MASTER'S THESIS

Gemeentelijk (wan)beleid omtrent online monitoring en wifi-tracking

Een onderzoek naar het gebruik van digitale systemen door gemeentelijke bestuursorganen in het kader van de privacywetgeving

Jurna, E.A.

Award date:
2022

Awarding institution:
Department of Public Law

Gemeentelijk (wan)beleid omtrent online monitoring en wifi-tracking

Een onderzoek naar het gebruik van digitale systemen door gemeentelijke bestuursorganen in het kader van de privacywetgeving

Masterscriptie aan de Open Universiteit

Afstudeerrichting:	Staats- en Bestuursrecht
Naam:	Mw. E.A. Jurna
Studentnummer:	852056102
Begeleidster:	Mw. mr. dr. B. Aarrass
Examinator:	Mw. mr. dr. C.L.G.H. Albers
Aantal woorden:	13.997
Inleverdatum:	15 april 2022

Voorwoord

Voor u ligt mijn scriptie: *"Gemeentelijk (wan)beleid omtrent online monitoring en wifi-tracking. Een onderzoek naar het gebruik van digitale systemen door gemeentelijke bestuursorganen in het kader van de privacywetgeving"*. Privacy en de daaronder vallende bescherming van persoonsgegevens spelen op verschillende vlakken van de samenleving een grote rol. Met enige regelmaat kwam ik tijdens mijn rechtenstudie, het dagelijks leven en op de werkvloer in aanraking met het onderwerp privacy en de AVG. Zo las ik veel nieuws- en tijdschriftartikelen over de knelpunten waar veel organisaties tegenaan lopen op het gebied van privacybescherming. Daarnaast had ik vaak gesprekken met mijn familie en vrienden waarin zij vertelden over hun ervaringen met de AVG binnen hun werkgebied. Ook had ik vlak voor het indienen van mijn scriptie-onderwerp tijdens een sollicitatieprocedure zelf een ervaring op het gebied van privacybescherming. Zo waren mijn persoonsgegevens al gedeeld door een overheidsinstantie en achteraf werd mij gevraagd of zij mijn toestemming konden krijgen om mijn gegevens door te geven aan een andere overheidsinstantie waar zij nog op zoek waren naar een geschikte sollicitant. Naast mijn interesse in dit actuele onderwerp dat nog volop in ontwikkeling is, was deze ervaring voor mij de reden om verder onderzoek te doen naar het beleid van gemeentelijke bestuursorganen en het gebruik van digitale systemen in het kader van de privacywetgeving.

Mijn dank gaat in de eerste plaats uit naar mijn scriptiebegeleidster mevrouw Aarrass. Haar eerlijke en kritische feedback hebben mij geholpen om het onderzoek continue aan te scherpen en gerichter te schrijven. Daarnaast wil ik graag mijn familie, vrienden en partner bedanken voor de onvoorwaardelijke steun tijdens het schrijfproces van dit onderzoek. Op de momenten dat ik door de bomen het bos niet meer zag, hebben zij mij weten te motiveren en geholpen door het tussentijds lezen van mijn hoofdstukken.

Ik wens u veel leesplezier.

Inhoudsopgave

1. Inleiding

1.1 Aanleiding

De snelle toenemende digitalisering en vele technologische ontwikkelingen van de laatste jaren hebben geleid tot een nieuw type overheid: een data-gedreven overheid.[1] Het verzamelen van data door (semi-)overheidsinstanties is, ter bescherming van de burger, gebonden aan diverse wet- en regelgeving zoals de Algemene Verordening Gegevensbescherming (AVG) en het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM).[2] De AVG is op 25 mei 2016 in werking getreden en sinds 25 mei 2018 van toepassing binnen de gehele Europese Unie.[3] Het recht op bescherming van persoonsgegevens in de AVG vormt een belangrijke uitwerking op het in artikel 8 EVRM verankerde grondrecht, het recht op privacy.[4]

Bij de verwerking van persoonsgegevens is het van belang dat burgers controle kunnen uitoefenen over hun persoonsgegevens en dat overheden op de hoogte zijn van waar de grenzen van hun bevoegdheden liggen. De praktijk wijst uit dat het verwerken van persoonsgegevens bij gemeentelijke bestuursorganen nog veelvuldig misgaat.[5] Dit is mogelijk het geval bij twee actuele cases, waarbij gemeentelijke bestuursorganen hun handhavings- en besluitvormingsbevoegdheden vermoedelijk op een onjuiste manier inzetten om persoonsgegevens te verwerken. Dit heeft mogelijk tot gevolg dat de privacy van burgers onvoldoende wordt beschermd.

De eerste case betreft online monitoring door Nederlandse gemeenten. De Rijksuniversiteit Groningen en NHL Stenden hebben in opdracht van de Politie onderzoek gedaan, waaruit is gebleken dat ambtenaren van gemeenten op grote schaal onder andere de Facebook en Twitter-accounts van burgers in de gaten houden om preventief te kunnen optreden bij demonstraties en rellen. De meerderheid van de onderzochte gemeenten overtreedt hiermee mogelijk de privacywetgeving, omdat de openbare orde wordt gehandhaafd door nepaccounts te gebruiken

[1] Çapkurt, *NTB* 2019/3.
[2] Çapkurt, *RMThemis* 2020/4, p. 181.
[3] Verordening (EU) 2016/679.
[4] H. van Kolfschooten, 'Europese harmonisatie van privacy – óók in crisistijd', *NJB* 8 juli 2020.
[5] 'Meldplicht datalekken: facts & figures Overzicht feiten en cijfers 2020', autoriteitpersoonsgegevens.nl. Zie ook: Rb. Noord-Nederland 12 januari 2021, ECLI:NL:RBNNE:2021:106, *JBP* 2021/32. Zie ook: Rb. Overijssel 11 augustus 2021, ECLI:NL:RBOVE:2021:3168.

om burgers online te monitoren.[6] Als een bestuursorgaan van de gemeente heeft de burgemeester de taak om de nodige maatregelen te treffen indien de openbare orde in het geding is.[7] De vraag is waar de bestuursrechtelijke grenzen liggen met betrekking tot het handhaven van de openbare orde en veiligheid door middel van digitale methoden en of het gebruik hiervan in overeenstemming is met de geldende wettelijke bepalingen uit onder andere de AVG en artikel 8 EVRM.

In de tweede case staat wifi-tracking centraal. De Autoriteit Persoonsgegevens (AP) heeft het college van burgemeester en wethouders van de gemeente Enschede een bestuurlijke boete van €600.000,- opgelegd wegens het zonder wettelijke grondslag verwerken van persoonsgegevens van gebruikers van mobiele apparaten waarop de wifi stond ingeschakeld.[8] Dit is de eerste keer dat de AP een boete oplegt aan een college van burgemeester en wethouders voor het overtreden van de AVG. Wifi-tracking maakt het mogelijk om door middel van mobiele apparaten gedetailleerde informatie te verkrijgen over onder meer het aantal voorbijgangers en de loopstromen per winkelstraat, gebied of stad. Bij deze overtreding werd de privacy van de burgers mogelijk onvoldoende gewaarborgd.[9] Ook hier is de vraag waar de bestuursrechtelijke grenzen liggen bij het gebruik van wifi-tracking.

1.2 Centrale vraag en deelvragen

De probleemstelling die in het onderzoek centraal staat is:
"In hoeverre is het gebruik van digitale systemen door gemeentelijke bestuursorganen in het kader van handhaving en besluitvorming, in overeenstemming met de bescherming van persoonsgegevens volgens de AVG en het recht op privacy in artikel 8 EVRM?"

De probleemstelling zal aan de hand van de volgende deelvragen worden beantwoord:

1. Wat is online monitoring en wifi-tracking en welke maatschappelijke en/of juridische problematiek hangt hiermee samen? (Hoofdstuk 2)
2. Welke nationale en Europese wet- en regelgeving omtrent de bescherming van persoonsgegevens is van toepassing op het gebruik van online monitoring en wifi-tracking door gemeentelijke bestuursorganen? (Hoofdstuk 3)

[6] K. Maree, 'Nederlandse gemeenten monitoren burgers anoniem op sociale media', *NRC* 18 mei 2021.
[7] Art. 6 jo. art. 172 Gemw. Zie ook: Bantema e.a. 2021, p.12.
[8] 'Rapport boete wifitracking Enschede', autoriteitpersoonsgegevens.nl.
[9] Van Canneyt, *Computerrecht* 2016/125.

3. In hoeverre is het gehanteerde gemeentelijke beleid ten aanzien van online monitoring en wifi-tracking in overeenstemming met het recht op privacy volgens artikel 8 EVRM? (Hoofdstuk 4)
4. In hoeverre is het gehanteerde gemeentelijke beleid ten aanzien van online monitoring en wifi-tracking in overeenstemming met de regels uit de AVG? (Hoofdstuk 5)

1.3 Doelstelling

Het doel van het onderzoek is om de bestuursrechtelijke grenzen van de handhavings- en besluitvormingsbevoegdheden van Nederlandse gemeenten in de context van gegevensbescherming in kaart te brengen.

1.4 Methodologie

Om een antwoord te geven op de probleemstelling zal in dit onderzoek gebruik worden gemaakt van academisch literatuuronderzoek, rechtsbronnen, rapportages, beleidstukken, relevante nationale en Europese wetgeving en jurisprudentie. Gezien de beperkte tijd en omvang van dit onderzoek voert het te ver om van alle gemeenten die gebruikmaken van digitale systemen, de bevoegdheden uiteen te zetten. Om deze reden is ervoor gekozen om aan de hand van twee actuele cases (online monitoring en wifi-tracking) na te gaan in hoeverre de bescherming van persoonsgegevens wordt gewaarborgd volgens het in artikel 8 EVRM verankerde grondrecht, recht op respect voor privacy en de AVG. Daarnaast zijn voor de analyses de drie grootste gemeenten van Nederland geselecteerd: Amsterdam, Rotterdam en Den Haag.[10] Hier is voor gekozen, omdat ik verwacht dat voornamelijk de grotere gemeenten meer ervaring hebben met het gebruik van deze digitale systemen.

Voor de beantwoording van de eerste deelvraag uit hoofdstuk 2 wordt middels academische literatuur als eerst uiteengezet wat er onder online monitoring en wifi-tracking valt en waarom gemeentelijke bestuursorganen kiezen voor het gebruik van deze digitale systemen. Daarnaast komt per case aan bod welke problematiek op maatschappelijk en/of juridisch gebied er heerst. Om de problematiek in kaart te brengen zullen voornamelijk academische literatuur, beleidstukken en rapportages worden geraadpleegd.

[10] 'Inwoners per gemeente', cbs.nl.

In het derde hoofdstuk wordt het juridisch kader van online monitoring en wifi-tracking geschetst. Hierbij zal gebruik gemaakt worden van Europese en nationale wet- en regelgeving. De rechtsbron die hierbij centraal staat is het EVRM, omdat het recht op privacy is verankerd in artikel 8 van dit verdrag en een (onjuiste) toepassing van online monitoring en wifi-tracking mogelijke inbreuken zijn op de privacy van burgers. Een andere rechtsbron die centraal staat is de AVG. Deze Europese verordening vormt een uitwerking van het in artikel 8 EVRM verankerde grondrecht, het recht op privacy. Het recht op privacy is eveneens gecodificeerd in artikel 8 Handvest van de grondrechten van de Europese Unie en artikel 10 Grondwet. De uitleg en interpretatie van deze bepalingen zijn vergelijkbaar met de rechten uit artikel 8 EVRM, omdat hiermee minimaal dezelfde bescherming wordt geboden.[11] Om deze reden zal niet nader worden ingegaan op het Handvest en de Grondwet. Ook zal de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) aan bod komen, omdat in deze wet de nationale keuzes bij de uitvoering van de AVG staan gecodificeerd. Daarnaast zal gebruik worden gemaakt van Europese en nationale jurisprudentie. Te denken valt aan de rechtspraak van het Europees Hof voor de Rechten van de Mens (EHRM), het Europees Hof van Justitie (HvJ EU), de Afdeling Bestuursrechtspraak Raad van State (ABRvS), nationale gerechtshoven en rechtbanken. Tevens zal recente literatuur worden geraadpleegd. Hierbij kan gedacht worden aan verschillende soorten vakliteratuur, zoals artikelen in bundels en tijdschriften, handboeken en internetpublicaties van de afgelopen tien jaar.

In het vierde en vijfde hoofdstuk wordt aan de hand van de geraadpleegde literatuur, rapportages, beleidstukken, nationale en Europese wet- en regelgeving, een analyse gemaakt van het in de praktijk gehanteerde gemeentelijke beleid omtrent online monitoring en wifi-tracking. Hier zal getoetst worden of de gemeentelijke bestuursorganen hun bevoegdheden op onjuiste wijze gebruiken.

1.5 Maatschappelijke en wetenschappelijke relevantie

De AVG kan worden gezien als het belangrijkste wettelijk kader op het gebied van de bescherming van persoonsgegevens. Vele rechtsgeleerden, deskundigen en burgers maken zich zorgen om de hoeveelheid informatie die de overheid verzamelt van de burger en de wijze waarop dit gedaan wordt. Vertrouwen in de uitvoering van het beleid door de overheid speelt

[11] Art. 52 lid 3 Handvest van de grondrechten van de Europese Unie. Zie ook: Barkhuysen & Bos, *JBplus* 2011, p. 17.

hierbij een aanzienlijke rol.[12] Recente gebeurtenissen zoals bijvoorbeeld de Toeslagenaffaire en een groot datalek bij de GGD, vergroten dit vertrouwen in de werkwijze van overheidsinstanties niet.[13] Tevens is uit de jaarlijkse barometer 'Vertrouwen in algoritmes' van KPMG gebleken dat burgers weinig vertrouwen hebben in het gebruik van algoritmes door overheidsinstanties. Ongeveer de helft van de burgers is van mening dat de overheid niet transparant en eerlijk is over het gebruik van algoritmes.[14] Gezien het feit dat algoritmes die door overheidsinstanties toegepast worden, bijna altijd direct van toepassing zijn op de privacy van burgers, maakt dit de impact van mogelijke inbreuken groter.[15]

Ondanks dat de Autoriteit Persoonsgegevens is belast met toezicht en handhaving van de AVG en zij forse bestuurlijke boetes uitdeelt bij overtredingen, is de capaciteit maar beperkt.[16] Dit kan tot gevolg hebben dat de privacy van burgers onvoldoende gewaarborgd wordt en dat overheden nog vaak op onjuiste wijze persoonsgegevens verwerken. De groei van de AP is dan ook noodzakelijk voor burgers.[17]

De ABRvS heeft onlangs besloten dat er de mogelijkheid voor gedupeerde burgers bestaat om op eenvoudige wijze bij de bestuursrechter een schadevergoeding onder de €25.000,- af te dwingen, indien overheden op onrechtmatige wijze met persoonsgegevens omgaan.[18] Door de Afdeling is een bestuursrechtelijke weg in het leven geroepen om de rechtmatigheid van het verwerken van persoonsgegevens en het feitelijk handelen door (gemeentelijke) bestuursorganen te toetsen.[19] Deze ontwikkeling lijkt in het kader van het waarborgen van de privacy-rechten van burgers, een stap in de goede richting te zijn. Echter, het heeft ook prioriteit om het beleid op het gebied van handhaving en besluitvorming binnen gemeenten dermate te vormen, zodat zij de privacyregels uit de AVG en het EVRM in acht nemen. Op dit moment is het nog onduidelijk waar de bestuursrechtelijke grenzen liggen. Een eenduidig en correct beleid op dit gebied lijkt momenteel dan ook te ontbreken.

---

[12] Van den Bos & Brenninkmeijer, *NJB* 2012/1216.
[13] R. Rutten, 'Komt het ooit nog goed met de Toeslagenaffaire?', *NRC* 15 oktober 2021. Zie ook: 'AP eist opheldering van GGD', autoriteitpersoonsgegevens.nl 27 januari 2021.
[14] Schermer, *Computerrecht* 2017/151.
[15] 'Onderzoek: Vertrouwen van de Nederlandse burger in algoritmes. Nederlander heeft weinig vertrouwen in eerlijke inzet algoritmes overheid', home.kpmg.
[16] Barkhuysen, *NJB* 2021/572.
[17] 'Groei AP noodzakelijk voor digitaliserende samenleving en vertrouwen in overheid', autoriteitpersoonsgegevens.nl, 19 mei 2021.
[18] ABRvS 1 april 2020, ECLI:NL:RVS:2020:898, r.o. 22.1.
[19] Polak, Minderhoud & Daalder, *Computerrecht* 2020/184.

1.6 Leeswijzer

Hoofdstuk twee beschrijft wat online monitoring en wifi-tracking inhoudt en wat de maatschappelijke en/of juridische problematiek is op dit gebied. In het derde hoofdstuk wordt het juridisch kader van het gebruik van online monitoring en wifi-tracking geschetst. Hierbij wordt een onderscheid gemaakt tussen het privacy-recht en het bestuursprocesrecht. Onder het privacy-recht wordt met name de reikwijdte van artikel 8 EVRM, de AVG en de UAVG uiteengezet. Daarnaast worden de relevante actoren en hun (bestuurlijke) bevoegdheden inzake online monitoring en wifi-tracking besproken. Hoofdstuk vier en vijf staan in het teken van een analyse van de gemeentelijke beleidspraktijk in het kader van online monitoring en wifi-tracking. De gevoerde beleidspraktijk zal worden getoetst aan de regels uit onder andere artikel 8 EVRM en de AVG. Hoofdstuk zes vormt de conclusie van het onderzoek, waarbij antwoord zal worden gegeven op de centrale vraag.

2. Online monitoring en wifi-tracking

2.1 Inleiding

In Nederland wordt zowel binnen de publieke als private sector steeds meer op grote schaal geïnvesteerd in digitale methoden voor het verzamelen van data.[20] Zo maken gemeenten gebruik van digitale systemen, zoals online monitoring en wifi-tracking. De verwerking van deze data heeft tot gevolg dat burgers door middel van hun handelingen en voorkeuren onbewust invloed uitoefenen op het beleid en processen binnen een stad.[21] Bij veel auteurs roept dit vragen op omtrent de privacy-rechten van burgers.[22] De deelvraag die in dit hoofdstuk zal worden behandeld is: *"Wat is online monitoring en wifi-tracking en welke maatschappelijke en/of juridische problematiek hangt hiermee samen?"* Allereerst zal worden uiteengezet wat online monitoring en wifi-tracking inhoudt en wat de redenen zijn voor de toepassing van dergelijke digitale systemen. Vervolgens komt aan bod wat de maatschappelijke en/of juridische problematiek is.

2.2 Online monitoring

Zowel de gemeente als de politie hebben wettelijke bevoegdheden in het kader van de handhaving van openbare orde en veiligheid. Volgens Kajsa Ollongren, voormalig minister van Binnenlandse Zaken, zijn deze wettelijke taken ook van toepassing in de onlinewereld.[23] Uit een onderzoek naar online monitoring is gebleken dat de meerderheid van de Nederlandse gemeenten de social-media accounts van burgers observeert om vervolgens preventief te kunnen optreden bij ordeverstoringen. Overlast van (groepen) jongeren, oproepen tot demonstraties en het organiseren van illegale evenementen, zijn volgens het rapport voorbeelden van de meest gemonitorde digitale dreigingen.[24] Met het gebruik van online monitoring willen gemeenten onder andere de veiligheidsrisico's tijdig in kaart brengen om vervolgens hierop te kunnen anticiperen.[25] Om online monitoring te bewerkstelligen maken gemeentelijke bestuursorganen gebruik van technische hulpmiddelen zoals monitoringtools of raadplegen zij handmatig de online openbare bronnen, zoals de Facebook of Twitteraccounts van burgers. In sommige gevallen monitoren gemeentelijke ambtenaren zelfs handmatig in

[20] Van der Sloot & Van Schendel, *NJB* 2019/2776.
[21] Van Os, *TBR* 2017/140.
[22] Van der Sloot & Van Schendel, *NJB* 2019/2776.
[23] *Aanhangsel Handelingen II* 2020/21, nr. 3157.
[24] Bantema e.a. 2021, p. 47.
[25] Bantema e.a. 2021, p. 18.

besloten Facebookgroepen.[26] Uit de literatuur blijkt dat vele auteurs van oordeel zijn dat online monitoring slechts in uitzonderlijke gevallen is toegestaan wanneer dit noodzakelijk is voor het vervullen van een taak in het kader van de uitoefening van openbaar gezag. Daarnaast zijn veel auteurs van mening dat het gebruik van online monitoring getoetst dient te worden aan de eisen van proportionaliteit, subsidiariteit en zorgvuldigheid.[27] Hierbij dient altijd een belangenafweging gemaakt te worden tussen enerzijds de belangen van de gemeente en anderzijds de privacy van de burger. Ook moeten gemeenten transparant zijn over het doel van online monitoring. De keuze om nepaccounts te gebruiken, staat volgens velen haaks op het transparantievereiste en is dus allesbehalve wenselijk.[28] Iedere gemeente is verplicht een Functionaris Gegevensbescherming (FG) aan te stellen die toezicht houdt op de toepassing en naleving van de AVG en dus ook op het gebruik van online monitoring door gemeenten.[29] Om ervoor te zorgen dat het online monitoren van burgers op juiste wijze gebeurt, moet de FG actief betrokken zijn bij de werkwijze omtrent online monitoring en dient deze tevens toe te zien op een juiste naleving van de AVG.[30] Uit het onderzoek van NH Stenden blijkt dat bij ongeveer een derde van de onderzochte gemeenten geen FG betrokken is bij online monitoring.[31]

2.2.1 Maatschappelijke en juridische problematiek

Online monitoring is bij de Nederlandse recherche al jaren een succesvolle methode om online strafbare feiten op te sporen en/of informatie te verkrijgen over mogelijke openbare ordeverstoringen.[32] Hierbij is de recherche gebonden aan strikte wettelijke eisen.[33] Deze wettelijke eisen vloeien voort uit de Politierichtlijn en zijn gecodificeerd in de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg).[34] In deze wetten staan specifieke regels over onder andere de rechtmatigheid van de verwerking van persoonsgegevens.[35] Daarnaast maken deze wetten het onderling uitwisselen van informatie

[26] Bantema e.a. 2021, p. 49.
[27] Bantema e.a. 2021, p. 38.
[28] I. Oeltz, 'Online monitoring, veel is mogelijk, zolang u het maar goed regelt', ictrecht.nl 21 juli 2021.
[29] Art. 37 lid 1 onder a jo. art. 39 lid 1 AVG. Zie ook: Bantema e.a. 2021, p. 68.
[30] Art. 38 lid 1 AVG. Zie ook: 'Richtlijnen voor de functionaris voor de gegevensbescherming (FG's)', autoriteitpersoonsgegevens.nl.
[31] Bantema e.a. 2021, p. 68. Zie ook: 'AP verzwaart toezicht op gemeente', autoriteitpersoonsgegevens.nl 6 mei 2021. Zie ook: Art. 3 Polw. 2012.
[32] Bantema e.a. 2021.
[33] Bantema e.a. 2021, p. 31.
[34] Richtlijn (EU) 2016/680. Zie ook: *Kamerstukken II* 2017/18, 34 889, 3, p 7-9.
[35] Art. 9 jo. art. 10 Wpg.

tussen overheidsorganen lastiger.[36] Echter, de burgemeesters hebben naast de recherche ook de taak om de nodige maatregelen te treffen indien de openbare orde en veiligheid in het geding is.[37] Veel gemeenteambtenaren zijn niet of nauwelijks op de hoogte van de geldende protocollen en wettelijke kaders omtrent online monitoring.[38] Deze onwetendheid en mogelijk onzorgvuldige toepassing van online monitoring roept bij deskundigen en rechtsgeleerden verontrustende vragen op met betrekking tot de wenselijkheid van online monitoring door gemeentelijke bestuursorganen.[39] Het ontbreken van een specifieke wettelijke grondslag, het monitoren buiten de rechterlijke macht en de burger om, en de hiermee samenhangende mate van transparantie en de beginselen van proportionaliteit en stelselmatigheid, zijn risico's die kunnen optreden.[40]

Volgens Custers ligt in dergelijke gevallen het gevaar van datalekken op de loer.[41] Door de onwetendheid van gemeentelijke ambtenaren op het gebied van online monitoring is de kans groter dat persoonsgegevens op straat komen te liggen en er ernstige inbreuken op de rechten van burgers worden gemaakt.[42] Naar aanleiding van deze problematiek zijn door diverse leden van de Tweede Kamer, vragen gesteld aan minister Ollongren. Ollongren was van mening dat online monitoring kan bijdragen aan een effectiever gemeentelijk beleid en aan een betere dienstverlening. Daarnaast was zij van mening dat de rijksoverheid en decentrale overheid het goede voorbeeld moeten geven als het gaat om de naleving van wettelijke normen en hierbij de eerbiediging van de persoonlijke levenssfeer en de bescherming van persoonsgegevens moeten waarborgen. Op dit moment lijken de nodige juridische kaders in het bestuursrecht te ontbreken. Om de bewustwording binnen Nederland te vergroten gaat het kabinet een handreiking opstellen, waarin duidelijk wordt aangegeven hoe departementen en uitvoeringsinstanties binnen de wettelijke kaders van de AVG kunnen monitoren.[43] Wanneer deze handreiking tot stand komt en hoe deze handreiking er concreet uit komt te zien is nog onduidelijk. Tevens is de vraag in hoeverre de handreiking ook daadwerkelijk zal bijdragen aan de bewustwording ten

[36] Art. 20 Wpg jo. art. 15 Wjsg.
[37] Art. 172 Gemw. Zie ook: Bantema e.a. 2021, p. 12.
[38] Bantema e.a. 2021.
[39] Bantema e.a. 2021, p. 37. Zie ook: *Comparative study on blocking, filtering and take-down of illegal internet content* 2017.
[40] Bantema e.a. 2021, p. 39.
[41] Hoogleraar Law and Data Science aan de Universiteit Leiden.
[42] H. von Piekartz, 'Ollongren wil opheldering van gemeenten over heimelijk volgen burgers', *Volkskrant* 18 mei 2021.
[43] *Aanhangsel Handelingen II* 2020/21, nr. 3157.

aanzien van de naleving van de wettelijke normen op het gebied van privacy en de bescherming van persoonsgegevens. Daarnaast zal moeten blijken in hoeverre handreiking de rechtszekerheid ten goede komt. Dit is uiteraard afhankelijk van de inhoud van de handreiking.

2.3 Wifi-tracking

Wifi-tracking is een technologie waarbij één of meerdere sensoren informatie over de locatie van mobiele apparatuur registreren aan de hand van het wifisignaal. In veel gemeenten zijn sensoren geplaatst in onder andere winkelgebieden. Het wifisignaal van mobiele apparatuur wordt opgevangen door de sensoren, waarbij het unieke Media Access Control (MAC)-adres wordt verzameld.[44] Dit is een uniek identificatienummer van een mobiel apparaat. Wanneer een smartphone, tablet of laptop verbinding probeert te maken met een wifi-netwerk, wordt het MAC-adres uitgezonden. In bijna alle gevallen worden persoonsgegevens verwerkt, waardoor op het gebruik van wifi-tracking de privacyregels van toepassing zijn.[45] De AP is van oordeel dat het digitaal volgen van burgers die zich op een openbare plek bevinden, een inbreuk op de privacy is. Dit mag alleen bij uitzondering toegepast worden.[46]

2.3.1 Maatschappelijke en juridische problematiek

Het gebruik van wifi-tracking vindt in Nederland op grote schaal plaats en staat in de top drie van de privacy zorgen van burgers.[47] De AP heeft in 2016 middels een brief aan de Vereniging van Nederlandse Gemeenten (VNG) kenbaar gemaakt dat er strikte wettelijke eisen zijn verbonden aan de toepassing van wifi-tracking. Het volgen van personen in (semi-) openbare ruimtes middels wifi-tracking is slechts in zeer uitzonderlijke gevallen toegestaan.[48] Met de brief aan de VNG beoogt de AP de inbreuken op de persoonlijke levenssfeer van burgers te voorkomen. Aan het gebruik van wifi-tracking zitten nadelen en risico's verbonden die van invloed kunnen zijn op de persoonlijke levenssfeer van burgers. In 2018 was maar liefst 87% van de Nederlanders tussen de 16 en 75 jaar in het bezit van een smartphone.[49] Van deze meerderheid van de smartphonebezitters gebruikt 84% de smartphone ook veelvuldig buitenshuis.[50] Een smartphone is dan ook onlosmakelijk met een eigenaar verbonden en bevat

[44] Valgaeren & Leitner, *Computerrecht* 2012/2.
[45] Raas, Elshof & Janssens, *WR* 2017/177.
[46] 'Bedrijven mogen mensen alleen bij hoge uitzondering met wifitracking volgen', autoriteitpersoonsgegevens.nl 30 november 2018.
[47] 'Nederland maakt zich zorgen over privacy', autoriteitpersoonsgegevens.nl 28 januari 2019.
[48] 'AP wijst winkels en gemeenten op voorwaarden wifitracking', autoriteitpersoonsgegevens.nl.
[49] 'Meeste Nederlanders beschermen gegevens op smartphone', cbs.nl 4 februari 2019.
[50] J. Arends, 'ICT-gebruik van huishoudens en personen', cbs.nl.

aanzienlijk veel persoonlijke informatie. Te denken valt aan privéfoto's, locatiegegevens, maar ook hoe lang en hoe vaak welke apps gebruikt worden.[51] De combinatie van het unieke MAC-adres, een tijdstip en een datum kunnen gemakkelijk tot identificatie van de eigenaar van een mobiel apparaat leiden. De AP wijst burgers er dan ook op dat het belangrijk is om een smartphone en/of tablet veilig in te stellen. Hiermee kan voorkomen worden dat persoonsgegevens in verkeerde handen terechtkomen.[52] Een goede ontwikkeling op dit gebied is dat mensen zich steeds bewuster worden van het beschermen van hun persoonsgegevens. Uit recent onderzoek van het Centraal Bureau voor de Statistiek is gebleken dat 70% van de Nederlandse smartphonebezitters de toegang tot persoonlijke gegevens zoals de locatie, privéfoto's of contactpersonen weigeren, wanneer zij een app op de smartphone of tablet installeren of gebruiken.[53] Desondanks is er momenteel een gebrek aan transparante informatievoorziening op het gebied van wifi-tracking. Burgers zijn in de meeste gevallen niet op de hoogte van wanneer sensoren in bepaalde gebieden gebruikt worden om hun verplaatsingsgedrag te volgen, welke gegevens hierbij gemeten worden en hoe lang de gegevens bewaard blijven.[54]

2.4 Tussenconclusie

De digitale systemen online monitoring en wifi-tracking worden veelvuldig en op grote schaal door gemeenten ingezet. Door middel van het gebruik van online monitoring proberen gemeenten onder andere de veiligheidsrisico's in kaart te brengen bij geplande rellen en/of demonstraties. Hierbij wordt in sommige gevallen gebruik gemaakt van technische hulpmiddelen zoals algoritmen. Ook komt het voor dat gemeentelijke ambtenaren handmatig de social-media accounts van burgers raadplegen. Bij wifi-tracking probeert een gemeentelijk bestuursorgaan inzicht te krijgen in de loopstromen in een bepaald gebied, om zo het gemeentelijk beleid te verbeteren. Het wifisignaal van mobiele apparatuur zoals smartphones wordt hierbij opgevangen door sensoren, waardoor onder andere het unieke MAC-adres wordt verzameld. In beide cases wordt het gebruik van dergelijke digitale systemen mogelijk op onjuiste wijze toegepast, waarbij de bescherming van persoonsgegevens onvoldoende wordt gewaarborgd. Op dit moment lijken gemeenten maar beperkt op de hoogte te zijn van hun

[51] 'Smartphones en apps', autoriteitpersoonsgegevens.nl. Zie ook: *Wifi-tracking van mobiele apparaten in en rond winkels door Bluetrace* 2015, p. 5.
[52] 'Smartphones en apps', autoriteitpersoonsgegevens.nl.
[53] '9 op de 10 internetgebruikers beschermen persoonsgegevens', cbs.nl 9 februari 2021.
[54] *Wifi-tracking van mobiele apparaten in en rond winkels door Bluetrace* 2015, p. 57.

bestuurlijke bevoegdheden op het gebied van online monitoring en wifi-tracking. Daarnaast zijn gemeenten onvoldoende transparant naar burgers toe, als het gaat om het verstrekken van informatie die betrekking heeft op de verwerking van persoonsgegevens.

3. Het juridisch kader

3.1 Inleiding

Het recht op privacy, waar de bescherming van persoonsgegevens een onderdeel van is, vormt de basis voor een democratische rechtstaat en staat centraal bij het verwerken van persoonsgegevens middels digitale systemen. Door het gebruik van online monitoring en wifi-tracking kan er (onbewust) een inbreuk worden gemaakt op de privacy-rechten van burgers. In dit hoofdstuk wordt de volgende deelvraag beantwoord: *Welke nationale en Europese wet- en regelgeving omtrent de bescherming van persoonsgegevens is van toepassing op het gebruik van online monitoring en wifi-tracking?* Als eerst komt het privacy-recht aan bod. Hier wordt onder andere het recht op privacy uit artikel 8 EVRM uiteengezet en de regels uit de AVG en de UAVG besproken. Daarnaast worden slechts de relevante actoren binnen het bestuursprocesrecht besproken. Zo worden de taken en bevoegdheden van de AP, de FG en de gemeentelijke bestuursorganen beschreven.

3.2 Het recht op privacy en de bescherming van persoonsgegevens

3.2.1 Artikel 8 EVRM

Op grond van artikel 8, eerste lid, EVRM heeft iedereen recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.[55] Dit verankerde mensenrecht heeft tot doel om burgers te beschermen tegen inbreuken door de overheid op de privacy.[56] Artikel 93 Gw bepaalt: *"bepalingen van verdragen en van besluiten van volkenrechtelijke organisaties, die naar haar inhoud een ieder kunnen verbinden, hebben verbindende kracht nadat zij zijn bekendgemaakt"*. Artikel 8 EVRM is zo 'een ieder verbindende bepaling' en werkt rechtstreeks door in het Nederlandse rechtsstelsel.[57] Uit artikel 94 Gw vloeit voort dat nationale wettelijke voorschriften buiten toepassing gelaten kunnen worden door de rechter, indien de toepassing van de nationale regeling niet verenigbaar is met een ieder verbindende bepaling van verdragen zoals het EVRM. In dergelijke gevallen heeft een Europese verdragsbepaling voorrang.[58]

[55] *Guide on Article 8 of the Convention - Right to respect for private and family life* 2021, p. 8.
[56] EHRM 16 december 1992, ECLI:NL:XX:1992:AD1800, r.o. 31 (*Niemietz*).
[57] Sanderink, *SteR* 2018/41. Zie ook: Art. 93 Gw.
[58] HvJ EG 15 juli 1964, ECLI:EU:C:1964:66 *(Costa/ENEL).*

Als een Europese of nationale rechter van oordeel is dat een (verwerkings)handeling het recht op eerbiediging van het privéleven van een individu schaadt, wordt onderzocht in hoeverre de inmenging gerechtvaardigd is. Ondanks dat het recht op privacy een belangrijk grondrecht is dat gewaarborgd dient te worden, is het geen absoluut recht. Het recht op privacy dient dan ook te worden afgewogen tegen andere gerechtvaardigde belangen en rechten.[59] In artikel 8 lid 2 EVRM is bepaald dat inmenging door de overheid in de persoonlijke levenssfeer onder enkele voorwaarden geoorloofd is.[60] Zo dient de inbreuk op het grondrecht gebaseerd te zijn op een wettelijke bepaling. Daarnaast moet er een legitiem doel worden nagestreefd. Ten slotte wordt vereist dat de inbreuk noodzakelijk is in een democratische samenleving.[61] Indien aan één van deze drie voorwaarden niet is voldaan, is inmenging door de overheid niet gerechtvaardigd en wordt er een onrechtmatige inbreuk gemaakt op het recht op privacy.[62] Deze drie limitatieve beperkingsvoorwaarden zullen in de volgende paragraaf nader worden uitgewerkt.

3.2.1.1 Beperkingsvoorwaarden

Bij de wet voorzien

Voor een gerechtvaardigde inbreuk op het recht op respect voor privacy dient er een nationale wettelijke grondslag aanwezig te zijn. Het EHRM interpreteert deze voorwaarde ruim door te oordelen dat het niet slechts een wet in formele zin hoeft te zijn, maar dat algemeen verbindende voorschriften of bepalingen van ongeschreven recht ook kunnen volstaan.[63] Daarnaast dient de wettelijke bepaling te voldoen aan enkele kwaliteitseisen volgens de 'rule of law'. Deze 'rule of law' gedachte dient als waarborg tegen willekeurig overheidsoptreden. Bij de beoordeling van de kwaliteit wordt gekeken of de desbetreffende wet voldoet aan de vereisten van toegankelijkheid en voorzienbaarheid.[64] Ten eerste dient de rechtsnorm kenbaar te zijn voor burgers, zodat zij weten welke regels van toepassing zijn en hoe zij in overeenstemming met de wet kunnen handelen.[65] Ten tweede is het voor burgers belangrijk om te weten welke

[59] Giakoumopoulos, Buttarelli & O'Flaherty 2018, p. 44.
[60] Kranenborg, in: *T&C Privacy- en gegevensbeschermingsrecht*, art. 8 EVRM, (online, bijgewerkt 1 oktober 2021).
[61] Van Toor, *SteR* 2017/32.
[62] Kranenborg, in: *T&C Privacy- en gegevensbeschermingsrecht*, art. 8 EVRM, (online, bijgewerkt 1 oktober 2021).
[63] EHRM 26 april 1979, ECLI:CE:ECHR:1979:0426JUD000653874 (*Sunday Times v. Verenigd Koninkrijk).*
[64] EHRM 26 april 1979, ECLI:CE:ECHR:1979:0426JUD000653874 (*Sunday Times v. Verenigd Koninkrijk).*
[65] EHRM 2 augustus 1984, ECLI:CE:ECHR:1984:0802JUD000869179, r.o. 67 (*Malone t. Verenigd Koninkrijk*).

bevoegdheden publieke autoriteiten hebben en dus ook welke inbreuken geoorloofd zijn.[66] De wettelijke bepaling dient voldoende duidelijk en gedetailleerd aan te geven in welke gevallen de overheid mag overgaan op online monitoring of wifi-tracking om misbruik en willekeur te voorkomen.[67] Het EHRM heeft geoordeeld dat het voor burgers mogelijk moet zijn een inschatting te maken wat de gevolgen van bepaalde handelingen zijn.[68] Het vereiste van voorzienbaarheid gaat echter niet zover dat een burger in specifieke gevallen zou moeten weten wanneer de overheidsorganen communicatie onderscheppen. Burgers zouden anders hun gedrag kunnen aanpassen en dit zou dan een ongewenst effect kunnen hebben op het functioneren van de diensten.[69] Gezien het feit dat de technieken om persoonsgegevens te verwerken zich steeds verder ontwikkelen en online monitoring en wifi-tracking in de meeste gevallen zonder medeweten van burgers plaatsvinden, kan het lastig zijn om te oordelen wanneer een bepaling voldoende duidelijk is om over te kunnen gaan op online monitoring en/of wifi-tracking.[70]

Legitiem doel

Volgens de tweede voorwaarde moet er een legitiem doel aanwezig zijn voor een gerechtvaardigde inmenging van de overheid.[71] Het tweede lid van artikel 8 EVRM geeft een limitatieve opsomming van de legitieme doelen. Zo moet de inbreuk in het belang zijn van: *"de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen"*.[72] Het EHRM interpreteert deze doelen ruim, zodat lidstaten gemakkelijk aannemelijk kunnen maken dat zij een legitiem doel nastreven. Het voldoen aan deze voorwaarde vormt in de praktijk vrijwel nooit een probleem.[73]

---

[66] Van Toor, *SteR* 2017/32. Zie ook: EHRM 6 september 1978, ECLI:CE:ECHR:1978:0906JUD000502971, (*Klass e.a./Duitsland*). Zie ook: EHRM 26 maart 1987, ECLI:CE:ECHR:1987:0326JUD000924881, r.o. 51 (*Leander t. Zweden*). Zie ook: *Kamerstukken II* 2016-2017, 34588 nr. 4, p. 8-9.
[67] EHRM 4 december 2008, ECLI:CE:ECHR:2008:1204JUD003056204 (*S. en Marper t. Verenigd Koninkrijk*).
[68] EHRM 26 maart 1987, ECLI:CE:ECHR:1987:0326JUD000924881, r.o. 51 (*Leander t. Zweden*). Zie ook: *Kamerstukken II* 2016-2017, 34588 nr. 4, p. 8-9.
[69] EHRM 2 augustus 1984, ECLI:CE:ECHR:1984:0802JUD000869179, r.o. 67-68 (*Malone t. Verenigd Koninkrijk*). Zie ook: *Kamerstukken II* 2016-2017, 34588 nr. 4, p. 27.
[70] EHRM 13 september 2018, ECLI:CE:ECHR:2018:0913JUD005817013 (*Big Brother Watch t. Verenigd Koninkrijk).*
[71] EHRM 28 januari 2003, ECLI:CE:ECHR:2003:0128JUD004464798 (*Peck t. Verenigd Koninkrijk).*
[72] Art. 8 lid 2 EVRM.
[73] Van Toor, *SteR* 2017/32.

Noodzakelijk in een democratische samenleving

Het derde criterium vereist dat de inbreuk op het recht op privacy noodzakelijk is in een democratische samenleving. Het EHRM heeft bepaald dat een maatregel als noodzakelijk kan worden beschouwd wanneer er een dwingende maatschappelijke behoefte bestaat en het doel met de toepassing van de maatregel bereikt kan worden.[74] Hierbij moet een redelijke belangenafweging worden gemaakt tussen enerzijds het te dienen doel en anderzijds het recht van het individu.[75] Lidstaten hebben bij deze belangenafweging een mate van beleidsruimte. De hoeveelheid beleidsruimte van een lidstaat is afhankelijk van het karakter van een democratische samenleving.[76] Bij de belangenafweging toetst het EHRM of lidstaten binnen de 'margin of appreciation' in een dwingende maatschappelijke behoefte voorzien door op een proportionele wijze een inbreuk op het recht op respect voor privacy te maken.[77]

Om te bepalen wat binnen de 'margin of appreciation' valt, wordt gekeken naar een drietal factoren. In de eerste plaats staat de Europese consensus op het gebied van privacy centraal. Hierbij gaat het voornamelijk om de wijze waarop de meerderheid van de Europese lidstaten tegen een bepaalde regulering aankijkt.[78] Daarnaast wordt gekeken welk belang een specifiek grondrecht voor de burger heeft. Bij inbreuken op artikel 8 EVRM is het belangrijk om te kijken in hoeverre de kern van privacy wordt aangetast.[79] Dit is het geval bij onderwerpen die gaan over de persoonlijke identiteit en de daarbij behorende persoonlijke data.[80] Als laatste wordt gekeken naar het doel dat met de inbreuk op het grondrecht wordt gediend. Bij het voorkomen en opsporen van strafbare feiten, geldt een zekere 'margin of appreciation' voor de nationale autoriteiten.[81] Vervolgens is het aan de verwerende lidstaat om aan te tonen of er sprake is van een dwingende maatschappelijke behoefte.[82] Het EHRM toetst in hoeverre de inbreuk effectief

[74] EHRM 22 oktober 1981, ECLI:CE:ECHR:1981:1022JUD000752576 (*Dudgeon t. Verenigd Koninkrijk)*. Zie ook: EHRM 25 februari 1997, ECLI:CE:ECHR:1997:0225JUD002200993 *(Z. t. Finland).*
[75] Van Toor, *SteR* 2017/32.
[76] EHRM 22 oktober 1981, ECLI:CE:ECHR:1981:1022JUD000752576, r.o. 51-53 (*Dudgeon t. Verenigd Koninkrijk).*
[77] Van Toor, *SteR* 2017/32.
[78] EHRM 4 december 2008, *ECLI:NL:XX:2008:BH1813,* r.o. 112, m.nt. Van der Staak *(S. & Marper vs. het Verenigd Koninkrijk).*
[79] EHRM 24 april 2012, 25446/06, r.o. 118 (ii) *(Yordanova en anderen vs. Bulgarije).*
[80] EHRM 27 oktober 2009, 21737/03 *(Haralambie v. Romania)*. EHRM 24 april 2018, ECLI:CE:ECHR:2018:0424JUD006235714 (*Benedik v. Slovenië*). Zie ook: *Guide on case-law of the Convention – Data protection* 2021, p. 7.
[81] EHRM 28 oktober 1994, ECLI:NL:XX:1994:AD2244, r.o. 90 *(Murray vs. het Verenigd Koninkrijk).*
[82] EHRM 24 januari 2017, ECLI:CE:ECHR:2017:0124**,** r.o. 179 *(Paradiso Campanelli v.Italy)*. Zie ook: EHRM 26 april 1979, ECLI:NL:XX:1979:AC6568, r.o. 62 *(Sunday Times vs. het Verenigd Koninkrijk)*.

kan bijdragen aan het vervullen van de maatschappelijke behoefte.[83] Bij het proportionaliteitsbeginsel wordt getoetst of de inbreuk in evenredige verhouding staat tot het doel.[84] De rechtbank Den Haag heeft bijvoorbeeld in een recente uitspraak geoordeeld dat het gebruik van het Systeem Risico Indicatie (SyRI) in strijd is met artikel 8 lid 2 EVRM. Op verzoek van enkele overheidsinstanties met een publieke taak wordt door de minister gebruik gemaakt van SyRI om fraude op het gebied van uitkeringen, toeslagen en belastingen te bestrijden.[85] In deze zaak is een belangenafweging gemaakt tussen enerzijds het gebruik van SyRI om fraude te bestrijden, en anderzijds de inmenging van de overheid op de persoonlijke levenssfeer van burgers. De rechtbank was van oordeel dat de inzet van SyRI een ontoelaatbare inbreuk op het privéleven creëerde, omdat het systeem onvoldoende inzichtelijk en controleerbaar was.[86] In combinatie met het proportionaliteitsbeginsel wordt ook getoetst aan het subsidiariteitsbeginsel, waarbij altijd gekozen moet worden voor de minst ingrijpende maatregel.[87]

3.2.2 De Algemene Verordening Gegevensbescherming

De AVG is een verordening van de Europese Unie waarin het recht op privacy specifiek voor persoonsgegevens wordt geregeld. De bescherming van persoonsgegevens is als een apart grondrecht gecodificeerd in artikel 8 van het Handvest van de grondrechten van de Europese Unie en artikel 16 van het Verdrag betreffende de werking van de Europese Unie.[88] Sinds 25 mei 2018 regelt de AVG de bescherming van persoonsgegevens binnen de gehele Europese Unie.[89] Sindsdien zijn op het gebied van het Europese privacy-recht enorme veranderingen doorgevoerd.[90] Zo zijn de door het Europees Parlement en de Raad opgestelde Richtlijn betreffende de bescherming van persoonsgegevens en de daarop gebaseerde Wet bescherming persoonsgegevens, vervangen door de AVG.[91] De aanzienlijke toename van technologische ontwikkelingen en de significante stijging van de mate waarin persoonsgegevens worden

[83] Van Toor, *SteR* 2017/32.
[84] EHRM 25 februari 1997, ECLI:CE:ECHR:1997:0225JUD002200993 *(Z. t. Finland).*
[85] Rb. Den Haag 5 februari 2020, ECLI:NL:RBDHA:2020:865, r.o. 3.3.
[86] Rb. Den Haag 5 februari 2020, ECLI:NL:RBDHA:2020:865, r.o. 6.7.
[87] Oerlemans, *Strafblad* 2017/4, p. 76. Zie ook: EHRM 28 januari 2003, ECLI:CE:ECHR:2003:0128JUD004464798 (*Peck t. Verenigd Koninkrijk*)
[88] Schermer, Hagenauw & Falot 2018, p. 19.
[89] Verordening (EU) 2016/679.
[90] F. van der Jagt, 'Algemene Verordening Gegevensbescherming (AVG)', navigator.nl.
[91] Richtlijn 95/46/EG.

verwerkt, hebben geleid tot dat de bescherming van persoonsgegevens voor nieuwe uitdagingen komt te staan.[92]

Materieel en territoriaal toepassingsgebied

De rechten en plichten die voortvloeien uit de AVG hebben rechtstreekse werking binnen de gehele Europese Unie en voorrang op nationale wetgeving.[93] Om te bepalen of de regels uit de AVG van toepassing zijn, wordt gekeken naar twee punten: het materiele toepassingsgebied en het territoriale toepassingsgebied. Artikel 2 AVG omschrijft de materiele reikwijdte, waarbij er wordt gekeken naar de vraag op welke handelingen de AVG van toepassing is. Het eerste lid van artikel 2 AVG stelt dat de regels van toepassing zijn op gehele of gedeeltelijke verwerking van persoonsgegevens, indien deze digitaal, elektronisch of computergestuurd verwerkt zijn.[94] Echter, één van de doelen van de AVG is dat de bescherming technologieneutraal moet zijn. Dit betekent dus dat het niet uit dient te maken op welke wijze en met welke middelen de persoonsgegevens worden verwerkt. De bescherming dient te gelden bij zowel geautomatiseerde verwerking als handmatige verwerking van persoonsgegevens, indien deze gegevens zijn opgeslagen of bedoeld zijn om opgeslagen te worden in een bestand.[95] Daarnaast is de AVG in beginsel van toepassing op alle rechtsgebieden, tenzij er bijzondere bepalingen zijn die de bescherming van persoonsgegevens nader regelen. Het materiele toepassingsgebied van de AVG beschrijft namelijk in artikel 2 lid 2 sub d een aantal gevallen wanneer de AVG niet geldt.[96] In dergelijke gevallen gelden de Europese Richtlijn gegevensbescherming opsporing en vervolging, de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens.[97]

Het territoriale toepassingsgebied is vastgelegd in artikel 3 AVG. Deze wet heeft betrekking op de verwerking van persoonsgegevens op Europees grondgebied of indien het gaat om de verwerking van persoonsgegevens van Unieburgers. Daarnaast worden er nog vier gevallen beschreven waarin de AVG ook van toepassing is, maar deze zijn minder van belang voor het bestuursrecht en zullen daarom niet verder behandeld worden.[98]

[92] Verordening (EU) 2016/679 (overweging 6).
[93] HvJ EG 15 juli 1964, ECLI:EU:C:1964:66 *(Costa/ENEL).*
[94] Artikel 2 lid 1 AVG.
[95] Verordening (EU) 2016/679 (overweging 15).
[96] Verordening (EU) 2016/679 (overweging 16-19).
[97] Richtlijn (EU) 2016/680.
[98] Verordening (EU) 2016/679 (overweging 22-25).

Beginselen verwerking persoonsgegevens

Artikel 5 AVG geeft algemene beginselen inzake de verwerking van persoonsgegevens weer. Volgens het eerste beginsel dienen persoonsgegevens op een rechtmatige, behoorlijke en transparante manier verwerkt te worden.[99] Er is sprake van rechtmatigheid wanneer er een deugdelijke rechtsgrondslag is voor de verwerking. In artikel 6 lid 1 AVG is een opsomming gegeven van deze rechtsgrondslagen. De rechtsgrondslagen die van toepassing kunnen zijn op de verwerking van persoonsgegevens bij online monitoring en wifi-tracking worden in de volgende paragraaf uiteengezet. Het begrip behoorlijkheid wordt altijd in samenhang met de begrippen rechtmatigheid en transparantie gebruikt.[100] Op gemeentelijke bestuursorganen rust de verplichting dat zij burgers dienen te informeren over de verwerking van de persoonsgegevens. Deze informatie moet eenvoudig toegankelijk en begrijpelijk zijn. Aan burgers dient duidelijk gemaakt te worden wat de risico's, regels, waarborgen en rechten zijn op het gebied van de verwerking van hun persoonsgegevens.[101] Volgens het tweede beginsel dienen persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen verzameld te worden.[102] Deze persoonsgegevens dienen dan ook enkel en alleen ten behoeve van deze doelen verzameld te worden. Het derde beginsel gaat over de minimale gegevensverwerking.[103] De verwerking van persoonsgegevens moet een volledig beeld van de burger schetsen met het oog op het te bereiken doel. Daarnaast dienen de persoonsgegevens betrekking te hebben op het na te streven doel.[104] Het vierde beginsel bepaalt dat persoonsgegevens juist zijn en zo nodig geactualiseerd moeten worden. Als dit niet het geval is, moeten alle redelijke maatregelen worden genomen om persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, te wissen of te rectificeren.[105] Bij het nemen van maatregelen die redelijk zijn spelen factoren zoals de soort gegevens, de techniek en de kosten een rol. Het vijfde beginsel is het opslagbeginsel.[106] In de AVG is niks opgenomen over een specifieke bewaringstermijn voor persoonsgegevens. Het beginsel van opslagbeperking lijkt in dit geval op het proportionaliteitsbeginsel.[107] Volgens de AP mogen organisaties en instanties

[99] Art. 5 lid 1 sub a AVG.
[100] Van Canneyt e.a., *Computerrecht* 2021/56. Zie ook: Art. 12, 13, 14 AVG.
[101] Verordening (EU) 2016/679 (overweging 39). Zie ook: De Vries, in: *T&C Privacy- en gegevensbeschermingsrecht*, commentaar op art. 5 AVG, (online, bijgewerkt 1 oktober 2021)
[102] Art. 5 lid 1 sub b AVG.
[103] Art. 5 lid 1 sub c AVG.
[104] Schermer, Hagenauw & Falot 2018, p. 22.
[105] Art. 5 lid 1 sub d AVG.
[106] Art. 5 lid 1 sub e AVG.
[107] HvJ EU 13 mei 2014, ECLI:EU:C:2014:317, r.o. 93 (*Google Spain and Google*). Zie ook: HvJ EU 24 september 2019, ECLI:EU:C:2019:773, r.o. 74 (*GC and Others*).

zelf beslissen voor welke termijn zij persoonsgegevens bewaren, tenzij er in andere wetten concrete bewaringstermijnen zijn bepaald.[108] Het laatste beginsel gaat over integriteit en vertrouwelijkheid. Om datalekken tegen te gaan dienen technische en organisatorische maatregelen ervoor te zorgen dat persoonsgegevens beveiligd zijn.[109] Voorbeelden van dergelijke maatregelen zijn pseudonimisering en versleuteling.[110]

Grondslagen rechtmatige verwerking

In artikel 6 lid 1 AVG worden zes grondslagen beschreven voor een rechtmatige verwerking van persoonsgegevens. Deze grondslagen zijn: toestemming, uitvoering van een overeenkomst, wettelijke verplichting, bescherming vitale belangen, taak van algemeen belang of in het kader van de uitoefening van het openbaar gezag, behartiging gerechtvaardigde belangen. Wanneer tenminste één van deze rechtsgrondslagen van toepassing is, is de verwerking van persoonsgegevens gerechtvaardigd.[111] Met De Vries en Meijer ben ik van mening dat voornamelijk de grondslagen 'toestemming', 'wettelijke verplichting' en/of 'noodzakelijk voor de vervulling van een taak van algemeen belang of in het kader van de uitoefening van openbaar gezag' relevant zijn voor gemeentelijke bestuursorganen bij het gebruik van online monitoring en wifi-tracking.[112] Deze drie grondslagen zullen dan ook hieronder nader worden uiteengezet.

Op grond van de eerste rechtsgrondslag moet een betrokkene toestemming geven voor de verwerking van zijn of haar persoonsgegevens voor één of meerdere specifieke doelen. Een verwerkingsverantwoordelijke, zoals een bestuursorgaan dient aan te tonen dat een burger uitdrukkelijk actieve toestemming heeft gegeven voor het verwerken van zijn of haar persoonsgegevens.[113] Deze uitdrukkelijke actieve toestemming kan door middel van een schriftelijke, elektronische of mondelinge verklaring geschieden.[114] In de AVG is bepaald dat stilzwijgen, het gebruik van reeds aangekruiste vakjes of inactiviteit niet onder het geven van toestemming door de betrokkene valt. Verder is de toestemming van toepassing op alle verwerkingsactiviteiten die betrekking hebben op hetzelfde doel. Wanneer er meerdere verwerkingsdoelen aanwezig zijn, moet voor elk van deze doelen toestemming worden

[108] A.H. Pool, 'Beveiliging van persoonsgegevens', Arbeidsovereenkomst, art. 5 AVG, aant. 1.7.1.
[109] Art. 5 lid 1 sub f AVG.
[110] Art. 32 AVG.
[111] *Kamerstukken II* 2017/18, 34851, nr. 3, p. 33. Zie ook: art. 6 lid 1 AVG.
[112] De Vries & Meijer, *Gst.* 2017/132.
[113] Art. 6 lid 1 onder a AVG jo. Art. 4 onder 11 AVG.
[114] Art. 7 lid 1 AVG. Zie ook: Verordening (EU) 2016/679 (overweging 32). Zie ook: HvJ EU 1 oktober 2019, ECLI:EU:C:2019:801 (*Planet49*).

gevraagd aan een betrokkene. In het geval een elektronisch verzoek om toestemming wordt gedaan, moet dit duidelijk en beknopt zijn, zodat het voor de betrokkene niet als onnodig storend wordt ervaren bij het gebruik van de betreffende dienst.[115]

Op grond van de volgende rechtsgrondslag moet de verwerking noodzakelijk zijn om te voldoen aan een wettelijke verplichting die rust op degene die verantwoordelijk is voor de verwerking van persoonsgegevens.[116] Deze wettelijke verplichting moet een grondslag hebben in het Europese of nationale recht.[117] Daarnaast dient de wettelijke verplichting volgens de rechtspraak van het Europees Hof van Justitie en het EHRM voldoende duidelijk en nauwkeurig te zijn. Tevens moet de toepassing van de wettelijke verplichting voorspelbaar zijn.[118]

De laatste rechtsgrondslag betreft de verwerking van persoonsgegevens die noodzakelijk is voor de vervulling van een taak van algemeen belang of een publieke taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen.[119] Het is aan de wetgever overgelaten om de rechtsgrond voor gegevensverwerking door overheidsinstanties te bepalen. De publieke taak van de overheidsinstantie hoeft niet in een wet in formele zin te zijn geregeld. Het is voldoende dat de hoofdlijnen kenbaar zijn uit de sectorspecifieke wetgeving die op de verwerkingsverantwoordelijke van toepassing is. Het doel van de verwerking van persoonsgegevens moet noodzakelijk zijn voor de vervulling van een publieke taak. De wetgeving kan nadere regels stellen aan de algemene voorwaarden voor rechtmatige gegevensverwerking. Te denken valt aan bijvoorbeeld doelbinding en de bewaringstermijn.[120]

3.2.3 De Uitvoeringswet Algemene Verordening Gegevensbescherming

De regels in het kader van de bescherming van persoonsgegevens worden grotendeels door de AVG geregeld. Toch verwijst de AVG op enkele punten naar nationaal recht en geeft lidstaten hierbij beleidsruimte om sommige privacyregels te preciseren. Op enkele punten heeft de AVG dan ook het karakter van een richtlijn. Zo beschrijft artikel 6 lid 3 AVG dat nationaal recht bepaalt wanneer er sprake is van een wettelijke rechtsgrond ten aanzien van de verwerking van

[115] Verordening (EU) 2016/679 (overweging 32).
[116] Art. 6 lid 1 onder c AVG. Zie ook: Verordening (EU) 2016/679 (overweging 40).
[117] Schermer, Hagenauw & Falot 2018, p. 38.
[118] Verordening (EU) 2016/679 (overweging 41).
[119] Art. 6 lid 1 onder e AVG.
[120] Verordening (EU) 2016/679 (overweging 47).

persoonsgegevens.[121] De nationale Uitvoeringswet AVG (UAVG) geeft uitvoering aan de beleidsruimte waarbij de privacyregels uit de AVG op enkele onderdelen nader worden uitgewerkt.[122] De nationale wetgever heeft ervoor gekozen om een beleidsneutrale invulling te geven aan de geboden beleidsruimte, waarbij continu wordt nagegaan in hoeverre het nationale recht kan worden gehandhaafd onder de verordening. In beginsel is ervoor gekozen om dicht bij het bestaande nationale recht te blijven.[123]

3.2.4 Algemene plaatselijke verordening (APV) en beleidsregels

De gemeenteraad stelt nadere regels op over onder andere de handhaving van de openbare orde en het privacy beleid. Deze regels worden opgenomen in de APV. Sommige bepalingen in de APV geven de burgemeester bevoegdheden om de openbare orde te handhaven.[124] Gemeentelijke bestuursorganen stellen ook beleidsregels omtrent de privacy op.[125] In deze beleidsregels wordt hetgeen dat in de AVG is vastgelegd nader uitgewerkt.[126] Zo heeft de gemeente Amsterdam bijvoorbeeld in de beleidsregels omtrent het online monitoren van burgers het volgende uitgangspunt geformuleerd: *"Iedereen in Amsterdam heeft het recht op respect voor zijn of haar privéleven. Het digitaal monitoren van burgers in de openbare ruimte komt steeds vaker voor. In Amsterdam is het uitgangspunt om onbespied in de openbare ruimte te kunnen zijn, de regel. Alleen in specifieke gevallen mag van dit uitgangspunt worden afgeweken, bijvoorbeeld wanneer de wet dit vereist of wanneer het college en/of de burgemeester hiermee heeft ingestemd."*[127] Wat betreft wifi-tracking is dit het uitgangspunt binnen de gemeente Amsterdam: "*Als er met (WiFi-)tracking of metingen signalen naar personen herleidbaar zijn zal de gemeente daarover proactief informeren dat er op dat moment gegevens worden verzameld en welke gegevens dit betreft."*[128]

---

[121] Hijmans, *NJB* 2018/356.
[122] *Kamerstukken II* 2017/18, 34939, nr. 3.
[123] Zwenne & Kranenborg, in: *T&C Privacy- en gegevensbeschermingsrecht*, commentaar op aanhef AVG, (online, bijgewerkt 1 oktober 2021).
[124] Art. 151b Gemw. Zie ook: Art. 2:1 lid 3 Algemene plaatselijke verordening gemeente Leiden 2020. Zie ook: Art. 2.3 Verordening van de gemeenteraad van de gemeente Amsterdam houdende regels omtrent gemeentelijke regelgeving op het gebied van openbare orde en veiligheid.
[125] Art. 4:84 Awb.
[126] Art. 1:3 lid 4 Awb.
[127] *Stedelijk kader verwerken persoonsgegevens door de gemeente Amsterdam* 2018, p. 5.
[128] *Stedelijk kader verwerken persoonsgegevens door de gemeente Amsterdam* 2018, p. 5.

3.3 De bestuursorganen en hun (bestuurlijke) bevoegdheden

3.3.1 De Autoriteit Persoonsgegevens

In Nederland heeft de Autoriteit Persoonsgegevens (AP) als zelfstandig bestuursorgaan de overheidstaak toebedeeld gekregen om toezicht op de AVG en de UAVG te houden.[129] De AP opereert zelfstandig met eigen rechtspersoonlijkheid, maar de minister van Justitie en Veiligheid heeft wel in zeker mate zeggenschap over de AP.[130] Andere taken van de AP zijn bijvoorbeeld voorlichting geven aan burgers en verwerkingsverantwoordelijken.[131] Ook kan de AP bestuurlijke boetes opleggen aan organisaties of instanties die de bepalingen uit de AVG of UAVG overtreden.[132] Op grond van bijzondere wetgeving, zoals bijvoorbeeld de Wet politiegegevens of de Wet justitiële gegevens kan de AP andere taken in het kader van de bescherming van persoonsgegevens uitoefenen. De AP is uiteraard pas bevoegd indien de AVG van toepassing is. Dit is afhankelijk van het materiele en territoriale toepassingsgebied.[133]

3.3.2 De Functionaris Gegevensbescherming

Overheidsinstanties zoals bijvoorbeeld gemeenten, zijn wettelijk verplicht om een Functionaris voor de Gegevensbescherming (FG) aan te stellen.[134] De FG is een onafhankelijke en deskundige privacyfunctionaris die binnen een instantie of organisatie verantwoordelijk is voor het opstellen en uitvoeren van het privacy-beleid.[135] Daarnaast houdt de FG toezicht op de toepassing en naleving van het beleid en adviseert hij/zij onder andere over de risico's van de bestaande wijze van verwerking van persoonsgegevens.[136]

3.3.3 De gemeenteraad

De taken van de gemeenteraad bestaan onder andere uit het vaststellen van gemeentelijk beleid in hoofdlijnen en het controleren van het college van burgemeester en wethouders.[137] Volgens de Grondwet wordt de wetgever geacht het gemeentebestuur *"zo in te richten dat de raad materieel invulling kan geven aan de centrale positie die hem door de grondwetgever in het*

[129] Art. 6 UAVG jo. Art. 14 UAVG. Zie ook: 'Organisatie', autoriteitpersoonsgegevens.nl. Zie ook: Besluit van de Autoriteit Persoonsgegevens van 23 april 2019 (*Stcrt*. 2019, 22146).
[130] Art. 1 jo. Art. 3 Kaderwet zelfstandige bestuursorganen.
[131] Art. 57 lid 1 AVG.
[132] Art 17 jo. Art. 18 UAVG. Zie ook: *Stcrt*. 2019, 14586.
[133] Kranenborg & Verhey 2018.
[134] Artikel 37 lid 1 AVG.
[135] Artikel 36 Polw.
[136] Artikel 35 lid 2 AVG.
[137] 'Wat doet de gemeenteraad', raadsleden.nl.

lokale bestuursmodel is toebedacht".[138] In artikel 127 Gw. jo. artikel 147 lid 1 Gemw. is bepaald dat de gemeenteraad gemeentelijke verordeningen opstelt waar de inwoners van die gemeente zich aan dienen te houden. Te denken valt aan het opstellen van de APV, waarin het handhavings- en veiligheidsbeleid met betrekking tot de openbare orde is bepaald. Of een specifieke gemeentelijke privacy-verordening, waarin staat beschreven hoe de gemeente in kwestie omgaat met de persoonsgegevens van burgers en hoe de gemeente ervoor zorgt dat de privacyregels worden nageleefd. De gemeenteraadsleden dienen bij het opstellen van dergelijke verordeningen te controleren in hoeverre de voorgestelde prioriteiten overeenkomen met wat er speelt in de samenleving.[139] In de meeste gevallen worden de voorstellen voor verordeningen door het college van burgemeester en wethouders voorbereid.[140] Artikel 147 lid 1 jo. 156 lid 1 Gemw. bepaalt daarnaast dat de verordenende bevoegdheid ook aan het college van burgemeester en wethouders kan worden toegekend. Via deze weg kan de burgemeester bijvoorbeeld noodverordeningen vaststellen. Het uitgangspunt is nog steeds dat de gemeenteraad verordeningen vaststelt, dus alleen de wetgever of de gemeenteraad kan de bevoegdheid aan het college of de burgemeester overdragen door middel van delegatie.[141] De gemeenteraad controleert ook of het college plannen naar behoren uitvoert.

3.3.4 Het college van burgemeester en wethouders

Het college van burgemeester en wethouders is onderdeel van het gemeentelijke bestuur.[142] De burgemeester en de wethouders vormen tezamen het college. De burgemeester is naast lid van het college, ook de voorzitter.[143] Het college oefent zelfstandig bestuurlijke bevoegdheden uit, die gecontroleerd kunnen worden door de gemeenteraad.[144] De bestuursbevoegdheid wordt uitgeoefend in autonomie en medebewind. De gemeenteraad kan op grond van artikel 156 lid 1 jo. lid 3 Gemw. door middel van delegatie de verordenende bevoegdheden overdragen aan het college.[145] Het college kan via deze weg dus ook regels opstellen op het gebied van privacy. Ambtenaren van de gemeente ondersteunen het college bij het uitvoeren van de werkzaamheden.

---

[138] *Kamerstukken II* 2000/01 27751 nr. 3, p. 6.
[139] 'Gemeentelijke toezichthouders en handhaving', raadsledenenveiligheid.nl.
[140] Art. 160 lid 1 onder b Gemw. Zie ook: Broeksteeg 2021, p. 104.
[141] Art. 176 Gemw. Zie ook: Broeksteeg 2021, p. 103.
[142] Art. 125 lid 2 Gw jo. Art. 6 Gemw.
[143] Art. 9 Gemw. jo. art. 34 Gemw.
[144] Broeksteeg 2021, p. 149.
[145] Broeksteeg 2021, p. 156.

3.3.5 De burgemeester

Artikel 172 Gemw. geeft een algemene wettelijke grondslag voor de taak van de burgermeester betreffende de feitelijke handhaving van de openbare orde. Daarnaast is de burgemeester bevoegd om overtredingen van wettelijke bepalingen in het kader van de openbare orde te beletten of te beëindigen. Dit wordt gedaan door de politie, die onder het gezag van de burgemeester staat. Tevens mag de burgemeester bij een verstoring van de openbare orde of een ernstige vrees hiervoor, bevelen geven die nodig zijn ter handhaving van de openbare orde.[146] Zo hoort het voorkomen van bepaalde ongewenste online gedragingen die potentieel kunnen leiden tot het verstoren van de fysieke, publieke ruimte, bij het handhaven van de openbare orde door de burgemeester. Hierbij speelt wel het risico dat er een onrechtmatige inbreuk kan worden gemaakt op de privacy-rechten van deze burgers.[147]

Het is wellicht relevant om eerst stil te staan bij het begrip 'openbare orde'. Uit onderzoek en naar aanleiding van diverse recente gebeurtenissen is gebleken dat online aangejaagde ordeverstoringen de afgelopen jaren sterk zijn toegenomen.[148] Denk bijvoorbeeld aan de ongeregeldheden bij Project X in Haren na een openbare uitnodiging op Facebook in 2012.[149] Of de online oproepen om te protesteren tegen het coronabeleid in Rotterdam, wat vervolgens uitmondde in heftige rellen.[150] De online en offlinewereld lopen steeds meer in elkaar over en de verwachting is dat deze twee domeinen de komende jaren nog meer zullen vervagen.[151] Op basis van de bestaande openbare-ordebevoegdheden is het voor burgemeesters niet vanzelfsprekend om online op te treden tegen acties die de offline openbare orde dreigen te verstoren.[152]

In de literatuur bestaan verschillende opvattingen over het openbare orde-begrip. Volgens de wetgever vormen strafbare gedragingen in de meeste gevallen een evident onderdeel van het begrip 'openbare orde'.[153] Echter, de Nederlandse regering stelt dat het openbare orde-begrip

[146] De Jong, in: *T&C GPW*, commentaar op art. 172 Gemw (online, bijgewerkt 1 juli 2017).
[147] Bantema e.a. 2018, p. 58.
[148] A. de Vries & W. Bantema, 'De lokale driehoek moet ook online weten wat er speelt', ccv-secondant.nl, 29 maart 2021. Zie ook: Bantema e.a. 2018. Zie ook: Bantema, Westers & Munneke 2020, p. 9.
[149] Wieringa, *VAR* 2015/11.
[150] 'Gemeenten lopen bij rellen achter feiten aan door besloten groepen', nos.nl 21 november 2021.
[151] A. de Vries & W. Bantema, 'De lokale driehoek moet ook online weten wat er speelt', ccv-secondant.nl, 29 maart 2021.
[152] Bantema, Westers & Munneke 2020, p. 9.
[153] *Kamerstukken II* 2013/14, 33882 nr. 6, p. 15.

niet enkel strafbare feiten behelst. Gedragingen die op zichzelf geen strafbare feiten zijn, kunnen onder omstandigheden worden aangemerkt als orde verstorende gedragingen.[154] De Nederlandse regering trekt het begrip openbare orde uit de Gemeentewet gelijk met die in de Politiewet en verordeningen, zoals de destijds geldende APV Amsterdam 2008.[155] Het begrip openbare orde ziet toe op de onmiddellijke handhaving van de openbare orde zoals omschreven in artikel 5:23 Awb.[156] Het handhaven van de openbare orde kan worden opgedeeld in twee componenten. In de eerste plaats betreft het de dagelijkse handhaving van de openbare orde door de politie. De politie treedt in dit geval feitelijk op onder het gezag van de burgemeester.[157] In de tweede plaats past de burgemeester ordemaatregelen toe om de feitelijke handhaving door de politie, indien dit noodzakelijk wordt geacht, te ondersteunen en/of te faciliteren. Om de ordemaatregelen toe te passen zijn aan de burgemeester enkele bevelsbevoegdheden toegekend in de artikelen 172, 174 en 175 Gemw. Ook heeft de burgemeester een aanwijzingsbevoegdheid in artikel 174b en een noodverordeningsbevoegdheid in artikel 176 Gemw.[158]

3.3.5.1 Beperkingen

De openbare orde wordt verstoord als een rechtsregel wordt geschonden door onrechtmatig gedrag. Dit betekent niet dat de burgemeester bij iedere onrechtmatige gedraging zijn bevoegdheid mag inzetten om in te grijpen. Er zijn drie beperkingen betreft de taak en de bevoegdheid van de burgemeester bij het handhaven van de openbare orde. De eerste bevoegdheidsbeperking ziet toe op de begrenzing van de bestuurlijke belangenafweging. Het moet gaan om een onrechtmatige gedraging die hinder of gevaar oplevert voor goed of lijf. Een tweede beperking houdt in dat de burgemeester slechts mag ingrijpen bij onrechtmatige gedragingen tussen burgers onderling, wanneer hiermee niet uitdrukkelijk een gemeentehuishoudelijk belang is gemoeid. Ten derde vloeit de bevoegdheid van de burgemeester voort uit de grondwettelijke beperkingssystematiek. De ordemaatregelen die de burgemeester neemt op grond van de gemeentewet is ter ondersteuning van handhaving van de openbare orde door de politie.[159]

---

[154] *Kamerstukken I* 2009/10, 31467 E, p. 5-6. Zie ook: Brouwer, *NJB* 2016/1561.
[155] Brouwer, *NJB* 2016/1561. Zie ook: *Kamerstukken II* 1989/90, 19403 nr. 16. Zie ook: HR 30 januari 2007, ECLI:NL:HR:2007:AZ2104, r.o. 3.4.1. Zie ook: ABRvS 12 november 2014, ECLI:NL:RVS:2014:4117 (*Sinterklaasintocht*).
[156] Brouwer & Wierenga 2014, p. 163-191.
[157] Art. 11 Polw. 2012. Zie ook: Brouwer, *NJB* 2016/1561.
[158] Brouwer, *NJB* 2016/1561. Zie ook: De Greef, *NTB* 2021/247.
[159] Brouwer, *NJB* 2016/1561.

3.4 Tussenconclusie

De bescherming van de persoonlijke levenssfeer is onder andere geregeld in artikel 8 EVRM. Inmenging door de overheid is slechts onder drie limitatieve beperkingsvoorwaarden toegestaan: bij de wet voorzien, legitiem doel en noodzakelijk in een democratische samenleving. Wanneer een bepaalde situatie specifiek betrekking heeft op de bescherming van persoonsgegevens, zijn naast het EVRM, de AVG en de UAVG van toepassing. In de APV worden wettelijke regels beschreven over onder andere de handhaving van de openbare orde. Deze regels zijn van toepassing binnen de desbetreffende gemeente. De regels uit de AVG worden in beleidsregels nader uitgewerkt.

De AP is in Nederland het bestuursorgaan dat toezicht uitoefent op de naleving van de AVG en de UAVG en kan indien nodig bestuurlijke boetes opleggen. Elke gemeente is wettelijk verplicht om een FG te benoemen die onder andere het privacy beleid opstelt, uitvoert en toeziet op de naleving hiervan. De gemeenteraad is het hoogste bestuursorgaan binnen een gemeente en beschikt over een verordenende bevoegdheid die zij ook kan attribueren aan het college van burgemeester en wethouders. Op grond van de Gemeentewet is de burgemeester bevoegd om de openbare orde te handhaven. Deze bevoegdheid is echter niet onbegrensd. Zo mag de burgemeester alleen ingrijpen indien er sprake is van hinder en/of gevaar tussen burgers onderling en wanneer de ordemaatregelen ter ondersteuning zijn aan de handhaving van de openbare orde door de politie.

4. Gemeentelijk beleid inzake online monitoring en wifi-tracking en het EVRM

4.1 Inleiding

De verwerking van persoonsgegevens door gemeentelijke bestuursorganen dient te voldoen aan de voorwaarden uit artikel 8 EVRM, dat onder meer het recht op privacy beschermt. In dit hoofdstuk zal de volgende deelvraag worden beantwoord: *"In hoeverre is het gehanteerde gemeentelijke beleid ten aanzien van online monitoring en wifi-tracking in overeenstemming met het recht op privacy volgens artikel 8 EVRM?"* Er zullen twee analyses gemaakt worden van het in de praktijk gehanteerde gemeentelijke beleid van de gemeenten Amsterdam, Rotterdam en Den Haag omtrent online monitoring en wifi-tracking. In beide cases zal getoetst worden of gemeentelijke bestuursorganen met het gebruik van de digitale methoden voldoen aan de limitatieve voorwaarden uit artikel 8 EVRM.

4.2 Analyse beleid online monitoring

Tijdens het analyseren van het gemeentelijk beleid is gekeken naar de APV's van de gemeenten Amsterdam, Rotterdam en Den Haag, diverse beleidstukken op het gebied van privacy en de gemeentelijke websites. Daarnaast zijn deze analyses gebaseerd op wat er uit diverse eerdere onderzoeken naar voren is gekomen.[160]

<u>Bij de wet voorzien</u>

Volgens de eerste voorwaarde uit artikel 8 lid 2 EVRM moet elke inbreuk door een overheidsinstantie op het recht op respect voor privacy, in overeenstemming zijn met een nationale wettelijke bepaling.[161] Of er een wettelijke grondslag bestaat voor het gebruik van online monitoring door gemeentelijke bestuursorganen, hangt af van hoe ingrijpend de wijze van online monitoring is. Er is momenteel geen mogelijkheid om aan een bestuursrechtelijk kader te toetsen, omdat een op online monitoring toegespitst kader ontbreekt. Ik zal in deze analyse het strafrechtelijk kader toepassen. In het kader van de toenemende digitalisering van de criminaliteit heeft de Commissie modernisering opsporingsonderzoek in het digitale tijdperk (hierna: Commissie-Koops) in opdracht van de toenmalige Minister van Justitie en Veiligheid

[160] Bantema e.a. 2021. Zie ook: Bantema e.a. 2018. Zie ook: Choi, Van Eck & Hukshorn 2021. Zie ook: *Onderzoek Monitoring in de openbare ruimte* 2019.

[161] *Guide on Article 8 of the Covention – Right to respect for private and family life* 2021, p. 10.

onderzoek gedaan naar de wettelijke regeling van het opsporingsonderzoek, zoals beschreven in het conceptwetsvoorstel van Boek 2 van het Wetboek van Strafvordering.[162] Hoewel het onderzoek van de Commissie-Koops van toepassing is op het strafrecht, kunnen de aanknopingspunten in dit onderzoek ook gehanteerd worden voor online monitoring binnen de gemeente.[163] Om te bepalen hoe ingrijpend de wijze van online monitoring is, moet worden gekeken naar de omvang en het type gegevens, de aard van de bron, de wijze van zoeken en het gebruik van gegevens.[164] Op deze manier kan worden vastgesteld of het gaat om niet-stelselmatige online monitoring of stelselmatige online monitoring.

Indien het gaat om niet-stelselmatige online monitoring kan de wettelijke grondslag worden gevonden in artikel 172 lid 1 Gemw. De burgemeester is op grond van de Gemeentewet bevoegd om de openbare orde zowel in het fysieke als online domein te handhaven.[165] De wettelijke grondslag voor de burgemeester om de openbare orde en veiligheid te handhaven komt eveneens naar voren in de APV's van de gemeenten Amsterdam, Rotterdam en Den Haag.[166] In de APV's van de drie gemeenten zijn namelijk enkele bepalingen opgenomen waar de bevoegdheid van de burgemeester om de openbare orde en veiligheid te handhaven naar voren komt.

Voor stelmatige online monitoring bestaat echter nog geen wettelijke grondslag die adequate en effectieve bescherming biedt tegen misbruik van persoonsgegevens.[167] Wanneer online monitoring als stelselmatig is te kwalificeren, volgt de Centrale Raad van Beroep de strafrechtelijke jurisprudentie.[168] Online monitoring is stelselmatig wanneer er een min of meer compleet beeld van bepaalde aspecten van iemands privéleven kan worden verkregen. Hierbij wordt normaal gesproken getoetst aan een aantal klassieke factoren: de plaats, duur, intensiteit en de frequentie.[169] Echter, niet alle criteria zijn van toepassing op stelselmatige online monitoring in online openbare bronnen. Zo zijn de factoren frequentie en duur minder relevant,

[162] Oerlemans, *PMSv* 2018 p, 2.
[163] Bantema e.a. 2021, p. 106.
[164] Bantema e.a. 2021, p. 106. Zie ook: *Stcrt*. 2017, nr. 39081. Zie ook: *Stcrt*. 2017, nr. 73969.
[165] Bantema e.a. 2018, p. 23.
[166] Art. 2.6 APV Amsterdam 2008. Zie ook: Art. 2:26 APV Rotterdam 2012. Zie ook: Art. 2:79 APV Den Haag.
[167] Bantema e.a. 2021, p. 100.
[168] Bantema e.a. 2021, p. 97. Zie ook: CRvB 15 maart 2016, ECLI:NL:CRVB:2016:947
[169] Blom, in: *T&C Wetboek van Strafvordering*, commentaar op artikel 126g WvSv (online, bijgewerkt 1 januari 2022).

omdat het bij online monitoring niet gaat om momentopnamen. De factoren die wel aanknopingspunten bieden voor stelselmatige online monitoring zijn:

- de omvang en het type gegevens;
- de aard van de bron;
- de wijze van zoeken en het gebruik van gegevens;
- de eventuele impact op de betrokken burger.[170]

Om te beoordelen wat de omvang en het type gegevens zijn die worden verwerkt bij het gebruik van online monitoring door de gemeentelijke bestuursorganen van Amsterdam, Rotterdam en Den Haag, is in de eerste plaats gekeken naar de bepalingen in de betreffende APV's. In de APV's zijn geen bepalingen opgenomen waaruit blijkt wat de omvang en het type gegevens zijn die worden verwerkt bij het gebruik van online monitoring.[171] Daarnaast zijn diverse beleidsstukken van de drie gemeenten hierop nageslagen, maar nergens wordt deze informatie gedeeld.[172] Voorstelbaar is dat bij het raadplegen van de social media-accounts van burgers een grote hoeveelheid persoonlijke informatie beschikbaar is en wordt verwerkt door gemeentelijke bestuursorganen. Uit het onderzoek van Bantema is naar voren gekomen dat de gegevens die het vaakst worden gemonitord betrekking hebben op onrust rondom politieke besluiten, overlast door groepen en individuen, oproepen tot demonstraties en polarisatie tussen burgers. In deze gevallen gaat het voornamelijk om het verwerken van berichten die worden geplaatst op de eigen social media-accounts van burgers, maar ook de berichten in besloten groepen. Deze berichten zijn niet anoniem, omdat in de meeste gevallen een voor- en achternaam en profielfoto wordt weergegeven.[173] De gegevens kunnen dus in bijna alle gevallen worden herleid tot een individu.[174]

De tweede factor ziet toe op de aard van de bron. Er kan worden gesteld dat social media-accounts van burgers naar hun aard grotendeels openbaar zijn en voor publiek toegankelijk.

---

[170] Koops e.a. 2018, p. 163.
[171] APV Amsterdam 2008. Zie ook: APV Rotterdam 2012. Zie ook: APV Den Haag.
[172] *Onderzoek Monitoring in de openbare ruimte* 2019. Zie ook: *Stedelijk kader verwerken persoonsgegevens door de gemeente Amsterdam* 2018. Zie ook: Privacyverordening Rotterdam 2018. Zie ook: Privacybeleid Gemeente Rotterdam, 17 mei 2018. Zie ook: 'Schriftelijke vragen: online monitoring door de gemeente Den Haag', denhaag.raadsinformatie.nl 18 mei 2021. Zie ook: 'Online monitoring door de gemeente Den Haag', denhaag.raadsinformatie.nl 13 juli 2021.
[173] EHRM 2 september 2010, 35623/05 (*Uzun t. Duitsland*), r.o. 47; Zie ook: EHRM 28 januari 2003, ECLI:CE:ECHR:2003:0128JUD004464798 (*Peck t. Verenigd Koninkrijk*), r.o. 60-63.
[174] Bantema e.a. 2021, p. 46.

Daarnaast gaat het om gegevens die zelf door burgers zijn geplaatst. Wanneer met het gebruik van bepaalde digitale methoden meer informatie van gedragingen, opvattingen en gevoelens kunnen worden achterhaald, heeft dit invloed op hoe ingrijpend de inbreuk door gemeentelijke bestuursorganen is.[175] Volgens het EHRM worden geschreven berichten als minder ingrijpend gezien dan foto's van herkenbare personen.[176] Bij het gebruik van online monitoring door gemeentelijke bestuursorganen is het dus voorstelbaar dat veel persoonlijke gegevens worden verwerkt via de social media-accounts van burgers.[177]

De derde factor gaat over de wijze van zoeken naar informatie. Het college van B&W van de gemeente Den Haag heeft aangegeven dat media-analisten dagelijks de social media-accounts van openbare groepen in de gaten houden. Hiervoor wordt er gebruik gemaakt van professionele monitoring software die rekening houdt met de privacywetgeving. Tevens wordt er nooit gebruik gemaakt van nep- of privé accounts bij online monitoring. Daarnaast worden de social media-accounts ook handmatig in de gaten gehouden met het account 'Newsroom Den Haag'. De media-analisten gebruiken dit account om openbare groepen en pagina's op social media te raadplegen. Indien een besloten groep op social media wordt gevolgd, wordt altijd eerst toestemming gevraagd aan de beheerder en wordt nadrukkelijk kenbaar gemaakt dat het gaat om een gemeentelijk account.[178] Naar mijn idee is het lastig te controleren of en in hoeverre een ambtenaar zich houdt aan het gemeentelijke beleid wat betreft de wijze van zoeken naar informatie. Ik kan mij zo voorstellen dat het in de praktijk met enige regelmaat voorkomt dat een ambtenaar uit nieuwsgierigheid doorklikt naar het persoonlijke profiel van een bepaald persoon. Zodra online monitoring zich richt op individuen, kan er sprake zijn van een inbreuk op het privéleven.[179] Over de wijze van zoeken door gemeentelijke bestuursorganen binnen de gemeenten Amsterdam en Rotterdam is niks bekend.

Het gebruik van gegevens en de mogelijke impact op de betrokkene is lastig te toetsen. Er is nauwelijks bestuursrechtelijke jurisprudentie te vinden over de rechtmatigheid van openbare-bronnenonderzoek.[180] Volgens het EHRM is bepaald dat er eerder sprake is van een inbreuk op iemands privéleven, wanneer de persoonlijke informatie wordt bekeken en dossiers worden

[175] EHRM 2 september 2010, 35623/05 (*Uzun t. Duitsland*), r.o. 52.
[176] EHRM 7 februari 2012, 40660/08 en 60641/08 (*Von Hannover t. Duitsland (nr. 2)*), r.o. 96.
[177] Bantema e.a. 2021, p. 93.
[178] 'Online monitoring door de gemeente Den Haag', denhaag.raadsinformatie.nl 13 juli 2021, p. 2.
[179] EHRM 2 september 2010, 35623/05 (*Uzun t. Duitsland*), r.o. 46.
[180] Oerlemans & Schuurmans, *NJB* 2019/1132.

opgebouwd.[181] Mijns inziens kan het verwerken van persoonsgegevens middels online monitoring een grote impact hebben op betrokkenen. Zo hebben burgers weinig grip op wat er exact met hun persoonsgegevens gebeurt. Gemeentelijke ambtenaren kunnen de persoonsgegevens bijvoorbeeld gebruiken voor andere doeleinden. Of de gegevens komen door een menselijke fout in handen van een andere partij.[182]

Legitiem doel

Het is aan de gemeentelijke bestuursorganen om aan te tonen dat er sprake is van een legitiem doel bij het gebruik van online monitoring.[183] Uit het rapport van Bantema blijkt dat het voornaamste doel is om de openbare orde te handhaven door preventief te kunnen optreden bij ordeverstoringen.[184] In de APV van de gemeenten Amsterdam, Rotterdam en Den Haag staat echter niks opgenomen over online monitoring op social media en dus ook niet over het eventuele doel hiervan.[185] Daarnaast zijn de gemeentelijke websites geraadpleegd door de zoektermen 'online monitoring', 'social media', 'Facebook', 'handhaving', 'openbare orde', 'demonstraties' en 'rellen' in te vullen. Echter, er wordt ook op de gemeentelijke websites geen doel van online monitoring door gemeentelijke bestuursorganen beschreven.[186] Mijns inziens zijn openbare veiligheid, het voorkomen van wanordelijkheden en strafbare feiten en de bescherming van rechten en vrijheden van anderen, de meest legitieme doelen voor het gebruik van online monitoring.[187] Aangezien het EHRM in de meeste gevallen aanneemt dat er een legitiem doel bestaat, is de verwachting dat ook in het geval van online monitoring door gemeentelijke bestuursorganen kan worden gesproken van een legitiem doel in de zin van artikel 8 lid 2 EVRM.

Noodzakelijk in een democratische samenleving

De inmenging van het gemeentelijke bestuursorgaan mag alleen plaatsvinden als dit noodzakelijk is in een democratische samenleving. Gemeentelijke bestuursorganen moeten hierbij een redelijke belangenafweging maken. Het EHRM toetst in hoeverre gemeentelijke

[181] EHRM 17 juli 2003, 63737/00 (*Perry t. Verenigd Koninkrijk*), r.o. 41.
[182] J. Goedegebuure, 'Aantal datalekken bij de gemeente stijgt fors', *Het Parool* 5 februari 2020. Zie ook: A. Liukku, 'Nog nooit kreeg de gemeente Rotterdam zoveel klachten over datalekken als vorig jaar', *AD* 19 januari 2020. Zie ook: J. Roopram, 'Gegevens bijstandsgerechtigden belanden zomaar op straat!', *AD* 28 mei 2020.
[183] EHRM 23 februari 2016, 11138/10, r.o. 194 (*Mozer v. the Republic of Moldova and Russia*).
[184] Bantema e.a. 2021, p. 57.
[185] APV Amsterdam 2008. Zie ook: APV Rotterdam 2012. Zie ook: APV Den Haag.
[186] https://www.amsterdam.nl/. Zie ook: https://www.rotterdam.nl/. Zie ook: https://www.denhaag.nl/nl.htm.
[187] Art. 8 lid 2 EVRM. Zie ook: Bantema e.a. 2021, p. 101.

bestuursorganen binnen de 'margin of appreciation' in een dwingende maatschappelijke behoefte voorzien door op een proportionele wijze inbreuk te maken op het recht op respect voor privacy. Zo moet gekeken worden naar de Europese consensus, het belang van het recht op respect voor privacy en het doel van de inbreuk.[188] Aan het recht op respect van privacy wordt veel waarde gehecht door de verdragstaten bij het EVRM. Dit fundamentele mensenrecht is tevens verankerd in artikel 7 jo. 8 van het Handvest van de Grondrechten van de EU. Ook de het aannemen van de Europese AVG laat zien dat in ieder geval de EU-lidstaten willen beschikken over dezelfde privacywetgeving. Hieruit maak ik op dat Europese lidstaten een gezamenlijke visie hebben wat betreft het essentiële belang van het recht op respect voor privacy. Als we kijken naar Nederland en specifieker naar de gemeenten Amsterdam, Rotterdam en Den Haag kan worden gesteld dat alle drie de gemeenten 'privacy' een belangrijk onderwerp lijken te vinden. Zo staan er op de website van de gemeente Amsterdam diverse uitgangspunten in het kader van privacy beschreven.[189] Binnen de gemeente Rotterdam geldt de Privacyverordening 2018. De gemeente Den Haag heeft een beleidskader opgesteld inzake gegevensbescherming.[190]

Het doel van het gebruik van online monitoring door gemeentelijke bestuursorganen is het preventief kunnen optreden bij rellen en of demonstraties ter voorkoming van de verstoring van de openbare orde. Het is goed denkbaar dat gemeentelijke bestuursorganen er alles aan willen doen om de openbare orde zo goed mogelijk te handhaven. Het handhaven van de openbare orde behoort immers tot één van de taken van de burgemeester.[191] Als er binnen de gemeente rellen uitbreken die gepaard gaan met geweld en/of vernieling kan dit enorm veel schade met zich meebrengen.[192] Het is dus begrijpelijk dat gemeentelijke bestuursorganen dit willen voorkomen. In de jurisprudentie is bepaald dat het gebruik van openbaar toegankelijk internetgegevens slechts een geringe inbreuk op de privacy van burgers vormt en dus is toegestaan op grond van artikel 8 lid 2 EVRM.[193] Hieruit concludeer ik dat gegevens die openbaar toegankelijk zijn op social media-accounts van burgers een geringe inbreuk

[188] Van Toor, *SteR* 2017/32.
[189] 'Privacybeleid gemeente Amsterdam', amsterdam.nl.
[190] Beleidskader en reglement inzake Gegevensbescherming Gemeente Den Haag 2018.
[191] Art. 172 Gemw.
[192] T. Ketelaar, 'Waar ging het mis in Rotterdam?', *NRC* 21 november 2021. Zie ook: W. Al Ali, 'Celstraffen tot één jaar voor coronarelschoppers in Rotterdam', *NRC* 10 februari 2022. Zie ook: 'Negentien aanhoudingen bij rellen Den Haag, vijf agenten gewond', *Trouw* 21 november 2021.
[193] CRvB 5 februari 2018, ECLI:NL:CRVB:2018:269. Zie ook: CRvB 11 oktober 2018, ECLI:NL:CRVB:2018:3205.

opleveren. Als het gaat om het automatisch verwerken van persoonsgegevens, zoals online monitoring middels algoritmen, toetst het EHRM strenger.[194] Het EHRM houdt bij de beoordeling rekening met hoe ernstig de verstoring van de openbare orde is of hoe ernstig dit leek te zijn. Bij een acute dreiging van de openbare orde zal het EHRM in de beoordeling meer neigen naar het toestaan van de inbreuk. Tenzij er ook voor een minder ingrijpende wijze gekozen had kunnen worden.[195]

4.3 Analyse beleid wifi-tracking

Bij de wet voorzien

Voor een gerechtvaardigde inbreuk op het recht op respect voor privacy moet er een nationale wettelijke grondslag zijn voor het gebruik van wifi-tracking. De Awb, Grondwet, Gemeentewet en de APV's van de gemeenten Amsterdam, Rotterdam en Den Haag zijn erop nageslagen. Een nationale wettelijke grondslag die specifiek ziet op wifi-tracking ontbreekt.

Legitiem doel

Het doel waarvoor wifi-tracking door gemeentelijke bestuursorganen wordt gebruikt ziet voornamelijk toe op het verbeteren van het gemeentelijk beleid. Het volgen van bewegingen van individuen en/of bezoekersaantallen tellen om in een bepaald gebied na te gaan waar het bijvoorbeeld druk is en op welk moment het gunstiger is om ergens te parkeren, heeft een grote impact op de persoonlijke levenssfeer. Volgens de AP zijn er vrijwel geen redenen die het volgen van winkelend publiek of reizigers rechtmatig maakt.[196] Het gebruik van wifi-tracking door gemeenten lijkt dan ook geen legitiem doel te hebben in de zin van artikel 8 lid 2 EVRM. Mogelijk ziet het EHRM dit anders, nu er vanwege de ruime interpretatie in de meeste gevallen wordt aangenomen dat een overheidsinstantie een legitiem doel nastreeft.[197] Wellicht dat het EHRM het economisch welzijn als legitiem doel beschouwt voor het gebruik van wifi-tracking. Voor gemeentelijke bestuursorganen ligt de focus dus op het verbeteren van het gemeentelijk beleid. Je zou kunnen beargumenteren dat het verbeteren van gemeentelijk beleid ook het economisch welzijn bevordert. Een efficiënter gemeentelijk beleid kan mogelijk zorgen voor

[194] EHRM 13 september 2018, ECLI:CE:ECHR:2018:0913JUD005817013 (*Big Brother Watch t. Verenigd Koninkrijk).*
[195] Bantema e.a. 2021, p. 101-102.
[196] L. Verhagen, 'Gemeente Amsterdam stopt met omstreden wifitracking', *Volkskrant* 27 september 2019.
[197] Van Toor, *SteR* 2017/32.

een aantrekkelijkere leefbaarheid binnen de gemeente en past binnen de doelen die genoemd zijn in artikel 8 lid 2 EVRM.

Noodzakelijk in een democratische samenleving

In het geval van wifi-tracking staan twee belangen tegenover elkaar. Enerzijds gaat het om het belang van de gemeente waarbij door middel van het verwerken van persoonsgegevens informatie wordt verkregen om het gemeentelijk beleid te verbeteren. Anderzijds gaat het om het belang van het individu, waarbij de privacy-rechten zo goed mogelijk gewaarborgd dienen te worden. Een smartphone is onlosmakelijk met de eigenaar verbonden, omdat een individu het mobiele apparaat onder andere overal mee naar toeneemt. De locatie van de smartphone geeft zo een intieme kijk in het persoonlijke leven van een individu. Het unieke MAC-adres in combinatie met de locatie, datum en tijd zorgt ervoor dat de eigenaar te herleiden is. Tevens kunnen dergelijke verwerkte persoonsgegevens worden doorgegeven aan andere partijen die deze gegevens voor andere doeleinden gebruiken. Denk hierbij aan de politie en veiligheidsdiensten die persoonsgegevens gebruiken voor onderzoek naar bewijsmateriaal.[198]

In mijn optiek is het niet noodzakelijk om middels wifi-tracking het gemeentelijk beleid te verbeteren. Zo kunnen gemeentelijke bestuursorganen in bepaalde gebieden bijvoorbeeld ook infrarood sensoren plaatsen, om bezoekersaantallen te tellen. Infraroodsensoren vormen een minder ingrijpend middel in het licht van persoonsgegevens en kunnen daardoor een meer geschikte oplossing vormen voor gemeentelijke bestuursorganen. Het gebruik van wifi-tracking is dan ook niet noodzakelijk in een democratische samenleving.

4.4 Tussenconclusie

Voor niet-stelselmatige online monitoring kan een wettelijke grondslag worden gevonden in art. 172 Gemw. De burgemeester is op grond van deze bepaling bevoegd om de openbare orde te handhaven. Voor stelselmatige monitoring en wifi-tracking ontbreekt een nationale wettelijke grondslag. In de tweede plaats lijkt zowel voor online monitoring als wifi-tracking een legitiem doel in de zin van artikel 8 lid 2 EVRM te ontbreken, maar is het aannemelijk dat het EHRM wel een legitiem doel aanwezig acht. De laatste voorwaarde uit artikel 8 lid 2 EVRM ziet toe op de noodzakelijkheid in een democratische samenleving. Gegevens die openbaar toegankelijk zijn leveren een geringe inbreuk op. Bij het verwerken van persoonsgegevens door

[198] 'Normuitleg grondslag 'gerechtvaardigd belang', autoriteitpersoonsgegevens.nl p. 3.

middel van algoritmen, wordt strenger getoetst en is er sneller sprake van een schending. Bij wifi-tracking is er geen sprake van een dringende maatschappelijke behoefte om persoonsgegevens te verwerken. Er bestaat namelijk de mogelijkheid om voor een minder ingrijpend middel te kiezen. Het gebruik van niet-stelselmatige online monitoring door gemeentelijke bestuursorganen kan wellicht als gerechtvaardigde inbreuk worden gezien wanneer slechts de openbaar toegankelijke gegevens worden verwerkt voor het legitieme doel. Stelselmatige online monitoring en wifi-tracking kunnen op grond van artikel 8 lid 2 EVRM een ongerechtvaardigde inbreuk leveren op de privacy van burgers, omdat in beide cases in principe de wettelijke grondslag ontbreekt.

5. Gemeentelijk beleid inzake online monitoring en wifi-tracking en de AVG

5.1 Inleiding

Gemeentelijke bestuursorganen moeten ervoor zorgen dat zowel de fysieke als digitale openbare ruimte veilig en toegankelijk zijn. Momenteel zijn veel gemeenten nog aan het zoeken hoe zij dit op de beste manier kunnen doen en wat hun rol is bij het verzamelen, gebruiken en delen van data.[199] In dit hoofdstuk komt de volgende deelvraag aan bod: *"In hoeverre is het gehanteerde gemeentelijke beleid ten aanzien van online monitoring en wifi-tracking in overeenstemming met de regels uit de AVG?".* Er worden analyses gemaakt van het in de praktijk gehanteerde gemeentelijke beleid omtrent online monitoring en wifi-tracking. In beide cases zal getoetst worden of gemeentelijke bestuursorganen van de gemeenten Amsterdam, Rotterdam en Den Haag met het gebruik van de digitale methoden voldoen aan de beginselen en grondslagen uit de AVG.

5.2 Analyse beleid online monitoring

Middels een analyse wordt gekeken of de gemeenten Amsterdam, Rotterdam en Den Haag momenteel voldoen aan de beginselen en wettelijke rechtsgrondslagen uit artikel 5 en 6 AVG voor een rechtmatige verwerking van persoonsgegevens.[200] Daarnaast is deze analyse onder andere gebaseerd op wat er uit diverse eerdere onderzoeken is gekomen.[201] Tevens is in deze analyse gekeken naar de APV's en beleidstukken op het gebied van privacy en persoonsgegevensbescherming van de gemeenten Amsterdam, Rotterdam en Den Haag.

<u>Algemene beginselen online monitoring</u>

Het eerste beginsel betreft de rechtmatigheid, behoorlijkheid en transparantie.[202] Voor een rechtmatige verwerking van persoonsgegevens moet er een deugdelijke grondslag zijn. Deze grondslagen staan beschreven in artikel 6 lid 1 AVG. De grondslagen die van toepassing kunnen zijn op online monitoring zullen later in deze analyse nader worden uitgewerkt. De verwerking van persoonsgegevens door middel van online monitoring moet daarnaast ook op behoorlijke

[199] 'Principes voor de digitale samenleving', vng.nl.
[200] 'Inwoners per gemeente', cbs.nl. Zie ook: Verordening (EU) 2016/679 (overweging 15).
[201] Bantema e.a. 2021. Zie ook: Bantema e.a. 2018. Zie ook: Choi, Van Eck & Hukshorn 2021. Zie ook: *Onderzoek Monitoring in de openbare ruimte* 2019.
[202] Art. 5 lid 1 sub a AVG.

en transparante wijze geschieden. Om na te gaan of de gemeentelijke bestuursorganen van de gemeenten Amsterdam, Rotterdam en Den Haag transparant zijn over het gebruik van online monitoring, zijn in de eerste plaats de APV's en de gemeentelijke websites geraadpleegd. Opvallend is dat er in de APV's en op de websites van de drie gemeenten niks concreets staat vermeld over het gebruik van online monitoring door de gemeentelijke bestuursorganen.[203] De gemeente Amsterdam beschrijft wel enkele uitgangspunten voor een zorgvuldige verwerking van persoonsgegevens. Zo wordt er onder andere aangegeven dat de gemeente Amsterdam met inachtneming van de wet, via verschillende kanalen informatie verstrekt en voorlichting geeft, zodat iedere Amsterdammer op de hoogte kan worden gesteld van de persoonlijke informatie waarover de gemeente Amsterdam beschikt.[204] Echter, er wordt niet nader gespecificeerd om welke persoonlijke informatie het gaat en via welke kanalen de informatie en voorlichting wordt gedeeld met de burgers. Gemeenteraadslid Judith Klokkenburg heeft naar aanleiding van het rapport van Bantema op 18 mei 2021 schriftelijke vragen gesteld aan de voorzitter van de gemeenteraad van Rotterdam betreft het gebruik van online monitoring binnen de gemeente Rotterdam. Zo stelde Klokkenburg onder andere de vraag wat het gemeentelijk beleid is op het gebied van online monitoring voor onderzoek en handhaving en op welke wijze dit beleid wordt gehandhaafd.[205] Het college van burgemeester en wethouders van de gemeente Rotterdam reageerde op de vragen van Klokkenburg door te stellen dat er voor de medewerkers van de afdeling Handhaving & Fraude een protocol is voor het raadplegen van social media-accounts van burgers. Dit protocol is nergens voor publiek te raadplegen en er kan dus ook niet worden nagegaan wat er exact in het protocol is vermeld. Wel is tijdens het beantwoorden van de schriftelijke vragen naar voren gekomen dat ambtenaren slechts openbare profielen en bronnen raadplegen.[206] Van de gemeenten Amsterdam en Rotterdam zijn geen gegevens te vinden over het gemeentelijk beleid omtrent online monitoring. Geconcludeerd kan worden dat de gemeenten Amsterdam, Rotterdam en Den Haag bij het gebruik van online monitoring niet transparant zijn over deze werkwijze.

Volgens het beginsel van doelbinding dienen doelen voorafgaand aan de verwerking van de persoonsgegevens afgebakend en nadrukkelijk vastgelegd te zijn.[207] Doordat burgers überhaupt

[203] APV Amsterdam 2008. Zie ook: APV Rotterdam 2012. Zie ook: APV Den Haag.
[204] *Stedelijk kader verwerken persoonsgegevens door de gemeente Amsterdam* 2018, p. 5.
[205] 'Schriftelijke vragen: online monitoring door de gemeente Den Haag', denhaag.raadsinformatie.nl 18 mei 2021.
[206] 'Online monitoring door de gemeente Den Haag', denhaag.raadsinformatie.nl 13 juli 2021.
[207] Art. 5 lid 1 sub b AVG.

niet weten wanneer gebruik wordt gemaakt van online monitoring, omdat door de gemeenten Amsterdam, Rotterdam en Den Haag niet gecommuniceerd wordt, is het voor hen ook niet duidelijk ten behoeve van welke doelen dit gedaan wordt. In het 'Stedelijk kader verwerken persoonsgegevens door de gemeente Amsterdam', is als een van de uitgangspunten opgenomen dat burgers onbespied en anoniem in de openbare ruimte moeten kunnen bewegen. Van dit uitgangspunt mag alleen in specifieke gevallen worden afgeweken wanneer dit in de wet is opgenomen of indien het college en/of de burgemeester hiermee heeft ingestemd.[208]

Het derde beginsel gaat over de minimale gegevensverwerking.[209] De gemeenten Amsterdam, Rotterdam en Den Haag streven naar een minimale gegevensverwerking.[210] Openbare bronnen zoals social media-accounts bevatten meestal veel informatie over het privéleven van burgers.[211] Denk hierbij aan privéfoto's, maar ook informatie over het verleden van iemand. Al deze gegevens kunnen worden verwerkt door gemeentelijke ambtenaren, indien zij in openbare bronnen monitoren. Onduidelijk is of de gemeentelijke bestuursorganen van de gemeenten Amsterdam, Rotterdam en Den Haag daadwerkelijk alle beschikbare informatie verwerken, maar het is in ieder geval mogelijk om meer persoonsgegevens te verzamelen dan nodig is voor het te verwezenlijken doel.

Het beginsel van juistheid houdt in dat gemeentelijke bestuursorganen bij de verwerking van persoonsgegevens, alle nodige maatregelen dienen te nemen om te zorgen dat deze gegevens up-to-date zijn of gerectificeerd worden.[212] Gegevens op social media hoeven in de eerste plaats niet altijd juist te zijn. Zo maken sommige burgers gebruik van andere namen of plaatsen zij nepprofielfoto's.[213] Daarnaast vindt het gebruik van online monitoring plaats zonder medeweten van de burger. Gemeentelijke bestuursorganen zullen in dergelijke gevallen dan ook geen contact met een burger opnemen om te vragen of zijn/haar gegevens juist zijn. Het is dus lastig na te gaan voor gemeentelijke ambtenaren of de persoonsgegevens die zij verwerken door middel van online monitoring juist zijn.

---

[208] *Stedelijk kader verwerken persoonsgegevens door de gemeente Amsterdam* 2018, p. 5.
[209] Art. 5 lid 1 sub c AVG.
[210] *Stedelijk kader verwerken persoonsgegevens door de gemeente Amsterdam* 2018, p. 5. Zie ook: *Privacybeleid Gemeente Rotterdam* 2018, p. 18. Zie ook: *Beleidskader en reglement inzake Gegevensbescherming Gemeente Den Haag* 2018, p. 5. Zie ook: 'Bewaartermijn', denhaag.nl.
[211] P. Kulche, 'Privacytest sociale netwerken', consumentenbond.nl 26 oktober 2021. Zie ook: 'Persoonsgegevens op internet', autoriteitpersoonsgegevens.nl.
[212] Art. 5 lid 1 sub d AVG.
[213] Schermer, Hagenauw & Falot 2018, p. 22.

Voor een rechtmatige verwerking van persoonsgegevens geldt een opslagbeperking.[214] De gemeenten Amsterdam, Rotterdam en Den Haag geven aan persoonsgegevens niet langer op te slaan dan noodzakelijk.[215] De drie gemeenten zijn niet duidelijk over wat er exact met de verwerkte persoonsgegevens gebeurt en of het überhaupt noodzakelijk is om persoonsgegevens te verwerken om het doel te bereiken. Uit beleidsstukken blijkt niet dat er een belangenafweging wordt gemaakt, waarbij het doel van de verwerking in verhouding staat tot de inbreuk op de privacy.[216] Een concrete bewaringstermijn lijkt te ontbreken.

Het laatste beginsel betreft de integriteit en vertrouwelijkheid. Uit het onderzoek naar het gebruik van algoritmen en mensenrechten blijkt dat enkele gemeenten toegeven dat er morele risico's kunnen zitten aan de toepassing van algoritmen. Om deze risico's zoveel mogelijk te beperken wordt van gemeentelijke ambtenaren verwacht dat zij zich moreel en verantwoord gedragen. Tevens hebben gemeenten de verplichting om bij het verwerken van persoonsgegevens middels online monitoring passende technische en organisatorische beveiligingsmaatregelen te treffen.[217] Ook dienen ambtenaren een eed en belofte af te leggen en zich te houden aan de gedragscode van de betreffende gemeente.[218]

De gemeente Amsterdam stelt het vertrouwen van de burgers belangrijk te vinden. Burgers kunnen bij het Meldpunt Integriteit terecht indien zij vermoeden dat een gemeentelijke ambtenaar niet of onvoldoende integer handelt. Te denken valt bijvoorbeeld aan misbruik van de toegang tot informatie.[219] Ook de inwoners van de gemeente Den Haag hebben de mogelijkheid om via de gemeentelijke website of per telefoon integriteitschendingen van gemeentelijke ambtenaren te melden.[220] De gemeente Rotterdam neemt enkele maatregelen om ervoor te zorgen dat ambtenaren zich integer gedragen. Naast dat alle nieuwe gemeentelijke ambtenaren een eed of belofte afleggen krijgen zij een training waarbij lastige casussen worden

[214] Art. 5 lid 1 sub e AVG.
[215] *Stedelijk kader verwerken persoonsgegevens door de gemeente Amsterdam* 2018, p. 4. Zie ook: 'Hoelang bewaart de gemeente Amsterdam mijn gegevens?', amsterdam.nl. Zie ook: 'Verwerkingsregister gemeente Rotterdam', rotterdam.nl. Zie ook: 'Verklaring inzake Gegevensbescherming', denhaag.nl.
[216] *Datastrategie 2020-2022.*
[217] De Vries, in: *T&C Privacy- en gegevensbeschermingsrecht*, commentaar op art. 5 AVG, (online, bijgewerkt 1 oktober 2021). Zie ook: Art. 32 AVG.
[218] Choi, Van Eck & Hukshorn 2021, p. 23. Zie ook: *Gedragscode voor ambtenaren van de gemeente Amsterdam* 2017, p. 11. Zie ook: *Gedragscode voor de medewerkers van de gemeente Rotterdam* 2016. Zie ook: Art. 2 Besluit betreffende de eed en belofte van de gemeente Rotterdam.
[219] 'Integriteit', amsterdam.nl.
[220] 'Schending integriteit melden', denhaag.nl.

voorgelegd, waarmee zij mogelijk in het werkveld geconfronteerd worden. Burgers kunnen zich melden wanneer zij twijfels hebben over onder andere het handelen van gemeentelijke ambtenaren. Een melding kan (anoniem) via de website of telefonisch gemaakt worden.[221] Mijns inziens is het goed dat ambtenaren een eed en belofte afleggen, omdat daarmee zwart op wit staat dat zij instemmen zich moreel en verantwoord te gedragen bij de uitoefening van hun taak. Dit is des te belangrijker in gevallen waarin de privacy en de bescherming van persoonsgegevens van burgers een grote rol spelen. Desondanks vraag ik me af of dit voldoende is, om de bescherming van dergelijke mensenrechten te waarborgen. Uit onderzoek blijkt dat veel gemeenten niet aan de wettelijke verplichting voldoen om een FG aan te stellen die toezicht houdt op de uitvoering en naleving van de AVG en dus ook op online monitoring en wifi-tracking.[222] De gemeenten Amsterdam, Rotterdam en Den Haag hebben echter wel een FG in dienst.[223] Het aanstellen van een FG draagt in mijn optiek bij aan het waarborgen van de integriteit en vertrouwelijkheid binnen de gemeentelijke organisatie.

Rechtsgrondslagen online monitoring

Er is sprake van een rechtmatige verwerking van persoonsgegevens wanneer aan tenminste één van de zes grondslagen uit artikel 6, eerste lid, AVG is voldaan. De eerste rechtsgrondslag die van toepassing is bij het gebruik van online monitoring is: toestemming. Het is van belang dat burgers toestemming geven voor het gebruik van hun persoonsgegevens. In het geval van online monitoring door gemeentelijke ambtenaren wordt de toestemming niet nadrukkelijk verzocht en dus ook niet verkregen.[224] Online monitoring wordt namelijk naar zijn aard toegepast zonder medeweten van de burger.

Daarnaast moet er een wettelijke rechtsgrondslag zijn voor een rechtmatige verwerking van persoonsgegevens. De burgemeester is op grond van art. 172 Gemw. bevoegd om de openbare orde te handhaven. Deze wettelijke grondslag zou kunnen gelden voor niet-stelselmatige monitoring. Echter, zoals uit de analyse over online monitoring uit paragraaf 4.2 is gebleken bestaat er geen wettelijke grondslag voor stelselmatige online monitoring. De

[221] 'Integriteitsschending melden', rotterdam.nl.
[222] Bantema e.a. 2021, p. 68.
[223] Art. 3 Privacyverordening Rotterdam 2018. Zie ook: Art. 3.6.1. Beleidskader en reglement inzake Gegevensbescherming Den Haag. Zie ook: 'Functionaris gegevensbescherming gemeente Amsterdam', amsterdam.nl.
[224] Art. 6 lid 1 onder a AVG.

handhavingsbevoegdheid van de burgemeester is te algemeen om als rechtmatige grondslag te dienen bij stelselmatige online monitoring en de verwerking van persoonsgegevens.

Wanneer online monitoring niet als stelselmatig valt te kwalificeren kan in dit geval de vijfde grondslag van toepassing zijn. Deze rechtsgrondslag ziet toe op de verwerking van persoonsgegevens wanneer het noodzakelijk is voor de vervulling van een taak van algemeen belang of een taak in het kader van de uitoefening van het openbaar gezag. Het gaat hier om wettelijke taken.[225] Op grond van art. 172 Gemw. is de burgemeester belast met het handhaven van de openbare orde. Van online monitoring wordt gebruik gemaakt om preventief te kunnen optreden bij openbare ordeverstoringen zoals rellen of demonstraties die uit de hand lopen.

5.3 Analyse beleid wifitracking

Algemene beginselen wifi-tracking

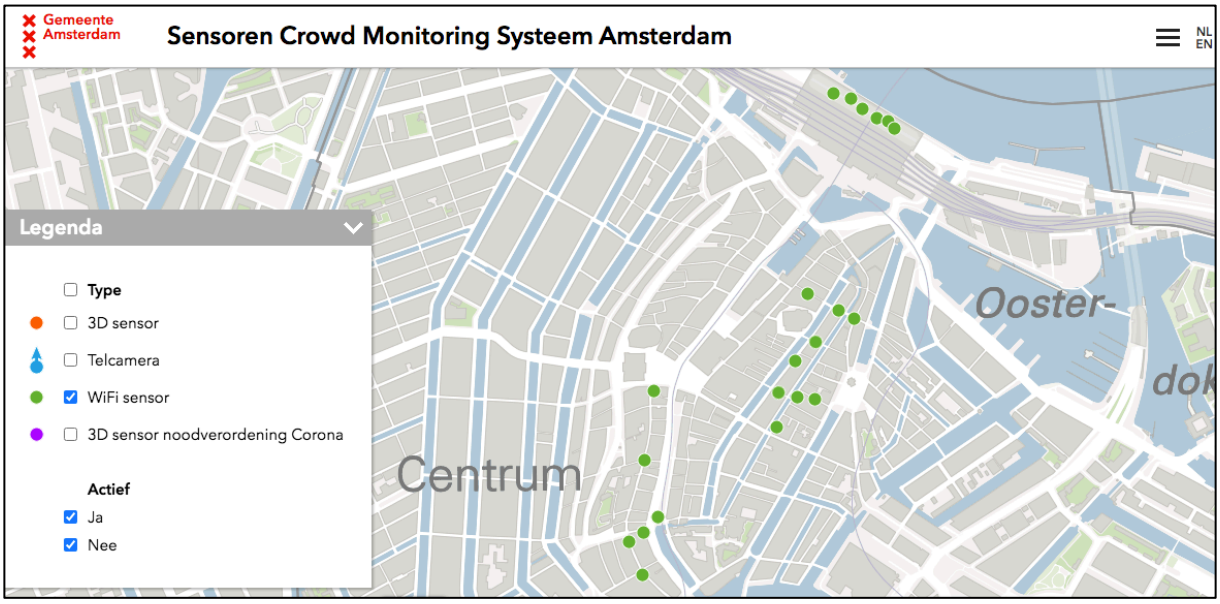
Of er sprake is van een rechtmatige verwerking van persoonsgegevens bij het gebruik van wifi-tracking zal verderop worden getoetst aan de grondslagen uit artikel 6 lid 1 AVG. Als we kijken naar de transparantie valt op dat bij het gebruik van wifi-tracking, sommige gemeenten in bepaalde gebieden stickers en/of borden plaatsen waarop staat vermeld dat er op die specifieke plek gebruik wordt gemaakt van wifi-tracking. Op afbeelding 1 is bijvoorbeeld te zien dat binnen de gemeente Amsterdam op verschillende plaatsen dergelijke borden en/of stickers zijn aan te treffen.

Afbeelding 1[226]

Wanneer deze borden zijn geplaatst, kan de burger er zelf voor kiezen om zijn wifi en/of bluetooth signaal uit te zetten. Het zal overigens vaak voorkomen dat onoplettende burgers dergelijke borden en/of stickers over het hoofd zien en dus niet op de hoogte zijn van het feit

[225] Art. 6 lid 1 sub e AVG. Zie ook: De Vries, in: *T&C Privacy- en gegevensbeschermingsrecht*, commentaar op art. 6 AVG, (online, bijgewerkt 1 oktober 2021).
[226] 'Zicht op sensoren openbare ruimte', amsterdam.nl.

dat hun persoonsgegevens middels wifi-tracking worden verwerkt. De gemeente Amsterdam geeft aan proactief te informeren wanneer middels wifi-tracking metingen plaatsvinden die herleidbaar zijn tot individuen.[227] Zo is op afbeelding 2 te zien dat de gemeente Amsterdam een online kaart heeft gepubliceerd, waarop staat aangegeven op welke plekken binnen de gemeente Amsterdam wifi-sensoren zijn geplaatst.[228] Mijns inziens gaat de gemeente Amsterdam de goede richting op om zo transparant mogelijk te zijn naar burgers toe wat betreft het gebruik van wifi-tracking. Desondanks is uit onderzoek gebleken dat de online kaarten onvolledige informatie weergeven. Zo zijn bijvoorbeeld tijdelijke sensoren niet zichtbaar op de kaarten. De informatie die naar de burger wordt verstrekt is om deze reden nog onvoldoende transparant.[229]



Afbeelding 2[230]

De gemeente Rotterdam en Den Haag beschikken niet over beleidsstukken of informatie op de gemeentelijke websites over het gebruik van wifi-tracking. Transparantie ontbreekt hier dus ook.

Volgens het beginsel van doelbinding moet er een specifiek doel zijn waarvoor de gemeente persoonsgegevens worden verwerkt middels wifi-tracking. Indien een gemeente stickers en/of borden heeft geplaatst met de melding van wifi-tracking, staat er in sommige gevallen bij voor

[227] *Stedelijk kader verwerken persoonsgegevens door de gemeente Amsterdam* 2018, p. 5.
[228] 'Sensoren Crowd Monitoring Systeem Amsterdam', maps.amsterdam.nl.
[229] *Onderzoek Monitoring in de openbare ruimte* 2019, p. 13.
[230] 'Sensoren Crowd Monitoring Systeem Amsterdam', maps.amsterdam.nl.

welk doel dit gedaan wordt: *"Voor het verbeteren van de kwaliteit van de binnenstad"*. Daarnaast staat er bijvoorbeeld in de Datastrategie 2020-2022 van de gemeente Den Haag het volgende over het gebruik van data om de parkeerdruk in Scheveningen te voorspellen: *"Belangrijkste doel is het beter kunnen informeren van strandbezoekers waar ze kunnen parkeren"*.[231] Op welke wijze de gemeente Den Haag dit exact gaat doen staat nergens beschreven. Het is voorstelbaar dat met het gebruik van deze methode een telling wordt gedaan om inzicht te krijgen in hoeveel personen in een bepaald gebied op een bepaald tijdstip zijn. Vervolgens kan er op basis van deze informatie worden geanticipeerd door de gemeentelijke bestuursorganen van de gemeente Den Haag om het beleid te verbeteren.

Het derde beginsel ziet toe op de minimale gegevensverwerking. Uit de analyse in paragraaf 5.2 is gebleken dat de gemeenten Amsterdam, Rotterdam en Den Haag streven naar een minimale gegevensverwerking.[232] Echter, bij het gebruik van wifi-tracking kan veel persoonlijke informatie worden achterhaald door middel van het koppelen van het unieke MAC-adres te koppelen aan bijvoorbeeld een locatie of datum. De APV's, gemeentelijke websites en diverse beleidstukken zijn erop nageslagen, maar het is niet duidelijk welke gegevens de gemeenten Amsterdam, Rotterdam en Den Haag precies gebruiken bij de verwerking van persoonsgegevens door middel van wifi-tracking.

Vervolgens moet worden gekeken of de bestuursorganen van de gemeenten Amsterdam, Rotterdam en Den Haag voldoen aan het beginsel van juistheid. Bij het gebruik van wifi-tracking wordt het MAC-adres automatisch verzameld wanneer de wifi is ingeschakeld op het mobiele apparaat. In mijn optiek mag een gemeentelijk bestuursorgaan uitgaan van de juistheid en betrouwbaarheid van dergelijke persoonsgegevens.

Net zoals in de analyse over online monitoring naar voren komt, dienen de gemeentelijke bestuursorganen van de gemeenten Amsterdam, Rotterdam en Den Haag persoonsgegevens niet langer op te slaan dan noodzakelijk voor het te verwezenlijken doel. Alle drie de gemeenten

[231] *Datastrategie 2020-2021*, p. 22.
[232] *Stedelijk kader verwerken persoonsgegevens door de gemeente Amsterdam* 2018, p. 5. Zie ook: *Privacybeleid Gemeente Rotterdam* 2018, p. 18. Zie ook: *Beleidskader en reglement inzake Gegevensbescherming Gemeente Den Haag 2018*, p. 5. Zie ook: 'Bewaartermijn', denhaag.nl.

geven aan zich hieraan te houden.[233] Er zijn echter in ieder geval in de gemeenten Amsterdam, Rotterdam en Den Haag nog geen concrete bewaringstermijnen vastgesteld voor de verwerkte persoonsgegevens middels wifi-tracking.[234]

Rechtsgrondslagen wifi-tracking

Ook bij het gebruik van wifi-tracking moet aan de rechtsgrondslag toestemming worden voldaan. Bij wifi-tracking wordt geen nadrukkelijke toestemming gevraagd aan de burger. Als de burger zijn wifi aan heeft staan, wordt het signaal automatisch opgevangen door de sensoren in de omgeving. In enkele gevallen hebben gemeenten in bepaalde gebieden stickers en/of borden geplaatst waarop staat vermeld dat er op die specifieke plek gebruik wordt gemaakt van wifi-tracking. Van uitdrukkelijke toestemming van de burger is dan ook geen sprake.

Vervolgens moet worden gekeken of er een wettelijke grondslag bestaat voor het gebruik van wifi-tracking. Een algemene taak zoals het handhaven van de openbare orde valt niet onder deze rechtsgrondslag.[235] Er bestaat ook geen wettelijke verplichting die het noodzakelijk maakt om wifi-tracking toe te passen.

De laatste rechtsgrondslag ziet toe op de verwerking van persoonsgegevens wanneer het noodzakelijk is voor de vervulling van een taak van algemeen belang of een taak in het kader van de uitoefening van het openbaar gezag. Gemeentelijke bestuursorganen zetten wifi-tracking in om op deze manier inzicht te krijgen in onder andere de loopstromen in een bepaald gebied. Op deze wijze proberen gemeenten voortijdig na te gaan hoe het bijvoorbeeld zit met de parkeerdrukte. De gemeente moet kunnen onderbouwen waarom het gebruik van wifi-tracking noodzakelijk is. Ik ben van mening dat de gemeente ook met andere methoden het aantal bezoekers kan tellen in een bepaald winkelgebied. Met deze methoden worden geen persoonsgegevens verzameld. Op deze manier kan het doel toch worden bereikt, zonder dat een onrechtmatige inbreuk wordt gemaakt op de privacy van burgers

[233] *Stedelijk kader verwerken persoonsgegevens door de gemeente Amsterdam* 2018, p. 4. Zie ook: 'Verwerkingsregister gemeente Rotterdam', rotterdam.nl. Zie ook: 'Verklaring inzake Gegevensbescherming', denhaag.nl.
[234] *Onderzoek Monitoring in de openbare ruimte* 2019, p. 26.
[235] 'Mag u persoonsgegevens verwerken?', autoriteitpersoonsgegevens.nl.

5.4 Tussenconclusie

Uit de analyses over online monitoring en wifi-tracking van de bestuursorganen van de gemeenten Amsterdam, Rotterdam en Den Haag kan worden geconcludeerd dat de drie gemeenten niet voldoen aan alle algemene beginselen uit artikel 5 AVG voor een rechtmatige verwerking van persoonsgegevens. Wat betreft de grondslagen voor een rechtmatige verwerking van persoonsgegevens kan zowel bij het gebruik van online monitoring als wifi-tracking worden gesteld dat aan de eerste rechtsgrondslag 'toestemming' niet wordt voldaan. Verder bestaat voor zowel (stelselmatige) online monitoring als wifi-tracking geen wettelijke verplichting. Daarnaast is het niet vastgesteld of online monitoring en wifi-tracking noodzakelijk zijn voor de vervulling van een taak van algemeen belang of een taak in het kader van de uitoefening van het openbaar gezag. Van een rechtmatige verwerking van persoonsgegevens bij online monitoring en wifi-tracking op grond van de AVG is dan ook geen sprake.

6. Conclusie

In dit onderzoek is antwoord gegeven op de centrale vraag: *"In hoeverre is het gebruik van digitale systemen door gemeentelijke bestuursorganen in het kader van handhaving en besluitvorming, in overeenstemming met de bescherming van persoonsgegevens volgens de AVG en het recht op privacy in artikel 8 EVRM?"*.

Uit diverse onderzoeken is gebleken dat gemeenten veelvuldig gebruik maken van de digitale systemen: online monitoring en wifi-tracking. Bij online monitoring raadplegen gemeentelijke ambtenaren handmatig of middels algoritmen de social media-accounts van burgers. Het doel hierachter is om preventief te kunnen optreden bij mogelijke rellen en/of demonstraties. Naast online monitoring maken gemeenten maken op grote schaal gebruik van wifi-tracking, waarbij aan de hand van het plaatsen van sensoren het wifi-signaal van mobiele apparaten van burgers wordt opgevangen. Het doel achter het gebruik van wifi-tracking is gelegen in het registreren van bewegingen en/of het tellen van bezoekersaantallen in een bepaald gebied, zodat deze verkregen gegevens vervolgens gebruikt worden om het gemeentelijke beleid aan te passen en te verbeteren. Bij het gebruik van beide digitale systemen worden grote hoeveelheden persoonsgegevens van burgers verwerkt.

Om te bepalen in hoeverre het gebruik van online monitoring en wifitracking door gemeentelijke bestuursorganen is toegestaan, is er gekeken naar het bestuursrechtelijk kader en de bescherming van privacy en persoonsgegevens binnen de kaders van de Europese Unie (met name de AVG) en het EVRM. Volgens artikel 8 EVRM is een inbreuk op de persoonlijke levenssfeer is slechts toegestaan als wordt voldaan aan drie limitatieve voorwaarden: bij de wet voorzien, legitiem doel en noodzakelijk in een democratische samenleving. Daarnaast staat de Europese AVG centraal, die specifiek toeziet op de bescherming van persoonsgegevens. Voor een rechtmatige verwerking van persoonsgegevens is gekeken naar de artikelen 5 en 6 AVG. Verder verwijst de AVG in bepaalde gevallen naar het nationale recht, waarbij lidstaten een zeker mate van beleidsruimte hebben op het gebied van sommige privacyregels. Deze nationale privacyregels worden beschreven in de UAVG. Tenslotte kan een gemeente nadere regels over het handhaven van de openbare orde en veiligheid opnemen in gemeentelijke APV's en beleidsregels. Het (bestuurs)procesrecht bepaalt welk orgaan waartoe bevoegd is. Zo is gekeken naar de bevoegdheden van de AP, de FG en de gemeentelijke bestuursorganen.

Uit de analyses in dit onderzoek is gebleken dat het gebruik van online monitoring en wifi-tracking door de bestuursorganen van de gemeenten Amsterdam, Rotterdam en Den Haag in sommige gevallen in strijd is met de voorwaarden uit artikel 8 lid 2 EVRM. Met name het ontbreken van een wettelijke grondslag vormt bij het gebruik van stelselmatige online monitoring en wifi-tracking een probleem. Slechts bij het gebruik van niet-stelselmatige online monitoring kan artikel 172 Gemw. een wettelijke grondslag bieden. Alhoewel de informatie uit dit onderzoek logischerwijs onvolledig is, is het goed denkbaar dat wanneer de gemeente in een gerechtelijke procedure is verwikkeld, een betere onderbouwing wordt gegeven en een wettelijke grondslag kan worden gevonden. Aangezien het EHRM in bijna alle gevallen aanneemt dat een overheidsinstantie een legitiem doel heeft, kan worden aangenomen dat ook in het geval voor online monitoring en wifi-tracking een legitiem doel aanwezig is. Daarnaast dient het gebruik van online monitoring en wifi-tracking noodzakelijk te zijn in een democratische samenleving. In het geval van niet-stelselmatige online monitoring waarbij slechts openbaar toegankelijke persoonsgegevens worden verwerkt, kan worden beargumenteerd dat dit een geringe inbreuk oplevert. Voor stelselmatige online monitoring en wifi-tracking is dit niet het geval.

Het gebruik van online monitoring en wifi-tracking is niet in overeenstemming met de regels voor een rechtmatige verwerking van persoonsgegevens in de zin van de AVG. De gemeenten Amsterdam, Rotterdam en Den Haag stellen burgers niet of onvoldoende op de hoogte van het gebruik van online monitoring en wifi-tracking. Burgers kunnen op deze manier dan ook nooit toestemming geven voor het verwerken van hun persoonsgegevens middels deze digitale systemen. Het is voor burgers ook niet duidelijk voor welke doelen gemeenten gebruik maken van online monitoring en wifi-tracking. Daarnaast kunnen gemeentelijke bestuursorganen middels online monitoring en wifi-tracking grote hoeveelheden persoonsgegevens verzamelen. Waarschijnlijk meer dan nodig is voor de te verwezenlijken doelen. De gemeenten Amsterdam, Rotterdam en Den Haag zijn niet duidelijk over hoe dergelijke persoonsgegevens bewaard worden en wat de concrete bewaringstermijn is. Op dit vlak schiet het gemeentelijke beleid tekort en wordt niet voldaan aan de grondslag voor integriteit en vertrouwelijkheid. Wat de integriteit en vertrouwelijkheid wel weer ten goede komt is dat de gemeenten Amsterdam, Rotterdam en Den Haag voldoen aan de wettelijke verplichting door het aanstellen van een FG.

Al met al, is het gemeentelijk beleid omtrent het gebruik van online monitoring en wifi-tracking bij de gemeente Amsterdam, Rotterdam en Den Haag momenteel niet (volledig) in

overeenstemming met de regels uit artikel 8 EVRM en de AVG. Hoewel het belang van de bescherming van persoonsgegevens en het waarborgen van mensenrechten bij vele gemeenten wel een onderwerp van gesprek is, ontbreekt een correct en eenduidig beleid.

Aanbevelingen

De gemeenten Amsterdam, Rotterdam en Den Haag dienen transparant te zijn over de werkwijze in het kader van online monitoring en wifi-tracking en dit te zorgvuldig te communiceren met burgers. Zo is het verstandig om op de gemeentelijke websites te vermelden dat er gebruik wordt gemaakt van online monitoring en wifi-tracking, ten behoeve van welk doel dit wordt gedaan en hoe de bescherming van persoonsgegevens wordt gewaarborgd. Vervolgonderzoek zou zich kunnen richten op het onderzoeken en uiteen te zetten hoe de gemeenten Amsterdam, Rotterdam en Den Haag hun beleid het beste kunnen aanpassen, zodat geen onrechtmatige inbreuk wordt gemaakt op de privacy-rechten van burgers.

Literatuurlijst

Al Ali, *NRC* 10 februari 2022

W. Al Ali, 'Celstraffen tot één jaar voor coronarelschoppers in Rotterdam', *NRC* 10 februari 2022.

Barkhuysen, *NJB* 2021/572

T. Barkhuysen, 'Handhaving van de AVG: de AP kan het niet alleen', *NJB* 2021/572.

Barkhuysen & Bos, *JBplus* 2011

T. Barkhuysen & A.W. Bos, 'De betekenis van het Handvest van de Grondrechten van de Europese Unie voor het bestuursrecht', *JBplus* 2011.

Bantema e.a. 2021

W. Bantema, S. Westers, M. Hoekstra, R. Herregodts & S.A.J. Munneke*, Black Box van gemeentelijke online monitoring,* Den Haag: Sdu Uitgevers 2021.

Bantema, Westers & Munneke 2020

W. Bantema, S. Westers, S.A.J. Munneke, *Niet bevoegd, wel verantwoordelijk? Handhavingsmogelijkheden bij online aangejaagde ordeverstoringen*, Den Haag: Boom juridisch 2020.

Bantema e.a. 2018

W. Bantema, S.M.A. Twickler, S.A.J. Munneke, M. Duchateau, W.Ph. Stol, *Burgemeesters in cyberspace*, Den Haag: Sdu Uitgevers 2018.

Van den Bos & Brenninkmeijer, *NJB* 2012/1216.

K. van den Bos & A.F.M Brenninkmeijer, 'Vertrouwen in wetgeving, de overheid en de rechtspraak', *NJB* 2012/1216.

Broeksteeg 2021

J.L.W. Broeksteeg, *Gemeenterecht* 2021, Deventer: Wolters Kluwer, p. 104-150.

Brouwer, *NJB* 2016/1561

J.G. Brouwer, 'Wat is openbare orde? Bevoegdheden van burgemeester niet onbegrensd', *NJB* 2016/1561.

Brouwer & Wierenga 2014, p. 163-191.

J.G. Brouwer & A.J. Wierenga, *'Toepassing van openbare-ordebevoegdheden in het systeem van het openbare-orderecht'*, in: E.R. Muller & J. de Vries, *Burgemeester: Positie, rol en functioneren van de burgemeester,* Deventer: Wolters Kluwer 2014.

Van Canneyt e.a., *Computerrecht* 2021/56

T. van Canneyt, A. Bertrand, S. Crouzet & L. Vanderdonckt, 'Data Protection: CJEU case law review – 1995-2020', *Computerrecht* 2021/56.

Van Canneyt, *Computerrecht* 2016/125

T. van Canneyt, 'Big brother in de winkel? – wifi-tracking en de verwerking van persoonsgegevens', *Computerrecht* 2016/125.

Çapkurt, *RMThemis* 2020/4

F. Çapkurt, 'Het bestuursrecht en gegevensbeschermingsrecht: de ontmoeting van twee rechtsgebieden in historisch perspectief', *RM Themis* 2020/4, p. 181.

Çapkurt, *NTB* 2019/11

F. Çapkurt, 'Bestuursrechtelijke uitdagingen bij de normering van de data-gedreven overheid', NTB 2019/11.

Choi, Van Eck & Hukshorn 2021

W. Choi, M van Eck & H. Hukshorn, *Hoe gemeenten besluiten over algoritmen & mensenrechten* 2021.

***Comparative study on blocking, filtering and take-down of illegal internet content* 2017.**

Comparative study on blocking, filtering and take-down of illegal internet content (Council of Europe), 2017.

Giakoumopoulos, Buttarelli & O'Flaherty 2018
C. Giakoumopoulos, G. Buttarelli & M. O'Flaherty, *Handbook on European data protection law*, Luxembourg: Publications Office of the European Union 2018

Goedegebuure, *Het Parool* 5 februari 2020
J. Goedegebuure, 'Aantal datalekken bij de gemeente stijgt fors', *Het Parool* 5 februari 2020.

De Greef, *NTB* 2021/247
R.J.M.H. de Greef, 'De paradox van democratische noodmaatregelen', *NTB* 2021/247.

Hijmans, *NJB* 2018/356
H. Hijmans, 'De AVG en de UAVG', *NJB* 2018/356.

De Jong, in: *T&C GPW*, commentaar op art. 172 Gemw
De Jong, in: *Tekst & Commentaar Gemeentewet Provinciewet, Handhaving openbare orde bij: Gemeentewet, Artikel 172 [Handhaving openbare orde]*, Deventer: Wolters Kluwer.

Ketelaar, *NRC* 21 november 2021
T. Ketelaar, 'Waar ging het mis in Rotterdam?', *NRC* 21 november 2021.

Van Kolfschooten, *NJB* 8 juli 2020
H. van Kolfschooten, 'Europese harmonisatie van privacy – óók in crisistijd', *NJB* 8 juli 2020.

Koops e.a. 2018
E.J. Koops, R.J. Verbeek, B.W. Schermer, M.J. Grapperhaus, A. Kuijer, D. Ven-Laheij & M. Viersma, *Commissie modernisering opsporingsonderzoek in het digitale tijdperk. Regulering van opsporingsbevoegdheden in een digitale omgeving* 2018.

Kranenborg, in: *T&C Privacy- en gegevensbeschermingsrecht*, art. 8 EVRM
H.R. Kranenborg, in: *Tekst & Commentaar Privacy- en gegevensbeschermingsrecht, Recht op eerbiediging van privé-, familie- en gezinsleven bij: Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, Artikel 8 Recht op eerbiediging van privé-, familie- en gezinsleven,* Deventer: Wolters Kluwer.

Kranenborg & Verhey 2018
H.R. Kranenborg & L.F.M. Verhey, *De AVG in Europees en Nederlands perspectief*, Mastermonografieën Staats- en bestuursrecht 2018/12.2.2.

Maree, *NRC* 18 mei 2021
K. Maree, 'Nederlandse gemeenten monitoren burgers anoniem op sociale media', *NRC* 18 mei 2021.

Liukki, *AD* 19 januari 2020
A. Liukku, 'Nog nooit kreeg de gemeente Rotterdam zoveel klachten over datalekken als vorig jaar', *AD* 19 januari 2020.

Oerlemans & Schuurmans, NJB 2019/1132
J.J. Oerlemans & Y.E. Schuurmans, 'Internetonderzoek door bestuursorganen', *NJB* 2019/1132.

Oerlemans, *PMSv* 2018
J.J. Oerlemans, 'Beschouwing rapport Commissie-Koops: strafvordering in het digitale tijdperk', *PMSv* 2018.

Oerlemans, *Strafblad* 2017/4
J.J. Oerlemans, 'De Wet computercriminaliteit III: meer handhaving op internet', *Strafblad* 2017/4.

Van Os, *TBR* 2017/140
V.H.M. van Os, 'The Emperor's New Clothes: Smart cities, smarter contracts & smartest decisions', *TBR* 2017/140.

Von Piekartz, *Volkskrant* 18 mei 2021
H. von Piekartz, 'Ollongren wil opheldering van gemeenten over heimelijk volgen burgers', *Volkskrant* 18 mei 2021.

Polak, Minderhoud & Daalder, *Computerrecht* 2020/184
J.E.M. Polak, E.A. Minderhoud en E.J. Daalder, *Computerrecht* 2020/184.

Raas, Elshof & Janssens, *WR* 2017/177

W. Raas, M. Elshof & N. Janssens, 'Het veranderende retail landschap: De opkomst van nieuwe technologieën', *WR* 2017/177.

Roopram, *AD* 28 mei 2020

J. Roopram, 'Gegevens bijstandsgerechtigden belanden zomaar op straat!', *AD* 28 mei 2020.

Rutten, *NRC* 15 oktober 2021

R. Rutten, 'Komt het ooit nog goed met de Toeslagenaffaire?', *NRC* 15 oktober 2021.

Sanderink *SteR* 2018/41

D.G.J. Sanderink, 'Doorwerking via rechtstreekse werking', *SteR* 2018/41.

Schermer, Hagenauw & Falot 2018

B.W. Schermer, D. Hagenauw & N. Falot, *Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming,* Den Haag: Ministerie van Justitie en Veiligheid 2018, p. 22.

Schermer, *Computerrecht* 2017/151.

B.W. Schermer, 'Van meldplicht naar registerplicht: de registratie van verwerkingen onder de AVG', *Computerrecht* 2017/151.

Van der Sloot & Van Schendel, *NJB* 2019/2776.

B. van der Sloot & S. van Schendel, 'De juridische randvoorwaarden voor een data-gedreven samenleving', *NJB* 2019/2776.

Van Toor, *SteR* 2017/32

D.A.G. van Toor, 'Het schuldige geheugen?', *SteR* 2017/32.

Valgaeren & Leitner, *Computerrecht* 2012/2.

E. Valgaeren & L. Leitner, 'Smartphones en privacy — Vrienden, vijanden of ergens tussenin?', Computerrecht 2012/2.

Verhagen, *Volkskrant* 27 september 2019
L. Verhagen, 'Gemeente Amsterdam stopt met omstreden wifitracking', *Volkskrant* 27 september 2019.

De Vries, in: *T&C Privacy- en gegevensbeschermingsrecht*, commentaar op art. 5 AVG
De Vries, in: Tekst & Commentaar Privacy- en gegevensbeschermingsrecht, Beginselen inzake verwerking van persoonsgegevens bij: Verordening (EU) 2016/679 bescherming natuurlijke personen i.v.m. verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG, Artikel 5 Beginselen inzake verwerking van persoonsgegevens, Deventer: Wolters Kluwer.

De Vries, in: *T&C Privacy- en gegevensbeschermingsrecht*, commentaar op art. 6 AVG
De Vries, in: Tekst & Commentaar Privacy- en gegevensbeschermingsrecht, Rechtmatigheid van de verwerking bij: Verordening (EU) 2016/679 bescherming natuurlijke personen i.v.m. verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG, Artikel 6 Rechtmatigheid van de verwerking, Deventer: Wolters Kluwer.

De Vries & Meijer *Gst.* 2017/132
H.H. de Vries & S.A.M. Meijer, 'Privacy en gemeenten: de Algemene Verordening Gegevensbescherming', *Gst.* 2017/132.

Wieringa, *VAR* 2015/11
A. Wieringa, 'Bestuur en openbare orde. Over openbare orde, de bevoegdheidsverdeling bij de handhaving daarvan en ordebevelen onder de Algemene wet bestuursrecht', *VAR* 2015/11.

***Wifi-tracking van mobiele apparaten in en rond winkels door Bluetrace* 2015**
Wifi-tracking van mobiele apparaten in en rond winkels door Bluetrace (College bescherming persoonsgegevens), 2015

Jurisprudentielijst

Europees Hof voor de Rechten van de Mens

EHRM 24 april 2018, ECLI:CE:ECHR:2018:0424JUD006235714 (*Benedik v. Slovenië*)

EHRM 13 september 2018, ECLI:CE:ECHR:2018:0913JUD005817013 (*Big Brother Watch t. Verenigd Koninkrijk)*

EHRM 24 januari 2017, ECLI:CE:ECHR:2017:0124 *(Paradiso Campanelli v.Italy)*

EHRM 23 februari 2016, 11138/10 (*Mozer v. the Republic of Moldova and Russia*)

EHRM 24 april 2012, 25446/06 *(Yordanova en anderen vs. Bulgarije)*

EHRM 7 februari 2012, 40660/08 en 60641/08 (*Von Hannover t. Duitsland (nr. 2)*)

EHRM 2 september 2010, 35623/05 (*Uzun t. Duitsland*)

EHRM 27 oktober 2009, 21737/03 *(Haralambie v. Romania)*.

EHRM 4 december 2008, ECLI:CE:ECHR:2008:1204JUD003056204 (*S. en Marper t. Verenigd Koninkrijk*)

EHRM 17 juli 2003, 63737/00 (*Perry t. Verenigd Koninkrijk*)

EHRM 28 januari 2003, ECLI:CE:ECHR:2003:0128JUD004464798 (*Peck t. Verenigd Koninkrijk*)

EHRM 25 februari 1997, ECLI:CE:ECHR:1997:0225JUD002200993 *(Z. t. Finland)*

EHRM 28 oktober 1994, ECLI:NL:XX:1994:AD2244 *(Murray vs. het Verenigd Koninkrijk)*

EHRM 16 december 1992, ECLI:NL:XX:1992:AD1800 (*Niemietz*)

EHRM 26 maart 1987, ECLI:CE:ECHR:1987:0326JUD000924881 (*Leander t. Zweden*)

EHRM 2 augustus 1984, ECLI:CE:ECHR:1984:0802JUD000869179 (*Malone t. Verenigd Koninkrijk*)

EHRM 22 oktober 1981, ECLI:CE:ECHR:1981:1022JUD000752576 (*Dudgeon t. Verenigd Koninkrijk)*

EHRM 26 april 1979, ECLI:CE:ECHR:1979:0426JUD000653874 (*Sunday Times v. Verenigd Koninkrijk)*

EHRM 6 september 1978, ECLI:CE:ECHR:1978:0906JUD000502971 (*Klass e.a./Duitsland*)

Hof van Justitie van de Europese Unie

HvJ EU 6 oktober 2020, ECLI:EU:C:2020:790

HvJ EU 1 oktober 2019, ECLI:EU:C:2019:801 (*Planet49*)

HvJ EU 24 september 2019, ECLI:EU:C:2019:773 (*GC and Others*)

HvJ EU 13 mei 2014, ECLI:EU:C:2014:317 (*Google Spain and Google*)

HvJ EG 15 juli 1964, ECLI:EU:C:1964:66 *(Costa/ENEL)*

Hoge Raad

HR 30 januari 2007, ECLI:NL:HR:2007:AZ2104

Afdeling Bestuursrechtspraak van de Raad van State

ABRvS 1 april 2020, ECLI:NL:RVS:2020:898

ABRvS 12 november 2014, ECLI:NL:RVS:2014:4117 (*Sinterklaasintocht*)

Centrale Raad van Beroep

CRvB 11 oktober 2018, ECLI:NL:CRVB:2018:3205

CRvB 5 februari 2018, ECLI:NL:CRVB:2018:269

CRvB 15 maart 2016, ECLI:NL:CRVB:2016:947

Rechtbanken

Rb. Overijssel 11 augustus 2021, ECLI:NL:RBOVE:2021:3168

Rb. Noord-Nederland 12 januari 2021, ECLI:NL:RBNNE:2021:106, *JBP* 2021/32

Rb. Den Haag 5 februari 2020, ECLI:NL:RBDHA:2020:865