[140] Bijzondere persoonsgegevens – toepasselijk in het geval van bijvoorbeeld de verwerking van (optische) sensoren die biometrische gegevensverwerking, of bij de verwerking van gegevens waaruit etnische afkomst of religieuze overtuigingen blijken – mogen in beginsel niet worden verwerkt, tenzij aan een van de voor de overheid geldende uitzonderingen is voldaan.[141] De verwerkingsverantwoordelijke is steeds gehouden passende technische en organisatorische maatregelen te treffen ter bescherming van de rechten en vrijheden van personen.[142]

Een gegevensbeschermingseffectbeoordeling (of DPIA) is verplicht bij verwerkingen van persoonsgegevens die waarschijnlijk een hoog risico met zich meebrengen voor de fundamentele rechten

[135] In Amsterdam waren oudere gevallen bekend van incassobedrijven die ANPR gebruikten om in contact te komen met klanten die in gebreke bleven met de betaling van hun leningen, maar die niet reageerden op pogingen van de private schuldeiser om contact op te nemen. Hiertoe rustte een incassobureau auto's uit met camerasensoren die door de stad reden om kentekengegevens van aangetroffen auto's vast te leggen en te verwerken met het oog op identificatie van de debiteur. Dit voorbeeld werd genoemd door een gemeentemedewerker; zie ook L. Fang, 'Debt collectors fight privacy advocates over limits for automated licence plate readers', *The Intercept* (8 mei 2015); Marcis en Bego 2022, p. 35.
[136] Gemeente Amsterdam, *Stedelijk kader verwerken persoonsgegevens door de gemeente Amsterdam*, 25 september 2018.
[137] Art. 4 lid 1 AVG.
[138] In de praktijk is binnen de gemeente de burgemeester verwerkingsverantwoordelijke.
[139] Art. 5 lid 1 AVG.
[140] Art. 6 lid 1 sub c en e AVG.
[141] Art. 9 lid 2 AVG.
[142] Art. 24 lid 1 AVG.

en vrijheden van personen.[143] Of dit risico aan de orde is, moet de verwerkingsverantwoordelijke per situatie waarin B2G-gegevensdeling wordt nagestreefd, beoordelen. Een DPIA is in ieder geval verplicht bij B2G-gegevensdelingen waarbij bijzondere persoonsgegevens worden verwerkt[144] of wanneer grootschalig en stelselmatig personen in openbare ruimten of in voor het publiek toegankelijke ruimten worden gevolgd.[145]

Betrokkenen hebben het recht jegens de verwerkingsverantwoordelijke de aan hen toegekende rechten in de AVG uit te oefenen. Zo hebben zij hebben het recht te worden geïnformeerd over de vraag of hun persoonsgegevens al of niet worden verwerkt en als dat het geval is, inzage te verkrijgen in onder meer de doeleinden en de ontvangers van die gegevens.[146]

Wanneer de private partij erin slaagt de persoonsgegevens voorafgaand aan de B2G-gegevensdeling te anonimiseren en de gegevens daarmee niet langer als persoonsgegevens kunnen worden aangemerkt, vervallen in beginsel de voor de verwerkingsverantwoordelijke toepasselijke verplichtingen uit de AVG. Het anonimiseren zelf kan echter niet altijd duurzaam worden gegarandeerd; zo kan het anonimiseren van een bepaald gegevensbestand in bepaalde gevallen teniet worden gedaan doordat het betreffende gegevensbestand wordt gecombineerd met een of meer andere gegevensbestanden: de combinatie van gegevens kan dan toch weer leiden tot gegevens die leiden naar identificeerbare personen in het geanonimiseerde gegevensbestand.[147] Ook andere factoren kunnen het succesvol anonimiseren van persoonsgegevens beperken.[148]

Deelvraag 1: handelingsperspectief bij betere naleving van de fundamentele rechten

Wat het handelingsperspectief van de gemeente betreft bij het beter beschermen van de fundamentele rechten bij de private verwerking van sensorgegevens uit de openbare ruimte, is het van belang te kijken naar de belegging van toezichthoudende en handhavende bevoegdheden in de AVG. De AP houdt toezicht op de naleving en de handhaving van de AVG. De AP is daartoe door de wetgever toegerust met een stevig sanctie- en boetestelsel.[149] Dit betekent dat voor gemeentelijk toezicht op de naleving van de AVG door private partijen geen formele rol is weggelegd.

Daarmee is niet gezegd dat de gemeente in het geheel geen handelingsperspectief bij de naleving van de AVG toekomt. De eerdergenoemde Amsterdamse Verordening meldingsplicht sensoren kan voor het afdwingen van een betere naleving van de grondrechten en meer specifiek de AVG door private partijen een nuttige basis bieden. Waar nu niet altijd duidelijk is of en waar private partijen met behulp van sensoren in de openbare ruimte persoonsgegevens verzamelen, moeten verwerkingsverantwoordelijken ingevolge deze verordening verplicht aangeven op het daartoe voorgeschreven meldformulier of met de sensor persoonsgegevens worden verwerkt en als dat het geval is, op basis van welke wettelijke grondslag dit gebeurt. In het meldingsformulier dient de verwerkingsverantwoordelijke ook een link naar de privacyverklaring op te nemen.[150] Op het moment van het schrijven van dit rapport was de link naar het meldingsformulier nog niet gemakkelijk vindbaar. Voor een goede naleving van de meldingsplicht is gemakkelijke vindbaarheid (eventueel in diverse talen) een belangrijke voorwaarde. Indien in de praktijk

[143] Art. 35 lid 1 AVG.
[144] Art. 35 lid 3 sub a.
[145] Art. 35 lid 3 sub c.
[146] Betrokkenenrechten zijn neergelegd in de artt. 13 – 22 AVG, maar niet alle rechten kunnen voluit jegens de gemeente worden uitgeoefend. Zie verder B. Schermer, D. Hagenauw en N. Falot, *Handleiding Algemene Verordening Gegevensbeschermingen Uitvoeringswet Algemene Verordening Gegevensbescherming* 2018 (rapport opgesteld in opdracht van het Ministerie van Justitie en Veiligheid), met name hoofdstuk 7.
[147] B. Van der Sloot, S. van Schendel & C. Augusto Fontanillo López, De invloed van (technische ontwikkelingen op het begrip persoonsgegevens in relatie tot de AVG, Rapport in opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum (Tilburg University, December 2022).
[148] Zie voor een overzicht van factoren die het anonimiseren kunnen hinderen of uitsluiten Agencia Espagñola Protección Datos, '10 Misunderstandings of anonymisation' (2021) https://edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf, bezocht op 12 september 2022.
[149] Zie onder meer artt. 83 AVG.
[150] https://formulier.amsterdam.nl/thema/privacy/sensorregistratie/sensorregistratie/.

blijkt dat deze informatie niet voldoende is, kan de gemeente het meldingsformulier met nieuwe informatievereisten uitbreiden. Het sensorenregister geeft daarmee een nadere en eigentijdse uitwerking aan de AVG.[151]

Het sensorenregister waarin de informatie uit het meldingsformulier wordt opgenomen, is toegankelijk voor het publiek en kan zo bijdragen aan een betere borging van onder meer het transparantiebeginsel.[152] Daarnaast kan het sensorenregister degenen die gebruik maken van openbare ruimten de mogelijkheid bieden te onderzoeken welke gegevens over hen worden ingewonnen. Met de publicatieplicht kan, indien de verordening wordt nageleefd, het probleem van het voor veel burgers onzichtbare karakter van veel gegevensverwerkingen met behulp van sensoren door private partijen in de openbare ruimte (deels) worden weggenomen.[153] De verplichte melding van onder meer de wettelijke grondslag zal hen informeren over de rechtmatigheid van de verwerking van de persoonsgegevens.

Met het voor eenieder toegankelijke sensorenregister wil de gemeente burgers wijzen op mogelijkheden tot uitoefening van de AVG-betrokkenenrechten (zoals inzagerechten,[154] het recht op gegevenswissing[155] en het recht niet te worden onderworpen aan geautomatiseerde besluitvorming[156]) jegens private partijen die met behulp van sensoren persoonsgegevens verwerken. Verwerkingsverantwoordelijken zijn zoals aangegeven in §3.2.1 gehouden de betrokkenenrechten na te leven. Zij blijken in de praktijk echter niet altijd genegen aan deze rechten gehoor te geven.[157] Op basis van zijn of haar bevindingen kan een betrokkene zelf besluiten een klacht in te dienen bij de AP, die vervolgens bij constatering van niet-naleving van de AVG (forse) administratieve boetes kan opleggen.[158] Blijkens recente publicaties reageert de AP om diverse redenen niet of traag op individuele klachten.[159] Dit kan de effectiviteit van betrokkenenrechten ondergraven, hetgeen onwenselijk is, omdat deze rechten en de mogelijkheid tot het indienen van een klacht de kurk zijn waarop de naleving van de AVG drijft.[160] Individuele klagers kunnen in plaats van het indienen van een klacht bij de AP ook overwegen een rechtszaak tegen de betreffende private partij aan te spannen wegens beweerde niet-naleving van de AVG.[161] Daarbij moet worden aangetekend dat rechtszaken lang kunnen duren en kostbaar kunnen zijn en dat (met name grotere) private spelers in de openbare ruimte veelal meer kunnen spenderen aan rechtsbijstand, waardoor deze weg vaak niet realistisch is. In dat verband verdient het overwegen van een collectieve actie op basis van de Wet afwikkeling massaschade in collectieve actie ('WAMCA') aanbeveling. Belangenorganisaties kunnen dergelijke acties voor individuen op touw zetten; gemeenten kunnen overwegen belangenorganisaties die zich toeleggen op kwesties die zich voordoen in gemeentelijke context steunen (subsidiëren).[162]

---

[151] De verordening verplicht alle partijen die gegevens inwinnen voor een professioneel doel in de openbare ruimte met behulp van vaste of mobiele sensoren, de sensoren die zij in de openbare ruimte plaatsen te melden, en kenbaar te maken welke gegevens worden ingewonnen of ingewonnen kunnen worden. Deze informatie wordt opgenomen in een openbaar register (zie §3.2.1).

[152] Art. 5 lid 1 sub a AVG.

[153] Dit zal ten dele het geval zijn, omdat de publicatieverplichting op zichzelf niet kan leiden tot nadere inzichten in details over waarom een bepaalde gegevensverwerking dient te geschieden of in de bedrijfsmodellen die de partijen hanteren. De betrokkenenrechten kunnen nog wel enkele nadere inzichten in de gegevensverwerking geven. De verordening ziet niet op voor het publiek toegankelijke plaatsen.

[154] Art. 15 AVG.

[155] Art. 17 AVG.

[156] Art. 22 AVG.

[157] J. Ausloos & P. Dewitte, 'Shattering One-Way Mirrors – Data Subject Access Rights in Practice' (2018) 8 *International Data Privacy Law* 4.

[158] Voor het indienen van een klacht zie art. 77 AVG; voor het opleggen van boetes zie Art. 83 lid 5 AVG.

[159] Q. Tjeenk Willink, 'Tempo moet omhoog bij de Autoriteit Persoonsgegevens', *Het Financieele Dagblad* 24 november 2021; C. Prins, 'Rutte IV: toezichtreflex en Autoriteit Persoonsgegevens', *NJB* 2022/233.

[160] G González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Law, Governance and Technology Series, Springer 2014), p. 194.

[161] Art. 79 lid 2 AVG.

[162] Zie nader §3.3.

Tot slot schrijft de AVG voor dat de verwerkingsverantwoordelijke betrokkenen bij het uitvoeren van een DPIA 'in voorkomend geval' vraagt naar hun mening over de voorgenomen verwerking met inachtneming van de bescherming van commerciële en andere belangen.[163] Omdat bedrijven zelf mogen invullen wat 'in voorkomend geval' inhoudt, valt gelet op de huidige praktijk niet te verwachten dat bedrijven hun gedrag – dat wil zeggen betrokkenen nauwelijks of niet polsen over een voorgenomen verwerking – zullen wijzigen. De AP kan bedrijven uitdrukkelijker wijzen op deze verplichting.

Deelvraag 2: normering B2G-gegevensdeling en deling met derden

De AVG biedt de gemeente zoals gezegd twee grondslagen op basis waarvan zij persoonsgegevens kan verwerken. Die gelden ook wanneer zij via B2G-gegevensdeling persoonsgegevens ontvangt van een private partij. Voorafgaand aan de ontvangst van de private sensorgegevens dient het specifieke doel van de verwerking vast te staan.[164] Het doel van de verwerking van de persoonsgegevens dient herleidbaar te zijn tot een formele wet. De gemeente moet ook de noodzaak en de evenredigheid van de verwerking kunnen aantonen.[165] Het tijdvak waarop het verzamelen en de opslag van de persoonsgegevens betrekking heeft, mag niet langer duren dan strikt noodzakelijk is om het door de gemeente gestelde doel te bereiken.[166] De AVG is met andere woorden in volle omvang van toepassing op B2G-gegevensdeling waarin persoonsgegevens worden verwerkt en op verdere verwerkingen van die gegevens door de gemeente (bijvoorbeeld het delen van persoonsgegevens met derden).

Private partijen kunnen op basis van een vraagstelling van de gemeente diverse typen gegevensbestanden aanleveren bij de gemeente. Zij kunnen een gegevensbestand samenstellen dat gebaseerd is op ruwe persoonsgegevens (zoals ze werden verzameld door de sensor), op zogenoemde 'pre-processed gegevens' (oftewel gegevens die werden geprepareerd om te kunnen worden verwerkt), op geaggregeerde gegevens (waarbij de gegevens reeds werden gecombineerd met andere gegevens) en/of als onderdeel van een overzicht op basis van de resultaten van de aggregatie(s).[167] In elk van deze vier typen gegevensbestanden kunnen persoonsgegevens aanwezig zijn. Indien de gemeente via B2G-gegevensdeling toegang verkrijgt tot een gegevensbestand waarin zich nog persoonsgegevens bevinden, is de gemeente verwerkingsverantwoordelijke ten aanzien van dat gegevensbestand. In de praktijk geeft de gemeente blijkens de afgenomen interviews echter de voorkeur aan het ontvangen van gegevensbestanden zonder persoonsgegevens:

> In de praktijk blijkt dat de gemeente omwille van de strikte vereisten uit de AVG bij voorkeur geen persoonsgegevens ontvangt, maar alleen 'schone gegevens', zoals puntjes op bepaalde plekken in de openbare ruimte, getallen die aangeven hoeveel mensen in- en uitstappen bij bepaalde stations en punten waar deelscooters in de openbare ruimte worden gestald, omdat dat in overeenstemming met de privacywetgeving is. De gemeente Amsterdam heeft bij het naleven van die wetgeving volgens deze gemeentemedewerkers een belangrijke voorbeeldfunctie.[168]

Private partijen kunnen inderdaad een gegevensbestand creëren waarvoor geen persoonsgegevens werden verwerkt. Toch moet de gemeente nagaan of en in hoeverre zij verwerkingsverantwoordelijke is voor een

---

[163] Art. 35 lid 9 AVG.
[164] Art. 6 lid 1 sub c of e, art. 6 lid 4 en overweging 50 AVG; zie ook B. Schermer, D. Hagenauw en N. Falot, *Handleiding Algemene Verordening Gegevensbeschermingen Uitvoeringswet Algemene Verordening Gegevensbescherming* 2018 (rapport opgesteld in opdracht van het Ministerie van Justitie en Veiligheid), p. 35 e.v.
[165] Idem. Het noodzaakcriterium in de AVG komt overeen met de wijze waarop het noodzaakcriterium dat is ook vastgelegd in het EVRM, het EU-Handvest voor de fundamentele rechten en in de Grondwet wordt ingevuld (zie §3.2.1); zie ook EU HvJ C-175/20 SS SIA t. *Valsts ieņēmumu dienests* (24 februari 2022) ECLI:EU:C:2022:124, r.o. 74.
[166] EU HvJ C-175/20, *SS SIA t. Valsts ieņēmumu dienests* (24 februari 2022) ECLI:EU:C:2022:124, r.o. 80.
[167] S. Verhulst, A. Young, M. Winowatan, A.J. Zahunanec (2019) 'Leveraging private data for public good. A descriptive analysis and typology of existing practices', *GovLab*, https://datacollaboratives.org/static/files/existing-practices-report.pdf, bezocht op 14 december 2022.
[168] Gemeentemedewerkers.

bestand. Een gegevensbestand dat is gebaseerd op gegevens niet zijnde persoonsgegevens (zoals meteorologische gegevens, gegevens over hoeveelheden fijnstof in de lucht of gegevens over louter aantallen deelscooters in de stad) zal onder de AVG waarschijnlijk zonder problemen kunnen worden gedeeld met de gemeente.
Daarnaast kan zich de situatie voordoen waarin een private partij een geanonimiseerd gegevensbestand beschikbaar stelt aan de gemeente, waarbij de private partij voor het creëren van het bestand wel persoonsgegevens verwerkte. In dat geval rijst de vraag of de gemeente voor het creëren van dat geanonimiseerde gegevensbestand optreedt als verwerkingsverantwoordelijke of dat haar die rol niet toekomt, omdat het ontvangen gegevensbestand geanonimiseerd is (en de AVG daarmee niet van toepassing zou zijn op de gemeente).

Wanneer een private partij persoonsgegevens gebruikt voor het creëren van een geanonimiseerd gegevensbestand en deze het betreffende gegevensbestand enkel *in opdracht* van de gemeente creëerde, ligt het voor de hand aan te nemen dat de gemeente optreedt als verwerkingsverantwoordelijke voor het betreffende gegevensbestand, ook al wordt het bestand in geanonimiseerde vorm beschikbaar gesteld aan de gemeente. De gemeente gaf de private partij immers opdracht tot het maken van het geanonimiseerde bestand en bepaalde daarmee het doel van de verwerking van de persoonsgegevens die de private partij verwerkte met het oog op het creëren van het gevraagde bestand. Zo zou in een hypothetisch geval een gemeente die een vergunning verleent aan een bedrijf dat deelfietsen in de openbare ruimte plaatst, van dat bedrijf in de voorwaarden voor de vergunningverlening willen eisen dat het geanonimiseerde informatie deelt over locaties in de openbare ruimte waar de deelfietsen vaker betrokken zijn bij ongelukken of over locaties waar de deelfietsen schade oplopen. De gemeente vindt het noodzakelijk om deze informatie te ontvangen, omdat zij er via andere manieren niet achter komt hoeveel verkeersongevallen met (deel)fietsen plaatsvinden, terwijl die kennis voor haar noodzakelijk is om meer precies te kunnen beoordelen op welke (kruis)punten verbeteringen moeten worden aangebracht om het aantal ongevallen met de (deel)fietsen terug te brengen. Wanneer het bedrijf voor het creëren van dat bestand ook tot personen herleidbare gegevens gebruikt (zoals tijdstippen van en locaties waarbinnen verplaatsingen plaatsvonden en de start- en eindtijd van de huur) om de door de gemeente gevraagde informatie in kaart te kunnen brengen, ligt het voor de hand aan te nemen dat de gemeente verwerkingsverantwoordelijke is.

Daarnaast zullen er situaties zijn waarin een bedrijf een geanonimiseerd gegevensbestand deelt met de gemeente waarvoor de gemeente *geen* opdracht gaf. Het ligt dan het minder voor de hand aan te nemen dat de gemeente verwerkingsverantwoordelijke is. De private partij bepaalde immers *zelf* het doel van de verwerking van de persoonsgegevens en niet de gemeente. Toch zal de gemeente ook dan moeten nagaan in hoeverre haar eigen doelstelling met het op (onder meer) persoonsgegevens gebaseerde gegevensbestand overeenkomt met de doelstelling van het bedrijf. In die gevallen kan de gemeente mogelijk een rol toekomen als gezamenlijk verwerkingsverantwoordelijke met het bedrijf.[169]

De juiste vaststelling van de rol van de gemeente ten aanzien van de persoonsgegevens is belangrijk, omdat die bepalend is voor de maatregelen die de gemeente ter bescherming van de rechten en belangen van de betrokkenen moet treffen. De vraag is echter niet eenduidig te beantwoorden en moet steeds per specifiek geval worden beoordeeld. Een belangrijke factor bij het bepalen van de rol is steeds of de gemeente het doel bepaalt waarvoor persoonsgegevens worden verwerkt (namelijk voor het creëren van een specifiek bestand). Voor het bepalen van de rol moet verder worden gekeken naar de bevoegdheidstoedeling in de specifieke wet en in voorkomende gevallen naar wijze waarop de gemeente een voorwaarde voor een vergunning, subsidie of concessie formuleert (zie hierna §3.3).

Daarnaast moet steeds worden bedacht dat de gemeente op basis van een geïsoleerd gegevensbestand niet kan uitgaan van de gedachte dat wanneer een ontvangen bestand eenmaal anoniem is, dit ook anoniem zal blijven, en dat de AVG niet van toepassing zal zijn of worden. Op de gemeente rust

[169] Art. 26 AVG.

een zorgvuldigheidsverplichting om regelmatig na te gaan of de anonimiteit steeds is geborgd, juist wanneer het geanonimiseerde bestand wordt gekoppeld met andere bestanden.

> Diverse bedrijfsmedewerkers gaven tijdens de interviews aan in beginsel open te staan voor het delen van gegevens die zij reeds zelf verzamelen, maar zij vinden het minder aantrekkelijk als zij voor de gemeente aanvullende gegevens zouden moeten verzamelen die zij zelf in eerste instantie niet verzamelen.

In sommige situaties krijgt de gemeente toegang tot gegevens via zogenoemde 'dashboards'.[170] In dergelijke dashboards kan informatie ter beschikking worden gesteld aan publieke en/of private verwerkingsverantwoordelijken (soms in publiek-private samenwerkingsverbanden), die de informatie voor eigen of gedeelde doeleinden kunnen gebruiken. Indien een dashboard persoonsgegevens bevat of informatie bevat die op persoonsgegevens is gebaseerd, dienen alle verwerkingen in of op basis van informatie uit het dashboard te voldoen aan de AVG. Wanneer meer verwerkingsverantwoordelijken voor een gemeenschappelijk doel gebruik maken van het dashboard, moeten zij als gezamenlijke verwerkingsverantwoordelijken beslissen hoe de verantwoordelijkheden ten aanzien van de persoonsgegevens verdeeld zijn. Dit met het oog op de verplichtingen die zij jegens betrokkenen hebben. Wanneer de gemeente door middel van B2G-gegevensdeling toegang verkrijgt tot persoonsgegevens in het dashboard, treedt zij op als verwerkingsverantwoordelijke (en eventueel als gezamenlijk verwerkingsverantwoordelijke).[171]

Het is niet uitgesloten dat een private partij een gegevensbestand met persoonsgegevens verstrekt aan de gemeente, waarvan niet duidelijk is of de oorspronkelijke verzameling door de private partij werd gebaseerd op een rechtmatige grondslag in de AVG.[172] Vanwege het beginsel van rechtsstatelijkheid en het belang van het vertrouwen van de samenleving in publieke diensten, dient de gemeente zich er steeds van te vergewissen dat de persoonsgegevens die zij eventueel verwerft door de private partij in overeenstemming met de AVG werden verwerkt. Zo is niet altijd duidelijk of voorafgaand aan de gegevensverzameling met een private sensor in openbare ruimten met (uitdrukkelijke) toestemming werd verkregen. De gemeente moet private partijen het goede voorbeeld geven, door bij elke voorgenomen verwerking van private sensorgegevens met persoonsgegevens – of een vermoeden daarvan – een DPIA te verrichten en de Commissie Persoonsgegevens Amsterdam te vragen om een advies over conformiteit met de AVG.[173] Indien en voor zover de gemeente voornemens is de verkregen persoonsgegevens beschikbaar te stellen aan derden, is zij gelet op het feit dat ook dan sprake is van een verwerking in de zin van de AVG, wederom gebonden aan het juridisch kader van de AVG.[174]

---

[170] Geïnterviewde gemeentemedewerkers droegen hiervan diverse voorbeelden aan. Een dashboard maakt onder meer evaluaties mogelijk nadat bijvoorbeeld een vorm van deelmobiliteit is geïmplementeerd. Op basis van het dashboard kunnen betrokken private partijen (zoals deelmobiliteitsaanbieders) en de gemeente op meer systematische wijze evalueren wat het gebruik van deelmobiliteit is, het effect op de openbare ruimte en het reisgedrag van gebruikers meten en besluiten waar ruimte voor verbetering/bijsturing ligt. CROW is een kennisplatform dat beoogt dergelijke dashboards tot ontwikkeling te laten komen zodat de betrokken verwerkingsverantwoordelijken hun eigen onderzoeken onder de gebruikers kunnen standaardiseren. Zie https://www.crow.nl/dashboard-autodelen/home/aan-de-slag-1/onderzoeken-deelmobiliteit-gemeenten, bezocht op 12 september 2022.

[171] Art. 26 AVG.

[172] Art. 6 lid 1 sub a, b of f AVG; zie §3.1.1.

[173] De Commissie Persoonsgegevens Amsterdam adviseert de gemeente Amsterdam onder meer over het privacy-beleid van de gemeente en de uitvoering daarvan. Daarnaast adviseert de commissie de ambtelijke organisatie bij complexe en/of politiek gevoelige kwesties rondom persoonsgegevens. Zie https://www.amsterdam.nl/bestuur-organisatie/organisatie/overige/adviesraden/commissie-persoonsgegevens-amsterdam/, bezocht op 28 juni 2022.

[174] Art. 4 sub 2 AVG.

3.2.3 AI-Verordening

Juridisch kader

Private sensoren die gegevens over personen in de openbare ruimte verzamelen, kunnen soms worden gekwalificeerd als "artificiële-intelligentiesystemen" (AI-systemen) in de zin van het voorstel voor een Europese AI-Verordening.[175] Private partijen die AI-systemen (willen) gebruiken voor de verzameling van gegevens in de openbare ruimte, zullen voorafgaand aan de inzet ervan moeten beoordelen of het systeem een 'onaanvaardbaar', 'hoog' of 'laag' risico met zich meebrengt voor de gezondheid, de veiligheid en de fundamentele rechten. Deze kwalificatie zal een private partij (mede) op basis van een DPIA, zoals die is voorgeschreven in AVG, moeten vaststellen.[176] Afhankelijk van de risicokwalificatie gelden specifieke regels. Sensoren uitgerust met software voor biometrische identificatie op afstand – zowel in real-time als achteraf – gelden bijvoorbeeld als AI-systemen met een hoog risico. De AI-Verordening voorziet in een meldingsplicht van hoog-risico systemen bij een toezichthoudende instantie.[177] Deze instantie kent conformiteitsbeoordelingen toe aan organisaties die voldoen aan de vereisten die de AI-Verordening stelt.[178]

Voor publieke actoren kent de concept-AI-Verordening geen zelfstandig regime rondom het gebruik van AI-systemen, al is het gebruik van AI-systemen die de betrouwbaarheid van natuurlijke personen op basis van hun gedrag analyseren ('social scoring') in beginsel verboden.[179] De overige bepalingen die het gebruik in de publieke sector reguleren, zien op toepassingen in de rechtshandhaving en vallen daarmee buiten het bestek van dit rapport.[180]

Voor het overige lijkt de AI-verordening het gebruik van biometrische identificatie op afstand toe te staan voor niet-wetshandhavingsdoeleinden, zoals crowd control of volksgezondheid.[181] Deze toepassingen vallen, voor zover er persoonsgegevens worden verwerkt, ook onder het bereik van de AVG. Bij verwerkingen van biometrische gegevens voor dergelijke publieke doeleinden dient de gemeente aldus steeds te voldoen aan de AVG en aan de grondwettelijke vereisten voor de verwerking. Gelet op het feit dat het bij de verwerking van biometrische gegevens steeds om bijzondere persoonsgegevens gaat, zullen de vereiste noodzaak, evenredigheid en subsidiariteit door de AP of de rechter aan een indringende toets worden onderworpen. Vanwege het hoge risico van AI-systemen voor fundamentele rechten en gegevensbescherming zijn publieke actoren bij voorgenomen gegevensverwerking met dergelijke systemen gehouden een DPIA uit te voeren.

Deelvraag 1: handelingsperspectief bij betere naleving van de fundamentele rechten

Op dit punt dient de gemeente de juridische kaders te volgen die zijn opgenomen bij de fundamentele rechten en bij de AVG zoals beschreven in §§3.2.1 en 3.2.2.

Deelvraag 2: normering B2G-gegevensdeling en deling met derden

In alle gevallen waarin de gemeente middels B2G-gegevensdeling sensorgegevens verkrijgt die met AI-systemen werden gegenereerd, gelden steeds de grondwettelijke vereisten, en waar persoonsgegevens bij de vorming van de gegevensbestanden of in de gegevensbestanden zelf aanwezig zijn, geldt bovendien

[175] European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021) 206 final); zie Art. 3 lid 1 sub 3 AI-Verordening.
[176] Artt. 29 lid 6 en 13 AI-Verordening en art. 35 AVG.
[177] Art. 30 AI-Verordening.
[178] Artt. 33 en 43 AI-Verordening. Bij goedkeuring ontvangt de private partij een certificaat voor een door de toezichthouder vastgestelde periode (Art. 44 AI-Verordening).
[179] Art. 5 lid 1 sub c AI-Verordening; het verbod wordt nader ingekleurd door twee voorwaarden, zie onder (i) en (ii) van hetzelfde artikel.
[180] Art. 5 lid 1 sub d en lid 2 t/m 4 AI-Verordening zien toe op AI-toepassingen in de strafvorderlijke sfeer.
[181] M. Veale & F. Zuiderveen Borgesius, 'Demystifying the draft EU Artificial Intelligence Act' (2021) *Computer Law Review International* 4, p. 97.

de AVG. Bij de verwerking van persoonsgegevens is de gemeente, gelet op risico's die kleven aan informatie die wordt gegenereerd met behulp van AI gehouden een DPIA uit te voeren. De gemeente zal bij het verrichten van een DPIA in gevallen waarin AI werd gebruikt mogelijk beperkte toegang tot relevante informatie voor de risicobeoordeling hebben. De gemeente was immers niet betrokken in het ontwerp- en ontwikkelstadium van het AI-systeem en heeft daarmee beperkt inzicht in de wijze waarop het AI-systeem werd getraind, in de bias van de trainingsgegevens of in de discriminerende vooringenomenheid die de op het AI-systeem gebaseerde private sensorgegevens met zich kunnen meebrengen, of in de foutmarges die de private partij acceptabel vond, maar die in publiekrechtelijke context problematisch zouden kunnen zijn, of in de ondoorzichtigheid en daarmee (veelal) beperkte interpreteerbaarheid van de modellen en hun voorspellingen. Private partijen zullen hun ontwerp, doelstelling en overige keuzes in het ontwerp van een AI-systeem immers inkleuren met commerciële waarden. Die waarden zijn niet voor elke toepassing in de publieke sector acceptabel. Daarmee kan het voor de gemeente erg lastig zijn om bijvoorbeeld beleids- en besluitvorming die (deels) is gebaseerd op een met een AI-systeem gegenereerde gegevens te motiveren, te rechtvaardigen en te verantwoorden.

3.2.4 Databankenwet en auteursrecht

Juridisch kader

Gegevensverzamelingen kunnen beschermd zijn op grond van het databankenrecht (het 'sui generis-databankenrecht') en op grond van het auteursrecht. Onder een databank wordt verstaan "een verzameling van werken, gegevens of andere zelfstandige elementen die systematisch of methodisch geordend en afzonderlijk met elektronische middelen of anderszins toegankelijk zijn". Voor het van toepassing zijn van het databankenrecht is vereist dat de selectie, ordening en/of presentatie van een databank getuigt van creatieve keuzes, die het persoonlijk stempel van de maker (auteur) tonen.[182] Daarnaast bestaat een sui generis databankenrecht alleen als "de verkrijging, de controle of de presentatie van de inhoud in kwalitatief of kwantitatief opzicht getuigt van een substantiële investering."[183] Kosten gemoeid met de creatie van (ruwe) gegevens tellen daarbij niet mee. Het Hof van Justitie van de Europese Unie heeft bij herhaling bepaald dat het databankenrecht niet tot doel heeft investeringen in het genereren van gegevens op zichzelf genomen, dus zonder substantiële investering in de verkrijging, de controle of de presentatie van de inhoud, te beschermen.[184]

Indien op basis van voornoemde criteria kan worden vastgesteld dat sprake is van een databank, kan een private partij zich beroepen op haar exclusieve recht om de gegevens over de databank op te vragen (geheel of gedeeltelijk overnemen, door direct of indirect kopiëren) en te hergebruiken (exploiteren, beschikbaar stellen voor anderen).[185] Andere partijen, zoals de gemeente, hebben zonder toestemming van de databankproducent geen toegang tot informatie over de databank.

Deelvraag 1: handelingsperspectief bij betere naleving van de fundamentele rechten

Ten aanzien van de verbetering van de bescherming van de fundamentele rechten van burgers zijn er geen nadere gemeentelijke handelingsperspectieven te melden die zouden kunnen voortvloeien uit deze wet.

[182] Richtlijn 96/9/EG van het Europees Parlement en de Raad van 11 maart 1996 betreffende de rechtsbescherming van databanken, Pb L 77, 27 maart 1996, p. 20; deze is omgezet in de Databankenwet (1999).
[183] Art. 1, lid 1 sub a Databankenwet.
[184] Het Hof van Justitie van de Europese Unie heeft een test ontwikkeld om na te gaan of de installatie van sensoren in een specifieke situatie kan worden aangemerkt als een investering om data te verkrijgen, zie C-444/02, (9 november 2004) *Fixtures Marketing Ltd v. Organismos Prognostikon Agonon Podosfairou* en zie T. Synodinou, 'Databases: sui generis protection and copyright protection', *Kluwer Copyright Blog* (20 december 2011).
[185] Art. 2 Databankenwet.

Deelvraag 2: normering B2G-gegevensdeling en deling met derden

Bij het sui generis databankenrecht wordt de gemeentelijke toegang tot gegevensbestanden mogelijk beperkt. De drempel voor bescherming op grond van het databankenrecht is echter niet erg hoog. Bij automatisch gegeneerde verzamelingen van sensorgegevens zal niet snel sprake zijn van een 'substantiële investering' in de 'de verkrijging, de controle of de presentatie'.[186] De Databankenwet staat dan niet in de weg aan het verkrijgen van toegang tot private sensorgegevens door de gemeente. Dat kan anders zijn als sensorgegevens zijn bewerkt en opgenomen worden in grotere gegevensverzamelingen. Sommige verzamelingen met machine-gegenereerde gegevens kunnen mogelijk profiteren van het databankenrecht, maar dit moet per geval worden beoordeeld. In die gevallen kunnen aanspraken van private partijen de gemeentelijke verwerking (en verdere deling met derde partijen) van private sensorgegevens beperken.

3.2.5 Wet bescherming bedrijfsgeheimen

Juridisch kader

Gegevensbestanden kunnen vertrouwelijke bedrijfsgegevens zijn die worden beschermd op grond van de Wet bescherming bedrijfsgeheimen (hierna: Wbbg). De houder (een natuurlijke persoon of een rechtspersoon) kan opkomen tegen derden die zich toegang verschaffen tot bedrijfsgeheime informatie of die deze informatie gebruiken. Onder een bedrijfsgeheim wordt verstaan informatie die (a) geheim is in die zin dat zij, in haar geheel dan wel in de juiste samenstelling en ordening van haar bestanddelen, niet algemeen bekend is bij of gemakkelijk toegankelijk is voor degenen binnen de kringen die zich gewoonlijk bezighouden met dergelijke informatie, (b) handelswaarde bezit omdat zij geheim is, en (c) onderworpen is aan redelijke maatregelen om deze geheim te houden.[187]

Deelvraag 1: handelingsperspectief bij betere naleving van de fundamentele rechten

Ten aanzien van de verbetering van de bescherming van de fundamentele rechten van burgers zijn er geen nadere gemeentelijke handelingsperspectieven te melden die zouden kunnen voortvloeien uit de Wbbg.

Deelvraag 2: normering B2G-gegevensdeling en deling met derden

De Wbbg beschermt houders van bedrijfsgeheimen tegen de onrechtmatige verkrijging daarvan door derden, oftewel de verkrijging zonder toestemming en op een wijze die als onrechtmatig wordt beschouwd,[188] en tegen het gebruik of openbaarmaking van het bedrijfsgeheim, wanneer dit zonder toestemming van de houder van het bedrijfsgeheim geschiedt.[189] Daarnaast kan informatie verzameld uit openbare bronnen ook de status bedrijfsgeheim krijgen, onder de voorwaarden dat die informatie wordt bewerkt of deze wordt gecombineerd met andere gegevens, en dat die informatie vervolgens geheim wordt gehouden. Daarbij dient te worden aangetekend dat op grond van de Wbbg niet kan worden voorkomen dat andere partijen dezelfde (openbare) informatie inwinnen. Het gaat er bij de beoordeling van de toepassing van de Wbbg steeds om dat de houder van de gegevens deze op een door haar bepaalde wijze heeft samengesteld en georganiseerd, en dat deze samenstelling economische waarde bezit *omdat* zij geheim is. Of private sensorgegevens verzameld in openbare ruimten onder de definitie van bedrijfsgeheimen vallen, moet steeds per geval moet worden beslist.

[186] Art. 1 lid 1 sub a Databankwet; Europese Commissie, *Evaluation of Directive 96/9/EC on the legal protection of databases*, SWD (2018) 146 final, p. 35.
[187] Art. 1 Wbbg.
[188] Art. 2 lid 1 Wbbg.
[189] Art. 2 lid 2 Wbbg.

Sommige bedrijfsmedewerkers gaven aan bereid te zijn gegevens met de gemeente te delen voor de veiligheid van openbare of voor het publiek toegankelijke ruimten, maar zij beperken dit tot niet-privacygevoelige informatie en informatie waarop geen wettelijk beschermd bedrijfsgeheim rust (en met inachtneming van overige wet- en regelgeving).

Vergelijkbaar met de Databankenwet kunnen de rechten die voortvloeien uit de Wbbg en die van toepassing zijn op een specifiek gegevensbestand de gemeentelijke toegang tot en de verwerking, waaronder het openbaar maken van private sensorgegevens beperken. Deze rechten beperken aldus de mate waarin de gemeente vrijheid toekomt private sensorgegevens die zij verkreeg via B2G-gegevensdeling verder te delen met derden. Aan het openbaren en het verder delen van via B2G gegevensdeling verkregen gegevens leggen de hierna te bespreken Wet open overheid en de recent aangenomen Datagovernanceverordening beperkingen op waarmee de gemeente rekening dient te houden. Ook kan het zijn dat de wetgever al heeft voorzien in beperkingen op de openbaarmaking van gegevens indien deze werden verkregen via B2G-gegevensdeling die gebaseerd is op een wettelijke verplichting. [190]

3.2.6 Wet open overheid

Juridisch kader

De Wet open overheid (Woo) is een generieke wet naast andere openbaarheidsregelingen. Wanneer de gemeente private sensorgegevens via B2G-gevensdeling gegevens heeft ontvangen die naar hun aard verband houden met de publieke taak, treedt een aantal wettelijke mechanismen in werking die ertoe kunnen leiden dat de gemeente deze gegevens openbaar moet maken. De Woo zet meer dan voorheen de Wet openbaarheid van bestuur deed in op actieve openbaarheid ('openbaar, tenzij').[191] Dit onder voorwaarde dat met de openbaarmaking geen onevenredige inspanning gemoeid is, de openbaarmaking een redelijk belang dient en er geen uitzonderingsgronden gelden, zoals de bescherming van privacy en persoonsgegevens, van vertrouwelijk meegedeelde bedrijfsgegevens of van intellectuele eigendomsrechten.[192] Het publieke belang bij openbaarheid wordt verondersteld aanwezig te zijn. Naast de in de Woo neergelegde geclausuleerde verplichting voor de overheid informatie openbaar te maken, staat voor eenieder de weg open om een mondeling of schriftelijk verzoek om publieke informatie in te dienen, zonder dat daartoe een belang moet worden gesteld.[193]

Voor bepaalde categorieën overheidsinformatie verplicht de Woo tot actieve openbaarmaking, maar sensorgegevens die van bedrijven werden verkregen vallen daar niet onder. Het openbaar maken van informatie blijft achterwege voor zover dit leidt tot openbaarmaking van bedrijfsgegevens die vertrouwelijk aan de overheid zijn meegedeeld, wanneer het gegevens betreft waarop intellectuele eigendomsrechten rusten of wanneer het persoonsgegevens betreft, tenzij de betrokkene uitdrukkelijk toestemming heeft gegeven voor de openbaarmaking van diens persoonsgegevens of deze door de betrokkene openbaar zijn gemaakt.

Deelvraag 1: handelingsperspectief bij betere naleving van de fundamentele rechten

Ten aanzien van de verbetering van de bescherming van de fundamentele rechten van burgers zijn er geen nadere gemeentelijke handelingsperspectieven te melden die zouden kunnen voortvloeien uit deze wet.

[190] Een uitwerking van een dergelijke beperking op het verder delen van is te vinden in bijvoorbeeld art. 19 lid 4 van de concessie voor het hoofdrailnet 2015 – 2025, die vermeldt dat gegevensverstrekking door de NS aan de concessieverlener vertrouwelijk gebeurt "zolang niet voor alle vervoerders de wettelijke verplichting geldt dat deze data openbaar worden gemaakt".
[191] Art. 3 lid 1 Woo.
[192] Art. 3 lid 1 Woo.
[193] Artt. 1.1 en 4.1 lid 1 sub 1 Woo.

Deelvraag 2: normering B2G-gegevensdeling en deling met derden

De gemeente kan private sensorgegevens die zij via B2G-gegevensdeling heeft verkregen openbaar maken, tenzij rechten en redelijke belangen zoals de bescherming van persoonsgegevens, en bedrijfsgeheimen en intellectuele eigendomsrechten van de betrokken private partijen zich daartegen verzetten.[194] In afwijking van deze uitzonderingen op de openbaarmakingsplicht kan de gemeente besluiten deze informatie alsnog openbaar te maken, indien een zwaarwegend algemeen belang, zoals het belang van de openbare veiligheid, de volksgezondheid, het milieu of de bescherming van de democratische rechtsorde, dat in een concreet geval vergt.

3.2.7 Richtlijn open data en de Wet hergebruik van overheidsinformatie

Juridisch kader

De Richtlijn open data regelt het hergebruik voor commerciële en niet-commerciële doeleinden van overheidsinformatie die reeds openbaar is.[195] De Richtlijn moedigt publieke organen aan informatie beschikbaar te stellen voor hergebruik met zo min mogelijk voorwaarden die dat hergebruik beperken.[196] Indien de overheid

- gegevens (van bijvoorbeeld private partijen) heeft verkregen,[197]
- deze gegevens openbaar zijn op grond van de Woo (of op grond van een andere openbaarheidsregeling), en
- deze gegevens binnen de reikwijdte van de Richtlijn open data en de Wet hergebruik van overheidsinformatie (hierna: Who) vallen,

kan eenieder verzoeken om de gegevens te mogen hergebruiken voor commerciële of niet-commerciële doeleinden. De overheid mag voorwaarden aan het hergebruik stellen, mits deze noodzakelijk, transparant en niet-discriminatoir zijn. Gelijke groepen afnemers moeten met het oog op het garanderen van een gelijk speelveld dus gelijk worden behandeld. De Richtlijn open data regelt niet de *toegang* tot overheidsinformatie.

De Richtlijn open data sluit in beginsel hergebruik en openstelling uit van gegevens waarvan de intellectuele eigendomsrechten en/of handelsgeheimen bij derden berusten,[198] alsook van documenten die persoonsgegevens bevatten waarvan het hergebruik wettelijk onverenigbaar is verklaard met de AVG.[199] Dat wil niet zeggen dat de overheid deze gegevens in het geheel niet kan openstellen voor hergebruik; indien nationale regelgeving voorziet in ruimere mogelijkheden voor hergebruik, kan zij deze alsnog ter beschikking stellen. De Who voorziet (vooralsnog) niet in deze uitzondering.[200]

Daarnaast kan de overheid volgens de Who een in de tijd beperkte exclusieve overeenkomst sluiten met één partij die (onder meer) persoonsgegevens of gegevens waarvan de intellectuele eigendomsrechten en/of handelsgeheimen bij derden berusten verwerkt. Zo kan de overheid een exclusief recht verlenen aan een private partij voor bijvoorbeeld de digitalisering van verzamelingen van overheidsinformatie die berusten bij musea of bibliotheken.[201] Een bepaalde periode van exclusiviteit kan noodzakelijk zijn zodat de private partij haar investering kan terugverdienen.[202] Een dergelijke exclusieve overeenkomst met één partij dient steeds noodzakelijk te zijn in het belang van het bieden van diensten of goederen met een

[194] Art. 5 lid 1 sub c en d Woo.
[195] Richtlijn 2019/1024 van het Europees Parlement en de Raad van 20 juni 2019 inzake open data en het hergebruik van overheidsinformatie (herschikking), *PbEU* L172/56.
[196] Art. 3 lid 1 Richtlijn open data.
[197] Art. 1 lid 1 sub a Richtlijn open data.
[198] Art. 1 lid 2 sub c (intellectuele eigendom) en d (iii) (handelsgeheim) Richtlijn open data.
[199] Art. 1 lid 2 sub h Richtlijn open data.
[200] Art. 2 lid 1 sub a, b en g jo art. 3 lid 5 Who.
[201] Art. 7 lid 3 Who.
[202] VNG, Handleiding Wet hergebruik van overheidsinformatie (April 2016), 28.

publiek karakter. De exclusieve overeenkomst moet daarnaast ook in overeenstemming te zijn met de bescherming van de intellectuele eigendomsrechten en/of handelsgeheimen die bij derden berusten en/of met de bescherming van persoonsgegevens. Daarnaast moet de betreffende exclusieve overeenkomst ook openbaar worden gemaakt, omdat de overheid een zo gelijk mogelijk speelveld dient te waarborgen.[203]

De recent herziene Richtlijn is tot op heden nog niet geïmplementeerd in de Nederlandse Wet hergebruik overheidsinformatie (Who); het implementatiewetsvoorstel wordt verwacht in 2023.

Deelvraag 1: handelingsperspectief bij betere naleving van de fundamentele rechten

Ten aanzien van de verbetering van de bescherming van de fundamentele rechten van burgers zijn er geen nadere gemeentelijke handelingsperspectieven te melden die zouden kunnen voortvloeien uit deze wet.

Deelvraag 2: normering B2G-gegevensdeling en deling met derden

Indien de gemeente private sensorgegevens via B2G-gegevensdeling van een private partij heeft verkregen[204] en deze gegevens binnen de reikwijdte van de Richtlijn open data en de Who vallen, kan de zij deze sensorgegevens in beginsel openstellen voor hergebruik.[205] De gemeente kan daarnaast voorwaarden aan het hergebruik stellen mits deze noodzakelijk, transparant en niet-discriminatoir zijn.

Wanneer de gemeente via B2G-gegevensdeling gegevens heeft verkregen waarvan de intellectuele eigendomsrechten en/of handelsgeheimen bij derden berusten[206] of persoonsgegevens heeft verkregen waarvan het hergebruik wettelijk onverenigbaar is verklaard met de AVG, stelt de gemeente deze, zolang de Who hierin niet voorziet, niet open voor hergebruik. Deling van deze gegevens door de gemeente met derden wordt op dit moment zoals gezegd belemmerd door de Who.[207] Afgewacht moet worden hoe de Who uiteindelijk luidt wanneer de Richtlijn open data geïmplementeerd is in de Who.

3.2.8 Datagovernanceverordening

Juridisch kader

In het verlengde van de Richtlijn open data ligt de Europese Datagovernanceverordening (hierna: DGA).[208] Hoofdstuk II van de DGA ziet op het hergebruik van bepaalde gegevenscategorieën in het bezit van openbare lichamen die zijn beschermd op grond van onder meer commerciële vertrouwelijkheid (o.a. bedrijfsgeheimen), intellectuele eigendomsrechten van derden of persoonsgegevens.[209] De DGA-bepalingen aangaande de verwerking van deze gegevenscategorieën komen overeen met de bepalingen in de Richtlijn open data die eveneens zien op deze gegevenscategorieën.

Deelvraag 1: handelingsperspectief bij betere naleving van de fundamentele rechten

Ten aanzien van de verbetering van de bescherming van de fundamentele rechten van burgers zijn er geen nadere gemeentelijke handelingsperspectieven te melden die zouden kunnen voortvloeien uit deze wet.

Deelvraag 2: normering B2G-gegevensdeling en deling met derden

De DGA staat op zichzelf genomen niet in de weg aan B2G-gegevensdeling. Wel heeft de DGA gevolgen wanneer de gemeente voornemens is de verkregen informatie te delen met andere private partijen. In

[203] Art. 7 lid 1, 2 en 5 Who.
[204] Art. 1 lid 1 sub a Richtlijn Open Data.
[205] Art. 3 lid 1 Richtlijn Open Data.
[206] Art. 1 lid 2 sub c (intellectuele eigendom) en d (iii) (handelsgeheim) Richtlijn open data.
[207] Zie voetnoot 200.
[208] Verordening 2022/868 van het Europees Parlement en de Raad van 30 mei 2022 betreffende Europese Datagovernance (Datagovernanceverordening) *PbEU* L152/1 van 30 juni 2022.
[209] Art. 3 DGA.

beginsel verbiedt de DGA dat gegevenscategorieën die commerciële vertrouwelijkheid (o.a. bedrijfsgeheimen), intellectuele eigendomsrechten van derden of persoonsgegevens betreffen, slechts aan één partij beschikbaar worden gesteld in een zogenoemde exclusieve overeenkomst, omdat een dergelijke overeenkomst het gelijke speelveld van marktpartijen kan verstoren. De DGA voorziet echter net als eerdergenoemde de Richtlijn open data en de Who in een uitzondering op deze regel, namelijk wanneer de beschikbaarstelling van de genoemde gegevens aan één partij noodzakelijk is in het belang van het bieden van diensten of goederen met een publiek karakter. De overeenkomst zelf dient in deze gevallen openbaar te worden gemaakt en mag met het oog op het niet verstoren van het gelijke speelveld maximaal 12 maanden duren. De DGA bevat net als de Richtlijn open data en de Who geen verplichting voor overheden tot het openstellen van beschermde gegevens. Wel verplicht de DGA openbare lichamen tot het vaststellen van voorwaarden die van toepassing zijn, indien wordt overgegaan tot beschikbaarstelling voor hergebruik.

3.2.9 Concept-Dataverordening

Juridisch kader

In 2022 publiceerde de Europese Commissie haar voorstel voor een Europese Dataverordening, met als doel het vastleggen van harmoniserende regelgeving voor een eerlijke toegang tot en gebruik van gegevens (inclusief persoonsgegevens, niet-persoonsgegevens en metagegevens).[210] Hoofdstuk 5 van de concept-Dataverordening ziet op regulering van situaties waarin bedrijven verplicht kunnen worden gegevens te delen met de overheid, al kan de verplichting niet aan het midden- en kleinbedrijf worden opgelegd.[211] Vrijwillige B2G-gegevensdeling op basis van bijvoorbeeld een contract valt evenmin onder de reikwijdte van de concept-Dataverordening.

Verplichte B2G-gegevensdeling kan zich voordoen in drie situaties. Allereerst kunnen bedrijven tot B2G-gegevensdeling worden verplicht wanneer die gegevens noodzakelijk zijn bij de bestrijding van uitzonderlijke noodsituaties waar een openbaar belang mee is gemoeid (zoals natuurrampen, pandemieën of situaties waarin zich cyberveiligheidsincidenten voordoen[212]) en waarin wetgeving daartoe ontoereikend of geheel afwezig is.[213] Een tweede, daaraan verwante categorie gevallen waarin B2G-gegevensdeling verplicht kan zijn doet zich voor wanneer zich nog geen uitzonderlijke noodsituatie voordoet, maar deze voorkomen dient te worden, of wanneer de samenleving van een uitzonderlijke noodsituatie moet herstellen en waar het gebrek aan private gegevens de overheid aantoonbaar hindert in het vervullen van haar publieke taak om die uitzonderlijke noodsituatie te voorkomen dan wel ervan te herstellen.[214]

De derde categorie betreft gevallen van 'uitzonderlijke noodzaak' waarin het gebrek aan beschikbare gegevens een overheidsinstantie hindert bij het vervullen van een specifieke taak van algemeen belang waarin uitdrukkelijk bij wet is voorzien.[215] Dergelijke gevallen doen zich voor wanneer het overheidsorgaan alle andere middelen die tot zijn beschikking stonden om de gegevens te verkrijgen heeft

[210] Voorstel voor een Verordening van het Europees Parlement en de Raad betreffende geharmoniseerde regels inzake eerlijke toegang tot en eerlijk gebruik van data van 23 februari 2022 (Dataverordening) COM(2022) 68 final.
[211] Hoofdstuk V is niet van toepassing op het mkb (minder dan 50 werknemers en jaarlijkse omzet van maximaal €10 miljoen (zoals gedefinieerd in Commissie Aanbeveling 2003/361 betreffende de definitie van het midden- en middenbedrijf, *PbEU* L 124 van 20 mei 2003, p. 6).
[212] Art. 2 lid 10 concept-Dataverordening definieert deze als "situations negatively affecting a major part of a member state's population or their fundamental rights, with a risk of serious and lasting repercussions on living conditions and the economic stability of the member state. Public emergencies include major natural disasters, public health emergencies as well as human-induced major disasters, such as those caused by terrorism".
[213] Art. 15 sub a Dataverordening.
[214] Art. 15 sub b Dataverordening. Voor de eerste categorie gevallen legt de concept-Dataverordening geen vergoeding vast voor de gegevensdeling. Voor de tweede categorie van gevallen voorziet de concept-Dataverordening in een vergoeding van de technische en organisatorische kosten die bedrijven moeten maken voor het beschikbaar maken van de gegevens (zie art. 20 Dataverordening).
[215] Art. 15 aanhef concept-Dataverordening.

uitgeput, door bijvoorbeeld (i) de gegevens op de markt te kopen tegen markttarieven, (ii) terug te vallen op bestaande verplichtingen om gegevens beschikbaar te stellen, of (iii) de vaststelling van nieuwe wetgevingsmaatregelen de tijdige beschikbaarheid van de gegevens niet kan garanderen.[216]

De overheid kan de bevoegdheid niet gebruiken voor strafrechtelijke of bestuursrechtelijke handhavingsbevoegdheden.[217] Gegevens die op grond van hoofdstuk 5 van de Verordening werden verkregen, mogen in beginsel niet beschikbaar woorden gesteld voor hergebruik in de zin van de Richtlijn open data. Hierbij is echter een uitzondering opgenomen; overheidsinstanties kunnen gegevens beschikbaar stellen aan personen en organisaties die wetenschappelijk onderzoek verrichten of aan nationale bureaus voor de statistiek en Eurostat.[218]

Deelvraag 1: handelingsperspectief bij betere naleving van de fundamentele rechten

Ten aanzien van de verbetering van de bescherming van de fundamentele rechten van burgers zijn er geen nadere gemeentelijke handelingsperspectieven te melden die zouden kunnen voortvloeien uit deze wet.

Deelvraag 2: normering B2G-gegevensdeling en deling met derden

De EU-wetgever plaatst verplichte B2G-gegevensdeling in de context van een 'uitzonderlijke noodzaak', hetgeen op het eerste gezicht de mogelijkheden van een wettelijk verplichte B2G-gegevensdeling lijkt te beperken. De concept-Dataverordening laat echter ruimte voor de nationale wetgever om verplichte B2G-gegevensdeling te reguleren. Dit blijkt uit de derde categorie van gevallen (zie het juridisch kader hierboven) in artikel 15 c concept-Dataverordening. Hieruit blijkt dat de EU-wetgever erkent dat er situaties kunnen bestaan waarin een overheidsinstantie wordt gehinderd een bij wet voorziene publieke taak te verrichten, omdat de overheidsinstantie niet kan terugvallen op bestaande wettelijke verplichtingen, omdat gegevens niet op een andere wijzen konden worden verkregen (bijvoorbeeld via aankoop op de markt) of omdat vaststelling van nieuwe wetgeving niet tijdig beschikbaar is. Hieruit leiden wij af dat de EU-wetgever erkent dat B2G-gegevensdeling in de context van een uitzonderlijke noodzaak verplicht kan zijn, ook wanneer bestaande wetgeving geen of onvoldoende grondslag biedt of de totstandkoming ervan tijdige beschikbaarheid van de gegevens niet kan garanderen. Of van een uitzonderlijke noodzaak sprake is moet de betrokken overheidsinstantie per specifiek geval aantonen.[219]

In de Nederlandse context is een mogelijkheid voor verplichte B2G-gegevensdeling bijvoorbeeld vastgelegd in een specifieke regeling van artikel 30c Wet personenvervoer (Wp). Op grond hiervan kan de minister van Infrastructuur en Waterstaat bij of krachtens algemene maatregel van bestuur regels over het verplicht beschikbaar stellen van geanonimiseerde gegevens over reizigersstromen die uit het gebruik van vervoerbewijzen zijn af te leiden.[220] De minister van IenW heeft van deze bevoegdheid tot nu toe echter nog geen gebruik gemaakt, maar de gemeente kan bij de minister aandringen op de uitvoering van deze bepaling. In vervolgonderzoek zou kunnen worden nagegaan of de huidige wetgeving andere, vergelijkbare specifieke wettelijke bepalingen kent die tot B2G-gegevensdeling kunnen verplichten, en waartoe binnen gemeenten een noodzaak bestaat. Voor zover vergelijkbare wetgeving al bestaat, lijkt meer algemeen aan wetgeving rondom B2G-gegevensdeling nog geen eenduidig beleid ten grondslag te liggen. Dat kan een versnipperd beeld over de toelaatbaarheid van verplichte B2G-gegevensdeling oproepen. Indien de gemeente aanleiding ziet voor regulering van B2G-gegevensdeling in andere sectoren, zou zij de formele wetgever kunnen aansporen dergelijke wetgeving in de gewenste sectoren tot stand te brengen.

---

[216] Art. 15 sub c Dataverordening.
[217] Art. 16 lid 2 concept-Dataverordening.
[218] Art. 21 Dataverordening. Om hiervoor in aanmerking te komen, moeten derden handelen zonder winstoogmerk of in het kader van een in het recht van de Europese Unie of van een lidstaat erkende opdracht van openbaar belang.
[219] Art. 3 lid 10 concept-Dataverordening definieert wat een "algemene noodsituatie" is; blijkens de aanhef van art. 15 is een "uitzonderlijke noodzaak" een uitwerking van een algemene noodsituatie.
[220] Zie hierna §3.3.3, waar we de concessie bespreken.

Een voorbeeld waarin de EU-wetgever onder meer B2G-gegevensdeling heeft gereguleerd is te vinden in de ITS-Richtlijn 2010/40 en de bijbehorende gedelegeerde Verordening over realtimeverkeersinformatiediensten.[221]

De concept-Dataverordening laat ruimte voor de nationale wetgever om B2G-gegevensdeling te reguleren, en voor vrijwillige B2G-gegevensdeling. De EU-wetgever laat echter een kans liggen om voorwaarden voor een wetsconforme, technisch haalbare, maatschappelijk aanvaardbare, financieel- en commercieel levensvatbare B2G-gegevensdelingen te creëren,[222] en daarmee op meer effectieve wijze de huidige machtsverschillen tussen publieke sectoren en grote platforms aan te pakken,[223] maar ook om toekomstige verschillen tussen lidstaten bij voorbaat zoveel mogelijk te vermijden en een gelijk speelveld te creëren. Ook de meest recente versie van de concept-Dataverordening bevat nauwelijks gedetailleerde voorwaarden of beginselen om transacties rondom B2G-gegevensdeling billijker te maken voor de publieke sector.[224]

Gemeenten kunnen bij vrijwillige B2G-gegevensdeling bovendien nog steeds geconfronteerd worden met onevenwichtige machtsverhoudingen, waaruit onrechtvaardige contractbepalingen en hoge prijzen voor gegevensbestanden kunnen voortvloeien. Op dit moment is er wellicht nog tijd om de nadere normering rondom B2G-gegevensdeling tot stand te (laten) brengen die het delen van private sensorgegevens ten behoeve van het algemeen belang onder redelijke condities mogelijk maken, zodat B2G-gegevensuitwisseling de samenleving ten goede kan komen. Het bepalen van een redelijke beprijzing van de gegevensdeling, de maximum levertijd of de kwaliteit van de gegevens die vereist is kunnen hierbij behulpzaam zijn.

Nederlandse overheden die B2G-gegevensdeling bij de wetgever willen bepleiten, moeten zich er evenwel van bewust zijn dat uit de publieksconsultatie naar voren kwam dat de industrie geen voorstander is van bindende regels rond het delen van B2G-gegevens, en dat het Nederlandse standpunt over B2G-gegevensdeling tot nu toe terughoudend is.[225]

---

[221] Zie Richtlijn 2010/40 van het Europees Parlement en de Raad van 7 juli 2010, *Pb EU* L 207/1 (6 augustus 2010) betreffende het invoeren van intelligente vervoerssystemen op het gebied van wegvervoer en voor interfaces met andere vervoerswijzen, die regels en voorwaarden vastlegt voor de invoering van Intelligente Transportsystemen, ofwel een systeem waarin communicatie- en informatietechnologie toegepast wordt voor wegvervoer, -infrastructuur, -voertuigen en -gebruikers. Art. 4 lid 5 verstaat onder ITS-dienstaanbieders ook particuliere aanbieders van ITS-diensten. Met de uitwisseling van informatie kunnen files verminderd worden, veiligheids- en andere digitale toepassingen in auto's beter werken en mensen gemakkelijker hun reis met het openbaar vervoer uitstippelen (uit: Kenniscentrum Europa Decentraal, *Intelligente Transportsystemen ITS*, 29 oktober 2022, https://europadecentraal.nl/onderwerp/vervoer/intelligente-transportsystemen-its/, bezocht op 27 november 2022). Lidstaten kiezen zelf of zij een ITS invoeren, maar wanneer zij hiertoe overgaan moet dit gebeuren volgens de regels van de (gedelegeerde) Verordening (EU) 2015/962 van de Commissie van 18 december 2014 ter aanvulling van Richtlijn 2010/40/EU van het Europees Parlement en de Raad wat de verlening van EU-wijde realtimeverkeersinformatiediensten betreft, *Pb Eu* L 157/21 (23 juni 2015). Deze Verordening wordt in 2025 vervangen door Gedelegeerde Verordening 2022/670/EU van 2 februari 2022 ter aanvulling van Richtlijn 2012/40/EU van het Europees Parlement en de Raad wat betreft de verlening van EU-wijde realtimeverkeersinformatie, PB EU L 122/1 van 25 april 2022). Zie ook Kennisplatform CROW, Real time Traffic Information. Zie voor een duiding van de nieuwe RTTI gedelegeerde verordening voor wegbeheerders: https://www.crow.nl/downloads/pdf/verkeer-en-vervoer/verkeersmanagement/d397_real-time-traffic-information_nl.aspx, bezocht 27 op november 2022.

[222] A. Tarkowski e.a., 'A public interest framework for Business to Government data sharing in the Data Act' (2022) Open Future Policy Brief no. 3.

[223] B. Martens & D. Brown, The economics of Business to Government data sharing, JRC Working Papers on Digital Economy 2020-04, Joint Research Centre, European Commission.

[224] Zie Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) - First Presidency compromise text (Chapters VI-XI) van 9 september 2022.

[225] Bij de openbare raadpleging heeft de industrie zich uitgesproken tegen verplichte B2G-gegevensdeling (C. Perarnaud & R. Fanni, *The EU Data Act: Towards a new European data revolution?*, Centre for European Data Studies (Vrije Universiteit Brussel 2022). De Nederlandse Rijksoverheid publiceerde een '*non-paper*' waarin het zijn positie met betrekking tot de concept-Dataverordening uiteenzet, zie https://www.permanentrepresentations.nl/permanent-representations/pr-eu-brussels/documents/publications/2021/10/1/non-paper-on-the-data-act, bezocht op 1 september 2022.

3.3 Bestuurlijke instrumenten voor gemeentelijke sturing op private sensorgegevens

In deze paragraaf gaan wij in lijn met de onderzoeksvraag en de deelvragen in op de bestuurlijke instrumenten die de gemeente kan inzetten om ten aanzien van de verzameling en het gebruik van gegevens, die worden vergaard met behulp van sensoren door private partijen in de openbare ruimte, aanvullende voorwaarden te stellen. Die voorwaarden kunnen gaan over de bescherming van fundamentele rechten in de openbare ruimte. Het kunnen ook voorwaarden zijn die zien op het delen van private sensorgegevens met de gemeente (B2G-gegevensdeling). Daarbij plaatsen wij nogmaals de kanttekening dat de gemeente niet uit is op alle private sensorgegevens die in de openbare ruimte zijn vergaard.

3.3.1 Inleiding en aanpak

De gemeente heeft zowel publiekrechtelijke als privaatrechtelijke instrumenten tot haar beschikking. Het instrument van een wet in formele zin valt daarbuiten, aanzien dat instrument is voorbehouden aan de regering en de Staten-Generaal. Wel is het mogelijk dat de gemeente er – al dan niet via de VNG en andere netwerkpartners – toe oproept om (een artikel in) een wet in formele zin vast te stellen over de verzameling en het gebruik van private sensorgegevens.[226] Vanuit het oogpunt van onder meer de borging van fundamentele rechten van private partijen (§3.2.1 e.v.) heeft het vaststellen van (een artikel in) een wet in formele zin over dit onderwerp de voorkeur.

Met het voorgaande in gedachten, wordt hier in overleg met de opdrachtgever ingegaan op de volgende *publiekrechtelijke* instrumenten: gemeentelijke verordening, vergunningstelsel, subsidie (§3.3.2)[227] en op de volgende *privaatrechtelijke* instrumenten: overeenkomst, overheidsopdracht, concessie (§3.3.3). Tot slot gaan wij in op de zogenoemde *soft law*-instrumenten, die zowel publiekrechtelijk als privaatrechtelijk van aard kunnen zijn (§3.3.4).

Een aan het publiekrecht ontleende bevoegdheid om een instrument in te zetten is rechtstreeks publiekrechtelijk genormeerd. Wat betreft die normering gaat het om (Europese) regelgeving, fundamentele rechten en algemene beginselen van behoorlijk bestuur. Gaat het om een aan het privaatrecht ontleende bevoegdheid om een instrument in te zetten, dan wordt dat instrument op grond van de schakelbepaling uit artikel 3:14 BW en vaste rechtspraak tevens genormeerd door fundamentele rechten en algemene beginselen van behoorlijk bestuur. Het uitgangspunt is aldus dat het bestuur die normering niet kan 'ontlopen' door gebruik te maken van zijn privaatrechtelijke bevoegdheden.[228] Vergelijk hierover verder §3.3.3.

---

[226] Zo ook de AP in: *Smart Cities. Onderzoeksrapport bescherming van persoonsgegevens in de ontwikkeling van Nederlandse Smart Cities*, juli 2021, p. 27.

[227] Vergelijk wat betreft de mogelijkheden op grond van de nog niet inwerking getreden Omgevingswet, de bijdrage van A. Nijboer in het boek *Smart & Leefbaar – Belangen borgen in de digitaliserende gemeente*.

[228] Vergelijk hierover R.J.N. Schlössels, 'De beginselen van behoorlijk bestuur bij 'privaat bestuur'. Algemene normen, gevarieerde rechterlijke toetsing en organisatorische breuklijnen' en C.J.H. Jansen, 'Toepassing van de beginselen van behoorlijk bestuur door de Nederlandse burgerlijke rechter', in: *De polsstok van de beginselen van behoorlijk bestuur. Export en reflexwerking?*, Nijmegen: Wolf Publishers 2021, p. 11-45 en p. 47-81; R. Ortlep & V.A. van Waarde, 'Revolverend publiek geld in het echt! Dienstbaar in alle mogelijke soorten en maten?', in: L.W. Verboeket e.a. (red.), *Bestuursrecht in het echt. Vriendenbundel voor prof. mr. drs. Willemien den Ouden*, Deventer: Wolters Kluwer 2021, p. 417-432.

3.3.2 Publiekrechtelijke instrumenten

Gemeentelijke verordening

Een eerste publiekrechtelijk instrument dat hier wordt besproken, is de autonome verordenende bevoegdheid. Dat instrument is in het bijzonder van belang omdat het de grondslag kan zijn voor een eventueel vergunningstelsel (zie de volgende paragraaf).[229] De bevoegdheid tot het vaststellen van een gemeentelijke verordening wordt zowel gevonden in de Grondwet (artikel 124, eerste lid) als in de Gemeentewet (artikel 108, eerste lid). Uit de wet en de rechtspraak volgen in elk geval drie grenzen aan de autonome verordenende bevoegdheid, te weten: de territoriale grens, de bovengrens en de benedengrens.[230] De geografische grens van de gemeente Amsterdam (de territoriale grens) spreekt hier voor zich, waarbij wij evenwel wijzen op de ruime definitie van 'sensoren' in §1.5.4.

Wat betreft de bovengrens gaat het om de hiërarchie van wettelijke normen en daarmee om de verhouding van een gemeentelijke verordening tot bijvoorbeeld algemene maatregelen van bestuur, provinciale verordeningen, ministeriële regelingen, wetten in formele zin, waaronder de Grondwet, verdragen en EU-regelgeving. Zowel de Grondwet als verdragen zijn in het bijzonder van belang voor de fundamentele rechten (besproken in §3.2.1 e.v.).

De artikelen 121 en 122 Gemeentewet zien op de *bovengrens* en zijn van kracht indien een artikel van een gemeentelijke verordening en een artikel van een hogere regeling betrekking hebben op hetzelfde onderwerp. Van hetzelfde onderwerp is sprake als zowel het onderwerp (materie) als het motief van beide artikelen overeenstemmen. Zien de artikelen op hetzelfde onderwerp maar met een ander motief, dan is er geen sprake van hetzelfde onderwerp en zijn de artikelen 121 en 122 Gemeentewet niet van kracht. Niettemin is het in een dergelijk geval niet toegestaan om met een lagere regeling een hogere regeling te doorkruisen.[231] Zien beide artikelen wel op hetzelfde onderwerp, dan wordt er een onderscheid gemaakt tussen een anterieure verordening en posterieure verordening. Op grond van artikel 121 Gemeentewet is de gemeenteraad bevoegd om een hogere regeling nadien, dus bij een latere (posterieure) verordening, aan te vullen, zolang dat geen strijd oplevert. Of daarvan sprake is, hangt niet alleen af van de verenigbaarheid van de tekst van beide regelingen, maar ook of de hogere regelgever de regeling uitputtend heeft bedoeld en of het artikel van een gemeentelijke verordening een artikel uit een hogere regeling dupliceert.[232] Gaat het om een eerdere (anterieure) verordening die bestaat op het moment dat een hogere regeling in hetzelfde onderwerp voorziet (de hogere regelgever heeft het onderwerp als het ware toegeëigend), dan vervalt het artikel uit een eerdere (anterieure) verordening op grond van artikel 122 Gemeentewet van rechtswege, zelfs als zich geen enkele strijd tussen beide artikelen voordoet.[233]

De laatste grens, de *benedengrens*, ziet erop dat een gemeentelijke verordening beperkt moet zijn tot het regelen van datgene dat zich in de openbare of publieke sfeer bevindt en daarmee een gemeentelijk belang dient.[234] Zowel in de Grondwet (artikel 124, eerste lid) als in de Gemeentewet (artikel 108, eerste lid) wordt gesproken van de 'huishouding' respectievelijk het 'belang van de gemeente' (artikel 149). Tot de gemeentelijke huishouding behoren bijvoorbeeld de bescherming van de openbare orde, het voorkomen van gevaar of hinder en de bescherming van veiligheid of gezondheid van personen. Het is verdedigbaar

[229] Vergelijk de Modelverordening smartcity toepassingen in de openbare ruimte van Kennedy Van der Laan (digitaal beschikbaar via https://future-city.nl/modelverordening/).
[230] Vergelijk de conclusie van advocaat-generaal E.J. Hofstee van 2 juni 2020, ECLI:NL:PHR:2020:517, met vele literatuurverwijzingen. Zie verder J.G. Brouwer & A.E. Schilder, 'Over een controversiële conflictregel. Verordening vervallen: fatale vergissing?', in: L.W. Verboeket e.a. (red.), *Bestuursrecht in het echt. Vriendenbundel voor prof. mr. drs. Willemien den Ouden*, Deventer: Wolters Kluwer 2021, p. 627-638 en H. van Kolfschooten c.s., *Juridisch instrumentarium voor een gezonde voedselomgeving in de stad*, Universiteit van Amsterdam 2020, p. 32 e.v.
[231] In de literatuur wordt dan gesproken van 'ontoelaatbare oneigenlijke aanvulling'.
[232] Een bekend voorbeeld is ABRvS 13 juli 2011, ECLI:NL:RVS:2011:BR1425 (*Blowverbod Amsterdam*).
[233] Vergelijk recent HR 15 december 2020, ECLI:NL:HR:2020:1993.
[234] Vergelijk de uitleg bij de Modelverordening smartcity toepassingen in de openbare ruimte van Kennedy Van der Laan (digitaal beschikbaar via https://future-city.nl/modelverordening/).

dat het belang van de bescherming van de fundamentele rechten van personen op wie private sensorgegevens uit Amsterdam betrekking hebben, binnen de gemeentelijke huishouding valt.

Hetzelfde is in mindere mate het geval voor het belang van de gemeente om ten behoeve van de uitvoering van haar publieke taken – en in het verlengde daarvan, het belang van andere in de stad opererende organisaties, zoals onderzoeksinstellingen of ondernemers actief binnen de gemeente – toegang te verkrijgen tot (informatie over) private sensorgegevens die zijn verkregen in de openbare ruimte, opdat zij die gegevens kunnen gebruiken voor de verwezenlijking van publieke doeleinden. Het belang moet duidelijk zijn en zien op de gevolgen voor de openbare ruimte, anders heeft de regulering geen betrekking op de huishouding van de gemeente en is er strijd met de benedengrens.

In aansluiting op het voorgaande mag een gemeentelijke verordening niet louter treden in een particulier belang. Dit betekent niet dat de enkele omstandigheid dat een gemeentelijke verordening naast publieke (openbare) belangen tevens particuliere belangen raakt, in strijd is met de benedengrens, maar wel dat, zoals gezegd, publieke (openbare) belangen duidelijk dienen te zijn.[235] Het betekent verder ook niet dat een gemeentelijke verordening vanwege een publiek belang – maar wel binnen de grenzen van de fundamentele rechten – gedragingen kan reguleren die zich afspelen op het particulier terrein. In de literatuur wordt hiervan als voorbeeld gegeven de in gemeenten geldende Verordening kwaliteitseisen kinderopvang en peuterspeelzalen. Een gemeenteraad stelt hierin kwaliteitseisen in aanvulling op de Wet kinderopvang en kwaliteitseisen peuterspeelzalen aan peuterspeelzalen die geen deel uitmaken van de openbare ruimte.[236] Zo bezien hoeft het niet in strijd te zijn met de benedengrens als in een gemeentelijke verordening een regeling wordt opgenomen over de verzameling en het gebruik van gegevens (waaronder persoonsgegevens), die worden vergaard met behulp van sensoren door private partijen in zowel de openbare ruimte als de niet-openbare ruimte.

Vergunningstelsel

Een volgend publiekrechtelijk instrument dat hier wordt besproken, is een vergunningstelsel.[237] De keuze voor een vergunningstelsel wordt in de gemeentelijke praktijk vaak afgewogen tegen de keuze van een stelsel van algemene regels met eventueel een meldingsplicht. In een gemeentelijke verordening heeft bijvoorbeeld de gemeente Amsterdam een meldingsplicht voor sensoren in de openbare ruimte ingevoerd en de gemeente Utrecht een meldingsplicht voor camera's in de openbare ruimte. Net zoals bij een vergunningstelsel is een stelsel van algemene regels met eventueel een meldingsplicht een instrument waarmee regulerend kan worden opgetreden. De eisen die worden gesteld, zijn opgenomen in voor eenieder geldende regels die bij verrichting van de betreffende handeling moeten worden nageleefd.[238] Met een stelsel van algemene regels met eventueel een meldingsplicht kan over het algemeen meer rechtszekerheid worden bereikt dan met een vergunningstelsel. Voordat aan een activiteit kan worden begonnen waarop algemene regels van toepassing zijn, is immers al duidelijk aan welke voorwaarden die activiteit moet voldoen. Een nadeel van een stelsel van algemene regels met eventueel een meldingsplicht ten opzichte van een vergunningstelsel is dat vaak pas achteraf, te weten als de activiteit reeds wordt verricht, door het bestuur zal worden getoetst of een handeling in overeenstemming is met de regels. Betreft het de bescherming van een zwaarwegende belangen, dan kan dit maatschappelijk gezien niet of moeilijk aanvaardbaar zijn.

---

[235] Hetzelfde is vereist voor de verwerking van persoonsgegevens in de openbare ruimte (vergelijk art. 6, eerste lid, onder e, AVG). Vergelijk de AP in: *Smart Cities. Onderzoeksrapport bescherming van persoonsgegevens in de ontwikkeling van Nederlandse Smart Cities*, juli 2021, p. 9-10.

[236] Brouwer & Schilder 2021, p. 630-631.

[237] Vergelijk de Modelverordening smartcity toepassingen in de openbare ruimte van Kennedy Van der Laan (digitaal beschikbaar via https://future-city.nl/modelverordening/). Let wel: op grond van art. 3 van die modelverordening is het doel van de verordening de bescherming van persoonsgegevens en het waarborgen van een duurzame inzet van sensoren, en dus (nog) niet dat de gemeente sensorgegevens kan gebruiken voor de verwezenlijking van publieke doeleinden.

[238] Vergelijk de conclusie van staatsraad advocaat-generaal R.J.G.M. Widdershoven van 12 november 2014, ECLI:NL:RVS:2014:4116; B.J. Schueler e.a., *Evaluatie van een drietal versnellingsinstrumenten uit de Awb*, Oisterwijk: WLP 2013 en *Kamerstukken II* 2013/14, 33750-VI, 100.

Het invoeren of aanpassen van een vergunningstelsel, alsmede een stelsel van algemene regels met eventueel een meldingsplicht, is rechtstreeks publiekrechtelijk genormeerd. Wat betreft die normering gaat het – zoals gezegd – om (Europese) regelgeving, fundamentele rechten en algemene beginselen van behoorlijk bestuur. Hier is in het bijzonder het specialiteitsbeginsel van belang. Het specialiteitsbeginsel hangt sterk samen met het verbod van *détournement de pouvoir* (vastgelegd in artikel 3:3 Awb) en het legaliteitsbeginsel: bestuursbevoegdheden worden toegekend met het oog op bepaalde doelen en mogen alleen daarvoor worden aangewend. Het specialiteitsbeginsel (vastgelegd in artikel 3:4, eerste lid, Awb) houdt in het bijzonder in dat de aanwending van bestuursbevoegdheden beperkt dient te blijven tot die belangen die de desbetreffende wettelijke regeling beoogt te beschermen. Zo verzet als uitgangspunt het specialiteitsbeginsel zich ertegen dat het bestuur een aanvraag voor een vergunning afwijst op gronden die zijn ontleend aan andere belangen dan die ter bescherming waarvan het vergunningstelsel in het leven is geroepen.[239] Hetzelfde uitgangspunt is van toepassing voor het aan een vergunning verbinden van (aanvullende) voorwaarden (voorschriften).[240]

Voor het invoeren of aanpassen van een vergunningstelsel, waaronder het aan een vergunning verbinden van (aanvullende) voorwaarden (voorschriften), is het gelet op het specialiteitsbeginsel noodzakelijk om het *belang* van het beter beschermen van de fundamentele rechten van *personen op wie de private sensorgegevens betrekking* hebben, in de wettelijke regeling op te nemen. Hetzelfde geldt in voorkomende gevallen voor het belang van de gemeente om ten behoeve van de uitvoering van haar publieke taken toegang te verkrijgen tot (informatie over) private sensorgegevens die zijn verkregen in de openbare ruimte en die te gebruiken voor de verwezenlijking van publieke doeleinden.

Heeft het invoeren of aanpassen van een vergunningstelsel, waaronder het aan een vergunning verbinden van (aanvullende) voorwaarden (voorschriften), (mede) betrekking op dienstverlening, dan moet ook de Dienstenrichtlijn (Richtlijn 2006/123) en de bijbehorende Dienstenwet in acht worden genomen.[241] Dit betekent dat een vergunningstelsel non-discriminatoir is, gerechtvaardigd wordt om een dwingende reden van algemeen belang en het nagestreefde doel niet door een minder beperkende maatregel kan worden bereikt (artikel 9 Dienstenrichtlijn).[242] Daarnaast moeten de voorwaarden om voor een vergunning in aanmerking te komen niet-discriminatoir, gerechtvaardigd om een dwingende reden van algemeen belang, evenredig, duidelijk en ondubbelzinnig, objectief, vooraf openbaar bekendgemaakt, transparant en toegankelijk zijn (artikel 10 Dienstenrichtlijn). Verder moet de vergunningsprocedure (artikel 13 Dienstenrichtlijn) worden gebaseerd op objectieve en transparante regels om te waarborgen dat aanvragen voor een vergunning onpartijdig worden behandeld en mag de procedure geen ontmoedigend effect hebben en de dienstverrichting niet onnodig bemoeilijken of vertragen. Tot besluit op dit punt mogen de vergunningsvoorwaarden niet worden gesteld wegens economische belangen (artikel 14, vijfde lid, Dienstenrichtlijn).

> Een voorbeeld biedt het vergunningstelsel voor deelvoertuigen c.q. bromfietsen in de gemeente Amsterdam. De gemeente verdeelt de vergunningen aan de hand van een vergelijkende toets als het aantal vergunningaanvragen het vergunningplafond van twee vergunningen overschrijdt.[243] In de Nadere regels voor deelvoertuigen Amsterdam 2019 worden aan vergunningaanvragers en -houders diverse eisen opgelegd met betrekking tot privacybescherming en het delen van sensorgegevens met de gemeente. Hierbij valt een aantal zaken op. Ten eerste zijn deze eisen niet (duidelijk) terug te voeren op de in artikel 2.50A, derde lid, APV Amsterdam geformuleerde doelen. Zij vloeien wel voort uit de achterliggende beleidsnota '*Deelmobiliteit,*

[239] Een bekend voorbeeld is ABRvS 12 november 2014, ECLI:NL:RVS:2014:4117 (*Intocht van Sinterklaas*).
[240] ABRvS 7 december 2016, ECLI:NL:RVS:2016:3253.
[241] De artikelen van de Dienstenrichtlijn hebben geen betrekking op het aangaan van overeenkomsten met het oog op het verrichten van een specifieke dienst, waarop de regels inzake overheidsopdrachten van toepassing zijn. De Dienstenrichtlijn is dus niet van toepassing op concessies voor openbare diensten die vallen onder de Concessierichtlijn (Richtlijn 2014/23) en daarmee de Aanbestedingswet.
[242] Vergelijk ABRvS 7 juni 2017, ECLI:NL:RVS:2017:1520 (*Rondvaartboten Amsterdam*).
[243] Zie art. 2.50A APV Amsterdam en de Nadere regels voor deelvoertuigen Amsterdam 2019.

kansen voor de stad. Beleid voor het delen van schone vervoermiddelen anders dan de auto'. Ten tweede zijn deze eisen niet alleen in de vorm van voorschriften (artikel 2.11) neergelegd, maar ook als weigeringsgronden (artikel 2.8) en als beoordelingscriteria (artikel 2.10). Hierbij merken wij op dat alle drie deze vormen onzes inziens moeten voldoen aan de hierboven geschetste wettelijke kaders, inclusief de voorwaarden die voortvloeien uit de Dienstenrichtlijn. Wat niet als voorschrift of als weigeringsgrond mag worden opgelegd, kan dus ook niet in een beoordelingscriterium worden vervat. Ten derde valt de betrekkelijk korte vergunningduur van twee tot maximaal drie jaar op (artikel 2.50A, lid 5c, APV Amsterdam). Daarbij merken wij op dat de rechter bij de beoordeling van vergunningstelsels rekening houdt met de terugverdientijd.[244] Eisen met betrekking tot het verzamelen en delen van sensorgegevens kunnen van invloed zijn op de terugverdientijd, zeker als die gepaard gaan met de nodige investeringen door de vergunninghouder.[245] Uit de interviews met bedrijfsmedewerkers blijkt evenwel dat zij over het algemeen positief zijn over het door de gemeente Amsterdam ingevoerde vergunningstelsel voor deelvoertuigen. Als voordelen noemen zij dat de vergelijkende toets de kwaliteit van de aanbieders bevordert en dat de eisen en criteria voor elke aanvrager gelijk zijn (*level playing field*). Verder kwam in de interviews met bedrijfsmedewerkers naar voren dat een of meer tussentijdse updates van de gemeente over de wijze waarop de sensorgegevens worden ingezet, op prijs zouden worden gesteld. Vergunninghouders weten dan beter 'waar zij het voor doen' en kunnen bovendien meedenken over het anders of vaker delen van sensorgegevens met de gemeente.

Subsidie

Het volgende publiekrechtelijk instrument dat hier wordt besproken, betreft de subsidie. Op grond van artikel 3, eerste lid, van de Algemene Subsidieverordening Amsterdam 2013 is het college van burgemeester en wethouders bevoegd om subsidie te verstrekken voor activiteiten op de beleidsterreinen die in de begroting zijn opgenomen, waaronder in ieder geval de beleidsterreinen die worden genoemd in artikel 2, eerste lid. Het gaat bijvoorbeeld om maatschappelijke dienstverlening en sociale voorzieningen, vervoer en infrastructuur, openbare ruimte, economie en stedelijke ontwikkeling. Deze ruime wettelijke grondslag voor subsidieverstrekking betekent dat het college van burgemeester en wethouders bevoegd is om subsidie te verstrekken voor c.q. ter stimulering van de aanschaf van sensoren door private partijen.[246] In dat verband kunnen aan deze sensoren eisen worden gesteld die erop zijn gericht om de fundamentele rechten van personen op wie de private sensorgegevens die de subsidieontvanger verzamelt betrekking hebben, te waarborgen. Voorts is het college van burgemeester en wethouders bevoegd om (incidenteel) subsidie te verstrekken aan belangenorganisaties die opkomen voor de fundamentele rechten van personen op wie in Amsterdam verzamelde private sensorgegevens betrekking hebben.

Kan het college van burgemeester en wethouders ook in andere (bestaande) subsidierelaties verplichtingen opleggen die verband houden met private sensorgegevens? Deze vraag valt in twee deelvragen uiteen:

- Kan het college van burgemeester en wethouders bij subsidieverstrekking aan de subsidieontvanger verplichtingen opleggen die ertoe strekken dat de fundamentele rechten van personen op wie de private sensorgegevens die de subsidieontvanger verzamelt betrekking hebben, worden beschermd?
- Kan het college van burgemeester en wethouders bij subsidieverstrekking aan de subsidieontvanger verplichtingen opleggen die ervoor zorgen dat de subsidieontvanger verplicht is om de gemeente Amsterdam private sensorgegevens die zijn verkregen in de openbare ruimte over te dragen, zodat de gemeente die gegevens kan gebruiken voor publieke doeleinden?

[244] Bijvoorbeeld ABRvS 21 juli 2021, ECLI:NL:RVS:2021:1588, *Gst.* 2021/127, m.nt. A. Drahmann. Vergelijk overweging 62 van de considerans bij de Dienstenrichtlijn.
[245] Vergelijk Christiaan Behrens e.a., *Schaarse vergunningen en terugverdientijd in de ambulante handel*, Amsterdam: SEO Economisch Onderzoek 2021.
[246] Vergelijk *Sensoren en de rol van gemeenten. VNG Realisatie Whitepaper*, Den Haag: VNG 2018, p. 26.

In de subsidietitel van de Algemene wet bestuursrecht zijn regels opgenomen over het opleggen van subsidieverplichtingen.[247] In de eerste plaats worden in artikel 4:37, eerste lid, Awb acht soorten subsidieverplichtingen genoemd die bestuursorganen in ieder geval kunnen verbinden aan besluiten tot subsidieverlening. Hiervoor is dus geen afzonderlijke grondslag nodig in een subsidieregeling. Het gaat hierbij onder meer om verplichtingen die zien op de aard en omvang van de activiteiten waarvoor de subsidie wordt verleend (onder a) en de administratie van aan de activiteiten verbonden uitgaven en inkomsten (onder b). Met name de a-grond is zeer ruim. Dit betekent dat indien het verzamelen van private sensorgegevens kan worden gerelateerd aan de activiteiten die worden gesubsidieerd en daarmee ook aan de verwezenlijking van het doel van de subsidie, het mogelijk is om hierover verplichtingen in het besluit tot subsidieverlening op te nemen. Dit zal dan in het besluit tot subsidieverlening goed moeten worden uitgelegd. Of het ook mogelijk is om onder deze noemer de verplichting op te nemen dat de verkregen private sensorgegevens worden gedeeld met de gemeente, hangt erg af van de doelstelling van de subsidie. Is het voor het bereiken van het doel van de subsidie noodzakelijk dat deze gegevens met de gemeente Amsterdam worden gedeeld? Een subsidie met een doelstelling die het *noodzakelijk* maakt dat private sensorgegevens met de gemeente moeten worden gedeeld, lijkt lastig voorstelbaar. Als de gemeente private sensorgegevens nodig heeft, dan ligt inkoop (§3.3.3) meer voor de hand dan subsidiëring.

Voor zover het niet mogelijk is om op grond van artikel 4:37, eerste lid, Awb een subsidieverplichting op te nemen die betrekking heeft op (het delen van) private sensorgegevens die zijn verzameld in de openbare ruimte, zou artikel 4:38 Awb uitkomst kunnen bieden. Op grond van artikel 4:38, eerste lid, Awb kan de subsidieverstrekker ook andere verplichtingen opleggen die strekken tot verwezenlijking van het doel van de subsidie. Het gaat daarbij om verplichtingen die redelijkerwijs noodzakelijk en geschikt zijn om het met de subsidie nagestreefde doel te bereiken. Voor zover de subsidie een wettelijke grondslag heeft,[248] moet ook een wettelijke grondslag bestaan voor het opleggen van doelgerichte subsidieverplichtingen. In de Algemene Subsidieverordening Amsterdam 2013 zijn geen doelgebonden verplichtingen opgenomen die samenhangen met (het delen van) private sensorgegevens die zijn verkregen in de openbare ruimte of in voor het publiek toegankelijke plaatsen. Op grond van artikel 3, tweede lid, onder f, van deze verordening kan het college van burgemeester en wethouders wel nadere regels vaststellen met betrekking tot de verplichtingen die aan de subsidie kunnen worden verbonden. Omdat in artikel 4:38, eerste lid, Awb is neergelegd dat doelgebonden verplichtingen bij of krachtens wettelijk voorschrift worden opgelegd, is het mogelijk dat het college van burgemeester en wethouders in een bijzondere subsidieregeling bepaalt dat doelgebonden verplichtingen kunnen worden opgelegd en dat de doelgebonden verplichting wordt opgenomen in de subsidiebeschikking.[249] Wel dient steeds te zijn voldaan aan de eis dat de verplichting dient ter verwezenlijking van het doel van de subsidieregeling. Of het mogelijk is om als doelgebonden verplichting in een subsidiebeschikking op te nemen dat de subsidieontvanger bij het verzamelen van private sensorgegevens de fundamentele rechten van burgers moet beschermen dan wel dat de verkregen private sensorgegevens moeten worden gedeeld met de gemeente, hangt dus erg af van de doelstelling van de subsidie. Is het voor het bereiken van het doel van de subsidie noodzakelijk dat de fundamentele rechten van burgers inzake private sensorgegevens worden beschermd en/of dat deze gegevens met de gemeente Amsterdam worden gedeeld?

Wanneer het ook niet mogelijk is om op grond van artikel 4:38 Awb doelgebonden verplichtingen op te leggen die betrekking hebben op het verzamelen of delen van private sensorgegevens die zijn

[247] Zie over subsidieverplichtingen uitgebreid W. den Ouden, M.J. Jacobs & J.E. van den Brink, *Subsidierecht (Mastermonografieën staats- en bestuursrecht),* Deventer: Wolters Kluwer 2021, p. 157.

[248] De hoofdregel is dat voor subsidiëring een wettelijke grondslag bestaat (zie art. 4:23, eerste lid, Awb). Dit betekent voor de gemeente concreet dat er een grondslag voor subsidiëring moet bestaan in een gemeentelijke verordening. Doorgaans is dit de algemene subsidieverordening. Er bestaan echter uitzonderingen op de eis van de wettelijke grondslag. Zie art. 4:23, derde lid, Awb.

[249] Zie hierover Den Ouden, Jacobs & Van den Brink 2021, p. 166-167.

verkregen in de openbare ruimte, dan komt artikel 4:39 Awb in beeld. Op grond van artikel 4:39, eerste lid, Awb is het mogelijk om verplichtingen die *niet* strekken tot verwezenlijking van het doel van de subsidie aan de subsidie te verbinden. In de literatuur worden dit oneigenlijke verplichtingen genoemd.[250] De Awb-wetgever heeft het opleggen van oneigenlijke verplichtingen niet willen verbieden, maar wel aan banden willen leggen; het opleggen van oneigenlijke verplichtingen staat immers op gespannen voet met het al genoemde verbod van détournement de pouvoir en het specialiteitsbeginsel. In de eerste plaats kunnen oneigenlijke verplichtingen worden opgelegd voor zover dit bij wettelijk voorschrift is bepaald (artikel 4:39, eerste lid, Awb). In de tweede plaats kunnen oneigenlijke verplichtingen slechts betrekking hebben op de wijze waarop of de middelen waarmee de gesubsidieerde activiteit wordt verricht (artikel 4:39, tweede lid, Awb). Dit betekent dat wanneer de wijze waarop of de middelen waarmee de gesubsidieerde activiteit wordt verricht kan worden gerelateerd aan (het verzamelen van) private sensorgegevens, het mogelijk is om dienaangaande verplichtingen op te leggen, ook als die verplichtingen niet strekken tot verwezenlijking van het doel van de subsidie.

Op grond van de Algemene Subsidieverordening Amsterdam 2013 gelden voor alle subsidieontvangers een aantal oneigenlijke verplichtingen. In dit kader is relevant artikel 11, tweede lid: 'De activiteiten van de subsidieontvanger mogen niet in strijd zijn met de op grond van internationale verdragen algemeen erkende rechten van de mens en het kind'. Wij nemen aan dat met de activiteiten de gesubsidieerde activiteiten worden bedoeld. Dit betekent dat wanneer bij het verrichten van de gesubsidieerde activiteiten private sensorgegevens in de openbare ruimte worden verzameld, niet in strijd mag worden gehandeld met de op grond van internationale verdragen algemeen erkende rechten van de mens en het kind, waaronder de rechten die zien op de bescherming van hun privacy.

Deze bepaling biedt echter geen grondslag voor een verplichting om de private gegevens die in de openbare ruimte zijn verkregen, te delen met de gemeente Amsterdam. Daarvoor zou een afzonderlijke wettelijke grondslag nodig zijn. Het is de vraag of die grondslag hier bestaat. In de Algemene Subsidieverordening Amsterdam 2013 is weliswaar neergelegd dat het college van burgemeester en wethouders nadere regels kan vaststellen met betrekking tot de verplichtingen die aan de subsidie kunnen worden verbonden, maar dit lijkt ons een te magere grondslag om ook de bevoegdheid te behelzen dat regels kunnen worden gesteld inzake oneigenlijke verplichtingen.

Het is wel mogelijk dat de gemeenteraad zelf een bijzondere subsidieverordening vaststelt waarin aanvullende niet-doelgebonden verplichtingen zijn opgenomen.[251] Let wel, los van de vraag of thans een voldoende wettelijke grondslag bestaat voor het opleggen van de oneigenlijke verplichting dat (bepaalde) private sensorgegevens die in de openbare ruimte zijn verkregen, met de gemeente Amsterdam moeten worden gedeeld, moet ook zijn voldaan aan de eis dat deze verplichting betrekking heeft op de wijze waarop of de middelen waarmee de gesubsidieerde activiteit wordt verricht. Uit de schaarse jurisprudentie over artikel 4:39 Awb blijkt dat de bestuursrechter kritisch is ten aanzien van oneigenlijke verplichtingen.[252] Uit de jurisprudentie blijkt namelijk dat het verband tussen de oneigenlijke verplichting en de gesubsidieerde activiteit niet te ver verwijderd mag zijn.[253]

Ten slotte plaatsen wij bij het voorgaande voor de zekerheid nog de kanttekening dat het anders ligt indien de private sensorgegevens ook persoonsgegevens bevatten. In dat geval geldt immers het kader van de AVG (§3.2.2). Wanneer private partijen persoonsgegevens verwerken door middel van sensoren, dan kunnen zij die niet zomaar overdragen aan derden (waaronder de gemeente). Wanneer het overdragen van sensorgegevens op grond van de AVG niet mogelijk is, dan kan dit niet worden omzeild door middel van het opleggen van subsidieverplichtingen.

[250] Zie over oneigenlijke verplichtingen Den Ouden, Jacobs & van den Brink 2021, p. 167 e.v.
[251] Wij nemen aan dat de laatste zin van de toelichting op art. 11 van de Algemene Subsidieverordening Amsterdam 2013 hierop doelt.
[252] Zie hierover uitgebreid Den Ouden, Jacobs & Van den Brink 2021, p. 168 e.v.
[253] Zie ABRvS 4 mei 2016, ECLI:NL:RVS:2016:1177, *AB* 2016/285, m.nt. W. den Ouden.

3.3.3 Privaatrechtelijke instrumenten

Naast de in de vorige paragraaf besproken publiekrechtelijke instrumenten, zou de gemeente Amsterdam ook privaatrechtelijke instrumenten kunnen inzetten om i) de fundamentele rechten te beschermen van personen op wie private sensorgegevens betrekking hebben en ii) toegang te verkrijgen tot (bepaalde) private sensorgegevens die zijn verkregen in de openbare ruimte. Alvorens wij ingaan op een aantal specifieke privaatrechtelijke instrumenten, schetsen wij eerst de algemene juridische kaders die gelden bij privaatrechtelijk overheidshandelen.

De gemeente Amsterdam heeft, net als elke publiekrechtelijke rechtspersoon, in beginsel de vrijheid om te kiezen tussen de publiekrechtelijke of de privaatrechtelijke weg om voormelde doelen te bereiken. Die keuzevrijheid wordt echter beperkt door de zogenoemde tweewegenleer en de bijbehorende doorkruisingsformule uit het Windmill-arrest.[254] In dat arrest heeft de Hoge Raad overwogen dat, wanneer de wet niet voorziet in een antwoord op de vraag of de overheid gebruik mag maken van haar privaatrechtelijke bevoegdheden in plaats van of in aanvulling op haar publiekrechtelijke bevoegdheden, voor de beantwoording van die vraag beslissend is of het gebruik van privaatrechtelijke bevoegdheden de betrokken publiekrechtelijke regeling op onaanvaardbare wijze doorkruist. Daarbij moet onder meer worden gelet op:

- de inhoud en strekking van de publiekrechtelijke regeling (mede in het licht van de wetsgeschiedenis);
- de wijze waarop en de mate waarin in het kader van die publiekrechtelijke regeling de belangen van burgers zijn beschermd; en
- of de overheid door gebruikmaking van de publiekrechtelijke regeling een vergelijkbaar resultaat kan bereiken als met de inzet van de privaatrechtelijke bevoegdheid, omdat dit een belangrijke aanwijzing is dat geen plaats is voor de privaatrechtelijke weg.

De voorvraag is dus altijd of de wet duidelijk is over de toelaatbaarheid van privaatrechtelijk overheidshandelen. Dat is meestal niet zo. Als de wet niet duidelijk is, moet de doorkruisingsformule worden toegepast aan de hand van onder meer de bovenstaande drie ijkpunten. Deze ijkpunten zijn niet limitatief: de rechter betrekt soms ook andere maatstaven bij de beantwoording van de vraag of privaatrechtelijk overheidshandelen is toegestaan, zoals de regel dat de overheid geen misbruik mag maken van een privaatrechtelijke bevoegdheid (artikel 3:13 BW).[255] De ijkpunten zijn ook niet cumulatief: privaatrechtelijk overheidshandelen kan reeds op basis van één ijkpunt worden uitgesloten of juist toegestaan. De formulering dat het privaatrechtelijk overheidshandelen de betrokken publiekrechtelijke regeling niet 'op onaanvaardbare wijze' mag doorkruisen, laat zien dat de rechter niet snel geneigd is om aan te nemen dat de overheid haar privaatrechtelijke bevoegdheden niet mag gebruiken in plaats van of naast haar publiekrechtelijke bevoegdheden.

De meest voor de hand liggende publiekrechtelijke regeling die de gemeente Amsterdam zou kunnen doorkruisen door via de privaatrechtelijke weg voorwaarden te stellen aan de verzameling en/of het gebruik van private sensorgegevens, is de (Uitvoeringswet) Algemene verordening gegevensbescherming (hierna: (U)AVG). De (wetsgeschiedenis van de) (U)AVG geeft zelf geen antwoord op de vraag of de gemeente dergelijke voorwaarden via het privaatrecht mag opleggen. Als het gaat om het doel dat de gemeente met die voorwaarden de fundamentele rechten van personen op wie de private sensorgegevens betrekking hebben, (beter) wil beschermen, dan doorkruist de gemeente vermoedelijk niet de (U)AVG door die

[254] HR 26 januari 1990, ECLI:NL:HR:1990:AC0965 (*Windmill*). Zie hierover uitgebreid P.J. Huisman en F.J. van Ommeren, *Hoofdstukken van privaatrechtelijk overheidshandelen. Publiekrechtelijke en privaatrechtelijke rechtspersonen op de grens van publiek- en privaatrecht*, Deventer: Wolters Kluwer 2019, p. 417 e.v.

[255] HR 5 juni 2009, ECLI:NL:HR:2009:BH7845 (*Amsterdam/Geschiere*). Zie over deze maatstaven uitgebreid Huisman & Van Ommeren 2019, p. 437 e.v.

voorwaarden via het privaatrecht op te leggen. Het beschermen van de fundamentele rechten van personen op wie sensorgegevens betrekking hebben, is immers in lijn met de inhoud en strekking van de (U)AVG en de wijze waarop de (U)AVG de belangen van burgers beschermt. In beginsel kan de gemeente verdergaande bescherming van die fundamentele rechten vereisen dan strikt genomen op grond van het EU-recht, waaronder de AVG, noodzakelijk is, mits daardoor de voorrang, eenheid en werking van het EU-recht c.q. de AVG niet in gevaar komen.[256] Anderzijds heeft de overheid, althans de AP, op grond van de (U)AVG allerlei publiekrechtelijke bevoegdheden om de bescherming van die fundamentele rechten te waarborgen, waaronder het opleggen van een bestuurlijke boete of een last onder dwangsom. Zodoende kan de overheid in het algemeen via het publiekrecht een vergelijkbaar resultaat bereiken als door via het privaatrecht voorwaarden te stellen over de bescherming van fundamentele rechten bij de verzameling van sensorgegevens.

Als het gaat om het doel dat de gemeente met de voorwaarden toegang verkrijgt tot (informatie over) private sensorgegevens, niet zijnde persoonsgegevens in de zin van de (U)AVG, voor de verwezenlijking van publieke doeleinden, dan is er (nog) geen wet die dit mogelijk maakt en die dus zou kunnen worden doorkruist. Mocht een dergelijke wet er komen, bijvoorbeeld in navolging van de concept-Dataverordening (§3.2.9), dan zou die ertoe kunnen leiden dat het de gemeente op grond van de doorkruisingsformule niet langer vrijstaat om via het privaatrecht sensorgegevens te verkrijgen.

Het privaatrechtelijk verkrijgen van sensorgegevens die in strijd met de (U)AVG zijn verwerkt, doorkruist overigens zonder meer de (U)AVG, aangezien dergelijk privaatrechtelijk overheidshandelen evident in strijd zou zijn met de wet (artikel 3:40, eerste lid, BW) en bovendien de fundamentele rechten zou schenden van de personen op wie de sensorgegevens betrekking hebben (artikel 3:14 BW).[257] Zoals gezegd kan de gemeente de normering van fundamentele rechten en algemene beginselen van behoorlijk bestuur immers niet 'ontlopen' door gebruik te maken van haar privaatrechtelijke bevoegdheden.[258]

Al met al is het uitgangspunt voor privaatrechtelijk handelen door de overheid (ja, de gemeente mag privaatrechtelijk handelen, tenzij zij daarmee het publiekrecht onaanvaardbaar doorkruist) fundamenteel anders dan het uitgangspunt voor publiekrechtelijk handelen door de overheid (nee, de gemeente mag niet publiekrechtelijk handelen, tenzij daar een wettelijke grondslag voor bestaat). Dit uitgangspunt voor publiekrechtelijk handelen is immers gestoeld op het legaliteitsbeginsel, dat niet geldt voor privaatrechtelijk overheidshandelen. Vergelijk hierover verder §3.3.2.

In de rest van deze paragraaf bespreken wij drie privaatrechtelijke instrumenten die voor dit rapport in het bijzonder relevant zijn. Het gaat dan om de 'gewone' privaatrechtelijke overeenkomst, de overheidsopdracht en de concessie. In het kader van dit onderzoek zijn twee vragen van belang:

- Kan de gemeente Amsterdam in een privaatrechtelijke overeenkomst, een overheidsopdracht of een concessie voorwaarden opnemen die ertoe strekken dat de fundamentele rechten van personen op wie de private sensorgegevens die de wederpartij verzamelt betrekking hebben, worden beschermd?
- Kan de gemeente Amsterdam in een privaatrechtelijke overeenkomst, een overheidsopdracht of een concessie voorwaarden opnemen die ervoor zorgen dat de wederpartij verplicht is om de gemeente Amsterdam private sensorgegevens die zijn verkregen in de openbare ruimte over te dragen, zodat de gemeente die gegevens kan gebruiken voor publieke doeleinden?

[256] Vergelijk HvJ EU 26 februari 2013, C-399/11, ECLI:EU:C:2013:107 (*Melloni*), r.o. 58-60.
[257] HR 26 april 1996, ECLI:NL:HR:1996:ZC2051 (*Rasti Rostelli*).
[258] Zie art. 3:14 BW en art. 3:1, tweede lid, Awb. Zie ook HR 27 maart 1987, ECLI:NL:HR:1987:AG5565 (*Amsterdam/IKON*), HR 24 april 1992, ECLI:NL:HR:1992:ZC0582 (*Zeeland/Hoondert*) en HR 26 april 1996, ECLI:NL:HR:1996:ZC2051 (*Rasti Rostelli*).

Privaatrechtelijke overeenkomst

Een overeenkomst is een meerzijdige rechtshandeling, aangezien een of meer partijen met een of meer andere partijen een verbintenis aangaan (artikel 6:213 BW). De gemeente Amsterdam is net als een 'gewone' natuurlijke persoon of een privaatrechtelijke rechtspersoon bevoegd tot het sluiten van overeenkomsten (artikel 2:1 en 2:5 BW). In de praktijk zijn de organen (bestuursorganen) van de gemeente dan aan zet. Het college van burgemeester en wethouders is bevoegd te besluiten tot privaatrechtelijke rechtshandelingen van de gemeente, waaronder het sluiten van overeenkomsten (artikel 160 Gemeentewet).[259] De burgemeester is bevoegd om namens de gemeente overeenkomsten te sluiten en kan die bevoegdheid opdragen aan een door hem/haar aan te wijzen persoon (artikel 171 Gemeentewet). Uit de jurisprudentie blijkt dat de vraag of degene die namens een publiekrechtelijke rechtspersoon een overeenkomst sluit daartoe wel bevoegd is, een belangrijk aandachtspunt is dat in de praktijk nog weleens wordt vergeten.[260]

De gemeente heeft in beginsel contractsvrijheid. Contractsvrijheid vloeit voort uit het beginsel van partijautonomie en betekent dat het een partij vrijstaat om wel of niet een overeenkomst aan te gaan, te kiezen voor een contractspartner en de inhoud van het contract naar eigen inzicht te bepalen.[261] De contractsvrijheid van de overheid wordt evenwel beperkt door publiekrechtelijke regels, zoals in bepaalde gevallen de Aanbestedingswet en in alle gevallen de fundamentele rechten en algemene beginselen van behoorlijk bestuur (artikel 3:14 BW).

Op zichzelf zien wij geen beperkingen met betrekking tot het opnemen van voorwaarden die zien op de verzameling en/of het delen van sensorgegevens in een 'gewone' privaatrechtelijke overeenkomst, mits de gemeente – zoals gezegd – daarmee niet het publiekrecht onaanvaardbaar doorkruist en/of in strijd handelt met geschreven of ongeschreven publiekrechtelijke regels, waaronder de fundamentele rechten en algemene beginselen van behoorlijk bestuur. De zojuist beschreven contractsvrijheid komt echter ook de wederpartij van de gemeente toe, die waarschijnlijk niet (zomaar) akkoord zal gaan met voorwaarden die zien op de verzameling en/of het delen van sensorgegevens. Dat akkoord is wel nodig voor een geldige overeenkomst, want die komt tot stand door een aanbod *en de aanvaarding daarvan*, oftewel wilsovereenstemming (artikel 6:217, eerste lid, BW). Anders gezegd: de gemeente kan een private partij met een overeenkomst niet eenzijdig dwingen tot het accepteren van voorwaarden die zien op de verzameling en/of het delen van sensorgegevens. Dat ligt anders als de gemeente bepaalde publiekrechtelijke instrumenten inzet (§3.3.2). Zo kan de gemeente met een vergunningstelsel een private partij die de vergunningplichtige activiteit wil uitvoeren, eenzijdig dwingen tot het accepteren van bepaalde voorwaarden (voorschriften).

Overigens hebben derden, in het bijzonder de personen op wie de sensorgegevens betrekking hebben, géén wilsovereenstemming bij een overeenkomst tussen de gemeente en een private partij die die sensorgegevens verzamelt. Zij zijn immers geen partij bij die overeenkomst. Dit benadrukt het reeds besproken belang van de bescherming van hun fundamentele rechten, bijvoorbeeld door als gemeente alleen niet tot personen herleidbare sensorgegevens te accepteren.

Hoewel de gemeente een private partij met een overeenkomst dus niet eenzijdig kan dwingen tot het accepteren van voorwaarden die zien op de verzameling en/of het delen van sensorgegevens, ligt de verhouding anders c.q. is de positie van de gemeente sterker als zij die voorwaarden verbindt aan het gunnen van een overheidsopdracht of een concessie aan de private partij. De gemeente heeft dan immers een (lucratieve) overheidsopdracht of concessie te bieden. De vraag is vervolgens welke grenzen het aanbestedingsrecht stelt aan het opleggen van voorwaarden aan gegadigden c.q. de ondernemer aan wie de gemeente de overheidsopdracht of de concessie gunt.

---

[259] Daarbij kan het college van burgemeester en wethouders overigens niet de gemeenteraad eenzijdig binden ten aanzien van een bevoegdheid van de gemeenteraad. Vergelijk recent ABRvS 20 januari 2021, ECLI:NL:RVS:2021:113, r.o. 5.3.
[260] Zie hierover uitgebreid Huisman & Van Ommeren 2019, p. 140 e.v.
[261] Asser/Sieburgh *6-III* 2022/41.

Overheidsopdracht

Een overheidsopdracht is een schriftelijke overeenkomst onder bezwarende titel tussen een aanbestedende dienst en een ondernemer, die betrekking heeft op het verlenen van een dienst, het leveren van een product of de uitvoering van een werk (artikel 1.1 Aanbestedingswet). Simpel gezegd koopt de overheid met een overheidsopdracht iets in. Dat kan gaan om bureaustoelen voor in het gemeentehuis, maar ook het ontwerp en de bouw van een heel nieuw gemeentehuis. Naar Nederlands recht is een overheidsopdracht een privaatrechtelijk instrument. Voor overheidsopdrachten geldt de Aanbestedingswet, op grond waarvan aanbestedende diensten verplicht kunnen zijn om een opdracht aan te besteden. De gemeente Amsterdam is een aanbestedende dienst (artikel 1.1 Aanbestedingswet). Over de band van artikel 3:14 BW heeft de gemeente Amsterdam zich ook als aanbestedende dienst aan de fundamentele rechten en algemene beginselen van behoorlijk bestuur te houden.

Welke voorwaarden ten aanzien van de verzameling en/of het gebruik van sensorgegevens kan de gemeente Amsterdam stellen aan deelnemers aan aanbestedingen? Voor alle voorwaarden geldt dat zij proportioneel moeten zijn. Dit betekent dat de gemeente uitsluitend voorwaarden mag stellen die in een redelijke verhouding staan tot het voorwerp van de opdracht.[262] Bovendien is de gemeente op grond van het transparantiebeginsel verplicht de relevante eisen en criteria voorafgaand aan de inschrijving bekend te maken.[263] Tot slot kunnen voorwaarden ten aanzien van de verzameling en/of het gebruik van sensorgegevens mogelijk worden aangemerkt als zogenoemde bijzondere voorwaarden, aangezien deze voorwaarden verband houden met de verwezenlijking van bepaalde publieke doeleinden. Bijzondere voorwaarden moeten bij Europese aanbestedingen verband houden met het voorwerp van de opdracht en worden vermeld in de aankondiging of de aanbestedingsstukken (artikel 2.80 Aanbestedingswet).

Het is lastig om precies te voorspellen welke voorwaarden over de verzameling en/of het gebruik van sensorgegevens door de aanbestedingsrechtelijke beugel kunnen. Veel hangt af van het voorwerp van de opdracht. Als de opdracht bijvoorbeeld draait om ICT-diensten waarmee persoonsgegevens zijn gemoeid, dan ligt het voor de hand om aan de opdrachtnemer eisen op te leggen die zien op de bescherming van de personen op wie de gegevens betrekking hebben.[264] Als de opdracht echter weinig tot niets te maken heeft met het verzamelen van sensorgegevens door de opdrachtnemer, die de sensorgegevens buiten het bestek van de opdracht in de eigen bedrijfsvoering verzamelt, dan staat de Aanbestedingswet niet toe dat de gemeente binnen het bestek van de opdracht over de verzameling van sensorgegevens voorwaarden stelt. Dergelijke voorwaarden zouden over de band van artikel 3:13 BW voorts kunnen leiden tot misbruik van een privaatrechtelijke bevoegdheid, in dit geval de bevoegdheid tot het sluiten van een overeenkomst van opdracht (artikel 7:400 BW).

Nog lastiger is het om via een overheidsopdracht af te dwingen dat de opdrachtnemer de aanbestedende dienst toegang verschaft tot door hem verzamelde sensorgegevens. De gemeente Amsterdam zou de verzameling van sensorgegevens als dienst kunnen inkopen, zodat het logisch is dat zij aan die opdracht de voorwaarde verbindt dat de opdrachtnemer de gemeente toegang verschaft tot de sensorgegevens. Maar ook hier geldt: als de opdracht daarentegen weinig tot niets te maken heeft met het verzamelen van sensorgegevens door de opdrachtnemer, die de sensorgegevens buiten het bestek van de opdracht in de eigen bedrijfsvoering verzamelt, dan staat de Aanbestedingswet niet toe dat de gemeente eist dat de opdrachtnemer die sensorgegevens met de gemeente deelt.

---

[262] Zie art. 1.10 Aanbestedingswet voor Europese aanbestedingen, art. 1.13 Aanbestedingswet voor nationale aanbestedingen en art. 1.16 Aanbestedingswet voor meervoudig onderhandse procedures. Deze artikelen verwijzen naar de Gids Proportionaliteit (GP) als verplicht te volgen richtsnoer. Afwijkingen van de GP moet de aanbestedende dienst kunnen motiveren (*comply or explain*).

[263] Zie voor Europese aanbestedingen art. 1.9 Aanbestedingswet en voor nationale aanbestedingen art. 1.12, tweede lid, Aanbestedingswet.

[264] Vergelijk art. 25 Gemeentelijke inkoopvoorwaarden bij IT (GIBIT) van de gemeente Amsterdam en *Sensoren en de rol van gemeenten. VNG Realisatie Whitepaper*, Den Haag: VNG 2018, p. 16.

Daar komt bij dat sensorgegevens waarde hebben. Het is niet proportioneel om de toegang tot waardevolle sensorgegevens over de band van een overheidsopdracht te vereisen, als de kostprijs voor de uitvoering van die opdracht daar niet op is afgestemd. Dan bestaat er immers geen redelijke verhouding tussen de voorwaarde (toegang tot sensorgegevens) en het voorwerp van de opdracht, die niet gaat over het verzamelen van de sensorgegevens en dus ook qua prijs daar niet op is afgestemd. Dergelijke voorwaarden zouden over de band van artikel 3:13 BW voorts kunnen leiden tot misbruik van een privaatrechtelijke bevoegdheid, in dit geval de bevoegdheid tot het sluiten van een overeenkomst van opdracht (artikel 7:400 BW).

In het uitzonderlijke geval dat voorwaarden over de verzameling of het gebruik van sensorgegevens de proportionaliteitstoets doorstaan en voldoende verband houden met het voorwerp van de opdracht, geniet de gemeente belangrijke voordelen: het is gebruikelijk dat aanbestedende diensten de inschrijvers op een aanbesteding om een onvoorwaardelijke aanvaarding van de conceptovereenkomst vragen.[265] Elk voorbehoud dat de inschrijver daarin maakt, zal leiden tot ongeldigheid van zijn inschrijving.[266] Dit laat onverlet dat potentiële inschrijvers altijd de kans dienen te krijgen om suggesties te doen voor aanpassingen aan de conceptovereenkomst. Het opleggen van een contract zonder enige mogelijkheid voor de inschrijver om daarover suggesties in te dienen, is in beginsel disproportioneel.[267] Los daarvan loopt de gemeente het risico om weinig tot geen (serieuze) inschrijvers op een opdracht aan te trekken, als zij de waarde van de opdracht niet (voldoende) afstemt op de kosten die de opdrachtnemer direct of indirect moet maken om te voldoen aan de eisen over de verzameling of het gebruik van sensorgegevens.

Concessie

Een concessie is een beschikking of een schriftelijke overeenkomst onder bezwarende titel waarbij een handeling wordt toegestaan en tot uitvoering van die handeling wordt verplicht. Een concessie kan dus zowel publiekrechtelijk als privaatrechtelijk van aard zijn. Een privaatrechtelijke concessie wordt ook wel concessieopdracht genoemd. Een concessieopdracht is een schriftelijke overeenkomst onder bezwarende titel die is gesloten tussen een ondernemer en een aanbestedende dienst en die betrekking heeft op het verlenen van diensten of de uitvoering van werken, waarvoor de tegenprestatie bestaat uit het recht de diensten of werken te exploiteren, al dan niet inclusief een betaling (artikel 1.1 Aanbestedingswet). Simpel gezegd gaat het bij concessies meestal om een privaatrechtelijke rechtspersoon die een bepaalde publieke taak verricht, zoals het verzorgen van openbaar vervoer. De concessiehouder is, anders dan een vergunninghouder (§3.3.2), verplicht om de concessie in gebruik te nemen en uit te voeren.[268]

De in artikel 1.9 en 1.10 Aanbestedingswet opgenomen beginselen van transparantie en proportionaliteit zijn in beginsel ook van toepassing op het plaatsen van een concessieopdracht, zodat de bovenstaande analyse over de toelaatbaarheid van voorwaarden over de verzameling of het gebruik van sensorgegevens bij overheidsopdrachten in zoverre van gelijke strekking is bij concessieovereenkomsten.[269]

Wat betreft het openbaar vervoer binnen de gemeente Amsterdam geldt op grond van artikel 63a, eerste lid, Wp een uitzondering op de aanbesteding van de concessie voor openbaar vervoer, anders dan per trein. Daarom exploiteert GVB Exploitatie BV tot op heden een onderhands gegunde concessie voor openbaar vervoer met metro, bus en tram. Voor een dergelijke concessieverlening is vereist dat de

[265] Vergelijk de soepele opstelling van de rechter ten aanzien van de vereiste overdracht van auteursrechten op in het kader van een overheidsopdracht verzamelde sensorgegevens en de openbaarmaking daarvan in Rechtbank Den Haag 27 maart 2019, ECLI:NL:RBDHA:2019:3623, *JAAN* 2019/114, m.nt. J.I. Kohlen en Gerechtshof Den Haag 25 april 2019, ECLI:NL:GHDHA:2019:906, *JAAN* 2019/105, m.nt. J.I. Kohlen.

[266] M.J.J.M. Essers en C.A.M. Lombert, *Aanbestedingsrecht voor overheden. Naar een maatschappelijk verantwoord aanbestedingsbeleid*, Deventer: Vakmedianet 2017, p. 216 e.v.

[267] Voorschrift 3.9 B GP.

[268] F.J. van Ommeren, 'Concessies 2.0: de concessie op de grens van de vergunning, de overheidsopdracht en de subsidie', *NTB* 2020/257, p. 639-648.

[269] De wetgever kan het aanbestedingsrecht van toepassing verklaren op publiekrechtelijke concessies, zoals in art. 61, eerste lid, Wp.

Vervoerregio Amsterdam als concessieverlener over GVB net als over haar eigen diensten zeggenschap uitoefent (quasi-inbesteding). Aangezien de gemeente Amsterdam slechts een van de vijftien gemeenten is die onderdeel uitmaken van de Vervoerregio Amsterdam, kan de gemeente Amsterdam niet op eigen houtje voorwaarden opleggen aan GVB die zien op de verzameling en/of het gebruik van sensorgegevens.[270]

Op grond van artikel 30c Wp kunnen bij of krachtens algemene maatregel van bestuur regels worden gesteld over het beschikbaar stellen van geanonimiseerde en niet tot personen herleidbare gegevens over reizigersstromen, die uit het gebruik van vervoerbewijzen zijn af te leiden. De minister van Infrastructuur en Waterstaat heeft aangegeven van deze mogelijkheid gebruik te willen gaan maken.[271] Dit zou ertoe kunnen leiden dat GVB dit type sensorgegevens moet delen met de Vervoerregio Amsterdam en de gemeente Amsterdam. De gemeente Amsterdam heeft echter zelf geen (directe) invloed op de inzet van deze bevoegdheid, aangezien algemene maatregelen van bestuur als instrument zijn voorbehouden aan de regering. Wel is het mogelijk dat de gemeente er – al dan niet via de VNG en andere netwerkpartners – toe oproept om een algemene maatregel van behoorlijk bestuur op grond van artikel 30c Wp vast te stellen, zoals de minister van Infrastructuur en Waterstaat heeft aangegeven te willen gaan doen, maar tot op heden nog niet heeft gedaan. In de interviews met bedrijfsmedewerkers kwam naar voren dat voor het voldoen aan een dergelijke algemene maatregel van behoorlijk bestuur mogelijk meer capaciteit (geld) nodig is.

Naast GVB exploiteert ook N.V. Nederlandse Spoorwegen (hierna: NS) diensten met betrekking tot het openbaar vervoer in Amsterdam, meer specifiek het openbaar treinvervoer. Daartoe is een landelijke concessie voor het hoofdrailnet onderhands gegund aan NS door de staatssecretaris van Infrastructuur en Milieu.[272] Het enkele feit dat NS met die concessie een publieke dienst verricht, leidt er niet toe dat NS verplicht is sensorgegevens te delen met de gemeente Amsterdam. De voorwaarden uit de concessie zijn wat dat betreft leidend.

In de concessie voor het hoofdrailnet 2015-2025 zijn voorwaarden opgenomen die zien op het verzamelen en delen van (sensor)gegevens door NS.[273] Hetzelfde geldt voor het Programma van Eisen (hierna: PvE) voor de nieuwe concessie voor het hoofdrailnet.[274] De voorwaarden uit het PvE zijn uitgebreider en gedetailleerder dan die uit de huidige concessie. Zo verwijst het PvE expliciet naar een DPIA, Mobility as a Service (MaaS) en een deels open-source Data Management System (DMS).

De voorwaarden uit het PvE geven de Vervoerregio Amsterdam en de gemeente Amsterdam vermoedelijk meer slagkracht bij het verkrijgen van (sensor)gegevens van NS dan zij op basis van de huidige concessie hebben, met dien verstande dat het nog niet om definitieve concessievoorwaarden gaat. Uit de interviews met gemeentemedewerkers is gebleken dat er vanuit de gemeente bezien behoefte is aan die slagkracht. Ook ten aanzien van NS is overigens een regierol weggelegd voor de minister van Infrastructuur en Waterstaat, aangezien deze directe invloed heeft op de (handhaving van) nieuwe concessievoorwaarden, en omdat de gegevensuitwisseling door NS niet alleen voor de gemeente Amsterdam van belang is.[275] De gemeente kan – al dan niet via de VNG en/of in samenwerking met andere netwerkpartners – de minister oproepen om die regierol (meer) te voeren in aanloop naar de nieuwe concessieperiode. Hetzelfde geldt

[270] Art. 3, derde lid, Gemeenschappelijke regeling Vervoerregio Amsterdam.
[271] Kamerbrief van de minister van Infrastructuur en Waterstaat over Wetgevingsopties bij het beschikbaar stellen van OV-reizigersinformatie van 24 maart 2020.
[272] Thans: staatssecretaris van Infrastructuur en Waterstaat. Vergelijk Rechtbank Den Haag 13 december 2022, ECLI:NL:RBDHA:2022:13391.
[273] Zie met name artt. 7, 11, 19, 28 en 57. Let wel: de gemeente Amsterdam is geen decentrale overheid volgens de definitie in art. 1. Gedeputeerde Staten en de Vervoerregio Amsterdam zijn dat wel (zie art. 20 lid 2 en 3 Wp en art. 36b Besluit personenvervoer 2000).
[274] Bijlage bij Kamerbrief van de staatssecretaris van Infrastructuur en Waterstaat over Programma van Eisen voorgenomen concessie hoofdrailnet van 3 oktober 2022. Zie met name artt. 7, 32, 37, 47, 48 en 49 en bijlage 6, tabel 4. Ook hier is de gemeente Amsterdam geen decentrale overheid volgens de definitie in het PvE. Gedeputeerde Staten en de Vervoerregio Amsterdam zijn dat wel (zie art. 20 lid 2 en 3 Wp en art. 36b Besluit personenvervoer 2000).
[275] Vergelijk Decisio, TwynstraGudde en inno-V in opdracht van het ministerie van Infrastructuur en Waterstaat, *Effecten van openbaar aanbesteden in het Openbaar Vervoer. Een overzicht van de ervaringen in de periode 2000-2020*, 18 maart 2020, p. 39 en 69-70.

voor de oproep om ook ten aanzien van NS een algemene maatregel van bestuur op grond van artikel 30c Wp vast te stellen.

3.3.4 Soft law-instrumenten

Het laatste instrument dat wij hier bespreken, zijn de zogenoemde soft law-instrumenten, die zowel publiekrechtelijk als privaatrechtelijk van karakter kunnen zijn. Hierbij kan bijvoorbeeld worden gedacht aan convenanten, intentieverklaringen en maatschappelijke akkoorden.[276] Het betreft geen vastomlijnde of wettelijk gedefinieerde begrippen.[277] Afspraken vastgelegd in dergelijke soft law-instrumenten zijn meestal niet in rechte afdwingbaar en zullen de gemeente Amsterdam daarom geen garanties kunnen bieden met betrekking tot de navolging van voorwaarden die zien op de verzamelen en/of het delen van sensorgegevens door private partijen.[278] Wel kan de inzet van soft law-instrumenten een (positief) effect hebben op de bewustwording bij private partijen en op de algemene publieke opinie in het voordeel van de betrokken private partijen. Zo bezien kan de inzet van soft law-instrumenten private partijen stimuleren om de fundamentele rechten van personen op wie hun sensorgegevens betrekking hebben, beter te beschermen.[279]

> Een voorbeeld biedt het in 2019 tussen de gemeente Amsterdam en Uber gesloten 'Social Charter'. Daarin zijn onder meer afspraken opgenomen over het proactief delen van in overeenstemming met de APV geaggregeerde sensorgegevens met de gemeente Amsterdam (onder 6).

[276] P.J. Huisman, 'Maatschappelijke akkoorden en de Aanwijzingen voor convenanten: tijd voor een update!', *RegelMaat* 2021, nr. 3, p. 210-229.
[277] In de Aanwijzingen voor convenanten (*Stcrt.* 2003, 18) staat weliswaar een definitie van een convenant, maar deze Aanwijzingen zien alleen op afspraken die de centrale overheid maakt en zijn niet juridisch afdwingbaar.
[278] Als deze afspraken wel in rechte afdwingbaar zijn, is waarschijnlijk materieel sprake van een overeenkomst. Vergelijk HR 13 maart 1981, ECLI:NL:HR:1981:AG4158 (*Haviltex*).
[279] Zoals ook naar voren gebracht door meerdere geïnterviewde gemeentemedewerkers. Vergelijk H.E. Bröring & K.J. de Graaf (red.), *Bestuursrecht 1. Systeem, bevoegdheid, bevoegdheidsuitoefening, handhaving*, Den Haag: Boom juridisch 2022, p. 584; Astrid Voorwinden & Sofia Ranchordás, 'Soft Law in City Regulation and Governance', in: U. Morth, E. Korhea-aho en M. Eliantonio (red.), *Research Handbook on Soft Law*, Edward Elgar Publishing 2022 (digitaal beschikbaar via https://doi.org/10.2139/ssrn.3978959) en Jorgen Schram, Henk den Uijl en Mark van Twist, *Actuele kwestie, klassieke afweging. Een verkenning naar de governance van het Nederlandse digitaliseringsbeleid*, Den Haag: NSOB 2021, p. 36-37.

4 Bevindingen en aanbevelingen

De centrale vraag in dit onderzoeksrapport luidde wat voor de gemeente Amsterdam de juridische mogelijkheden zijn om ten aanzien van de verzameling en het gebruik van gegevens die door private partijen met behulp van sensoren in de openbare ruimte worden verzameld, binnen het bestuurlijke instrumentarium aanvullende voorwaarden te stellen. Deze vraag valt uiteen in twee deelvragen, te weten: biedt het huidige juridisch kader mogelijkheden voor de gemeente om meer bescherming te bieden aan de fundamentele rechten van personen op wie de private sensorgegevens betrekking hebben? En: kan het juridisch kader de gemeente helpen om ten behoeve van de uitvoering van haar publieke taken – en in het verlengde daarvan, het belang van andere in de stad opererende organisaties – toegang te verkrijgen tot private sensorgegevens die zijn verkregen in de openbare ruimte? Hiertoe hebben we in hoofdstuk 3 het relevante juridisch kader dat nodig is om deze deelvragen te beantwoorden weergegeven en per deelvraag geanalyseerd. In dit hoofdstuk vatten we per deelvraag de gevonden knelpunten en kansen uit hoofdstuk 3 samen en geven we per deelvraag enkele aanbevelingen die de gemeente in overweging zou kunnen nemen bij verdere beleidsvorming op deze twee deelvragen.

4.1 Betere bescherming van de fundamentele rechten

4.1.1 Knelpunten

Wanneer een private partij gegevens verwerkt en die gegevensverwerking raakt aan fundamentele rechten, waaronder het recht op privacy, dan is die gegevensverwerking in beginsel toegestaan, tenzij de formele wet daar beperkingen aan stelt. De verwerking van persoonsgegevens door private partijen wordt bijvoorbeeld gereguleerd door de AVG en de Telecommunicatiewet. In specifiek omschreven gevallen kan het Wetboek van Strafrecht van toepassing zijn. Uit de verdere analyse van de wetgeving komt naar voren dat de gemeente in beginsel geen rol toekomt bij het normeren van gegevensverwerkingen door private partijen; die taak is primair belegd bij de formele wetgever. Gemeentelijke inzet van publiekrechtelijke instrumenten (verordening, vergunning, subsidie) moet terug te voeren zijn op een wettelijke grondslag. Wat betreft de handhaving van de AVG is primair een rol weggelegd voor de AP, al kan de gemeente meldingen doen over de omgang van persoonsgegevens bij de AP.

In de analyse constateerden we verder dat de gemeentelijke Verordening meldingsplicht sensoren tot doel heeft meer zichtbaarheid te bieden in het aantal sensoren dat in de stad aanwezig is, inclusief sensoren van private partijen. De meldingsplicht is niet vrijblijvend. Private partijen zijn verplicht kenbaar te maken welke gegevens (kunnen) worden ingewonnen. Daarnaast zijn zij, indien daarbij persoonsgegevens worden verwerkt, verplicht aan te geven op basis van welke wettelijke grondslag uit de AVG de persoonsgegevens worden verwerkt. Daarbij moeten zij een link naar hun privacy-beleid opnemen. Deze informatie komt in een openbaar register te staan, zodat gebruikers van openbare ruimten kunnen nagaan welke gegevens daar over hen worden ingewonnen.

Met de Verordening meldingsplicht sensoren kan de gemeente op indirecte wijze bescherming van de fundamentele rechten aan burgers bieden. Een cruciale voorwaarde hierbij is dat de genoemde Verordening door alle partijen met sensoren in de openbare ruime wordt nageleefd en dat sensoren worden gemeld zoals voorgeschreven in het meldingsformulier van de gemeente; dat de Verordening wordt gehandhaafd wanneer het aan de naleving schort (bijvoorbeeld als blijkt dat partijen hun sensor niet of gebrekkig aanmelden); en dat het register wordt onderhouden (bijvoorbeeld doordat wijzigingen in het gebruik van een sensor die gevolgen hebben voor hetgeen zij waarnemen, de duur van de waarneming, etc., tijdig worden doorgegeven aan de registerhouder). Handhaving kan lastig zijn, omdat niet elke private sensor direct zichtbaar is voor gemeentelijke handhavers.

Het sensorenregister geeft, indien het accuraat is, burgers de mogelijkheid kennis te nemen van de identiteit van private partijen die mogelijk hun persoonsgegevens verwerken. Zij kunnen op basis van die informatie bijvoorbeeld besluiten hun AVG-betrokkenenrechten jegens de verwerkings-verantwoordelijke uit te oefenen.[280] Zij kunnen eventuele klachten over niet-naleving van die rechten melden bij de AP.

Met de invoering van de betrokkenenrechten in het EU-Handvest en in de AVG is een belangrijk instrument voor de rechtsbescherming van betrokkenen gecreëerd.[281] De EU-wetgever had de bedoeling de uitoefening van deze rechten eenvoudig en toegankelijk te maken voor betrokkenen. In de praktijk blijkt echter dat betrokkenenverzoeken zelden leiden tot betekenisvolle informatie voor betrokkenen of tot (betere) naleving van de AVG door de verwerkingsverantwoordelijke in kwestie. Dit heeft te maken met problematische naleving door verwerkingsverantwoordelijken[282] en vaak ook met de afwezigheid van expertise, kennis, tijd en middelen bij betrokkenen. Het indienen en effectueren van een betrokkenenverzoek kan maanden duren en veel correspondentie in vaktaal en (andere) bureaucratische obstakels met de verwerkingsverantwoordelijke met zich meebrengen.[283] De effectieve uitoefening van betrokkenenrechten blijkt in de praktijk aldus weerbarstig, al kan de WAMCA hier mogelijk betere perspectieven bieden.

4.1.2 Aanbevelingen

Maak de link naar het meldingsformulier goed vindbaar

De gemeente Amsterdam is na een 'wenperiode' voornemens de Verordening meldingsplicht sensoren te gaan handhaven. Het meldformulier is nu echter nog niet goed vindbaar. Het verdient aanbeveling om het te hechten aan het portaal waar het register kan worden ingezien en op andere plaatsen die door de betrokken partijen regelmatig worden bezocht. Van belang is dat de betrokken partijen die straks verplicht worden te melden, snel terecht kunnen bij het meldingsformulier en bij andere relevante informatie.

Overweeg het ondersteunen van collectieve uitoefening van betrokkenenrechten

Zoals gezegd blijkt de effectieve uitoefening van betrokkenenrechten in de praktijk weerbarstig. Niettemin doemen nieuwe perspectieven op die een meer kansrijke uitoefening en daarmee mogelijk een betere naleving van deze rechten (en in het verlengde daarvan de AVG) kunnen bewerkstellingen. Het sensorenregister kan daarbij meer indirect van betekenis zijn.

De waarde en effectiviteit van betrokkenenrechten kunnen met name tot uitdrukking komen wanneer die rechten gezamenlijk worden uitgeoefend.[284] Wanneer betrokkenenrechten collectief en dus op schaal worden uitgeoefend, is de kans groter dat ze kwestieuze praktijken en niet-naleving van de AVG en andere fundamentele rechten onthullen. Zo hebben recentelijk enkele NGO's en ad hoc burgerrechtbewegingen de uitoefening van betrokkenenrechten, waaronder het inzagerecht, in collectief verband gecoördineerd. Campagnevoerders in Duitsland hebben bijvoorbeeld strategisch en in collectief verband gebruikgemaakt van betrokkenenrechten om discriminerende algoritmes bij de berekening van

[280] Respectievelijk artt. 15 en 17 AVG.
[281] Respectievelijk art. 8 lid 2 EU-Handvest; art. 12 – 22 AVG. Zie ook G. Gonzáles Fuster, *The emergence of Personal Data Protection as a Fundamental Right of the EU* (Law, Governance and Technology Series, Springer 2014), p. 194; O. Lynskey, *The foundations of EU Data Protection Law* (Oxford Studies in European Law, OUP 2016), 11.
[282] J. Ausloos & P. Dewitte, 'Shattering One-way mirrors – data subject rights in practice' (2018) *International Data Privacy Law* (8) 4; Privacy International, '*Our complaints against Axciom, Criteo, Equifax, Experian, Oracle, Quantcast, Tapad*', Rapport 8 november 2018, https://privacyinternational.org/advocacy/2426/our-complaints-against-acxiom-criteo-equifax-experian-oracle-quantcast-tapad, bezocht op 29 augustus 2022.
[283] R. Mahieu, H. Ashgari en M. van Eeten, 'Collectively exercising the right of access: individual effort, societal effect' (2018) *Internet Policy Review* 1
[284] Mahieu e.a., 'Collectively exercising the right of access: individual effort, societal effect' (2018) *Internet Policy Review* 1.

kredietscores aan het licht te brengen.[285] Een andere NGO kreeg met een vergelijkbare methode zicht op de niet-naleving van werknemersrechten.[286] Op basis van de antwoorden van de verwerkingsverantwoordelijke in reactie op de betrokkenenverzoeken, kon de coördinerende NGO inzicht verkrijgen in de werkwijze van de betreffende verweringsverantwoordelijke. Zonder coördinatie van de betrokkenverzoeken door een NGO waren deze praktijken waarschijnlijk onder de radar gebleven, omdat deze in *individuele* betrokkenenverzoeken nauwelijks of niet te detecteren zijn. Daarnaast vereisen analyses van een groot aantal inzageverzoeken specialistische kennis, die bij gespecialiseerde organisaties voorhanden is.

Coördinatie van collectieve betrokkenenverzoeken door het maatschappelijk middenveld kan aldus effectief zijn bij het detecteren van niet-naleving van de AVG. Betrokkenenrechten zijn in hun doelstelling immers niet gebonden aan een AVG-doelstelling.[287] In het verlengde hiervan zou de gemeente kunnen overwegen organisaties te steunen (subsidiëren) die zich willen toeleggen op het collectief uitoefenen van betrokkenenrechten.

Laat onderzoeken hoe naleving en handhaving van sensorenregisters kan worden verbeterd

Het succes van het sensorenregister als instrument om de naleving van de AVG en daarmee ook het bredere mensenrechtelijk kader te borgen, hangt mede af van de mate waarin het register wordt nageleefd en gehandhaafd. Omdat sensoren niet altijd zichtbaar zijn en omdat het aan partijen zelf is een sensor te melden, zal de gemeente moeten nadenken over effectieve handhaving. Op dit moment kan de gemeente Amsterdam de verplichtingen die voortvloeien uit de Verordening meldingsplicht sensoren bestuursrechtelijk handhaven door middel van het opleggen van een last onder bestuursdwang of onder dwangsom. Naast Amsterdam zijn meer gemeenten bezig met het opzetten van een sensorenregister. Aandacht voor de naleving en handhaving op nationaal niveau kan helpen bij de bewustwording van 'meldingsplichtige' partijen.[288] Dit kan met name van bang zijn voor partijen die mobiele sensoren exploiteren die in openbare ruimten van verschillende gemeenten operationeel zijn. Mogelijk kan daarbij worden meegenomen onder welke voorwaarden niet-naleving strafbaar zou moeten worden, indien en voor zover strafbaarstelling wenselijk wordt geacht.

De gemeente Amsterdam kan samen met andere gemeenten, die waarschijnlijk met vergelijkbare vragen en onzekerheden rondom de naleving en handhaving zullen moeten omgaan, door wetenschappers en/of de regering en haar adviesorganen laten onderzoeken of beleid en/of wetgeving ten behoeve van de naleving en handhaving op landelijk niveau zou kunnen bijdragen aan de verbetering van de naleving.

---

[285] 'OpenSCHUFA – Shedding Light on Germany's Opaque Credit Scoring', *AlgorithmWatch* 22 mei 2017, https://algorithmwatch.org/en/openschufa-shedding-light-on-germanys-opaque-credit-scoring-2, bezocht op 17 augustus 2022; R. Mahieu & J. Ausloos, 'Recognising and Enabling the Collective Dimension of the GDPR and the Right of Access' *ArXiv*, 2 July 2020, https://osf.io/preprints/lawarxiv/b5dwm/, bezocht op 28 augustus 2022; L Kelion, 'Amazon's Ring logs every doorbell press and app action', *BBC News* 4 maart 2020 https://www.bbc.com/news/technology-51709247; L. Kelion, 'Amazon: Why Amazon knows so much about you', *BBC News*, blog 2020, https://bbc.co.uk/news/extra/CLQYZENMBI/amazon-data, bezocht op 28 augustus 2022.

[286] Zo kon een NGO (onder meer Workers Info Exchange) op basis van informatie uit inzageverzoeken die waren gedaan door een grote groep taxichauffeurs een analyse opmaken over de wijze waarop hun werkgever (Ola en Uber) gebruik maakte van hun persoonsgegevens en algoritmische besluitvorming; zie J. Toh, 'Empowering Workers Through Digital Rights', *Digital Freedom Fund*, 30 April 2021, https://digitalfreedomfund.org/empowering-workers-through-digital-rights/ bezocht 18 maart 2022; zie ook Rb AMS 11 maart 2021, ECLI:NL:RBAMS:2021:1020.

[287] Rb AMS 11 maart 2021, ECLI:NL:RBAMS:2021:1020; J. Ausloos, R. Mahieu & M. Veale, 'Getting Data Subject Rights Right. A Submission to the European Data Protection Board from International Data Rights Academics, to Inform Regulatory Guidance (2020) 10 *Journal of International Property, Information Technology and Electronic Commerce Law* (JIPITEC).

[288] Zie bijvoorbeeld Interprovinciaal Overleg (IPO), 'Gezamenlijke oproep ontwikkeling landelijk sensorenregister', 20 juni 2022, https://www.ipo.nl/lobby/gezamenlijke-oproep-ontwikkeling-landelijk-sensorenregister/; VNG, 'Gemeenten starten meteen algoritme- en sensorenregister', 15 juni 2022, https://vng.nl/nieuws/gemeenten-starten-met-een-algoritme-en-sensorenregister en Sensorenregister NL, een initiatief van het Kadaster (2020) waarbij meer gemeenten zich hebben aangesloten, en dat een nationaal gestandaardiseerd sensorenregister nastreeft (zie https://www.digitaleoverheid.nl/innovatieproject/sensorenregister-nl/) alle bezocht op 28 november 2022.

Zoek binnen het bestaande wettelijk kader ruimte om te experimenteren

De inzet van vrijwel alle bestuurlijke instrumenten vereist ten eerste proportionaliteit van de eisen met betrekking tot de naleving van fundamentele rechten, indien de gemeente dergelijke eisen wil opnemen als voorwaarde voor bijvoorbeeld het verkrijgen van een vergunning. Daarnaast vereist de inzet van die instrumenten een duidelijk en nauw verband tussen die eisen en het achterliggende doel van de inzet van het instrument (connexiteit). Daarbij geldt in het algemeen dat de drempels voor het opleggen van eisen met betrekking tot de naleving van fundamentele rechten, lager zijn dan voor het opleggen van eisen met betrekking tot B2G-gegevensdeling.

De gemeente dient, gelet op de vereiste proportionaliteit, connexiteit en de noodzaak van een specifieke wettelijke grondslag, het opleggen van eisen met betrekking tot het naleven van de fundamentele rechten op weloverwogen wijze te doen. Zij zou daarbij echter niet bang moeten zijn om te experimenteren. Hier kan 'regulatory sandboxing' wellicht mogelijkheden bieden om te verkennen welke ruimte de gemeente heeft. Of en welke experimenteerruimte bestaat is niet op voorhand te zeggen, aangezien die ruimte afhangt van de specifieke context van de regelgeving.

4.2 B2G-gegevensdeling en gegevensdeling met derden

4.2.1 Knelpunten

Uit de analyse van het fundamenteelrechtelijke kader komt naar voren dat B2G-gegevensdeling en verwerkingen van die gegevens alleen kunnen plaatsvinden als daarvoor een specifieke wettelijke grondslag bestaat, wanneer de betrokken gegevens raken aan fundamentele rechten van burgers en private partijen en/of wanneer het om persoonsgegevens gaat. Ook de analyse van de Awb en de algemene beginselen van behoorlijk bestuur[289] in §3.3 laat zien dat de gemeente weinig ruimte toekomt om B2G-gegevensdeling met behulp van een in een verordening of vergunning neergelegde verplichting te effectueren, indien de eerdergenoemde wettelijke grondslag afwezig is. Ook het subsidie-instrument lijkt de gemeente niet veel ruimte te bieden voor B2G-gegevensdeling zonder wettelijke grondslag.

Wanneer persoonsgegevens bij een B2G-gegevensdeling in het geding zijn, moet de gemeente (en ook de private partij) voldoen aan alle verplichtingen die de AVG aan verwerkingsverantwoordelijken oplegt, waarbij tevens in het oog springt dat wanneer de gemeente een private partij een opdracht geeft een gegevensbestand te maken waarin zich geen persoonsgegevens (meer) bevinden, maar waarvoor wel persoonsgegevens werden gebruikt, de gemeente optreedt als verwerkingsverantwoordelijke voor het betreffende bestand. In situaties waarin private partijen vrijwillig gegevensbestanden zonder persoonsgegevens (of andere gegevens waarop rechten rusten) deelt met de gemeente, moet zorgvuldig worden nagegaan wat de rol van de gemeente ten aanzien van het betreffende gegevensbestand is, al ligt gemeentelijke gegevensverantwoordelijkheid hier minder snel voor de hand. Wanneer de gemeente het verkregen, geanonimiseerde gegevensbestand na ontvangst koppelt aan andere gegevensbestanden, rust op haar de zorgvuldigheidsplicht om na te gaan of zich niet alsnog tot personen herleidbare gegevens in het met haar gedeelde bestand bevinden.[290]

Gemeenten lijken soms de overtuiging te hebben dat gegevens verzameld in de openbare ruimte het karakter van een publiek goed hebben en daarmee "van ons allemaal" zijn, mits het geen persoonsgegevens zijn. Vanuit die optiek kan meer algemeen de wens bestaan om zoveel mogelijk gegevens open te (laten) stellen met het oog op innovatie binnen de gemeentegrenzen. De gemeente dient bij het delen van private sensorgegevens echter rekening te houden met de legitieme rechten en belangen van de betrokken private partijen, waaronder intellectuele eigendomsrechten en de bescherming van

[289] Meer specifiek het legaliteitsbeginsel, het specialiteitsbeginsel en het verbod van détournement de pouvoir.
[290] Art. 3.2 en 3.4 lid 2 Awb.

handelsgeheimen, en met het feit dat er geen wet- en regelgeving is die een dergelijk 'publiek eigenaarschap' van gegevens erkent.

De Databankenwet (en het auteursrecht), de Wet bescherming bedrijfsgeheimen, de onlangs in werking getreden Wet open overheid, de Richtlijn open data en de Wet hergebruik van overheidsinformatie (waarin de Richtlijn open data momenteel wordt geïmplementeerd) stellen meer specifieke eisen aan B2G-gegevensdeling en meer specifiek het verder delen van de verkregen gegevens door de gemeente. Uit de analyse komt naar voren dat het verder delen in beginsel mogelijk is, maar dat de gemeente telkens na dient te gaan of de bescherming van bedrijfsgeheimen en intellectuele eigendomsrechten en/of de bescherming van persoonsgegevens die door de gegevensverwerking kunnen worden geraakt, op passende wijze worden geborgd.

De Datagovernanceverordening is relevant voor zover de gemeente overweegt de via B2G-gegevensdeling verkregen gegevens verder te delen, maar voegt geen nieuwe eisen toe aan de eisen omtrent het delen van gegevens uit de Richtlijn open data. De concept-Dataverordening staat een verplichting voor B2G-gegevensdeling toe in drie situaties, die uitwerking geven aan de uitzonderlijke noodzaak tot gegevensdeling. De derde situatie – de vaststelling van wetgeving om gegevens beschikbaar te stellen voor B2G-gegevensdeling – biedt indirect aanknopingspunten voor de gemeente: de formele wetgever zal hiertoe bestaande wetgeving moeten uitwerken of initiatieven voor nieuwe wetgeving moeten nemen. De concept-Dataverordening legt voor B2G-gegevensdeling in de huidige versie geen algemeen materieel normenkader vast. Dat betekent dat voor het materiële normenkader vooralsnog de huidige wetgeving zoals die in §3 is geschetst, als uitgangspunt moet worden genomen en dat mogelijke rechtsonzekerheid over de precieze toepassing van het wettelijk kader met de komende Dataverordening (nog) niet wordt weggenomen.

Afrondend is B2G-gegevensdeling een relatief nieuw fenomeen waarvoor nog geen coherent en materieel omvattend wettelijk kader bestaat. De concept-Dataverordening lijkt een dergelijk kader ook (nog) niet te bieden. De gemeente is nu aangewezen op de toepassing van een mozaïek van (sectorale) wetten, waarbij het nu eerder toeval lijkt of B2G-gegevensdeling wettelijk is geregeld of niet. Om deze redenen is het voor de gemeente belangrijk meer duidelijkheid en inzicht te verkrijgen in situaties waarin B2G-gegevensdeling is toegestaan en onder welke voorwaarden B2G-gegevensdeling kan plaatsvinden. Om de gemeentelijke slagkracht bij verplichte B2G-gegevensdeling te vergroten is ingrijpen door de Nederlandse en/of Europese wetgever noodzakelijk.

4.2.2 Aanbevelingen

Onderzoek of en waar nieuwe wettelijke grondslagen nodig zijn

Zonder specifieke wettelijke grondslag bieden de besproken (concept-)wetgeving en bestuurlijke instrumenten de gemeente op dit moment een beperkt handelingsperspectief bij B2G-gegevensdeling. Vrijwillige B2G-gegevensdeling in het kader van publiek-private samenwerking of op basis van contracten is binnen het geschetste wettelijk kader eveneens beperkt mogelijk. Om het perspectief voor B2G-gegevensdeling te verbreden naar diverse sectoren is ingrijpen door de formele Nederlandse en/of EU-wetgever dus noodzakelijk, al dan niet gesteund door een regierol van de betrokken minister(s).

De gemeente kan onderzoek (laten) verrichten naar welke wetgeving op dit moment al mogelijkheden biedt voor B2G-gegevensdeling. We gaven al aan dat artikel 30c Wp een opening biedt voor een verplichte medewerking door private partijen aan een specifiek type B2G-gegevensdeling. De gemeente zou bij de minister van Infrastructuur en Waterstaat kunnen aandringen op uitvoering van deze in de wet neergelegde mogelijkheid. Daarnaast zou de gemeente kunnen laten onderzoeken of dergelijke openingen in andere wettelijke bepalingen voorhanden zijn of kunnen laten onderzoeken bij welke wettelijke bepalingen een dergelijke opening noodzakelijk zou zijn. Tegelijkertijd zou de wetgever ook moeten voorkomen dat een gefragmenteerd beeld ontstaat van situaties waarin B2G-gegevensdeling wel of niet is toegestaan en hierop beleid moeten ontwikkelen, zodat wetgeving op dit punt wat meer voorspelbaar wordt

(zie ook hierna de volgende aanbeveling, waarin wordt aanbevolen aan te dringen op coherente EU-wetgeving rondom B2G-gegevensdeling).

Wanneer bestaande wetgeving geen eenduidig antwoord geeft op de vraag of B2G-gegevensdeling in een bepaald geval toelaatbaar is, kan de gemeente overwegen over te gaan tot 'regulatory sandboxing', waarbij zij een gecontroleerde testomgeving creëert om te onderzoeken of een bepaalde wet voor een specifieke B2G-gegevensdeling openingen met voldoende waarborgen biedt (of zou moeten bieden). Een dergelijke experimenteeromgeving vereist een zorgvuldige en doordachte voorbereiding en opzet, gelet op het belang van onder meer de betrouwbaarheid van het experiment en op de (borging van de) van de betrokken belangen van de gemeente, bedrijven en burgers.[291]

Dring aan op verduidelijking van het wetgevend kader voor B2G-gegevensdeling in de Dataverordening

Meer rechtszekerheid rondom B2G-gegevensdeling is, gelet op de groeiende belangstelling in B2G-gegevensdeling en de rechten, de belangen en de machtsverhoudingen die met B2G-gegevensdeling (en verdere deling) gemoeid kunnen zijn, urgent en noodzakelijk. De concept-Dataverordening pakt deze handschoen echter (nog) niet op. Daarmee laat de EU-wetgever een belangrijke kans liggen, namelijk de gelegenheid voorwaarden te creëren voor een wetsconforme, maatschappelijk aanvaardbare en succesvolle B2G-gegevensdeling en om de machtsverschillen aan te pakken tussen de publieke sector en (grote) bedrijven, die aan B2G-gegevensdeling ten behoeve van een betere vervulling van de publieke taak in de weg staan. Hoewel de concept-Dataverordening B2G-modellen (zoals de aankoop van gegevens, vrijwillige B2G-gegevensdeling en publiek-private samenwerkingsovereenkomsten) en nationale wetgeving die B2G-gegevensdeling reguleert niet verbiedt, bevat de concept-Dataverordening geen regelgeving of beginselen om transacties rondom B2G-gegevensdeling billijker te maken voor de publieke sector. In plaats daarvan laat de concept-Dataverordening rechtsonzekerheid rondom belangrijke concepten voortbestaan, zoals bij de definitie van de 'taak van algemeen belang', waardoor verdere ontwikkeling van B2G-gegevensdeling ten behoeve van taken van algemeen belang mogelijk wordt belemmerd.[292] Ook kan afwezigheid van materiële normen en beginselen misbruik in de hand werken (zoals het vragen van hoge prijzen voor B2G-gegevensdeling in een monopolistische markt), omdat er geen beperkingen lijken te bestaan.

De gemeente Amsterdam zou in samenwerking met andere gemeenten kunnen overwegen bij de namens Nederland onderhandelende departementen en bij het Europees Parlement te wijzen op de noodzaak van wettelijke regulering, die met een meer uitgewerkt juridisch en materieel-normatief kader meer rechtszekerheid kan bieden bij B2G-gegevensdeling, zodat rechtsonzekerheid over B2G-gegevensdeling bij gemeenten en anderen (private partijen, burgers, betrokkenen) zoveel mogelijk kan worden weggenomen. Ook kan de gemeente onderzoeken of zij samen met gelijkgestemde gemeenten in de EU kan optrekken richting het Europees Parlement. Nederlandse gemeenten moeten zich er overigens van bewust zijn dat uit de publieksconsultatie van de concept-Dataverordening naar voren is gekomen dat de industrie geen voorstander is van bindende regels rond het delen van B2G-gegevens, en dat het Nederlandse standpunt over B2G-gegevensdeling tot nu toe terughoudend is.

Zoek binnen het bestaande wettelijk kader ruimte om te experimenteren

De inzet van vrijwel alle bestuurlijke instrumenten vereist zoals gezegd proportionaliteit van de eisen met betrekking tot het verzamelen en/of delen van private sensorgegevens, alsmede een duidelijk en nauw verband tussen die eisen en het achterliggende doel van de inzet van het instrument (connexiteit). Bij de

[291] Zie over de mogelijkheden en valkuilen bij 'regulatory sandboxes' onder meer S. Ranchordás, *Sunset Clauses and Experimental Legislation: Blessing of Curse for Innovation?* (diss. Tilburg), Zutphen: Koninklijke Wöhrmann 2014; M. Finck, Blockchains: regulating the unknown (2018) *German Law Journal* 19(4) p. 677, M.A. Heldeweg, Experimental legislation concerning technological & governance innovation – an analytical approach' (2015) *The Theory and Practice of Legislation* 3(2) en M.J. Jacobs, *Experimentele wetgeving* (Oratie VU). Wolters Kluwer: 2018.
[292] Art. 14 lid 1 concept-Dataverordening.

inzet van publiekrechtelijke instrumenten is een specifieke wettelijke grondslag noodzakelijk. De gemeente dient, gelet op de vereiste proportionaliteit, connexiteit en de noodzaak van een specifieke wettelijke grondslag, het opleggen van eventuele eisen met betrekking tot het verzamelen en/of delen van private sensorgegevens op weloverwogen wijze te doen, maar daarbij zou zij niet bang moeten zijn om te experimenteren. Ook hier kan 'regulatory sandboxing' wellicht mogelijkheden bieden. De interviews met bedrijfsmedewerkers wijzen immers uit dat niet alleen bilateraal, maar ook unilateraal ingrijpen tot positieve ervaringen voor zowel de gemeente als private partijen kan leiden. Uit de interviews met gemeentemedewerkers en bedrijfsmedewerkers komt met andere woorden geen duidelijke voorkeur naar voren voor unilaterale of bilaterale bestuurlijke instrumenten. Die voorkeur is immers contextafhankelijk. Zo zijn geïnterviewde bedrijfsmedewerkers die te maken hebben gekregen met een vergunningstelsel (een unilateraal instrument), daar over het algemeen positief over. Deze route lijkt met name aangewezen bij 'nieuwe' marktpartijen, die een dienst aanbieden die mede afhankelijk is van een goede inrichting van de openbare ruimte. Anderzijds zijn ook bedrijfsmedewerkers die betrokken zijn bij individuele overeenkomsten met de gemeente over het verzamelen en/of delen van sensorgegevens (een bilateraal instrument), daar gematigd positief over. Deze route zet de gemeente met name in bij private partijen die een publieke dienst aanbieden, waaronder vervoerders, en bij gevestigde private partijen waarvan de bedrijfsvoering voor een belangrijk deel is gestoeld op de verzameling van sensorgegevens, maar niet per se op een goede inrichting van de openbare ruimte. Let wel: uit dit onderzoek kan geen causaal verband worden afgeleid. Dat wil zeggen dat vooralsnog niet kan worden geconcludeerd dat marktpartijen zich welwillend opstellen jegens de gemeente als het om het delen van sensorgegevens gaat, omdat de gemeente unilateraal of juist bilateraal heeft gehandeld om die sensorgegevens te verkrijgen of omdat het gaat om een nieuwe of juist meer gevestigde marktpartij en het type dienstverlening dat zij aanbiedt.

Gebruik naast de DPIA het IAMA voor het inschatten van risico's bij B2G-gegevensdeling

Voor de beoordeling of zich risico's voor persoonsgegevens voordoen bij een specifieke B2G-gegevensdeling, zal de gemeente in veel gevallen een DPIA moeten verrichten. Zij zou ook kunnen overwegen naast de DPIA het IAMA te gebruiken. Het IAMA sluit in opzet aan bij de DPIA en onderzoekt niet alleen risico's voor de verwerking van persoonsgegevens en privacy, maar biedt ook zicht op risico's voor andere grondrechten als gevolg van B2G-gegevensdeling. Het IAMA beoogt overheden in staat te stellen in het ontwerp- en ontwikkelstadium van een voornemen tot B2G-gegevensdeling na te gaan of deze gegevens conform het fundamenteel-rechtelijk kader kunnen worden verwerkt. Het IAMA biedt een praktisch kader: het legt uit hoe de gemeente kan nagaan of het gebruik van de techniek noodzakelijk, evenredig en subsidiair is en geeft voorbeelden van maatregelen om restrisico's te mitigeren.

5 Achtergrond bij de interviews

Voor dit onderzoek werden in totaal 14 semigestructureerde interviews afgenomen, waarvan 8 interviews met medewerkers van de gemeente Amsterdam en 6 interviews met medewerkers van bedrijven (waarvan één voormalig medewerker). De interviews vonden vanwege de toetertijd geldende coronamaatregelen grotendeels online (met behulp van MS Teams) plaats; enkele interviews werden live afgenomen. Gemiddeld duurde een interview tussen de 30 en 60 minuten; de interviews werden afgenomen door twee personen. Indien de geïnterviewde daarmee instemde, werd een geluidsopname gemaakt die naderhand ook kon worden getranscribeerd. Het transcript van elk interview werd gepseudonimiseerd en vervolgens naar de geïnterviewde gestuurd, zodat deze zijn of haar antwoorden kon herzien, redigeren, verduidelijken of corrigeren. Voor zover de te interviewen personen geen toestemming gaven voor de opname en de transcriptie, werd afgesproken dat de interviewers in plaats van een geluidsopname aantekeningen konden maken tijdens het interview. In die gevallen werden de door de interviewers gemaakte aantekeningen met de geïnterviewde gedeeld, zodat de geïnterviewde deze zo nodig kon aapassen.

Voorafgaand aan het interview werden de te interviewen personen middels een daartoe geprepareerde informatiebrief op de hoogte gesteld van de inhoud en het doel van het onderzoek, de interviewprocedure en de identiteit van de interviewers. De te interviewen personen verleenden middels een toestemmingsformulier toestemming voor het afnemen van het interview, de opname en het laten transcriberen van de (gepseudonimiseerde) geluidsopname naar tekst door een transcriptieservice. De informatiebrief en het toestemmingsformulier zijn voorafgaand aan de interviews goedegekeurd door de Ethische Commissie van de Faculteit der Rechtsgelerdheid van de Universiteit van Amsterdam. Met alle geïnterviewden werd afgesproken dat zij konden meewerken op basis van anonimiteit. Dit houdt in dat de antwoorden in het onderzoeksrapport en in communicatie richting derden niet aan een naam, bedrijf of afdeling werden gekoppeld, om te voorkomen dat deze tot de geïnterviewden herleidbaar zouden kunnen zijn.

Aan gemeentemedewerkers en aan bedrijfsmedewerkers werden vragen gesteld die met name gericht waren op het verkrijgen van een beter beeld van de pratijk bij de tweede onderzoeksvraag, omdat er over de praktijk van het B2G-gegevensdelen relatief weinig bekend is – zo is niet eerder uitgezocht welke juridische knelpunten en onzekerheden zich in de praktijk kunnen voordoen en welke noodzaak (gemeentemedewerkers) voor en welke bereidheid (bedrijfsmedewerkers) bestaat tot B2G-gegevensdeling. De beantwoording van de vragen is tevens relevant voor de beantwoording van de eerste onderzoeksvraag, omdat de geschetste praktijk een impressie geeft van de (beperkingen van het) juridisch kader met het oog op het beter beschermen van de fundamentele rechten van personen op wie de private sensorgegevens betrekking hebben.

6 Geraadpleegde bronnen

Literatuur

- Z. Allam, *Cities and the Digital Revolution: Aligning Technology and Humanity* Palgrave Macmillan: London, UK, 2020.
- J. Ausloos & P. Dewitte, Shattering One-Way Mirrors – Data Subject Access Rights in Practice' (2018) 8 *International Data Privacy Law 4*.
- J. Ausloos, R. Mahieu & M. Veale, 'Getting Data Subject Rights Right. A Submission to the European Data Protection Board from International Data Rights Academics, to Inform Regulatory Guidance (2020) 10 *Journal of International Property, Information Technology and Electronic Commerce Law* (JIPITEC).
- W. Bantema, 'De locale Facebookpagina als café. Een discussie over het bestaan van publieke plaatsen op het internet en de regulering daarvan', (2020) *Bestuurswetenschappen* 74(2).
- E. Baumer, 'Toward human-centered algorithm design' (2017) *Big Data & Society* 4(2).
- B. Bodo & H. Janssen, Maintaining trust in a technologized public sector (2022) *Policy & Society* 41(3).
- H.E. Bröring & K.J. de Graaf (red.), *Bestuursrecht 1. Systeem, bevoegdheid, bevoegdheidsuitoefening, handhaving*, Den Haag: Boom juridisch 2022.
- J.G. Brouwer & A.E. Schilder, 'Over een controversiële conflictregel. Verordening vervallen: fatale vergissing?', in: L.W. Verboeket e.a. (red.), *Bestuursrecht in het echt. Vriendenbundel voor prof. mr. drs. Willemien den Ouden*, Deventer: Wolters Kluwer 2021.
- M. Bovens & S. Zouridis, 'From street-level to system-level bureaucracies: How information and communication technology is transforming administrative discretion and constitutional control' (2002) *Public Administration Review* 62(2) 174.
- J. Cobbe, M. Seng Ah Lee, H. Janssen, J. Singh. 'Centring the law in the digital state' (2020) *IEEE Computer* 54.
- J. van Dijck, T. Poell en M. Janssen, *The Platform society. Public values in a connected world.* Oxford University Press: 2018.
- M.J.J.M. Essers en C.A.M. Lombert, *Aanbestedingsrecht voor overheden. Naar een maatschappelijk verantwoord aanbestedingsbeleid*, Vakmedianet: Deventer 2017.
- L. Fang, 'Debt collectors fight privacy advocates over limits for automated licence plate readers', *The Intercept* (8 mei 2015).
- M. Finck, 'Blockchains: regulating the unknown' (2018) *German Law Journal* 19(4) p. 677.
- M. Galič, *Surveillance and privacy in smart cities and living labs: Conceptualising privacy for public space.* (Diss. UvT 2019), Optima Grafische Communicatie, Rotterdam: 2019).
- G. González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Springer Science & Business 2014.
- M.A. Heldeweg, 'Experimental legislation concerning technological & governance innovation – an analytical approach' (2015) *The Theory and Practice of Legislation* 3(2).
- P.J. Huisman, 'Maatschappelijke akkoorden en de Aanwijzingen voor convenanten: tijd voor een update!', *RegelMaat* 2021, nr. 3.
- P.J. Huisman en F.J. van Ommeren, *Hoofdstukken van privaatrechtelijk overheidshandelen. Publiekrechtelijke en privaatrechtelijke rechtspersonen op de grens van publiek- en privaatrecht*, Deventer: Wolters Kluwer 2019.
- M.J. Jacobs, *Experimentele wetgeving*, oratie VU, Deventer: Wolters-Kluwer 2018.
- C.J.H. Jansen, 'Toepassing van de beginselen van behoorlijk bestuur door de Nederlandse burgerlijke rechter', in: *De polsstok van de beginselen van behoorlijk bestuur. Export en reflexwerking?*, Nijmegen: Wolf Publishers 2021, p. 47-81.

- H. Janssen, 'An approach for a fundamental rights impact assessment to automated decision-making '(2020) *International Data Privacy Law* 10(1).
- H. Janssen, J. Cobbe, C. Norval en J. Singh, Decentralised data processing. Personal data stores and the GDPR (2020) *International Data privacy Law* 10(4).
- I. Kamara & P. de Hert, 'Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach', Brussels Privacy Hub, Vol. 4, No. 12, August 2018.
- E. Keymolen, M. Noorman, B. van der Sloot, C. Cuijpers en B-J. Koops, *Op het eerste gezicht. Een verkenning van gezichtsherkenning en privacyrisico's in horizontale relaties*. Studie verricht in opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum (2020).
- A.K. Koekkoek, *De Grondwet: een systematisch en artikelsgewijs commentaar,* derde druk, Deventer 2000.
- H. van Kolfschooten c.s., *Juridisch instrumentarium voor een gezonde voedselomgeving in de stad*, Universiteit van Amsterdam 2020.
- O. Lynskey, *The foundations of EU Data Protection Law* (Oxford Studies in European Law, OUP 2016).
- R. Mahieu, H. Ashgari en M. van Eeten, 'Collectively exercising the right of access: individual effort, societal effect' (2018) *Internet Policy Review* 1.
- R Mahieu & J Ausloos, 'Recognising and Enabling the Collective Dimension of the GDPR and the Right of Access' *ArXiv*, 2 July 2020, https://osf.io/preprints/lawarxiv/b5dwm/.
- J. Mercille. 'Inclusive smart cities: beyond voluntary corporate data sharing' (2021) *Sustainability* 8135.
- G. Nesti, 'Defining and assessing the transformational nature of smart city governance: insights from four European cases', (2020) *International Review of Administrative Sciences* 30.
- C. Nevejan, City science for urban challenges, Pilot assessment and future potential of the City science Initiative 2019–2020, 46.
- A. Nijboer, *Smart & Leefbaar – Belangen borgen in de digitaliserende gemeente* (digitaal beschikbaar via www.future-city.nl/smartenleefbaar/).
- F.J. van Ommeren, 'Concessies 2.0: de concessie op de grens van de vergunning, de overheidsopdracht en de subsidie', *NTB* 2020/257.
- R. Ortlep & V.A. van Waarde, 'Revolverend publiek geld in het echt! Dienstbaar in alle mogelijke soorten en maten?', in: L.W. Verboeket e.a. (red.), *Bestuursrecht in het echt. Vriendenbundel voor prof. mr. drs. Willemien den Ouden*, Deventer: Wolters Kluwer 2021.
- W. den Ouden, M.J. Jacobs & J.E. van den Brink, *Subsidierecht (Mastermonografieën staats- en bestuursrecht),* Deventer: Wolters Kluwer 2021.
- C. Prins, 'Rutte IV: toezichtreflex en Autoriteit Persoonsgegevens', *NJB* 2022/233.
- S. Ranchordás, *Sunset Clauses and Experimental Legislation: Blessing of Curse for Innovation?* (diss. Tilburg), Zutphen: Koninklijke Wöhrmann 2014.
- H. Reamer Anderson, 'The mythical right to obscurity: a pragmatic defense of no privacy in public', (2012*) I/S A Journal of Law and Policy for the Information Society*, 7(3).
- G. Ritsema van Eck, *Privacy and participation in public data protection issues of crowdsourced surveillance* (diss. RUG 2021).
- A.E. van Rooij, *Orde in het semi-publieke domein: particuliere en publiek-private orderegulering in juridisch perspectief* (diss. Amsterdam VU), Den Haag: Boom juridisch 2017.
- T. Scassa, 'Sharing data in the platform economy: a public-interest argument for access to platform data' (2017) *UBC Law Review* 50(4).
- Jorgen Schram, Henk den Uijl en Mark van Twist, *Actuele kwestie, klassieke afweging. Een verkenning naar de governance van het Nederlandse digitaliseringsbeleid*, Den Haag: NSOB 2021.
- R.J.N. Schlössels, 'De beginselen van behoorlijk bestuur bij 'privaat bestuur'. Algemene normen, gevarieerde rechterlijke toetsing en organisatorische breuklijnen', in: *De polsstok van de beginselen van behoorlijk bestuur. Export en reflexwerking?*, Nijmegen: Wolf Publishers 2021, p. 11-45.

- B.J. Schueler e.a., *Evaluatie van een drietal versnellingsinstrumenten uit de Awb*, Oisterwijk: WLP 2013.
- C.H. Sieburgh, *Mr. C. Assers Handleiding tot de beoefening van het Nederlands Burgerlijk Recht. 6. Verbintenissenrecht. Deel III. Algemeen overeenkomstenrecht*, Deventer: Wolters Kluwer 2022 (Asser/Sieburgh 6-III 2022).
- I. Susha, Å. Grönlund, R. van Tulder, 'Data driven social partnerships: Exploring an emergent trend in search of research challenges and questions', (2019) Go*vernment Information Quarterly 3*6.
- M. Veale & I. Brass, 'Administration by algorithm? Public management meets public sector machine learning', In: M. Veale & I. Brass (Eds.), *Algorithmic regulation*. Oxford University Press: 2019.
- M. Veale & F. Zuiderveen Borgesius, 'Demystifying the draft EU Artificial Intelligence Act' (2021) *Computer Law Review International* 4.
- M.J. Vetzo, J.H. Gerards en R. Nehmelman, *Algoritmes en fundamentele rechten*, Den Haag: Boomjuridisch 2018.
- A. Voorwinden, Regulating the Smart city in European municipalities: a case study of Amsterdam' (2022) *European Public Law*.
- Astrid Voorwinden & Sofia Ranchordás, 'Soft Law in City Regulation and Governance', in: U. Morth, E. Korhea-aho en M. Eliantonio (red.), *Research Handbook on Soft Law*, Edward Elgar Publishing 2022 (digitaal beschikbaar via https://doi.org/10.2139/ssrn.3978959).
- L. Van Zoonen, Privacy concerns in smart cities (2016) *Government Information Quarterly* 33 (3).

Rapporten

- Article 29 Data Protection Working Party ('WP29'), Opinion 03/2013 on purpose limitation (WP 203 van 2 april 2013).
- AP, *Smart Cities: Onderzoeksrapport bescherming van persoonsgegevens in de ontwikkeling van Nederlandse Smart Cities* (juli 2021).
- D. van Barneveld, C. Corver en A. Yeh, Sensoren en de rol van gemeenten. VNG Realisatie Whitepaper (maart 2018).
- Decisio, TwynstraGudde en inno-V in opdracht van het ministerie van Infrastructuur en Waterstaat, *Effecten van openbaar aanbesteden in het Openbaar Vervoer. Een overzicht van de ervaringen in de periode 2000-2020*, 18 maart 2020.
- Christiaan Behrens e.a., *Schaarse vergunningen en terugverdientijd in de ambulante handel*, Amsterdam: SEO Economisch Onderzoek 2021.
- Digitale Infrastructuur Amsterdam (DI020).
- European Data Protection Board (EDPB*) Guidelines 3/2019 on Processing of personal data through video devices* (9–10 juli 2019).
- European Data Protection Board (EDPB), Opinion 5/2019 *on the interplay between the Privacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities.*
- Europese Commissie, *Evaluation of Directive 96/9/EC on the legal protection of databases*, SWD (2018) 146 final.
- R. L. Finn, D. Wright en A. Donovan, L. Jacques en P. de Hert, *Study on privacy, data protection and ethical risks in civil remotely piloted aircraft: final report*, Publications Office, 2015.
- Gemeente Amsterdam, Tada-principes, https://www.amsterdam.nl/innovatie/digitalisering-technologie/data/tada-waarden/; Datastrategie Gemeente Amsterdam. Zelfbeschikking over data 2021 – 2022 (januari 2021).
- Geonovum. *Verkenning Publiek Gebruik Data van Derden* (rapport, 27 mei 2021).
- P. de Hert & S. Gutwirth Data protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in action. In: Y. Poullet, S. Gutwith, C. De Terwanghe, & P. de Hert (Eds.), *Reinventing Data Protection?* Springer: Dordrecht 2009.

- High-Level Expert Group on Business-to-Government Data Sharing European Commission, *Towards a European Strategy on Business-To-Government Data Sharing for the Public Interest*. Eindrapport (2020), HEC Paris Research Paper No. LAW-2020-1394.
- M. Heezen, D. Louwerse en E. Riedstra (Platform 31) *Smart city? Graag. Maar dan wel met bewuste burgers!* Rapport juni 2018.
- Kennedy Van der Laan, Modelverordening smartcity toepassingen in de openbare ruimte (digitaal beschikbaar via https://future-city.nl/modelverordening/).
- L. Kool, J. Timmer, L. Royakkers, R. Van Est. *Opwaarderen. Borgen van publieke belangen in de digitale samenleving*. Den Haag, Rathenau Instituut 2017.
- T. Marsic en K. Bego, *When billboards stare back. How cities can reclaim the digital public space* (mei 2022), Nesta.
- B. Martens & D. Brown, The economics of Business to Government data sharing, JRC Working Papers on Digital Economy 2020-04, Joint Research Centre, European Commission.
- 'OpenSCHUFA – Shedding Light on Germany's Opaque Credit Scoring', AlgorithmWatch (22 May 2017), https://algorithmwatch.org/en/openschufa-shedding-light-on-germanys-opaque-credit-scoring-2.
- Price Waterhouse Coopers *Monitoring in de openbare ruimte* (20 juni 2019); onderzoeksrapport in opdracht van de Commissie Persoonsgegevens Amsterdam.
- Privacy International, '*Our complaints against Axciom, Criteo, Equifax, Experian, Oracle, Quantcast, Tapad*', Rapport 8 november 2018, https://privacyinternational.org/advocacy/2426/our-complaints-against-acxiom-criteo-equifax-experian-oracle-quantcast-tapad.
- Raad voor het openbaar bestuur, 'Sturen of gestuurd worden? Over legitimiteit van sturen met data', Adviesrapport (mei 2021).
- B. Schermer, D. Hagenauw en N. Falot, *Handleiding Algemene Verordening Gegevensbeschermingen Uitvoeringswet Algemene Verordening Gegevensbescherming* 2018 (rapport opgesteld in opdracht van het ministerie van Justitie en Veiligheid).
- B. Van der Sloot, S. van Schendel & C. Augusto Fontanillo López, De invloed van technische ontwikkelingen op het begrip persoonsgegevens in relatie tot de AVG, Rapport in opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum (Tilburg University, December 2022).
- S. Verhulst, A. Young, M. Winowatan, A.J. Zahunanec (2019) 'Leveraging private data for public good. A descriptive analysis and typology of existing practices', *GovLab*, https://datacollaboratives.org/static/files/existing-practices-report.pdf.
- VNG, *Handleiding Wet hergebruik overheidsinformatie*, Den Haag: Ministerie van BZK (2016).
- VNG, *Sensoren en de rol van gemeenten. VNG Realisatie Whitepaper*, Den Haag: VNG (2018).
- VNG, *Principes voor de digitale samenleving*. Deel 1 De digitale openbare ruimte (2020).
- Waag Society Code Future Internet Lab, *Digitisation of the physical public space* (15 mei 2021).
- S. van der Waal, *European Digital Spaces*. Waag Technology & Society 2020.
- Wetenschappelijke Raad voor het Regeringsbeleid (WRR), *Opgave AI. De nieuwe systeemtechnologie* (2021).
- J.H. Gerards, A. Vankan, M.T. Schäfer, I. Muis, *Impact Assessment Mensenrechten en Algoritmes* (2021) (rapport opgesteld in opdracht van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties).

Overig

- L Kelion, 'Amazon's Ring logs every doorbell press and app action', *BBC News* 4 maart 2020, https://www.bbc.com/news/technology-51709247.
- L. Kelion, 'Amazon: Why Amazon knows so much about you', *BBC News*, blog 2020, https://bbc.co.uk/news/extra/CLQYZENMBI/amazon-data.

- T. Synodinou, 'Databases: sui generis protection and copyright protection', *Kluwer Copyright Blog* (20 december 2011).
- Q. Tjeenk Willink, 'Tempo moet omhoog bij de Autoriteit Persoonsgegevens', *Het Financieele Dagblad* 24 november 2021.
- A. Tarkowski e.a., 'A public interest framework for Business to Government data sharing in the Data Act' (2022) Open Future Policy Brief no. 3.
- J. Toh, 'Empowering Workers Through Digital Rights', *Digital Freedom Fund*, 30 April 2021, https://digitalfreedomfund.org/empowering-workers-through-digital-rights/.

Rechtspraak

Europees Hof voor de Rechten van de Mens

- EHRM 7 december 1976, nr. 5493/72 (*Handyside t. Verenigd Koninkrijk*).
- EHRM 26 maart 1987, nr. 9248/81 *(Leander v Sweden*).
- EHRM 16 december 1992, nr. 13710/88 (*Niemitz t. Duitsland*).
- EHRM 25 juni1997, nr. 20605/92 (*Halford t. Vereningd Koninkrijk*).
- EHRM 29 april 2002 nr. 2346/02 (*Pretty t. Verenigd Koninkrijk*).
- EHRM 28 januari 2003, nr. 44647/98 (*Peck t. het Verenigd Koninkrijk*).
- EHRM 24 juni 2004, nr. 59320/00 (*Von Hannover t. Duitsland*).
- EHRM 10 april 2007, nr. 6339/05 (*Evans t. het Verenigd Koninkrijk*).
- EHRM 4 december 2008 (Grote Kamer), nrs. 30562/04 & 30566/04 *(S. and Marper v the UK).*
- EHRM 15 januari 2010, nr. 1234/05 (*Reklos en Davourlis t. Griekenland*).
- EHRM 12 januari 2010, nr. 4158/05 (*Gillan en Quinton t. Verenigd Koninkrijk*).
- EHRM 28 oktober 2016, nr. 61838/10 (*Vukota-Bojić v. Switzerland*).
- EHRM 5 september 2017, nr. 61496 (*Bărbulescu t. Roemenië*).

Hof van Justitie van de Europese Unie

- HvJ EU 20 november 2004, C-444/02 (*Fixtures Marketing Ltd v. Organismos Prognostikon Agonon Podosfairou).*
- HvJ EU 26 februari 2013, C-399/11, ECLI:EU:C:2013:107 (*Melloni*).
- HvJ EU 8 maart 2014, C-293/12 en C-594/12 ECLI:EU:C:2014:238 (*Digital Rights Ireland*).
- HvJ EU 11 december 2014, C-212/13, EU:C:2014:2428 (*František Ryneš v Úřad pro ochranu osobních údajů*).
- HvJ EU 24 februari 2022, C-175/20, ECLI:EU:C:2022:124 (*SS SIA t. Valsts ieņēmumu dienests*).

Hoge Raad

- HR 13 maart 1981, ECLI:NL:HR:1981:AG4158 (*Haviltex*).
- HR 27 maart 1987, ECLI:NL:HR:1987:AG5565 (*Amsterdam/IKON*).
- HR 26 januari 1990, ECLI:NL:HR:1990:AC0965 (*Windmill*).
- HR 24 april 1992, ECLI:NL:HR:1992:ZC0582 (*Zeeland/Hoondert*).
- HR 26 april 1996, ECLI:NL:HR:1996:ZC2051 (*Rasti Rostelli*).
- HR 5 juni 2009, ECLI:NL:HR:2009:BH7845 (*Amsterdam/Geschiere*).
- Conclusie procureur-generaal Knigge van 7 november 2017, ECLI:NL:PHR:2017:1407.
- Conclusie advocaat-generaal E.J. Hofstee van 2 juni 2020, ECLI:NL:PHR:2020:517.
- HR 15 december 2020, ECLI:NL:HR:2020:1993.

Afdeling bestuursrechtspraak van de Raad van State

- ABRvS 13 juli 2011, ECLI:NL:RVS:2011:BR1425 (*Blowverbod Amsterdam*).

- Conclusie staatsraad advocaat-generaal R.J.G.M. Widdershoven van 12 november 2014, ECLI:NL:RVS:2014:4116.
- ABRvS 12 november 2014, ECLI:NL:RVS:2014:4117 (*Intocht van Sinterklaas*).
- ABRvS 4 mei 2016, ECLI:NL:RVS:2016:1177.
- ABRvS 7 december 2016, ECLI:NL:RVS:2016:3253.
- ABRvS 7 juni 2017, ECLI:NL:RVS:2017:1520 (*Rondvaartboten Amsterdam*).
- ABRvS 20 januari 2021, ECLI:NL:RVS:2021:113.
- ABRvS 21 juli 2021, ECLI:NL:RVS:2021:1588.

Gerechtshoven

- Gerechtshof Amsterdam 13 september 2016, ECLI:NL:GHAMS:2016:3749.
- Gerechtshof 's-Hertogenbosch 28 maart 2017, ECLI:NL:GHSHE:2017:1534.
- Gerechtshof Den Haag 25 april 2019, ECLI:NL:GHDHA:2019:906.

Rechtbanken

- Rechtbank Amsterdam 4 september 2014, ECLI:NL:RBAMS:2014:5688.
- Rechtbank Den Haag 27 maart 2019, ECLI:NL:RBDHA:2019:3623.
- Rechtbank Amsterdam 11 maart 2021, ECLI:NL:RBAMS:2021:1020.
- Rechtbank Noord-Holland 2 mei 2022, ECLI:NL:RBNHO:2022:3696.
- Rechtbank Den Haag 13 december 2022, ECLI:NL:RBDHA:2022:13391.

7 Over de auteurs

Alle auteurs (hieronder in alfabetische volgorde weergegeven) zijn verbonden aan de Faculteit der Rechtsgeleerdheid, Universiteit van Amsterdam.

Dr. Balázs Bodo is universitair hoofddocent en sociologisch-juridisch onderzoeker bij het Instituut voor Informatierecht (IViR). In 2018 ontving hij een ERC Starting Grant om de juridische en politieke implicaties van blockchain gebaseerde technologieën te bestuderen. Hij is expert voor de Europese Commissie voor verschillende blockchain-gerelateerde projecten. Kernthema's binnen zijn onderzoek zijn het auteursrecht en economie, informele media-economieën, en aanverwante regelgevingsconflicten rond nieuwe technologische architecturen.

Prof. mr. Jacobine van den Brink is hoogleraar Bestuursrecht en voorzitter van de afdeling Publiekrecht en de sectie Staats- en bestuursrecht. Kernthema's binnen haar onderzoek betreffen de Europeanisering van het bestuursrecht, Europese en Nederlandse financieringsinstrumenten van de overheid, (Europees) subsidierecht, staatssteun en de verdeling van schaarse publieke rechten.

Prof. Mireille van Eechoud is hoogleraar Informatierecht aan het IViR. Kernthema's binnen haar onderzoek betreffen het internationale, Europese en nationale intellectuele eigendomsrecht, met name auteurs-, databankenrecht en naburige rechten; en internationaal privaatrechtelijke aspecten.

Mr. dr. Joris van Hoboken is universitair hoofddocent bij het Instituut voor Informatierecht (IViR), aan de Universiteit van Amsterdam, en hoogleraar 'Fundamental Rights and the Digital Transformation' aan de Vrije Universiteit Brussel. Hij is expert op het gebied van de regulering van internetdiensten en fundamentele rechten. Hij geeft mede leiding aan het Digital Transformation of Decision Making-initiatief op de UvA. Hij was lange tijd voorzitter van de stichting Bits of Freedom.

Mr. dr. Heleen Janssen is onderzoeker bij het Instituut voor Informatierecht (IViR) aan de Universiteit van Amsterdam, en onderzoeker bij het Departement of Computer Science & Technology, University of Cambridge (VK). Thans is zij als fellow tijdelijk werkzaam bij het Netherlands Institute of Advanced Study (KNAW). Kernthema's binnen haar onderzoek betreffen data governance-vraagstukken met een focus op gedecentraliseerde gegevensverwerking, databemiddelingsdiensten ('data intermediary') en gegevensdeling in overeenstemming met fundamentele rechten inclusief het gegevensbeschermingsrecht.

Mr. Arlette Meiring is junior onderzoeker aan het IViR, werkzaam aan projecten op het gebied van gegevensbescherming, open data en digitale soevereiniteit.

Prof. mr. Rolf Ortlep is universitair hoofddocent Bestuursrecht bij de afdeling Publiekrecht (sectie Staats- en bestuursrecht) en hoogleraar (Europees) bestuursrecht aan de Open Universiteit. Kernthema's binnen zijn onderzoek betreffen de algemene rechtsleer, (Europees) bestuursrecht, staatsrecht, bestuursprocesrecht, burgerlijk procesrecht, belastingprocesrecht, privaatrechtelijk overheidsoptreden en aansprakelijkheidsrecht.

Mr. Louise Verboeket is onderzoeker en docent bij de afdeling Publiekrecht (sectie Staats- en bestuursrecht). Zij doet promotieonderzoek naar publieke financiering via prijsvragen op nationaal en Europees niveau. Kernthema's binnen haar onderzoek betreffen het (Europese) aanbestedingsrecht, financieel bestuursrecht en privaatrechtelijk overheidsoptreden.