Spioneren met hobbydrones en andere technologieën door burgers: een verkenning van de privacyrisico's en reguleringsmogelijkheden

Maša Galič, Merel Noorman, Bart van der Sloot, Bert-Jaap Koops, Colette Cuijpers, Raphaël Gellert, Esther Keymolen en Thierry van Delden

Universiteit van Tilburg

TILT – Tilburg Institute for Law, Technology, and Society

Postbus 90153

5000 LE Tilburg

m.galic@uvt.nl

Tel: 013 466 3534

7 mei 2020

Inhoudsopgave

Afkortingen

ANSSI	Nationaal Agentschap voor Cyberveiligheid (Agence nationale de la sécurité des systèmes d'information)
AP	Autoriteit Persoonsgegevens
APV	Algemene Plaatselijke Verordening
AVG	Algemene Verordening Gegevensbescherming
Aw	Auteurswet
BNA	Federaal Netwerkagentschap (Bundesnetzagentur)
BVerfG	Duitse Federale Constitutionele Hof (Bundesverfassungsgericht)
BW	Burgerlijk Wetboek
CCTV	Closed-circuit television
CP	Franse Wetboek van Strafrecht (Code pénal)
EASA	European Union Aviation Safety Agency
EHRM	Europees Hof voor de Rechten van de Mens
EVRM	Europees Verdrag voor de Rechten van de Mens
EU	Europese Unie
FAG	Wet op de telecommunicatieapparatuur (Fernmeldeanlagengesetz)
GDPR	General Data Protection Regulation
GG	Duitse Grondwet (Grundgesetz)
Gw	Gemeentewet
Handvest	Handvest van de Grondrechten van de Europese Unie
HR	Hoge Raad
Sr	Wetboek van Strafrecht
StGB	Duits Wetboek van Strafrecht (Strafgesetzbuch)
Sv	Wetboek van Strafvordering
TKG	Duitse telecommunicatiewet (Telekommunikationsgesetz)
UAVG	Uitvoeringswet Algemene Verordening Gegevensbescherming
UWV	Uitvoeringsinstituut Werknemersverzekeringen
VNG	Vereniging van Nederlandse Gemeenten
VS	Verenigde Staten
VK	Verenigd Koninkrijk
WWM	Wet wapens en munitie

DANKWOORD

De auteurs willen graag de leden van de begeleidingscommissie, prof. dr. Paolo Balboni, dr. ir. Mortaza Shoae Bargh, mr. dr. Marc B. Schuilenburg, mr. Just J. Stam en dr. Anouk L. van Leeuwen, danken voor hun kritische maar te allen tijde constructieve commentaar gedurende dit onderzoek. Ook willen wij alle personen bedanken die bereid waren om deel te nemen aan de interviews en de focusgroepen. De inzichten en de kennis uit deze gesprekken zijn bijzonder waardvol geweest in het onderzoek en hebben een grote bijdrage geleverd aan het tot stand komen van dit rapport. Anne de Laat, Lieke Sterk en Alissa Verhagen willen wij hartelijk danken voor hun werk als student-assistenten aan het onderzoek en het rapport. Tenslotte willen wij ook Georgios Bouchagiar en Aldo Sghirinzetti die als stagairs een bijdrage hebben geleverd aan het onderzoek voor dit rapport.

Samenvatting

1. Achtergrond en onderzoeksvraag

Spionageproducten zoals miniatuurcamera's, afluisterapparatuur en locatietrackers stellen burgers in staat om elkaar te bespioneren, oftewel elkaar heimelijk te observeren. Heimelijk observeren kun je echter ook doen met middelen die niet direct ontworpen zijn voor spionage, maar daar wel heel geschikt voor zijn, zoals hobbydrones met sensoren. Het is in dat licht zinvol onderscheid te maken tussen **spionageproducten in enge zin** (dat wil zeggen apparaten die in de eerste plaats zijn ontworpen of aangepast voor het heimelijk verzamelen van informatie over personen) en **spionageproducten in brede zin** (dat wil zeggen apparaten die kunnen worden gebruikt om heimelijk informatie over een persoon te verzamelen, maar waarvan een dergelijke heimelijke verzameling van informatie niet het hoofddoel is van ontwerp of gebruik). Voorbeelden van de eerste categorie zijn minicamera's, een pen met ingebouwde afluisterapparatuur, en locatietrackers (zowel fysieke apparaten als spyware). Smartphones en hobbydrones met camera's zijn voorbeelden van de tweede categorie.

De brede beschikbaarheid van beide typen producten op de markt, zowel in fysieke winkels als in webwinkels, en het feit dat ze steeds goedkoper worden, heeft geleid tot een toename van mogelijkheden tot spionage in onze samenleving. Omdat sensoren steeds kleiner worden, kunnen ze in elk alledaags voorwerp worden verborgen of ingebouwd. Zo kunnen camera's en afluisterapparatuur verborgen zitten in knopen en knuffels, en kan dit soort apparatuur ook stiekem worden aangebracht in auto's, toiletten en op smartphones van mensen ('spyware'). De steeds betere kwaliteit van opnames maakt het mogelijk om anderen vanaf grotere afstanden te bespioneren, zelfs door fysieke barrières als muren heen. Ten slotte is de mogelijkheid om informatie stiekem vast te leggen en te verspreiden inmiddels nagenoeg onbeperkt. Spionageproducten kunnen steeds langer, op afstand en in *realtime* opnames maken. Dergelijke opnames kunnen vervolgens worden gemanipuleerd (denk aan *deep fakes*) en/of met een klik via het internet wereldwijd worden verspreid.

De vraag die centraal staat in dit rapport is*: Hoe zou het gebruik van hobbydrones en spionageproducten in enge zin door burgers beter kunnen worden gereguleerd, opdat de privacy van de burger beter wordt beschermd?* Om deze vraag te beantwoorden hebben wij gebruik gemaakt van een combinatie van methodes: literatuurstudie, rechtsverkenning van Nederlands, Duits en Frans recht en het recht van de Europese Unie, internet quickscans, twee focusgroepen over hobbydrones en tien semigestructureerde interviews met experts op het gebied van hobbydrones (inclusief academici, praktijkmensen en beleidsmakers).

Het onderscheid tussen spionageproducten in enge en brede zin is met name nuttig voor het doel van deze studie: de inventarisatie van reguleringsmogelijkheden. Spionageproducten in

enge zin kunnen namelijk **aan de bron worden gereguleerd** ("upstream-regulering"; bijv. vergunningsvereisten of verbod op verkoop of bezit), terwijl spionageproducten in brede zin het beste **aan het einde kunnen worden gereguleerd** ("downstream-regulering"; bijv. criminalisering van kwaadaardig gebruik en toekenning van schadevergoeding).

Dit rapport beoordeelt de privacyrisico's in horizontale (burger-burger) relaties, evalueert mogelijke lacunes in het Nederlandse rechtssysteem en geeft een overzicht van reguleringsmogelijkheden om die lacunes te verhelpen, met behulp van Lessig's bekende categorisering van regulering door de markt, sociale normen en wet- en regelgeving en code/ architectuur.

2. Privacyrisico’s in horizontale relaties

De talloze soorten spionageproducten die wereldwijd op de markt verkrijgbaar zijn, kunnen op verschillende manieren inbreuk maken op de privacy van personen (dat wil zeggen 'het vermogen om jezelf te zijn').

Ten eerste maken spionageproducten het mogelijk om opnamen te maken in huizen en op andere privéplekken, zoals in auto's of hotelkamers. Ze kunnen in het geheim beelden of geluid opnemen, zowel binnenshuis (bijv. door een afluisterapparaat in de vorm van een wandklok in de keuken te plaatsen) als buitenshuis (bijv. door drones die door ramen 'gluren' of via infraroodcamera's). Dit zet het idee van de woning als besloten privéruimte onder druk, en daarmee **ruimtelijke privacy**, omdat de bewoner van de woning controle verliest over wie er toegang heeft tot die ruimte.

Ten tweede kan spionage binnen (of buiten) het huis ook inbreuk maken op intieme zaken en dus op **lichamelijke privacy**. Zo kunnen drones personen filmen terwijl ze topless in de achtertuin zonnebaden. Bovendien moet worden opgemerkt dat dergelijke intieme beelden ook in de openbare en semi-openbare ruimte kunnen worden vastgelegd. Denk aan een drone die over een naaktstrand vliegt of aan verborgen camera's in sauna's en kleedkamers van fitnesslocaties.

Ten derde kan de **communicatieve privacy** van burgers worden verstoord, onder meer door afluisterapparatuur in een huis of kantoor te plaatsen, waarmee privégesprekken kunnen worden opgenomen. Zowel van aanwezige personen, maar bijvoorbeeld ook telefoongesprekken. Een andere manier om af te luisteren, is door tracking-apps (spyware) op iemands smartphone te plaatsen. Hiermee kunnen gesprekken, e-mails en andere vormen van privécommunicatie die via het apparaat plaatsvinden, worden afgeluisterd.

Ten vierde, de mogelijkheid om beelden, geluiden en locaties op te nemen in privé, openbare en semi-openbare ruimtes, gecombineerd met het (gevoel van) verlies van controle door burgers en de onmogelijkheid om zeker te weten of en wanneer dergelijke opnames gemaakt worden, kan leiden tot veranderingen in het gedrag van mensen. Personen die (denken dat ze) worden

gecontroleerd, kunnen zich steeds meer geremd voelen in hoe zij zich gedragen. Zij gaan zich bijvoorbeeld conservatiever kleden, kunnen voorzichter worden in wat zij zeggen in gesprekken en kunnen misschien zelfs aarzelen om met bepaalde vrienden om te gaan, zowel in het openbaar als privé (bijvoorbeeld als ze denken dat een jaloerse ex-partner hun bewegingen volgt). Dit leidt tot een verstoring van de **gedragsmatige** en **relationele privacy** van burgers.

Ten vijfde, en misschien wel het meest voor de hand liggend, spionageproducten maken het verzamelen en verwerken van informatie mogelijk, waardoor de **informationele privacy** van burgers in gevaar komt. Zodra informatie is vastgelegd en/of geaggregeerd, kan deze verder worden verspreid. Dit kan inhouden dat de informatie online wordt gepubliceerd of met derden wordt gedeeld, wat de reputatie van een persoon kan schaden. Dreigen om bepaalde informatie te delen kan gebruikt worden als chantagemiddel, hetzij voor geldelijk gewin of voor andere (kwaadaardige) doeleinden.

Ten slotte is het belangrijk om **het cumulatieve effect van privacy schendingen** te belichten. Hoewel elke opname op zichzelf relatief weinig (intieme) informatie kan onthullen, kunnen ze een veelzeggend beeld schetsen van iemands privéleven wanneer tientallen of honderden verschillende 'onschadelijke' informatiebronnen worden gecombineerd. Informatie die bijvoorbeeld gedurende een week is verzameld door locatietracking, kan veel onthullen over iemands professionele en persoonlijke leven: waar iemand woont en werkt; hoe deze zijn tijd 's avonds en in het weekend besteedt en met wie, enzovoort.

3. Lacunes in rechtsbescherming in Nederland

Met het oog op het aanpakken van bovengenoemde privacyrisico's, hebben wij mogelijke lacunes in de rechtsbescherming in Nederland, onderzocht. Hierbij is gekeken naar bestaande privacy- en gegevensbeschermingswetgeving, strafrecht, de onrechtmatige daad, het portretrecht, algemene plaatselijke verordeningen en dronevoorschriften. Omdat veel van deze regels direct of indirect voortvloeien uit EU-richtlijnen en verordeningen en de regels van de Raad van Europa, kunnen de bevindingen van dit rapport over de juridische lacunes en reguleringsmogelijkheden voor veel Europese landen van belang zijn.

Dit onderzoek toont aan dat de huidige (of toekomstige) wetgeving een substantiële bescherming biedt tegen de meeste privacyrisico's. Het huidige gebruik van hobbydrones en spionageproducten om anderen te bespioneren is in feite al in strijd met bestaande wetgeving. Desalniettemin hebben wij een paar kleine lacunes in de wetgeving ontdekt, die vooral verduidelijking of een lichte verruiming van de reikwijdte vereisen.

Onderzoek dat voor deze verkenning is uitgevoerd, toont aan dat de **voornaamste kloof** met betrekking tot de regulering van hobbydrones en spionageproducten een **gebrek aan naleving en handhaving van de bestaande regels** betreft. Dit komt door een combinatie van factoren. Ten eerste is het voor de hand liggende probleem, in geval van heimelijke observaties, dat het

slachtoffer vaak niet weet dat hij of zij wordt bespioneerd. Dit is met name het geval met spionageproducten in enge zin, die zijn ontworpen voor heimelijke observatie. Maar zelfs als het slachtoffer wel bewust is of wordt van de spionage, bijvoorbeeld omdat er online beelden zijn geplaatst, is het vaak erg moeilijk vast te stellen wie verantwoordelijk is voor de spionage (en het online plaatsen van de beelden). Bovendien is dit moeilijk te bewijzen in eventuele strafrechtelijke of privaatrechtelijke procedures.

Ten tweede is de hoogte van de **vergoeding** die in privaatrechtelijke procedures wordt toegekend voor immateriële schade die is geleden door een privacy-inbreuk erg laag. Dit betekent dat zelfs wanneer slachtoffers op de hoogte zijn van de inbreuk en een oorzakelijk verband kunnen aantonen tussen de spionage en de immateriële schade, de toegekende geldelijke vergoeding over het algemeen laag is. Dit kan betekenen dat het starten van gerechtelijke procedures niet als een zinvolle onderneming wordt beschouwd, omdat gerechtelijke procedures een aanzienlijke emotionele en financiële last vormen.

Ten slotte zijn de **handhavingsmogelijkheden** ook beperkt omdat het niet naleven van de wet door het gebruik van hobbydrones en spionageproducten in enge zin vaak een groot aantal relatief kleine incidenten tot gevolg heeft. Als zodanig kan van de Autoriteit Persoonsgegevens niet worden verwacht dat zij elke foto, video of geluidsopname van een burger met een drone of een smartphone onderzoekt en controleert op rechtmatigheid. Ook kan van het Openbaar Ministerie niet worden verwacht dat het elke heimelijke en onrechtmatige opname vervolgt. Op basis van onze interviews en focusgroepen vinden gemeenten het ook moeilijk om de regels met betrekking tot het verbod op spionage en overlast in de Algemene Plaatselijke Verordeningen te handhaven. Zelfs in het geval van drones, die het meest zichtbaar zijn van alle spionageproducten, moeten buitengewone opsporingsambtenaren de hinder die drones veroorzaken persoonlijk waarnemen. Het is voor hen echter onmogelijk om constant de straten en de lucht in de gaten te houden om drones te spotten en ze vervolgens te volgen naar hun rechtmatige eigenaar. Handhaving van de wet biedt dus alleen bescherming tegen de meest ingrijpende incidenten, waarbij bijvoorbeeld de fysieke of ruimtelijke privacy van mensen op het spel staat.

4. Reguleringsmogelijkheden voor Nederland

Hoewel de Nederlandse wet al een substantiële bescherming biedt tegen privacyrisico's als gevolg van het gebruik van hobbydrones en spionageproducten in enge zin, zijn er ook enkele kleinere en enkele grotere lacunes, die mogelijk nog door de wetgever kunnen worden opgevuld. Voor de regulering van spionageproducten in enge zin stellen wij voor te leren van voorbeelden uit Frankrijk (een licentiesysteem voor audiobewakingsapparatuur) en Duitsland (een verbod op bepaalde soorten beeld- en geluidsrecorders). Aangezien de belangrijkste geconstateerde lacune betrekking heeft op naleving en handhaving, kan wetgeving alleen dit niet voldoende

verhelpen; er moeten ook andere soorten reguleringsinstrumenten worden gebruikt. Daarom structureren we onze aanbevelingen voor regelgeving volgens de vier soorten reguleringsinstrumenten van Lessig: markt, sociale normen, recht en code.

Markt

Het tegengaan van privacy-inbreuken zou aan de markt zelf kunnen worden overgelaten. Uit deze studie komt naar voren dat vrijwel alle websites en winkels die spionageproducten verkopen, ook **anti-spionageproducten** aanbieden. Een optie is om het aan burgers zelf te laten om zich te beschermen tegen spionerende medeburgers, bijvoorbeeld door stoorzenders aan te schaffen of apparaten die opnameapparatuur van anderen kunnen ontdekken. Daarbij is het evenwel de vraag of het wenselijk is om een wapenwedloop op dit punt tussen burgers onderling te laten bestaan. Hierbij zou de mate waarin iemands privacy adequaat wordt beschermd immers afhangen van hoeveel er geïnvesteerd wordt in anti-spionageproducten.

Een ander type marktregulering is te vinden in de **informatie over privacy die beschikbaar is op de websites van verkopers en producenten**. Verschillende onderzochte websites van verkopers of producenten van drones, bevatten links naar lokale dronewetgeving. Sommige hebben ook een deel van de website gewijd aan 'correct gebruik' van drones met betrekking tot privacy. Verschillende dronefabrikanten werken ook aan *privacy-by-design*-oplossingen, hetzij uit eigen beweging, hetzij als reactie op (aanhangige) wetgeving. Er bestaan ook bedrijven die **trainingen** verzorgen voor zowel recreatieve als professionele dronepiloten, waarbij privacy een rol speelt. Door de aanstaande EU-dronevoorschriften zal de vraag naar opleidingen waarschijnlijk toenemen, aangezien het voor de meeste dronepiloten verplicht wordt om ten minste een theorie-examen te halen.

De situatie is heel anders in vergelijking met de onderzochte webwinkels die spionageproducten in enge zin verkopen. Deze webwinkels bieden kopers weinig of geen uitleg over wat al dan niet is toegestaan volgens de wet. Bedrijven verklaren ook dat ze niet aansprakelijk kunnen worden gesteld voor onrechtmatig gebruik van spionageproducten die bij hen zijn gekocht. Dit legt de last bij de gebruiker om te controleren of het product, en welk gebruik daarvan, legaal is in hun land. Bovendien moedigen verschillende webwinkels in hun advertenties rechtstreeks illegale activiteiten aan. Bijvoorbeeld: 'Met een spionagecamera kunt u onopgemerkt alle bewegingen in een huis, vergaderruimte en op het werk volgen.' Derhalve, leidt het uitsluitend of hoofdzakelijk in handen laten van de bescherming van privacy door verkopers en producenten waarschijnlijk niet tot de meest bevredigende uitkomst.

Sociale normen

Er zouden ook inspanningen kunnen worden geleverd om meer bewustzijn te creëren over privacyrisico's die voortvloeien uit het gebruik van hobbydrones en spionageproducten in enge zin. Er zouden bijvoorbeeld **nationale bewustwordingscampagnes** kunnen worden opgezet

om burgers bewust te maken van de gevaren van spionageproducten en hen bewust te maken van wat niet is toegestaan. Er zouden websites kunnen worden gelanceerd die zich richten op de privacyaspecten van spionageproducten en de wettelijke verplichtingen die voortvloeien uit het gebruik ervan. Dergelijke informatiebronnen zijn met name belangrijk in verband met de aanstaande EU-dronevoorschriften, die een breed scala aan verplichtingen introduceren die zeer complex en moeilijk te begrijpen zijn. Dergelijke bewustwordingscampagnes zijn waarschijnlijk effectief als het gaat om het gebruik van spionageproducten waarbij mensen in het algemeen niet van plan zijn de privacy van anderen te schenden; dus vooral met betrekking tot spionageproducten in brede zin, zoals drones. Met betrekking tot spionageproducten in enge zin, die zijn gemaakt voor geheime monitoring van anderen, zullen dergelijke bewustmakingscampagnes waarschijnlijk minder effectief zijn, omdat onbekendheid met het juridische kader niet het probleem is.

Uit ons onderzoek blijkt dat er ook **initiatieven** zijn **van maatschappelijke organisaties, verenigingen en individuen** die een waardevolle bron van informatie over privacy zijn. Zo bezoeken beginnende dronepiloten vaak de websites van dergelijke verenigingen (bijv. Dronewatch.nl) om informatie te krijgen over wat wel en niet mag met drones. Forums zijn ook een goede plek voor hobby-dronepiloten om met elkaar te communiceren en bieden rijke informatiebronnen, ook met betrekking tot privacy. Er zijn verschillende manieren waarop de overheid dergelijke initiatieven zou kunnen ondersteunen, zoals door middel van financiële steun, het organiseren van workshops, enz. Ook hier geldt dat dergelijke initiatieven waarschijnlijk minder effectief zijn bij gemeenschappen die spionageproducten in enge zin gebruiken. Hier wordt mogelijk zelfs eerder advies gegeven over de beste manieren om anderen te bespioneren.

Code

Technoregulering kan een belangrijke rol spelen bij het handhaven van horizontale privacy. De EU-regelgeving voor drones voorziet al in verschillende technische oplossingen, zoals **geofencing**, **unieke serienummers** van drones en een **systeem voor identificatie op afstand** (waardoor identificatie van drones op afstand mogelijk is). Geofencing kan bijvoorbeeld worden gebruikt om te voorkomen dat drones bepaalde zones binnenkomen. Het unieke serienummer en het systeem voor identificatie op afstand zijn echter niet vereist voor drones met of zonder sensor die minder dan 250 gr weegt. Het kan echter wenselijk zijn om deze technische eisen verplicht te stellen voor alle drones die persoonlijke gegevens kunnen vastleggen, ongeacht het gewicht. Deze technische oplossingen vergroten namelijk de mogelijkheid om de dronepiloot te identificeren die inbreuk maakt op de privacy van anderen. Opgemerkt moet worden dat technieken als identificatie op afstand en geofencing met een paar simpele ingrepen kunnen worden uitgeschakeld. Deze technische oplossingen zullen er dus niet in slagen te voorkomen dat alle, vooral technisch onderlegde, burgers anderen bespioneren. Desalniettemin helpen ze

de gemiddelde hobby-dronevlieger om het risico op (onopzettelijke) privacyschendingen te verminderen.

Technische maatregelen om privacy schendingen te voorkomen zijn minder geschikt voor apparaten die primair zijn ontworpen om anderen te bespioneren. Aangezien spionageproducten in enge zin in de eerste plaats bedoeld zijn om stiekem gegevens over anderen te verzamelen zonder toestemming, zou het implementeren van de bovenstaande technische vereisten de bestaansreden van dergelijke producten tenietdoen. Wettelijke regels, zoals verboden en licentieregelingen, zijn daarom geschikter om deze producten te reguleren.

Recht

Er zijn een aantal punten in het Nederlandse strafrecht die verduidelijking behoeven.

- Ten eerste is het enigszins onduidelijk of het verbod op geheime bewaking in de privé- en openbare ruimte ook geldt voor opnames gemaakt met een hobbydrone (hetzelfde geldt voor opnames gemaakt met een smartphone). Neem **het vereiste van heimelijkheid,** het is onduidelijk in hoeverre het filmen met drones als verborgen kan worden beschouwd. Hoewel relatief bekend is dat veel of de meeste drones camera's hebben, is het moeilijk of onmogelijk om te weten of er in een concreet geval daadwerkelijk een opname wordt gemaakt en van wat. Bovendien kunnen mensen zich niet goed beschermen tegen ongewenste droneopnames.
- Een ander punt dat de aandacht van de wetgever verdient, betreft de reikwijdte van het verbod op het opnemen van gesprekken, wat momenteel alleen verboden is als het gaat om het opnemen van gesprekken van anderen, namelijk gesprekken waarbij de spion zelf niet betrokken is. Men kan echter ook heimelijk een gesprek opnemen waaraan men zelf deelneemt. De wetgever zou dus kunnen overwegen om over te schakelen van een model voor toestemming van één partij (*one-party consent model*) naar een model waarbij allen toestemming moeten geven (***all-party consent model***).
- Aangezien drones ook worden gebruikt om bepaalde misdaden te plegen, zoals inbraken (bijvoorbeeld door rond het huis te vliegen om te controleren of iemand thuis is of dat er een raam open is), zou de wetgever ook de mogelijkheid kunnen overwegen om aan de **strafbaarstelling van heimelijke observatie een lid toe te voegen** dat specifiek ziet op het observeren van objecten zoals woningen, schuren, loodsen (in plaats van personen) met het oogmerk bepaalde misdrijven voor te bereiden.
- Ten slotte is het heimelijk plaatsen van fysieke locatietrackers op de auto van een andere burger momenteel alleen strafbaar als een object tijdens de installatie wordt beschadigd. De wetgever zou kunnen overwegen om **een direct verbod op fysieke locatietrackers in te voeren** zonder enige eis van schade in het Wetboek van Strafrecht, gelijk aan hoe digitale trackers zijn verboden.

Echter, zoals opgemerkt in paragraaf 3, is de belangrijkste tekortkoming, met betrekking tot privacybescherming die voortvloeit uit het gebruik van drones en spionageproducten, handhaving en naleving van het huidige wettelijke kader. Deze voornaamste kloof kan in het algemeen op twee manieren worden aangepakt: (1) meer aandacht voor **handhaving en compensatie ex-post** (*downstream*-regulering) en/of (2) meer nadruk op **ex-ante-regulering van de verkoop en aankoop van spionageproducten** (*upstream*-regulatie). De eerste zal met name belangrijk zijn voor spionageproducten in brede zin, inclusief drones, terwijl de tweede vooral zal gelden voor spionageproducten in enge zin.

Onder de *ex-post* opties zou de wetgever kunnen overwegen of de vergoedingen voor immateriële schade in geval van privacyschendingen in **privaatrechtelijke procedures** hoog genoeg zijn. Voor veel burgers wegen de inspanningen en de kosten van geschillen niet op tegen de mogelijke toegekende schadevergoeding, die momenteel erg laag is. Een mogelijke oplossing zou zijn om hogere vergoedingsrichtlijnen voor rechtbanken vast te stellen of een minimumbedrag vast te stellen voor schendingen van de privacy als gevolg van spionage.

Met betrekking tot de **Algemene Plaatselijke Verordening** is uit deze studie gebleken dat er bij gemeenten onzekerheid bestaat over hoe nieuwe soorten spionageproducten, met name hobbydrones, kunnen en moeten worden gereguleerd door de verordeningen, en in hoeverre de nieuw ingevoerde regels zullen standhouden in een rechtsprocedure. Gezien deze onduidelijkheid kan de Vereniging van Nederlandse Gemeenten door middel van bestaande of aanvullende bepalingen in de Algemene Plaatselijke Verordening richting geven aan de mogelijkheden om drones en spionageproducten in enge zin te reguleren.

Gezien de beperkte mogelijkheden om de handhaving te verbeteren (als een soort ex-post-regulering), moeten de mogelijkheden van ***ex-ante*-regulering** nader worden bekeken.

Voor drones kan er een registratieverplichting komen voor dronepiloten. Hoewel een dergelijke verplichting al bestaat (en in werking zal treden met de komende EU-verordening inzake drones in juli 2020), zou de Nederlandse wetgever ook kunnen overwegen de verplichte vereisten, voor **unieke serienummers** en het **systeem voor identificatie op afstand** in de EU-verordening inzake drones, te verruimen tot alle drones met een sensor wat de identificatie van de dronepiloot vergemakkelijkt.

Wat *ex-ante*regulering van spionageproducten in enge zin betreft, zijn twee soorten instrumenten bijzonder geschikt. De Nederlandse wetgever zou het voorbeeld van Frankrijk kunnen volgen en een **licentiesysteem kunnen opzetten voor zowel kopers als verkopers van spionageproducten in enge zin**. Een dergelijk licentiesysteem vereist dat elk spionageproduct in enge zin een uniek identificatienummer heeft. Dit vergemakkelijkt de identificatie van de personen die de spionage uitvoeren. Hoewel de Franse licentieverplichting alleen van toepassing is op spionageproducten in enge zin die audio-opnames mogelijk maken, zou de

Nederlandse wetgever kunnen overwegen de reikwijdte ervan uit te breiden tot spionageproducten die visuele observatie en locatietracering mogelijk maken. Er zouden ook aanvullende regels kunnen worden ingevoerd, zoals een verplichte uitleg op het moment van verkoop van wat wel of niet is toegestaan met betrekking tot het gebruik van dergelijke producten, vergelijkbaar met apothekers die het juiste gebruik, de gevaren en risico's van de producten die ze verkopen moeten toelichten. Natuurlijk mag een dergelijk licentiesysteem niet worden gezien als een wondermiddel voor het spionageprobleem, aangezien de verkopers of kopers van spionageproducten het licentievereiste vrij eenvoudig kunnen omzeilen door een product te bestellen bij een buitenlandse onlinewinkel (zoals Alibaba.com) of door hun bedrijf op te zetten in een land zonder een dergelijk vereiste.

In navolging van Duitsland zou de Nederlandse wetgever ook kunnen overwegen **de productie, distributie en het gebruik van bepaalde soorten spionageproducten in enge zin te verbieden**. Het Duitse verbod is specifiek van toepassing op spionageproducten die geschikt zijn voor het heimelijk onderscheppen van andermans privégesprekken en het heimelijk opnemen van andermans beelden, en die de vorm hebben van een alledaags object of hierin ingebed kunnen worden. Hieronder vallen bijvoorbeeld spionagecamera's in de vorm van pennen of poppen met verborgen afluisterapparatuur. Het Duitse verbod omvat echter geen spionageproducten die ‘in het volle zicht’ kunnen worden verborgen vanwege hun miniatuurformaat, zoals een spioncamera in de vorm van een zwarte doos ter grootte van 1,5 cm^3. Bovendien is het Duitse verbod alleen van toepassing op spionageproducten die draadloos gegevens kunnen verzenden; een spionageproduct dat stiekem gegevens kan opnemen maar via USB uitgelezen moet worden, valt niet onder het verbod. De Nederlandse wetgever zou daarom kunnen overwegen het verbod uit te breiden met spionageproducten, die vanwege hun miniatuurformaat bijzonder geschikt zijn om te bespioneren, en die niet draadloos maar anderszins zijn uit te lezen. Door deze twee toevoegingen te introduceren, zou het omzeilen van het verbod (zowel voor verkopers als kopers) veel moeilijker worden. Ten slotte zou de Nederlandse wetgever het Duitse voorbeeld kunnen volgen door een specifieke autoriteit aan te wijzen (in Duitsland is dit de Bundesnetzagentur) met duidelijk omschreven bevoegdheden en een duidelijk aanspreekpunt voor klachtenbehandeling. Bevoegdheden zijn het intrekken van producten, het opleggen van boetes of het gelasten van vernietiging van producten.

Een beknopte selectie van de belangrijkste regelgevingsopties die de Nederlandse wetgever kan aannemen, is te vinden in het stroomschema op de volgende pagina:


1: Verbod
• Ten eerste zou kunnen worden bekeken of en zo ja welke producten zouden kunnen worden verboden, ofwel bij de productie ofwel bij de verkoop.
• Daarbij zou met name kunnen worden gekeken naar alledaagse producten met sensoren en naar mini-microfoons en –camera's die in alledaagse objecten kunnen worden verstopt.
2: Certificering
• Ten tweede zou kunnen worden onderzocht in hoeverre de verkoop en het gebruik van niet-verboden producten zouden kunnen worden gecertificeerd.
• Daarbij zou met name moeten worden gekeken naar de mogelijke certificering van fysieke en virtuele spyshops en naar het gebruik van drones in gebieden met woonhuizen.
3: Technische eisen I
• Ten derde zou kunnen worden onderzocht in hoeverre technische eisen kunnen worden gesteld om bepaalde opnames onmogelijk te maken (of, in ieder geval, veel moeilijker), zoals geo-fencing ten aanzien van no-flyzones of het automatisch blurren van gezichten of personen bij drones.
4: Technische eisen II
• Ten vierde zou kunnen worden onderzocht in hoeverre er technische eisen kunnen worden gesteld aan producten om de heimelijkheid van opnameapparatuur te verkleinen.
• Hierbij kan worden gedacht aan het verplicht afgeven van een geluidssignaal of lichtsignaal als producten opnames starten of maken.
5: Strafrecht
• Ten vijfde zou kunnen worden bekeken in hoeverre strafrechtelijke bepalingen aanpassing behoeven, met name in hoeverre opnames door middel van zichtbare camera's onder het verbod op heimelijk observatie moeten vallen, in hoeverre het heimelijk opnemen van gesprekken door een gespreksdeelnemer zelf ook verboden zou moeten zijn, en in hoeverre het plaatsen van hardwarematige locatietrackers strafbaar moet zijn.
6: Richtlijnen
• Ten zesde zou kunnen worden onderzocht in hoeverre er meer duidelijkheid kan worden geven omtrent de interpretatie van het huidige regelgevende kader ten aanzien van spionageproducten en drones.
• Daarbij kan in het bijzonder worden gedacht aan het ontwikkelen van een modelbepaling in de Algemene Plaatselijke Verordening door de Vereniging van Nederlandse Gemeenten en aan een richtsnoer door de Autoriteit Persoonsgegevens ten aanzien van de gegevensbescherming.
7: Bewustwording
• Ten zevende zou kunnen worden onderzocht in hoeverre kan worden ingezet op het creëren van meer bewustwording, bijvoorbeeld door landelijke campagnes, door lokale signalen en verbodsborden te plaatsen of door het ontwikkelen van een app waarmee dronegebruikers snel en eenvoudig kunnen zien waar zij wel en niet mogen vliegen.
8: Audits en controles
• Ten achtste zou kunnen worden onderzocht in hoeverre drones en andere spionageapparatuur standaard zouden kunnen worden uitgerust met mechanismen die audits en controles mogelijk maken, zoals het loggen van het gebruik en de locatie van het apparaat.
9: Handhaving
• Ten negende zou kunnen worden onderzocht hoe de handhaving van het juridische kader kan worden versterkt, door het ontwikkelen van een gezamenlijke strategie door de gemeenten, de Autoriteit Persoonsgegevens en het Openbaar Ministerie.
10: Vergoeding
• Tot slot zou kunnen worden onderzocht in hoeverre het mogelijk is om burgers een standaardvergoeding toe te kennen bij onrechtmatige gegevensverzameling door medeburgers door middel van drones en spionageproducten.

Summary

1. Background and research question

Spy products such as miniature cameras, eavesdropping devices and location trackers enable citizens to spy on, that is covertly surveil, each other. However, citizens can also covertly surveil others with the use of products that are not directly designed for spying, but that are very suitable for it, such as hobby drones with sensors. As such, it makes sense to distinguish between **spy products in a narrow sense** (that is, devices designed or adapted primarily for the surreptitious gathering of information about persons) and **spy products in a broad sense** (that is, devices that can be used to covertly collect information about a person, but of which such covert collection of information is not the main purpose of design or use). Examples of the former are spy-cams or eavesdropping devices in the shape of everyday of objects and location trackers (both physical devices and spyware). Smartphones and drones are examples of the latter.

The wide availability of both types of products on the market, both in physical spy-shops and in web-shops, and the fact that they are becoming increasingly cheap, has led to a stark increase in the possibility and opportunity to spy on others. As sensors are becoming increasingly small, they can be hidden or built into any everyday object imaginable, from a shampoo bottle to a cuddly toy, and secretly placed in houses and toilets, as well as on people's smartphones (‘spyware’). The constantly improving quality of recording makes it possible to spy on others from greater distances, and new capabilities enable penetrating physical barriers, such as walls. Finally, the possibility to surreptitiously record and disseminate information is by now almost unlimited. Spy products can record for increasingly long periods of time, remotely and in real-time. Such recordings can then be adapted (think of deep fakes) and/or spread globally via the internet with a matter of clicks.

The main question investigated in this report is *how the regulation of hobbydrones and spy products in a narrow sense can be optimised in light of protecting citizens’ privacy.* Answers to this question are based on desk research, legal analysis on Dutch, German and French law and the acquis of the European Union, internet quickscans, two focus groups on hobby drones and 10 semi-structured interviews with stakeholders connected to hobby drone flying and experts on drones (including academics, practitioners, organisations).

The distinction between spy products in a narrow and broad sense is particularly useful for the goal of this study: the inventory of regulatory options. Spy products in a narrow sense can namely be **regulated at the source** (‘upstream regulation’; e.g. licensing requirements or prohibition of sales or possession), whereas spy products in a broad sense can best be **regulated at the end** (‘downstream regulation’; e.g. criminalisation of malicious use and awarding damages).

This report assessed the privacy risks in horizontal (citizen-citizen) relations, evaluated potential lacunae in the Dutch legal system and specified regulatory options to remedy those lacuna's, using Lessig's well-known categorisation of regulation through the market, social norms, code (or architecture) and law.

2. Privacy risks in horizontal relations

Numerous types of spy products available globally on the market can intrude into persons' privacy (that is, 'the ability to be yourself') in a number of ways.

Firstly, spy products enable making recordings within citizens' homes and other private places, such as cars or hotel rooms. They can secretly record images or sound both from the inside (e.g. by placing a listening device in the shape of a wall clock in the kitchen) or the outside of the home (e.g. by drones 'peeking' through windows or through infrared cameras). This puts pressure on the idea of the dwelling as an enclosed private space ('one's castle'), and therefore **spatial privacy**, because the occupant of the dwelling loses control over who has access to that space.

Second, spying within (or inside) the home may also intrude upon intimate matters and thus **bodily privacy**. For example, drones can record persons while they are sunbathing topless in one's backyard. In addition, it should be noted that such intimate images can also be recorded in public and semi-public space. Think of a drone flying over a nudist beach or of hidden cameras in saunas and changing rooms of fitness venues.

Third, citizens' **communicational privacy** can be interfered with, inter alia, by placing listening devices in a home or an office, which can record private conversations either of persons present or via the phone. Another way to do so is by placing tracking apps (spyware) on someone's smartphone, allowing one to eavesdrop on every conversation, e-mail exchange or other private communication transmitted via that device.

Fourth, the possibility to record images, sounds and tracking location in private, public and semi-public space, combined with the (feeling of) loss of control by citizens and the impossibility of knowing for sure whether and when such recordings might be made, can lead to a notable change in people's behaviour. Persons who (think they) are surveilled may begin to behave in an increasingly inhibited manner (for instance by dressing more conservatively), may reveal less in conversations, and may even hesitate to associate with certain friends both in public or private (for example, if they think that a jealous ex-partner is tracking their movements). This leads to an interference with citizens' **behavioural** and **associational privacy**.

Fifth, and perhaps most obviously, spy products enable the collection and processing of information, putting citizens' **informational privacy** at risk. Once information has been captured and/or aggregated, it can then be further disseminated. This may involve publishing the

information online or sharing it with third parties, which can damage a person's reputation. Threatening with such actions can be used for blackmail, either for monetary gain or other (malicious) purposes.

Finally, it is important to consider **the cumulative effect of privacy violations**. While each recording in itself can reveal relatively little (intimate) information, when tens or hundreds of different 'harmless' sources of information are combined, they can paint a rather concise picture of someone's private life. For example, information collected by location tracking for a week can reveal a lot about a person's professional and personal life: where they live and work, how they spend their time in the evenings and weekends, whom they spend time with, and so on.

3. Gaps in legal protection in the Netherlands

In order to address the aforementioned privacy risks, we have investigated possible gaps in legal protection in the Netherlands. We have examined existing privacy and data protection legislation, criminal law, private law, the portrait right, general local ordinances and drone regulations. Because many of these rules stem directly or indirectly from EU Directives and Regulations, and the rules by the Council of Europe, the findings of this report as to the legal lacunae and regulatory options may have significance for many European countries.

This research shows that the current (or upcoming) legislation offers substantial protection against most of the identified privacy risks. In fact, most current use of hobby drones and spy products for the purpose of spying on others already violates existing laws. Nevertheless, a few smaller gaps (or lacunae) in the laws do exist, mainly requiring clarification or a slight broadening of scope.

Research carried out for this study, however, shows that the **main gap** relating to the regulation of hobby drones and spy products concerns **a lack of compliance and enforcement of the existing rules**. This is due to a combination of factors. Firstly, in the case of covert recordings the obvious problem is that the victim often is unaware that she is being spied upon. This is particularly the case regarding spy products in a narrow sense, which are designed for surreptitious surveillance. However, even if the victim does become aware of the spying, for example because recorded images have been placed online, it is often very difficult to determine who is responsible for the spying (and the placing online) and, moreover, to prove this in criminal or private legal proceedings afterwards.

Secondly, the amount of **compensation** granted in private law proceedings for immaterial damage suffered from the intrusion into privacy is currently very low. This means that even in case victims are aware of and can prove a causal link between the spying and the immaterial damage, the awarded monetary compensation is often low. This may mean that beginning legal proceedings is not considered a worthwhile endeavour, because legal proceedings amount to a significant emotional and financial burden.

Finally, **possibilities for enforcement** are also limited because non-compliance with the law through the use of drones and spy products often involves relatively a high number of relatively small incidents. As such, it cannot be expected of the Data Protection Authority to investigate every photo, video or sound recording taken by a citizen using a drone or a smartphone, and to check whether it was done lawfully. It also cannot be expected of the Public Prosecution to prosecute every surreptitious and unlawful recording. Based on our interviews and focus groups, municipalities also find it difficult to enforce the rules concerning the prohibition of spying and nuisance in the general local ordinances. Even in the case of drones, which are the most visible of all spy products, Special Investigation Officers need to perceive the nuisance caused by the drone personally. However, it is impossible for them to constantly monitor the streets and skies in order to spot drones and to then follow them to their rightful owner. Enforcement of the law will thus provide protection only against the most intrusive incidents in which, for example, people's physical or spatial privacy is at stake.

4. Regulatory options

Consequently, while Dutch law already offers substantial protection against privacy risks stemming from use of hobby drones and spy products in a narrow sense, there are also several smaller and some larger gaps, which may still be filled by the legislator. We also suggest possibilities for the regulation of spy products in a narrow sense based on examples from France (a licensing system for audio-surveillance equipment) and Germany (a prohibition of certain types of image- and sound-recorders). Considering that the main identified gap concerns compliance and enforcement, the law on itself cannot sufficiently address it; other types of regulatory tools also need to be employed. We therefore structure our recommendations for regulation according to Lessig's four types of regulatory tools: market, social norms, code and law.

Market

One regulatory option is to leave the protection of privacy up to the market. For instance, almost all web-shops that sell spy products also offer **anti-spying products**, such as jammers (devices that transmit signals on certain radio frequencies in order to disrupt communication between devices) and devices that can detect hidden recording devices. One option is thus to leave it up to citizens themselves to protect themselves against spying fellow citizens by purchasing such devices. However, relying too much on this option may not be desirable as it would lead to a kind of arms race between citizens, where the question of whether someone's privacy is adequately protected depends on how much she is able to invest (in terms of money, expertise and time) in anti-spying products.

Another type of market regulation can be found in the **information concerning privacy available on sellers' and producer's websites**. Several examined websites selling or

producing drones include links to local drone legislation. Some also include a part on the website dedicated to 'proper use' of drones with reference to privacy. Several drone manufacturers are also working on privacy-by-design solutions, either of their own accord or as a response to (upcoming) legislation. Companies also exist that provide **training courses** both for recreational and professional drone pilots, in which privacy plays a role. The upcoming EU drone regulations are likely to increase the demand for training, as they make it compulsory for most drone pilots to pass at least a theory exam.

The situation is very different in relation to the examined web-shops selling spy products in a narrow sense. These web-shops offer little or no explanation to buyers as to what is allowed or not according to the law. Companies also declare that they cannot be held liable for unlawful use of spy products purchased from them, placing the burden on the individual to check, what types of use of the product (or the product itself) are legal in their country. Furthermore, several web-shops directly encourage activity which is illegal, at least in most countries around the world, in their advertisements. For instance: 'With a spy camera you can follow all movements in a home, meeting room and at work unnoticed.' Therefore, leaving the protection of privacy purely or mainly in the hands of these sellers ('the market') may not lead to the most satisfactory outcome.

Social norms

Efforts could also be made in order to create more awareness about privacy risks stemming from the use of hobby drones and spy products in narrow sense. For example, **national awareness campaigns** could be launched, trying to increase the awareness of citizens of the dangers of spy products and make them aware of what is what is not allowed. Websites could be launched that focus on the privacy aspects of spy products and the legal obligations stemming from their use. Such sources of information are particularly important in relation to the upcoming EU drone regulations, which introduce a wide range of obligations that are very complex and difficult to understand. Such awareness-raising campaigns are likely to be effective when it comes to the use of spy products in which people generally have no intention of violating the privacy of others; thus, especially in relation to spy products in a broad sense, such as drones. Concerning spy products in a narrow sense, which are made for covert monitoring of others, such awareness campaigns are likely to be less effective, because unfamiliarity with the legal framework is not the problem.

Based on this research, **initiatives by civil society organisations, associations and individuals** are also a valuable source of information concerning privacy. For instance, novice drone pilots often visit the websites of such associations (e.g. dronewatch.nl) to obtain information about what may and may not be done with drones. Forums are also a good place for hobby drone pilots to communicate with each other, offering rich sources of information, also in relation to privacy. There are several ways through which the government could support such initiatives, such as through monetary support, organisation of workshops, etc. Again, such

initiatives are likely less effective with communities that use spy products in the narrow sense, which are more likely to offer advice on the best ways to spy on others.

Code

Techno-regulation could play an important role in maintaining horizontal privacy. The EU regulations on drones already envision several technical solutions, such as **geofencing**, **unique serial numbers** of drones and a **remote identification system** (enabling remote identification of drones). For example, geofencing can be used to prevent drones from entering certain zones. The unique serial number and the remote identification system are, however, not required for drones with or without a sensor weighing less than 250g. It may, however, be desirable to make these technical requirements mandatory for all drones that can record personal data, no matter the weight. These technical solutions would namely enhance the possibility to identify the drone pilot that is intruding into others' privacy. It should be noted that, techniques such as remote identification and geofencing can be switched off with a few simple interventions. These technical solutions thus will not succeed in preventing all, especially the more tech-savvy, citizens spying on others. Nevertheless, they will help the average hobby drone pilot to reduce the risk of (accidental) privacy breaches.

Technical measures to prevent privacy breaches are less suitable in relation to devices that are designed primarily for spying on others. Considering that spy products in a narrow sense are primarily intended to surreptitiously collect data about others without permission, implementing the above technical requirements would negate the raison d'être of such products. Legal rules, such as prohibitions and licensing regimes, are therefore more suitable to regulate these products.

Law

There are a number of points in Dutch **criminal law** that require clarification and possibly adjustment.

- First, it is somewhat unclear whether the prohibition of covert surveillance in private and public space also covers recordings made with a drone (the same applies to recordings made with a smartphone). Considering the **requirement of surreptitiousness**, it is unclear to what extent recording drones can be regarded as covert. Although it is relatively known that many or most drones have cameras, it is difficult or impossible to know, whether in a concrete instance a recording is actually being made, and people can hardly effectively protect themselves against unwanted recordings.
- Another point that would merit attention from the legislator concerns the scope of the prohibition of recording of conversations, which is currently forbidden only when it concerns the recording of conversations of others, that is conversations in which the spy itself is not involved. However, one can also covertly record a conversation in which one is participating.

The legislator might thus consider switching from a so-called one-party consent model to an **all-party consent model**.

- Considering that drones are also used to commit certain crimes such as burglaries (for example, by flying around the house to check whether someone is at home or whether a window is open), the legislator could also consider introducing a **criminalisation of covert observation of objects** such as houses, barns, sheds (rather than persons) as a preparatory act of committing certain crimes.
- Finally, the surreptitious placement of physical location trackers on another citizen's car is currently only punishable if an object is damaged during installation. The legislator could consider introducing **a direct prohibition of physical location trackers** in the Criminal Code, similarly to how digital location trackers are prohibited.

However, as noted in section 3, the main shortcoming in relation to privacy protection stemming from the use of drones and spy products concerns enforcement and compliance with the current legal framework. This main gap can generally be addressed in two ways: (1) a greater focus on ***ex post* enforcement and compensation** (downstream regulation) and/or (2) a greater emphasis on ***ex ante* regulation of the sale and purchase** of spy products (upstream regulation). The first will be particularly important with regard to spy products in a broad sense, including drones, while the second will mainly apply to spy products in a narrow sense.

Among the *ex post* options, the legislator could consider, whether compensations for immaterial damage in cases of privacy violations in **private law** proceedings are high enough. For many citizens, the effort and costs involved in litigation do not outweigh the possible damages awarded, which are currently very low. A possible solution would be to set higher compensation guidelines for courts or to lay down a minimum amount for privacy violations caused by spying.

In relation to the **general local ordinances**, this study has found that there is uncertainty among municipalities about how new types of spy products, especially drones, can and should be regulated by local ordinances, and to what extent the newly introduced rules will stand up in court. In view of this lack of clarity, the Dutch Association of Municipalities could provide guidance on the possibilities of regulating drones and spy products in a narrow sense through existing or additional provisions in the local ordinances.

Considering the limited possibilities to enhance enforcement (as a type of ex post regulation), possibilities of ***ex ante* regulation** should be looked at more closely.

With respect to drones, an obligation might be introduced for drone pilots to register. While such an obligation already exists (and will enter into force with the forthcoming EU Regulation on drones in July 2020), the Dutch legislator might also consider broadening the obligatory requirement for **unique serial numbers** and the **remote identification system** in the EU

Regulation on drones to all drones with a sensor thus facilitating the identification of the drone pilot.

Regarding *ex ante* regulation of spy products in a narrow sense, two types of instruments are particularly suitable. The Dutch legislator could follow the example of France and establish a **licensing system for both buyers and sellers of spy products in the narrow sense**. Such a licensing system requires each spy product to have a unique identification number and can thus facilitate the identification of persons conducting the espionage. While the French licensing obligation only applies to spy products in a narrow sense that enable audio recording, the Dutch legislator could consider broadening its scope to include spy products enabling visual observation and location tracking. Additional rules could also be introduced, such as a mandatory explanation at the time of sale of what is or is not allowed with regard to the use of such products, comparable to pharmacists, who have to explain the correct use, dangers and risks of the products they sell. Of course, such a licensing system should not be seen as a panacea to the spying problem, considering that the sellers or buyers of spy products can fairly easily circumvent the licensing requirement by ordering a product from a foreign online shop (such as Alibaba.com) or by setting up their company in a country without such a requirement.

Following the example of Germany, the Dutch legislator could also consider simply **prohibiting the production, distribution and use of particular types of spy products in a narrow sense**. The German prohibition specifically applies to spy products suitable for the surreptitious interception of others' private conversations and surreptitious recording of others' images, which need to be shaped as an everyday object or embedded in one. This includes, for instance, spy cams in the shape of pens or dolls with a hidden listening device. However, the German ban does not include spy products that can be hidden 'in plain sight' due to their (increasingly) miniature size, such as a spy cam shaped as a black box the size of 1,5cm³. Furthermore, the German prohibition only applies to spy products that can transmit data wirelessly; a spy product that can surreptitiously record data but transmits it via USB does not fall within the scope of the prohibition. The Dutch legislator might thus consider broadening the prohibition to include spy products, which are particularly suitable for spying due to their miniature size, and, which cannot be read out wirelessly, but can be read out in any other way. By introducing these two additions, circumventing the ban (both for sellers and buyers) would become much more difficult. Finally, the Dutch legislator could follow the German example by designating a specific authority (in Germany this is the *Bundesnetzagentuur*) with clearly defined powers and a clear point of contact for handling complaints, withdrawing products, imposing fines or ordering the destruction of products.

1 Introductie

Met de snelle ontwikkelingen op technologisch gebied wordt horizontale privacy, dat wil zeggen privacy in burger-burger en bedrijf-burger relaties, een steeds prangender onderwerp in het kader van de beleidsvorming. Producten zoals steeds kleiner wordende camera's en geluidsopname apparatuur, maar ook het gebruik van drones voor recreatieve doeleinden ('hobbydrones') stellen burgers in staat om in het geheim anderen te observeren. Dit kan ertoe leiden dat burgers zich steeds meer geobserveerd voelen, ongeacht of dat feitelijk gebeurt.[1] In deze context verstaan wij onder observatie niet alleen visuele observatie (bekijken en vastleggen van beelden) maar ook auditieve observatie (afluisteren en vastleggen van geluid) en het volgen van bewegingen (locatietracking).

Dat burgers elkaar bespieden met behulp van technische middelen is op zich niet nieuw; al in de jaren '60 van de vorige eeuw ontstond door de opkomst van zoomlenzen en richtmicrofoons discussie over heimelijk fotograferen en afluisteren, die leidde tot strafbaarstellingen van diverse vormen van 'spionage'.[2] Maar de schaal waarop burgers met nieuwe technologieën elkaar kunnen bespioneren en informatie over anderen kunnen verspreiden, lijkt sterk te zijn toegenomen ten opzichte van de vorige eeuw. Ook bieden dit soort technologieën, ofwel *spionageproducten*, meer mogelijkheden om mensen stiekem te volgen en te observeren in hun dagelijkse bezigheden dan weleer. In 1970 kon men wellicht nog meegaan met het advies van Kamerlid freule Wttewaall van Stoetwegen aan geliefden die niet in hun tuin wilden worden gefotografeerd: 'Hoe men zich daartegen dan moet beschermen, moeten de mensen zelf beoordelen. Ik geloof dat binnenshuis blijven in dergelijke gevallen het allerbeste is.'[3] Minister Polak kon destijds instemmen met deze 'eenvoudige raad (…) tot bescherming van de eigen privacy', die 'een effectievere bescherming van de privacy van deze personen [biedt] dan welke strafbepaling ooit zou kunnen doen.'[4] Anno 2020 biedt zelfs binnenblijven geen soelaas meer: hobbydrones bieden zicht op voorheen onzichtbare dakterrassen en woonkamers op de achtste verdieping, miniatuurdrones kunnen door ramen naar binnen vliegen en minicamera's en afluisterapparatuur vermomd als alledaagse voorwerpen kunnen heimelijk in huizen, douchehokjes en toiletten alsook op andermans smartphones worden geplaatst.

---

[1] Dit past bij de tendens die in de surveillance-literatuur wordt aangeduid als 'participatory surveillance'. Zie *T. Timan & M. Galič & B. Koops, 'Surveillance Theory and Its Implications for Law', in: R. Brownsword, E. Scotford & K. Yeung (eds), The Oxford Handbook of Law, Regulation, and Technology, Oxford: Oxford UP 2017, p. 731-753;* M. Galič & Timan & B. Koops, 'Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation', 30 *Philosophy & Technology* (1) 2016, p. 9-37 op p. 29-30.
[2] Zie *Kamerstukken II* 1967/68, 9649, nrs. 1-3 e.v., *Kamerstukken II* 1967/68, 9419, nrs. 1-3 e.v. en *Stb.* 1971, 180.
[3] *Handelingen II* 1970/71, p. 471 (22 oktober 1970).
[4] *Handelingen II* 1970/71, p. 483 (22 oktober 1970).

De vraag hoe men zich kan beschermen tegen gluren en heimelijke observatie door andere burgers die gebruik kunnen maken van een groeiend aantal technische hulpmiddelen werd aan de orde gesteld in de Tweede Kamer in de initiatiefnota van het lid Koopmans over Onderlinge privacy.[5] In deze nota komen zowel spionageproducten als hobbydrones aan de orde als mogelijke technische hulpmiddelen die burgers kunnen gebruiken om de privacy van anderen te schenden. Naar aanleiding van deze Initiatiefnota heeft het Wetenschappelijke Onderzoek en Documentatie Centrum (WODC) van het Ministerie van Justitie en Veiligheid aan het Tilburg Institute for Law, Technology, and Society (TILT), van de Tilburg University de opdracht gegeven om een verkennend onderzoek uit te voeren naar de privacyrisico's van en reguleringsmogelijkheden voor het gebruik van hobbydrones en spionageproducten door burgers. Het doel van deze verkenning is om de belangrijkste potentiële aangrijpingspunten voor en hoofdlijnen van regulering te schetsen waarmee de gesignaleerde privacyrisico's en lacunes in de rechtsbescherming zouden kunnen worden ondervangen. De opdrachtgever heeft daarbij aangegeven, conform de Initiatiefnota, ook geïnteresseerd te zijn in praktische waarborgen in binnen- en buitenland om privacy-inbreuken door hobbydrones te voorkomen of te beperken en mogelijke vergunningstelsels of andere vormen van overheidsregulering uit het buitenland om het gebruik van spionageproducten aan banden te leggen.[6]

In navolging van de onderzoeksopdracht vanuit het WODC hebben wij in dit verkennende onderzoek zowel gekeken naar producten die specifiek gemaakt zijn voor heimelijke observaties, zoals minicamera's en locatietrackers, als naar hobbydrones. Maar in plaats van een strikte scheiding tussen deze twee te maken, hebben wij hobbydrones opgevat als een type spionageproduct. Ook met drones kunnen burgers immers heimelijk informatie verzamelen over anderen. Ook al zijn drones niet hoofzakelijk gemaakt om te bespioneren, ze kunnen daar wel toe worden ingezet.

Wel wordt in deze studie waar relevant gedifferentieerd tussen verschillende technologieën, omdat er specifieke wetgeving van toepassing kan zijn op bepaalde dragers van spionagesensoren (zoals drones) en/of omdat reguleringsopties verschillen afhankelijk van het type drager of gebruik. Voor eventuele regulering van smartphones als drager van sensoren, zoals camera's of tracking-software, zullen bijvoorbeeld reguleringsopties substantieel verschillen van producten specifiek ontwikkeld voor het heimelijk observeren van anderen, zoals minicamera's verborgen in pennen of horloges.

Daarom wordt in deze studie een onderscheid gemaakt tussen enerzijds spionageproducten *in enge zin* (b.v. minicamera's en locatietrackers) en anderzijds spionageproducten *in ruime zin*

[5] *Kamerstukken II* 2017/18, 34926, nr. 2.
[6] Ibid. p. 5

(waaronder drones). De term spionageproducten (zonder toevoeging) refereert in deze verkenning aan zowel hobbydrones als minicamera's.[7]

1.1 De onderzoeksvraag

De overkoepelende vraagstelling die wij voor de uitvoering van deze verkenning hebben gehanteerd is:

> *Hoe zou het gebruik van hobbydrones en spionageproducten in enge zin door burgers beter kunnen worden gereguleerd, opdat de privacy van de burger beter wordt beschermd?*

1.2 Afbakening

Alvorens wij de onderzoeksvraag verder uitsplitsen in subvragen, zijn een tweetal afbakeningen van belang.

Een eerste afbakening betreft de term *privacy*. In het kader van dit rapport hanteren wij een breed begrip van privacy, namelijk 'het vermogen om jezelf te zijn'.[8] De focus in dit rapport ligt specifiek op privacy als onderdeel van de relaties tussen burgers onderling. Het gaat in deze verkenning dus over de zogeheten horizontale (of wederzijdse) privacy. Horizontale privacy onderscheidt zich van verticale privacy, waar de nadruk ligt op de relatie tussen burgers en overheid. Een brede interpretatie van 'horizontale privacy' zou dan betekenen dat alle relaties tussen particulieren en organisaties binnen de reikwijdte van het onderzoek vallen, inclusief bijvoorbeeld de relatie tussen consument en bedrijf en werkgever en werknemer (wat 'diagonale privacy' genoemd zou kunnen worden). Deze verkenning richt zich echter in het bijzonder op min of meer gelijkwaardige burger-burger relaties en minder op hiërarchische relaties, zoals tussen ouder-kind, leraar-leerling, werkgever-werknemer. Relaties waarin een onevenwichtige machtsverhouding een rol speelt en waarbij het voor de geobserveerde persoon moeilijk is om de observerende persoon te ontlopen, zoals tussen ouder-kind of leraar-student, zijn niet betrokken in deze studie. Rechtsgebieden die ongelijke horizontale (of 'diagonale') verhoudingen reguleren, zoals familierecht, kinderrechten en onderwijsrecht, worden daarom buiten beschouwing gelaten. Relaties tussen burgers en bedrijven (of andere private organisaties) en tussen werknemers en werkgevers worden in dit onderzoek alleen meegenomen voor zover die betrekking hebben op de verkoop van spionageproducten en hobbydrones.

De tweede afbakening betreft de term *privacyrisico*. Wederom hanteren wij een ruim begrip van privacyrisico's: elke inbreuk op de privacy levert in principe een privacyrisico op, evenals een

---

[7] In deze verkenning gebruiken wij drones en hobbydrones als synoniemen, tenzij anders aangegeven.
[8] Vgl. *Kamerstukken II* 1967/68, 9419, nr. 3, p. 3: 'Onder persoonlijke levenssfeer wordt, globaal uitgedrukt, verstaan de reeks van situaties, waarin de mens, al dan niet in zelfgekozen gezelschap, onbevangen zichzelf wil zijn.' Zie ook P. Blok, *Het recht op privacy*, Den Haag: Boom Juridische uitgevers 2002, p. 43.

mogelijke inbreuk voor zover die tot gevolg heeft dat iemand zich redelijkerwijs belemmerd kan voelen onbevangen zichzelf te zijn (bijvoorbeeld als er een drone over de tuin vliegt, ongeacht of deze daadwerkelijk is uitgerust met een camera).[9] Dit is in lijn met de rechtspraak van het EHRM, dat het begrip privéleven in artikel 8 lid 1 EVRM zeer ruim interpreteert. Deze ruime opvatting van privacyrisico's betekent niet dat elk privacyrisico per definitie problematisch is: er zijn tal van meer of minder triviale privacy-inbreuken die lang niet allemaal de drempel van beleidsrelevantie halen. Een zekere mate van alledaagse privacy-inbreuken (denk aan nieuwsgierige Aagjes, roddel en achterklap, het stiekem meeluisteren met een gesprek in een café, of het snuffelen in papieren als iemand even weg is) zal de burger moeten accepteren. De privacy-inbreuken gepleegd door middel van nieuwe technologieën halen die drempel echter vaak wel. Denk bijvoorbeeld aan het met een drone naar binnen kijken op de achtste verdieping van een woonflat. Ook kan de drempel overschreden worden wanneer bestaande privacy-inbreuken invasiever worden door schaalvergroting, zoals bij het online zetten van een opgenomen vertrouwelijk gesprek, of wanneer voorheen uitzonderlijke privacy-inbreuken een systematisch en cumulatief karakter krijgen.

De scheidslijn tussen welke privacyrisico's wel of juist niet regeluring vergen valt niet altijd scherp te trekken. Desalniettemin hanteren wij als vuistregel dat voor het bepalen van privacyrisico's die regulering vergen, wij met name zullen kijken naar inbreuken op privacy die *dusdanig verschillen* van bestaande (en maatschappelijk geaccepteerde) privacy-inbreuken *dat zij substantieel afbreuk doen* aan de mogelijkheden die burgers redelijkerwijs ervaren om in bepaalde situaties onbevangen zichzelf te kunnen zijn. Eén aspect verdient hierbij bijzondere aandacht: de wisselwerking tussen technologie en maatschappelijke verwachtingen van wat redelijk is en de consequenties die het recht daaraan verbindt. Een voorbeeld ter verduidelijking: de eerste generatie camera's in de 19^{e} eeuw kon alleen foto's nemen als mensen enige tijd poseerden voor de camera. Met de komst van draagbare camera's die direct foto's konden maken, werd het fotograferen als een aanzienlijke inbreuk op de privacy gezien. Naarmate camera's alomtegenwoordig werden, zijn mensen gaan accepteren dat zij gefotografeerd konden worden en verschoof de kern van de privacy-inbreuk van het maken van een foto naar het publiceren van foto's.[10] Toen de eerste zoomlenzen werden gebruikt, was het heimelijk (want niet kenbaar voor de gefotografeerde) fotograferen een aanzienlijke privacy-inbreuk, die de vraag kon oproepen of het gebruik van zoomlenzen niet aan banden zou moeten worden gelegd om de privacy te beschermen. Naarmate zoomlenzen echter gemeengoed werden, hebben burgers het gebruik daarvan door andere burgers moeten accepteren als een risico dat nu eenmaal bestaat als je je in publieke of semi-private ruimten begeeft. Saillant is dat reeds in 1969 de wetgever het niet

[9] Het gaat hier dus om een ruime betekenis van risico die afwijkt van een meer kwantificeerbare definitie van risico zoals deze doorgaans gebruikt wordt in het veld van risicomanagement.
[10] De opkomst van mobiele fotografie en de publicatie daarvan in dagbladen was een van de aanleidingen van het artikel van Warren en Brandeis, 'The Right to Privacy', 4 *Harvard Law Review* 193 1890.

nodig vond om heimelijke observatie *buiten* de woning strafbaar te stellen, omdat 'tegenwoordig telelenzen zo veelvuldig worden gebruikt, dat men bij de vraag of men zich gevrijwaard mag achten van waarneming door onbekenden, veelal met dat gebruik rekening behoort te houden".[11]

1.3 Deelvragen

Zoals eerder gezegd, luidt de hoofdvraag: *Hoe zou het gebruik van hobbydrones en spionageproducten in enge zin door burgers beter kunnen worden gereguleerd, opdat de privacy van de burger beter wordt beschermd?* Om deze vraag te kunnen beantwoorden hebben wij de vraag aan de hand van drie groepen deelvragen uitgewerkt. Elke deel belicht een aspect van de hoofdvraag: privacyrisico's, inventarisatie van andere vormen van regulering en reguleringsmogelijkheden voor Nederland.

Deel 1: Privacyrisico's

1. Hoe kunnen spionageproducten worden gedefinieerd en geclassificeerd, met het oog op het vaststellen van relevante (verschillen in) privacyrisico's en aangrijpingspunten voor regulering?

2. Welke spionageproducten zijn—nu of in de voorzienbare nabije toekomst—te koop of anderszins beschikbaar voor het publiek en kunnen aldus door burgers worden gebruikt?

3. Hoe kan het gebruik van spionageproducten door burgers een inbreuk vormen op de privacy van andere burgers? Wat zijn de belangrijkste privacyrisico's?

4. In welke mate worden de geïdentificeerde privacyrisico's (vraag 3) voorkomen of beperkt door huidige of aanhangige wet- en regelgeving? Wat zijn de (mogelijke) lacunes?

Deel 2: inventarisaties van andere vormen van regulering

5. Hoe trachten de ons omringende landen privacy-inbreuken door het gebruik van spionageproducten door burgers te voorkomen of te beperken via vergunningstelsels of andere vormen van overheidsregulering? Welke maatregelen zijn succesvol en welke niet?

6. Wat zijn succesvolle, praktische waarborgen van binnen- en buitenlandse bedrijven en organisaties om privacy-inbreuken door spionageproducten te voorkomen of te beperken? En waarom zijn andere waarborgen niet succesvol?

[11] *Kamerstukken II* 1969/70, 9419, nr. 4, p. 8. Merk op dat in 2003 de strafbaarstelling werd uitgebreid tot het heimelijk maken van beelden buiten de woning of niet voor het publiek toegankelijke lokalen (art. 441b Sr, ingevoerd bij *Stb.* 2003, 198).

7. Zijn er *buiten* de ons omringende landen nog interessante voorbeelden te vinden van succesvolle of juist mislukte vormen van overheidsregulering of zelfregulering om privacy-inbreuken door spionageproducten te voorkomen of te beperken?

Deel 3: Reguleringsmogelijkheden voor Nederland

8. Welke oplossingsrichtingen zijn er voor het Nederlandse beleid om de privacyrisico's door gebruik van spionageproducten door burgers te voorkomen of beperken, gelet op de gesignaleerde overheidsreguleringslacunes (vraag 4) en de uit Deel 2 naar voren komende praktische waarborgen en maatregelen?

9. Voor zover uit de inventarisatie van praktische waarborgen en maatregelen uit deel 2 geen duidelijke of voldoende oplossingsrichtingen naar voren komen om (alle) gesignaleerde reguleringslacunes (vraag 4) te adresseren, hoe zouden deze reguleringslacunes anderszins kunnen worden afgedekt?

Deze vragen zullen wij beantwoorden aan de hand van een literatuurstudie, internet quickscans, interviews, focusgroepen en een rechtsverkenning. Deze onderzoeksmethode lichten wij verder toe in het volgende hoofdstuk.

1.4 Opbouw rapport

In het volgende hoofdstuk zullen wij eerst de methodologie van deze verkenning nader toelichten. Vervolgens staan deelvragen 1 en 2 centraal in hoofdstuk 3, waarin wij een definitie en classificatie geven van spionageproducten en een overzicht van de beschikbaarheid van deze producten in Nederland. In hoofdstuk 4 brengen wij vervolgens de privacyrisico's van deze spionageproducten in kaart (deelvraag 3). De analyse in dit hoofdstuk vormt het startpunt voor de beantwoording van vraag 4 in hoofdstuk 5. In dit hoofdstuk verkennen wij in hoeverre de wetgeving in Nederland de geïdentificeerde privacyrisico's voorkomt of beperkt en identificeren wij mogelijke lacunes. Tevens belichten wij ook manieren om deze lacunes te adresseren en beantwoorden daarmee een deel van vraagt 8. In hoofdstuk 6 staan de vragen uit Deel 2 centraal (deelvragen 5, 6 en 7). Tot slot geven wij in hoofdstuk 7 een samenvattend conclusie alsmede een antwoord en een overzicht een overzicht van mogelijke reguleringsmogelijkheden voor Nederland. Daarmee beantwoorden tevens vraag 8 en 9.

2 Methodologie

Om de deelvragen (en daarmee de hoofdvraag van dit onderzoek) te beantwoorden hebben wij gebruik gemaakt van een combinatie van onderzoeksmethode zijnde: literatuurstudie, internet quickscans, interviews, focusgroepen en een rechtsverkenning. Wij lichten de invulling en het gebruik van de verschillende onderzoeksmethodes hieronder verder toe.

2.1 Literatuurstudie

Vanwege het verkennend karakter van dit onderzoek, hebben wij ervoor gekozen om bestaande inzichten en kennis over spionageproducten in enge zin en hobbydrones in kaart te brengen en te analyseren middels een literatuurstudie en deze aan te vullen met inzichten uit de internetquickscans, interviews en focusgroepen (zie volgende paragrafen). Deze literatuurstudie vormde de basis voor de beantwoording van de deelvragen 1 tot en met 8, voor zover die gaan over de privacyrisico's en privacybeschermende praktische waarborgen en maatregelen. Met name voor het in kaart brengen van mogelijke privacyrisico's van het gebruik van *spionageproducten in enge zin* achtte wij een theoretisch benadering op basis van bestaande literatuur vruchtbaarder voor dit verkennende onderzoek dan empirisch onderzoek, omdat het lastig is om empirisch materiaal te verzamelen. De aard van deze spionageproducten is immers dat men het gebruik verborgen wil houden, waardoor het binnen dit onderzoek lastig is te achterhalen hoe vaak deze producten worden gebruikt en waar zich mogelijke inbreuken op de privacy voordoen. Bovendien kan het gebruik van deze producten raken aan complexe en gevoelige problematiek (denk bijvoorbeeld aan spionage of *stalking* van ex-partners). Dat maakt dat het praktisch onmogelijk is om respondenten te vinden die willen praten over hun ervaring met spionageproducten binnen het tijdsbestek van deze verkenning. Voor hobbydrones - die meer zichtbaar zijn en ook voor andere doeleinden worden gebruikt - was het daarentegen wel mogelijk om ook aanvullend empirisch onderzoek te doen, waaronder interviews en focusgroepen, waarover meer in paragraaf 2.3 en 2.4.

Voor de literatuurstudie hebben wij gebruik gemaakt van academische literatuur, (beleids)rapporten, vakmatige publicaties over spionageproducten, nieuwsartikelen en verschillende websites, inclusief online fora. Bij het zoeken naar literatuur hebben wij gebruik gemaakt van internetzoekmachines, de zoekfunctie van de universiteitsdatabase en referentielijsten uit eerdere rapporten en academische literatuur. We hebben in het bijzonder gezocht naar literatuur die zich richt op spionage tussen burgers en de producten die zij daarvoor gebruiken. Voor het in kaart brengen van de ontwikkelingen hebben wij ons gericht op de nabije toekomst (vijf jaar).

2.1.1 Analyse van de privacyrisico's

In het literatuuronderzoek hebben wij gebruik gemaakt van twee theoretisch modellen om de privacyrisico's gestructureerd in kaart te brengen (deelvraag 3): de privacytypologie ontwikkeld door Koops et al.[12] en de taxonomie van activiteiten die privacy kunnen schaden zoals beschreven door de Amerikaanse privacy expert Solove.[13] Wij zullen deze modellen in hoofdstuk vier verder uit een zetten. Hier lichten wij alleen verder toe hoe en waarom wij deze modellen gebruiken voor het in kaart brengen van de privacyrisico's.

Koops et al.'s privacytypologie is gericht op een systematische en uitgebreide classificatie van privacytypen. De typologie kan dienen als analytisch en evaluatief hulpmiddel om de impact van nieuwe technologieën, sociale praktijken en wettelijke maatregelen op privacybelangen die verder gaan dan gegevensbescherming te helpen beoordelen.[14] Zij heeft tot doel verschillende soorten privacy te identificeren en is gebaseerd op een analyse van de grondwettelijke bescherming van de persoonlijke levenssfeer. Hierbij is gekeken naar jurisprudentie en wetenschappelijke analyses in negen landen, met zowel *common-law*-stelsels als *civil-law*-stelsels. De hoofdgedachte achter de typologie is dat de identificatie van verschillende 'objecten' van bescherming van het recht op privacy (bijv. de woning, communicatie en persoonlijke gegevens; zoals het zich de afgelopen 120 jaar in de wet heeft ontwikkeld), ondersteund door een theoretische privacystudie van elk rechtsgebied, kan bijdragen aan het onderscheiden van de meest relevante vormen van privacy, met behoud van belangrijke culturele verschillen.

In de typologie zijn privacytypen gegroepeerd langs een spectrum van interactie met de omgeving, lopend van een strikt persoonlijke sfeer tot aan de publieke sfeer en langs een spectrum van negatieve (met rust worden gelaten) tot positieve (jezelf kunnen zijn) vrijheid. Deze aanpak maakt het mogelijk per sfeer de belangrijkste privacy-inbreuken te identificeren gekoppeld aan de soort activiteit. Hobbydrones en spionageproducten in enge zin kunnen inbreuk maken op allerlei soorten privacy, zoals gedragsmatige, relationele, lichamelijke en ruimtelijke privacy.

De typologie van Koops et al. kan ons helpen om op een systematische manier de grote verscheidenheid aan activiteiten die inbreuk kunnen maken op privacy te identificeren. Belangrijk daarbij is vooral dat privacy-inbreuken verder kunnen gaan dan de activiteiten die in de eerste plaats inbreuk maken op de bekendste vorm van privacy – informationele privacy of gegevensbescherming. Bij sommige activiteiten, zoals het vliegen met een drone over een dakterras of voor het raam van een woonkamer, gaat het immers niet alleen om de informatie die

[12] B. Koops & e.a., 'A Typology of Privacy', 38 *University of Pennsylvania Journal of International Law* (2) 2017, p. 483-575.
[13] D. J. Solove (2008), *Understanding privacy*, Harvard: Harvard University Press.
[14] B. Koops e.a, 'A Typology of Privacy', 38 *University of Pennsylvania Journal of International Law* (2) 2017, p. 483-575. pp. 487-488.

daarbij wordt verzameld, maar ook om de fysieke inbreuk op de huisvrede en het gevoel te worden bekeken.

Om de verschillende soorten inbreuken op de *informationele privacy* te identificeren en te begrijpen heeft Solove een taxonomie ontwikkeld van privacyschade (privacy harms). Volgens Solove gaat het bij inbreuken op dit type privacy om verschillende soorten schadelijke of problematische activiteiten (informatieverzameling, informatieverwerking, informatieverspreiding en overschrijding). Zijn taxonomie heeft als doel om aan te tonen dat de verstoringen van de privacy van elkaar verschillen en toch belangrijke overeenkomsten vertonen. Daarnaast is het doel van de taxonomie ook om een 'goed onderbouwde verantwoording te geven waarom privacy problemen schadelijk zijn'.[15] Als zodanig is het een nuttig hulpmiddel, als aanvulling op de typologie, bij het analyseren van de privacyproblemen die ontstaan door burgers die andere burgers bespioneren wanneer die betrekking hebben op *informationele privacy*.

In de analyse van de privacyrisico's in hoofdstuk vier hebben wij ook gebruik gemaakt van een viertal casussen om een beeld te schetsen van hoe het gebruik van spionageproducten de verschillende typen privacy kan schaden. Deze casussen hebben wij geselecteerd op basis van de mate waarin zij iets zeggen over de verschillende privacytypen en het soort spionageproduct dat erin centraal staat. Drie casussen zijn gebaseerd en geïnspireerd op nieuwsartikelen over het gebruik van spionageproducten (minicamera's, smart-watches en GPS-trackers) en een op de ervaringen van de Kinderdijk bewoners met hobbydrones. Deze laatste casus is gebaseerd op aanvullend onderzoek - waaronder een focusgroep, interviews, en literatuurstudie – omdat de aard van de casus het toeliet om binnen het bestek van de verkenning empirisch materiaal te verzamelen (zie voor verder toelichting 2.3 en 2.4).

2.2 Internetquickscans

Ter aanvulling van het literatuuronderzoek hebben wij in dit onderzoek een drietal internetquickscans uitgevoerd naar: 1) het aanbod van spionageproducten in enge zin voor Nederlanders, 2) internationale wet- en regelgeving omtrent spionageproducten in enge zin en 3) internationale wet- en regelgeving omtrent het gebruik van hobbydrones. Hieronder leggen wij per quickscan uit waarom wij voor deze methode hebben gekozen en hoe wij ze hebben uitgevoerd.

2.2.1 Internet quickscan naar de verkoop van spionageproducten in enge zin

Het doel van de eerste quickscan was om een globaal overzicht te krijgen van het aanbod aan spionageproducten in enge zin voor burgers, ter beantwoording van deelvraag 2. Wij hebben deze methode gekozen vanwege het verkennende karakter van het onderzoek: aan de hand van deze

[15] Daniel J Solove, 'Conceptualizing Privacy' (2002) 90 California Law Review 1087

methode konden wij snel inzicht konden krijgen in welke spionageproducten mensen in Nederland makkelijk kunnen verkrijgen. Alhoewel deelvraag 2 over spionageproducten in het algemeen gaat, is deze quickscan toegespitst op spionageproducten in enge zin, omdat wij voor hobbydrones hebben voorgebouwd op het eerdere WODC-onderzoek over drones uit 2015 en het overzicht tijdens het literatuuronderzoek verder hebben uitgewerkt.[16]

Wij hebben voor deze eerste quickscan de Google-database doorzocht - in de periode van 1 mei 2019 tot en met 1 augustus 2019 - naar websites die spionageproducten aanbieden voor de verkoop. Gezien het bereik van de wereldwijde markt, waarin iemand een spionageproduct net zo gemakkelijk kan kopen in een lokale technologiewinkel (bijvoorbeeld de Media Markt), via een lokale internetwinkel (bijvoorbeeld bol.com of spyshop4u.nl) als bij een internetwinkel uit de VS, China of Israël (bijvoorbeeld alibaba.com), hebben wij ook verder gekeken dan de Nederlandse markt. Desalniettemin besteden wij bijzondere aandacht aan lokale verkopers om een beeld te krijgen van de belangrijkste spionageproducten voor Nederlanders. Voor de geïnventariseerde aanbieders hebben wij vervolgens gekeken welke en hoeveel producten zij aanbieden en wat de kosten ongeveer zijn.

De quickscan bestond uit twee verschillende onderdelen. Ten eerste hebben wij een overzicht gemaakt welke spionageproducten *in enge zin* er in Nederland voornamelijk te koop zijn. Hierbij hebben wij een onderscheid gemaakt tussen fysieke winkels, internetwinkels die specifiek spionageapparatuur verkopen en internetwinkels die een breed assortiment aanbieden, waaronder ook spionageapparatuur (zoals bol.com en coolblue.nl). Om de fysieke winkels in kaart te brengen hebben wij de zoekterm ‘Spionagewinkels in Nederland’ gebruikt. Dit resulteerde in 198.000 zoekresultaten en vijf fysieke winkels gericht op de verkoop van spionageapparatuur.[17] Van de vijf fysieke winkels waren er drie van een bedrijf (twee filialen in Nederland en een in België).

Voor de internetwinkels die specifiek spionage apparatuur verkopen hebben wij de volgende zoektermen gebruikt: “Online spionage winkel Nederland’’ en ‘’Spyshop Nederland’’. Dit resulteerde in 151.000 en 22.500 zoekresultaten. Uit deze zoekresultaten zijn vervolgens 28 sites gefilterd,[18] waarvan er 11 terug zijn te leiden tot één online verkooppunt (Alle 11 websites zijn websites van SITCON).[19] De filtering vond plaats op basis van of het criterium dat het online winkels betrof die spionageproducten aanboden.

---

[16] B. Custers e.a., Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen, WODC, Amsterdam: Boom Lemma Uitgevers 2015.
[17] SpyShop Amsterdam, Spywebshop Nieuwegein, Spy Camera Shop Nieuwegein, Sitcon BV Winkel Utrecht, Spyshop Breda, Sitcon BV Winkel Amsterdam, Spy & Security Shop Breda, Spywebshop BV Nieuwegein, Spy3K Rotterdam.
[18] Zie bijlage I.
[19] Spywebshop.nl, sitconsecurity.nl, spycamerashop.nl, spygadgetstore.nl, detectiveshop.nl, spy-shop.info, afluisterapparatuurshop.nl, spycamera.nu, draadlozecamerashop.nl, bewakingscameraspecialist.nl, spyphoneshop.nl.

Ook hebben wij gezocht naar internetwinkels met een breder aanbod die ook spionageproducten in enge zin verkopen. Bij het invoeren van de zoekterm ‘’Spionagewinkels in Nederland’’, ‘’Online spionage winkel Nederland’’ en ‘’Spyshop Nederland’’ zijn de volgende internetwinkels met een breed assortiment geïdentificeerd, namelijk: bol.com, beslist.nl en marktplaats.nl. Gezien de wereldwijde omvang van de markt hebben wij ook de Duitse versie van webwinkel Amazon meegenomen in de quickscan, Amazon.de. Wij hebben voor de Duitse versie gekozen omdat de Nederlandse versie slechts boeken aanbiedt en geen spionageproducten. Nederlanders kunnen deze producten wel bestellen op de Duitse versie van Amazon.

Ten tweede hebben wij, naast het doorzoeken van de Googledatabase, de Apple Store (IOS) en de Play Store (Android) doorzocht op het aanbod van spionageapps. Hiervoor zijn meerdere zoektermen gebruikt omdat het om specifieke apps ging die onder verschillende namen worden aangeboden. Het betrof de volgende zoektermen gebruikt ‘’spionage app’’, ‘’spy app’’, ‘’stalkerware’’, ‘’ spyware’’, ‘’location tracking app’’ en ‘’spouseware’’. Hier was vooral de beschrijving, alsmede het doel van de app, doorslaggevend in het meenemen van resultaten in de inventarisatie.

2.2.2 Internetquickscan naar wet- en regelgeving in het buitenland omtrent spionageproducten in enge zin

De tweede quickscan was bedoeld om een eerste globaal overzicht te krijgen van de wet- en regelgeving in het buitenland omtrent spionageproducten in enge zin ter beantwoording van deelvraag 5, 6 en 7. Wij hebben voor spionageproducten in enge zin en voor hobbydrones aparte quickscans uitgevoerd omdat ze verschillende zoektermen vereisten. De wet- en regelgeving in Nederland hebben wij in kaart gebracht in de uitgebreide rechtsverkenning (zie paragraaf 2.5). Vanwege de focus op wet- en regelgeving betreft het hier een ander soort quickscan dan de eerste quickscan: de zoektermen zijn meer specifiek gericht op het zoeken naar wet- en regelgeving. Het globale overzicht is vervolgens gebruikt als startpunt voor de verdere analyse in de internationale rechtsverkenning (zie paragraaf 2.5.2). In de periode van 1 mei 2019 tot en met 26 augustus 2019 is de Googledatabase doorzocht. De zoektermen in deze quickscan betroffen:

“[country name (hereafter, cn)] spy products licence”; “[cn] spy products license requirements”; “[cn] spy products sale license”; “[cn] spy products license regulation”; “[cn] spy products regulation”; “[cn] spy gadgets regulation”; “[cn] spy products webshop”

“[cn] spy cams regulation”; “[cn] surveillance cameras regulation”

“[cn] surveillance products regulation”; “[cn] surveillance regulation”; “[cn] eavesdropping regulation”

De landen waarop wij hebben gezocht zijn: Argentinië, België, Brazilië, Canada, Chili, China, Denemarken, Duitsland, Finland, Frankrijk, Hong Kong, Noorwegen, Singapore, Spanje, de Verenigde Staten, Zweden, Israël, Rusland en Zuid-Korea. Deze selectie is het resultaat van een eerdere test-quickscan die in het kader van de voorbereiding van dit onderzoek volgens het bovenstaande protocol is uitgevoerd.[20] Deze test-quickscan hebben wij uitgevoerd om te kijken welke landen en informatie er met de verschillende zoektermen het meest prominent naar voren kwamen. De zoektermen zijn ook ingevoerd in de oorspronkelijke taal van bepaald landen die naar boven kwamen, met behulp van Google translate (bijv. 'licence de produits d'espionnage' for 'spy products license' bij het verder zoeken naar Frankrijk). Per land is ook gekeken naar websites van de gegevensbeschermingstoezichthouders (de landelijke varianten van onze Autoriteit Persoonsgegevens) en webshops die spionageproducten aanbieden. Deze hebben wij bekeken om te zien of er verwijzingen naar relevante wetgeving in stonden.

Op basis van deze test-quickscan hebben wij de ons inziens, qua relevante regulering, relevantste landen geselecteerd. Uit deze quickscan kwam Frankrijk naar voren land omdat het een vergunningstelsel voor bepaalde spionageproducten heeft en Duitsland, dat een relevant verbod op spionageapparatuur met een zendfunctie kent. In andere landen was de algemene indruk dat het gebruik van spionageproducten grotendeels is gereguleerd via het (algemene) strafrecht en gegevensbeschermingsrecht.

2.2.3 Internet quickscan naar internationale wetgeving omtrent het gebruik van drones

Het doel van de derde quickscan was om een overzicht te krijgen van de relevante wetgeving omtrent hobbydrones in het buitenland ter beantwoording van deelvraag 5, 6 en 7. De landen die onderdeel waren van de derde quickscan zijn: Frankrijk, Duitsland, Rusland, Noorwegen, de Verenigde Staten, Spanje, Zweden, Noorwegen, Finland, Denemarken, Chili, Brazilië, Argentinië, Canada, Zuid-Korea, China/Hong Kong en Singapore. Wij hebben hierbij dus dezelfde landenselectie gehanteerd als bij de tweede quickscan. In de periode van 1 mei 2019 tot en met 26 augustus 2019 is de Googledatabase doorzocht. Drie zoektermen zijn hierbij gebruikt:

''[country name (hierna: cn)] drones regulation'', ''[cn] drone rules'', ''[cn] drone laws''

De zoektermen zijn per land ingevoerd, wat resulteerde in verschillende hoeveelheden zoekresultaten variërende van 10.400.000 tot 17.400.000. De Googledatabase is voornamelijk gebruikt als eerste indicatie voor de wet- en regelgeving omtrent het gebruik van drones. Relevante websites zijn gefilterd uit de Google Database, wat resulteerde in gemiddeld 4 tot 6 websites. Deze websites vermeldde veelal lijsten met de hoofdpunten uit de wet- en regelgeving

[20] Aldo Sghirinzetti, 'Spy products regulation', maart 2019 (ongepubliceerd, beschikbaar bij de onderzoekers).

van desbetreffend land. Via deze websites werden de officiële wet- en regelgeving omtrent drones van het desbetreffend land geïdentificeerd en verder geanalyseerd voor relevante informatie.

Uit deze internet quickscan bleek dat de meeste landen, zowel binnen als buiten de Europese Unie, drones vooral reguleren met betrekking tot de veiligheidsaspecten van het vliegen met drones, vergelijkbaar met de komende EU-verordeningen over drones (geanalyseerd in par. 5.6). Verder wijzen sommige landen ook specifiek op privacyrisico's die voortvloeien uit drones, waarbij wordt verwezen naar de nationale wetgeving inzake gegevensbescherming en/of het strafrecht, die vergelijkbaar zijn met de Nederlandse (en dus Europese) wetgeving inzake gegevensbescherming en met de voor drones relevante bepalingen in het Nederlandse strafrecht (die we in par. 5.1 en 5.4 analyseren).

2.3 Interviews over hobbydrones

Ter aanvulling en ondersteuning van de literatuurstudie en internetquickscan hebben wij semi-gestructureerde interviews gehouden met belanghebbenden van recreatief dronevliegen. Zoals gezegd hebben wij de interviews tot vraagstukken rond hobbydrones beperkt, omdat wij daar een duidelijke meerwaarde verwachtten van deze empirische methodes. De interviews dienen om inzichten ten aanzien van de praktijk van het gebruik van hobbydrones, bijvoorbeeld over hoe en waarom mensen drones gebruiken en hoe men tegen regelgeving aankijkt, mee te kunnen nemen in de verdere analyse van de privacyrisico's, praktische waarborgen en reguleringsmogelijkheden (deelvragen 3, 4, 6, en 8). Deze inzichten kunnen soms verschillen van of verdere nuance geven aan de inzichten uit de literatuur, bijvoorbeeld als het gaat om wat er mogelijk is met een hobbydrone of in hoeverre bestaande regelgeving effectief is. In de interviews richtten wij ons aldus voornamelijk op hoe hobbydrones gebruikt worden en wat mogelijk is, hoe zij een privacyrisico kunnen vormen (deelvraag 2), hoe hobbydronevliegers op de hoogte blijven van de regels (deelvraag 8), welke vormen van zelfregulering er (in ontwikkeling) zijn (deelvraag 6) en wat verwachte ontwikkelingen zijn (deelvraag 2 en 3). Omdat het hier om een verkennend onderzoek gaat zijn de inzichten uit deze interviews louter indicatief en kunnen er geen generieke conclusies uitgetrokken worden. Desalniettemin helpen deze inzichten bij het aanscherpen van de analyses in deze verkenning, bijvoorbeeld bij het identificeren van mogelijke blinde vlekken in de literatuurstudie. Dergelijke aanscherpingen zijn dus niet mogelijk voor spionageproducten in enge zin.

Wij hebben ervoor gekozen om mensen te interviewen die bekend zijn met de praktijk van het vliegen van drones in Nederland. Omdat vooral ook het gebruik hier van belang is hebben wij de gegadigden gezocht bij Nederlandse verenigingen, websites en online fora die zich bezighouden met recreatief vliegen van drones. De tien experts die wij hebben geïnterviewd komen van drone-organisaties en dronebedrijven, maar betreffen ook universitaire drone-onderzoekers,

beheerders van dronewebsites en vertegenwoordigers van plaatselijke overheden die voorlichtingscampagnes organiseren (zie bijlage I). Deze personen dragen ook bij aan praktische waarborgen op verschillende gebieden, zoals technisch ontwerp, toepassing, opleiding, voorlichting, handhaving en gebruikerspraktijken (deelvraag 6 en 8). Het is ons niet gelukt om ontwikkelaars van drones of representanten van bedrijven die drones maken te interviewen. Wij hebben geen hobbydronevliegers geïnterviewd, omdat wij voor deze ervaringsdeskundige gekozen hebben voor een focusgroep methode (die volgende paragraaf).

De interviews duurde gemiddeld een uur en werden met toestemming opgenomen en getranscribeerd. We hebben gebruik gemaakt van een interviewleidraad om de interviews te structureren (zie bijlage II). Deze leidraad diende vooral als geheugensteun om specifieke onderwerpen aan bod te laten komen. Omdat het open interviews betrof kon er ook afgeweken worden van de leidraad. De interviews vonden zowel telefonische plaats als op locatie.

2.4 Focusgroepen over hobbydrones

Ter aanvulling van de uit de literatuurstudie geïdentificeerde privacyrisico's (Deel 1 van de onderzoeksvragen) en voor het nader verkennen en aanscherpen van reguleringsmogelijkheden (Deel 2 en 3 van de onderzoeksvragen) hebben wij ook twee focusgroepen georganiseerd. Het doel van de focusgroepen was om in kaart te brengen wat burgers en hobbyvliegers als privacyrisicos zien ten aanzien van hobbydrones en over de manieren waarop deze risico's zouden kunnen worden beheerst.

Wij hebben voor deze vorm gekozen omdat wij meerdere ervaringsdeskundigen wilden spreken over het gebruik van hobbydrones. Bovendien maakt deze methode het mogelijk om met een relatief homogene groep een aantal kwesties omtrent het gebruik van drones en de mogelijke privacyrisico's verder uit te diepen dan mogelijk zou zijn met individuele interviews. Door de deelnemers aan de focusgroep met elkaar in gesprek te laten gaan (aan de hand van vragen, een open discussie en vignetten), kunnen er inzichten boven komen die wellicht niet geanticipeerd waren door een interviewer. De deelnemers aan de focusgroep spreken immers vanuit hun eigen ervaring die onderzoekers vooraf niet volledig in beeld hebben.

Wij richtten de focusgroepen uitsluitend op hobbydrones, omdat dit een relatief afgebakende context betreft. Wij achtte spionageproducten te divers om binnen een verkennend onderzoek met focusgroepen te kunnen bestuderen. Bovendien, zoals gezegd, schatten wij in dat het lastig zou zijn om verkopers, gebruikers of slachtoffers van spionageproducten bereid te vinden om deel te nemen aan een focusgroep binnen het tijdsbestek van deze verkenning.

De twee focusgroepen die wij hebben gedaan zijn complementair aan elkaar, waarbij de een het perspectief van de gebruiker geeft en de ander het perspectief van de geobserveerde. De eerste focusgroep bestond aldus uit hobbydronevliegers en de tweede groep bestond uit personen die de privacy-inbreuken van het vliegen met drones regelmatig ondervinden: bewoners van de Kinderdijk molens. Ieder focusgroep had zes deelnemers. Daarbij was ons streven zes tot tien deelnemers, opdat de discussies genoeg ruimte konden krijgen en wij dieper op relevante punten in konden aan. Voor elke focusgroep hadden wij een aantal vragen geformuleerd om het gesprek te structuren; verder hadden de discussies een open vorm, om zo ook onvoorziene onderwerpen aanbod te kunnen laten komen. Elke focusgroep duurde ongeveer drie uur. De focusgroepen zijn opgenomen en er is van elke groep een verslag gemaakt. Deze verslagen zijn in het onderzoeksteam besproken.

2.4.1 Focusgroep hobbydrone vliegers

De hobbyvliegers werden met name benaderd door middel van berichten op sociale media (e.g. de Faceboek groep Drone vliegers Nederland en Vlaanderen en het online forum www.dronepilots.nl). Dat betekent dat deze focusgroep bestond uit deelnemers die vrijwillig deelnamen aan het gesprek en geïnteresseerd waren in het onderwerp.

Bij deze focusgroep lag de nadruk vooral op ervaringen met verantwoord vliegen en reguleringsmogelijkheden. Naast vragen gericht op privacy, ontwikkelingen op dronegebied en wet- en regelgeving hebben wij twee vignetten gebruikt om het met de deelnemers te hebben over wat er wel en niet mogelijk is met drones als het gaat om mensen bespieden (zie Bijlage III). Deze twee vignetten waren gebaseerd op voorbeelden uit onze literatuurstudie en de internet quickscans. Bovendien heeft een hobbydrone vlieger een filmpje laten zien van wat de verschillende soorten perspectieven die je vanuit de lucht met een drone hebt. Ook rondom dit filmpje vond een gesprek plaats over wat er mogelijk is met drones.

2.4.2 Focusgroep molenbewoners Kinderdijk

De tweede focusgroep betrof een zes burgers die reeds ervaring hadden met drones en reguleringsinterventies: de molenbewoners van Kinderdijk. Deze hebben wij telefonisch en via emailverzoeken benaderd met behulp van contacten in de gemeente. Bewoners hebben veel overlast van toeristen die drones gebruiken om de molens te filmen. Onlangs zijn er maatregelen genomen, zoals het plaatsen van borden. Alhoewel dit een tamelijk uitzonderlijk groep burgers betreft (er zijn maar weinig mensen in Nederland die in zo'n toeristische trekpleister wonen), verwachtten wij dat deze focusgroep inzicht kon bieden in de privacy impact van hobbydrones en de mogelijkheden voor het reguleren van het gebruik van drones boven een bepaald gebied. Onze inschatting was dat een dergelijke groep beter inzicht biedt in de privacy-impact van hobbydrones en in mogelijke mitigatiestrategieën dan een willekeurige groep mensen die over het algemeen nog weinig drone-observatie aan den lijve zullen hebben ondervonden.

Wij hebben voor deze focusgroep een beperkt aantal vragen rond privacy voorbereid, praktisch waarborgen die zij zelf hebben genomen en hoe zij aankijken tegen wet- en regelgeving. Voor deze focusgroep hebben wij geen vignetten gebruikt omdat wij genoeg ruimte wilden bieden aan de eigen ervaringen van de bewoners.

2.5 Rechtsverkenning

2.5.1 Juridisch-dogmatisch onderzoek

De analyse van de mate waarin het huidige wettelijke kader in Nederland de privacyrisico's van spionageproducten in enge zin en hobbydrones afdekt (deelvraag 4), hebben wij uitgevoerd middels klassiek juridisch-dogmatisch onderzoek. Dat wil zeggen dat wij een nauwgezette analyse hebben uitgevoerd van de wetgeving en jurisprudentie en van juridisch-wetenschappelijke literatuur. Waar nodig hebben wij daarbij de gebruikelijke wetsinterpretatiemethoden toegepast:

- grammaticale interpretatie, oftewel de betekenis van termen en begrippen in het algemene spraakgebruik;
- historische interpretatie, oftewel de betekenis van begrippen en bepalingen die voortvloeit uit opmerkingen en toelichtingen die tijdens de wetsgeschiedenis zijn gemaakt;
- teleologische interpretatie, oftewel de betekenis die in lijn is met de bedoeling van de wetgever bij de totstandkoming van de desbetreffende bepaling of wet.

Het onderzoek naar huidige wettelijke kaders richt zich op Nederlands recht, waaronder begrepen toepasselijk EU-recht (zoals de Algemene Verordening Gegevensbescherming). Wij concentreren ons op de rechtsgebieden die meest relevant kunnen zijn om horizontale privacyrisico's door spionageproducten in enge zin en hobbydrones te adresseren.

In de eerste plaats betreft dat de wetgeving betreffende privacy en gegevensbescherming, aangezien die vanzelfsprekend het meest direct bedoeld is om privacyrisico's te adresseren. Hieronder vallen de privacy-gerelateerde grondrechten van artikelen 10-13 Gw en art. 8 EVRM (waarbij voor horizontale verhoudingen met name de positieve verplichtingen van belang zijn) en het gegevensbeschermingsrecht: de AVG en de Nederlandse Uitvoeringswet AVG. Hierbij behandelen we niet allen de belangrijkste beginselen maar kijken we ook naar de reikwijdte in verband met de huishoudexceptie in burger-burger-relaties, evenals naar specifieke regels voor cameratoezicht door particulieren binnen het gegevensbeschermingsrecht.

In de tweede plaats behandelen we de rechtsgebieden die meer algemeen rechtsbescherming in horizontale relaties bewerkstelligen en daarbij ook privacybescherming (kunnen) bieden. Dat is ten eerste het materiële strafrecht, dat via de nodige strafbepalingen grenzen stelt aan het visueel of auditief observeren en het volgen van burgers door medeburgers. Vervolgens gaan we in op het specifieke rechtsgebied van het portretrecht, een onderdeel van het auteursrecht dat

onder bepaalde omstandigheden grenzen stelt aan het openbaar maken van afbeeldingen van personen. Daarna behandelen we het civiele onrechtmatigedaadsrecht, dat aanvullende rechtsbescherming kan bieden in situaties van privacy-inbreuken die niet onder specifieke bovenstaande wet- en regelgeving vallen.

In de derde plaats behandelen we wet- en regelgeving die niet direct bedoeld is om privacyrisico's te ondervangen, maar die van toepassing is of kan zijn op hobbydrones en daarbij (indirect) rechtsbescherming zou kunnen bieden tegen privacyrisico's van drones. Dit betreft de luchtvaartwetgeving die het recreatief gebruik van drones reguleert, bestaande uit zowel Nederlandse als Europese regelgeving. Verder kijken we nog naar gemeentewetgeving in de vorm van Algemene Plaatselijke Verordeningen (APV's), die ook bepalingen kunnen bevatten ter regulering van drones of spionageproducten. Naast de model-APV kijken we daarbij naar de APV's van enkele gemeenten met specifieke bepalingen om overlast van drones tegen te gaan.

2.5.2 Internationale rechtsverkenning

Voor de internationale rechtsverkenning (deelvragen 5 en 7) hebben wij een juridisch-dogmatische analyse gemaakt (vergelijkbaar met de in de vorige paragraaf genoemde methode) van wetgeving betreffende spionageproducten in enge zin in Duitsland en Frankrijk (om de in 2.2.3 genoemde redenen hebben we geen aanvullende internationale juridische analyse uitgevoerd met betrekking tot de regulering van drones). We hebben voor deze twee landen gekozen op basis van de resultaten van de eerdergenoemde internet quickscan naar wetgeving in diverse landen omtrent spionageproducten in enge zin, waarbij we gekeken hebben naar België, Denemarken, Finland, Ierland, Italië, Noorwegen, Rusland, Spanje, Verenigd Koninkrijk, Zweden en acht staten in de Verenigde Staten. Van deze landen bleken Duitsland en Frankrijk (voor zover vast te stellen viel in een beperkte quickscan) relevante wetgeving te hebben die het meest direct van toepassing is op spionageproducten in enge zin. Daarbij zijn deze landen interessant voor deze verkenning vanwege hun geografisch ligging (dichtbij Nederland) en omdat zij een vergelijkbaar rechtsstelsel hebben.

Uit de quickscan bleek dat Duitsland relevant is omdat §90 Telekommunikationsgesetz een verbod op spionageapparatuur kent, voor zover deze zend- of telecommunicatieonderdelen bevat.[21] In dat kader heeft het Bundesnetzagentur bijvoorbeeld een verbod op verkoop van kinderhorloges met een afluisterfunctie uitgevaardigd.

Verder bleek uit de derde quickscan dat Frankrijk interessant is om te onderzoeken omdat het als een van de weinig landen een vergunningstelsel voor spionageproducten in enge zin kent, met een strafbaarstelling van o.a. het zonder ministeriële toestemming produceren, bezitten,

[21] Zie 'Bundesnetzagentur takes action against children's watches with "eavesdropping" function', Bundesnetzagentur.de 7 april 2020

aanbieden of verkopen van producten die ontworpen zijn om op afstand gesprekken op te vangen en het mogelijk maken om privacy-inbreuken te plegen door het vertrouwelijk gesproken woord af te luisteren (art. 226-3 j^{o} art. 226-1 Code pénal).

2.6 Tot slot

De hierboven beschreven combinatie van onderzoeksmethoden stelt ons instaat om: (1) een overzicht te verkrijgen van de huidige stand van zaken en toekomstige ontwikkelingen op het gebied van hobbydrones en spionageproducten; (2) de privacyrisico's van het gebruik van deze producten globaal te beschrijven; (3) de toereikendheid en lacunes van bestaande reguleringsinstrumenten en praktische waarborgen voor het voorkomen en beperken van deze privacyrisico's te analyseren; (4) oplossingsrichtingen te formuleren voor het Nederlandse beleid om privacyrisico's door gebruik van spionageproducten (waaronder hobbydrones) te voorkomen of te beperken.

3 Spionage en spionageproducten

Drones, locatietrackers, minatuurcamera's en andere recent ontwikkelde spionageproducten zijn geen nieuw fenomeen, maar een nieuwe en steeds ingrijpendere verschijningsvorm van oude manieren waarop burgers andere burgers heimelijk observeren.[22] Zo kwamen met de opkomst van telegrammen en telefoons ook apparaten op de markt voor het onderscheppen van vertrouwelijke telefoon- en telegraafcommunicatie.[23] In het begin van de vorige eeuw werd er op grote schaal reclame gemaakt voor afluisterapparatuur voor telefoongesprekken en werden deze wereldwijd ook aan burgers verkocht.[24] Bedrijven en particulieren kochten ze om concurrenten, werknemers en echtgenoten te bespioneren.[25] Het aantal spionageproducten is sindsdien in verscheidenheid en verfijning toegenomen. In de jaren veertig en vijftig werden in de postordercatalogi locatiezoekers, spionagecamera's, afluisterapparatuur, en kleine bandrecorders verkocht.[26] Destijds kwamen er diverse afluisterapparaten in fantasierijke vormen op de markt: apparaten verborgen in martini olijven, handgrepen van koffers, oorbellen en dassluitingen.[27] Miniatuurafluisterapparatuur kon gesprekken uitzenden naar een ontvanger die zich een blok verderop bevond.[28] Parabolische microfoons konden stemmen oppikken zonder dat ze op het terrein werden geplaatst. Verkopers waarschuwden klanten om afluisterapparatuur te gebruiken 'volgens de wetten van uw gemeenschap'.

Sindsdien hebben de steeds lagere kosten van spionageapparaten de wijdverbreide adoptie ervan aangewakkerd. Bedrijven installeerden microfoons in de muren van toiletten en bureaus voor werknemers.[29] De modelwoningen en verkoopruimten voor auto's werden uitgerust met verborgen afluisterapparatuur om verkopers in staat te stellen de overpeinzingen van potentiële kopers af te luisteren.[30] Echtgenoten hielden in de gaten wat er zich afspeelde in de slaapkamers of in de kantoren van hun partners en wat voor gesprekken er via de telefoon werden gevoerd.[31] Vandaag de dag lijkt het repertoire van spionageproducten alleen maar te zijn uitgebreid.

---

[22] Zie D. Solove, *The future of reputation: gossip, rumor, and privacy on the internet*, New Haven: Yale University Press 2007 (waar hij de geschiedenis van de roddels onderzoekt).
[23] D. Citron, 'Spying Inc.' *Washington and Lee Law Review* 2015, p. 1253; zie ook S. Dash, *The intruders: unreasonable searches and seizures from King John to John Ashcroft*, New Brunswick: Rutgers University Press 2004 (beschrijving van de bewakingsapparatuur die in de loop van de geschiedenis is gebruikt).
[24] A. F. Westin, 'The Wire-Tapping Problem: An Analysis and a Legislative Proposal.' *Columbia Law Review*, vol. 52, no. 2, 1952, pp. 165–208.
[25] Ibid.
[26] A. Westin, *Privacy and freedom,* London: The Bodley Head 1967 (bespreking van de beschikbare bewakingsinstrumenten in de loop der decennia).
[27] Ibid.
[28] M. Brenton, *The privacy invaders*, New York: Coward-McCann 1964.
[29] S. Dash, *The intruders: unreasonable searches and seizures from King John to John Ashcroft*, New Brunswick: Rutgers University Press 2004, p. 84.
[30] Ibid.
[31] Ibid.

In dit hoofdstuk zetten wij uiteen wat te verstaan valt onder hedendaagse spionageproducten en maken wij een inventarisatie van het soort producten waar Nederlandse burgers tegenwoordig beschikking over kunnen hebben. Wij beginnen aldus met de beantwoording van onderzoeksdeelvraag 1: *Hoe kunnen spionageproducten worden gedefinieerd en geclassificeerd, met het oog op het vaststellen van relevante (verschillen in) privacyrisico's en aangrijpingspunten voor regulering?* En deelvraag 2: *Welke spionageproducten zijn—nu of in de voorzienbare nabije toekomst—te koop of anderszins beschikbaar voor het publiek, en kunnen aldus door burgers worden gebruikt?* Om tot een definitie en classificatie van spionageproducten te komen, moeten wij echter eerst kort het concept spionage verder verduidelijken, met name in verband met andere nauw verwante begrippen - overheidsspionage, surveillance en stalken. Dat doen wij in de volgende paragraaf. Daarna gaan wij over tot een definitie van spionageproducten en lichten wij de classificatie in spionageproducten in enge en brede zin verder toe. Tot slot, zal het antwoord op de twee deelvragen in een notendop worden weergegeven in de korte conclusie van dit hoofdstuk.

3.1 Spionage tussen burgers onderling

Spionage is een begrip met veel verschillende maar samenhangende betekenissen.[32] Het is bovendien nauw verbonden met andere soortgelijke en overlappende termen: overheidsspionage, surveillance en stalken.[33] Op basis van onze literatuurstudie belichten wij daarom een aantal van de verschillende betekenissen die aan 'spionage' worden toegekend alvorens wij verder benoemen wat wij verstaan onder spionage en spionageproducten in deze verkenning.

In algemene zin betekent spionage of spioneren het stiekem onderzoeken of achterhalen van geheimen.[34] De term wordt vooral gebruikt om de activiteiten te beschrijven van inlichtingendiensten en overheden die heimelijk informatie verzamelen in andere landen ter bevordering van hun nationale belangen.[35] In het dagelijks leven heeft de term echter ook een bredere betekenis. Het kan bijvoorbeeld refereren aan het heimelijk verzamelen van bedrijfsgeheimen om de eigen marktpositie te verbeteren of het stiekem verzamelen van informatie over de gedragingen van bepaalde burgers door andere burgers.

---

[32] Watson, PhD. Dit is te zien in de relatief weinige privacy papers over spionage, waarin diverse termen door elkaar worden gebruikt, zonder dat wordt uitgelegd hoe deze zich tot elkaar verhouden. Zie bijv. D. Citron, 'Spying Inc.' *Washington and Lee Law Review* 2015, p.1252 (over spionage, surveillance en stalking).
[33] Zo wordt in de OED-definitie van surveillance, bijvoorbeeld, verwezen naar spionage; zie 'Surveillance', Oed.com 7 april 2020.
[34] Van Dale Groot woordenboek van de Nederlandse taal, Utrecht: Van Dale 2015 (ook online). Zoek op: Spionage.
[35] De Algemene Inlichtingen- en Veiligheidsdienst van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties definieert spionage als "het op heimelijke wijze verzamelen van informatie door andere landen in en over ons land", zie 'Spionage', Aivd.nl 7 april 2020.

Zoals gezegd richten wij ons in deze verkenning uitsluitend op spionage tussen burgers onderling. Dit is geen concept dat uitgebreid wordt besproken in academische literatuur in vakgebieden als rechtsgeleerdheid, filosofie, politieke wetenschappen, privacy-theorie en surveillancestudies. [36] Zelfs wanneer de term wordt gebruikt om relaties tussen burgers onderling te beschrijven, wordt hij zelden gedefinieerd, alsof de betekenis ervan duidelijk en eenvoudig is.[37]

Een van de weinige privacy wetenschappers die over spionage tussen burgers onderling heeft geschreven is Anita Allen. Volgens haar is

> '[s]pioneren' het in het geheim in de gaten houden of onderzoeken van andermans overtuigingen, intenties, handelingen, nalatigheden of capaciteiten, vooral zoals die in anderszins verborgen of vertrouwelijke mededelingen en documenten naar voren komen.[38]

Allen hanteert een specifieke definitie door te stellen dat het gaat over geheime observatie van iemands 'overtuigingen, intenties, handelingen, nalatigheden of capaciteiten'. Als zodanig is deze definitie niet van toepassing op enkele andere manieren van informatieverzameling die mensen normaal gesproken zouden overwegen om te spioneren. Een van deze manieren is het in het geheim achterhalen van iemands *fysieke toestand*. Bijvoorbeeld, als Andrew in het geheim Brandons bloedtesten uit het verleden verwerft en te weten komt dat Brandon Hiv-positief is, heeft Andrew Brandon dan bespioneerd? [39] De meeste mensen zijn geneigd om 'ja' te zeggen. Toch is Andrew niet stiekem Brandons 'overtuigingen, intenties, handelingen, nalatigheden of capaciteiten' in de gaten aan het houden of aan het onderzoeken en dus, volgens Allen, niet aan het bespioneren.

Ronald Watson bouwt verder op Allen's definitie om een ruimere set van manieren van informatieverzameling onder spionage te laten vallen. Alhoewel de politiekfilosoof Watson schrijft over overheidsspionage, formuleert hij een meer algemene definitie die ook op spionage tussen burgers onderling van toepassing is:

---

[36] R. Watson, Spying: A Normative Account of the Second Oldest Profession (diss. St. Louis Washington University; All theses and dissertations) Missouri (V.S.): Washington University Open Scholarship 2013, p. 7.
[37] Zie bijv. F. Schoeman, *Philosophical dimensions of privacy: an anthology*, Cambridge: Cambridge University Press 1980; D. Lyon, *Surveillance studies: an overview*, Polity 2007 en D. Omand & M. Phythian, *Principled Spying: The Ethics of Secret Intelligence,* Oxford: Oxford University Press 2018.
[38] 'To 'spy' is secretly to monitor or to investigate another's beliefs, intentions, actions, omissions, or capacities, especially as revealed in otherwise concealed or confidential, communications and documents' (A. Allen, 'The Virtuous Spy: Privacy as an Ethical Limit'*, The Monist,* Vol 91, no. 1, 2008, p. 3); vertaling door M. Galič.
[39] Voorbeeld uit Watson, Spying: A Normative Account of the Second Oldest Profession (diss. St. Louis Washington University; All theses and dissertations) Missouri (V.S.): Washington University Open Scholarship 2013.

> ‘Agent A bespioneert agent B, wanneer en enkel wanneer zij informatie verzamelt die betrekking heeft op B en van plan is haar informatieverzameling voor B te verbergen.’[40]

In de definitie van Watson kunnen we vier verschillende componenten van spionage onderscheiden: (a) het subject (wie of wat bespioneert); (b) het object (op wat of wie de spionage wordt uitgevoerd); (c) de actie (wat het subject doet); en (d) de bedoelingen van het subject (het doel van het subject). Volgens Watson moet het subject een persoon zijn, maar kan de persoon ook spioneren voor een collectiviteit, zoals de overheid.[41] Om deze reden spreekt Watson van de individuele of collectieve ‘agent’ van spionage. De actie moet een soort van informatieverzameling zijn. Het kan verwijzen naar het visueel waarnemen, maar het kan ook andere vormen van observatie omvatten, ongeacht het betrokken zintuig. Het omvat ook het verzamelen van informatie met behulp van technologische middelen. De bedoeling van de spion is om informatie te verzamelen over het object van de spionage. In die zin is het algemene doel van spionage het verzamelen van informatie, hetzij voor goede, hetzij voor vijandige bedoelingen.

Voor zowel Watson als Allen hoeven de bedoelingen van de persoon die spioneert niet vijandig te zijn ten opzichte van het doel van de spionage.[42] Beide geven het voorbeeld van de goede bedoelingen van een ouder. Van een vader die in het geheim luistert naar de telefoontjes van zijn zoon omdat hij vermoedt dat hij drugs koopt of van plan is om niet naar school te gaan, kan worden gezegd dat hij een goede bedoeling heeft. Zijn motief kan eenvoudigweg zijn: het voorkomen dat zijn zoon zichzelf of anderen schade toebrengt. Toch zou het vreemd zijn om te zeggen dat de vader zijn zoon niet heeft bespioneerd, simpelweg omdat zijn bedoelingen niet vijandig waren. De intentie om te verbergen dat hij luistert naar de telefoongesprekken van zijn zoon lijkt in dit geval voldoende om zijn daden spionage te noemen, volgens Watson en Allen.[43]

Indien wij Watson’s definitie volgen, is de enige kernvoorwaarde voor spionage dan het opzettelijk verbergen van het doel van de spionage. Spionage is dus de combinatie van een actie en intentie. Echter, opzettelijke verhulling is niet noodzakelijkerwijs een succesvolle verhulling. Bijvoorbeeld als Sjoerd, de postbode, Marieke’s post leest en dit feit voor haar wil

---

[40] ‘Agent A spies on agent B, if and only if she collects information that relates to B and intends to conceal her information collection from B’ (Watson, Spying: A Normative Account of the Second Oldest Profession (diss. St. Louis Washington University; All theses and dissertations) Missouri (V.S.): Washington University Open Scholarship 2013, p. 7); vertaling door M. Galič.

[41] Voor meer informatie hierover zie Watson, Spying: A Normative Account of the Second Oldest Profession (diss. St. Louis Washington University; All theses and dissertations) Missouri (V.S.): Washington University Open Scholarship 2013.

[42] A. Allen, ‘The Virtuous Spy: Privacy as an Ethical Limit’*, The Monist,* Vol 91, no. 1, 2008; Watson, Spying: A Normative Account of the Second Oldest Profession (diss. St. Louis Washington University; All theses and dissertations) Missouri (V.S.): Washington University Open Scholarship 2013, p. 12.

[43] Watson, Spying: A Normative Account of the Second Oldest Profession (diss. St. Louis Washington University; All theses and dissertations) Missouri (V.S.): Washington University Open Scholarship 2013, p. 23.

verbergen, betekent dit niet noodzakelijkerwijs dat Marieke geen kennis heeft van Sjoerds daad. Sjoerd kan heel slordig zijn in het verbergen van zijn daden.[44] Bovendien hoeft de spion de informatieverzameling niet eindeloos te verbergen. De spion kan – en zal vaak – zijn spionage in de toekomst aan de geobserveerde onthullen. Dat Sjoerd op een bepaald moment in de toekomst zijn informatieverzameling aan Marieke wil onthullen, heeft geen invloed op de vraag of Sjoerd inderdaad heeft gespioneerd.

In dit rapport nemen wij Watson's brede definitie van spionage over om verschillende vormen van *heimelijke* observatie mee te kunnen nemen, waaronder goedaardige (of zelfs welwillende) en vijandige doeleinden, maar ook de observatie van fysieke conditie en locaties van personen, die niet onder Allen's nauwere definitie vallen. Deze brede definitie van spionage overlapt met het veelbesproken begrip 'surveillance'. In de volgende paragraaf gaan we daarom kort in op wat surveillance is en de relatie tussen spionage en surveillance.

3.1.1 Spionage en surveillance

Surveillance[45] wordt gewoonlijk gedefinieerd als 'nauwkeurige observatie, met name van een verdachte persoon' of als 'het zorgvuldig in de gaten houden van iemand of iets, met name om een misdrijf te voorkomen of op te sporen'.[46] De meeste surveillance wordt tegenwoordig echter niet specifiek toegepast op verdachten, maar alom en zonder onderscheid, op iedereen en in alle contexten - alle plaatsen, tijden, netwerken en groepen mensen.[47] David Lyon, een belangrijke surveillancetheoreticus, geeft als definitie van surveillance: 'de gerichte, systematische en routinematige aandacht voor persoonlijke details ten behoeve van invloed, beheer, bescherming of leiding'.[48] Vergelijkbaar met onze definitie van spionage, ziet Lyon surveillance als een kwestie van zowel zorg als controle.[49] Het subject van de surveillance wordt met een bepaald doel in de gaten gehouden, namelijk het controleren en disciplineren van de persoon in bepaald gedrag of een reeks normen, maar ook - tegelijkertijd mogelijk - het beschermen en verzorgen van de persoon in kwestie.

In tegenstelling tot spionage kan, maar hoeft surveillance niet geheim te zijn. Stelt u zich bijvoorbeeld voor dat een universiteit camera's installeert in kantoren en duidelijk aan het

---

[44] Voorbeeld uit Watson, Spying: A Normative Account of the Second Oldest Profession (diss. St. Louis Washington University; All theses and dissertations) Missouri (V.S.): Washington University Open Scholarship 2013, p. 22.
[45] Wij hanteren hier de Frans/Engelse term, omdat deze in academische zin een bredere betekenis heeft dan toezicht of bewaking.
[46] Gebaseerd op de Oxford English en Merriam-Webster woordenboeken.
[47] G. Marx, 'What's New About the "New Surveillance"? Classifying for Change and Continuity', *Surveillance & Society* (1) 2002, p. 10.
[48] D. Lyon, *Surveillance studies: an overview*, Polity 2007, p. 14. Haggerty en Ericson geven een vergelijkbare definitie: 'het verzamelen en analyseren van informatie over de bevolking met het oog op het controleren van hun activiteiten' (K. Haggerty en R. Ericson, 'The surveillant assemblage', *The British journal of sociology* Vol. 51, no. 4, 2000; vertaling door M. Galič).
[49] D. Lyon, *Theorizing surveillance: the panopticon and beyond*, Routledge 2006.

personeel verklaart dat men in de gaten wordt gehouden. Afgezien van kwesties met betrekking tot het recht op gegevensbescherming en het recht op privacy kan deze vorm van observeren door de universiteit door haar medewerkers als opdringerig worden ervaren. Deze vorm van waarneming kan daarom worden aangeduid als surveillance, maar kan niet worden gezien als spionage. Surveillance is dus een term die zowel heimelijke als openlijke observatie omvat, terwijl spionage alleen heimelijke observatie betreft.

3.1.2 Spionage en stalken

De laatste term die moet worden genoemd met betrekking tot spionage is ‘stalken’. Verschillende juristen en privacy wetenschappers die de privacyrisico's van drones of andere spionageproducten bespreken, betrekken stalken namelijk in hun discussie.[50] De term wordt ook vaak gebruikt in verband met apps en andere software, die kunnen worden gebruikt voor spionage (bv. lokalisatietracering) en die steeds vaker worden aangeduid als ‘stalkerware’ in plaats van ‘spyware’.[51] Om het onderscheid te verduidelijken, gaan we kort in op het begrip ‘stalking’ als Engels werkwoord, omdat de Nederlandse term ‘stalken’ afkomstig uit het Engels is.

De Oxford English Dictionary definieert het werkwoord ‘stalking’ als: ‘Het lastigvallen of achtervolgen (van een persoon, met name een publieke figuur) met ongewenste, obsessieve en meestal dreigende aandacht gedurende een langere periode’.[52] Een ‘stalker’ is dan een ‘persoon die een ander achtervolgt, met name in het kader van een onderzoek of met criminele bedoelingen; iemand die iemand anders (vaak een publieke figuur), met wie hij of zij geobsedeerd is geraakt, volgt of lastigvalt’.[53]

Er bestaat geen overeenstemming over de exacte definitie van stalking, maar waar het in wezen op neerkomt is dat iemand opzettelijk en herhaaldelijk wordt lastiggevallen door een andere persoon.[54] Stalking kan bestaan uit tal van verschillende activiteiten, zoals het volgen van een persoon, het voeren van telefoongesprekken, het sturen van ongewenste geschenken, iemands huis in de gaten houden, het bestellen van ongewenste goederen in naam en ten koste van iemand anders, het plaatsen van rouwberichten, het verspreiden van valse geruchten en het

---

[50] E.g. D. Citron, ‘Spying Inc.’ *Washington and Lee Law Review* 2015, p. 1243; R. Clarke, ‘The regulation of civilian drones’ impacts on behavioural privacy’, *Computer Law & Security Review Elsevier* 3, p. 290; U. Volovelsky, ‘Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study’, Computer Law & Security Review Vol. 30, no. 3 p. 318; B. Gonzalez, ‘Drones and privacy in the golden state’, Santa Clara Computer & High Tech. LJ Vol. 33, p. 297.
[51] Bijv. C. Parsons e.a., *The predator in your pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry* Munk school of global affairs & public policy, University of Toronto (2019); C. Khoo e.a., *Installing fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications* Munk school of global affairs & public policy, University of Toronto (2019).
[52] Artikel 285b Wetboek van Strafrecht; Merriam-Webster definieert stalking ook als "het obsessief en tot op het punt van intimidatie najagen".
[53] Artikel 285b Wetboek van Strafrecht.
[54] P. Mullen, ‘Stalking: New constructions of human behaviour’, 35 *The Australian and New Zealand journal of psychiatry* (1) 2001, p. 9.

vernielen van iemands huis.[55] Dit kan ook escaleren tot mishandeling of zelfs moord. Bovendien hoeven deze activiteiten niet noodzakelijkerwijs beperkt te blijven tot het slachtoffer. Familieleden, werkgevers, collega's, vrienden en kennissen kunnen ook het doelwit zijn van de stalker.[56]

Op basis van deze beschrijving wordt de relatie tussen ‘stalking’ en ‘spioneren’ duidelijk. Stalking kan betrekking hebben op een breed scala aan gedrag, waaronder geheime observatie met de bedoeling om informatie te verzamelen, dat wil zeggen ‘spioneren’. Beide begrippen impliceren een inbreuk op de privacy van een persoon. Echter is het uiteindelijke doel van de stalker een vorm van intimidatie en dus om uiteindelijk (vroeg of laat) de stalking aan de gestalkte persoon te onthullen. Spionage (en surveillance in het algemeen, verwijzend naar openlijke controle) kan daarom een door de stalker gebruikte methode zijn. Dit gebeurt dan ook vaak. Het is echter wel een methode die op zich nog niet als stalking kan worden beschouwd. Spionage kan wel het begin zijn van een hellend vlak dat uiteindelijk tot stalking leidt. Daarom is het belangrijk om het verband tussen spionage en stalking in gedachten te houden, met name bij het reguleren van spionageproducten.

3.2 Spionageproducten: twee typen

Nadat we het begrip spionage hebben gedefinieerd en hebben weergegeven hoe dit zich tot aanverwante concepten (‘surveillance’ en ‘stalking’) verhoudt, kunnen we nu overgaan tot de definitie en de classificatie van spionage*producten*. Ook deze classificatie heeft weer plaatsgevonden op basis van onze literatuurstudie. In de volgende paragrafen zullen wij, zoals gezegd, deelvraag 1 beantwoorden. Om dit te doen, gaan wij eerst nader in op wat wij verstaan onder spionageproducten en delen spionageproducten vervolgens op in twee hoofdgroepen: spionageproducten in enge en brede zin.

In deze verkenning verstaan wij onder een product een ‘technisch hulpmiddel’. [57] Maar wanneer is een product nu een *spionage*product? Enorm veel producten kunnen worden gebruikt om ‘heimelijk informatie over iemand’ te verzamelen. Het betreft niet alleen de nieuwste James Bond-snufjes of producten met ‘spy’ in de naam (zoals *spycams*), maar ook klassieke voorwerpen waarmee een persoon iemand kan bespioneren – denk aan de aloude verrekijker of aan het champagneglas waarmee door een hotelwand een gesprek kan worden afgeluisterd. In deze verkenning kijken wij naar de uitdagingen die ontwikkelingen op het gebied van digitale

[55] S. van der Aa, Stalking in the Netherlands: Nature and prevalence of the problem and the effectivenessof anti-stalking measures (diss. Tilburg University) Apeldoorn, Antwerpen, Portland: Maklu Uitgevers 2010, p. 31.
[56] Sinds de jaren negentig hebben veel landen stalking gecriminaliseerd. In het Nederlandse Wetboek van Strafrecht wordt het misdrijf stalking bijvoorbeeld in Artikel 285b gedefinieerd als: ‘het wederrechtelijk, stelselmatig, opzettelijk inbreuk maken op eens anders persoonlijke levenssfeer met het oogmerk die ander te dwingen iets te doen, niet te doen of te dulden dan wel vrees aan te wakkeren’.[56]
[57] Zie voor ‘technisch hulpmiddel’ ook Art. 6(1)(a)(i) Cybercrime-verdrag, CETS 185 en §72 Explanatory Memorandum.

technologie met zich meebrengen als het gaat om spionage tussen burgers onderling. Voor een eerste afbakening van de term spionageproducten sluiten wij daarom aan bij het begrip 'technisch hulpmiddel' zoals dit in de strafvordering wordt gehanteerd in het kader van stelselmatige observatie: het moet gaan om technische hulpmiddelen *die méér bieden dan alleen versterking van de zintuigen*.[58] Verrekijkers en gehoorapparaten vallen dus buiten het bestek van dit onderzoek.

De belangrijkste manier waarop hulpmiddelen meer doen dan alleen de zintuigen versterken, is registratie, dat wil zeggen de vastlegging van een beeld of geluid in een min of meer duurzame vorm die een authentieke weergave van het oorspronkelijke beeld of geluid mogelijk maakt. Het *vastleggen* van observaties vormt een privacyrisico bovenop het enkele geobserveerd worden; hiermee wordt de observatie immers potentieel beschikbaar voor een aanzienlijk grotere groep dan de observator zelf. Dit betekent dat fotocamera's en smartphones, die inmiddels standaard zijn uitgerust met camera's van hoge kwaliteit, ook voor spionage gebruikt kunnen worden. Een normale consumentencamera heeft tegenwoordig zo'n 20 tot 30 keer optische zoom, waarmee het mogelijk is om foto's en filmpjes van anderen te maken zonder dat zij dit in de gaten hebben. De smartphonecamera is eveneens geschikt om heimelijk personen te fotograferen, van kortere afstand dan met camera's mogelijk is, omdat het voor de geobserveerde vaak niet duidelijk zal zijn dat een smartphone in cameramodus wordt gebruikt.[59]

3.2.1 Onderscheid tussen twee typen spionageproducten

Fotocamera's en smartphone-camera's zijn ruim beschikbare hulpmiddelen om medeburgers heimelijk te observeren, maar zijn dit ook spionageproducten? Men kan er mee spioneren, maar zij lijken toch anders te zijn dan producten waarin een spionagemogelijkheid verwerkt zit die niet tot de reguliere functionaliteiten van dat product behoort, zoals een pen of petje waarin een mini-camera is ingebouwd of een bril waarin een richtmicrofoon is ingebouwd.[60]

Het onderscheidt tussen deze twee is van belang, met name als het gaat om regulering. Zoals eerder opgemerkt in hoofdstuk 1, vragen producten die niet ontwikkeld zijn voor spionage doeleinden een andere aanpak dan producten die dat wel zijn, als het gaat om de privacyrisico's van het *gebruik* van spionageproducten. In het bijzonder met het oog op de oorspronkelijke beleidsvraag naar een mogelijk vergunningstelsel voor *specifiek voor spionage bedoelde* producten, maken wij daarom een onderscheid tussen deze twee soorten producten:

---

[58] *Kamerstukken II* 1996/97, 25403, nr. 3, p. 27.
[59] Zie bijv. 'Pervert Alert: Japanese IPhone Shutter Sound Cannot Be Switched Off', Wired.com 8 april 2020.
[60] Dit lijkt ook de primaire behoefte van de opdrachtgever, gezien de verwijzing in de startnotitie naar de vraag uit de Initiatiefnota om onderzoek naar "een mogelijk vergunningenstelsel voor de verkoop van specifiek voor spionage bedoelde producten zoals *spy*-camera's en spionagesoftware".

a) Spionageproducten in enge zin: hulpmiddelen die *hoofdzakelijk ontworpen of geschikt gemaakt zijn* voor het heimelijk verzamelen van informatie over personen;

b) Spionageproducten in brede zin: hulpmiddelen die *gebruikt kunnen worden* voor het heimelijk verzamelen van informatie over iemand, maar waarvan zulke heimelijke informatievergaring *niet het hoofddoel* van ontwerp of gebruik is.

Ondanks dat de privacyrisico's voor beide typen producten voor een belangrijk deel vergelijkbaar zullen zijn, is het onderscheid tussen spionageproducten in enge en in brede zin met name voor de latere juridische analyse en de inventarisatie van de reguleringsmogelijkheden noodzakelijk. Hiermee blikken wij dus tevens vooruit op de onderzoeksvragen over overheidsregulering. Bij spionageproducten in enge zin is immers denkbaar dat de ontwikkeling, verkoop of verspreiding op een bepaalde manier wordt gereguleerd (regulering 'stroomopwaarts' oftewel bij de bron), terwijl bij spionageproducten in brede zin de regulering zich vermoedelijk eerder zal richten op het gebruik ervan (regulering 'stroomafwaarts', oftewel aan het eind).

3.2.2 Spionageproducten in enge zin

Spycams (spionagecamera's), miniatuurmicrofoons en GPS-trackers vallen onder spionageproducten in enge zin. Het zijn apparaten die in de eerste plaats zijn ontworpen of geschikt gemaakt zijn voor het op verschillende manieren – bijvoorbeeld door middel van video- en/of audiobewaking, thermische beeldvorming en locatiebepaling – in het geheim verzamelen van informatie over iemand. Hoewel onze definitie van spionage geen kwaadwillig doel vereist, brengt de algemene beschikbaarheid van spionageproducten in enge zin een voldoende hoog risico met zich mee dat ze kunnen worden gebruikt voor kwaadwillige doeleinden, met name met betrekking tot de privacy. Ze kunnen echter ook worden gebruikt voor andere kwaadwillige doeleinden, zoals drones die dieven helpen bij het inbreken in huizen of het helpen van personen bij het vinden van hun ex-partners om ze fysiek aan te vallen (stalking). Ook traceerapps en andere spionage-apps ('spyware') kunnen worden gedefinieerd als spionageproducten in enge zin. Deze softwareproducten stellen een gebruiker op afstand in staat om heimelijk gegevens over de activiteiten van een ander individu op een elektronisch apparaat te verkrijgen, door heimelijk gegevens van het apparaat naar een ander computersysteem door te sturen.[61]

3.2.3 Spionageproducten in brede zin

Een eerste onderscheid tussen spionageproducten in enge en brede zin is het doel waarvoor het product is ontwikkeld. Hobbydrones kunnen worden gezien als een voorbeeld van een

[61] C. Khoo e.a., *Installing fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications* Munk school of global affairs & public policy, University of Toronto (2019), p. 16.

spionageproduct in brede zin. Dit op afstand bestuurde, onbemande luchtvaartuig wordt doorgaans voor recreatieve of professionele doeleinden gebruikt, bijvoorbeeld om mooie beelden te schieten van natuurgebieden of om daken te inspecteren.[62] Drones zijn meestal uitgerust met een camera, maar kunnen ook andere sensoren dragen zoals microfoons of infraroodcamera's. Zij kunnen dan ook worden beschouwd als apparaten die kunnen worden gebruikt voor het in het geheim verzamelen van informatie over iemand. Dergelijke informatieverzameling is echter niet het hoofddoel van het ontwerp of gebruik van het apparaat. In die zin vallen hobbydrones onder spionageproducten in brede zin.

Hiermee samenhangend is een verschil met spionageproducten dat er een bedoeling is om te spioneren. Personen hebben over het algemeen niet standaard een spionagecamera of afluisterapparatuur bij zich. Pas nadat de persoon zich heeft voorgenomen om te spioneren, zal deze persoon het spionageapparaat in enge zin dragen en gebruiken. Dat hoeft niet het geval te zijn bij spionageproducten in brede zin, zoals een zoomlenscamera, hobbydrone of een smartphone. Mensen hebben doorgaans hun smartphone dagelijks op zak en kunnen hun hobbydrone in de rugzak meenemen, bijvoorbeeld, op toeristische tripjes, zodat de spionageactiviteit spontaan kan plaatsvinden, 'wanneer zich een goede gelegenheid voordoet'. In die zin worden de privacyrisico's versterkt, omdat het spionageapparaat op elk moment kan worden ingezet.

Een derde onderscheid tussen spionageproducten in enge en brede zin heeft betrekking op de sensoren en de vorm van de drager. Spionageproducten in brede zin, zoals drones, maar ook smartphones, worden geleverd met sensoren (of payloads) die al in het apparaat (de drager) zijn ingebouwd (bv. een drone met een camera), maar sensoren kunnen ook aanvullend op het apparaat worden gemonteerd (bv. montage op een drone van een microfoon, infraroodcamera, stemspanningsanalysator of het inbouwen van een extra mogelijkheid in de software, zoals een tracking functionaliteit). Daarentegen kunnen spionageproducten in enge zin meestal geen extra payload hebben, met name vanwege de beperkte afmetingen. Deze apparaten zijn bedoeld om onopgemerkt te blijven en zijn dus zeer klein van formaat. In plaats daarvan bestaat hun oorspronkelijke ontwerp over het algemeen uit een of twee soorten sensoren, bijvoorbeeld een camera of een microfoon.

Een vierde onderscheid ten opzichte van spionageproducten in enge zin betreft de verschijningsvorm. De drager bij spionageproducten in brede zin heeft doorgaans de vorm van het primaire apparaat, zoals bijvoorbeeld een smartphone een rechthoekig blokje is en een drone de vorm van een dunne kleine rechthoek heeft, meestal met vier kleine rotoren, waardoor de drone kan vliegen. Als zodanig zijn ze vrij gemakkelijk herkenbaar. Spionageproducten in

---

[62] B. Custers & e.a., *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Amsterdam: Boom Lemma Uitgevers 2015.

enge zin komen daarentegen in een grote verscheidenheid aan vormen voor. Ze kunnen de vorm hebben van hangers, armbanden, sleutelhangers, glazen, gehoorapparaten, rookmelders, pennen, aanstekers en zelfs een martini olijf. [63] Spionageproducten in enge zin maken dus gebruik van de vorm en het ontwerp van een ander veel gebruikt product om het spionagedoel ervan te verhullen. Enkele van de meest voorkomende dragers en kenmerken van spionageproducten in enge zin bespreken we verder in de volgende paragraaf (3.3), wanneer we de verschillende producten die momenteel beschikbaar zijn voor Nederlanders onderzoeken.

Het onderscheid tussen spionageproducten in enge en brede zin is van belang vooral wanneer wij later in deze verkenning kijken naar de lacunes in de rechtsbescherming en reguleringsmogelijkheden, omdat er specifieke wetgeving van toepassing kan zijn op bepaalde dragers van spionagesensoren (zoals drones) en/of omdat reguleringsopties verschillen afhankelijk van het type drager of gebruik. Opties om hobbydrones als drager van sensoren zoals camera's of tracking-software te reguleren, zullen immers substantieel verschillen van reguleringsopties voor spionageproducten in enge zin zoals *spycams* verborgen in pennen of horloges.

3.2.4 Spionageproducten op het grensvlak

Bij het bovenstaande onderscheid tussen spionageproducten in enge en brede zin dat wij in deze verkenning hanteren, moet worden opgemerkt dat de scheidslijn niet altijd scherp te trekken is. Denk bijvoorbeeld aan een *smartwatch* (een slim horloge), zoals afgebeeld in Afbeelding 1, met een geïntegreerde camera en microfoon. Dit is een breed beschikbaar product. Een smartwatch kan het best omschreven worden als een spionageproduct tussen de enge en brede zin van het woord in. In eerste instantie is men geneigd het te beschouwen als een spionageproduct in brede zin. Het is namelijk in de eerste plaats een horloge, dat ook voor spionage kan worden gebruikt. Deze redenering is echter discutabel. De extra functies van een smartwatch kunnen namelijk op den duur even belangrijk (of minstens even belangrijk) worden als het bijhouden van de tijd. Een soortgelijke ontwikkeling hebben we eerder gezien bij mobiele telefoons. Omdat mobiele telefoons naast het bellen, vooral met de introductie van de smartphone, steeds meer functies hebben gekregen, is hun belangrijkste functie veranderd van het ontvangen en doorsturen van gesprekken naar het functioneren als een kleine, draagbare computer. Maar waar smartphones tegenwoordig tal van functies mogelijk maken (van het versturen van e-mails, het bekijken van films, het luisteren naar muziek en het maken van video- of spraakopnamen), blijven de mogelijkheden van een smartwatch veel beperkter. In die zin kunnen we het opnemen van beelden, video's en geluiden beschouwen als een van de belangrijkste functies van de smartwatch, naast het bijhouden van de tijd. De smartwatch is

[63] Zie bijv. Westin, *Privacy and freedom,* London: The Bodley Head 1967, p. 70.

echter geen spionageproduct in enge zin: hij is niet ontworpen of wordt niet vooral gebruikt voor spionage.

De smartwatch is wel vergelijkbaar met spionageproducten in enge zin omdat het bijna niet te onderscheiden is van gewone horloges. In tegenstelling tot de “niet-smart” mobiele telefoons, die steeds zeldzamer worden, komen gewone horloges nog steeds veel voor. Hoewel deze mobiele telefoons qua ontwerp aanzienlijk verschillen van smartphones (en als zodanig gemakkelijk te onderscheiden zijn), verschillen slimme horloges met de ingebouwde functies van video- en geluidsregistratie niet in ontwerp van gewone horloges (zie bijvoorbeeld het Time Berlin smartwatch in Figuur 3.1 hieronder).[64] Daardoor is het bijna onmogelijk om een horloge dat in staat is om te spioneren, te onderscheiden van een gewoon horloge zonder dergelijke functionaliteit.

Voor een product zoals de smartwatch is het dus lastig een scherpe scheidslijn te trekken. De classificatie in brede en enge zin zou dus in de toekomst kunnen worden aangevuld met een classificatie in termen van verminderde zichtbaarheid (bijvoorbeeld beginnend met drones, gevolgd door een smartphone, een smartwatch en tenslotte een typisch spionageproduct in de vorm van een pen of een knop). In deze verkenning hanteren wij, zoals gezegd, echter het onderscheid tussen spionageproducten in enge en brede zin, om te benadrukken dat hobbydrones ook als spionageproduct ingezet kunnen worden.

[64] Zie daarom het voorstel om alle horloges tijdens examens in het Verenigd Koninkrijk te verbieden: ‘Ban all watches from exams to stop cheating’, Bbc.com 8 april 2020.

FIGUUR 3.1: 'TIME BERLIN' SMART WATCH MET INGEBOUWDE VIDEOCAMERA EN MICROFOON (ZOALS BESCHIKBAAR OP VLUCHTEN VAN AUSTRIAN AIRLINES; FOTOCREDIT MAŠA GALIČ, 31 AUGUSTUS 2019)

3.3 Spionageproducten in enge zin: een overzicht

In deze en de volgende paragraaf beantwoorden wij deelvraag 2: *Welke spionageproducten zijn—nu of in de voorzienbare nabije toekomst—te koop of anderszins beschikbaar voor het publiek, en kunnen aldus door burgers worden gebruikt?* Wij geven in deze paragraaf een overzicht van spionageproducten in enge zin die voor burgers beschikbaar zijn. Dit overzicht is gebaseerd op de literatuurstudie en de internet quickscan die wij hebben uitgevoerd naar de (online) verkoop van spionageproducten' (zie hoofdstuk 2). Wij richten ons hierbij met name op de Nederlandse markt, waaronder fysieke winkels, online internetwinkels die gespecialiseerd zijn in de verkoop van spionageproducten[65] en algemene online internetwinkels.[66]

Aan de hand van de quickscan vonden wij zes fysieke winkels in Nederland (in Amsterdam, Weesp, Nieuwegein, Rotterdam, Breda en Utrecht), waarvan er drie van hetzelfde bedrijf zijn. Alle winkels bieden verschillende soorten spionageproducten aan met name voor bewakings- en beveiligingsdoeleinden, maar ook voor spionage. Zo bieden deze winkels bewakingscamera's aan maar ook miniatuur opnameapparatuur. Alle fysieke winkels bieden hun producten ook aan

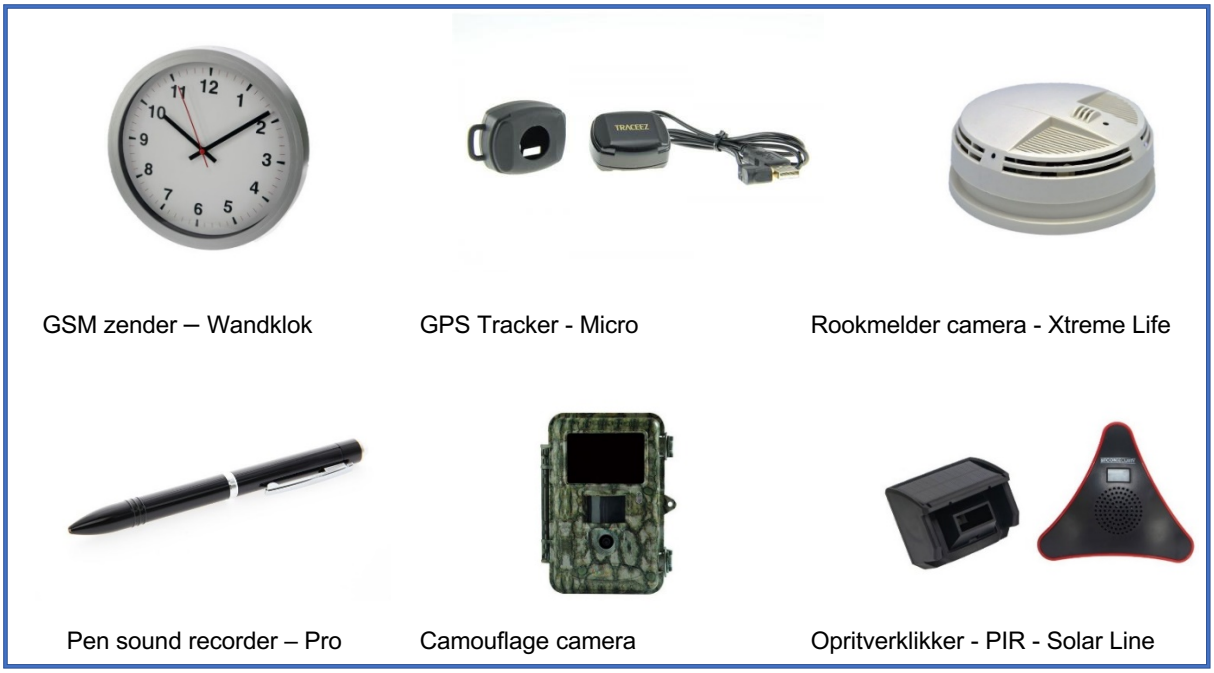
[65] Bijv. Gabstore.nl; Sitconsecurity.nl.
[66] Bijv. Bol.com; Mediamarkt.nl; Beslist.nl en Marktplaats.nl.

via hun eigen webshop.[67] We geven daarom in het onderstaande overzicht alleen de producten die in online webwinkels beschikbaar zijn weer.

Online vonden wij meer aanbieders van spionageproducten in enge zin. In Nederland kwamen we tot een lijst van 28 sites die zich specifiek richten op spionageproducten (online spyshops), waarvan er 11 waren terug te leiden tot een bedrijf. De online spyshops bieden naast spionageproducten doorgaans ook, en soms hoofdzakelijk, beveiligingsproducten aan zoals alarmsystemen, beveiligingscamera's, kluizen en sloten. Wij vonden verder ook spionageproducten in de volgende algemene online winkels specifiek gericht op Nederland: bol.com, beslist.nl en marktplaats.nl. Ook op Amazon.de konden dergelijke producten besteld worden van uit Nederland. In de Apple Store (IOS) en de Play Store (Android) worden verschillen spionage apps aangeboden aan Nederlandse gebruikers.

Op basis van de quickscan van de online winkels hebben wij de aangeboden spionageproducten onderverdeeld in vier soorten producten, die het meest voorkomen op de websites van de door ons onderzochte online winkels in vergelijking met andere soorten producten op deze websites: (1) spycams, (2) verborgen microfoons, (3) GPS-trackers en (4) anti-spionageproducten. Deze categorisering wordt doorgaans ook door verkopers zelf gebruikt.[68] Zie tabel 3.1 voor een overzicht van het aantal producten per categorie en per online spyshop en Figuur 3.2 voor enkele voorbeelden van spionageproducten. Daarnaast waren er ook andere soorten spionageproducten die andere vormen van observatie voor burgers mogelijk maken. Zoals draagbare 'voice-stress analyzers', geur- en feromoondetectoren die inzicht kunnen geven in iemands gemoedstoestand, en chemische sensoren die kunnen bepalen wat iemand doorspoelt en wegspoelt.[69] Deze vormen echter maar een relatief klein deel van het aanbod in de onderzochte online winkels.

[67] In Amsterdam moeten fysieke 'spyshops' sinds september 2019 onder een vergunning opereren en ook in andere steden, zoals Breda, bestaan er plannen voor vergunning. Zie paragraaf 5.3. Zie 'Gemeenteblad van Amsterdam: Aanwijzingsbesluit vergunningsplicht voor spyshops, gemeente Amsterdam' Zoek.officielebekendmakingen.nl 8 april 2020; 'VVD Breda wil vergunning spy shop. Daar zeggen ze: 'Als het moet, dan moet het', Bndestem.nl 8 april 2020. De vergunningsplicht in Amsterdam was naar aanleiding van een liquidatie van een spyshop eigenaar en het vermoeden dat deze winkels (zware) criminaliteit faciliteren.
[68] Sitcon.nl; Spyshop4u.nl; Eyepopper.nl; Megaspyshop.nl; Gadget-plaza.nl; Spycity.nl; Spy3k.nl; Gabstore.nl; Spywebshoposs.nl.
[69] Denk ook aan DNA-kits of online DNA-bedrijven waarmee – bijvoorbeeld op basis van iemands speeksel- of bloedsporen die heimelijk met een wattenstaafje worden opgenomen – iemands genoom in kaart kan worden gebracht om medische of afkomstgegevens uit af te leiden; of biometrische inbreuken, zoals het namaken van vingerafdrukken om identiteitsfraude te plegen. Deze laatste categorie (rond lichamelijke privacy) roept volgens ons wel belangrijke vragen rond onderlinge privacy op, maar die zijn veelal van een andere aard en vergen andere reguleringsinterventies dan het heimelijk maken van beelden of geluidsopnamen.



FIGUUR 3.2VERSCHILLENDE SOORTEN BESCHIKBARE SPIONAGEPRODUCTEN (VAN SITCON.NL)

Aantal artikelen per website	Spycams	Afluisterapparatuur	GPS-trackers	Anti-spionage apparatuur
1. https://www.sitconsecurity.nl/[70]	105	20	15	39
2. https://spyshop4u.nl/	26	14	5	3
3. https://www.eyepopper.nl/	2	7	15	4
4. https://www.spyshop.nl/#nl/p/home.html	20	13	5	4
5. https://www.megaspyshop.nl/	51	9	13	15
6. https://www.gadget-plaza.nl/spy-gadgets	57	17	4	3
7. https://www.spycity.nl/	12	7	8	9
8. https://www.spyshopbreda.nl/	98	19	24	10
9. http://www.spy3k.nl/	23	19	12	20
10. https://www.gabstore.nl/	98	38	34	x
11. https://www.spywebshoposs.nl/nl	52	29	6	6
12. https://www.lockpickshop.nl/	7	4	7	4

[70] Zelfde assortiment als https://www.spywebshop.nl/, https://www.spycamerashop.nl/, https://www.spygadgetstore.nl/, https://www.detectiveshop.nl/, https://www.afluisterapparatuurshop.nl/, https://www.spy-shop.info/spy-cameras/, https://www.spycamera.nu/, https://www.draadlozecamerashop.nl/, https://www.bewakingscameraspecialist.nl/, https://www.spyphoneshop.nl/.

13. https://www.topsjop.nl/	21	1	-	-
14. https://www.kabelshop.nl/Camera-s/Spy-cameras-p9870.html	9	-	-	-
15. https://www.epine.nl/camerashop/spy-camera/[71]	26	-	-	-
16. https://www.camerashop24.nl/	3	-	-	-
17. https://www.beveiligingswinkel.nl/	17	-	-	-
18. https://www.onlinecamerashop.nl/	46	12	6	-
Totaal	673	209	154	111

TABEL 3.1: OVERZICHT SPIONAGEPRODUCTEN PER AANBIEDER

1. Spycams

Het merendeel van de aangeboden spionageproducten zijn spycams.[72] De aangeboden producten met daarin een camera kunnen worden onderverdeeld in drie hoofdcategorieën, namelijk alledaagse (vaste) objecten in huis, verplaatsbare/draagbare objecten en objecten voor in voertuigen. Onder alledaagse objecten in huis hebben we de volgende artikelen gevonden: bluetooth speaker, klok, rookmelder, adapter, balpen, blackbox, computer muis, lasdoos, pinhole camera, afstandsbediening, plantenbak, stick camera, gsm-alarm camera, spiegel camera, infraroodcamera, 3GP camera, sprinkler design-camera, bewakingscamera, deurspion camera en mini spy LEDs. De verplaatsbare of draagbare objecten bestaan uit: sleutelhanger, horloge, bril, aansteker, USB-camera, knop-type camera, powerbank, notitieboek, koptelefoon, koffie deksel, handtas camera, koptelefooncamera en de portable touchscreen. Daarnaast zijn er enkele spionagecamera's voor in een voertuig, zoals de auto USB-camera en de telefoonhouder. Daarnaast zijn twintig van de honderdvijf artikelen (inclusief de bluetooth speaker, klokcamera, blackbox, powerbank, lasdoos, sleutelhanger, knoopcamera en rookmelder) te gebruiken via Wi-Fi en kunnen de artikelen worden gekoppeld aan een app, zowel beschikbaar voor iOS als Android. De prijzen voor spycams kunnen uiteenlopen van enkele tientjes tot meer dan duizend euro. Zo kan men al een pen met camera kopen voor rond de 30 euro en zijn er wandklokken met camera's beschikbaar van ongeveer 150 euro. Een professionele knoopcamera kan al snel 1100 euro kosten.

[71] Epine.nl; Camerashop24.nl; Beveiligingswinkel.nl; Onlinecamerashop.nl; zijn online winkels gericht op de verkoop van (beveiligings)camera's.
[72] De 28 websites bieden in totaal 673 verschillende spionagecamera's aan. De grootste retailer van spionagecamera's is SITCON, met in totaal 105 artikelen; zie Sitconsecurity.nl.

2. Afluisterapparatuur

Na de spionagecamera wordt afluisterapparatuur het meest aangeboden op de websites. Om een idee te geven van het soort apparatuur dat wordt aangeboden, nemen wij hier de gespecialiseerde online winkel Gabstore.nl als voorbeeld. Deze winkel maakt onder de kop 'audio monitor om mee te luisteren' een onderverdeling in meeluisteren via de telefoon, stemrecorders en muurmicrofoon/richtmicrofoon. Het meeluisteren via de telefoon is mogelijk via onder andere een klok (zie Figuur 3.1), powerbank, asbak, rekenmachine, fotocamera, rookmelder, computermuis, stekkerdoos of wereldstekker met ingebouwde gsm-module. Ook zijn er verschillende monitors beschikbaar die zowel audio als video opnemen, en enkele hebben ook nog een geluids- of bewegingssensor. Het goedkoopste product om mee te luisteren via de telefoon is een mini-monitor van 55 euro en het duurste product is een stekkerdoos van 139 euro. Gabstore.nl kent ook verschillende stemrecorders. Veelal zijn deze in de vorm van een USB-stick, maar ook zijn ze beschikbaar als hanger, sleutelhanger of pen. De stemrecorders die deze winkel aanbiedt zijn veelal draadloos en hebben een opslagcapaciteit voor meer dan 20 opnames. De prijzen lopen uiteen van 40 tot 160 euro. Daarnaast bestaat er nog een aanbod van verschillende muur- en richtmicrofoons. Deze zijn ook voor enkele tientjes tot 200 euro te koop. Andere online spyshops bieden soortgelijke producten aan waarbij de prijzen kunnen oplopen tot 1000 euro.

3. GPS-trackers

Het derde meest voorkomende spionageproduct dat online te koop is, is de GPS-tracker. Gabstore.nl, bijvoorbeeld, maakt bij de GPS-trackers een onderverdeling in persoonlijke GPS-trackers, GPS-trackers voor huisdieren, GPS-trackers voor voer/vaartuigen en GPS-locatie bepaling. De persoonlijks GPS-trackers bestaan uit GPS-tracker in hangers, (mini) monitors, sleutelhangers, USB sticks en kinderhorloges.[73] Sommige van deze trackers hebben naast een volgfunctionaliteit nog andere functionaliteiten, zoals een terugbelmogelijkheid, een SOS knop of een valdetectie functie. De SOS-knop kan gebruikt worden om direct contact op te nemen met telefoonnummers die in de tracker zijn opgegeven. Met een app op een mobiele telefoon kan men zien waar de GPS-tracker zich bevindt tot op een paar meter nauwkeurig. Ook kan er met behulp van een app een gebied ingesteld worden waarbinnen de tracker moet blijven. Als de tracker buiten dit gebied komt, wordt er een bericht gestuurd naar de opgegeven mobiele nummers. Gabstore.nl beschrijft diverse mogelijke gebruiken voor de persoonlijke trackers, zoals het terugvinden van personen en of objecten. "Ideaal voor kinderen en senioren", aldus de site.[74] De GPS-trackers voor huisdieren komen in de vorm van een hondenhalsband en een waterdichte GPS-tracker.[75] GPS-trackers voor voer/vaartuigen bestaan uit een jack, USB stick,

[73] Gabstore.nl
[74] Gabstore.nl, zoek op: GPS tracker hanger.
[75] Gabstore.nl, zoek op: GPS trackers voor huisdieren.

monitor en volgsystemen.[76] De GPS-locatie bepaling bestaat uit een display in een sleutelhangerbehuizing.[77] Andere websites bieden soortgelijke GPS-trackers aan. De prijzen van GPS-trackers lopen uiteen van enkele tientjes tot duizenden euro's.

4. Anti-spionageproducten

Het laatste type producten dat hier vermeld dient te worden, zijn anti-spionageproducten. Technisch gezien kunnen deze producten niet als spionageproducten worden beschouwd, maar we noemen ze hier wel zo omdat ze een belangrijke rol spelen als het gaat om de risico's voor de horizontale privacy die spionageproducten met zich meebrengen. Als individuen zich namelijk gemakkelijk kunnen beschermen tegen de spionage van andere burgers, in ieder geval tegen bepaalde vormen van spionage, kan de behoefte aan regelgeving kleiner zijn. Desalniettemin is het aanbod van deze producten op dit moment nog vrij beperkt. De meeste anti-spionageapparatuur die aangeboden wordt bestaat uit zender-/gsm-/camera-/tracker-/simkaartdetectoren, en de beveiligingstas (die alle signalen naar de telefoon blokkeert). Overige artikelen bestaan uit de spectrum analyzer, cameralens zoeker, stemvervormer, ruisgenerator, signaal blokkeer folie, 'reverse peephole viewer', 'laser defeater', gecodeerde USB-stick, stekkerdoos *bug-detector*, EMF meter, GMS-safe, spionagetelefoon detector, anti-afluister plug, privacy router en de privacy USB-stick. Ook hier weer lopen prijzen uiteen van enkele tientjes tot duizenden euro's. Zo heb je al signaalblokkeerfolie voor 30 euro, een cameralensvinder voor 100 euro, en kan een professionele Spectrum Analyser bijna 10.000 euro kosten.

3.4 Hobbydrones als spionageproducten in brede zin

In deze paragraaf beantwoorden wij deelvraag 2 voor zover het gaat over hobbydrones. We beschouwen hobbydrones, zoals gezegd, in deze verkenning als spionageproducten in brede zin en bespreken daarom ook wat er mogelijk is met hobbydrones vanuit dit perspectief. Om in het volgende hoofdstuk ook een inschatting te kunnen maken van de privacyrisico's van deze drones, geven we ook een kort overzicht van het gebruik van drones in Nederland. Dit overzicht van het aanbod en gebruik van drones is gebaseerd op de resultaten uit de literatuurstudie, interviews, en focusgroep met hobbydronevliegers (zie hoofdstuk 2).

In Nederland bestaat al een lange traditie van het vliegen met op afstand bestuurbare modelluchtvaartuigen. Hobbydrones zijn een relatief nieuwere ontwikkeling. Het gaat hierbij om op afstand bestuurbare luchtvaartuigen met vier of meer propellers. Op de meeste drones kunnen sensoren, zoals camera's of microfoons worden bevestigd en veel drones hebben een

[76] Gabstore.nl, zoek op: GPS tracker voor voer/vaartuigen.
[77] Gabstore.nl, zoek op: GPS locatie bepaling.

ingebouwde camera. Alhoewel ze primair bedoeld zijn voor recreatieve doeleinden, zoals vliegen en fotografie, kunnen ze ook ingezet worden voor spionage doeleinden.

Op recreatief gebied worden drones op verschillende manieren gebruikt. Ze kunnen worden gebruikt om binnens- en buitenshuis te vliegen. Veel mensen zullen een drone kopen om mee te spelen, maar er is ook een grote groep mensen die met drones vliegen om foto's en filmpjes te maken. Aangezien er in Nederland boven de bebouwde kom niet gevlogen mag worden (waarover later meer in paragraaf 5.5), zijn dit vooral beelden van landschappen. Sommige mensen doen dit voor eigen gebruik, maar andere hobbyisten plaatsten de beelden ook online op hun eigen website of op sociale media. Er zijn verschillende websites en sociale mediagroepen speciaal gericht op deze recreatieve gebruikers. Daarnaast is er sinds kort ook een groeiende groep gebruikers die drones gebruiken voor het maken van *selfies*; oftewel foto's van zichzelf. Tot slot is er een groep mensen die racen met drones. De drones die hiervoor gebruikt worden, worden veelal met behulp van een virtual-reality bril en *first-person-view* (FPV) camera's (camera's die direct *streamen* naar een VR-bril of andere monitor) bestuurd in afgesloten omgevingen. Tot slot, zoals onder andere blijkt uit onze interviews, is er ook een groep gebruikers die de drones gebruiken voor het heimelijk observeren van personen of privéruimtes. Zo worden de drones gebruikt voor voorverkenningen voor inbraak en om bij huizen binnen te kijken.[78]

Drones hebben verschillende vormen maten, gewichten en prijsklassen, variërende van de professionele grotere en zwaardere drones tot simpelere kleine lichtgewicht drones (nano-drones). Er zijn drones beschikbaar met vier, zes of acht propellers, waarbij geldt dat hoe meer propellers hoe stabieler de drone. De nano-drones zijn doorgaans maar een paar honderd gram en passen in de palm van een hand. Ze zijn bedoeld als speelgoed en hebben niet altijd een camera, al zijn er ook drones van een paar honderd gram met een (FPV) camera. Deze drones hebben een relatief korte vliegtijd van zo'n vijf tot tien minuten.[79] Vooral vanwege hun gewicht zijn ze zeer gevoelig voor de wind en er kan dus niet altijd buiten mee gevlogen worden. Sinds kort zijn er ook drones die speciaal gemaakt zijn om *selfies* te maken. Dit zijn lichtgewicht drones die op een klein afstandje van een persoon blijven vliegen om foto's van de persoon te maken.[80]

Uit de focusgroep met hobbydronevliegers en de interviews blijkt dat de drones die veel gebruikt worden door hobbydronevliegers vaak wat groter en zwaarder zijn, waardoor ze beter bestuurbaar zijn en uitgerust kunnen worden met een betere camera met meer functionaliteiten (b.v. een zoomlens) en sterkere batterijen. Dergelijke drones kunnen ongeveer een half uur vliegen. Een in 2019 uitgekomen populaire drone - speciaal gemaakt voor de vlieger die graag

[78] Er zijn bijvoorbeeld gevallen gerapporteerd in de media van drones die voor een slaapkamerraam hangen. Zie bijvoorbeeld 'Drone gluurt door het slaapkamerraam', Ad.nl 8 april 2020.
[79] Airdronecraze.nl, zoek op: Looking for a new nano or mini drone?
[80] Zie bijvoorbeeld Airselfiecamera.com, zoek op: Air pix.

foto's of video's maakt - weegt minder dan 250 gram en is uitgerust met een camera.[81] Deze drone kan worden opgevouwen en in een grote jaszak of rugtas meegenomen worden. Maar de vliegers uit de focusgroep vliegen ook met drones die een of twee kilo kunnen wegen. Ook op fora voor recreatieve gebruikers zijn er vliegers met zwaardere drones.[82] De drones die voor professionele doeleinden worden gebruikt, zijn doorgaans wat groter en zwaarder (meerdere kilo's) dan de recreatieve drones.

De mogelijkheden en functionaliteiten van de verschillende soorten drones kunnen sterk variëren. Zo zijn er drones die uitsluitend kunnen vliegen doordat ze op afstand bestuurd worden met behulp van een *controller* of *smartphone app*, maar er zijn ook drones die zelf kunnen opstijgen en landen of bepaalde manoeuvres in de lucht kunnen uitvoeren. Over het algemeen worden drones aangestuurd via wifi-(of radio)signalen en hebben daardoor een beperkt bereik en zijn daardoor redelijk kwetsbaar. Veel drones hebben een *geofencing* functionaliteit die op basis van locatiedata het gebied softwarematig begrenst waarin de drone kan vliegen.[83] Zo kan een drone uitgerust met deze functionaliteit bijvoorbeeld automatisch buiten een no-fly zone blijven, zoals bijvoorbeeld in de buurt van vliegvelden. Daarnaast zijn veel drones uitgerust met een *return-to-home* functie, voor als het signaal wegvalt (of als de accuspanning beneden een bepaalde waarde komt).[84] De drone vliegt dan zelfstandig terug naar het startpunt van de vlucht. Sommige drones kunnen zelfs vooraf geprogrammeerde routes afleggen, ook als er geen signaal is. Momenteel zijn dat vooral de duurdere professionele drones. Omdat drones tegen objecten aan kunnen vliegen, zijn ze steeds vaker ook uitgerust met *obstacle avoidance* technologie.[85] Met behulp van deze technologie kan de drone een object detecteren en uit de weg gaan.

Functionaliteiten zoals *obstacle avoidance* en automatisch vliegen zijn ontwikkeld met het oog op het vergroten van de gebruikersvriendelijkheid. Het vraagt enige vaardigheid, zoals blijkt uit de focusgroep met hobbydronevliegers en de interviews, om met een drone te vliegen. Dat is voor veel vliegers deel van het vermaak, maar voor mensen die vooral geïnteresseerd zijn in het maken van foto's kan dat tot frustratie leiden wanneer het vliegen van de drone in de weg staat van het maken van de foto. De selfiedrones die nu op de markt zijn, zijn ontworpen om het vliegen makkelijker te maken. Zo zijn er drones die met handgebaren bestuurd kunnen worden en er zijn zelfs drones die automatisch mensen volgen. Met behulp van bijvoorbeeld gezichtsdetectie en -herkenning kan zo'n drone een persoon blijven volgen. Een drone die in

[81] De MAVIC-mini van DJI. Dji.com, zoek op: Mavic-mini.
[82] Zie bijvoorbeeld Dronepilots.nl.
[83] Zie bijvoorbeeld: drones.nl, zoek op: Dienst Justitiële Inlichtingen blij met geofencing op DJI-drones
[84] 'Wat is RTH en waarom moet je goed op deze instelling letten?', Dronewatch.nl 8 april 2020.
[85] Zie bijvoorbeeld '12 Top collision avoidance drones and obstacle detection explained', Dronezon.com 8 april 2020.

2020 op de markt is gebracht kan ook zelfstandig mensen in beeld brengen en een foto maken; met een druk op de knop kan deze dan direct via sociale media worden gedeeld.[86]

Drones zijn beschikbaar via gespecialiseerde winkels, zoals droneland.nl en droneshop.nl, maar zijn ook te koop in speelgoedwinkels, waaronder Intertoys, en op (internet)winkels met een breder aanbod, zoals mediamarkt, bol.com en coolblue.nl. Bij speelgoedwinkels zijn doorgaans drones te koop voor een paar tientjes, terwijl bij de gespecialiseerde websites ook professionele drones te koop zijn waarvan de prijzen kunnen oplopen tot enkele duizenden euro's. Er zijn een aantal dronefabrikanten, waarvan het Chinese DJI veruit het grootste marktaandeel heeft.[87] Daarnaast zijn er ook nog andere producenten zoals het Franse Parrot en Yuneec in Hong Kong. Bovendien zijn er ook aanbieders van zelfbouw drones.

Momenteel zijn hobbydrones nog volop in ontwikkelingen en wordt er gewerkt aan het verbeteren van, bijvoorbeeld, de vliegtijd, de gebruikersvriendelijkheid en het gewicht. De experts die wij geïnterviewd hebben verwachten vooral ontwikkelingen op het gebied van het automatisch (of autonoom) vliegen, *object avoidance*, en sensoren. Ook verwachten zij dat drones kleiner en lichter zullen worden. Een belangrijk punt van ontwikkeling is het geluid: de meeste drones maken behoorlijk wat lawaai. Daarom zijn er meerdere partijen bezig met het ontwikkelen van stillere drones.[88] Al deze ontwikkelingen maken het makkelijker om mensen heimelijk te observeren met behulp van een hobbydrone.

3.5 Conclusie

In dit hoofdstuk hebben wij spionageproducten verder gedefinieerd en in kaart gebracht welke spionageproducten beschikbaar zijn voor burgers, ter beantwoording van de eerste en tweede deelvraag.

Antwoord deelvraag 1 over definitie en classificatie van spionageproducten

Wij definiëren deze producten als technische hulpmiddelen waarmee personen heimelijk informatie kunnen verzamelen over andere personen. Wij hebben hierbij onderscheid gemaakt tussen spionageproducten in enge zin en spionageproducten in brede zin. Spionageproducten in *enge* zin zijn hulpmiddelen die hoofdzakelijk ontworpen of geschikt gemaakt zijn voor het heimelijk verzamelen van informatie over personen. Spionageproducten in *brede* zin zijn hulpmiddelen die gebruikt kunnen worden voor het heimelijk verzamelen van informatie over iemand, maar waarvan zulke heimelijke informatievergaring niet het hoofddoel van ontwerp of gebruik is. In deze verkenning behandelen wij hobbydrones als spionageproducten in brede zin.

[86] Airselfiecamera.com, zoek op: Air pix
[87] Drones.nl, zoek op: Drone-industrie naar verwachting 14 miljard dollar waard in 2030
[88] Drones.nl, zoek op: Alphabet gaat stillere bezorgdrones maken na klachten over geluid

Antwoord deelvraag 2 over het aanbod van spionageproducten voor Nederlandse burgers

Op het gebied van *spionageproducten in enge zin* is er een breed aanbod van producten, variërend van camera's in rookmelders en klokken tot GPS-trackers en stalkerware voor op mobiele telefoons. De belangrijkste groepen producten in deze categorie zijn spycams, afluisterapparatuur en locatietrackers.

Onder de categorie van *spionageproducten in brede zin* kunnen producten worden geschaard die niet specifiek voor spionagedoeleinden ontwikkeld zijn, maar die wel gebruikt kunnen worden voor het bespioneren van anderen, zoals een smartphone, camera met zoomlens en smartwatches. Hobbydrones kunnen ook onder deze categorie worden geschaard. Momenteel zijn er verschillende drones beschikbaar voor burgers, variërend van kleine lichtgewicht drones tot grotere en zwaardere drones waar allerhande sensoren op gemonteerd kunnen worden. De meeste drones zijn echter uitgerust met een camera, of zoals een van de door ons geïnterviewde experts het verwoorde: "drones zijn vliegende camera's". Momenteel vragen veel drones nog enige vaardigheid bij het vliegen, maar wij zien een trend in de technologische ontwikkelingen richting makkelijk bestuurbare drones als gevolg van onder andere automatisch vliegen, personen detectie en gezichtsherkenning. Ook zullen drones en sensoren in de toekomst waarschijnlijk lichter, kleiner en krachtiger worden. Deze ontwikkelingen maken drones in toenemende mate geschikt voor heimelijke observaties.

4 Privacyrisico's van spionageproducten

In dit hoofdstuk beantwoorden wij de derde deelvraag in deze verkenning: *Hoe kan het gebruik van spionageproducten door burgers een inbreuk vormen op de privacy van andere burgers? Wat zijn de belangrijkste privacyrisico's?* Wij doen dat op basis van de literatuurstudie, aangevuld met inzichten uit de internetquickscan naar het aanbod van spionageproducten in enge zin, en de interviews en focusgroepen met hobbydrone experts en betrokkenen (zie hoofdstuk 2). Om dit op een systematische manier te doen, maken wij gebruik van de door Koops et al. ontwikkelde typologie van privacy en de privacytaxonomie van Solove. Zoals eerder uitgelegd in hoofdstuk 2 gebruiken wij deze twee kaders als heuristische instrumenten, die ons helpen om na te gaan hoe het gebruik van zowel spionageproducten in enge zin als hobbydrones (als spionageproducten in brede zin) in horizontale relaties inbreuk kan maken op privacy en wat daarbij de belangrijkste risico's zijn. Wij zullen daarom eerst verder uiteenzetten hoe wij de belangrijkste privacyrisico's identificeren en de twee kaders verder toelichten, alvorens wij de privacyrisico's van spionageproducten in relaties tussen burgers onderling beschrijven.

4.1 Privacy en privacyrisico's

Privacy is een term die zeer uiteenlopende aspecten omvat en daarom zeer uiteenlopende definities kent.[89] De waarde van privacy voor de ontwikkeling van een eigen identiteit is een van de meest voorkomende thema's in de privacytheorie.[90] Zo definieert men privacy bijvoorbeeld als de vrijheid om zich te ontwikkelen of om zonder onredelijke beperkingen een eigen identiteit op te bouwen.[91] Deze opvatting van privacy heeft dus duidelijk waarde voor het individu. Privacy is echter ook van belang voor de samenleving in bredere zin. Het kan een brug slaan tussen de tweedeling in het publieke debat over veiligheid en privacy, en kan bijdragen aan een meer 'common sense'-debat over de beste manier om beide te bereiken.[92] We zullen in deze verkenning geen onderscheid maken tussen de individuele en maatschappelijke waarde van

---

[89] Privacy wordt vaak afgebeeld met behulp van illustratieve simulaties die de complexiteit en incoherentie van het concept laten zien. Zo is het bijvoorbeeld beschreven als een "hooiberg in een orkaan" (Ettore v. Philco Television Broadcasting Corp., 229 F.2d 481 (3d Cir. 1956)) en het onderzoeken ervan wordt vergeleken met "het verkennen van een onbekend moeras" (J. C. Inness, *Privacy, intimacy and isolation,* Oxford: Oxford University Press 1996, p. 3.).

[90] Zie bijv. I. Altman, *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding,* Monterey: Brooks/Cole Publishing Company 1975; M. Hildebrandt, 'Profiling: From data to knowledge The challenges of a crucial technology', *Datenschutz und Datensicherheit* (30) 2006, 548-552; M. Hildebrandt & E.J. Koops, 'The challenges of ambient law and legal protection in the profiling era', 73 *Modern Law Review* (3) 2010, 428-460; J. Reiman, 'Privacy, intimacy, and personhood', in: F. D. Schoeman (red.) *Philosophical dimensions of privacy: an anthology*, Cambridge: Cambridge University Press 1984.

[91] P. Agre, 'Introduction', in: P.E. Agre & M. Rotenberg (red.) *Technology and privacy: the new* landscape, Cambrige, Massachusetts: MIT Press 1998, p. 7.

[92] P.M. Regan, 'Privacy and the common good: revisited', in: B. Roessler & D. Mokrosinska (red.) *Social dimensions of privacy*, Cambridge: Cambridge University Press 2015, p. 52.

privacy. In plaats daarvan stellen we ons op het standpunt dat het twee kanten van de waarde van privacy zijn, die elkaar aanvullen, aangezien de waarden die ten dienste staan van individuen ook de samenleving als geheel dienen, en *vice versa*. In die zin zou je het individu en de sociale waarde van privacy als twee kanten van een medaille kunnen zien.

Daarbij komt dat privacy niet alleen een waarde op zich is, maar ook een waarde die van cruciaal belang is in relatie tot andere fundamentele rechten en vrijheden, zoals de vrijheid van meningsuiting en de vrijheid van vergadering en vereniging. Privacy is dus een “onderdeel van een pakket van met elkaar verweven grondrechten”[93] dat niet alleen onze individuele maar ook sociale en politieke emancipatie garandeert. Met andere woorden, privacy is een *infrastructurele voorwaarde*.[94] Het is een belangrijke voorwaarde voor autonomie, zelfontplooiing en de andere waarden (bijvoorbeeld het voorkomen van discriminatie, (her)stigmatisering en het behoud van vertrouwen).[95] Bovendien speelt privacy een belangrijke rol, niet alleen op privéplekken, zoals in huis, maar ook op openbare plekken.[96] Dit zal met name van belang zijn in verband met de privacyrisico's die voortvloeien uit het gebruik van spionageproducten in zowel privé als openbare ruimte.

Ook de relatie tussen privacy en overlast moet hier worden vermeld. Hobbydrones produceren een nogal luid en bijzonder geluid, dat door mensen vaak als storend wordt ervaren. Bovendien kan het bewustzijn van het feit dat men (mogelijk) wordt bespioneerd ook leiden tot overlast. Dergelijke overlast kan worden opgevat als een vorm van inmenging in het privéleven van een persoon, omdat het de ontwikkeling en vervulling van haar identiteit kan belemmeren, het genieten van de eigen woning kan verstoren, en relaties met anderen bemoeilijken. Dit perspectief op de relatie tussen privacy en overlast komt ook terug in de jurisprudentie van het Europees Hof voor de Rechten van de Mens, dat de term 'overlast' heeft gebruikt om diverse verschijnselen te beschrijven, waarbij lawaai, stank en gezondheidsrisico's een rol spelen. [97]

Zoals aangeven in hoofdstuk 1 kijken wij om te bepalen wat de belangrijkste *privacyrisico’s* zijn met name naar inbreuken op de privacy die kwalitatief of kwantitatief dusdanig verschillen van bestaande (en maatschappelijke geaccepteerde) privacy-inbreuken dat zij substantieel afbreuk doen aan de mogelijkheden die burgers redelijkerwijs ervaren om in bepaalde situaties onbevangen zichzelf te kunnen zijn. Meer specifiek zullen wij daarom in de analyse van

---

[93] S. Gutwirth, *Privacy and the Information Age,* Maryland: Rowman & Littlefield Publishers 2002, p. 45.
[94] J. E. Cohen, ‘Surveillance versus Privacy: Effects and Implications’, in: D. Gray & S.E. Henderson, *The Cambridge handbook of surveillance law*, Cambridge: Cambridge University Press 2017.
[95] B.J. Koops e.a., ‘The reasonableness of remaining unobserved: A comparative analysis of visual surveillance and voyeurism in criminal law’, *Law & Social Inquiry* 2018, p. 621.
[96] E. Ruppert, Rights to Public Space: Regulatory Reconfigurations of Liberty’, 27 Urban Geography 3, 2006; H. Lefèbvre, *The Production of Space*, Cambridge: Blackwell1991; D. Mitchell, *The right to the city*, New York: The Guilford Press 2003.
[97] W.A. Schabas, *The European Convention on Human Rights: A commentary*, Oxford: Oxford University Press 2017, p. 388

privacyrisico's de volgende criteria gebruiken als indicatie dat de drempel van een maatschappelijk aanvaardbare privacy-inbreuk overschreden kan worden:

Kwalitatief:

- Wanneer nieuwe privacy-inbreuken ontstaan die voorheen niet mogelijk waren (denk aan het met een drone naar binnen kijken op de achtste verdieping);
- Wanneer voorheen uitzonderlijke privacy-inbreuken een systematisch karakter krijgen (denk aan het fotograferen met een verborgen camera, wat voorheen uitzonderlijk was maar met smartphones nu min of meer voor iedereen mogelijk is) waardoor de inbreuk een andere aard krijgt;

Kwantitatief

- Wanneer bestaande privacy-inbreuken ernstiger worden door schaalvergroting (denk aan het op internet plaatsen van een opgenomen vertrouwelijk gesprek);
- Wanneer het cumulatieve effect van privacy-inbreuken een grote invloed kan hebben op het vermogen van burgers om zichzelf op een ongeremde manier te zijn.[98]

Een privacyrisico verdient de aandacht als de inbreuk aan een van deze criteria voldoet.

Om systematisch in kaart te brengen hoe privacyrisico's zich kunnen voordoen als gevolg van het gebruik van spionageproducten in enge en brede zin en welke daarbij de belangrijkste risico's zijn gebruiken wij de privacytypologie van Koops et al. en de taxonomie van activiteiten die privacy kunnen schaden van Solove. Hieronder lichten wij deze twee instrumenten verder toe.

4.1.1 Koops et al.'s typologie van privacy

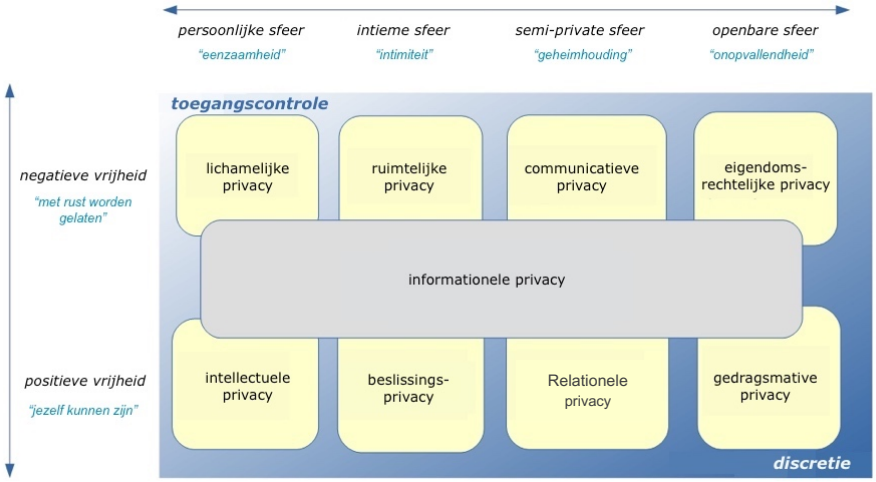
Wij bespreken eerst het driedimensionale model van privacytypen dat Koops et al.[99] (zie Figuur 4.1) introduceerden, gevolgd door een beschrijving van de door hen geïdentificeerde vormen van privacy. De typologie van privacy bevat drie assen. De horizontale as beweegt zich langs een spectrum van de persoonlijke of volledig private zone naar intieme, semi-private en publieke zones.[100] Belangrijk is dat de termen 'publiek' en 'privé' niet alleen verwijzen naar ruimtes, maar ook naar de aard en het karakter van (eventuele) interpersoonlijke relatie.

---

[98] Zie ook bijvoorbeeld Vedder, A., van der Wees, J.G.L., Koops, B.J. and de Hert, P., 2007. 'Van privacyparadijs tot controlestaat? Misdaad-en terreurbestrijding in Nederland aan het begin van de 21ste eeuw.' *Den Haag: Rathenau Instituut, Studie*, *49*, p.90.

[99] B. Koops e.a., 'A Typology of Privacy', 38 *University of Pennsylvania Journal of International Law* (2) 2017, p. 483-575.

[100] Ibid. p. 545



FIGUUR 4.1: DE NEGEN PRIVACYTYPEN UIT DE TYPOLOGIE VAN KOOPS ET AL.[101]

De *persoonlijke sfeer* wordt gekenmerkt door eenzaamheid of isolement. De *intieme sfeer* wordt gekenmerkt door een verschuiving in de richting van sociale betrokkenheid, zij het beperkt tot intieme partners, familieleden en goede vrienden. Deze sfeer wordt ook gekenmerkt door activiteiten die plaatsvinden in privé- en omheinde ruimtes, zoals het huis waar mensen hun leven delen met intieme partners en familie. De *semi-private sfeer* omvat sociale interactie met een breder scala aan actoren, waaronder kennissen, collega's en professionele relaties (bijvoorbeeld interactie met een arts of een verkoper), en activiteiten die plaatsvinden in een meer quasi-openbare ruimte. De *publieke sfeer* wordt getypeerd door activiteiten die in het openbaar plaatsvinden - bijvoorbeeld op een openbaar plein, in het openbaar vervoer of op publiek toegankelijke elektronische platforms - waarbij het privacybelang wordt gekenmerkt door het verlangen om onopvallend te zijn ondanks de fysieke of virtuele zichtbaarheid in de publieke ruimte. Deze sfeer ligt aan de rand van de buitenste laag van privacy en sociaal leven.

Op de verticale as wordt het spectrum van negatieve en positieve vrijheid gebruikt, dat gekenmerkt kan worden door de kernbegrippen 'alleen gelaten worden' (nadruk op negatieve vrijheid, d.w.z. wat anderen niet kunnen doen) en 'zelfontplooiing' (nadruk op positieve vrijheid, d.w.z. wat het individu kan doen). Het eerste begrip zullen wij aanduiden als ‘vrijheid van’ en het tweede als ‘vrijheid om’. Hoewel er geen scherpe grens is tussen deze twee begrippen draagt het presenteren van de ideaaltypen van privacy langs dit spectrum bij aan het begrip van de variatie die zich binnen privacy voordoet.[102]

Verder is er een derde as die voortvloeit uit het onderscheid dat in de literatuur wordt gemaakt

[101] Ibid, p. 484.
[102] Ibid, p. 565.

tussen beperkte toegang en latere controle nadat toegang is verleend. Deze as (die in Figuur 4.1 niet zichtbaar is) is niet onafhankelijk van de andere twee asses, maar combineert beide in die zin dat beperkte toegang meer (maar niet uitsluitend) geassocieerd wordt met de private zone in plaats van met de publieke zone, en meer met negatieve dan met positieve vrijheid. Controle nadat de toegang al is verleend is belangrijker in de semi-private en publieke zones en heeft meer het karakter van een positieve vrijheid (zelfbeschikking). Deze as loopt dus over beide assen van linksboven naar rechtsonder. Zo heeft elk privacybelang in het gedrag van een persoon in de openbare ruimte meer te maken met het beheersen van het gebruik van informatie over die activiteit dan met het beperken van de toegang (aangezien een deel van de toegang al is verleend door de aard van de ruimte zelf). Aan de andere kant is lichamelijke privacy typisch (maar niet altijd) een kwestie van toegang in plaats van controle.

Deze derde as loopt dus langs een spectrum van mogelijkheden om controle uit te oefenen op het verdere gebruik van informatie/persoons/plaatsen/-dingen nadat enige vorm van toegang, expliciet of impliciet, is verleend. Aan de ene kant van dit spectrum beschermt de privacy het recht van een persoon om de toegang tot zijn lichaam, huis (en andere privé-plaatsen) en eigendommen, alsook zijn persoonlijke gedachten en processen van de geest uit te sluiten. Aan de andere kant van het spectrum beschermt privacy het vertrouwelijke karakter van de communicatie, de geheimhouding van de gegevens en de controle op het gebruik van persoonsgegevens (ook nadat toegang is verleend) en activiteiten in semi-openbare of openbare zones. Aan deze kant van het spectrum kan de toegang tot hetgeen beschermt dient te worden, gemakkelijker worden afgeleid op basis van het openbare karakter van de ruimte (d.w.z. dat de toegang niet kan worden ontzegd aan openbare activiteiten, in praktische zin).

Koops et al. identificeerden binnen dit model acht basistypen privacy. Daarnaast onderscheiden zij informationele privacy als een overkoepelend type privacy dat overlapt maar niet samenvalt met de andere acht basistypen. Deze in totaal negen vormen van privacy zijn ideaaltypen die kunnen helpen om systematisch privacy en privacy-inbreuken in kaart te brengen.[103]

De geïdentificeerde ideaaltypen van privacy worden als volgt gekarakteriseerd:

1. *Lichamelijke privacy* wordt gekenmerkt door het belang dat individuen hebben bij de privacy van hun fysieke lichaam, waarbij de nadruk ligt op negatieve vrijheid - de mogelijkheid om mensen uit te sluiten van het aanraken van hun lichaam of het beperken van hun bewegingsvrijheid.
2. *Ruimtelijke privacy* wordt gekenmerkt door het belang van privacy van de privéruimte. Het gaat hier dan om het beperken van de toegang van anderen tot de privéruimte of het controleren van het gebruik ervan. Als zodanig verwijst het naar de bescherming van de

[103] C. Nippert-Eng, *Islands of privacy*, Chicago: The University of Chicago Press 2010, p. 5

privacy van mensen in relatie tot de 'plekken waar zij hun privéleven inrichten'.[104] Ruimtelijke privacy mag dan verder reiken dan de intieme zone, het ideaaltype is in deze positie in het model het best gesitueerd vanwege de rol die de private ruimte speelt bij het verhinderen van de toegang tot intieme activiteiten. De woning is het prototypische voorbeeld van de plek waar ruimtelijke privacy wordt toegepast, nauw verbonden met de intieme relaties en het gezinsleven die zich in de woning afspelen. Ruimtelijke privacy kan echter ook verwijzen naar andere plaatsen, zoals hotelkamers, werkplekken, garages, zelfs voertuigen en computers (zie hoofdstuk 6 van de jurisprudentie van het EHRM).

3. *Communicatieve privacy* wordt getypeerd door het belang dat een persoon heeft bij het beperken van de toegang tot communicaties of het controleren van het gebruik van informatie die aan derden wordt gecommuniceerd. Communicatie kan al dan niet via verschillende media plaatsvinden, waarbij er verschillende manieren zijn om de toegang te beperken of de gecommuniceerde berichten te controleren.
4. *Eigendomsrechtelijke privacy* wordt gekenmerkt door het belang dat iemand heeft bij het gebruik van eigendom als middel om activiteiten, feiten, dingen of informatie te beschermen tegen de mening van anderen. Een persoon kan bijvoorbeeld een tas gebruiken om voorwerpen of informatie te verbergen die hij/zij liever privé houdt terwijl hij/zij zich in openbare ruimtes verplaatst
5. *Intellectuele privacy* wordt gekenmerkt door het belang dat iemand heeft bij privacy van gedachten en geest, en de ontwikkeling van meningen en overtuigingen. Hoewel dit belangrijke relationele aspecten kan hebben, is het geschikt als een ideaal type van de persoonlijke zone, omdat de geest de plaats is waar mensen het meest zichzelf kunnen zijn.
6. *Beslissingsprivacy* wordt gekenmerkt door intieme beslissingen, voornamelijk van seksuele of voortplantende aard, maar ook door andere beslissingen over gevoelige onderwerpen binnen de context van intieme relaties. Net als bij ruimtelijke privacy is beslissingsprivacy als ideaal type binnen de intieme zone nauw verbonden met het gezinsleven.
7. *Relationele privacy* wordt getypeerd door het feit dat het individu er belang bij heeft vrij te zijn om te kiezen met wie hij of zij wil communiceren: vrienden, verenigingen, groepen en gemeenschappen. Dit past in de semi-private zone omdat de relaties zich vaak buiten strikt private plaatsen of intieme omgevingen afspelen, in semi-publieke ruimtes zoals

[104] B. Koops & e.a., 'A Typology of Privacy', 38 *University of Pennsylvania Journal of International Law* (2) 2017, p. 516.

kantoren, ontmoetingsruimten of cafés

8. *Gedragsmatige privacy* wordt gekenmerkt door de privacybelangen die een persoon heeft tijdens het uitvoeren van voor het publiek zichtbare activiteiten. In tegenstelling tot zaken die mensen in het openbaar bij zich dragen (die verborgen kunnen zijn en daardoor deels buiten het zicht van anderen kunnen worden gehouden), is het persoonlijke gedrag in de openbare ruimte moeilijker te verbergen voor anderen en is het dus een ideaaltype van privacy waar de behoefte aan controle of, beter nog, discretie na het verlenen van toegang het meest dringend is. 'Zichzelf zijn' in het openbaar kan alleen worden bereikt als anderen privacy respecteren door burgerlijke onoplettendheid, maar verder kan controle alleen worden uitgeoefend door te proberen onopvallend te blijven in de massa's in de openbare ruimte.

9. *Informationele privacy*, zoals hierboven vermeld, wordt geconceptualiseerd als een overkoepelend type dat overlapt met de andere acht basistypes. Kenmerkend voor dit privacytype is het belang van een persoon om te voorkomen dat informatie over haarzelf wordt verzameld en om informatie over haarzelf te controleren waartoe anderen legitieme toegang hebben. Elk van de andere acht privacytypes bevat een element van informationele privacy – dat wil zeggen, er bestaat een privacybelang bij het beperken van de toegang of het controleren van het gebruik van informatie over dat aspect van het menselijk leven.[105] Lichamelijke privacy beperkt zich bijvoorbeeld niet alleen tot het beperken van de fysieke toegang tot het lichaam, maar ook tot het beperken en controleren van informatie over het lichaam (bijv. gezondheids- of genetische informatie). Aangezien informationele privacy zowel negatieve vrijheid (exclusief toegang tot informatie) als positieve vrijheid (informationele zelfbeschikking) combineert en die informatie uit elk van de vier levenszones kan betreffen, wordt informationele privacy in dit model gezien als een overkoepelend type.

Zoals uit de privacytypologie blijkt zijn er diverse soorten privacy die van belang zijn voor individuen en de maatschappij. Informationele privacy verdient in een verkenning naar privacyrisico's van het gebruik van hobbydrones en spionageproducten in enge zin bijzondere aandacht vanwege de alomtegenwoordige aanwezigheid van digitale technologieën in ons leven die ons en ons leven van gegevens voorzien. Solove licht dit type verder uit in zijn beschrijving van activiteiten die (informationele) privacy kunnen schaden.

4.1.2 Solove's taxonomie van (informationelle) privacy schade

De taxonomie van Solove bestaat uit vier basisgroepen van activiteiten die schadelijk kunnen zijn voor privacy: (1) informatieverzameling, (2) informatieverwerking, (3) informatieverspreiding

[105] Zie ook P. Blok, *Het recht op privacy*, Den Haag: Boom Juridische uitgevers 2002.

en (4) overschrijding.[106] Elk van deze groepen bestaat verder uit verschillende verwante subgroepen (deze worden hieronder kort besproken). De eerste drie groepen hebben duidelijk betrekking op informatie, waarbij de verschillende stappen (van verzamelen via verwerken tot verspreiden) steeds verder buiten de controle van het individu liggen. Dat wil zeggen dat bij verzamelen (als het bij het individu zelf gebeurt) de persoon hierop veelal nog enige invloed zou kunnen uitoefenen – vanzelfsprekend afhankelijk van de omstandigheden – maar dat het verwerken en met name op het verspreiden van eenmaal verzamelde informatie meestal buiten de controlemacht van het individu liggen.

Privacy-inbreuken kunnen echter ook rechtstreeks betrekking hebben op de persoon in kwestie en niet noodzakelijkerwijs (alleen) op informatie over de persoon.[107] Hoewel Solove dit niet expliciet erkent, is zijn taxonomie dus sterk gericht op de privacy van informatie. De niet-informationele inbreuken op privacy zoals besproken door Koop et al. (denk bijvoorbeeld aan handtastelijkheid als inbreuk op lichamelijke privacy, of het hinderlijk volgen als inbreuk op de gedragsmatige privacy) blijven in deze taxonomie onderbelicht. Vanwege deze bijzondere focus zullen we de taxonomie van Solove gebruiken als aanvulling op de typologie van Koops et al., in het bijzonder waar het gaat om informationele privacy als een overkoepelend aspect van alle onderliggende typen van privacy. Solove's taxonomie is aldus vooral bruikbaar om activiteiten te onderscheiden die kunnen leiden tot inbreuken op de informationele privacy. Omdat hobbydrones of spionageproducten in enge zin beide vormen van informatie- en communicatietechnologie betreffen, zal het gebruik daarvan ook altijd het verzamelen van (vaak persoonlijke) gegevens omvatten. Dit kan bovendien leiden tot gegevensverwerking en -verspreiding, waardoor de privacy van informatie verder wordt aangetast.

De taxonomie van Solove kan in Tabel 4.1 als volgt worden samengevat.

INFORMATIEVERZAMELING	**INFORMATIEVERWERKING**	**INFORMATIEVERSPREIDING**	**OVERSCHRIJDING**
Surveillance	Aggregatie	Schending van de geheimhouding	Indringing
Ondervraging	Identificatie	Openbaarmaking	Inmenging in besluitvorming
	Onveiligheid	Blootstelling	
	Secundair gebruik	Grotere toegankelijkheid	
	Uitsluiting	Chantage	
		Toe-eigening	

[106] D. J. Solove, *Understanding privacy*, Harvard: Harvard University Press, 2008.
[107] D. J. Solove, 'Conceptualizing Privacy' 90 California Law Review 1087, 2002, p. 489.

		Vervorming	

TABEL 4.1: SCHADE AAN DE PERSOONLIJKE LEVENSSFEER DOOR INFORMATIEVERSTREKKING[108]

De eerste groep activiteiten die van invloed zijn op de privacy betreft het *Informatieverzameling*. Zelfs als er geen informatie openbaar wordt gemaakt, kan het verzamelen van informatie schade veroorzaken. Solove onderscheidt twee vormen van *informatieverzameling*: *surveillance* en *ondervraging*. *Surveillance* verwijst naar het kijken, luisteren naar of vastleggen van iemands activiteiten.[109] *Ondervraging* verwijst naar het onderzoeken of onder druk zetten van individuen om informatie te onthullen. Beide vormen van *informatieverzameling* kunnen ongemak veroorzaken, zelfs als de informatie nauwelijks wordt verspreid. Op het gebied van spionage is met name heimelijke surveillance van belang. Volgens Solove is heimelijke surveillance problematisch omdat het een 'chilling effect' kan hebben op gedrag: mensen voelen zich beperkt in hun gedragingen. Dit chilling effect is nog groter wanneer mensen zich over het algemeen bewust zijn van de *mogelijkheid* van surveillance, maar nooit zeker weten of ze op een bepaald moment in de gaten worden gehouden. In het geval waarin de surveillance zo heimelijk is dat de geobserveerde zich totaal niet bewust zijn van de mogelijkheid om geobserveerd te worden, ligt het kwaad in de mogelijkheid voor de observerende om een aanzienlijke mate van informatie over mensen te verzamelen en dus macht over de persoon die hij in de gaten houdt, te krijgen.

De tweede groep activiteiten, *informatieverwerking*, betreft de manier waarop informatie wordt opgeslagen, gemanipuleerd en gebruikt.[110] Bij *aggregatie* worden verschillende gegevens over een persoon gecombineerd. *Identificatie* verwijst naar het koppelen van informatie aan bepaalde personen. *Onveiligheid* houdt in dat opgeslagen informatie onzorgvuldig wordt beschermd tegen lekken en ongeoorloofde toegang. *Secundair gebruik* is het gebruik van informatie voor een ander doel dan waar het in eerste instantie voor is verzameld, zonder toestemming van de betrokkene. *Uitsluiting* heeft betrekking op het feit dat de betrokkene niet op de hoogte wordt

---

[108] D. J. Solove, *Understanding privacy*, Harvard: Harvard University Press, 2008, p. 104

[109] D. J. Solove, 'Conceptualizing Privacy' 90 California Law Review 1087, 2002, p. 500.

[110] We hebben het niet over 'secundair gebruik', 'uitsluiting', 'verhoogde toegankelijkheid', 'toe-eigening' en ' inmenging in besluitvorming' omdat deze - om verschillende redenen - niet relevant zijn voor de gevallen van spionage tussen burgers. Secundair is het gebruik van gegevens voor doeleinden die geen verband houden met de doeleinden waarvoor de gegevens oorspronkelijk werden verzameld zonder toestemming van de betrokkene. Aangezien er geen toestemming is in het geval van spionage, is deze specifieke schade niet bijzonder relevant voor de focus van dit verslag. Evenzo heeft uitsluiting betrekking op het feit dat personen niet op de hoogte worden gesteld van en worden geïnformeerd over hun gegevens en betreft het in de eerste plaats de verantwoordingsplicht van overheidsinstanties en bedrijven die gegevens over personen bijhouden. Verhoogde toegankelijkheid heeft betrekking op de situatie waarin gegevens die al beschikbaar zijn voor het publiek gemakkelijker toegankelijk worden gemaakt (bv. wanneer bepaalde soorten openbaar beschikbare gegevens online toegankelijk worden), zodat een verschil in kwantiteit een verschil in kwaliteit wordt, waardoor het risico van de schade van openbaarmaking toeneemt. Toe-eigening heeft betrekking op de manier waarop een individu zich aan de samenleving wil presenteren en verwijst naar het gebruik van zijn identiteit of persoonlijkheid voor de doeleinden van een ander. Tot slot gaat het bij 'inmenging in besluitvorming ' om de inmenging van de overheid in de beslissingen van de betrokkene over zijn privézaken.

gesteld van de gegevens die anderen over hem of haar hebben en niet kan deelnemen aan de verwerking en het gebruik ervan.

De gevaren van aggregatie zijn inmiddels bekend. Terwijl een stukje informatie hier of daar niet erg veelzeggend is, vormen stukjes en beetjes gegevens samen een portret van een persoon. 'Het geheel wordt groter dan de delen.'[111] Zo kan geaggregeerde informatie nieuwe feiten over een persoon aan het licht brengen waarvan ze niet verwachtte dat ze bij het verzamelen van de geïsoleerde gegevens bekend zouden worden. Als zodanig vergroot aggregatie de macht die iemand heeft over een ander, vooral wanneer deze gegevens worden gebruikt als een manier om een persoon te beoordelen.[112]

Identificatie is het verbinden van informatie met individuen. Het is vergelijkbaar met aggregatie, omdat het in beide gevallen gaat om de combinatie van verschillende stukjes informatie, waaronder de identiteit van een persoon. Identificatie verschilt echter van aggregatie in die zin dat er een verband is met de persoon in levenden lijve. Er kunnen bijvoorbeeld uitgebreide aggregaties van gegevens over een persoon in veel databases zijn, maar deze aggregaties kunnen zelden met die persoon in verband worden gebracht tijdens haar dagelijkse activiteiten.[113] Omdat identificatie mensen verbindt met gegevens, koppelt het diverse soorten informatie uit verschillende bronnen aan mensen. Dit verandert wat anderen weten over mensen als zij deelnemen aan verschillende transacties en activiteiten. Identificatie kan dus een negatieve invloed hebben op de identiteit. Bovendien kan het iemands vermogen belemmeren om anoniem of pseudoniem te zijn. Anonimiteit beschermt mensen tegen vooroordelen op basis van hun identiteit en stelt hen in staat om vrijer te stemmen, te spreken en te verenigen, door hen te beschermen tegen het gevaar van vergelding.

Onveiligheid is een probleem dat wordt veroorzaakt door de manier waarop onze informatie wordt behandeld en beschermd.[114] Het gaat onder meer om storingen, veiligheidslacunes, misbruik en illegaal gebruik van persoonlijke informatie, die mensen blootstellen aan mogelijke toekomstige schade (bijv. identiteitsdiefstal).

De derde groep activiteiten betreft de verspreiding van informatie, waarbij de schade bestaat uit het onthullen van persoonsgegevens of de dreiging van de verspreiding van informatie.[115] De *schending van de geheimhouding* is het verbreken van een belofte om de informatie van een persoon vertrouwelijk te houden. *Openbaarmaking* houdt in dat waarheidsgetrouwe informatie

---

[111] D. J. Solove, 'Conceptualizing Privacy' 90 California Law Review 1087, 2002, p. 507.
[112] De kredietrapporten, bijvoorbeeld, worden gebruikt om gegevens over de financiële reputatie van een persoon te evalueren en dan besluiten te nemen die diep het leven van een persoon, met inbegrip van of zij een lening, een huur, of een hypotheek krijgt; Ibid, p. 507.
[113] Ibid, p. 510-1.
[114] Ibid, p. 515.
[115] Ibid, p. 491.

over een persoon wordt onthuld, die van invloed is op de manier waarop anderen haar karakter beoordelen. *Blootstelling* is het onthullen van andermans naaktheid, verdriet of lichamelijke gesteldheid. Een *grotere toegankelijkheid* vergroot de toegankelijkheid van informatie. *Chantage* is de dreiging om persoonlijke informatie vrij te geven. *Toe-eigening* houdt in dat de identiteit van de betrokkene wordt gebruikt om de doelen en belangen van een ander te dienen. *Vervorming* bestaat uit het verspreiden van onjuiste of misleidende informatie over personen. Alle informatieverspreidingsactiviteiten hebben betrekking op de verspreiding of overdracht van persoonsgegevens of de dreiging dat dit gebeurt.

Terwijl de schade bij de inbreuk op de vertrouwelijkheid, de schending van het vertrouwen in de relatie is, heeft de schade bij de openbaarmaking betrekking op de schade aan de reputatie die door de verspreiding van de informatie wordt veroorzaakt. Bescherming tegen openbaarmaking bevordert dus de individuele autonomie. Het risico van openbaarmaking kan mensen ervan weerhouden activiteiten te ontplooien die hun eigen zelfontplooiing bevorderen. Bovendien kan openbaarmaking mensen ervan weerhouden om zich met anderen te verenigen, waardoor de vrijheid van vereniging wordt aangetast, en kan het ook de anonimiteit aantasten, die soms van cruciaal belang is voor de bevordering van de vrije meningsuiting.[116] Als zodanig brengt openbaarmaking het democratische zelfbestuur in gevaar. Openbaarmaking houdt ook in dat informatie wordt verspreid buiten de bestaande netwerken van informatiestromen.[117] 'De schade van openbaarmaking is niet zozeer het wegnemen van geheimhouding, maar de verspreiding van informatie over de verwachte grenzen heen. Mensen geven vaak informatie vrij aan een beperkte kring van vrienden, en ze verwachten dat de informatie binnen deze groep blijft.'[118]

Volgens Solove houdt blootstelling het openbaren van bepaalde fysieke en emotionele eigenschappen van een persoon aan anderen in. Dit zijn eigenschappen die mensen hebben geleerd om te verbergen, zodat hun blootstelling vaak tot schaamte en vernedering leidt. Dit zijn onder andere verdriet, lijden, trauma, verwondingen, naaktheid, seks, urineren en ontlasting, wat allemaal primaire aspecten van ons leven met zich meebrengt.[119] Blootstelling leidt tot verwondingen omdat we sociale praktijken hebben ontwikkeld om aspecten van het leven te verbergen die we kwetsbaar, zwak, dierlijk of walgelijk vinden. Mensen kunnen zo een ernstige en soms slopende vernedering en een verlies aan waardigheid ervaren.[120]

Chantage maakt het mogelijk dat een persoon gedomineerd en gecontroleerd wordt door een ander. De schade zit niet in het daadwerkelijk vrijgeven van informatie, maar in de controle die

---

[116] Ibid, pp. 529-30.
[117] Zie H. Nissenbaum, *Privacy in context: technology, Policy, and the Integrity of Social Life,* California: Stanford University Press 2009.
[118] D. J. Solove, 'Conceptualizing Privacy' 90 California Law Review 1087, 2002, p. 532.
[119] Ibid, p. 533.
[120] Ibid, p. 535.

degene die de dreiging over de betrokkene uitspreekt, uitoefent. Hoe meer mensen over ons weten, hoe meer ze controle over ons kunnen uitoefenen. Daarom maakt het vertellen van de diepste geheimen aan een ander kwetsbaar. Het doel van het beperken van chantage is dan ook niet om openbaarmaking te beperken, maar om te voorkomen dat de dreiging van openbaarmaking wordt gebruikt als een instrument om macht en dominantie over anderen uit te oefenen.[121]

Vervorming is de beïnvloeding van de manier waarop een persoon door anderen wordt waargenomen en beoordeeld, waarbij een persoon onnauwkeurig aan het publiek wordt blootgesteld. Het beperkt dus de controle over de manier waarop men door de samenleving wordt bekeken.[122] Vervorming, evenals openbaring, houdt in dat er informatie wordt verspreid die van invloed is op de manier waarop de samenleving tegen een persoon aankijkt. Vervorming houdt echter in dat onjuiste en misleidende informatie wordt onthuld. Net als bij verdraaiing kan openbaarmaking leiden tot verlegenheid, vernedering, stigmatisering en reputatieschade. Volgens Solove heeft vervorming niet alleen gevolgen voor het benadeelde individu, maar ook voor de maatschappij die dat individu beoordeelt. Het belemmert onze relaties met dat individu en het belemmert ons vermogen om het karakter te beoordelen van degenen met wie we te maken hebben: “We zijn dus misleid in onze relaties met anderen; deze relaties zijn besmet door valse informatie die ons verhindert om een goed en eerlijk oordeel te vellen.”[123]

De vierde en laatste groep activiteiten betreft inbreuken in de privésfeer van mensen. Anders dan bij de andere groepen hoeft er bij inbreuken geen sprake te zijn van persoonlijke informatie (hoewel dit in veel gevallen wel het geval is). Inbreuk betreft invasieve handelingen die iemands dagelijkse activiteiten verstoren, haar routines veranderen, haar afzondering beperken en haar vaak een oncomfortabel en onaangenaam gevoel geven. Inbreuk in de privésfeer kan niet alleen veroorzaakt worden door fysieke inbreuk en nabijheid, maar ook door staren (bewaking) of vragen (ondervraging).[124] Bescherming tegen indringers houdt in dat het individu beschermd wordt tegen ongewenste sociale bemoeienissen, wat mensen de mogelijkheid geeft om 'het recht om met rust gelaten te worden', zoals Warren en Brandeis het noemden, uit te oefenen.[125] Afzondering stelt mensen namelijk in staat om uit te rusten van de druk van het leven in het openbaar en het vervullen van publieke functies.[126] Echter verwachten mensen vaak ruimte van anderen, ook als ze bij anderen zijn. Want als we met een vriend in een restaurant of een andere openbare ruimte praten, hebben we nog steeds ruimte nodig van andere mensen om vrijuit te kunnen spreken. Met andere woorden, we hebben ‘persoonlijke ruimte’ nodig, een soort luchtbel

---

[121] Ibid, p. 541.
[122] Ibid, p. 547.
[123] Ibid, p. 548.
[124] Ibid, p. 550.
[125] S.D. Warren en L.D. Brandeis, ‘The Right to Privacy’, 4 *Harvard Law Review* 193 1890.
[126] D. J. Solove, ‘Conceptualizing Privacy’ 90 California Law Review 1087, 2002, p. 551.

om ons heen om ons van anderen te scheiden, wat ons 'comfort, gemak en ontspanning' oplevert.[127]

4.2 Privacyrisico's van spionageproducten

Zoals we gezien hebben zijn er veel spionageproducten en hobbydrones voor handen voor burgers om heimelijk informatie te verzamelen over anderen en deze al dan niet te gebruiken, bijvoorbeeld door de informatie publiek te maken. Dit kan mogelijk de privacy van de mensen die worden geobserveerd schaden. Alhoewel het bespieden en begluren van mensen met behulp van technologisch middelen op zich niet nieuw is, maken nieuwe technologieën meer mogelijk op het gebied van spionageactiviteiten en creëren daarmee mogelijkerwijs nieuwe risico's.

Hierbij gebruiken wij de typologie van Koops et al. als heuristiek om de verschillende privacy typen die mogelijk kunnen worden geschaad systematisch in kaart te brengen. Wij hebben de volgende sub-paragrafen gestructureerd langs de horizontale as van het model. Zoals beschreven in het vorige hoofdstuk loopt in het model van Koops et al. de horizontale as van de persoonlijke sfeer naar de publieke sfeer. In privéruimtes zijn er meestal weinig mensen die geobserveerd worden of verwachten dat ze geobserveerd worden; in publiek toegankelijke ruimtes daarentegen kunnen mensen geobserveerd worden of verwachten dat ze geobserveerd worden. De privacyrisico's in private of publieke ruimten zullen dus verschillen. Zoals blijkt uit de typologie van Koops et al. Raken risico's die voorkomen in privé-sfeer in de eerste plaats aan *lichamelijke* en *ruimtelijke* vormen van privacy ('vrijheid van') en in de tweede plaats *intellectuele* en *beslissingsprivacy* ('vrijheid om'). Risico's die voortkomen uit het gebruik van spionageproducten op openbare plekken zullen vooral betrekking hebben op *eigendomsrechtelijke* ('vrijheid van') en *gedragsmatige privacy* ('vrijheid om'). In relatie tot semi-publieke of semi-private plaatsen, dat wil zeggen plaatsen die algemeen toegankelijk zijn voor iedereen, maar die in de praktijk het lidmaatschap vereisen (zoals een privéclub) of een andere vorm van toegang (bijvoorbeeld een eersteklas treincoupé of een ziekenhuis) zullen risico's vooral raken aan *communicatieve* en *relationele privacy*. Maar uit ons onderzoek blijkt dat *gedragsmatige privacy* ook geraakt kan worden door het gebruik van spionageproducten in de privésfeer. Daarom kijken we in de onderstaande sub-paragrafen eerst naar de risico's voor dit type privacy die zich in alle sferen kunnen voordoen. Vervolgens kijken we meer specifiek naar de privé-sfeer (4.2.2) en daarna naar de semi-private en publieke sfeer (4.2.3). Tot slot gebruiken wij de taxonomie van Solove om de risico's rondom informationele privacy verder in kaart te brengen (4.2.4).

[127] Ibid, p. 552.

4.2.1 Algemene privacyrisico's van spionageproducten: gedragsmatige privacy

Om een indruk te geven van wat het (heimelijk) observeren van mensen met behulp van spionageproducten zoals een drone bij mensen teweeg kan brengen volgt hier eerst een beschrijving van een casus. Deze casus is gebaseerd op de focusgroep met de bewoners van de Kinderdijk molens.

"Binnen zonder kloppen"

De Molens van Kinderdijk zijn benoemd tot UNESCO Werelderfgoed en zijn een (intern)nationale toeristische trekpleister. Van de 19 molens zijn er 15 bewoond door molenaars en hun familie. De overige molens betreffen bezoekersmolens.[128] Een deel van deze bezoekers vliegt met drones rondom de molens.

In 2016 slaan de molenaars van Kinderdijk alarm. De overlast van toeristen die vliegen met drones over en tussen de molens waarin zij wonen wordt te groot. "Om likes te scoren op Facebook en op Instagram, doen ze steeds gekkere dingen. Ze laten de onbemande vliegtuigjes tussen de draaiende wieken vliegen of voor de ramen hangen en naar binnen gluren", aldus Peter Paul Klapwijk, een van de leden van de bewonersvereniging.[129] Hij stelt ook: "Je gaat je anders gedragen als je je bespiedt voelt. Het is hetzelfde als je met je gezin in de tuin aan het eten bent en er loopt een vreemde de tuin in en begint je te filmen."[130] De molenbewoners hebben twee jaar lang bijgehouden hoeveel drones er rond de molens vliegen. Er waren zo'n honderd meldingen per jaar. De bewoners vermoeden dat dat er nog veel meer zijn.

Tijdens onze focusgroep met de molenbewoners kwam nadrukkelijk naar boven dat de aanwezigheid van drones als indringing wordt ervaren. De bewoners merken de drones aan als 'voyeurs'. Plots zijn de drones er, als zoemende insecten vliegen ze rond de molens, ramen en in de tuinen. De bewoners kunnen hier niets tegen doen. Dit gevoel van onmacht leidt tot frustratie, irritatie en soms zelfs tot een gevoel van agressie bij de bewoners. De bewoners geven aan dat ze best wel gewend zijn aan camera's van toeristen en filmploegen maar dat drones anders zijn. "Een drone vliegt en je weet niet van wie hij is". Een bewoner zegt dat het voelt alsof mensen "binnenkomen zonder te kloppen". Een andere bewoner stelt: "het penetreert je privédomein". Dat roept een gevoel van agressie bij deze bewoner op; een gevoel dat hij eigenlijk liever niet wil hebben.

---

[128] In 2018 waren er 309.000 betalende bezoekers en circa 400.000 niet-betalende bezoekers (schatting). Het is aannemelijk dat deze aantallen bezoekers aan de Molens van Kinderdijk in de nabije toekomst alleen maar zullen toenemen. Zie: M. Pietersma e.a., *Balans tussen sightseeing, erfgoed en leefbaarheid*, Gebiedsperspectief Kinderdijk 2030, 2019.

[129] W. de Jager, 'Kinderdijkers zijn overlast van drones beu', Dronewatch.nl 17 april 2020.

[130] T. van 't Einde, 'Molenaars: 'Drones groot probleem in Kinderdijk', Eenvandaag.avrotros.nl 17 april 2020.

Ook de kinderen van de bewoners hebben last van de drones. Eén bewoner zegt: “Mijn dochter is 16. Ze zwemt graag of ligt te zonnen in de tuin. Het is niet fijn als er dan een drone boven haar hangt. Het is smerig. De toeristen op de rondvaartboten kijken ook naar de bewoners, maar bij een drone gaat het om iemand die je niet kent en niet ziet. Het geeft een onbestemd gevoel, een gevoel van onmacht”. Een andere bewoner vertelt dat de kinderen het ook vervelend vinden voor vrienden en vriendinnen die langskomen en zonnend bij hen in de tuin plots geconfronteerd worden met die drones. Haar dochter zegt: “ik weet het wel, maar mijn vriendinnen niet”. Het is ook weleens voorgekomen dat een drone voor het slaapkamerraam van de dochter hing. Het is een schrikbeeld voor haar dat dit gebeurt als ze juist uit de douche komt. Verschillende bewoners geven aan het meegemaakt te hebben dat drones voor woonkamerramen of slaapkamerramen rondvliegen. In sommige gevallen zelfs 10 minuten lang. “Ze keken echt naar binnen.”

Een bewoner geeft aan dat ze haar kledij aanpast door de aanwezigheid van drones. Ze draagt vaker capuchonvesten en vroeger bij het zwemmen droeg ze ook een T-shirt om haar rug-tatoeage te verbergen. Ook heeft ze nu op de bovenverdieping gordijnen opgehangen om filmende drones het zicht te ontnemen. Ze geeft aan het soms zo zat te zijn dat ze handgebaren gaat maken naar de drone. “Dat wil ik eigenlijk liever niet doen”. Ze vertelt dat haar buurman (niet aanwezig bij de focusgroep), stopt met het opzeilen (openrollen van de zijlen van de molen) wanneer er drones in zijn buurt vliegen. Hij gaat dan naar binnen en wacht tot de drones vertrokken zijn. Andere bewoners bevestigen dat activiteiten rondom de molen en draaiende molens de drones aantrekken.

Een andere molenaar vertelt dat wanneer er drones zijn ze liever niet meer in de tuin koffiedrinkt. Ze geeft aan “helemaal gek” te worden van het geluid. Vooral als ze blijven rondvliegen. “Het zit meteen weer onder je huid”. Mochten drones geen geluid maken, dan zou het probleem echter niet opgelost zijn. Het geluid van de drone geeft immers ook hun aanwezigheid aan. Als dat wegvalt, wordt het controleverlies alleen maar groter. Een bewoner geeft aan te denken dat er nu al drones bestaan die geruisloos kunnen rondvliegen. “Dat maakt het eng. Dat maakt het echt heel eng”. Een andere molenaar vult aan dat drones ook rondvliegen en filmen als je niet thuis bent. Dat bezorgt hem ook een eng gevoel.

Bewoners geven aan dat door de aanwezigheid van drones ze het gevoel hebben dat: “mijn eigen plekje komt te verdwijnen”. Zelfs boven de plekken die vanaf de dijk niet zichtbaar zijn hangen geregeld drones. Eén molenaar brengt beide handen naar zijn borst wanneer hij vertelt over de drones die zijn privéruimte filmen. Hij geeft aan dat hij die inbreuk op zijn privacy ook echt fysiek voelt. Een andere bewoner: “Mensen realiseren zich niet dat wij verworden zijn tot een onderdeel van het geheel. Op Kinderdijk zijn de molenbewoners de props; de aap in de Dierentuin.”

Een type privacy die in de bovenstaande voorbeelden van de molenbewoners duidelijk wordt aangetast in zowel de persoonlijke als semi-private sfeer is gedragsmatige privacy.[131] De molenbewoners passen hun gedrag aan in hun tuin, bij het zwemmen en zelfs in huis als de drones in de buurt zijn. In termen van de privacytypologie kunnen we zeggen dat de gedragsmatige privacy in het gedrang komt in gevallen waar mensen zich bewust zijn (of op enig moment bewust worden) van – mogelijke –gluren of spionage.

Gedragsmatige privacy, volgens de typologie, wordt gekenmerkt door de privacybelangen die een persoon heeft bij het uitvoeren van activiteiten in de publieke sfeer. Het ontstaat echter ook wanneer men wordt waargenomen op een private of semi-private plek, zoals in de tuin van de molen of in huis. De woning, als 'ultieme' privéplek, wordt nog steeds vaak omschreven als 'het kasteel' (*one's castle*).[132] Mensen verwachten dus niet dat ze thuis en op andere privéplekken (zoals een hotelkamer of garage) worden geobserveerd. Wanneer de geobserveerde persoon zich bewust wordt dat zij mogelijk heimelijk wordt geobserveerd, zal haar gedrag waarschijnlijk worden beïnvloed. Dit wordt algemeen aangeduid als het 'chilling effect'. De persoon wordt bewustgemaakt van het (potentieel) deel uitmaken van de observatie van de ander en dus van het feit dat zij een object is, met als gevolg een angstige toestand en het verlies van een zekere mate van autonomie.[133]

Het chilling effect verwijst naar wat bekend staat als het Panoptische effect, verwijzend naar Benthams Panopticon gevangenisontwerp.[134] Wanneer iedereen potentieel onder toezicht kan staan, zal men zich deze externe controle eigen maken. De moraal en de waarden-discipline is dus een soort macht, een strategie en een soort technologie.[135] Zoals Schofield het mooi verwoordde:

> 'Het belangrijkste punt was niet dat de gevangenen van Panopticon voortdurend in de gaten werden gehouden, maar ... dat ze zich ervan bewust zouden zijn dat ze misschien wel in de gaten werden gehouden. De inspecteur zag een overtreding. Hij strafte niet onmiddellijk, maar wachtte. Hij zag een tweede overtreding. Op een gegeven moment zou hij de dader confronteren met zijn recordboek. "Zie hier uw overtredingen, met datum en tijd. Dit is uw straf". Toen eenmaal een straf was opgelegd en de gevangenen zagen dat wanneer ze zich zouden misdragen, de straf

---

[131] Zie ook R. Clarke, 'The regulation of civilian drones' impacts on behavioural privacy', *Computer Law & Security Review Elsevier* 3.

[132] Dit idee werd in 1604 in het Engelse recht verankerd met de uitspraak dat 'het huis van iedere man zijn kasteel is' ('the house of everyman is his castle'); D. Vincent, *Privacy*: *a short history*, Cambridge: Polity 2016, p. 33

[133] B.J. Koops e.a., 'The reasonableness of remaining unobserved: A comparative analysis of visual surveillance and voyeurism in criminal law', *Law & Social Inquiry* 2018, p. 2.

[134] Het verwijst ook naar Foucaults conceptualisering van de discipline, die beschreef hoe Benthams Panopticon gevangenen kon disciplineren.

[135] M. Galič e.a., 'Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation', 30 *Philosophy & Technology* (1) 2016, p. 9-37.

> zeker opgelegd werd, zouden ze zich niet langer misdragen. Er zou geen noodzaak meer zijn om ze in de gaten te houden. Ze zouden worden hervormd'.[136]

Met andere woorden, heimelijke waarneming of ongewenste openlijke waarneming veranderen de feitelijke omstandigheden waarin een persoon kiest en handelt, want wat anderen weten over de persoon kan het beeld dat de persoon van zichzelf heeft radicaal beïnvloeden. Daardoor kan het voor haar onmogelijk zijn om te handelen op de manier waarop ze wil handelen, of om te kiezen op de manier waarop ze wil kiezen (beperking van haar autonomie).

Hoewel de observatie van een ander niet noodzakelijkerwijs schadelijk is, kan observatie in situaties van asymmetrische monitoring, zoals bij spionage, een verlies van autonomie betekenen voor de geobserveerde persoon. Autonomie verwijst hier naar het vermogen van de persoon om de omstandigheden waarin zij door anderen wordt geobserveerd te controleren, wat cruciaal is voor haar vermogen om haar eigen verlangens te vormen en te handelen. Wanneer iemand zich realiseert dat anderen haar hebben geobserveerd of hebben kunnen observeren in omstandigheden waarin zij liever niet geobserveerd was (inclusief maar niet beperkt tot gênante en vernederende situaties), zal er een onvrijwillige verschuiving in het perspectief van de persoon plaatsvinden. Zoals Koops e.a. het verwoordde:

> 'Waar voorheen [de persoon] vrij was om beslissingen te nemen op basis van haar eigen verlangens, moet ze die nu nemen in het licht van de kennis die anderen door ongewenste observatie hebben verworven. Bij het maken van keuzes zal ze waarschijnlijk rekening houden met wat de perceptie van de ander van haar kan zijn en hoe die percepties zijn houding en gedrag ten opzichte van haar kunnen beïnvloeden. Het resultaat is waarschijnlijk remming, zelfcensuur of een neiging tot sussen.'[137]

Hoewel dit de persoon kan raken in haar intellectuele en beslissingsprivacy (in de typologie met name gekoppeld aan de persoonlijke en intieme sfeer), zal dit meestal in de eerste plaats gevolgen hebben voor het gedrag van de persoon in kwestie. Risico's voor gedragsmatige privacy kunnen zich dus in de verschillende sferen voor doen bij het gebruik van spionageproducten, onder andere om dat deze producten de grenzen tussen deze sferen doen vervagen. De belangrijkste privacyrisico risico's voor gedragsmatige privacy volgen dus uit het feit dat hobbydrones activiteiten mogelijk maken die voorheen niet mogelijk waren, zoals het filmen op plekken die normaal afgesloten zijn voor bezoekers.

---

[136] P. Schofield, *Bentham: A Guide for the Perplexed*, New York: Continuum 2009, p. 92; vertaling door onderzoekers.

[137] B.J. Koops e.a., 'The reasonableness of remaining unobserved: A comparative analysis of visual surveillance and voyeurism in criminal law', *Law & Social Inquiry* 2018, p. 3.

4.2.2 Privacyrisico's in privé-plaatsen: ruimtelijke en lichamelijke privacy

In de vorige subparagraaf hebben wij een aantal risico's besproken die zowel in de private sfeer als in publieke sferen kunnen voorkomen. Sommige risico's doen zich echter specifiek voor in de private sfeer. In deze subparagraaf richten we ons op deze risico's. Om weer een indruk te geven van de gevolgen voor mensen van het gebruik van spionageproducten in privéplaatsen geven wij opnieuw eerst een casus beschrijving. Deze casus beschrijving is gebaseerd op een krantenartikel, en illustreert een vaker voorkomend gebruik van minicamera's om mensen heimelijk te bespieden.[138]

Begluurd in de douche

Een eigenaar van een Bed and Breakfast in Hawke's Bay in New Zeeland werd in December 2017 aangehouden omdat hij stiekem opnames had gemaakt van 34 vrouwelijke gasten terwijl zij aan het douchen waren. Hij had op afstand bestuurbare camera's in shampooflessen verstopt en deze flessen in de gedeelde badkamer gezet. Hij sprak tijden af met de gasten waarop zij konden douchen, zodat hij de camera's op afstand kon aanzetten. 's Avonds haalde bij de beelden van de camera's en zette deze vervolgens op een pornografische website. Bij sommige beelden gaf hij ook nog een beschrijving van de vrouw in kwestie, bijvoorbeeld van haar persoonlijkheid. Bezoekers van de site konden commentaar geven op de beelden en over de vrouwen. In totaal heeft de man 219 opnames gemaakt van de vrouwen, waarop niet alleen hun naakte lichaam was te zien maar ook vaak hun gezicht.

Toen de man uiteindelijk opgepakt was en de politie de vrouwen kon inlichten, zeiden meerdere vrouwen in hun aangifte dat zij zich "geshockeerd, beschaamd, boos en gedenigreerd voelden".

Wanneer privéplekken - opgevat als plaatsen waar normaal gesproken weinig mensen aanwezig zijn en kunnen zijn - zoals een huis, hotelkamer of een auto - onder observatie komen, komt ook de ruimtelijke privacy in gevaar. Ruimtelijke privacy verwijst naar het belang om de toegang van anderen te beperken en het gebruik ervan te controleren. Maar zoals hobbydrones, spionagecamera's, GPS-trackers en verborgen microfoons laten zien, kunnen mensen zich echter ook in andermans ruimtelijke privacy begeven door te 'kijken' door ramen of te gluren in douches en door naar gesprekken te luisteren door middel van een afluisterapparaat. In Solove's termen is de schadelijke activiteit hier indringing: invasieve handelingen die de rust of afzondering verstoren. Een dergelijke intrusie verstoort iemands dagelijkse activiteiten, verandert

[138] Deze casus is gebaseerd op een zaak in Nieuw Zeeland. D. Brennan, 'Man hid shower cameras in shampoo bottles to spy on hotel guests and make porn', Newsweek.com 17 april 2020. Met enige regelmaat verschijnen er nieuwsberichten over mensen die anderen bespioneren met een camera in de douche, via een gat in de muur, een camera in een shampoofles of op een andere manier. Zie ook bijvoorbeeld M. Kessel, 'Huisbaas die camera in douche studenten plaatste voor de rechter', AT5.nl 5 januari 2017.

haar routines, beperkt haar afzondering en geeft haar vaak een oncomfortabel, ongemakkelijk en in sommige gevallen een onveilig gevoel.

Dit heeft te maken met de speciale rol die privéplaatsen, met name ons huis en de eigen auto, maar ook hotelkamers, Airbnb accommodaties, en tuinen spelen in ons leven. Op dergelijke plaatsen laten we namelijk onze waakzaamheid verslappen. Naar buiten toe hebben we de neiging om een bepaald beeld van onszelf te presenteren, waarbij we bepaalde zaken accentueren en andere verbergen.[139] Privéplekken zijn de plekken waar we kunnen uitrusten van de druk van het vervullen van deze publieke rollen. Zo kleden we ons bijvoorbeeld meer comfortabel, hebben we vettig haar, plukken we onze neus, lopen we naakt rond, vloeken we hardop en roddelen we over anderen. Ongewenste indringing via spionageproducten in deze ruimtelijke privacy kan leiden tot reputatieschade, verstoring van sociale relaties en, meer in het algemeen, verstoring van iemands identiteitsvorming.

Spionageproducten met een sensor die beelden kan opnemen kunnen ook inbreuk maken op de lichamelijke privacy, zoals in de casus in het begin van deze subparagraaf. Wanneer er sprake is van naaktheid (of gedeeltelijke naaktheid), is er ook sprake van lichamelijke privacy. Het is duidelijk dat dit soort privacyrisico's alleen betrekking heeft op spionageproducten die in staat zijn tot visuele observatie, zoals drones met een camera en spycams. Het plaatsen van een verborgen camera in een douche of het stiekem filmen van mensen op een naaktstrand vormt een inbreuk op de lichamelijk privacy. Hoewel deze vorm van privacy over het algemeen verwijst naar de mogelijkheid om anderen te weerhouden van het aanraken van het lichaam, kan het ook worden aangetast wanneer het lichaam visueel wordt "betreden". Naaktheid wordt vaak geassocieerd met het huis en andere plaatsen die er specifiek voor bedoeld zijn (bijvoorbeeld nudistenstranden en sauna's), maar mensen kiezen er ook voor om naakt te zijn en verwachten ongezien te blijven op openbare plaatsen die afgezonderd zijn.

Het gebruik van spionageproducten kan dus belangrijke risico’s creëren voor ruimtelijke en lichamelijke privacy omdat ze activiteiten mogelijk maken die zonder deze technische hulpmiddelen niet mogelijk zijn. Voor beslissings- en intellectuele privacy hebben wij geen dergelijke zwaarwegende inbreuken kunnen identificeren in ons onderzoek.

4.2.3 Privacyrisico's in semi-private en openbare ruimten: relationele en communicatieve privacy

We beginnen deze paragraaf weer met een casus. Deze keer is het een fictieve casus, gebaseerd op incidenten in Duitsland waarbij ouders de smart watches van hun kinderen

[139] E. Goffman, *Relations in public: microstudies oft he public order*, New York: Basic Books 1971, p. 270.

gebruiken om mee te luisteren in de les op school.[140] Het gaat hier dus om een casus van privacyrisico's van het gebruik van een type sensor.

Meeluisteren tijdens de les

Monica is bezorgd dat haar zoon, Marc, niet goed wordt behandeld door zijn leraren op school. Hij klaagt de laatste tijd vaker dat de wiskundeleraar hem oneerlijk behandeld en hem slechte cijfers geeft. Monica neemt deze klachten serieus en wil meer weten. Ze vindt in een online webwinkel een horloge met verschillende functies, zoals een camera, microfoon en een GPS-tracker, maar ook een functie om audio-opnames direct via Wifi te versturen naar een gelinkt smartphone.[141] Monica kan zo mee luisteren met wat er in de les wordt gezegd. Ze bestelt het horloge en geeft het Marc mee met de instructie om de microfoon aan te zetten tijdens de wiskundeles.

De volgende dag tijdens wiskunde zet Marc de microfoon op zijn horloge aan en Monica luistert mee met wat er gezegd wordt in de klas. De kinderen lossen sommen op het schoolbord op. De leraar roept Marc naar voren om een som op te lossen, een die hij heel moeilijk vindt. Wanneer het hem niet lukt, begint hij te klagen dat hij altijd de moeilijke sommen krijgt. De leraar ontkent dit en geeft hem een standje omdat hij niet goed voorbereid naar de les komt, zelfs nadat ze deze sommen hebben opgelost in de laatste paar dagen. Op dit moment, hoor de klas een vreemde vrouwelijke stem en als snel hebben de leraar en studenten door dat stem uit het horloge van Marc komt. Monica spreekt de leraar aan via de smartwatch, en verwijt de leraar dat hij haar zoon harder aanpakt dan de andere leerlingen. De wiskunde leraar is niet voorbereid op zo een inbreuk in de les en voelt zich heel oncomfortabel. Na een korte reactie richting Monica, sommeert hij Marc om de microfoon en de verzendfunctie uit te zetten op het horloge en besluit het incident te melden bij het hoofd van de school. De volgende dagen tijdens de les observeert hij aandachtig de horloges van de studenten en merkt hij dat hij zichzelf ongewild censureert, bang dat andere bozen ouders aan het meeluisteren zijn tijdens de klas.

Privacy-inbreuken kunnen optreden als we met andere mensen en buitenshuis zijn, met name op semi-private plekken, zoals leslokalen, cafés, treincoupés en de wachtruimte in een gezondheidscentrum, maar ook in de openbare ruimte. Mensen verwachten namelijk 'ruimte' van anderen, ook als ze bij of in de buurt van anderen zijn. Dit hangt samen met het concept van 'persoonlijke ruimte', een soort kleine beschermende luchtbel die we om ons heen dragen om ons van anderen te scheiden en die ons comfort, gemak en ontspanning biedt in niet-intieme sociale

[140] 'Eltern spionieren ihre Kinder mit Abhör-Uhren aus - jetzt reagiert der Staat', Hna.de 17 april 2020; 'Bundesnetzagentur geht gegen Kinderuhren mit Abhörfunktion vor', Bundesnetzagentur.de 17 april 2020.

[141] Zie voor een aantal voorbeelden van smartwatches bijvoorbeeld 'Top 10 smartwatches voor kinderen', Mamaliefde.nl 17 april 2020 en 'Smartwatch review: Beste smartwatches voor kinderen', Smartwatchreview.nl 17 april 2020.

interacties.[142] Wanneer de omstandigheden mensen dwingen dichterbij te komen, bijvoorbeeld in liften of drukke bussen, zullen zij gebruik maken van mechanismen van discretie (zoals het afwenden van de ogen en het recht naar beneden houden van de armen) om te laten zien dat zij niet opzettelijk de persoonlijke luchtbellen van anderen binnendringen.[143] Hobbydrones met videocamera's en geluidssensoren, en spionageproducten in enge zin, kunnen zich duidelijk gemakkelijk in deze persoonlijke ruimte begeven en informatie over ons vastleggen die anders niet (gemakkelijk) toegankelijk zou zijn. Inbreuk buitenshuis (of een andere privéruimte) kan dus leiden tot extra inmenging met de relationele privacy.[144]

Hoewel de privacyrisico's die voortvloeien uit het gebruik van spionageproducten (zowel in brede als enge zin), zoals beschreven in het bovenstaande geval, over het algemeen niet afhankelijk zullen zijn van het type sensor, zijn er een paar uitzonderingen. Met name spionageproducten met een auditieve sensor kunnen inbreuk maken op communicatieve privacy. Communicatieve privacy verwijst naar het belang dat iemand heeft bij het beperken van de toegang tot (al dan niet bemiddelde) communicatie of het controleren van het gebruik van informatie die aan derden wordt meegedeeld. Deze vorm van privacy zal vooral worden verstoord wanneer er gebruik wordt gemaakt van auditieve sensoren. Hoewel de communicatieve privacy ook vanuit de woning of de tuin kan worden aangetast, hebben personen vaak ook buiten de woning privégesprekken. Vriendinnen delen details over hun relaties en collega's bespreken hun werk of hun bazen. Mensen praten soms over diep persoonlijke zaken met vreemden, vooral op 'bepaalde plaatsen waar de echte wereld "buiten" lijkt te worden opgeschort - zoals treinen, boten en bars - [die] zich lenen voor een vrij gesprek'.[145] Ondanks hun verscheidenheid wekken dergelijke gesprekken een hoge verwachting van privacy, vooral wanneer mensen zich inspannen om de uitwisseling privé te houden (bijvoorbeeld door te fluisteren of dichter bij elkaar te komen als iemand anders dichterbij komt).[146] Dit komt omdat onze communicatie met anderen meestal in een sterk afgebakende regio plaatsvindt en beperkt is in de tijd. Ze zijn ook sterk afhankelijk van de context. Zo is het leslokaal een omgeving waarin men ervanuit gaat dat een selecte groep mensen betrokken is in de interactie, in het bovenstaande voorbeeld de leerlingen, en dus niet alle ouders van de studenten. Spionageproducten in brede en enge zin maken het mogelijk om deze vormen van communicatie stiekem op te nemen, te verspreiden en zelfs te manipuleren.

---

[142] E.T. Hall, *The hidden dimension*, New York: Anchor Books, p. 119; evenzo I. Altman, The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding, Monterey: Brooks/Cole Publishing Company 1975; R. Sommer, Personal space; the behavioral basis of design, Michigan: Prentice-Hall 1969; G. Simmel, 'Exkurs über den Fremden', in: G. Simmel, Soziologie: Untersuchungen über die Formen der Vergesellschaftung, Berlin: Duncker & Humblot 1908, p. 509-512.

[143] B.J. Koops, 'Privacy spaces', West Verginia Law Review 2018, p. 631

[144] D.J. Solove, 'A Taxonomy of Privacy', 154 University of Pennsylvania Law Review (3) 2006.

[145] A.F. Westin, *Privacy and freedom,* London: The Bodley Head 1967, p. 38.

[146] B.J. Koops, 'Privacy spaces', *West Verginia Law Review* 2018, p. 637.

Soms is de informatie in kwestie gevoelig of vertrouwelijk, zodat een buitenstaander, als hij deze verwerft, veel macht kan verwerven over de gesprekspartners. De informatie kan gebruikt worden om een collega of een concurrent dwars te zitten, mensen onder druk te zetten of beslissingsprocessen te beïnvloeden.

Een ander type privacy die aangetast kan worden door het gebruik van spionageproducten in semi-private of publieke ruimtes is relationele privacy. Relationele privacy is gerelateerd aan het ontwikkelen en onderhouden van gevarieerde en betekenisvolle interpersoonlijke relaties.[147] Met andere woorden, individuen hebben er belang bij vrij te zijn om te kiezen met wie ze willen communiceren, inclusief vrienden, verenigingen, groepen en gemeenschappen. Hoewel privacy meestal wordt geassocieerd met eenzaamheid en intieme relaties, speelt het in feite een belangrijke rol bij het vormen van sociale relaties.[148] We bouwen namelijk onze sociale identiteiten niet alleen (of zelfs vooral) op door de nauwste banden met anderen te ontwikkelen (bijvoorbeeld tussen familie, geliefden en naaste vrienden, waarbij persoonlijke, biografische, eigenzinnige en vaak emotionele aspecten van het zelf worden gedeeld), maar ook door lossere banden te vormen met die zelfde en die verschillende aspecten van het individu, waarbij slechts zeer beperkte categorieën van het individu in de interactie worden betrokken.[149] Dit omvat sociale interactie met een breed scala aan actoren, waaronder kennissen, collega's, vreemden, professionele relaties (bijv. interactie met een arts), en andere secundaire soorten relaties. Met andere woorden, het is niet alleen dat privacy het sociale leven *draaglijk* maakt,[150] het is ook dat privacy het sociale leven mogelijk maakt. Zoals Kasper het uitdrukte: “De vorming en het behoud van sociale relaties hangt zowel af van discretie, verbergen en terugtrekken als van openheid, openbaring en samenkomen.”[151]

Aangezien sociale interacties op allerlei plekken kunnen plaatsvinden, kan ook de relationele privacy op al deze plekken in het geding zijn. Aangezien de meeste vormen van associaties (dwz. relaties) zich echter voordoen in de semipublieke en openbare ruimte, is dit type privacy het meest aan de orde wanneer de spionage ook in die ruimtes plaatsvindt.

Relationele privacy kan worden geschonden door middel van heimelijke observatie in welke vorm dan ook (visuele, auditieve of locatiebepaling) en kan leiden tot gebrekkige sociale relaties. Zo is

---

147 C. Fried, ‘Privacy (a moral analysis), in: F.D. Schoeman (red.), *Philosophical dimensions of privacy: an anthology*, Cambridge: Cambridge University Press 1984; J. Rachels, ‘Why privacy is important, in: F.D. Schoeman (red.), *Philosophical dimensions of privacy: an anthology*, Cambridge: Cambridge University Press 1984; B. Roessler & D. Mokrosinska, ‘Privacy and social interaction’, 39 *Philosophy and Social Criticism* (8) 2013, p. 771-791.

148 Bijv. I. Altman, *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding,* Monterey: Brooks/Cole Publishing Company 1975; K. Merton, *Social theory and social structure*, New York: The Free Press 1968; G. Simmel, *The Sociology of Georg Simmel*, New York: The Free Press 1964.

149 L.H. Lofland, *The Public Realm Exploring the City's Quintessential Social Territory*, Abingdon-on-Thames: Routledge 1998, p. 54.

150 J.A. Oravec, ‘The transformation of privacy and anonymity: beyond the right to be let alone’, 31 Sociological imagination 1 2003.

151 D.V.S Kasper, ‘Privacy as a social good’, 28 Social thought & research 2007, p. 175.

bijvoorbeeld gebleken dat het niet voldoen aan de verwachtingen ten aanzien van de privacy op de werkplek leidt tot onzekerheid bij de werknemers, een aanzienlijke verslechtering van de werksfeer en een algemene verslechtering van de motivatie van de werknemers - uiteindelijk tot 'disfunctioneel rolgedrag'.[152] Volgens Roessler en Mokrosinska hebben we in het licht van deze externe bedreiging op de relationele privacy niet alleen 'privacy (van individuen) *binnen* de relatie' nodig (deelnemers van de relatie die zich aan de privacy normen houden), maar ook - en in toenemende mate - 'privacy *van* de relatie'.[153] Met andere woorden, we hebben privacy nodig bij de vorming en uitvoering van de relatie. Door de brede beschikbaarheid van spionageproducten is de macht om toezicht en controle uit te oefenen op met wie een persoon wel of niet mag omgaan (bijvoorbeeld door het plaatsen van spionagecamera's in het favoriete café van een geliefde) sterk uitgebreid.

Naast het belang voor het individu, heeft relationele privacy heeft een belangrijke waarde voor de democratie. Spionageproducten en drones kunnen gebruikt worden om mensen te verhinderen zich te verenigen en te protesteren. Een belangrijk doel van activisme en protesteren is 'gezien' of, beter gezegd, 'gehoord' worden, maar er is hier sprake van een bepaalde vorm van zichtbaarheid. Om deel te nemen aan democratische politiek, moet men op een specifieke manier worden gezien. Het idee is niet dat personen individueel identificeerbaar zijn of zouden moeten zijn (behalve wanneer een individu persoonlijke identificeerbaarheid zoekt om een persoonlijke claim in te stellen). Integendeel, een zekere mate van obscuriteit (vaak anonimiteit genoemd), met name ten opzichte van de staat, maar ook ten opzichte van andere burgers met verschillende politieke opvattingen, is vereist om veel van de politieke rechten, met name de vrijheid van meningsuiting, te kunnen uitoefenen.[154] Wanneer de identiteit van personen gemakkelijk herkenbaar wordt gemaakt door middel van verschillende soorten sensoren (video, audio of locatie tracking), kan de politieke participatie en vereniging van personen worden verstikt. In die zin kan worden gezegd dat er sprake is van inmenging in hun relationele privacy.

Een dergelijk toezicht houdt niet alleen risico's in voor individuele relaties (verenigingen), maar houdt ook risico's in voor de samenleving en het sociale leven in het algemeen. Toezicht kan namelijk de gezelligheid en openheid van de openbare ruimte aantasten, met name door het vertrouwen in de openbare ruimte aan te tasten. Democratie vereist zowel inclusie als verbondenheid tussen burgers. Dit is belangrijk om twee algemene redenen. Ten eerste omdat gemeenschap alleen mogelijk is als er sprake is van interpersoonlijke communicatie en sociale ontmoetingen. En ten tweede omdat individuen, groepen en mensenmassa's een

---

[152] B. Roessler & D. Mokrosinska, 'Privacy and social interaction', 39 *Philosophy and Social Criticism* (8) 2013, p. 780.

[153] Ibid, p. 775.

[154] H. Arendt, *On revolution*, London: Penguin Books 2006; cf. G. Agamben, *Nudities*, Stanford: Stanford University Press 2011; O. Kudina & M. Baş, '"The end of privacy as we know it": Reconsidering public space in the age of Google Glass', *Routledge* 2018, p. 126; M.H. Nagenborg, 'Hidden in plain sight: Conceptual and Regulatory Challenges', Edward Elgar 2017, p. 47-63.

gemeenschappelijk 'podium' nodig hebben waar ze - zichtbaar voor anderen - politieke subjecten worden. Burgers moeten dus in staat zijn om met elkaar te communiceren en met elkaar om te gaan in een gemeenschappelijke (openbare) ruimte, buiten intieme en andere nauwe relaties om. Hoewel door de uitbreiding van het toezicht, met name het toezicht door de staat, sommige mensen zich veiliger zouden kunnen voelen (hoewel ook dat wordt betwist),[155] leidt het ook tot toenemende angst, wantrouwen en zelfs racistische paranoia onder mensen.[156] Als te veel plaatsen (potentieel) willekeurig worden bewaakt, dan kan iedereen die daar aanwezig is zich onbetrouwbaar gaan voelen. Bovendien zou men, in de veronderstelling dat er reden is om een hoog niveau van toezicht in een bepaalde openbare ruimte te plaatsen, kunnen beginnen te kijken naar anderen - vreemden - in de openbare ruimte met een verhoogde mate van argwaan.

4.2.4 Solove's activiteiten die informationele privacy schaden

De volgende casus van een vrouw die door haar ex-partner wordt gevolgd met behulp van een GPS-tracker, schets een beeld van de risico's van het gebruik van spionageapparatuur op het gebied van informationele privacy. Deze casus is gebaseerd op een zaak uit de VS.[157]

Ik weet wat je allemaal hebt gedaan

In 2018 bracht de Amerikaanse zender National Public Radio (NPR) een rapportage over een zaak van vrouw wiens ex-partner een GPS-tracker gebruikte om haar in de gaten te houden.[158] In de zomer van 2016 kreeg de vrouw M. het ongemakkelijke gevoel dat ze gevolgd werd door haar ex. Zij had hem een jaar eerder verlaten omdat de fysieke mishandelingen steeds erger werden. Ze was bang voor haar ex en verbleef op verschillende plekken uit veiligheidsoverwegingen. Uit de stukken van de rechtbank bleek echter dat haar ex precies wist waar ze was geweest, met wie en wanneer. Ze paste, volgens de NPR-journalisten, haar gedrag daarop aan: in de auto reed ze extra rondjes of heel langzaam, voor het geval dat ze gevolgd werd door een privédetective. Maar ze zag nooit iemand haar volgen. Na wat zoeken op het internet kwam zij te weten over GPS-trackers. Ze zocht deze eerst zelf in haar auto -die nog op hun beider naam stond- maar kon niks vinden. Toen ze later haar auto liet nakijken bij de garage vond de monteur een GPS-tracker die er al een zeker paar weken op had gezeten, afgaande op het laadniveau van de batterij.

Voor M. was dit een zeer beangstigende ervaring "Ik ben mij nu heel bewust dat al die keren dat ik dacht dat ik mijzelf in veiligheid bracht - dat ik de stad uit ging, dat ik op verschillende plekken

---

[155] C. Norris, 'From personal to digital: CCTV, the panopticon, and the technological mediation of suspicion and social control, in: D. Lyon (red.), *Surveillance as social sorting: privacy, risk and digital* discrimination, Oxon: Routledge 2003.

[156] M. Davis, *The city of quartz: excavating the future in Los* Angeles, London: Verso 2006.

[157] De beschrijving van deze zaak is gebaseerd op de NPR rapportage: A. Shahani & L. Silverman, 'I know where you've been: Digital spying and divorce in the smartphone age', Npr.org 17 april 2020.

verbleef, dat ik bij vrienden bleef - dat ik nooit veilig was". Tijdens het verhoor bij de politie, vertelde M. dat ze verschrikkelijk bang was: "Ik functioneer misschien nog wel, maar dat betekent niet dat is vreselijk bang ben." Volgens de journalisten, dacht M. dat haar ex ook andere spionageproducten had gebruikt om de controle over haar te behouden, zoals spionagesoftware op haar telefoon. Ten tijde van de rapportage was ze nog altijd bang dat haar ex haar kon volgen met behulp van spionageproducten en voelde ze zich nooit helemaal veilig.

Privacyrisico's die voortvloeien uit het gebruik van spionageproducten in de persoonlijke, semi-private en publieke sfeer houden verband met het inherente gevaar van het gebruik van informatie- en communicatietechnologieën, die het verzamelen en verwerken van informatie mogelijk maken. In deze zin verwijzen we naar informationele privacyrisico's die in detail worden beschreven in de taxonomie van Solove (zie 4.1.2). Het gebruik van spionageapparatuur kan de effecten van de observatie op de autonomie van personen aanzienlijk versterken. Zodra gegevens (in de vorm van een beeld, een video- en geluidsopname of een kaart van locaties) zijn verzameld en/of geaggregeerd, kunnen ze worden gebruikt om personen te identificeren en vervolgens kunnen deze verder worden verspreid. Opnamemateriaal haalt de geobserveerde persoon ook uit zijn oorspronkelijke context en plaatst hem of haar in een andere context, waardoor de persoon controle verliest over hoe zij zichzelf presenteert naar de buitenwereld.[159] De technologische ontwikkelingen op het gebied van spionageproducten, zoals goedkopere, kleinere en krachtigere sensoren, snellere communicatie op grotere schaal en grotere opslagcapaciteit, kunnen deze risico's vergroten.

Bovendien bestaat het risico dat de persoon met de digitale informatie deze op een later tijdstip op de een of andere schadelijke manier kan gebruiken. Beeld- en geluidopnames van mensen die zich onbespied wanen en wellicht beschamend gedrag vertonen dat anders alleen zou worden waargenomen door andere aanwezigen op een locatie zoals een feest, lopen nu het risico om gezien of gehoord te worden door een veel groter publiek als het materiaal op Youtube-video of een ander internetplatform terecht komt. Bovendien is het door de wijdverbreide verspreiding van de video's mogelijk dat de personen die zich in deze gênante situaties bevinden, relatief gemakkelijk kunnen worden geïdentificeerd. Een dergelijke identificatie kan een negatieve invloed hebben op hoe iemand zich voortaan gedraagt in het openbaar. Het privacybelang ligt hier in de bescherming van personen die zich in een hulpeloze situatie bevinden, al dan niet vanwege hun eigen schuld (zoals in het geval van dronken personen) of niet (bijvoorbeeld slachtoffers van verkeersongevallen).

[159] Helen Nissenbaum's theorie van privacy als contextuele integriteit laat zien hoe de context van belang is bij privacyverwachtingen. H. Nissenbaum, *Privacy in context: technology, Policy, and the Integrity of Social Life,* California: Stanford University Press 2009.

Heimelijke waarneming kan ook de waarnemer in staat stellen een grote hoeveelheid informatie te verzamelen over degene die is waargenomen, waardoor de waarnemer een bijzondere macht over deze persoon kan krijgen. De zaak van M. laat zien dat hoe heimelijk verkregen informatie te positie van de waarnemer kan versterken en waardoor deze op afstand controle kan uit oefenen. De ex van M. kan na een lange periode van korte observaties van haar ritten met de auto, informatie verzamelen over met wie zij contact heeft, de plekken die zij bezoekt en wat zij dagelijks doet. Dit stelt hem in staat om informatie te verzamelen voor de rechtszaak, maar ook om M. te beperken in haar dagelijkse activiteiten en contacten en haar te laten weten dat ze op haar hoede moet blijven. Spionageproducten, zoals GPS-trackers en spionagesoftware, worden steeds vaker voor dergelijke doeleinden ingezet en de technologische ontwikkelingen maken het makkelijker en goedkoper. Volgens een recente rapportage van RTL Nieuws zijn het aantal stalkerware-infecties op mobiele telefoons van enkele honderden in 2018 opgelopen naar meer dan 6500 in 2019.[160]

De casus laat ook zien dat heimelijke observatie, vooral wanneer de bewaakte persoon zich bewust is van de mogelijkheid van observatie, een *chilling effect* kan hebben. Als mensen zich bewust zijn van de mogelijkheid dat ze stiekem waargenomen worden door bijvoorbeeld een GPS-tracker, geheimen camera's of een stille drone en dat er informatie wordt verzameld die hen mogelijk kan schaden, kan dat hun handelen en denken beïnvloeden. *Informatieverzameling*, zoals beschreven door Solove, met spionageproducten kan dan een activiteit zijn die de privacy schaadt.

Als de kans dat men achter de spionage komt zeer gering is, dan ligt het gevaar in de macht die kan worden opgebouwd. De activiteiten uit Solove's taxonomie die hierbij centraal staan zijn *informatieverwerking* en *informatieverspreiding*. Spionage met het gebruik van verschillende digitale apparaten, verandert namelijk de anders (min of meer) gelijke machtsverhoudingen tussen burgers. Door middel van spionage kan de spionerende burger een zekere macht verzamelen over de bespioneerde burger. Spionage is asymmetrische surveillance op afstand. Bij visuele observatie kunnen bijvoorbeeld problematische machtsverhoudingen ontstaan tussen actieve mannelijke waarnemers en passieve vrouwelijke observatieobjecten.[161] Dit type machtsverhoudingen is uitgebreid onderzocht in relatie tot mannelijke CCTV-operators die voor persoonlijk genot inzoomen en de specifieke lichaamsdelen van de vrouw registreren.[162]

Bovendien, als iemand lang genoeg wordt bekeken, kan hij of zij worden betrapt op een of andere vorm van illegale of immorele activiteit, en deze informatie kan vervolgens worden

---

[160] 'Gehackt door je partner: duizenden mensen bespioneerd via stalkerware', Rtlnieuws.nl 17 april 2020. Zie ook Kaspersky, 'The State of Stalkerware in 2019', Securelist 2 oktober 2020.

[161] A.M. Brighenti, 'Visibility: A Category for the Social Sciences', 55 Current sociology 3 2007, p. 355.

[162] Zie bijv. H. Koskela, 'Video surveillance, gender, and the safety of public urban space: "Peeping Tom" goes tech', 23 Urban geography 3 2002.

gebruikt om haar in diskrediet te brengen of zelfs te chanteren. Met andere woorden, het veelgebruikte argument voor (véél) toezicht - 'we hebben niets te verbergen' - is niet steekhoudend. Solove geeft het voorbeeld van de FBI's uitgebreide afluisterpraktijken van Martin Luther King, Jr., waarvan algemeen wordt aangenomen dat ze zijn geïnitieerd om de vermeende communistische banden van King bloot te leggen. Hoewel het toezicht geen enkel bewijs van dergelijke banden aan het licht bracht, bracht het wel King's buitenechtelijke relaties aan het licht. Dit stelde de FBI in staat om te proberen King te chanteren met de informatie en om de informatie te lekken om King in diskrediet te brengen.[163]

Digitale informatie kan bovendien worden bewerkt en verspreid om mensen in diskrediet te brengen. Door opgenomen beelden of gesprekken selectief te tonen, los van de oorspronkelijke context, aan een groter publiek of door de opnames te bewerken kan een kwaadwillende partij het imago van de geobserveerde aantasten. Als een van de bewoners, bijvoorbeeld een keer, uit zijn slof zou schieten na de meerdere langs vliegende drones getolereerd te hebben en vloekend en tierend op beeld wordt vastgelegd, zou dat beeld gebruikt kunnen worden om de molenbewoners in een kwaad daglicht te stellen. Hier is de schade van verstoring zichtbaar. Volgens Solove heeft een dergelijke vervorming niet alleen gevolgen voor de gedupeerde individuen, maar ook voor de samenleving in het algemeen, omdat dit het vermogen beperkt om het karakter van de mensen waarmee men te maken heeft, te beoordelen.

Tot slot kan het aggregeren van informatie met behulp van spionageproducten privacy schade, aangezien de verblijfplaats van een persoon (verleden en heden) veel kan onthullen over zijn activiteiten en gedrag. In het geval van M. de gevolgd werd door haar ex-partner, zou de ex de locatie van M. kunnen gebruiken om erachter te komen of zij een nieuwe vriend heeft of niet. Door het vinden van het adres dat ze regelmatig laat in de avond bezoekt en dit adres in te voeren in Google Maps, kan hij vaststellen dat het een privéadres is (in plaats van een bedrijf). Door haar in zijn eigen auto te volgen, kan hij bovendien zeker weten of ze een nieuw vriend heeft en kan hij hem identificeren.

4.3 Conclusie: belangrijkste privacyrisico's

In dit hoofdstuk hebben wij verkend welke privacy-inbreuken zich kunnen voordoen bij het gebruik van spionageproducten in enge zin en hobbydrones en wat de voornaamste privacyrisico's zijn. Op basis hiervan kunnen wij antwoord geven op deelvraag 3. Zoals wij hebben gezien zijn er verschillende soorten privacyrisico's verbonden aan het gebruik van spionageproducten, zowel in enge als in brede zin.

---

[163] D.J. Solove, 'A Taxonomy of Privacy', 154 University of Pennsylvania Law Review (3) 2006.; see also Garrow, *The FBI and Martin Luther King, Jr.*, Open Road Media 1981.

Bij spionageproducten in enge en brede zin doen de belangrijkste privacyrisico's zich enerzijds voor in het intieme (of persoonlijke) deel van het privéleven, dat tot de 'kern' van privacy behoort. Waar men in het nabije verleden nog ongewenste anderen kon uitsluiten van zijn huis of van het observeren van delen van zijn lichaam, is dat tegenwoordig steeds moeilijker. Een inbreuk op de **ruimtelijke** of **lichamelijke privacy** kan nu plaatsvinden op manieren die voorheen onmogelijk waren (bijvoorbeeld een drone die in het raam van een appartement op een hoge verdieping kijkt of minicamera's die personen in een sauna bespioneren) en op grote schaal (iedereen kan spionageproducten op een dergelijke manier gebruiken en de opnames vervolgens online verspreiden).

Aan de andere kant zijn er ook belangrijke privacyrisico's in de semi-private en publieke sfeer die vooral betrekking hebben op de **gedragsmatige, communicatieve** en **relationele privacy**. Andere uitsluiten, zoals nodig is bij ruimtelijke en lichamelijke privacy, is hier niet mogelijk. Toch hebben mensen tot nu toe ook in de (semi-)publieke ruimte een behoorlijke mate van privacy genoten - beperkingen met betrekking tot de menselijke waarneming en het menselijk geheugen lieten dat toe (men kan alleen maar zoveel observeren en onthouden). Vanwege het huidige aanbod aan digitale spionageproducten kunnen mensen tegenwoordig niet langer een vergelijkbaar niveau van privacy verwachten in (semi-)publieke ruimtes. Er zijn nieuwe vormen van indringing mogelijk (bijv. privégesprekken die men in een bar tegen een goede vriend fluistert kunnen nog steeds worden opgenomen) en deze kunnen plaatsvinden op een schaal die voorheen onmogelijk of onwaarschijnlijk was (bijv. de bewegingen van de persoon kunnen door een locatietracker over een langere periode worden gevolgd). Bovendien is er een cumulatief effect van het verwachten van steeds minder privacy in de (semi-)publieke ruimte, welke een nadelig effect hebben op de gedragsmatige en relationele privacy. Het kan leiden tot ongewilde veranderingen in het gedrag van mensen (bijvoorbeeld mensen kunnen zich minder vrij voelen om zichzelf te zijn), de communicatie tussen mensen (bijvoorbeeld door minder vertrouwen kunnen mensen hun mening niet zo vrij uiten) en hun relaties met anderen (bijvoorbeeld mensen kunnen minder associëren met bepaalde anderen in de fysieke ruimte).

Tot slot zijn er ook privacyrisico's met betrekking tot **informationele privacy**. Zoals in 4.2.4 wordt uitgelegd, leidt het gebruik van informatie- en communicatietechnologieën, die het verzamelen en verwerken van informatie mogelijk maken tot een inherent gevaar van verspreiding of een of ander schadelijk gebruik van de informatie (bijv. schending van de geheimhouding of chantage). Bovendien vergroten deze technologieën de schaal waarop informatie kan worden verspreid en vergroten zij de mogelijkheden om informatie uit verschillende bronnen aan elkaar te knopen. Stiekem opgenomen digitale filmpjes of foto's zijn makkelijke gedeeld met een groot publiek via websites of sociale media, met mogelijk grote gevolgen voor de veiligheid en reputatie van de geobserveerde.

5 Nederlandse rechtsverkenning en reguleringsmogelijkheden

Dit hoofdstuk betreft een inventarisatie van de Nederlandse wet- en regelgeving die van toepassing is op hobbydrones en spionageproducten in enge zin in de horizontale relatie. Hier geven we het antwoord op de vierde deelvraag van deze verkenning: *In welke mate worden de geïdentificeerde privacyrisico's voorkomen of beperkt door huidige of aanhangige wet- en regelgeving? Wat zijn de (mogelijke) lacunes?* Om de resultaten van de juridische analyse en de implicaties daarvan tastbaar te maken, geven we waar relevant ook een palet aan opties hoe de geïdentificeerde lacunes kunnen worden aangepakt. In dit hoofdstuk beantwoorden we dus ook de eerste deel van de achtste deelvraag: *Welke oplossingsrichtingen zijn er voor het Nederlandse beleid om de privacyrisico's door gebruik van spionageproducten (waaronder hobbydrones) door burgers te voorkomen of beperken, gelet op de gesignaleerde reguleringslacunes (vraag 4)?* Het tweede deel van deze vraag dat betrekking heeft op praktische waarborgen beantwoorden wij in Hoofdstuk 7 (para. 7.2.1 en 7.2.2).

Sectie 5.1 richt zich op grondrechten, 5.2 op het privaatrecht, 5.3 betreft het portretrecht, 5.4 het strafrecht, 5.5 algemene plaatselijke verordeningen en 5.6 de luchtvaartwetgeving. Om herhaling te voorkomen, geven we geen gezamenlijke conclusie, maar geven we aan het eind van elke paragraaf een deelconclusie met antwoorden op deelvragen 4 en 8. We moeten er ook op wijzen dat de onderzochte soorten wetgeving veelal de privacy op een algemene manier beschermen; wanneer een bepaalde bepaling gericht is op, of gebruikt kan worden voor, de bescherming van specifieke soorten privacy, zullen we dit specificeren.

De analyse van de mate waarin het huidige wettelijke kader in Nederland de privacyrisico's van hobbydrones en spionageproducten in enge zin afdekt (deelvraag 4) en de reguleringsmogelijkheden voor Nederland (deelvraag 8), hebben wij uitgevoerd middels klassiek juridisch-dogmatisch onderzoek en analyse van wetenschappelijke literatuur (zie par. 2.5.1).

5.1 Grondrechten, privacy en gegevensbescherming

Er is een aantal rechtsprincipes relevant in het kader van het recht op privacy en gegevensbescherming, zoals artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM),[164] waarin het recht op de bescherming van het privé- en familieleven, de woning en communicatie is vervat, artikelen 10 (persoonlijke levenssfeer), 11 (lichamelijke integriteit), 12 (onschendbaarheid woning) en 13 (briefgeheim) van de Nederlandse Grondwet[165] en het gegevensbeschermingsrecht, zoals dat met name in de Algemene Verordening

[164] [Europees] Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden.
[165] Grondwet.

Gegevensbescherming (AVG) van de Europese Unie (EU) is vervat.[166] Hieronder zal eerst op het recht op privacy, zoals vervat in artikel 8 EVRM en uitgewerkt in de jurisprudentie van het Europees Hof voor de Rechten van de Mens, worden ingegaan. Dit zal slechts kort gebeuren, omdat deze doctrine primair ziet op verticale relaties en slechts indirect, door de horizontale werking van grondrechten en de positieve verplichting van de staat om de rechten van burgers ook tegen inmenging van derden te beschermen, op privacyschendingen in horizontale verhoudingen. Daarna wordt ingegaan op de implicaties van het gegevensbeschermingsrecht voor het gebruik van hobbydrones en spionageproducten in enge zin.[167] Het recht op gegevensbescherming is nader uitgewerkt in de AVG, maar is ook te zien als fundamenteel grondrecht, zoals onder meer volgt uit artikel 10 lid 2 van de Nederlandse Grondwet en artikel 8 van het Handvest van de Grondrechten van de Europese Unie.[168]

5.1.1 Het recht op privacy

De materiële reikwijdte van Artikel 8 van het EVRM is sinds de jaren ’50 van de vorige eeuw, toen het Verdrag werd aangenomen, flink uitgebreid. Aanvankelijk was het bedoeld als negatief en verticaal afweerrecht, dat primair negatieve verplichtingen voor de staat met zich bracht. Het EHRM heeft echter, met de living instrument doctrine in de hand, de reikwijdte van het recht op privacy stelselmatig uitgebreid. Artikel 8 EVRM biedt niet langer alleen bescherming aan negatieve rechten voor burgers, het omvat volgens het EHRM ook veel positieve rechten: het vereist niet alleen dat staten zich onthouden van misbruik van hun bevoegdheden, maar ook dat zij hun bevoegdheden gebruiken om de burger actief te beschermen.

Meer in het algemeen biedt artikel 8 EVRM, en dan in het bijzonder het begrip ‘privéleven’, bescherming aan vrijwel alles dat enigszins raakt aan persoonlijke belangen en de persoonlijke ontwikkeling van een individu.[169] Ook aan de andere drie elementen van artikel 8 EVRM, de bescherming van het familieleven, de woning en de correspondentie, is door het EHRM een ruime reikwijdte toegekend. Bovendien heeft het recht op privacy andere rechten die in het EVRM zijn vervat in meer of mindere mate opgeslokt, wordt naar artikel 8 EVRM verwezen om belangen te beschermen die expliciet uit het Verdrag zijn geweerd door de verdragsopstellers en wordt naar deze bepaling verwezen door het EHRM als het gaat om nieuwe rechten

---

[166] B.H.M. Custers e.a., *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Amsterdam: Boom Lemma Uitgevers 2015.
[167] Voor drones specifiek kunnen ook privacy beperkingen volgen uit: Uitvoeringsverordening (EU) 2019/947 van de Commissie van 24 mei 2019 inzake de regels en procedures voor de exploitatie van onbemande luchtvaartuigen (*PbEU* 2019, L 152/45).
[168] Handvest van de Grondrechten van de Europese Unie (2016/C 202/02).
[169] Zie uitgebreider: B. van der Sloot, ‘Privacy as personality right: why the ECtHR’s focus on ulterior interests might prove indispensable in the age of Big Data’, 80 *Utrecht Journal of International and European Law,* 2015, p. 25-50; B. van der Sloot, ‘Where is the harm in a privacy violation? Calculating the damages afforded in privacy cases by the European Court of Human Rights’, 4 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 2017.

bescherming te bieden. Hieronder zal daarvan een aantal voorbeelden worden gegeven, voor zover die relevant zijn in relatie tot spionageproducten en drones.

1. Privéleven: hoewel het recht op bescherming van het privéleven oorspronkelijk was beperkt tot persoonlijke zaken in het privédomein, biedt het momenteel bescherming aan bijna elk aspect van iemands leven. Zo valt onder de bescherming van het privéleven onder meer de persoonlijke ontwikkeling van een individu, toegang tot onderwijs, de ontwikkeling van sociale relaties (relationele privacy), privacy in het publieke domein (met name gedragsmatige privacy) en het biedt in bepaalde gevallen zelfs bescherming tegen ontslag, omdat het EHRM van mening is dat werk belangrijk is voor de persoonlijke ontwikkeling van een mens. Dit heeft twee belangrijke implicaties in relatie tot spionageproducten in enge zin en hobbydrones. Ten eerste geldt het recht op privéleven ook in de publieke ruimte; het Europees Hof voor de Rechten van de Mens benadrukt dat het juist op het werk, in sociale relaties en in het publieke domein is waar mensen zich ontplooien en tot wasdom kunnen komen. Ten tweede kan ook een chilling effect als gevolg van de wetenschap dat iemands privacy kan worden geschonden als een inbreuk op Artikel 8 EVRM worden gezien.

2. Woning: hoewel het Europees Hof voor de Rechten van de Mens in zijn vroege jurisprudentie een vrij traditionele benadering koos ten aanzien van wat onder het begrip ‘woning’ kon worden verstaan, valt in de huidige interpretatie van het EHRM vrijwel elk object waar een persoon woont, leeft of anderszins aan verbonden is daaronder. Het EHRM biedt zelfs bescherming aan schuren, bedrijfsruimtes en openbare gebouwen, met een verwijzing naar dit begrip; zo kan het feit dat de politie een hoofdkantoor binnentreedt om stukken in beslag te nemen onder omstandigheden worden gezien als een inbreuk op het woningrecht van dat bedrijf. Dit betekent dat spionage in iemands woning uiteraard zal vallen onder het recht op privacy, maar dit kan ook in andere ruimtes gelden als iemand daarvan zijn privédomein heeft gemaakt (ruimtelijke privacy).

3. De bescherming van de reputatie: artikel 8 EVRM is gebaseerd op artikel 12 van de Universele Verklaring voor de Rechten van de Mens, dat ook bescherming biedt aan de reputatie, de eer en goede naam, naast de bescherming van privé- en gezinsleven, de woning en communicatie. De bescherming van reputatie werd door de opstellers van het EVRM expliciet uitgesloten van de werkingssfeer van artikel 8 EVRM[170] en is verplaatst naar artikel 10, tweede lid, EVRM. Een van de redenen was dat het recht op reputatie met name ook in horizontale verhoudingen een rol speelt, terwijl het EVRM was bedoeld voor verticale verhoudingen (dat wil zeggen tussen burger en overheid). Lid 1 van artikel 10 EVRM bevat het recht op vrijheid van meningsuiting en lid 2, zoals lid 2 van artikel 8

[170] B. van der Sloot, *Privacy as virtue*, Cambridge: Intersentia 2017.

EVRM, voorziet in de voorwaarden voor beperking van dit recht. Bijgevolg was de bescherming van de reputatie niet bedoeld als een subjectief recht van burgers, maar als een grond op basis waarvan regeringen de vrijheid van meningsuiting mogen (en niet moeten) beperken. Hoewel het EHRM deze principiële keuze lang heeft gerespecteerd, is hier sinds 2009 verandering in gekomen, toen het expliciet heeft bepaald dat de bescherming van de reputatie, eer en goede naam wel een subjectief recht is onder het EVRM, namelijk als onderdeel van het recht op privacy.[171] De bescherming van iemands reputatie, eer of goede naam kan onder meer worden ondermijnd als spionageproducten in enge zin of hobbydrones worden ingezet om geheimen of intieme details over iemand te verzamelen en vervolgens openbaar te maken.

4. Lichamelijke integriteit: Ook het recht op lichamelijke integriteit, dat niet expliciet wordt genoemd in artikel 8 EVRM, maar in artikel 2 (het recht op leven) en artikel 3 (het verbod op foltering) is beschermd, wordt met name behandeld met een verwijzing naar het recht op privacy. Artikelen 2 en 3 hebben, net zoals artikel 12 EVRM (het recht om te huwen en een gezin te stichten), een beperkte materiële reikwijdte gekregen, terwijl Artikel 8 EVRM juist een zeer ruime reikwijdte is toegekend. Bijgevolg wordt ten aanzien van vraagstukken rond medische procedures, verplichte vaccinatie, abortus, euthanasie en andere medisch-ethische vraagstukken met name verwezen naar het recht op privacy.[172] Uiteraard worden ook basale inbreuken op de lichamelijke en psychologische integriteit van personen (lichamelijke privacy) als een inperking van het recht op privacy gezien. Hiervan kan sprake zijn als bijvoorbeeld naaktbeelden worden opgenomen door middel van drones of spionageproducten.

5. Het recht op een schone en gezonde leefomgeving: alhoewel het Europese Hof voor de Rechten van de Mens nog niet een recht op leven in een schone en gezonde leefomgeving als zodanig aanvaardt, is het wel degelijk bereid om daar aan relaterende zaken te behandelen met een verwijzing naar artikel 8 EVRM. Voorbeelden zijn onder meer kwesties die draaien om geluidshinder, luchtvervuiling, geurvervuiling en andere vormen van milieuschade, zolang de vervuiling de 'kwaliteit van leven' van de klager maar heeft aantast (waarbij het EHRM toegeeft dat dat een zeer vaag en subjectief

---

[171] Zie over dit onderwerp: EHRM 24 augustus 1999, ECLI:CE:ECHR:1999:0824DEC003113596 (*Saltuk/Turkije*); EHRM 5 december 2000, ECLI:CE:ECHR:2000:1205DEC004201598 (*Marlow/VK*); EHRM 24 juni 2004, ECLI:CE:ECHR:2004:0624JUD005932000 (*von Hannover/Duitsland I*); EHRM 10 oktober 2006, ECLI:CE:ECHR:2006:1010JUD000750802 (*L. L./Frankrijk*) ; EHRM 15 november 2007, ECLI:CE:ECHR:2007:1115JUD001255603 (*Pfeifer/Oostenrijk*); EHRM 4 december 2012, ECLI:CE:ECHR:2012:1204JUD000649007 (*Rothe/Oostenrijk*); EHRM 9 april 2009, ECLI:CE:ECHR:2009:0409JUD002807006 (*A./Norwegen*).

[172] EHRM 16 mei 2005, ECLI:CE:ECHR:2005:0616JUD006160300 (*Storck/Duitsland*); EHRM 22 juli 2003, ECLI:CE:ECHR:2003:0722JUD002420994 (*Y.F./Turkije*); EHRM 27 augustus 1992, ECLI:CE:ECHR:1992:0827JUD001285087 (*Tomasi/Frankrijk*); EHRM 29 april 2002, ECLI:CE:ECHR:2002:0429JUD000234602 (*Pretty/VK*); EHRM 4 januari 2005, ECLI:CE:ECHR:2005:0104DEC001446203 (*Pentiacova & 48 anderen/Moldavië*).

begrip is).[173] Zoals blijkt uit de voor dit onderzoek gehouden case studies is een van de problemen die mensen aandragen de geluidsoverlast die wordt veroorzaakt door drones. Of deze overlast dusdanig is dat die tot een klacht kan leiden onder het EVRM is niet duidelijk.[174]

6. Het recht op gegevensbescherming: Alhoewel het EVRM geen verwijzing naar een recht op gegevensbescherming (dat komt grotendeels overeen met informationele privacy) bevat, biedt het EHRM aan vrijwel alle aspecten van dit recht bescherming met een verwijzing naar artikel 8 EVRM.[175] Dit recht zal in de volgende paragrafen worden behandeld aan de hand van de Algemene Verordening Gegevensbescherming.

Bij al deze rechten moet worden bedacht dat personen onder het Europees Verdrag voor de Rechten van de Mens alleen mogen klagen over het gedrag van lidstaten, zoals Nederland. Wel heeft het Europees Hof voor de Rechten van de Mens steeds meer nadruk gelegd op het feit dat staten ook zorg moeten dragen voor een goede privacybescherming in horizontale verhoudingen. Dat betekent onder meer dat een land moet zorgen dat mensen geen onevenredige hinder ondervinden van vliegvelden of industrieën, dat het adequate wetgeving moet neerleggen waardoor burgers hun rechten ook in horizontale verhoudingen kunnen claimen en dat het actief moet streven naar een leefomgeving waarin privacyschendingen tot een minimum worden beperkt. Vooralsnog zijn er geen zaken gewezen door het EHRM waarin dit implicaties heeft gehad voor de regulering van spionageproducten in enge zin en hobbydrones.

5.1.2 Toepasselijkheid AVG

Vanuit gegevensbeschermingsperspectief is het van belang om onderscheid te maken tussen hobbydrones met sensoren en drones zonder geluids-, beeld- of andere sensoren. Al is dit soort in de minderheid, er bestaan drones die slechts zijn geëquipeerd met GPS om de locatie van de drone door te kunnen geven aan het besturingsapparaat.[176] Dit soort drones verwerken geen persoonsgegevens anders dan wellicht gegevens over de gebruiker zelf en zullen daarmee in principe niet onder het gegevensbeschermingsrecht vallen. Voor spionageproducten in enge zin

---

[173] EHRM 16 november 2004, ECLI:CE:ECHR:2004:1116JUD000414302 (*Moreno Gomez/Spanje*); EHRM 14 november 2000, ECLI:CE:ECHR:2000:1114DEC003673597 (*Villa/Italië*); EHRM 22 mei 2003, ECLI:CE:ECHR:2003:0522JUD004166698 (*Kyrtatos/Griekenland*); EHRM 10 februari 2011, ECLI:CE:ECHR:2011:0210JUD003049903 (*Dubertska e.a./ Oekraïne*).
[174] Artikel 35 lid 3 sub b [Europees] Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden.
[175] EHRM 6 september, ECLI:CE:ECHR:1978:0906JUD000502971 (*Klass e.a./Duitsland*); EHRM 26 maart 1987, ECLI:CE:ECHR:1987:0326JUD000924881 (*Leander/Zweden*); EHRM 16 februari 2000, ECLI:CE:ECHR:2000:0216JUD002779895 (*Amann/Zwitserland*); EHRM 25 september 2001, ECLI:CE:ECHR:2001:0925JUD004478798 (*P.G. & J.H./VK*); EHRM 17 juli 2003, ECLI:CE:ECHR:2003:0717JUD006373700 (*Perry/VK*); EHRM 5 oktober 2010, ECLI:CE:ECHR:2010:1005DEC000042007 (*Köpke/Duitsland*); EHRM 2 september 2010, ECLI:CE:ECHR:2010:0902JUD003562305 (*Uzun/Duitsland*).
[176] *Opinion of the European Data Protection Supervisor, on the Communication from the Commission to the European Parliament and the Council on: A new era for aviation - Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner*, p. 4.

anders dan drones geldt dat zij vanzelfsprekend zullen zijn uitgerust met sensoren die geluiden, beelden of andere informatie kunnen registreren.

Van de hobbydrones en andere spionageproducten in enge zin die met sensoren zijn geëquipeerd is een minderheid met zulke rudimentaire sensoren uitgerust dat deze ook niet onder het gegevensbeschermingsrecht zullen vallen. Er bestaat bijvoorbeeld apparatuur waarbij de beelden die met de camera's worden opgevangen zo weinig pixels bevatten dat die een persoon niet in staat stellen personen en hun omgeving die op de beelden staan te identificeren noch daar relevante informatie uit af te leiden.[177] Andere drones of spionageproducten in enge zin vangen informatie op die niet direct naar personen zijn te herleiden: denk bijvoorbeeld aan infrarood camera's die worden gebruikt om te lokaliseren of iemand zich begeeft op verboden terrein, maar niet wie.

Van de hobbydrones en spionageproducten in enge zin geëquipeerd met sensoren die beeld, geluid of andere informatie opvangen die de gebruiker of anderen in staat stelt personen te identificeren is het vervolgens van belang niet alleen te bekijken of de sensoren ook aan staan en worden benut als de gebruiker het product in kwestie gebruikt, maar ook voor welk doeleinde de drone wordt benut. Het gegevensbeschermingsrecht kent immers een uitzondering voor het verwerken van persoonsgegevens voor persoonlijke en huishoudelijke doeleinden. Een overweging uit de AVG stelt: 'Tot persoonlijke of huishoudelijke activiteiten kunnen behoren het voeren van correspondentie of het houden van adresbestanden, het sociaal netwerken en online-activiteiten in de context van dergelijke activiteiten. Deze verordening geldt wel voor verwerkingsverantwoordelijken of verwerkers die de middelen verschaffen voor de verwerking van persoonsgegevens voor dergelijke persoonlijke of huishoudelijke activiteiten.'[178]

Derhalve geldt dat voor zover hobbydrones en spionageproducten in enge zin worden gebruikt op een wijze waarbij persoonsgegevens over derden worden verzameld voor persoonlijke of huishoudelijke doeleinden, daarbij valt te denken aan het filmen van een eigen familiefeest in de eigen tuin waarbij alle gasten van de filmactiviteit op de hoogte zijn gesteld, de Algemene Verordening Gegevensbescherming, de Nederlandse Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) en aanpalende wetgeving niet van toepassing zijn. Toch zijn er in de jurisprudentie de nodige beperkingen op deze uitzonderingsgrond neergelegd. Daarbij zijn met name twee zaken van het Europees Hof van Justitie van belang.

De ene restrictie volgt uit de zaak Bodil Lindqvist uit 2003, waar een dame een soort persoonlijke hobbypagina bijhield op het internet en daar ook informatie en wetenswaardigheden over

---

[177] Agencia Espanola Proteccion Datos, Drones and Data Protection', Aepd.es 9 april 2020.
[178] Overweging 18 van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (*PbEU* 2016, L 119/1) (Algemene verordening gegevensbescherming).

kennissen en collega's deelde, zoals onder meer dat een van hen en been had gebroken. De vraag was of een dergelijke handeling onder de huishoudelijke exceptie viel, nu het doeleinde waarvoor de gegevens werden verwerkt primair persoonlijk was, nu de internetpagina vooral voor de dame zelf en een kleine kring bekenden was bedoeld. Het Hof van Justitie ging daar echter niet in mee en stelde dat:

> 'Die uitzondering moet derhalve aldus worden uitgelegd, dat zij uitsluitend betrekking heeft op activiteiten die tot het persoonlijke of gezinsleven van particulieren behoren, hetgeen klaarblijkelijk niet het geval is met de verwerking van persoonsgegevens die bestaat in hun openbaarmaking op internet waardoor die gegevens voor een onbepaald aantal personen toegankelijk worden gemaakt.'[179]

Het openbaar maken van gegevens aan een onbepaalde groep mensen is in ieder geval geen verwerking voor puur persoonlijke of huishoudelijke doeleinden, al was het maar omdat de verdere verwerking niet kan worden begrensd voor wat betreft die doeleinden.

Ook als persoonlijke informatie wordt gedeeld met mensen buiten een kleine kring van vrienden en familieleden zal de verwerking niet snel onder de huishoudelijke exceptie vallen. Zo gaf de voormalig Article 29 Working Party, het adviesorgaan op het gebied van gegevensbescherming in de Europese Unie, bijvoorbeeld ten aanzien van Social Network Sites (SNS) aan dat die sites

> 'standaard en gratis privacy-vriendelijke settings dienen te hanteren die de toegang tot informatie limiteren tot de door gebruikers geselecteerde contacten. Wanneer toegang tot profielinformatie verder gaat dan deze contacten, zoals wanneer toegang tot het profiel wordt geboden aan alle deelnemers van een SNS of wanneer de data wordt geïndexeerd door zoekmachines, dan gaat de toegang verder dan de persoonlijke of huishoudelijke sfeer. Als een gebruiker zelf informatie deelt buiten de cirkel van geselecteerde vrienden, dan zal hij als verantwoordelijke worden aangemerkt. Effectief zal dan hetzelfde juridische regime van toepassing zijn als wanneer een person een ander technologisch platform gebruikt om persoonlijke informatie te publiceren op het web.'[180]

Een tweede begrenzing volgt uit de zaak Ryneš uit 2013. De zaak draaide om een persoon die een camera had gericht op de toegang tot zijn erf, voor veiligheidsdoeleinden. Wederom was de vraag of deze toepassing onder de huishoudelijke exceptie viel, nu het doel van de werking van persoonsgegevens (in casu van mensen die toegang zochten tot het huis) primair van

---

[179] HvJ EU 6 november 2003, C-101/01, ECLI:EU:C:2003:596 (Bodil Lindqvist), r.o. 47.
[180] 'Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking, 01189/09/EN WP 163, 12 June 2009, Brussels', Ec.europa.eu 9 april 2020. Citaat vertaald door projectteam op verzoek van WODC.

persoonlijke aard was en de gegevens niet waren bedoeld om openbaar te worden gemaakt. Toch oordeelde het Hof van Justitie ook in deze zaak anders.

> 'Voor zover het gebruik van een videobewakingssysteem, zoals dat in het hoofdgeding, de openbare ruimte bestrijkt – zelfs gedeeltelijk – en hierdoor buiten de privésfeer geraakt van degene die door middel van dit systeem gegevens verwerkt, kan het niet worden beschouwd als een activiteit die met uitsluitend „persoonlijke of huishoudelijke doeleinden" wordt verricht'.[181]

Dat betekent dus in ieder geval dat in zoverre slimme deurbellen deels zijn gericht op de openbare ruimte, de gegevensverzameling die daarmee geschiedt niet onder de huishoudelijke exceptie zal vallen. Datzelfde geldt waarschijnlijk, mutatis mutandis, voor gevallen waarin niet de openbare ruimte, maar de privéruimtes van anderen worden gefilmd. Een strikte interpretatie van dit arrest zou ook met zich mee kunnen brengen dat in zoverre drones opnames maken van ruimte buiten de privéruimte van de eigenaar en daar persoonsgegevens worden verzameld, er geen beroep op de huishoudelijke exceptie kan worden gedaan, ongeacht het doeleinde (bijvoorbeeld recreatief en dus van persoonlijke aard) van de verwerking.

Alhoewel er dus situaties kunnen zijn waarin er via hobbydrones en spionageproducten in enge zin persoonsgegevens worden verwerkt, maar deze verwerking niet onder de reikwijdte van de Algemene Verordening Gegevensbescherming valt, zullen deze situaties relatief beperkt zijn.[182] Ook als een spionageproduct slechts binnenshuis wordt gebruikt, bijvoorbeeld om de partner in de gaten te houden en te kunnen betrappen op eventueel overspel, zal niet snel onder deze exceptie vallen. Een uitzondering kan wellicht worden gevonden in producten als babyfoons of producten die binnenshuis worden gebruikt om communicatie te vergemakkelijken.

Tot slot is nog relevant in dit verband of de verwerking geschiedt in het kader van de vrijheid van meningsuiting en/of journalistieke werkzaamheden. Onder het recht op de vrijheid van meningsuiting valt immers ook het recht op het vergaren van informatie. Hobbydrones en tot op zekere hoogte spionageproducten in eneg zin kunnen worden gebruikt voor het verzamelen van informatie door burgers of van feiten en achtergronden door journalisten. De Algemene Verordening Gegevensbescherming geeft aan dat landen nadere regels kunnen stellen ten aanzien van de verwerking van persoonsgegevens voor dergelijke doeleinden. Opvallend is dat Nederland er in de UAVG voor heeft gekozen om slechts op voor journalistieke werkzaamheden uitzonderingen op het gegevensbeschermingsrecht neer te leggen en niet voor activiteiten in het

---

[181] HvJ EU 11 december 2014, C-212/13, ECLI:EU:C:2014:2428 (František Ryneš v Úřad pro ochranu osobních údajů), r.o. 33.

[182] De voormalige Artikel 29 Werkgroep heeft zich zelfs laten ontvallen dat de huishoudelijke exceptie wellicht verder zou moeten worden beperkt. 'The regulation should differ from the current Directive in that all processing of personal data performed – even for exclusively personal or household purposes – should to some extent come within the scope of the Regulation.' *Proposals for Amendments regarding exemption for personal or household activities*, Annex 2.

kader van vrijheid van meningsuiting in het algemeen. Onderstaande tabel zet de teksten uit de AVG en de UAVG naast elkaar om het verschil te illustreren.

AVG	UAVG
Artikel 85 Verwerking en vrijheid van meningsuiting en van informatie	Artikel 43. Uitzonderingen inzake journalistieke doeleinden of academische, artistieke of literaire uitdrukkingsvormen
1. De lidstaten brengen het recht op bescherming van persoonsgegevens overeenkomstig deze verordening wettelijk in overeenstemming met het recht op vrijheid van meningsuiting en van informatie, daaronder begrepen de verwerking voor journalistieke doeleinden en ten behoeve van academische, artistieke of literaire uitdrukkingsvormen. 2. Voor verwerking voor journalistieke doeleinden of ten behoeve van academische, artistieke of literaire uitdrukkingsvormen stellen de lidstaten uitzonderingen of afwijkingen vast van hoofdstuk II (beginselen), hoofdstuk III (rechten van de betrokkene), hoofdstuk IV (de verwerkingsverantwoordelijke en de verwerker), hoofdstuk V (doorgifte van persoonsgegevens naar derde landen of internationale organisaties), hoofdstuk VI (onafhankelijke toezichthoudende autoriteiten), hoofdstuk VII (samenwerking en coherentie) en hoofdstuk IX (specifieke gegevensverwerkingssituaties) indien deze noodzakelijk zijn om het recht op bescherming van persoonsgegevens in	Deze wet, met uitzondering van de artikelen 1 tot en met 4 en 5, eerste en tweede lid, is niet van toepassing op de verwerking van persoonsgegevens voor uitsluitend journalistieke doeleinden en ten behoeve van uitsluitend academische, artistieke of literaire uitdrukkingsvormen. 2De navolgende hoofdstukken en artikelen van de verordening zijn niet van toepassing op de verwerking van persoonsgegevens voor uitsluitend journalistieke doeleinden en ten behoeve van academische, artistieke of literaire uitdrukkingsvormen: a.artikel 7, derde lid, en artikel 11, tweede lid: b.hoofdstuk III; c.hoofdstuk IV, met uitzondering van de artikelen 24, 25, 28, 29 en 32; d.hoofdstuk V; e.hoofdstuk VI; en f.hoofdstuk VII. 3De artikelen 9 en 10 van de verordening zijn niet van toepassing voor zover de verwerking van de in die artikelen bedoelde gegevens noodzakelijk is voor het journalistieke doel of

overeenstemming te brengen met de vrijheid van meningsuiting en van informatie. 3. Elke lidstaat deelt de Commissie de overeenkomstig lid 2 vastgestelde wetgevingsbepalingen mee, alsook onverwijld alle latere wijzigingen daarvan.	de academische, artistieke of literaire uitdrukkingsvorm.

In hoeverre er dus sprake kan zijn van een uitzondering voor het verwerken van persoonsgegevens door burgers voor niet journalistieke werkzaamheden die desalniettemin zijn te kwalificeren als de verwerking van persoonsgegevens in het kader van de vrijheid van meningsuiting blijft onduidelijk. Wel is duidelijk dat burgers zich in een conflict waarbij de ene burger ongewenst persoonsgegevens verzamelt van de andere burger met gebruikmaking van een drone of spionageproduct in enge zin zich zullen kunnen beroepen op het grondwettelijke recht op gegevensbescherming enerzijds en het grondwettelijke recht op vrijheid van meningsuiting anderzijds, daarbij ofwel verwijzend naar de Nederlandse Grondwet, het EU Verdrag voor de Fundamentele Rechten ofwel het Europees Verdrag voor de Rechten van de Mens. Via die lijn zou dan eventueel alsnog een beperking ten aanzien van de gegevensbeschermingsregels kunnen worden afgedwongen.

Voor journalisten geldt dat zij, voorover zij persoonsgegevens verwerken voor journalistieke doeleinden, ontheven kunnen zijn van een groot aantal van de verplichtingen die de AVG aan hen oplegt. Toch benadrukt de Leidraad van de Raad voor de Journalistiek expliciet dat journalisten te alle tijden zijn gehouden aan het respect voor privacy:

> ‘In een publicatie mag de privacy van personen niet verder worden aangetast dan in het kader van de berichtgeving redelijkerwijs noodzakelijk is. Een inbreuk op de privacy is onzorgvuldig wanneer deze niet in redelijke verhouding staat tot het maatschappelijk belang van de publicatie. Journalisten publiceren geen foto’s en zenden geen beelden uit die zijn gemaakt van personen in niet algemeen toegankelijke ruimten zonder hun toestemming, en gebruiken evenmin brieven en persoonlijke aantekeningen zonder toestemming van betrokkenen.∗ Journalisten mogen personen niet langdurig lastig vallen, hinderlijk volgen of schaduwen.* Journalisten dienen te voorkomen dat informatie of beelden worden gepubliceerd

waardoor verdachten en veroordeelden door het grote publiek eenvoudig kunnen worden geïdentificeerd en getraceerd.'[183]

Ook journalisten zijn dus, voor zover dat hun werkzaamheden niet ondermijnt, gehouden aan privacy- en gegevensbeschermingsprincipes.

5.1.3 Legitieme verwerkingsgrondslag

Een van de belangrijkste obstakels die volgt uit het van toepassing zijn van de AVG en het nationale gegevensbeschermingsrecht is dat er een legitieme verwerkingsgrondslag zal moeten worden gevonden door de burger die de drone of het andersoortige spionageproduct gebruikt. Juridisch is deze burger te kwalificeren als verantwoordelijke. De verantwoordelijke is gehouden de diverse regels uit het gegevensbeschermingsrecht in acht te nemen. Daarbij zijn twee situaties te onderscheiden: enerzijds het geval waarin er gewone persoonsgegevens worden verwerkt en anderzijds het geval waarin er gevoelige oftewel bijzondere persoonsgegevens worden verwerkt. Op de verwerking van beide type persoonsgegevens is een andersoortig beschermingsregime van toepassing.

Onder de eerste categorie valt vrijwel alle informatie die direct of indirect naar een persoon te herleiden is. Beelden van personen, maar ook bijvoorbeeld opnamen van gesprekken, zijn te kwalificeren als persoonsgegevens omdat ze refereren aan personen; het is niet nodig dat de persoon die de drone of ander spionageproduct gebruikt ook de naam of identiteit van de persoon waarvan opnames worden gemaakt kent. Ook is het niet nodig dat het doel is om personen te identificeren. Als er beelden, geluidsopnamen of andersoortige fragmenten worden geregistreerd die aan personen relateren, zoals een landschapsfoto, waar in een vergezicht één wandelaar duidelijk te onderscheiden valt, zal zijn te kwalificeren als het verwerken van persoonsgegevens.[184]

Onder de tweede categorie valt de verwerking 'persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid zijn verboden.'[185] Belangrijk is dat de AVG hierbij een belangrijke begrenzing heeft neergelegd: 'De verwerking van foto's mag niet systematisch worden beschouwd als verwerking van bijzondere categorieën van persoonsgegevens, aangezien foto's alleen onder de definitie van biometrische

---

[183] "∗ Het afwijken van deze norm kan worden gerechtvaardigd wanneer er evident sprake is van een misstand én wanneer dit noodzakelijk is om de desbetreffende kwestie aan de orde te stellen." *Leidraad van de Raad voor de Journalistiek December 2019*.
[184] 'Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, WP 136, 20 june 2007, Brussels', Ec.europa.eu 9 april 2020.
[185] Artikel 9 lid 1 Algemene verordening gegevensbescherming.

gegevens vallen wanneer zij worden verwerkt met behulp van bepaalde technische middelen die de unieke identificatie of authenticatie van een natuurlijke persoon mogelijk maken.'[186] Toch heeft de Hoge Raad in een uitspraak uit 2010 bepaald dat foto's een verwerking van rasgegevens met zich kunnen meebrengen.[187] In deze strengere lijn zou iedere foto waaruit rederlijkwijs iemands ras of etniciteit zou zijn af te leiden zijn aan te merken als een verwerking van bijzondere persoonsgegevens.[188] Deze strenge lijn lijkt ook te worden gevolgd door de eerder genoemde Artikel 29 Werkgroep, het voormalige samenwerkingsverband van de nationale handhavende organisaties van de EU landen.[189]

Ook de Autoriteit Persoonsgegevens geeft aan dat strikt genomen bijna alle beelden moeten worden gezien als een verwerking van bijzondere persoonsgegevens, maar gaat hier om opportuniteitsredenen toch anders mee om. 'Gelet hierop beschouwt de Autoriteit Persoonsgegevens camerabeelden van een persoon thans, ook om opportuniteitsredenen, niet als bijzondere persoonsgegevens als:

- het doeleinde van de verwerking niet gericht is op het verwerken van bijzondere persoonsgegevens dan wel op het onderscheid maken op grond van een bijzonder persoonsgegeven,
- het voor de verantwoordelijke redelijkerwijs niet voorzienbaar is dat de verwerking zal leiden tot het maken van onderscheid op grond van een bijzonder persoonsgegeven, en
- de verwerking van die bijzondere persoonsgegevens onvermijdelijk is bij die verwerking. Indien de verwerking van camerabeelden echter identificatie tot doel heeft, worden deze beelden wel als een rasgegeven aangemerkt.'[190]

In ieder geval is duidelijk dat foto's ook andere bijzondere gegevens kunnen registreren, zoals bijvoorbeeld gegevens over iemands medische toestand. Iemand die een mitella draagt, in een rolstoel zit of anderszins een uiterlijke vertoning heeft van een medische conditie en waarvan een foto wordt gemaakt zal als verwerking van bijzondere persoonsgegevens zijn aan te merken. Of daar ook al onder valt het dragen van een bril is onduidelijk; wel is duidelijk dat het Hof van Justitie de lat wat dit betreft laag legt. Zo had in de eerder genoemde zaak uit 2003 een mevrouw op haar internetpagina vermeld dat een collega haar voet had bezeerd en was het de vraag of dit afdoende was om aangemerkt te worden als een verwerking van bijzondere

---

[186] Overweging 51 Algemene verordening gegevensbescherming.
[187] HR 23 maart 2010, ECLI:NL:HR:2010:BK6331.
[188] G. J. Zwenne & L. Mommers, 'Zijn foto's en beeldopnamen 'rasgegevens' in de zin van art. 126nd Sv en art. 18 Wbp?', *Privacy en Informatie* (11) 2010.
[189] 'Article 29 Data Protection Working Party, Advice paper on special categories of data ("sensitive data"), 4 April 2011, Brussels', Ec.europa.eu 9 april 2020.
[190] *Cameratoezicht*: *Beleidsregels voor de toepassing van bepalingen uit de Wet bescherming persoonsgegevens en de Wet politiegegevens*, Autoriteit Persoonsgegevens 28 januari 2016.

persoonsgegevens en oordeelde het Hof van Justitie: ‘de vermelding van het feit dat iemand zijn voet heeft bezeerd en met gedeeltelijk ziekteverlof is, [is] een persoonsgegeven betreffende de gezondheid’.[191]

Bij de verwerking van gewone (niet-bijzondere) persoonsgegevens geldt een ‘ja, mits’ regime, bij de verwerking van bijzondere persoonsgegevens een ‘nee, tenzij’ regime. In principe is het uitgangspunt dat partijen gewone persoonsgegevens mogen verwerken, mits zij daar een redelijk belang bij hebben, terwijl zij geen bijzondere persoonsgegevens mogen verwerken, tenzij zij daar een speciaal en bijzonder belang bij hebben. Er zijn twee gronden die eventueel kunnen worden ingeroepen bij het verwerken van persoonsgegevens door middel van drones en andere spionageproducten in de context van burger-burger relaties.[192]

Ten eerste kan het verwerken van persoonsgegevens legitiem zijn als alle personen waarover gegevens worden verwerkt hiervoor hun toestemming geven.[193] Toestemming zal uiteraard niet worden gegeven bij heimelijk spionage, maar kan wel worden gegeven voor de openlijke inzet van spionageproducten of producten die voor spionage kunnen worden ingezet, zoals bij filmbeelden gemaakt door drones.[194] Bij toestemming voor het verwerken van bijzondere persoonsgegevens is daarbij vereist dat de toestemming expliciet moet zijn gegeven, waarmee wordt uitgedrukt dat de toestemming nog uitdrukkelijker en actiever moet zijn gegeven dan normaal al het geval is.[195] De vereisten voor legitieme toestemming, zowel voor het verwerken van gewone persoonsgegevens als voor het verwerken van bijzondere persoonsgegevens, zijn:[196]

- Vrij: Ten eerste moet de toestemming ‘vrij’ zijn gegeven door een datasubject (in het Nederlands officieel ‘de betrokkene’ genoemd). Toestemming mag niet onder dreiging tot stand komen of een voorwaarde worden gemaakt voor diensten of gebruiken waar de burger recht op heeft. Een buurt kan bijvoorbeeld niet een buurtdrone voor veiligheidsdoeleinden inzetten en van alle inwonenden eisen dat zij akkoord gaan en anders moeten verkassen en van alle bezoekers instemming eisen en hen anders de toegang tot de wijk ontzeggen.

---

[191] HvJ EU 6 november 2003, C-101/01, ECLI:EU:C:2003:596 (Bodil Lindqvist), r.o. 51.
[192] Het zal in burger-burger relaties immers niet gaan om contractuele relaties of verwerking in het publiek belang of verrichting van een taak van algemeen belang waarbij deze taak aan de burger is opgedragen bij wet. Het gebruik van spionageproducten in het vitale belang van het datasubject zelf zal slechts uitzonderlijke gevallen mogelijk zijn. Denk hierbij aan een dementerende oudere die door middel van spionagetechniek wordt gelokaliseerd als hij langer dan 3 uur van huis is.
[193] Artikel 4 lid 1 Algemene verordening gegevensbescherming geeft de definitie van toestemming.
[194] Article 29 Data Protection Working Party, Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones, 01673/15/EN WP 231, 16 June 2015, Brussels, Ec.europa.eu 9 april 2020 (P.12-13).
[195] Zie voor het verschil artikel 6 lid 1 sub a en artikel 9 lid 2 sub a Algemene verordening gegevensbescherming. ‘Article 29 Working Party Guidelines on consent under Regulation 2016/679, 17/EN, WP259 rev.01, Adopted on 28 November 2017, As last Revised and Adopted on 10 April 2018’, Ec.europa.eu 9 april 2020.
[196] Zie artikel 7 Algemene verordening gegevensbescherming.

- Specifiek: Daarnaast moet de toestemming ‘specifiek’ zijn. Bij het geven van toestemming moet het gaan om een specifiek en afgebakend doel waarvoor een specifiek en afgebakende hoeveelheid persoonsgegevens worden verwerkt. Een voorbeeld kan bijvoorbeeld zijn ‘Ik ga akkoord met het maken van een luchtfoto door middel van een drone tijdens het familiefeest op het moment dat de taart wordt aangesneden.’

- Geïnformeerd: De toestemming moet ‘geïnformeerd’ zijn. Het datasubject moet geïnformeerd worden over welke gegevens er worden verwerkt, voor welke doeleinden en hoe ze worden gebruikt.

- Ondubbelzinnig: De toestemming moet ‘ondubbelzinnig’ zijn. Dat betekent dat de toestemming voor het verwerken van persoonsgegevens duidelijk onderscheiden moet zijn van eventuele andere zaken waarvoor toestemming wordt gevraagd en dat de toestemming actief wordt gegeven. ‘Stilzwijgen, het gebruik van reeds aangekruiste vakjes of inactiviteit mag derhalve niet als toestemming gelden.’[197] Het is does niet zo dat als mensen tijdens een familiefeest zien dat er een film wordt gemaakt door middel van een drone en zij daar niet actief bezwaar tegen maken, dit als impliciete toestemming mag worden gezien.

- Bewijsbaar: De toestemming moet bewijsbaar zijn. Het is aan de verantwoordelijke voor de gegevensverwerking om aan te tonen dat het datasubject inderdaad zijn toestemming heeft gegeven en dat dit legitiem is gebeurd. Als er dus een juridisch conflict is, dan is er een omkering van de bewijslast. Niet het datasubject moet aantonen dat hij geen (legitieme) toestemming heeft gegeven, maar het is aan de data-verwerkende organisatie om aan te tonen dat dit wel is gebeurd. Dit kan extra documentatie vergen.

Het is in dergelijke gevallen nodig dat alle personen over wie gegevens worden verwerkt toestemming geven. Er mogen dus niet op de achtergrond van gemaakte foto of film herkenbare personen staan die geen toestemming hebben gegeven. De eerder genoemde Artikel 29 Werkgroep geeft een voorbeeld van een drone die wordt gebruikt in de context van sportbeoefening, maar benadrukt daarbij dat er geen omstanders of toeschouwers dienen te worden gefilmd (zeker nu met name bij openbare trainingswedstrijden er doorgaans geen goed zicht is op wie de wedstrijd gade slaat). ‘Toestemming zou een legitieme verwerkingsgrondslag kunnen vormen voor het verwerken van persoonsgegevens middels drone-camera’s,

[197] Overweging 32 Algemene verordening gegevensbescherming.

bijvoorbeeld als die wordt gebruik voor het filmen van een trainingssessie van een sportteam (zonder toeschouwers).'[198]

Ten tweede kan het gaan om het geval waarin 'de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.'[199] Deze verwerkingsgrond kan evenwel alleen dienen als legitimering van het verwerken van gewone persoonsgegevens en niet voor het verwerken van bijzondere persoonsgegevens. Als er geen bijzondere persoonsgegevens worden verwerkt, dan kan deze grondslag worden ingeroepen door, onder meer, journalisten, voor zover die aan de AVG zijn gehouden, en door mensen die hun eigen huis of erf willen beveiligen. In de eerder besproken zaak, waarin het Hof van Justitie bepaalde dat filmen van ruimtes, gedeeltelijke zijnde de openbare ruimte, niet onder de huishoudelijke exceptie valt, merkte het Hof evenwel terzijde op dat het in dergelijke gevallen mogelijk is 'rekening te houden met de gerechtvaardigde belangen van de verantwoordelijke voor de verwerking, die, zoals in het hoofdgeding, met name de bescherming van de eigendom, de gezondheid en het leven van de verantwoordelijke en zijn familie betreffen.'[200]

Voor zover er dus een beperkt aantal persoonsgegevens, niet zijnde bijzondere persoonsgegevens, worden verwerkt voor legitieme en zwaarwichtige belangen van de verantwoordelijke kan dit legitiem zijn onder de AVG. Het is echter de vraag of dat ook geldt voor het recreatief gebruik van drones en spionageproducten in enge zin. De Artikel 29 Werkgroep verwijst bij een bespreking van deze verwerkingsgrond in relatie tot het gebruik van drones dan ook met name naar zwaarwichtige doeleinden.[201]

5.1.4 Beginselen inzake verwerking van persoonsgegevens

De Algemene Verordening Gegevensbescherming geeft een aantal beginselen inzake de verwerking van persoonsgegevens, waarvan er een aantal hieronder kort zullen worden toegelicht.

Ten eerste legt de AVG de nadruk op doel en doelbinding.[202] Persoonsgegevens dienen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden te worden verzameld en

---

[198] 'Article 29 Data Protection Working Party, Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones, 01673/15/EN WP 231, 16 June 2015, Brussels', Ec.europa.eu 9 april 2020. Vertaling door de auteurs van dit rapport.
[199] Artikel 6 lid 1 sub f Algemene verordening gegevensbescherming.
[200] HvJ EU 11 december 2014, C-212/13, ECLI:EU:C:2014:2428 (František Ryneš v Úřad pro ochranu osobních údajů).
[201] Article 29 Data Protection Working Party, Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones, 01673/15/EN WP 231, 16 June 2015, Brussels', Ec.europa.eu 9 april 2020.
[202] Artikel 5 lid 1 sub b Algemene verordening gegevensbescherming.

mogen vervolgens niet verder worden verwerkt op een met die doeleinden onverenigbare wijze. ‘Meer bepaald dienen de specifieke doeleinden waarvoor de persoonsgegevens worden verwerkt, expliciet en gerechtvaardigd te zijn en te zijn vastgesteld wanneer de persoonsgegevens worden verzameld.’[203] Dat betekent dat burgers die persoonsgegevens verzamelen middels drones en andere spionageproducten al van te voren een specifiek en helder omschreven doel voor deze verwerking moeten vastleggen. Bij voorkeur geschiedt deze vastlegging schriftelijk. Het doel moet specifiek zijn in de zin dat er duidelijk moet worden omschreven welk specifiek doel, bijvoorbeeld het maken van een filmpje van een trouwerij, er wordt nagestreefd en waarom daarvoor persoonsgegevens moeten worden verwerkt.

Ten tweede stelt de Algemene Verordening Gegevensbescherming dat er slechts zoveel gegevens mogen worden verwerkt als noodzakelijk is voor dat specifieke doel. Uit het zogenoemde dataminimalisatieprincipe[204] volgt dat persoonsgegevens, als ze worden verwerkt, toereikend dienen te zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden en uit het opslagbeperkingsprincipe volgt deze persoonsgegevens niet langer mogen worden bewaard in een vorm die het mogelijk maakt personen te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is.[205] Ten aanzien van dat eerste principe geeft de AVG ter nadere duiding aan dat persoonsgegevens alleen mogen ‘worden verwerkt indien het doel van de verwerking niet redelijkerwijs op een andere wijze kan worden verwezenlijkt.’[206] Wat redelijk is en wat niet kan niet exact worden gesteld, maar zeker ten aanzien van pleziergebruik van drones en andere spionageproducten is het de vraag of dergelijke bezigheden niet net zo goed zonder het verzamelen van persoonsgegevens zou kunnen.

Dan is tot slot nog relevant het principe dat gegevensverwerking transparant moet geschieden. Dit principe is verder uitgewerkt in een tweetal artikelen in de Algemene Verordening Gegevensbescherming.[207] Allereerst het geval waarin degene die de hobbydrone bestuurt of spionageproduct in enge zin inzet gegevens direct verkrijgt van of door middel van observatie van personen waarover persoonsgegevens worden verzameld en anderzijds het geval waarin die gegevens op een andere weg worden verkregen, bijvoorbeeld via derden. Bij het verzamelen van persoonsgegevens door middel van hobbydrones worden de gegevens verkregen door middel van observatie van personen zelf. De European Data Protection Board, de opvolger van de eerder genoemde Article 29 Working Party, stelt in dit verband dat onder deze categorie moet

[203] Overweging 39 Algemene verordening gegevensbescherming.
[204] Artikel 5 lid 1 sub c Algemene verordening gegevensbescherming.
[205] Artikel 5 lid 1 sub e Algemene verordening gegevensbescherming.
[206] Overweging 39 Algemene verordening gegevensbescherming.
[207] Artikel 13 & 14 Algemene verordening gegevensbescherming.

worden meegenomen de situatie waarin een verantwoordelijke gegevens direct van het datasubject verkrijgt.[208]

Dat betekent dat de personen over wie gegevens worden verzameld op de hoogte moeten worden gesteld van het feit dat er gegevens over hen worden verzameld, niet later dan het moment van de verzameling zelf. De informatie die dient te worden verstrekt aan iedere persoon over wie gegevens wordt verzameld behelst onder meer de identiteit en de contactgegevens van de verantwoordelijke, de verwerkingsdoeleinden en de legitieme verwerkingsgrond, de bewaartermijn voor de gegevens en de diverse rechten van de personen over wie gegevens worden verzameld. Dit levert een groot praktisch obstakel op voor personen die hobbydrones wensen in te zetten en daarbij zich niet beroepen op de vooraf gegeven toestemming van ieder datasubject, maar op hun eigen gerechtvaardigde belangen. 'In de regel geldt dat de betrokkenen moeten worden geïnformeerd dat er cameratoezicht plaatsvindt alvorens zij daadwerkelijk worden gefilmd. Dat kan in het geval van cameratoezicht door middel van drones problematisch zijn.'[209] Voor spionageproducten in enge zin die worden ingezet om heimelijk informatie over anderen te verzamelen geldt dat eens te meer als obstakel.

In principe is het heimelijk verzamelen van persoonsgegevens middels hobbydrones en spionageproducten in enge zin dus verboden. De enige uitzondering op deze informatieplicht wordt geboden door het eerder genoemde Artikel 85 AVG, dat in Nederland is geïmplementeerd in Artikel 43 UAVG. Daarbij is het opvallend dat Nederland er in de UAVG voor heeft gekozen om slechts voor journalistieke werkzaamheden uitzonderingen op het gegevensbeschermingsrecht neer te leggen en niet voor activiteiten in het kader van vrijheid van meningsuiting in het algemeen. Dat betekent als burgers drones en spionageproducten in enge zin niet inzetten voor journalistieke doeleinden of academische, artistieke of literaire uitdrukkingsvormen, maar voor hun persoonlijke doeleinden, deze uitzondering op de informatieplicht in principe niet opgaat. Eventueel zou een opening kunnen worden geboden als er sprake is van een botsing van grondrechten van twee of meer burgers, waarbij de ene burger een beroep doet op het recht op gegevensbescherming en de andere op een ander grondrecht, waarbij die laatste claimt dat het recht van de eerste zou moeten komen te vervallen of moeten kunnen worden beperkt. Echter, hiervan zal slechts sprake zijn als een burger kan aantonen dat de heimelijke verzameling van persoonsgegevens over anderen noodzakelijk was voor de uitoefening van een van zijn grondrechten, zoals zijn recht op vrijheid van meningsuiting. Het is niet uitgesloten dat zulks in uitzonderlijke gevallen zal worden aangenomen door een rechter,

---

[208] 'European Data Protection Board, Guidelines on Transparency under Regulation 2016/679, 17/EN WP260 rev.01, 29 November 2017, Brussels', Ec.europa.eu 9 april 2020.
[209] *Cameratoezicht*: *Beleidsregels voor de toepassing van bepalingen uit de Wet bescherming persoonsgegevens en de Wet politiegegevens*, Autoriteit Persoonsgegevens 28 januari 2016.

maar het is onwaarschijnlijk dat dit solaas zal bieden voor de meest voorkomende vormen van gebruik van spionageproducten en drones.

5.1.5 Deelconclusie en discussie: mogelijke lacunes en reguleringsmogelijkheden

Op basis van bovenstaande discussie bieden we hier een samenvatting van de geïdentificeerde mogelijke lacunes (antwoord op deelvraag 4) en bespreken we verder de mogelijkheden voor hun regulering (antwoord op deelvraag 8).

Hobbydrones en spionageproducten in enge zin kunnen raken aan tal van aspecten van het recht op privacy, zoals vervat in artikel 8 van het Europees Verdrag voor de Rechten van de Mens, zoals onder meer aan de bescherming van het privéleven, de woning, de eer en goede naam, de lichamelijke integriteit en het recht op een schone en gezonde leefomgeving. Daarbij moet evenwel worden bedacht dat personen onder het Europees Verdrag voor de Rechten van de Mens alleen mogen klagen over het gedrag van lidstaten, zoals Nederland. Wel heeft het Europees Hof voor de Rechten van de Mens steeds meer nadruk gelegd op het feit dat staten ook zorg moeten dragen voor een goede privacybescherming in horizontale verhoudingen. Dat betekent onder meer dat een land moet zorgen dat mensen geen onevenredige hinder ondervinden van vliegvelden of industrieën, dat het adequate wetgeving moet neerleggen waardoor burgers hun rechten ook in horizontale verhoudingen kunnen claimen en dat het actief moet streven naar een leefomgeving waarin privacyschendingen tot een minimum worden beperkt. Vooralsnog zijn er geen zaken geweest waarin dit implicaties heeft gehad voor de regulering van spionageproducten in enge zin en hobbydrones.

De meeste hobbydrones en spionageproducten in enge zin zullen onder de reikwijdte van de Algemene Verordening Gegevensbescherming vallen. Dit lijdt slechts uitzondering als er geen persoonsgegevens worden verzameld of als deze verzameling slechts en alleen voor persoonlijke doeleinden geschiedt en de gegevens niet openbaar worden gemaakt noch worden vergaard in andere ruimtes dan de privéruimte van de verantwoordelijke. Journalisten kunnen een bijzondere positie innemen als zij drones of andere spionageproducten inzetten ten einde feiten en informatie te verzamelen in het kader van hun journalistieke werkzaamheden.

Er is discussie over de vraag in hoeverre foto’s en video’s per definitie moet worden gezien als het verwerken van bijzondere persoonsgegevens, aangezien met dergelijke beeltenis vaak de etniciteit of het ras waartoe een persoon behoord kan worden achterhaald. Zelfs als deze automatische link niet wordt gemaakt dan nog zal uit beeldmateriaal niet zelden andere bijzondere persoonsgegevens kunnen worden afgeleid, zoals medische informatie, informatie over seksuele gerichtheid of activiteiten of de religieuze overtuiging van een persoon (waardoor met name de beslissingsprivacy wordt verstoord). Ook hierbij is de vraag of alle beeltenissen waarop bijvoorbeeld iemand met een mitella, een hoofddoek of kledij waaruit een seksuele

voorkeur valt af te leiden moeten worden gezien als de verwerking van bijzondere persoonsgegevens, or dat het hiervoor is vereist dat de beeltenis is genomen met het oog op de verwerking van bijzondere persoonsgegevens.

Als er bijzondere persoonsgegevens worden verwerkt dan moet ieder datasubject daar afzonderlijk, geïnformeerd en specifiek zijn toestemming voor hebben gegeven. Dergelijke toestemming moet actief en expliciet zijn gegeven en mag niet worden afgeleid uit stilzwijgen. Ook moet deze toestemming vrijelijk worden gegeven en mag de toestemming niet afhankelijk worden gemaakt van bepaalde rechten, zoals toegang tot een wijk waarin het buurtcomité heeft besloten drones in te zetten voor veiligheidsdoeleinden. Dat betekent dat heimelijke opnames (beeld, geluid of anderszins) waarin gegevens over iemands seksuele leven of gezondheid kan worden afgeleid in principe te allen tijde verboden is.

Als er slechts gewone persoonsgegevens worden verwerkt dan kan als alternatief voor toestemming worden gekeken naar de gerechtvaardigde belangen van de verantwoordelijke, die boven de belangen van de datasubjecten uitgaan. Het moet hier dan evenwel gaan om gewichtige redenen, zeker als er ook persoonsgegevens over kinderen worden verwerkt. Het is duidelijk dat van dergelijke gewichtige redenen die de belangen van het datasubject overstijgen niet snel sprake zal zijn bij de inzet van spionageproducten in enge zin, zoals wanneer een jaloerse echtgenoot zijn partner in de gaten houdt. Het is de vraag in hoeverre deze grond kan worden ingeroepen als drones worden ingezet voor recreatieve doeleinden; vermoedelijk zal de beantwoording van deze vraag afhangen van de omstandigheden van het geval.[210]

Dan zijn er nog een aantal additionele principes die in acht worden genomen als burgers hobbydrones of spionageproducten in enge zin inzetten. Daarbij kan worden gedacht aan het van te voren neerleggen van een duidelijk omschreven en afgebakend doel. Ook mogen slechts die gegevens worden verwerkt die noodzakelijk zijn voor het bereiken van dat doel. Als het doel redelijkerwijs kan worden bewerkstelligd zonder het verzamelen van persoonsgegevens of door het verzamelen van minder persoonsgegevens, dan geniet dat de voorkeur. Tot slot heeft een ieder die persoonsgegevens direct over datasubjecten verzamelt de plicht om die datasubjecten daar niet later dan het moment van de verzameling duidelijk van op de hoogte te stellen. Ook dient de verantwoordelijke onder meer mede te delen waarom de gegevens worden verzameld, op basis van welke verwerkingsgrondslag dit geschiedt, hoe lang de gegevens zullen worden bewaard en hoe het datasubject de verantwoordelijke kan bereiken. Zeker in gevallen waarin geen voorafgaande toestemming is verkregen zal dit niet eenvoudig zijn. Dit betekent dat in principe, heimelijke spionage helemaal verboden is onder het huidige wettelijke kader. Hierop kan slechts een uitzondering worden gemaakt wanneer de opnames worden gemaakt voor

[210] In ieder geval heeft het data subject altijd het recht bezwaar te maken tegen deze verwerking. Zie artikel 21 Algemene verordening gegevensbescherming.

journalistieke doeleinden en eventueel als er sprake is van een botsing van grondrechten, waarbij bijvoorbeeld het recht op vrijheid van meningsuiting van de ene burger voorrang heeft boven het recht op gegevensbescherming van de andere burger. Hiervan zal slechts in uitzonderlijke gevallen sprake zijn.

Het blijkt dus dat er weinig tot geen juridische lacunes op deze gebieden zijn. We leveren dus weinig nieuwe bouwstenen voor oplossingsrichtingen (met betrekking tot deelvraag 8 van dit onderzoek). Eerder roept dit een andere vraag op. De regels uit de AVG zijn zo streng dat het maar de vraag is of een groot deel van het huidige gebruik van bijvoorbeeld smartphones voor het maken van foto's en filmpjes wel legitiem is, wat eens te meer geldt voor hobbydrones en zeker voor spionageproducten in enge zin. Enerzijds wijst dit op een handhavingslacune, anderzijds sluiten de geldende regels niet aan bij de huidige praktijk. Zelfs als dit wenselijk zou worden bevonden, is het de vraag of het bijvoorbeeld nog realistisch is om te verwachten dat burgers, zoals vereist is, bij alle foto's en filmpjes van anderen die zij nemen en delen op sociale media, diegenen daarvan steeds van te voren op de hoogte stellen.

5.2 Privaatrecht

In Nederland worden horizontale rechtsverhoudingen grotendeels gereguleerd via het Burgerlijk Wetboek. In boek 6 van het Burgerlijk wetboek staat het verbintenissenrecht. Een verbintenis is een juridisch afdwingbare verplichting tussen twee of meer personen. Het verbintenissenrecht kan een rol spelen wanneer er schade ontstaat door het gebruik van drones en spionageproducten. Denk hierbij aan immateriële schade doordat men zich bespied voelt, of letselschade wanneer een drone tegen een mens aanvliegt. De belangrijkste rechtsgrond in het BW voor dit soort gevallen is de onrechtmatige daad, aangezien er niet snel sprake zal zijn van een contractuele relatie bij het gebruik van drones en/of spionageproducten.

Alvorens dieper in te gaan op de onrechtmatige daad, volgen eerst twee kanttekeningen die relevant zijn om de scope van dit privaatrechtelijk deel van het onderzoek te verduidelijken. In de eerste plaats, het gebruik van hobbydrones kan ook zonder enige inbreuk op privacy leiden tot schade die via het civielrecht verhaald kan worden. Zo kan een drone op verschillende manieren hinder veroorzaken die kan leiden tot schade. Een vliegveld kan ontregeld raken doordat er een drone in het luchtruim vliegt, beesten in natuurgebieden kunnen hinder ondervinden van drones waardoor ecologische schade kan ontstaan en een keeper in een voetbalwedstrijd kan gehinderd worden wanneer een drone in zijn buurt vliegt, het hierdoor verliezen van een wedstrijd zal leiden tot vermogensschade bij de club.[211] Ook kan een drone zaakschade en letselschade veroorzaken, als de drone ergens tegenaan vliegt, of – door bijvoorbeeld een

[211] 'Drone legt vliegverkeer Amerikaanse luchthaven plat', 10 april 2020; Malini Witlox, 'Jacht op dronepiloten in natuurgebied: 'Runderen kunnen echt in paniek raken'', Omroepbrabant.nl 10 april 2020. Yves Leroi, 'Hoe een drone een voetbalwedstrijd liet ontsporen', Volkskrant.nl 10 april 2020.

software update – spontaan uit de lucht valt.[212] In dit soort zaken kan het openbaar ministerie in Nederland beslissen om de hobbydrone-eigenaar te vervolgen, aangezien het op veel plaatsen niet is toegestaan met een drone te vliegen. Voor de private partij bestaat ook de mogelijkheid om de schade te verhalen via een civielrechtelijke procedure. Gezien de focus van dit onderzoek, wordt hieronder niet ingegaan op deze vormen van schadevergoeding. Het onderstaande beperkt zich tot het gebruik van hobbydrones en/of spionageproducten in enge zin die schade veroorzaken door een inbreuk te maken op de persoonlijke levenssfeer van een natuurlijke persoon.

De tweede kanttekening laat zien dat de onrechtmatige daad een beroep op de AVG onverlet laat. Wanneer het gebruik van een drone waarmee opnamen gemaakt worden of het gebruik van spionageproducten in strijd is met de AVG, is het niet noodzakelijk om een beroep te doen op de onrechtmatige daad. Zoals besproken in paragraaf 5.1 over gegevensbescherming, biedt de AVG een zelfstandige grond voor het verhalen van schade (artikel 82 AVG). In Nederland zijn in 2019 twee rechtszaken geweest waarbij private partijen deze rechtsgrond benut hebben voor het verhalen van schade geleden door onrechtmatige verwerking van persoonsgegevens. In een zaak tegen de gemeente Deventer is wegens schending van de AVG een schadevergoeding opgelegd van 500 euro.[213] In een zaak tegen het Uitvoeringsinstituut Werknemersverzekeringen (UWV) is een schadevergoeding opgelegd van 250 euro wegens immateriële schade geleden door onrechtmatige verwerking van persoonsgegevens.[214] Hoewel in deze zaken dus geen beroep wordt gedaan op de onrechtmatige daad, oordeelt de rechter wel dat voor de toekenning van schadevergoeding aansluiting mag en moet worden gezocht bij het Nederlandse rechtsbestel. Dit betekent dat eiser op grond van artikel 82 van de AVG in samenhang met artikel 6:106 van het BW recht heeft op een naar billijkheid vast te stellen schadevergoeding.

In het navolgende wordt de vraag behandeld hoe het Burgerlijk Wetboek uitkomst kan bieden bij het verhalen van schade ontstaan door schending van privacy door een drone of ander spionageproduct. De rol van het voorkomen van schade is hierbij beperkt, het gaat namelijk om een instrument dat enkel ingezet kan worden om daadwerkelijk geleden schade te verhalen. Echter, de wetenschap dat bepaald gedrag kan leiden tot de plicht om schadevergoeding te betalen, kan een prikkel inhouden om dit gedrag achterwege te laten. Bovendien is in de Nederlandse rechtspraak erkend dat het voor een inbreuk op privacy niet noodzakelijk is dat een

---

[212] 'Nederlandse inspectie waarschuwt voor neerstortende DJI-drones', Nu.nl 10 april 2020. Maaike Borst, 'Drone stort neer bij crèche in Groningen en raakt peuter', Dvhn.nl 10 april 2020.
[213] Rb. Overijssel 28 mei 2019, ECLI:NL:RBOVE:2019:1827.
[214] Iris de Groot, 'UWV moet werknemer 250 euro schadevergoeding betalen na datalek', ictrecht.nl 10 april 2020. Onder verwijzing naar de betreffende rechtszaken Rb. Overijssel 28 mei 2019, ECLI:NL:RBOVE:2019:1827 en Rb. Amsterdam 2 september 2019, ECLI:NL:RBAMS:2019:6490 en naar een uitspraak van de Hoge Raad van 15 maart 2019 waarin bepaald is dat "ook buiten gevallen van geestelijk letsel sprake kan zijn van aanspraak op vergoeding van immateriële schade." HR ECLI:NL:HR:2019:376. Ik kan deze zaak niet vinden.

drone is uitgerust met een daadwerkelijk filmende camera. Er is ook sprake van een onrechtmatige inbreuk op de privacy indien iemand zich bespied kan voelen.[215] Deze zaak wordt hieronder nader besproken. In de volgende paragraaf wordt eerst ingegaan op de wettelijke vereisten voor een onrechtmatige daad. Daarna worden enkele zaken behandeld waarin het gebruik van drones of spionageproducten hebben geleid tot een onrechtmatige daadsactie.

5.2.1 De onrechtmatige daad

Een van de rechtsgebieden opgenomen in het Nederlandse Burgerlijk Wetboek (BW) is het verbintenissenrecht (Boek 6 en 7 BW). In het verbintenissenrecht gaat het om rechten die tegenover een wederpartij gehandhaafd kunnen worden. Een verbintenis kan voortkomen uit de wet, een overeenkomst of een natuurlijke verbintenis. In onderstaande gaan we uit van een situatie waarin er geen overeenkomst bestaat tussen degene die een hobbydrone of spionageproduct in enge zin gebruikt, en degene die claimt hierdoor geschaad te worden. Een verbintenis is dan het gevolg van een feitelijke handeling tussen (rechts-)personen. Een feitelijke handeling is bijvoorbeeld de onrechtmatige daad. In artikel 6:162 BW staat de onrechtmatige daad als volgt beschreven:

> 1. Hij die jegens een ander een onrechtmatige daad pleegt, welke hem kan worden toegerekend, is verplicht de schade die de ander dientengevolge lijdt, te vergoeden.
>
> 2. Als onrechtmatige daad worden aangemerkt een inbreuk op een recht en een doen of nalaten in strijd met een wettelijke plicht of met hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt, een en ander behoudens de aanwezigheid van een rechtvaardigingsgrond.
>
> 3. Een onrechtmatige daad kan aan de dader worden toegerekend, indien zij te wijten is aan zijn schuld of aan een oorzaak welke krachtens de wet of de in het verkeer geldende opvattingen voor zijn rekening komt.

Zoals hierboven aangegeven biedt de AVG een eigen grond voor het verhalen van geleden schade, maar deze kan ook gebaseerd worden op de onrechtmatige daad, evenals schendingen van de Grondwet of het EVRM.[216] Als er wel sprake is van een schending van privacy maar niet van de AVG, biedt de onrechtmatige daad een grond om de geleden schade te verhalen. Een voorbeeld is de situatie waarin een camera aan een hobbydrone beelden van personen blurt (wazig maakt) zodat ze niet meer herkenbaar zijn.[217] Hoewel de AVG niet van toepassing is omdat anonieme gegevens geen persoonsgegevens zijn, kan de aanwezigheid van de

---

[215] Rb. Gelderland (ktr.) 10 mei 2017, ECLI:NL:RBGEL:2017:2663, ro. 2.4.
[216] M. van Emmerik, 'Schadevergoeding bij schending van mensenrechten revisited', *Verkeersrecht* (1) 2016, p. 6-12.
[217] In dit voorbeeld gaan we ervan uit dat de personen door het blurren niet meer te identificeren zijn.

hobbydrone alleen wel reeds een inbreuk op privacy opleveren. Hetzelfde geldt voor situaties waarin de drone mogelijk geen persoonsgegevens verwerkt, maar wel hinderlijk is, bijvoorbeeld door het geluid dat de drone maakt. Het enkele aanwezig zijn van een hobbydrone kan reeds als hinderlijk, en daarmee als een inbreuk op de persoonlijke levenssfeer (met name op de ruimtelijke privacy), ervaren worden. In het Burgerlijk Wetboek is in het burenrecht expliciet bepaald dat hinder een onrechtmatige daad kan opleveren. Artikel 5:37 BW stelt dat: 'De eigenaar van een erf mag niet in een mate of op een wijze die volgens artikel 162 van Boek 6 onrechtmatig is, aan eigenaars van andere erven hinder toebrengen zoals door het verspreiden van rumoer, trillingen, stank, rook of gassen, door het onthouden van licht of lucht of door het ontnemen van steun.' Of sprake is van onrechtmatige hinder hangt af van 'de aard, de ernst en de duur van de hinder en de daardoor toegebrachte schade in verband met de verdere omstandigheden van het geval. Daarbij moet onder meer rekening worden gehouden met het gewicht van de belangen die door de hinder toebrengende activiteit worden gediend en de mogelijkheid - mede gelet op de daaraan verbonden kosten - en de bereidheid om maatregelen ter voorkoming van schade te treffen'.[218] Zie over hinder ook paragraaf 5.5.1 waarin de modelverordening van de Vereniging van Nederlandse Gemeenten besproken is.

Uit de omschrijving van de onrechtmatige daad in het Burgerlijk Wetboek blijkt dat hiervan pas sprake is als aan vijf vereisten voldaan is: onrechtmatigheid, toerekenbaarheid, schade, causaliteit en relativiteit.

a) Onrechtmatigheid

In de casuïstiek die in deze studie centraal staat, zal de onrechtmatigheid over het algemeen voortvloeien uit een schending van de wet: de AVG of het recht op privacy zoals neergelegd in de Nederlandse Grondwet en het EVRM. Eventueel kan dit handelen – het gebruik van een drone en/of spionageproduct – als zodanig ook onbetamelijk worden geacht.

b) Toerekenbaarheid

Een onrechtmatige daad kan aan de dader worden toegerekend, indien de gedraging die leidt tot schade te wijten is aan zijn schuld of aan een oorzaak welke krachtens de wet of de in het verkeer geldende opvattingen voor zijn rekening komt.[219] De term schuld betekent dat de dader rechtens een verwijt van zijn onrechtmatige gedraging moet zijn te maken.[220] Het moet dus gaan om verwijtbaar handelen van degene die de hobbydrone of het spionageproduct in enge zin gebruikt. Wanneer gebruik gemaakt wordt van drones of spionageproducten waardoor derden schade lijden ligt toerekenbaarheid voor de hand. Ten eerste gelden er strikte regels voor het vliegen met drones (zie par. 5.6.2) en is het volgens de in het verkeer geldende

---

[218] HR 21 oktober 2005, ECLI:N :PHR:2005:AT8823.
[219] Artikel 6:162 Burgerlijk Wetboek.
[220] B. Reehuis, '*Zwaartepunten van het vermogensrecht',* Deventer: Wolters Kluwer 2015, p. 367.

maatschappelijke opvattingen onacceptabel om anderen te bespioneren. Hoewel de gebruiker van een hobbydrone of een spionageproduct in enge zin mogelijk niet van tevoren kan weten wat hij precies vast zal leggen aan beeld- en of geluidsmateriaal, staat dit er niet aan in de weg dat hem de gedraging wel kan worden toegerekend. Hij neemt immers willens en wetens het risico voor het gebruik van de drone en/of het spionageproduct. Zoals hieronder zal blijken, in de rechtspraak is voor inbreuk ook niet bepalend of een drone binnen een bepaald gebied gebleven is, maar wat de camera daadwerkelijk heeft opgenomen. Wat in dit verband een probleem kan zijn, is dat het mogelijk niet altijd duidelijk is van wie een drone of een spionageproduct is. Wanneer dit voor het slachtoffer niet duidelijk is, of niet te bewijzen is, zal het lastig zijn de gedraging die leidt tot de schade aan de veroorzaker ervan toe te rekenen.

c) Schade

Artikel 6:162 BW geeft niet uitdrukkelijk aan wat de definitie is van schade. In artikel 6:95 BW staat dat schadevergoeding kan bestaan uit vermogensschade (materiële schade) en/of ander nadeel (immateriële schade). Zowel de hoogte van vermogensschade als van immateriële schade is niet altijd eenvoudige te bewijzen in zaken betreffende een schending van privacy. Uit de jurisprudentie blijkt voorts dat de hoogte van de gevorderde schadevergoeding vaak lager uitvalt dan hetgeen is geëist. Zoals hierboven reeds aangegeven zijn recentelijk bedragen van 500 euro en 250 euro toegekend voor een schending van de AVG. Of dit voldoende is om een zaak te starten wegens schending van privacy is discutabel, gezien de tijd en inspanning die een rechtszaak vergt. Bekende zaken waarin een schadevergoeding is toegekend wegens schending van privacy zijn een zaak tegen SBS en de zaak van Patricia Paay tegen Geenstijl. In de zaak tegen SBS was sprake van een televisie-uitzending waarbij de eiser herkenbaar in beeld kwam. Er werd een schadevergoeding geëist van 500.000 euro, maar er werd 3000 euro toegekend.[221] Dit vanwege een gebrek aan deugdelijke onderbouwing van het gevorderde bedrag, en omdat de eiser niet negatief in beeld was gebracht.[222] In de zaak die Patricia Paay tegen Geenstijl heeft aangespannen wegens het verspreiden van een seksvideo, werd 450.000 euro schadevergoeding geëist.[223] In deze zaak werd er 30.000 euro toegekend voor het verspreiden van de naaktbeelden (waardoor inbreuk wordt gemaakt op de lichamelijke privacy), waarbij de rechter in overweging neemt dat niet alleen via Geenstijl aandacht was voor de video, maar dat Geenstijl wel de verspreiding van bewegende beelden gefaciliteerd heeft (en waardoor een inbreuk op informationele privacy), hetgeen een andere associatie geeft dan enkel het vermelden dat een dergelijke video bestaat. Volgens de rechter leidt dit wel degelijk tot een

[221] Rb. Gelderland 27 december 2017, ECLI:NL:RBGEL:2017:6890.
[222] Idem, ro 4.15. Er wordt hier verwezen naar een zaak waarin het smartengeld wel hoger uitviel, € 75.000, omdat de klager in die zaak in een kwaad daglicht werd gesteld (Smartengeld, ANWB 22e druk 2017, nr. 1.177). In casu is de eiser in de tv-uitzending niet in een kwaad daglicht gesteld, Endemol c.s. heeft een feitelijk juist verhaal gebracht.
[223] Rb. Amsterdam 25 juli 2018, ECLI:NL:RBAMS:2018:5130.

rechtstreeks en af te zonderen gevolg van hun handelwijze, waarvoor 30.000 euro immateriële schade wordt toegekend, zonder de hoogte van dit bedrag nader te onderbouwen.

d) Causaal verband

Het causaal verband is geregeld in artikel 6:162 lid 1 BW juncto artikel 6:98 BW. Om de gebruiker van een drone of spionageproducten aansprakelijk te kunnen stellen, moet degene die schade heeft geleden kunnen bewijzen dat er verband bestaat tussen de geleden schade en het gebruik van de drone en/of het spionageproduct. Wanneer de dader stelt dat de schade ook zou zijn ontstaan als er geen sprake zou zijn geweest van het gebruik, geldt de omkeringsregel. Het is dan aan de dader om te bewijzen dat de schade ook zonder het gebruik van de drone en/of het spionageproduct zou zijn ontstaan.[224]

e) Relativiteitsvereiste

Naast het feit dat de gedraging onrechtmatig moet zijn op grond van artikel 6:162 lid 1 BW, moet ook de aard van de schade evenals de wijze waarop deze is ontstaan onder bescherming van de geschonden norm vallen.[225] Dit volgt uit het relativiteitsvereiste dat is neergelegd in artikel 6:163 BW. Bij schending van privacy door het gebruik van een hobbydrone of een spionageproduct in enge zin wordt er voldaan aan het relativiteitsvereiste. Het recht op privacy en het recht op gegevensbescherming zijn immers bedoeld om diegenen die in deze rechten worden aangetast bescherming te bieden.

Na analyse en toepassing van artikel 6:162 BW kan worden geconcludeerd dat de onrechtmatige daad een mogelijkheid biedt om de gebruiker van een hobbydrone of spionageproduct in enge zin civielrechtelijk aansprakelijk te stellen voor hierdoor geleden materiële en immateriële schade. Natuurlijk zal de definitieve beoordeling of sprake is van een onrechtmatige daad bij de rechter liggen en afhankelijk zijn van de feiten en omstandigheden van ieder geval. Bij de beoordeling van onrechtmatige daad en de omvang van de schadevergoeding moet er volgens de Hoge Raad een vergelijking worden gemaakt tussen de situatie waarin de benadeelde als gevolg van de onrechtmatige daad verkeert, en de situatie waarin hij zonder de onrechtmatige daad zou verkeren.[226] Voor wat betreft de geleden schade is het hierbij in het bijzonder van belang om de hoogte van de gevorderde schadevergoeding zeer goed te onderbouwen.

5.2.2 De onrechtmatige daad in Nederlandse rechtspraak

Dat de onrechtmatige daad ook in de praktijk een instrument biedt om op te treden tegen schade die veroorzaakt wordt door drones of spionageproducten blijkt uit de Nederlandse rechtspraak. In

---

[224] HR 29 november 2002, ECLI:NL:PHR:2002:AE7345.
[225] B. Reehuis, '*Zwaartepunten van het vermogensrecht',* Deventer: Wolters Kluwer 2014, p. 364.
[226] HR 18 januari 2002, HR 18-01-2002, ECLI:NL:HR:2002:AD4915.

de Nederlandse databank met rechtspraak[227] is gekeken of er zaken zijn waarin burgers op grond van de onrechtmatige daad schadevergoeding hebben gevorderd wegens een inbreuk op privacy veroorzaakt door het gebruik van hobbydrones of spionageproducten. Ten eerste is gezocht op de combinatie “drone en onrechtmatige daad”.[228] Uit deze zoekopdracht bleek dat er enkele relevante zaken zijn over hobbydrones. Om te kijken of er reeds zaken zijn rondom het gebruik van spionageproducten in enge zin in horizontale relaties is gezocht op een combinatie van onrechtmatige daad en de volgende woorden, welke geselecteerd zijn omdat zij vaker voorkomen in deze studie: ‘spionage’, ‘surveillance’, ‘stalken’, ‘richtmicrofoons’, ‘afluisteren’, ‘tracking’ en ‘tracing’. Hieruit bleek dat deze zoekopdrachten niet veel opleverde in horizontale relaties. Als de zoekopdrachten al tot resultaten leidden, ging het vooral om zaken in de relatie overheid–burger. Aangezien het in deze studie gaat om horizontale spionage, zijn deze zaken buiten beschouwing gelaten. Bij het zoeken op ‘onrechtmatige daad en camera’s’ en ‘onrechtmatige daad en heimelijk’ waren er veel resultaten. Aangezien het in dit onderzoek gaat om privacy en persoonsgegevens, zijn deze zoektermen toegevoegd aan de zoekopdracht. De relevante zaken die voortvloeien uit de hierboven beschreven zoekopdrachten worden hieronder kort beschreven.

a) Rechtsprak over drones en de onrechtmatige daad

Bij het zoeken op drone en onrechtmatige daad komen drie zaken naar boven die gaan over het gebruik van een drone in een horizontale relatie, waarbij twee zaken dezelfde feitelijke gedragingen betreffen. Het gaat om een zaak tussen twee buren waarin de vraag centraal staat of het vliegen me een drone en het vervolgens neerhalen van de drone rechtmatig zijn. De ene buur vliegt met een drone over het perceel van de andere buur, waardoor deze zich in zijn privacy (in dit geval vooral ruimtelijke en gedragsmatige privacy) voelt aangetast en daarom besluit de drone met een luchtbuks neer te schieten.[229] In de zaak die hierop volgt, staat de vraag naar vergoeding van de geleden schade centraal, waarbij het zowel gaat om de schade die geleden is door de inbreuk op de privacy, als om de schade die geleden is aan de drone.[230] De rechter oordeelt dat allebei de gedragingen onrechtmatig zijn en dat ieder de helft van de schade moet dragen. In deze zaak is geen schadebedrag gevorderd voor de inbreuk op de privacy, enkel het verbieden om met de drone te vliegen boven het perceel toebehorend aan de buurman en/of te filmen met een aan een drone verbonden camera boven dit perceel, op straffe van een dwangsom van € 250,00 per overtreding. Daarnaast moet een afschrift worden verstrekt van de gemaakte camerabeelden, binnen veertien dagen, op straffe van een dwangsom van € 100,00 per dag indien hieraan niet wordt voldaan. De rechter oordeelt dat beter bewijs overlegd

[227] Rechtspraak.nl.
[228] Voor de volledigheid is ook nog gekeken naar “drone en privacy” en “drone en AVG” maar dit levert geen andere relevante zoekresultaten op.
[229] Rb. Gelderland 21 december 2016, ECLI:NL:RBGEL:2016:7155.
[230] Rb. Gelderland, 10 mei 2017, ECLI:NL:RBGEL:2017:2663.

moet worden voor de geleden schade aan de drone, welk schadebedrag dus gedeeld moet worden, en compenseert de proceskosten zodanig dat iedere partij de eigen kosten draagt.

Interessant in beide zaken is dat de rechter bevestigd dat het voor een inbreuk op privacy niet noodzakelijk is dat een drone is uitgerust met een daadwerkelijk filmende camera. Een onrechtmatige inbreuk op de privacy bestaat reeds indien de bewoner zich bespied kan voelen, welke situatie zich voordoet als de bewoner in onzekerheid verkeert over de vraag of de drone filmbeelden registreert. In deze zaak was overigens wel degelijk sprake van een filmende GoPro-camera, aangezien de beelden hiervan zijn gebruikt om aan te tonen dat de drone met een buks uit de lucht is geschoten. Daarmee staat aldus de rechter vast dat sprake was van een situatie waarin gedaagde zich bespied heeft gevoeld en kon voelen, zodat onrechtmatig gehandeld werd door eiser.

Dat partijen beide de helft van de schade moeten betalen wordt gebaseerd op het feit dat beide onrechtmatige handelingen samen de schade aan de drone hebben veroorzaakt. Indien geen inbreuk was gemaakt op de privacy van gedaagde had deze niet geschoten en was de drone niet beschadigd door het schot. Op grond van artikel 6:101 BW geldt dat de schade in een dergelijk geval wordt verdeeld over beide partijen, in evenredigheid met de mate waarin de aan ieder toe te rekenen omstandigheden tot de schade hebben bijgedragen. Daar kan een billijkheidscorrectie op worden aangebracht indien de ernst van de gemaakte fouten of andere omstandigheden dat eisen. De rechter oordeelt dat hiervan geen sprake is:

> Een inbreuk op het recht op privacy is niet minder of zwaarder dan de inbreuk op het eigendomsrecht. Ook zijn de omstandigheden niet zodanig dat een billijkheidscorrectie als bedoeld in dit artikel aan de orde is. Zelfs indien moet worden aangenomen dat, zoals [gedaagde] stelt, sprake is van stelselmatige pesterijen, dan nog stond het [gedaagde] niet vrij het eigendom van [eiser] uit de lucht te schieten en had hij voor andere, minder ver gaande maatregelen moeten kiezen, zoals een verzoek aan [eiser] om te stoppen (eventueel via een kort geding) of het inschakelen van de wijkagent. Dit brengt mee, dat ieder van partijen 50% van de schade dient te dragen.[231]

Hieruit lijkt te volgen dat het een gemiste kans is van de gedaagde partij om geen tegenvordering in te dienen voor een schadevergoeding voor de schade geleden door de privacy-inbreuk, welke inbreuk wel door de rechter bevestigd is.

Ook de rechtbank Midden Nederland moest zich buigen over de rechtmatigheid van het vliegen met een drone boven het perceel van een buurman (waarbij vooral sprake is van ruimtelijke en gedragsmatige privacy), en ook in deze zaak wordt geoordeeld dat dit niet is toegestaan. De rechter verbiedt: “om opnames te maken van het erf van [eiser] (…), daaronder onder meer

[231] Idem, overweging 2.7.

begrepen het laten vliegen van een drone; (…) indien zij niet voldoen (…) zal een dwangsom worden verbeurd van € 250,00 per dag, totdat een maximum is bereikt van € 10.000,00."[232] Interessant in deze zaak is dat de rechter het argument verwerpt dat het niet onrechtmatig is om met een drone boven eigen erf te vliegen. De rechtbank geeft aan dat het boven het eigen erf laten vliegen van een drone geenszins meebrengt dat de reikwijdte van de opnames ook beperkt blijft tot de eigen zaken. De rechtbank wees op het feit dat drones, anders dan (stationaire) camera's, een *bird's eye view* (vogelvluchtperspectief) geven, waardoor opnames verder kunnen reiken dan het eigen terrein en dus inbreuk kunnen maken op het recht van privacy van personen buiten dit terrein.[233]

b) Rechtspraak over spionageproducten in enge zin

In de databank rechtspraak.nl is nog geen jurisprudentie te vinden op het gebied van privaatrecht met betrekking tot burgers die elkaar bespioneren met spionageproducten in enge zin. Toch kunnen er enkele relevante conclusies worden getrokken op basis van zaken met betrekking tot stalken en spionage door journalisten.

De zoekopdracht naar onrechtmatige daad en stalken levert één uitspraak op die relevant is om te vermelden. Hoewel het hier niet gaat om het gebruik van spionageproducten, blijkt uit deze zaak wel dat jarenlange anonieme stalking/belaging met het oogmerk om de belaagde emotioneel en geestelijk te raken en hem bang te maken, zodat hij overspannen zou raken, een onrechtmatige daad betreft.[234] Hoewel dit niet het geval hoeft te zijn bij spionageproducten in enge zin, kan er toch sprake zijn van een onrechtmatige verstoring van de privacy (bijv. gedragsmatige en relationele privacy) door zich bespioneerd te voelen. Indien voldaan is aan de hierboven vermelde voorwaarden, kan hiertegen mogelijk civielrechtelijk worden opgetreden.

Het in de databank rechtspraak.nl zoeken naar "onrechtmatige daad en afluisteren" levert ook één relevante zaak met betrekking tot journalisten op.[235] In deze zaak neemt een journalist heimelijk een gesprek op met een politicus en maakt dit gesprek openbaar (waardoor inbreuk wordt gemaakt op communicatieve en informationele privacy). De rechter oordeelt dat hier geen sprake is van een onrechtmatige daad omdat niet aan alle vereisten voor schadeplichtigheid uit hoofde van de onrechtmatige daad is voldaan. Volgens de rechter staat het causaal verband tussen het onrechtmatig handelen en de gestelde schade, het verwoesten van de politieke carrière van eiser, niet vast. Bovendien bestaat er voor het delen van de opname een rechtvaardigingsgrond die het onrechtmatig karakter doet vervallen. Het maatschappelijk belang van het aan de kaak stellen van de integriteit van een publiek figuur weegt zwaarder dan het belang van het publiek figuur. Met betrekking tot burgers die voor niet-journalistieke doeleinden

---

[232] Rb. Midden-Nederland, 25 augustus 2017, ECLI:NL:RBMNE:2017:4224, ro 7.3 & 7.4.
[233] Rb. Midden-Nederland 25 augustus 2017, ECLI:NL:RBMNE:2017:4224 ro. 5.20-5.21.
[234] Hof Arnhem-Leeuwarden 14 april 2015, ECLI:NL:GHARL:2015:2650.
[235] Rechtbank Midden-Nederland 19-10-2016, ECLI:NL:RBMNE:2016:5408.

spioneren op andere burgers die geen publieke figuren zijn, kunnen we - a contrario - speculeren dat het hof over het algemeen geen publiek belang zal vinden. Een dergelijke conclusie is ook in overeenstemming met artikel 8 van de jurisprudentie van het EHRM, waarin wordt gesteld dat particuliere ('gewone') burgers een ruimere bescherming van het privéleven (ook in de publieke sfeer) hebben, zodat zij niet zonder hun medeweten of toestemming kunnen worden geregistreerd.[236]

5.2.3 Deelconclusie en discussie: mogelijke lacunes en reguleringsmogelijkheden

Op basis van bovenstaande discussie bieden we hier een samenvatting van de geïdentificeerde mogelijke lacunes (antwoord op deelvraag 4) en bespreken we verder de mogelijkheden voor hun regulering (antwoord op deelvraag 8).

Na analyse van artikel 6:162 BW kan worden geconcludeerd dat de onrechtmatige daad een mogelijkheid biedt om de gebruiker van een hobbydrone of spionageproduct in enge zin privaatrechtelijk aansprakelijk te stellen voor hierdoor geleden materiële en immateriële schade. Voor wat betreft inbreuken op het recht op gegevensbescherming gaat het om een aanvullende grond, aangezien ook rechtstreeks op grond van de AVG schadevergoeding gevorderd kan worden. Het is maar de vraag of het risico dat schade vergoed moet worden voldoende afschrikwekkende werking heeft om bepaald gedrag te voorkomen.

Hoewel het recht op schadevergoeding het slachtoffer iets in handen geeft, is de inbreuk op privacy echter vaak niet meer te herstellen, ofwel het kwaad is al geschied. Met betrekking tot mogelijke lacunes (deelvraag 4), zal het ook niet altijd duidelijk zijn wie de eigenaar is van een hobbydrone of een spionageproduct in enge zin, hetgeen het voor een slachtoffer nog lastiger kan maken om de schade op de dader te verhalen. Bij drones kun je lang niet altijd de bestuurder zien of vinden en bij spionageproducten in enge zin (bijv. een spycam die je in een gehuurd appartement aantreft) is het ook niet altijd duidelijk wie die geplaatst heeft. Bij drones en spionageproducten in enge zin zal er over het algemeen ook geen sprake zijn van een intermediair die je kunt vragen om identificerende gegevens van de gebruiker.[237] Bij het niet kunnen identificeren van een dader zal het slachtoffer met lege handen staan. Deze problemen kunnen echter niet worden opgelost door wijzigingen in het Burgerlijk wetboek (deelvraag 8). Zoals gesuggereerd in de zaak over het uit de lucht schieten van de drone kan een burger

---

[236] EHRM 15 januari 2009, ECLI:CE:ECHR:2009:0115JUD000123405 (*Reklos en Davourlis*/Griekenland), par. 40; EHRM 11 januari 2005, ECLI:CE:ECHR:2005:0111JUD005077499 (*Sciacca*/Italië), par. 57.

[237] Vergelijk bijvoorbeeld met de zaak Lycos/Pessers waarin een hosting provider verplicht werd tot het verstrekken van de naam en het adres van een websitehouder aan een derde die stelde schade te hebben geleden door een op de 'gehoste' website gepubliceerde anonieme beschuldiging. HR 25 november 2005, ECLI:NL:PHR:2005:AU4019 & Hof Amsterdam 24 juni 2004, ECLI:NL:GHAMS:2004:AR2103.

mogelijk de hulp van een wijkagent inschakelen, of in geval van een strafrechtelijke gedraging aangifte bij de politie doen (zie par. 5.4 over Strafrecht).

Een ander problematisch punt en een mogelijke lacune (met betrekking tot deelvraag 4) is het aantonen van de hoogte van de geleden schade. Zowel de hoogte van vermogensschade als van immateriële schade is niet altijd eenvoudige te bewijzen in zaken betreffende een schending van privacy. En ook bij het toekennen van schadevergoeding blijkt lang niet altijd sprake van een deugdelijke onderbouwing van het toegekende schadebedrag. Deze lacune kan echter worden opgelost door hogere schade toe te kennen voor zowel materiële als immateriële inbreuk op de privacy (deelvraag 8). Het toekennen van hogere schade zou kunnen leiden tot een grotere afschrikking van inbreuk op de privacy of, althans, de mogelijkheid om civielrechtelijke stappen te ondernemen een betere optie maken voor slachtoffers van inbreuk op de privacy.

Tot slot verdient het nog opmerking dat het voor onrechtmatigheid verschil kan maken wie er gebruik maakt van drones en spionageproducten en voor welk doel dit gebeurt. Er zijn in de rechtspraak verschillende situaties erkend waarin de bescherming van een ander belang, zoals de vrijheid van meningsuiting waaronder het recht om informatie te vergaren en te ontvangen, zwaarder weegt dan een inbreuk op de privacy.

5.3 Het portretrecht

Het portretrecht, dat is opgenomen in de Auteurswet (en als zodanig deel uitmaakt van het intellectueel eigendomsrecht), kent rechten toe aan personen van wie een ‘portret’ is vastgelegd. Als portret moet, volgens de parlementaire geschiedenis van de Auteurswet, worden begrepen: ‘een afbeelding van het gelaat van een persoon, met of zonder die van verdere lichaamsdelen, op welke wijze zij ook vervaardigd is’.[238] Dit recht heeft dus het meest direct betrekking op de lichamelijke privacy, hoewel het ook belangen kan beschermen die verband houden met andere vormen van privacy, met name gedragsmatige en relationele privacy (aangezien het nemen van een foto vaak ook onthult wat men doet en met wie men relaties aangaat). Zoals het EHRM het stelt, wordt de bescherming van het imago van een persoon beschouwd als een van de ‘essentiële onderdelen van de persoonlijke ontwikkeling’, omdat het de unieke kenmerken van de persoon blootlegt en de persoon onderscheidt van zijn of haar gelijken.[239] Hierbij wordt dus geen onderscheid gemaakt in hoe de afbeelding tot stand is gekomen. Foto’s, video’s, maar ook schilderijen en tekeningen kunnen als portret worden aangemerkt. De Auteurswet maakt onderscheid tussen portretten die in opdracht van de afgebeelde persoon zijn gemaakt (art. 19 en 20 Aw), en portretten die niet in diens opdracht gemaakt zijn (art. 21 Aw). In het geval van

[238] J. Spoor e.a., *Recht en Praktijk 42: Auteursrecht: Auteursrecht, naburige rechten en databankenrecht*, Deventer: Wolters Kluwer 2005, p. 306.
[239] EHRM 15 januari 2009, ECLI:CE:ECHR:2009:0115JUD000123405 (*Reklos en Davourlis*/Griekenland), par. 40.

particulier dronegebruik of andere spionageproducten in enge zin zal de laatstgenoemde situatie, en dus art. 21 Aw, het meest van toepassing zijn.

5.3.1 Redelijk belang

Art. 21 Aw geeft aan dat publicatie van een portret dat zonder toestemming is gemaakt ongeoorloofd *kan* zijn indien een 'redelijk belang' van de geportretteerde zich tegen die publicatie verzet. Het bestaan van een dergelijk belang wordt door de rechter bepaald aan de hand van een belangenafweging tussen het belang van informatievrijheid in de zin van art. 10 EVRM en het belang van de bescherming van de persoonlijke levenssfeer in de zin van art. 8 EVRM.[240] Het maken van een dergelijke belangenafweging wordt ook bevestigd door het Europese Hof voor de Rechten van de Mens (EHRM).[241]

Wat tevens relevant is voor de bepaling of sprake is van een redelijk belang, is de wijze waarop het beeld tot stand is gekomen. Hierbij moet gedacht worden niet alleen aan het geven van toestemming, maar ook of de geportretteerde zich bewust was van het feit dat de foto werd genomen dan wel dat de foto werd genomen middels geheime of ongeoorloofde middelen.[242] In gevallen waar de geportretteerde zich niet bewust was van het tot stand komen van het portret, is de rechter eerder geneigd een redelijk belang van de geportretteerde aan te nemen. Een voorbeeld hiervan kan gevonden worden in het arrest Paul de Leeuw/Story, waarin een ongeoorloofde inbreuk werd vastgesteld door de rechtbank nadat met een fototoestel met telelens zonder zijn medeweten foto's zijn gemaakt van De Leeuw en zijn kind door het raam van zijn woning.[243] Het is niet ondenkbaar om te stellen dat het gebruik van spionageproducten vergelijkbare situaties in het leven roept: zij kunnen van een afstand en van boven (vooral bij drones) van boven beelden maken van personen, hun gedrag en anderen naast hen, zonder dat zij enige weet hebben van de aanwezigheid van het spionageproduct dan wel (bij drones) van de identiteit van diens bediener.

5.3.2 Beperkingen van het portretrecht

Het is belangrijk om vast te stellen dat de Hoge Raad heeft bepaald dat voor geoorloofde publicatie niet altijd toestemming is vereist.[244] Publicatie van een portret dat zonder opdracht is gemaakt en zonder toestemming is gepubliceerd, kan bijvoorbeeld geoorloofd zijn in gevallen dat iemand zich in de publieke ruimte begeeft. In een arrest van het gerechtshof Amsterdam is bijvoorbeeld gebleken dat het belang van informatievoorziening meebrengt dat in sommige gevallen foto's gepubliceerd worden waarbij het onvermijdelijk is dat toevallige passanten daarop

---

[240] HR 21 januari 1994, ECLI:NL:HR:1994:ZC1240, *NJ* 1994/473 (*Ferdi E.*).
[241] EHRM 24 juni 2004, ECLI:CE:ECHR:2004:0624JUD005932000 (*Caroline von Hannover/Duitsland I*).
[242] EHRM 7 februari 2012, ECLI:CE:ECHR:2012:0207JUD004066008 (*Caroline von Hannover/Duitsland 2*), par. 113.
[243] Rb. Amsterdam 7 mei 2003, ECLI:NL:RBAMS:2003:AF8332 (*Paul de Leeuw/Story*).
[244] HR 14 juni 2013, ECLI:NL:HR:2013:CA2788, *LJN* CA2788 (*Cruijff/Tirion*).

zichtbaar zijn.[245] Het is van belang om vast te stellen dat dit arrest het belang van informatievoorziening (aan het publiek) betrof, hetgeen meestal niet aanwezig zal zijn bij gevallen van particuliere spionage. Het kan dus niet zonder meer gezegd worden dat het publiceren van afbeeldingen met toevallige passanten op foto's bij privaat gebruik van drones of spionageproducten toelaatbaar zal zijn.

In het geval van bekende personen vormt de bevordering van het publieke debat een sterke indicator voor de geoorloofdheid van de publicatie: als er een bijdrage wordt geleverd aan het publieke debat, is geen toestemming vereist.[246] In het geval van de gemiddelde burger (zowel de burger die beelden publiceert, als de burger wiens beeld gepubliceerd wordt) zal het publieke debat echter weinig relevant zijn, hetgeen meer aandacht laat voor de bescherming van de persoonlijke levenssfeer.

Er bestaan meer situaties waarin het portretrecht minder bescherming biedt aan personen. Het betreft dan situaties waarin iemand zelf al zijn beeltenis verkoopt of openbaar maakt,[247] situaties waarin iemand geen bezwaar maakt tegen en niet bang is voor de onaangekondigde aanwezigheid van camera's,[248] situaties waarin iemand als toeschouwer naar een openbaar evenement gaat waar beeldmateriaal gemaakt wordt[249] of situaties waarin iemand als zichtbare deelnemer naar een openbaar evenement gaat.[250] Er lijkt dus een lijn te bestaan in de rechtspraak dat als personen zelf iets doen of hebben gedaan om aandacht op zichzelf te vestigen, of zich op plekken begeven waar weinig privacy kan worden verwacht, deze personen op minder bescherming kunnen rekenen van het portretrecht. Bij hobbydrones (en andere spionageproducten in brede zin, zoals smartphones), is het echter waarschijnlijk (zie de discussie over smartphones in par. 5.4.1) dat personen zich vaak niet bewust zijn van het feit dat ze worden gefotografeerd of gefilmd, zelfs als deze producten zichtbaar zijn – het is namelijk zeer moeilijk om vast te stellen of iemands beeld is opgenomen. Bovendien is het bijna onmogelijk om bezwaar te maken tegen de opname in het geval van drones, waarbij de bediener van de drone het meestal onbekend is. Onder deze omstandigheden kunnen we concluderen dat het portretrecht slechts een beperkte oplossing biedt voor de inbreuken op de privacy (met betrekking tot deelvraag 4). Desalniettemin, zal de rechter over het algemeen wel snel

---

[245] Hof Amsterdam 27 januari 2009, ECLI:NL:GHAMS:2009:BH3726, *LJN* BH3726 (*X/Hollandse Hoogte)*.
[246] EHRM 24 juni 2004, ECLI:CE:ECHR:2004:0624JUD005932000 (*von Hannover/Duitsland I*) en Rb. Amsterdam 6 februari 2008, ECLI:NL:RBAMS:2008:BC3781 (*Prins Willem-Alexander c.s./Audax)*. Beide arresten betreffen leden van koningshuizen buiten de uitvoering van publieke taken. Beide gerechtelijke instanties hebben erkend dat het publieke figuren betrof, maar deze zijn in de respectievelijke casussen beschouwd als individuen in hun persoonlijke levenssfeer.
[247] EHRM 23 juli 2009 (legal summary), ECLI:CE:ECHR:2009:0723JUD001226803 (*Hachette/Frankrijk*).
[248] Hof Amsterdam 22 september 2009, nr. B9 8216. Dit betrof een televisieprogramma, echter ligt het voor de hand dat als dit geldt voor opnames van een televisieprogramma, dit ook geldt voor opnames door een private partij.
[249] Rb. 's-Hertogenbosch (vzr.) 22 augustus 2002, ECLI:NL:RBSHE:2002:AE6844.
[250] Hof Amsterdam (vzr.) 15 mei 2012, ECLI:NL:GHAMS:2012:BW5768.

bescherming bieden in het geval iemand in een compromitterende toestand wordt geportretteerd (bijvoorbeeld topless zonnebaden).[251]

Toch betekent het simpelweg zich begeven in de publieke ruimte betekent niet dat het portretrecht helemaal geen bescherming meer biedt. Zo heeft de Hoge Raad in het Vondelpark-arrest, betreffende een foto gemaakt van een omarmend stel in het Vondelpark, geoordeeld tegen de publicatie van die foto, ondanks dat deze gemaakt was in een openbaar park.[252] Indien iemand zich begeeft in een 'nogal afgesloten plek' in de publieke ruimte waar iemand zich 'onbespied' kan wanen, kan dit eveneens leiden tot een redelijk belang.[253] Ook de rechtspraak van het EHRM bevestigt de bescherming van het portretrecht in de publieke ruimte,[254] door in een arrest te stellen dat de publicatie van beelden van iemand die zich op de openbare weg van het leven neigde te beroven veel meer openbaarmaking veroorzaakte dan diegene kon voorzien. [255] Het Hof verwijst hier naar het onthullen van niet alleen het portret, maar ook andere aspecten van het privéleven, zoals het gedrag en de relaties (dus met betrekking tot gedragsmatige en relationele privacy). Dat de persoon in kwestie zich op de openbare weg had begeven deed niet af aan zijn bescherming.

5.3.3 Rechtsmiddelen

Op de tekst bekeken biedt art. 21 Aw alleen bescherming tegen openbaarmaking van een portret. Dit artikel kan enkel worden ingeroepen als er daadwerkelijk beelden van een persoon worden gemaakt. Als een individu wil klagen via de weg van het portretrecht, moet er immers een portret zijn. De lezing van het portrecht is echter uitgebreid om 'in de meeste gevallen' een recht te omvatten om bezwaar te maken tegen de creatie van een portret (lees: het maken van de foto, het opnemen van een video, etc.) te omvatten.[256] Ook kan via het middel van onrechtmatige daad (art. 6:162 BW) opgetreden worden tegen het maken en bewaren van portretten. De onrechtmatige daad is een civiel rechtsmiddel om schadevergoeding te ontvangen wegens het handelen van een ander in strijd met een wettelijke plicht of zorgvuldigheidsnormen (voor meer over de onrechtmatige daad zie het deel in par. 5.2.2). Deze samenhang met onrechtmatige daad is niet vreemd, aangezien art. 21 Aw algemeen gezien wordt als een

---

[251] J.H. Spoor e.a., *Recht en Praktijk 42: Auteursrecht: Auteursrecht, naburige rechten en databankenrecht*, Deventer: Wolters Kluwer 2005, p. 304.
[252] HR 1 juli 1988, NJ 1988/1000 (*Vondelpark*).
[253] O.M.B.J. Volgenant, 'VII.8.5.1.2 Redelijk belang aangenomen', in C.J.J.M. Stolker (red.), *Groene Serie Onrechtmatige Daad*, Deventer: Wolters Kluwer; Rb. Amsterdam (vzr.) 13 oktober 2003, ECLI:NL:RBAMS:2003:AL8451, *Mediaforum* 2004/2 (*Bloemen/Audax*) en Rb. Amsterdam 29 maart 2006, ECLI:NL:RBAMS:2006:AV7581 *Mediaforum* 2006/13.
[254] Voor een overzicht van de jurisprudentie van het EHRM met betrekking tot de bescherming van de privacy in de openbare ruimte, zie M. Galič, 'Surveillance and privacy in smart cities and living labs: conceptualising privacy *for* public space' 2019.
[255] EHRM 28 januari 2003, ECLI:CE:ECHR:2003:0128JUD004464798 (*Peck/VK*).
[256] EHRM 15 januari 2009, ECLI:CE:ECHR:2009:0115JUD000123405 (*Reklos & Davourlis/Griekenland*), par. 40. Het Hof spreekt over 'in most cases', maar specificeert niet wat voor situaties hier wel of niet onder vallen. Het Hof legt echter wel nadruk op het feit dat de bescherming van iemands beeltenis (image) essentieel is voor persoonlijke ontwikkeling, en dat dit controle over het gebruik van die beeltenis veronderstelt.

verbijzondering van de onrechtmatige daad.[257] De rechtbank Gelderland is in 2016 nog een stap verder gegaan en heeft aangenomen dat – volgens de onrechtmatige daad – het vliegen met een drone op een wijze waarop de camera van de drone beelden kan maken van wat er in een woning gebeurt, ook als de camera niet aan staat, een ongerechtvaardigde schending van de persoonlijke levenssfeer oplevert.[258]

Met betrekking tot lacunes (deelvraag 4), kunnen we concluderen dat deze middelen echter vooraf geen uitkomst kunnen bieden, als een geportretteerde wel een drone opmerkt, maar niet kan achterhalen wie de eigenaar is van de drone om diegene aan te spreken of om anderszins bezwaar te maken tegen het maken van het portret. Noch zullen deze middelen op voorhand tot hulp zijn in andere gevallen van heimelijke of onopgemerkte surveillance.

Ten slotte vermelden we nog dat een schending van het portretrecht, meer specifiek het zonder daartoe gerechtigd te zijn openbaar maken van een portret, ook een overtreding is waar een geldboete van de vierde categorie op staat, op basis van Art. 35 Aw. Dit betekent dat er naast een civielrechtelijke mogelijkheid tegen schending van het portretrecht in theorie ook een strafrechtelijke mogelijkheid bestaat, hoewel die in de praktijk zelden wordt toegepast (zie par. 5.4 over andere mogelijkheden binnen het strafrecht).

5.3.4 Deelconclusie en discussie: mogelijke lacunes en reguleringsmogelijkheden

Op basis van bovenstaande discussie bieden we hier een samenvatting van de geïdentificeerde mogelijke lacunes (antwoord op deelvraag 4) en bespreken we verder de mogelijkheden voor hun regulering (antwoord op deelvraag 8).

Het portretrecht is een juridisch instrument om inbreuken op de privacy van het beeld van een persoon (dus vooral lichamelijke privacy, maar ook gedragsmatige en relationele privacy) te beperken. Op basis van de rechtsverkenning die in deze subparagraaf is beschreven, concluderen we dat het mogelijke effect van dit recht op het beperken van de inbreuk op de persoonlijke levenssfeer beperkt is.

Zoals met betrekking tot privaatrecht en mogelijke lacunes (deelvraag 4), houdt de belangrijkste beperking voor het bereiken van deze bescherming in de praktijk verband met het feit dat het geen oplossing biedt in twee gevallen: (1) in het geval waarin de geportretteerden niet op de hoogte zijn van de inbreuk, en (2) in het geval waarin zij zich ervan bewust zijn (bijv. bij een vliegende hobbydrone), maar de eigenaar van de drone niet kunnen identificeren. Dit zijn echter veel voorkomende situaties. Wat betreft reguleringsmogelijkheden (deelvraag 8) voorzien wij niet dat veranderingen van het portretrecht tot een oplossing voor deze problemen zouden kunnen

[257] O.M.B.J. Volgenant, 'VII.8.9.1 Aanvullende bescherming van art. 6:162 BW', in C.J.J.M. Stolker (red.), *Groene Serie Onrechtmatige Daad*, Deventer: Wolters Kluwer.
[258] Rb. Gelderland 21 december 2016, ECLI:NL:RBGEL:2016:7155.

leiden. Daarbij zijn de twee soorten rechtsmiddelen die uit het portretrecht voortvloeien – zoals bij privaatrecht – monetair van aard: compensatie en boete. Dit kunnen soms geen bevredigende oplossingen bieden voor een vorm van inmenging die leidt tot niet-monetaire schade, vooral gezien de zeer lage bedragen (zie par. 5.2.1 (c)).

5.4 Strafrecht[259]

Het strafrecht vormt een belangrijk onderdeel van de normstelling in Nederland. De strafbaarstelling van bepaalde handelingen vormt als het ware de ondergrens van wat maatschappelijk aanvaardbaar handelen wordt geacht. Overschrijding van deze grens leidt niet alleen tot sancties, maar deze sancties hebben ook een punitief karakter, dat gepaard gaat met een moreel oordeel over het handelen. Een belangrijk verschil met het civiele recht is immers dat strafrechtelijke sancties niet alleen aangeven dat iemand onjuist heeft gehandeld, maar ook dat dit *moreel* onjuist gedrag betreft.

De belangrijkste strafbepalingen zijn te vinden in het commune strafrecht: het Wetboek van Strafrecht (Sr). Er zijn ook strafbepalingen in het bijzondere strafrecht, zoals de Opiumwet of de Wet op de economische delicten, maar daarin zijn geen bepalingen te vinden die van toepassing zijn op hobbydrones of spionageproducten in enge zin.[260] Het Wetboek van Strafrecht kent misdrijven (Tweede Boek) en overtredingen (Derde Boek). Bij misdrijven zou de onrechtmatigheid normaliter op voorhand voor iedereen duidelijk moeten zijn (‘onrecht vóór de wet’), terwijl bij overtredingen de onrechtmatigheid vooral door de strafbaarstelling zelf wordt bewerkstelligd (‘onrecht dóór de wet’).[261] Ook is bij overtredingen, in tegenstelling tot misdrijven, meestal niet expliciet opzet (dolus) of schuld (culpa) vereist; wie de handeling als omschreven pleegt, is in beginsel zonder meer strafbaar, tenzij een wettelijke strafuitzonderingsgrond (art. 39-43 Sr, bijvoorbeeld overmacht of noodweer) van toepassing is.[262]

De meeste misdrijven bevatten het element van ‘wederrechtelijkheid’. Dit is een algemene term die aanduidt dat de desbetreffende handeling alleen strafbaar is als deze plaatsvindt zonder toestemming of in strijd met een wettelijk voorschrift of met wat in het maatschappelijk verkeer betaamt; daarmee wordt voorkomen dat alledaagse handelingen (zoals het aanzetten van je

[259] Delen van deze paragraaf zijn ontleend aan het rapport van een parallel WODC-onderzoek naar gezichtsherkenning, Keymolen e.a., ‘Op het eerste gezicht: Een verkenning van gezichtsherkenning en privacyrisico’s in horizontale relaties”, WODC 2020.
[260] Hypothetisch kunnen sommige bijzondere strafbepalingen wel van toepassing zijn. Zo valt een killer-drone met een sensor voor automatische object- of persoonsherkenning onder de Wet wapens en munitie, omdat het in zo’n geval een hulpstuk van wezenlijke aard is voor het wapen (art. 3 lid 1 WWM). Zulke toepassingen laten wij buiten beschouwing omdat ze, zeker in horizontale relaties, te hypothetisch zijn.
[261] C.P.M. Cleiren e.a., *Tekst & Commentaar Strafrecht (Derde Boek)*, Deventer: Wolters Kluwer 2018, Inleidende opmerkingen, aantekening 1.
[262] Ibid., aantekening 2. In theorie kan iemand daarnaast ook een beroep doen op de buitenwettelijke uitzonderingsgrond ‘afwezigheid van alle schuld’, maar die wordt in de praktijk zelden erkend.

computer) onder een strafbaarstelling (zoals hacken: het opzettelijk *en wederrechtelijk* binnendringen in een computer, art. 138ab Sr) vallen.

De Nederlandse strafwet is van toepassing op strafbare feiten die in Nederland (art. 2 Sr) of aan boord van een Nederlands (lucht)vaartuig (art. 3 Sr) worden gepleegd. In sommige andere gevallen is de wet ook extraterritoriaal van toepassing (art. 4 t/m 8d Sr), maar de hieronder te behandelen bepalingen die relevant zijn voor spionageproducten vallen daar niet onder.[263]

Voor de interpretatie van de reikwijdte van strafbepalingen moet men voor ogen houden dat Nederland het opportuniteitsbeginsel hanteert: het Openbaar Ministerie bepaalt welke strafbare feiten worden vervolgd, en kan ook besluiten om van vervolging af te zien, onder andere op gronden van algemeen belang (art. 167 en 242 Sv). Het opportuniteitsbeginsel maakt het mogelijk om strafbepalingen enigszins ruim te formuleren, waardoor ook de nodige (relatief) triviale handelingen binnen de reikwijdte van de strafbaarstelling kunnen vallen, die dan normaliter niet zullen worden vervolgd. Zo valt het zonder toestemming opzettelijk verfrommelen van het boodschappenlijstje van iemand anders onder zaakbeschadiging, art. 350 Sr, maar dit zal niet tot vervolging en strafrechtelijke sanctionering leiden. Dit betekent dat, om te onderzoeken of bepaalde maatschappelijke onwenselijke gedragingen voldoende door het strafrecht worden bestreden, niet alleen naar de letter van de bepaling moet worden gekeken, maar ook naar de waarschijnlijkheid van strafvervolging.

Met deze algemene kenmerken van het strafrecht in gedachten, bespreken we in de volgende subparagrafen de strafrechtelijke bepalingen die mogelijk van toepassing zijn op spionageproducten en hobbydrones. Hiervoor hebben we gekeken naar de strafbepalingen die van toepassing zijn op computercriminaliteit,[264] omdat zowel hobbydrones als spionageproducten in enge zin gebaseerd zijn op computertechnologie. We bespreken daarvan de bepalingen die relevant zijn in het licht van de in dit rapport gesignaleerde privacyrisico's en de in hoofdstuk 4 gegeven voorbeelden van verschillende typen gebruik van spionageproducten. Achtereenvolgens behandelen we bepalingen betreffende visuele observatie (heimelijke observatie en seksuele afbeeldingen), auditieve observatie (afluisteren en opnemen van communicatie), heling van gegevens, en bepalingen die mogelijk van toepassing kunnen zijn op locatietracking.

---

[263] Wel is de wet ook van toepassing op Nederlanders (of vreemdelingen met een vaste woon- of verblijfplaats in Nederland) die in het buitenland misdrijven plegen die aldaar ook strafbaar zijn gesteld (art. 7 Sr), maar voor de analyse van de toepasbaarheid van strafbepalingen op spionageproducten is dat niet relevant.
[264] B.J. Koops & J.J. Oerlemans, 'Materieel strafrecht en ICT', in: Koops & Oerlemans (red.), *Strafrecht en ICT*, 3e druk, Den Haag: Sdu 2019, p. 29-116.

5.4.1 Heimelijke observatie

De meest voor de hand liggende bepalingen die van toepassing kunnen zijn op visuele observatie met hobbydrones of spionageproducten in enge zin, zijn de in 1971 ingevoerde (en nadien aangepaste) strafbaarstellingen van heimelijke visuele observatie in art. 139f en 441b Sr.[265]

Er zijn twee bepalingen die het heimelijk en wederrechtelijk maken van afbeeldingen van een persoon strafbaar stellen, de eerste in niet-publiek toegankelijke plaatsen (een misdrijf), de tweede in publiek toegankelijke plaatsen (een overtreding).

> **Artikel 139f Sr**
>
> Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie[266] wordt gestraft degene die, gebruik makende van een technisch hulpmiddel waarvan de aanwezigheid niet op duidelijke wijze kenbaar is gemaakt, opzettelijk en wederrechtelijk van een persoon, aanwezig in een woning of op een andere niet voor het publiek toegankelijke plaats, een afbeelding vervaardigt.

> **Artikel 441b Sr**
>
> Met hechtenis van ten hoogste twee maanden of geldboete van de derde categorie267 wordt gestraft hij die, gebruik makende van een daartoe aangebracht technisch hulpmiddel waarvan de aanwezigheid niet op duidelijke wijze kenbaar is gemaakt, van een persoon, aanwezig op een voor het publiek toegankelijke plaats, wederrechtelijk een afbeelding vervaardigt.

Hiermee wordt een duidelijk onderscheid gemaakt tussen het heimelijk observeren van personen in woningen en andere besloten plaatsen enerzijds en het heimelijk observeren van personen op publiek toegankelijke plaatsen anderzijds. Met niet voor het publiek toegankelijke plaatsen bedoelt de wetgever plaatsen waar niet een in beginsel onbeperkte groep toegang toe heeft; voorbeelden zijn hotelkamers, plaatsen die uitsluitend toegankelijk zijn voor leden van een vereniging of een bepaald gezelschap en kantoor- en bedrijfsruimten.[268] Een plaats is wel voor het publiek toegankelijk 'indien het feitelijk toegankelijk is voor een in beginsel onbeperkt aantal personen b.v. een restaurant, een museum.'[269] Binnen publiek toegankelijke plaatsen kunnen wel bepaalde deelruimten gelden als een besloten plaats; zo zal het heimelijk maken van

---

[265] Wet van 7 april 1971, houdende *enige strafbepalingen tot bescherming van de persoonlijke levenssfeer*, *Stb*. 1971, 180.
[266] Een geldboete van de vierde categorie is een boete van maximaal 21.750 € (art. 23 lid 4 Sr).
[267] Een geldboete van de derde categorie is een boete van maximaal 8.700 € (art. 23 lid 4 Sr).
[268] *Kamerstukken II* 1967/68, 9649, nr. 3, p. 4.
[269] Ibid.

afbeeldingen op een toilet in een restaurant of museum wel onder art. 139f Sr vallen,[270] evenals het heimelijk fotograferen of filmen van personen in een (afsluitbaar) omkleedhokje van een zwembad[271] of in pashokjes in een kledingzaak.[272]

Oorspronkelijk (bij de invoering in 1971) was art. 139f Sr beperkt tot woningen en niet voor het publiek toegankelijke *lokalen*, en art. 441b Sr was beperkt tot 'voor het publiek toegankelijke besloten ruimte[n], waarin spijzen, dranken of andere waren aan particulieren worden geleverd'; het ging dus om bepaalde ruimten met beperkte zichtbaarheid en niet om de openbare ruimte. In 2003[273] werd de strafbaarstelling echter uitgebreid tot alle voor het publiek toegankelijke plaatsen, waaronder ook de openbare weg, omdat het recht op privacybescherming 'thans ruimer [wordt] uitgelegd dan ten tijde van de totstandkoming van de artikelen 441b en 139f Sr. Ook op voor het publiek toegankelijke plaatsen kan onder omstandigheden sprake zijn van een aantasting van de persoonlijke levenssfeer.'[274] Dat komt mede door 'de toename van het gebruik van camera's voor toezicht en beveiliging ook op andere plaatsen dan in winkels of horecagelegenheden, zoals bijvoorbeeld op stations, in uitgaansgebieden, in het openbaar vervoer, in banken en casino's.'[275]

Niettemin bestaat er nog steeds een duidelijk verschil in normstelling tussen heimelijke observatie in besloten en niet-besloten plaatsen. Dit heeft vooral te maken met het verschil in redelijke privacyverwachting: in woningen en andere besloten plaatsen voelt men zich veelal vrijer om onbevangen zichzelf te zijn, in de wetenschap niet zichtbaar te zijn voor het algemene publiek. Niettemin geeft de strafbaarstelling van art. 441b Sr aan dat men ook in niet-besloten plaatsen een zekere privacyverwachting mag koesteren: weliswaar moet men er (vanzelfsprekend) rekening mee houden dat men zichtbaar is, maar men hoeft er geen rekening mee te houden dat anderen je zo maar mogen fotograferen of filmen. De **heimelijkheid** van de (technische) observatie speelt daarbij een cruciale rol: de strafbaarstelling geldt voor technische hulpmiddelen waarvan de aanwezigheid niet duidelijk kenbaar is gemaakt.

De nadruk op heimelijkheid blijkt ook uit een andere aanpassing in de wetsgeschiedenis van art. 139f en 441b Sr. Aanvankelijk, in 1971, was de strafbaarstelling van art. 139f Sr beperkt tot gevallen waarin de fotograaf of filmer gebruik maakt 'van een door een list of een kunstgreep daartoe geschapen gelegenheid' om een afbeelding van iemand te maken 'waardoor diens rechtmatig belang kan worden geschaad' (art. 139f Sr-oud). Daarbij dacht de wetgever vooral

---

[270] Rb. Almelo 16 augustus 2011, ECLI:NL:RBALM:2011:BR5076 (in casu ging het om een toilet in een kapperszaak).
[271] HR 14 februari 2012, ECLI:NL:HR:2012:BU5254. Het Hof overwoog in deze casus: '[d]oor het kleedhokje af te sluiten, maakte aangeefster duidelijk zich in afzondering en buiten het gezichtsveld van derden te willen aan- en uitkleden.'
[272] *Kamerstukken II* 2000/01, 27 732, nr. 3, p. 13.
[273] *Stb.* 2003, 198.
[274] *Kamerstukken II* 2000/01, 27 732, nr. 3, p. 3.
[275] *Kamerstukken II* 2000/01, 27 732, nr. 3, p. 5.

aan ‘candid camera’-gevallen, oftewel ‘een speciaal daartoe gecreëerde situatie, welke in het bijzonder door de afgebeelde persoon als zodanig redelijkerwijs niet kan worden onderkend’.[276] Daarbij moest bovendien de gefotografeerde in een rechtmatig belang zijn geschaad, omdat anders ‘te veel gevallen onder de strafbepaling vallen die niet strafwaardig zijn te achten. Het gebeurt vaak dat men door op onverwachte wijze een foto te maken een meer ongedwongen afbeelding hoopt te verkrijgen, zonder dat daardoor enig belang van de gefotografeerde wordt geschaad.’[277] Alleen gevallen waarin iemand door de foto in een rechtmatig belang was geschaad, werden dus strafwaardig geacht.

Bij de wetswijziging in 2003 gaf de wetgever echter blijk van een gewijzigd inzicht. Art. 441b Sr kende geen bestanddeel dat de afgebeelde in een rechtmatig belang was geschaad, en het was onwenselijk dat art. 441b in dat opzicht meer rechtsbescherming zou bieden dan art. 139f Sr. Daarbij ging het volgens de wetgever niet meer om de **aard** van de afbeelding om te bepalen of het fotograferen strafwaardig was.

> Dit strookt niet meer met de huidige opvattingen omtrent de bescherming van de persoonlijke levenssfeer. Immers ongeacht de aard van de afbeelding moet het met een daartoe aangebracht technische hulpmiddel heimelijk vervaardigen van een afbeelding van een persoon op een voor het publiek toegankelijke plaats als strafwaardig worden aangemerkt. Datzelfde dient ook, of misschien wel in versterkte mate, te gelden voor woningen en andere niet voor het publiek toegankelijke plaatsen.[278]

Hieruit blijkt duidelijk dat de wetgever het gebruik maken van (vaste of verborgen) camera’s om heimelijk afbeeldingen van iemand te maken, strafwaardig acht, ongeacht hoe de persoon is afgebeeld en ongeacht wat de mogelijke gevolgen voor de afgebeelde persoon kunnen zijn. De **heimelijkheid** van deze vorm van observatie staat daarbij dus voorop, niet **wat** er precies wordt geobserveerd of vastgelegd.

De strafbaarstelling is voorts beperkt tot het maken van afbeeldingen met een technisch hulpmiddel, zoals (foto- of film)camera’s; tekeningen met een potlood of stift vallen daar niet onder, ‘omdat zij de uiterlijke schijn van authenticiteit ontberen.’[279] Daarbij is van belang dat de afbeeldingen niet per se hoeven te worden **vastgelegd**. Hoewel de strafbaarstelling primair bedoeld is om tegen te gaan dat zonder toestemming afbeeldingen van personen worden gemaakt die vervolgens een eigen leven kunnen gaan leiden als een exacte weergave van die persoon op een bepaalde plaats en tijd, valt ook het in *real time* doorgeven van afbeeldingen

---

[276] *Kamerstukken II* 1967/68, 9649, nr. 3, p. 5.
[277] *Kamerstukken II* 1969/70, 9649, nr. 8, p. 5.
[278] *Kamerstukken II* 2000/01, 27 732, nr. 5, p. 2.
[279] *Kamerstukken II* 1967/68, 9649, nr. 3, p. 4.

zonder vastlegging eronder.[280] Dit betekent dat het gebruik van camera's met *live streaming* van beelden ook onder de strafbaarstelling valt, voor zover de aanwezigheid van de camera's niet duidelijk kenbaar is gemaakt. Dat is bijvoorbeeld het geval bij webcams die verstopt zijn in een kast in een AirBNB-appartement.

Voor spionageproducten in enge zin en hobbydrones met een functionaliteit voor visuele observatie betekent dit alles dat het maken van afbeeldingen hiermee veelal strafbaar zal zijn, tenzij de aanwezigheid van die camera duidelijk kenbaar is gemaakt. Wel zijn er uitzonderingen in gevallen waarin heimelijke observatie niet wederrechtelijk wordt geacht, bijvoorbeeld als een journalist heimelijk beelden maakt om een publieke misstand aan de kaak te stellen[281]. In het algemeen zullen genoemde strafbepalingen een belangrijk deel van de maatschappelijk onwenselijke vormen van het gebruik van spionageproducten in enge zin en hobbydrones voor visuele observatie kunnen afdekken, omdat dit vaak heimelijk zal gebeuren. Voor hobbydrones is daarbij belangrijk dat ook het gebruik van een heimelijke camera om live beelden te bekijken, zonder afbeeldingen op te slaan, gezien de wetsgeschiedenis onder de strafbaarstelling valt.

Niettemin zijn er toch enkele mogelijke belemmeringen bij de toepassing van deze bepalingen, die we in onderstaande subparagrafen bespreken.

Voorbereiding van inbraak

Uit de verkenning van de privacyrisico's van hobbydrones blijkt dat één van de mogelijke toepassingen is het voorverkennen voor een inbraak (zie par. **Error! Reference source not found.**), wat een inbreuk op de ruimtelijke privacy oplevert. Dat zal meestal niet onder de strafbaarstelling van heimelijke observatie vallen, omdat het gaat om het maken van afbeeldingen (of het *live* bekijken van doorgegeven beelden) van *objecten* (een huis, schuur, opslagloods, etc.) en niet van een persoon. Voorverkennen voor een inbraak zou wel onder strafbare voorbereiding kunnen vallen. Artikel 46 Sr bevat een algemene strafbaarstelling van voorbereidingshandelingen, waaronder het voorhanden hebben van voorwerpen of informatiedragers bestemd tot het begaan van het misdrijf. Strafbare voorbereiding is echter beperkt tot misdrijven met een maximumgevangenisstraf van ten minste acht jaar. Een inbraak 's nachts of door twee of meer verenigde personen kent een maximumstraf van negen jaar (art. 311 lid 2 Sr). Op een 'simpele' inbraak in een woning (door één persoon overdag, als de inbreker binnenkomt zonder braak, inklimming of misleiding) of een inbraak in een schuur of loods (die niet op het erf van een woning staat) staat echter maximaal zes jaar gevangenisstraf (art. 311 lid 1 Sr). Bij een voorverkenning met een drone – die bijvoorbeeld erop gericht kan zijn te zien of een deur open staat – is het misschien moeilijk te bewijzen of iemands opzet gericht is het

[280] Fokkens, Noyon/Langemeijer/Remmelink Strafrecht, commentaar op 139f Sr, aant. 2. Zie bijv. Rb. Gelderland 29 augustus 2016, ECLI:NL:RBGEL:2016:4801: het *live* uitkijken van webcambeelden moet worden aangemerkt als het vervaardigen van afbeeldingen in de zin van art. 139f Sr.
[281] Vgl. *Kamerstukken II* 2000/01, 27 732, nr. 5, p. 13.

plegen van een diefstal zoals genoemd in lid 1 of zoals genoemd in lid 2; in het eerste geval is de voorbereiding niet strafbaar, in het tweede geval wel. Ook het element 'bestemd tot het begaan van dat misdrijf' levert mogelijk bewijsproblemen op, aangezien een drone multifunctioneel is, en het niet altijd eenduidig bewijsbaar zal zijn dat het rondvliegen in de buurt van een huis of opslagloods bestemd is om een diefstal voor te bereiden.

Met betrekking tot deelvraag 4, kunnen we hier dus een mogelijke lacune vaststellen, aangezien het strafrecht heimelijke observatie van objecten met het oog op de voorbereiding op bepaalde misdrijven niet strafbaar stelt. Op basis van deze verkennende studie kunnen we niet inschatten hoe groot het probleem van inbraakvoorbereiding met drones is; daarvoor zou nader onderzoek nodig zijn. Met betrekking tot deelvraag 8 en reguleringsmogelijkheden, mocht blijken dat dit fenomeen vaak genoeg voorkomt om tot strafrechtelijke aanpak te nopen, dan zou de wetgever kunnen overwegen om aan de strafbaarstelling van heimelijke observatie een lid toe te voegen dat specifiek ziet op het observeren van objecten (in plaats van personen) met het oogmerk bepaalde misdrijven voor te bereiden.

Draagbare camera's

Een eerste punt is dat de strafbaarstellingen spreken van een technisch hulpmiddel 'waarvan de aanwezigheid niet op duidelijke wijze kenbaar is gemaakt'. Dit roept de nodige vragen op in relatie tot toepassingen van spionage met mobiele camera's, waaronder hobbydrone-camera's. Hoewel dit rapport focust op spionageproducten in enge zin en hobbydrones, moeten we op dit punt ook enige aandacht besteden aan spionageproducten in brede zin, vanwege de wenselijkheid van consistentie in beleid en regelgeving. Het zou immers weinig zin hebben om specifieke regels te stellen voor het maken van afbeeldingen met hobbydrones ter bescherming van privacy, als dezelfde of grotendeels vergelijkbare privacyrisico's optreden bij andere spionageproducten in brede zin, zoals smartphones, terwijl daarop heel andere regels van toepassing zouden zijn. Om die reden gaan we hier eerst in op draagbare camera's, alvorens we nader inzoomen op hobbydrone-camera's.

Als observatie plaatsvindt met een camera die wel zichtbaar aanwezig is, zijn de bepalingen niet van toepassing. Zo heeft de minister toegelicht dat het maken van beelden voor infotainment-programma's niet onder de strafbaarstelling valt, omdat het niet heimelijk plaatsvindt; immers, '[i]n het geval van reality tv-programma's wordt openlijk met een camera op de schouder (…) gefilmd.'[282] Nu is een tv-filmcamera iets prominenter en zichtbaarder dan een smartphone-camera, maar in het huidige tijdsgewricht zal men zich ervan bewust moeten zijn dat smartphones camera's bevatten, zodat bezwaarlijk kan worden gezegd dat een smartphone-camera niet duidelijk aanwezig is als men een smartphone ziet. Dat ligt natuurlijk anders als de

[282] *Kamerstukken II* 2000/01, 27 732, nr. 5, p. 12-13.

smartphone verstopt is, bijvoorbeeld in een shampoo-fles in een doucheruimte, om heimelijk beelden te maken (in welk geval de lichamelijke privacy kan worden geschaad).[283] In het laatste geval is de smartphone, en dus ook de camera, niet duidelijk aanwezig.

Dit hangt samen met een volgende beperking: in publiek toegankelijke plaatsen is de strafbaarstelling beperkt tot '*een daartoe aangebracht* technisch hulpmiddel waarvan de aanwezigheid niet op duidelijke wijze kenbaar is gemaakt' (art. 441 Sr, cursivering toegevoegd). De camera moet dus zijn *aangebracht* voor het doel van het fotograferen of filmen van mensen, die in de eerste plaats inbreuk kan maken op de gedragsmatige en relationele privacy. Het gaat daarbij om 'in beginsel een enigszins permanente installatie'.[284] De strafbaarstelling is dus in beginsel beperkt tot vaste en enigszins duurzaam gemonteerde camera's, zoals CCTV-bewakingscamera's op publiek toegankelijke plaatsen.[285] Onder omstandigheden kunnen ook mobiele camera's eronder vallen, maar alleen

> [w]anneer een extra handeling is verricht met de handcamera waardoor diens aanwezigheid niet meer duidelijk kenbaar is – deze is bijvoorbeeld verstopt in een voorwerp of voertuig – dan is ook sprake van een «daartoe aangebracht technisch hulpmiddel». Ook in dat geval kan het vervaardigen van een afbeelding van een persoon een strafbaar feit opleveren. Is echter niets extra ondernomen met de handcamera en wordt deze gewoon door een persoon uit de hand bediend dan is artikel 441b Sr niet van toepassing.'[286]

Hieruit blijkt dat de wetgever wel voorzien heeft dat foto- of filmcamera's verstopt worden in andere voorwerpen, en dat ook verstopte camera's (die al dan niet zijn ingebed in een ander product) onder de strafbaarstelling vallen. Echter, smartphone-camera's stonden in 2001 nog niet op het netvlies van de wetgever. Het gaat hier om producten waarin een camera-functionaliteit is ingebouwd op een manier dat de aanwezigheid van de camera-functionaliteit kenbaar is; naar algemene bekendheid hebben moderne smartphones immers allemaal een camera. De wetsgeschiedenis suggereert dat het maken van afbeeldingen met smartphone-camera's niet onder art. 441 Sr valt zolang de smartphone gewoon in de hand wordt gehouden; er wordt dan immers geen extra handeling verricht om de aanwezigheid ervan te verbergen. Alleen als de smartphone (of een smartwatch of ander apparaat met camera-functionaliteit) verstopt is, bijvoorbeeld in een tas of kleding, kan de strafbaarstelling van toepassing zijn. Dit impliceert een mogelijke lacune in de wet (deelvraag 4).

---

[283] Vgl. 'Naakte meisjes filmen met een shampoofles', *NRC* 11 maart 2019.
[284] *Kamerstukken II* 2000/01, 27 732, nr. 5, p. 11.
[285] Machielse, Noyon/Langemeijer/Remmelink Strafrecht, commentaar op 441b Sr, aantekening 2.
[286] *Kamerstukken II* 2000/01, 27 732, nr. 5, p. 10.

Het probleem hierbij is dat de smartphone niet hetzelfde functioneert in het maatschappelijk verkeer als een foto- of filmcamera. Wie over straat loopt en iemand ziet met een camera, zal zich bewust moeten zijn van de mogelijkheid dat de ander een afbeelding maakt met deze camera. Dat is ook een handeling die men veelal zal zien aankomen (de camera wordt opgetild en gericht), wat iemand de (soms theoretische maar niet verwaarloosbare) mogelijkheid biedt om bezwaar te maken (bijvoorbeeld door de hand voor de camera te houden of zich af te wenden) en aldus duidelijk te maken dat men niet wil worden gefotografeerd. Dit werkt anders bij smartphones, omdat men zich weliswaar bewust is van de aanwezigheid van camera's bij anderen die een smartphone in de hand houden, maar daarbij niet weet of die smartphone gebruikt wordt als camera of voor een van de vele andere functionaliteiten van de smartphone. Anders dan bij camera's is het vaak ook moeilijk(er) te zien of een smartphone-camera op jou is gericht, zodat je je minder dan bij camera's bewust bent van het feit dat iemand een foto of filmpje aan het maken is. Zelfs als een smartphone duidelijk naar voren is gericht, weet je nog niet of op dat moment een foto van je wordt gemaakt of dat de smartphone-eigenaar een selfie maakt of in de spiegel-app kijkt of zijn haar nog goed zit – de camera kan immers in twee richtingen werken. Een smartphonecamera *fungeert* in die zin van nature een stuk heimelijker dan een foto- of filmcamera, ook al is de *aanwezigheid* ervan in beginsel kenbaar.

Vanuit dat perspectief valt er iets voor te zeggen om ook smartphonecamera's te interpreteren als aangebrachte camera's waarvan de aanwezigheid niet op duidelijke wijze kenbaar is gemaakt, door een teleologische interpretatie van het element aanwezigheid. Een dergelijke brede interpretatie van de relevante bepaling(en) (zonder dat deze hoeven te worden gewijzigd) zou een mogelijke oplossing bieden voor de privacyrisico's die voortvloeien uit een dergelijk gebruik van smartphones als een soort spionageproduct in brede zin (deelvraag 8).

Een bijkomend argument voor zo'n interpretatie is de schaal waarop handcamera's respectievelijk smartphones aanwezig zijn in het maatschappelijk verkeer. Hoewel handcamera's in het begin van deze eeuw veelvuldig voorkwamen, waren ze nog steeds relatieve uitzonderingen; behalve op toeristische plaatsen kon men zich veelal door de openbare ruimte bewegen zonder al te veel mensen met camera's in de aanslag tegen te komen. Dat maakte het ook maatschappelijk aanvaardbaar om de relatief niet al te vaak voorkomende gevallen waarin met handcamera's heimelijk snapshots van mensen werden gemaakt, als ongemak te beschouwen waarmee burgers maar moeten leren leven. (Voor de gevallen waarin zulke beelden vervolgens in de openbaarheid werden gebracht, kon – en kan – het portretrecht nog soms rechtsbescherming bieden. Zie par. 5.3.) In het huidige tijdperk zijn smartphones echter alomtegenwoordig en is het nauwelijks mogelijk (behalve misschien op afgelegen plaatsen op nachtelijke tijdstippen) om zich door de openbare ruimte te bewegen zonder op enig moment in de nabijheid van iemand met een smartphone te zijn. Waar men bij handcamera's nog kon stellen dat burgers er maar verdacht op moesten zijn dat anderen hun konden fotograferen of

filmen, en in voorkomende gevallen hun gedrag moesten aanpassen om ongewenste afbeeldingen te voorkomen, valt dat in het smartphonetijdperk niet meer vol te houden; de enige effectieve gedragsaanpassing om te voorkomen dat je mogelijk door iemand gefotografeerd of gefilmd wordt, is thuis te blijven. Dit argument komt echter neer op een permanent vrijwillig huisarrest voor mensen die niet het risico willen lopen ergens te worden gefotografeerd. De gewijzigde omstandigheden bieden goede argumenten om de strafbepalingen zodanig te interpreteren dat er bij smartphones, anders dan bij handcamera's, sprake is van een aangebrachte camera waarvan de aanwezigheid niet duidelijk is kenbaar gemaakt.

Een aanvullend argument daarvoor biedt nog de wetswijziging uit 2003, waarbij heimelijke observatie strafbaar werd geacht ongeacht de mogelijke gevolgen voor de afgebeelde persoon; de *heimelijkheid* van deze vorm van observatie staat immers voorop, niet *wat* er precies wordt geobserveerd of vastgelegd. De redeneerlijn van de wetgever volgend, valt er iets voor te zeggen dat het maken van afbeeldingen met smartphones onder de strafbepalingen valt, tenzij de persoon die de smartphone hanteert heel duidelijk heeft gemaakt dat zij op dat moment de camerafunctionaliteit van de smartphone gebruikt of wil gaan gebruiken. Ook hier gaat het immers om een belemmering van de vrijheid om onbevangen zichzelf te kunnen zijn, in beslotenheid, in gezelschap of op de openbare weg (en dus met betrekking tot ruimtelijke, gedragsmatige en relationele privacy).

Vanuit het perspectief van burgers die liever niet door anderen willen worden gefotografeerd – om wat voor reden dan ook – valt er om bovengenoemde redenen dus het nodige te zeggen om de strafbaarstelling van heimelijke observatie ook, in elk geval in beginsel, van toepassing te laten zijn op het gebruik van smartphones om anderen te fotograferen of filmen zonder het duidelijk vooraf kenbaar maken dat de camera in de smartphone gebruikt gaat worden.

Vanuit het perspectief van smartphonegebruikers leidt dat echter wel tot een zeer (en vermoedelijk te) ruime reikwijdte van de strafbepalingen. Het argument van schaal kan immers ook de andere kant op worden gebruikt: zoals het in het begin van de eeuw een relatieve uitzondering was om foto's te nemen van andere personen, worden tegenwoordig veel meer foto's en filmpjes gemaakt, in veel meer situaties dan de aloude toeristische omstandigheden waarvoor handcamera's dienden. Voor burgers die hun smartphone gebruiken om de nodige foto's of filmpjes te maken van wat zij op een dag zoals zien of meemaken, zou het een grote inperking van de gebruiksvrijheid zijn als de afbeeldingen strafbaar worden geacht zodra er een andere persoon (zonder diens expliciete of impliciete toestemming) op staat. Er lijkt ons momenteel geen maatschappelijke norm te bestaan om bij het maken van afbeeldingen met de smartphone eerst aan omstanders duidelijk kenbaar te maken dat men de camerafunctionaliteit van de smartphone gaat gebruiken, om de omstanders de gelegenheid te geven om bezwaar te maken of zich af te wenden. Zo'n norm wordt echter wel verondersteld indien we de strafbaarstelling van heimelijke observatie zouden interpreteren in de zin dat ook smartphones

aangebrachte camera's zijn waarvan de aanwezigheid niet duidelijk is kenbaar gemaakt. Dit betekent onzes inziens dat een dergelijke interpretatie, naar huidig recht, te ver gaat.

Dat wil echter niet zeggen dat smartphonecamera's – of soortgelijke apparaten met een camerafunctionaliteit – onproblematisch zijn. De alomtegenwoordigheid van camera's maakt het meer dan ooit mogelijk dat in vrijwel elke situatie ter plekke een afbeelding kan worden gemaakt. Dat heeft positieve kanten – denk aan het filmen van geweldplegers door omstanders – maar ook negatieve kanten, bijvoorbeeld bij het sensatiebelust fotograferen van slachtoffers van verkeersongevallen.

Met betrekking tot reguleringsmogelijkheden (deelvraag 8), zou wellicht bij het beoordelen van strafwaardigheid van visuele observatie in het huidige tijdperk de nadruk niet langer alleen moeten liggen op de *heimelijkheid* ervan, maar zouden ook andere omstandigheden moeten worden meegewogen wanneer de observatie openlijk gebeurt. Dat kan bijvoorbeeld bepaalde omstandigheden betreffen waarin de afgebeelde persoon zich bevindt of de plaats waar de afbeelding wordt gemaakt (bijvoorbeeld de wachtkamer of hal van een abortus- of geslachtsziektenkliniek). We concluderen dat er voldoende aanleiding voor de wetgever is om de huidige vormgeving van de strafbaarstelling van heimelijke observatie te heroverwegen in het licht van de alomtegenwoordigheid van draagbare camera's.[287] De vraag is onder welke omstandigheden burgers in het huidige tijdperk zich voldoende vrij zouden moeten kunnen voelen van observatie door anderen; en die vraag is breder dan alleen situaties waarin observatie plaatsvindt met heimelijk aangebrachte camera's. Factoren die bij deze vraag een rol spelen zijn onder andere of er plaatsen en contexten zijn in de (semi-)openbare ruimte waarin mensen (meer dan bij andere plaatsen of contexten) onbevangen zichzelf moeten kunnen zijn, de mate van kenbaarheid dat anderen afbeeldingen van je maken, het gebruik van dergelijke afbeeldingen, en de mogelijkheden die mensen hebben om te voorkomen dat zij ongewenst worden gefotografeerd of gefilmd.

Drone-camera's

Voor met een camera uitgeruste hobbydrones geldt deels dezelfde argumentatie als we hierboven voor draagbare camera's hebben gegeven; ongeacht de kenbaarheid van de aanwezigheid van de camera, zal het vaak niet duidelijk zijn voor iemand of de drone op dat moment afbeeldingen aan het maken is van hem of haar. De onzekerheid die dat voor burgers met zich meebrengt, en de moeilijkheid om hun gedrag dienovereenkomstig aan te passen als ze niet willen worden afgebeeld, zijn argumenten om het maken van afbeeldingen wel strafwaardig te achten. (Zie bijvoorbeeld de gevoelens van onmacht en frustratie die de

[287] Vgl. ook Bert-Jaap Koops, Bryce Clayton Newell, Andrew Roberts, Ivan Škorvánek, en Maša Galič (2018), 'The reasonableness of remaining unobserved. A comparative analysis of visual surveillance and voyeurism in criminal law', *Law & Social Inquiry* 2018, p. 24.

Kinderdijk-bewoners ervaren, zie 4.2.1). Tegelijkertijd levert het een aanzienlijke inperking op van de handelingsvrijheid van burgers als zij nooit foto's of filmpjes kunnen maken van anderen met hun hobbydrone. Op plaatsen waar met drones mag worden gevlogen gaat het immers lang niet altijd om woonhuizen en tuinen die de volledig private of intieme zone van het leven uitmaken, zoals bij Kinderdijk, maar om de publieke zone van het leven waar mensen vaak meer toevallige voorbijgangers zullen zijn. Ook hier lijkt ons een maatschappelijk en politiek debat nodig om deze twee kanten van de medaille tegen elkaar af te wegen.

Een mogelijk verschil is dat bij een drone, anders dan bij smartphones, het niet altijd duidelijk zal zijn of deze is uitgerust met een camera. Bij smartphones mag men daarvan uitgaan; bij drones zal het kunnen afhangen van het type, en mogelijk de omstandigheden, of men kan of zou moeten verwachten dat deze een camera dragen. Het ministerie van (destijds) Veiligheid en Justitie stelde echter in 2015 het volgende:

> Een redelijke wetsuitleg brengt mee dat onder "niet op duidelijke wijze kenbaar gemaakt" ingeval van drones moet worden verstaan: een zodanig gebruik van een drone dat deze redelijkerwijs niet waarneembaar is. Als een drone wel waarneembaar is, dient men ermee rekening te houden dat deze een camera als "payload" meevoert en is van heimelijkheid dus geen sprake.[288]

Hoewel deze wetsuitleg niet nader wordt toegelicht, vermoeden wij dat de aanname eraan ten grondslag ligt dat veel drones een camera als payload hebben en dat burgers zich daarvan bewust zullen (moeten) zijn. Of burgers zich daadwerkelijk bewust zijn van de mogelijkheid dat elke zichtbare drone een camera heeft, valt binnen het bestek van dit onderzoek niet te beantwoorden. Hoewel een wetsinterpretatie van het ministerie niet per se doorslaggevend is, kan deze wel richtinggevend zijn (bij gebrek aan andere gezaghebbende interpretaties), zodat wij voor dit onderzoek hierbij zullen aansluiten.

Evenals bij andere mobiele camera's wil dat echter niet zeggen dat drone-camera's daarmee onproblematisch zijn. Ook als we ervan uitgaan dat de aanwezigheid van de camera kenbaar gemaakt is en het fotograferen niet heimelijk gebeurt, lijkt ons het maken van afbeeldingen potentieel strafwaardig, met name omdat er nauwelijks mogelijkheden zijn voor mensen om ongewenste afbeeldingen te voorkomen. Vooral op niet-publiek toegankelijke plaatsen, zoals in en rondom de woning, zou het een ingrijpende aantasting van de ruimtelijke en gedragsmatige privacy zijn als mensen weg zouden moeten gaan of hun gedrag zouden moeten aanpassen vanwege de komst van een drone met een kenbare camera. Het zou niet nodig moeten zijn voor Kinderdijkbewoners om naar binnen te gaan als er drones in de buurt vliegen, en dan ook nog de gordijnen te moeten dichtdoen omdat drones voor het raam hangen. Maar ook op publiek

---

[288] *Drones en privacy. Handleiding voor een gebruik van drones dat voldoet aan de waarborgen voor bescherming van de privacy*, Bijlage bij *Kamerstukken II* 2015/16, 30806, nr. 34, p. 15.

toegankelijke plaatsen, zoals een wandel- of fietsgebied, is het onwenselijk als mensen hun gedrag substantieel zouden moeten aanpassen (bijvoorbeeld afwijken van de route om een drone te ontwijken, of continu omlaag kijken om niet met het gezicht in beeld te komen).

Bovendien is het niet goed mogelijk om bezwaar te maken. Bij hand- en smartphonecamera's kun je, als je ziet of vermoedt dat iemand een foto van je wil maken, nog duidelijk aangeven dat je dit niet wilt, bijvoorbeeld door met een handgebaar of hoofdschudden 'nee' te zeggen. Je ziet dan meestal of de persoon die een afbeelding wilde gaan maken, daarvan afziet; en mocht deze doorgaan, dan kun je in principe nog naar de persoon toestappen en vragen of deze de afbeelding wil verwijderen. Bij drones kun je wel wuiven of nee schudden, maar je hebt geen idee of degene die de drone bedient dat signaal oppakt; evenmin kun je naar de drone-bestuurder toestappen om verwijdering van eventuele afbeeldingen te eisen. Alleen in gevallen waarin de dronebestuurders zichtbaar in de buurt zijn en je hen direct kunt benaderen, zoals bij Kinderdijk wel voorkomt, is er een reële mogelijkheid om bezwaar te maken; maar die mogelijkheid is niet heel laagdrempelig en heeft soms maar niet altijd succes, zoals uit de casus blijkt.

Wij concluderen dat de strafbaarstelling van heimelijke observatie mogelijke lacunes kent in het licht van alomtegenwoordige draagbare camera's en ten aanzien van drone-camera's (deelvraag 4). Omdat burgers zich nauwelijks kunnen verweren tegen ongewenste afbeeldingen met draagbare of drone-camera's waarvan de aanwezigheid kenbaar is, moeten er duidelijke grenzen worden gesteld aan het maken van afbeeldingen met zulke camera's. Waar die grenzen precies moeten liggen en hoe deze moeten worden bewaakt is een politieke keuze die op basis van een geïnformeerd politiek en maatschappelijk debat moet worden gemaakt.

5.4.2 Seksuele afbeeldingen en wraakporno

Visuele observatie vormt in het bijzonder een risico voor de lichamelijke en beslissingsprivacy, wanneer het afbeeldingen van naaktheid of seksuele handelingen betreft. In januari 2020 is een wet in werking getreden die de strafbaarstelling van heimelijke observatie aanvult, voor zover het gaat om afbeeldingen van seksuele aard.[289]

> **Artikel 139h Sr**
> 1. Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt gestraft:
> a. hij die opzettelijk en wederrechtelijk van een persoon een afbeelding van seksuele aard vervaardigt;

[289] Wet herwaardering strafbaarstelling actuele delictsvormen (*Stb.* 2019, 311), inwerkingtreding 1 januari 2020 (*Stb.* 2019, 421).

b. hij die de beschikking heeft over een afbeelding als bedoeld onder a terwijl hij weet of redelijkerwijs moet vermoeden dat deze door of als gevolg van een onder a strafbaar gestelde handeling is verkregen.

2. Met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie wordt gestraft:

a. hij die een afbeelding als bedoeld in het eerste lid, onder a, openbaar maakt terwijl hij weet of redelijkerwijs moet vermoeden dat deze door of als gevolg van een in het eerste lid, onder a, strafbaar gestelde handeling is verkregen;

b. hij die van een persoon een afbeelding van seksuele aard openbaar maakt, terwijl hij weet dat die openbaarmaking nadelig voor die persoon kan zijn.

Aldus stelt lid 1 strafbaar het opzettelijk en wederrechtelijk maken van een afbeelding van seksuele aard, bijvoorbeeld *upskirt*-foto's en de heling van zulke afbeeldingen, terwijl lid 2 de openbaarmaking van aldus gemaakte foto's strafbaar stelt met een hogere straf. In lid 2 is ook in meer algemene zin wraakporno strafbaar gesteld, ook in gevallen waarin de afbeelding met toestemming is gemaakt, bijvoorbeeld naaktfoto's gemaakt in een affectieve relatie die na het verbreken van deze relatie openbaar worden gemaakt.

Voor hobbydrones en spionageproducten in enge zin is vooral het eerste lid van belang. Een afbeelding van seksuele aard is 'een afbeelding die een zodanig intiem seksueel karakter heeft dat deze door ieder redelijk denkend mens als privé zal worden beschouwd.'[290] Zulke afbeeldingen zullen veelal alleen heimelijk worden gemaakt, bijvoorbeeld op naaktstranden, in sauna's of in nudistengebieden waar het openlijk gebruik van camera's vaak gelimiteerd of überhaupt niet geaccepteerd wordt, zodat de strafbaarstelling van heimelijke observatie daar normaliter al van toepassing is. Omdat er echter enige discussie mogelijk is of draagbare camera's wel vallen onder een '*daartoe aangebracht* technisch hulpmiddel waarvan de aanwezigheid niet op duidelijke wijze kenbaar is gemaakt' (art. 441b Sr, onze cursivering; zie par. 5.4.1), biedt artikel 139h Sr een belangrijk vangnet. De in een shampoofles verstopte camera in een doucheruimte zal sowieso onder de strafbaarstelling van heimelijke observatie vallen, maar iemand die in een doucheruimte op zijn smartphone lijkt te kijken maar daarbij stiekem een foto probeert te maken van een ander, valt wellicht niet onder die strafbaarstelling. Daarvoor biedt artikel 139h Sr dus een vangnet. Belangrijk daarbij is ook de hogere strafmaat: een gezamenlijke doucheruimte en de gezamenlijke gedeeltes van omkleedruimtes in gymzalen of zwembaden zijn, anders dan afsluitbare pashokjes, meestal een publiek toegankelijke ruimte (tenzij het bijvoorbeeld een interne douche- of fitnessruimte van een bedrijf betreft), zodat het maken van afbeeldingen aldaar onder artikel 441b Sr valt, met een relatief lage strafmaat van

[290] *Kamerstukken II* 2018/19, 35 080, nr. 3, p. 22.

maximaal twee maanden gevangenisstraf. Voor dergelijke gezamenlijke ruimtes waarin mensen zich (gedeeltelijk) blootgeven, biedt artikel 139h Sr dus een belangrijke aanvullende bescherming tegen heimelijk gemaakte afbeeldingen.

5.4.3 Afluisteren en opnemen van communicatie

Zoals blijkt uit onze quickscan met betrekking tot de meest voorkomende soorten spionageproducten in enge zin die beschikbaar zijn voor de burgers (zie 3.3), is naast visuele observatie auditieve observatie een belangrijke vorm van spionage, die in de eerste plaats inbreuk kan maken op de communicatieve privacy. De wetgever heeft het wederrechtelijk afluisteren van gesprekken of andere communicatie strafbaar gesteld.

Gesprekken

Bij het afluisteren van gesprekken wordt evenals bij heimelijke visuele observatie een normatief onderscheid gemaakt tussen bepaalde besloten en niet-besloten plaatsen. Het ‘direct afluisteren’ of opnemen van gesprekken die in een besloten sfeer plaatsvinden is strafbaar gesteld in artikel 139aSr.

> **Artikel 139a Sr**
> 1. Met gevangenisstraf van ten hoogste zes maanden of geldboete van de vierde categorie wordt gestraft hij die met een technisch hulpmiddel een gesprek dat in een woning, besloten lokaal of erf wordt gevoerd opzettelijk:
> 1°. anders dan in opdracht van een deelnemer aan dat gesprek afluistert;
> 2°. zonder deelnemer aan dat gesprek te zijn en anders dan in opdracht van zulk een deelnemer opneemt.
> 2. Het eerste lid is niet van toepassing op het opnemen:
> 1°. van gegevens die worden verwerkt of overgedragen door middel van telecommunicatie of door middel van een geautomatiseerd werk;
> 2°. behoudens in geval van kennelijk misbruik, met een technisch hulpmiddel dat op gezag van degene bij wie de woning, het lokaal of het erf in gebruik is, niet heimelijk aanwezig is;
> 3°. ter uitvoering van de Wet op de inlichtingen- en veiligheidsdiensten 2017.

Voor andere plaatsen dan woningen, besloten lokalen en erven (hierna kortheidshalve ‘niet-besloten plaatsen’ genoemd) geldt de volgende bepaling.

> **Artikel 139b Sr**
> 1. Met gevangenisstraf van ten hoogste drie maanden of geldboete van de derde categorie wordt gestraft hij die, met het oogmerk een gesprek dat elders dan in een

woning, besloten lokaal of erf wordt gevoerd af te luisteren of op te nemen, dat gesprek met een technisch hulpmiddel heimelijk:

1°. anders dan in opdracht van een deelnemer aan dat gesprek afluistert;

2°. zonder deelnemer aan dat gesprek te zijn en anders dan in opdracht van zulk een deelnemer opneemt.

2. Artikel 139a, tweede lid, onder 1° en 3°, is van overeenkomstige toepassing.

Op niet-besloten plaatsen geldt dus een lager strafmaximum – drie maanden gevangenisstraf of geldboete van de derde categorie. Beide bepalingen kennen een uitzondering voor gegevensoverdracht (waarvoor de specifieke bepaling van artikel 139c Sr geldt, zie onder) en voor de inlichtingen- en veiligheidsdiensten; het laatste is voor dit rapport niet relevant. Artikel 139b Sr kent echter niet de uitzondering van artikel 139a lid 2 onder 2º: op besloten plaatsen is de gebruiker van de plaats in beginsel gerechtigd om gesprekken af te luisteren als de microfoon (al dan niet gekoppeld aan een camera) openlijk aanwezig is (althans strafrechtelijk gesproken; er moet wel aan de regels van het gegevensbeschermingsrecht worden voldaan). Buiten besloten plaatsen valt het met een openlijk aanwezige microfoon afluisteren of opnemen van gesprekken sowieso niet onder de strafbaarstelling, omdat het dan niet heimelijk gebeurt. Het verschil laat zich verklaren door het element 'behoudens kennelijk misbruik' in artikel 139a Sr: de uitzonderingsgrond is ingevoerd om de rechthebbenden van woningen en besloten lokalen wel de gelegenheid te geven om afluisterapparatuur te gebruiken (bijvoorbeeld om hun eigendom te beveiligen of door werknemers om fraude te voorkomen[291]), mits dat maar kenbaar is voor bezoekers en er voldoende reden is om gesprekken af te luisteren. De uitzonderingsgrond perkt dus de mogelijkheden in voor rechthebbenden om op besloten plaatsen met kenbaar aanwezige apparatuur gesprekken af te luisteren. Van misbruik is bijvoorbeeld sprake als er wordt afgeluisterd 'uit nieuwsgierigsheid [sic], of om andere niet aanvaardbare beweegredenen, dan wel in strijd met instructies van de "heer des huizes"'.[292]

Interessant is dat de wetgever ten aanzien van de kenbaarheid een onderscheid maakt tussen (in onze terminologie) spionageproducten in enge en in brede zin. Voor afluisterapparatuur 'in de beperkte zin van het woord' moeten degenen wier gesprekken (zullen) worden afgeluisterd vooraf zijn ingelicht over het bestaan ervan; voor apparaten die (al dan niet toevallig) ook voor afluisteren geschikt zijn, zoals 'normale geluidsinstallaties e.d.', zal het voldoende zijn dat deze 'goed zichtbaar zijn aangebracht.'[293] Degenen die aanwezig zijn in de desbetreffende ruimte zullen dan uit zichzelf moeten beseffen dat het apparaat mogelijk kan worden gebruikt om hun gesprekken af te luisteren.

---

[291] *Kamerstukken II* 1967/68, 9419, nr. 3, p. 7.
[292] Ibid.
[293] Ibid.

Een beperking bij de strafbaarstelling is dat het moet gaan om communicatie tussen twee of meer personen: een monoloog valt er niet onder.[294] Het geluid van een menigte valt evenmin onder de strafbepaling, ook niet als men daaruit flarden van gesprekken kan afleiden.[295] Evenmin valt babygehuil (ondanks de communicatieve functie daarvan) onder 'gesprekken'.[296] Ook andere geluiden dan gesproken woorden vallen er niet onder, bijvoorbeeld geluiden die worden gemaakt 'bij amoureuze activiteiten'.[297] Dat vond de wetgever geen probleem, omdat als iemand kon verwachten dat er ook gesproken zou worden en als er daadwerkelijk wordt gesproken, hetgeen zich volgens de wetgever bij amoureuze activiteiten veelal zal voordoen, de afluisteraar toch strafbaar zal zijn.[298] Hoewel dit destijds een verdedigbare beperking was (het opnemen van privacygevoelige niet-communicatieve geluiden zal weinig zijn voorgekomen), lijkt ons deze beperking inmiddels achterhaald en een mogelijke lacune suggereren (deelvraag 4). Het heimelijk opnemen van geluiden die iemand maakt bij bijvoorbeeld een toiletbezoek of tijdens (woordloze) seksuele activiteiten vormt een significante privacy-inbreuk in de volledig private of intieme zone van het leven (die mogelijk leidt tot een inbreuk op de ruimtelijke en communicatieve privacy), die nog aanzienlijk groter wordt als zulke opnamen met naam en toenaam van de persoon op sociale media zouden worden geplaatst (een inbreuk op informationele privacy). Ook het heimelijk opnemen van geluiden van menigten, waaruit met huidige technieken ongetwijfeld veel beter dan in 1970 individuele uitingen te destilleren zijn, levert een privacy-inbreuk op die afhankelijk van de context minstens zo groot kan zijn als het afluisteren van een gesprek tussen twee personen in een park. De wetgever zou in dat licht kunnen overwegen om het element 'gesprekken' aan te passen in de wettekst (of een richtinggevende nieuwe interpretatie van 'gesprekken' te geven), zodat het ook persoonlijke geluiden omvat.[299]

De belangrijkste beperking in beide artikelen (deelvraag 4) is echter dat alleen het afluisteren of opnemen van gesprekken *tussen anderen* strafbaar is. Iemand die gesprekken opneemt waaraan zij zelf deelneemt, is niet strafbaar, ook niet als dit heimelijk gebeurt voor de andere gespreksdeelnemer(s). Onder deelnemers vallen diegenen die partner in het gesprek zijn, dus niet omstanders of andere aanwezigen, 'zoals degeen, die tijdens het gesprek consumpties serveert.'[300] De wetgever vond bij de invoering het heimelijk opnemen van gesprekken waaraan

---

[294] *Kamerstukken II* 1969/70, 9419, nr. 8, p. 5: 'Zo vallen (…) woorden die iemand in eenzaamheid uitspreekt, niet onder dit begrip.'
[295] *Kamerstukken II* 1967/68, 9419, nr. 3, p. 7.
[296] *Kamerstukken II* 1969/70, 9419, nr. 8, p. 6.
[297] *Kamerstukken II* 1969/70, 9419, nr. 7, p. 4.
[298] *Kamerstukken II* 1969/70, 9419, nr. 8, p. 5.
[299] Een aanvullend argument is de discrepantie tussen artikelen 139a-b enerzijds en 139c anderzijds: het opnemen van gesproken uitingen die geen gesprekken zijn is niet strafbaar, terwijl het opnemen van gedigitaliseerde uitingen die geen communicatie vormen, wel strafbaar is onder art. 139c (zie onder). Een gesproken monoloog wordt dus niet beschermd, een ingetikte monoloog wel. Zoals E.J. Koops, *Strafvorderlijk onderzoek van (tele)communicatie 1838-2002. Het grensvlak tussen opsporing en privacy,* Deventer: Kluwer 2002, p. 177, aangeeft, is de ratio hiervan moeilijk te vatten.
[300] *Kamerstukken II* 1967/68, 9419, nr. 3, p. 5.

iemand zelf deelneemt niet strafwaardig; soms is het ‘onschuldig of maatschappelijk gerechtvaardigd’, soms ook een schending ‘van het vertrouwen, dat de gespreksgenoten in elkaar stellen.’[301] Dat kan weliswaar moreel afkeurenswaardig zijn, maar het bereikt niet de drempel van strafwaardigheid.[302]

Jurisdicties maken echter verschillende rechtspolitieke keuzes om het heimelijk opnemen van eigen gesprekken wel of niet strafbaar te stellen. Illustratief zijn de Verenigde Staten: de meeste staten van de VS hebben dezelfde keuze gemaakt als de Nederlandse wetgever (zogenoemde ‘one-party consent’-staten), maar een dozijn staten heeft afluisteren strafbaar gesteld als niet alle gespreksdeelnemers toestemming hebben gegeven (zogenoemde ‘all-party consent’-staten).[303]

Evenals bij visuele observatie kan de vraag worden gesteld of normatieve keuzes gemaakt rond 1970 nog steeds voldoende grondslag hebben in het huidige tijdperk. Dit is belangrijk in verband met de mogelijkheden voor regulering (deelvraag 8). Het opnemen van mondelinge gesprekken was in de jaren ’70 goed mogelijk, maar niet per se simpel; men had er speciale apparatuur voor nodig, die ergens geplaatst moest worden of in of onder de kleding worden gedragen, zodat er de nodige moeite voor moest worden gedaan. Anno 2020 kan vrijwel iedereen eenvoudig geluid (en dus ook mondelinge gesprekken) opnemen, vanwege de geluidsopnamefunctionaliteit die op de alomtegenwoordige smartphones zit. Het risico dat een gesprekspartner zonder jouw medeweten een gesprek opneemt, is daardoor aanzienlijk groter geworden. De enige drempel dat heimelijk opnemen van gesprekken voorkomt is nu het vertrouwen dat gesprekspartners in elkaar stellen; de praktische drempels zijn vrijwel weggevallen. De vraag kan daarbij worden gesteld of het maken van inbreuk op het vertrouwen in gesprekspartners nog steeds buiten het strafrecht moet vallen.

Koops en Oerlemans wijzen er in het kader van deze vraag op dat de wetgever eind jaren ’90 van de vorige eeuw bij de Wet bijzondere opsporingsbevoegdheden heeft bepaald dat ook het direct afluisteren door justitie met toestemming van een gespreksdeelnemer onder de wettelijke bevoegdheid valt (art. 126l Sv), omdat het een inbreuk op de privacy betreft.[304] Zo kan een infiltrant opnameapparatuur bij zich dragen en inschakelen als hij gesprekken voert met een verdachte. De wetgever stelde daarbij:

> Wanneer dergelijke gesprekken worden opgenomen, is het recht op bescherming van de persoonlijke levenssfeer in het geding, omdat achteraf een exacte en volledige

[301] Ibid.
[302] Ibid.
[303] J.H. Alderman, ‘Police Privacy in the iPhone Era: The Need for Safeguards in State Wiretapping Statutes to Preserve the Civilian's Right to Record Public Police Activity’, 9 *First Amendment Law Review* (3), p. 487-545 op p. 495 e.v.
[304] B.J. Koops & J.J. Oerlemans, *Strafrecht en ICT: Reeks: Monografieën Recht en Informatietechnologie,* Den Haag: Sdu Uitgevers 2019, p. 43.

> weergave van het gesprek mogelijk is, terwijl de gesprekspartner van de opsporingsambtenaar daarop niet bedacht kan zijn.[305]

Deze argumentatie geldt niet alleen in de verticale verhouding tussen opsporingsinstanties en burgers, maar evenzeer in horizontale relaties tussen burgers onderling. Burgers zullen normaliter nauwelijks bedacht zijn op het feit dat wat zij tegen iemand zeggen, exact en volledig gereproduceerd zou kunnen worden. Met betrekking tot deelvraag 8, volgen we Koops en Oerlemans die suggereren dan ook dat het gewijzigde privacy-inzicht zou kunnen leiden tot het schrappen van de uitsluiting voor gespreksdeelnemers in artikelen 139a-b Sr.[306]

Een ander punt dat relevant voor deelvraag 4 is betreft de strafmaat. Het afluisteren van gesprekken kent een relatief laag strafmaximum (zes of drie maanden gevangenisstraf, afhankelijk van de plaats) in vergelijking met het afluisteren van telecommunicatie- of gegevensverkeer (artikel139c Sr), waarop maximaal twee jaar gevangenisstraf staat. Dat is mede een gevolg van de implementatie van een Europese Richtlijn die een maximum van minstens twee jaren gevangenisstraf eiste voor computerdelicten.[307] Ook is de strafbedreiging bij afluisteren lager dan bij visuele observatie (een jaar gevangenisstraf voor besloten plaatsen). Deze verschillen zijn wellicht inhoudelijk te onderbouwen, bijvoorbeeld omdat beeldopnamen een grotere impact kunnen hebben dan geluidsopnamen (een beeld zegt immers soms meer dan duizend woorden). Tegelijkertijd kan een stiekem gemaakte foto van iemand in haar woonkamer aanzienlijk minder privacygevoelig zijn dan een stiekem opgenomen gesprek dat zij aldaar voert. Het hangt sterk van de context en inhoud af, of beeld dan wel geluid de grootste privacyrisico's oplevert. Wat de mogelijkheden voor regulering betreft (deelvraag 8), zou de wetgever ook de onderlinge consistentie van de strafmaxima bij de verschillende vormen van spionage kunnen bezien en waar nodig de strafmaxima van artikelen 139a en 139b herijken.

Telecommunicatie en computergegevens

Het aftappen of opnemen van telecommunicatie of (andere vormen van) computergegevens-verkeer is strafbaar gesteld in de volgende bepaling.

> **Artikel 139c Sr**
>
> 1. Met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie wordt gestraft hij die opzettelijk en wederrechtelijk met een technisch hulpmiddel gegevens aftapt of opneemt die niet voor hem bestemd zijn en die worden verwerkt of

[305] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 38.
[306] B.J. Koops & J.J. Oerlemans, *Strafrecht en ICT: Reeks: Monografieën Recht en Informatietechnologie,* Den Haag: Sdu Uitgevers 2019, p. 43.
[307] *Stb.* 2015, 165, ter implementatie van Richtlijn 2013/40/EU over aanvallen op informatiesystemen.

overgedragen door middel van telecommunicatie of door middel van een geautomatiseerd werk.

2. Het eerste lid is niet van toepassing op het aftappen of opnemen:

1°. van door middel van een radio-ontvangapparaat ontvangen gegevens, tenzij om de ontvangst mogelijk te maken een bijzondere inspanning is geleverd of een niet toegestane ontvanginrichting is gebruikt.

2°. door of in opdracht van de gerechtigde tot een voor de telecommunicatie gebezigde aansluiting, behoudens in geval van kennelijk misbruik;

3°. ten behoeve van de goede werking van een openbaar telecommunicatienetwerk, ten behoeve van de strafvordering, dan wel ter uitvoering van de Wet op de inlichtingen- en veiligheidsdiensten 2017.'

Dit artikel is het complement van artikelen 139a-b Sr en omvat alle vormen van digitale communicatie anders dan gesprekken. Het zonder toestemming aftappen of opnemen van gegevensverkeer zal dan ook in de meeste gevallen strafbaar zijn, zodat artikel 139c Sr een robuuste privacybescherming oplevert tegen spionageproducten waarmee telecommunicatie of gegevensverkeer binnen een computersysteem wordt onderschept.

Een opmerkelijk verschil met het afluisteren van gesprekken, naast de hogere strafmaat, is dat bij het aftappen of opnemen van telecommunicatie of computergegevens geen onderscheid wordt gemaakt naar de plaats. Het aftappen van gegevensverkeer of communicatie op publiek toegankelijke plaatsen, zoals een café, bibliotheek of een bankje in het park, valt onder dezelfde bepaling als het aftappen binnen een woning (al kan de rechter bij de strafmaat wel rekening houden met de privacygevoeligheid van de plaats). Evenals bij afluisteren van gesprekken geldt een uitzondering voor rechthebbenden van de telecommunicatieaansluiting, zoals werkgevers, behoudens kennelijk misbruik. Specifiek voor aftappen van gegevens is de uitzondering van lid 2 onder 1°: het opvangen van radiosignalen is niet strafbaar, tenzij een bijzondere inspanning wordt verricht om de signalen op te vangen, zoals het blijven volgen van een auto vanwaaruit signalen worden uitgezonden.[308] De reden hiervan is dat signalen in de ether in beginsel vrij zijn.[309] Dit betekent volgens Schermer dat bijvoorbeeld het uitlezen van onbeveiligde RFID-chips,[310] wat geen bijzondere inspanning vergt, niet strafbaar is.[311] Aangezien radiosignalen

[308] Wel is het openlijk bekend (doen) maken van de inhoud van aldus rechtmatig opgevangen signalen strafbaar, als die inhoud redelijkerwijs niet voor de persoon bedoeld is, volgens de overtreding van artikel 441 Sr, met maximaal drie maanden hechtenis of geldboete van de derde categorie.
[309] B.J. Koops & J.J. Oerlemans, *Strafrecht en ICT: Reeks: Monografieën Recht en Informatietechnologie,* Den Haag: Sdu Uitgevers 2019, p. 44.
[310] Radiofrequentie-identificatie chips maken gebruik van elektromagnetische velden voor het automatisch identificeren en volgen van tags die aan objecten zijn bevestigd
[311] B. Schermer, 'Criminaliteit en RFID', in: Zwenne & Schermer (red.), *Privacy en andere juridische aspecten van RFID*, Den Haag: Elsevier Juridisch 2005, p. 85 & 88.

tegenwoordig veelal beveiligd zijn tijdens transmissie door de ether, vormt het opvangen ervan geen privacyrisico.

Aanvullende bepalingen

Het Wetboek van Strafrecht kent nog enkele aanvullende bepalingen die bepaalde handelingen voor of na het afluisteren strafbaar stellen. Zo is volgens artikel 139d lid 1 Sr het plaatsen van afluisterapparatuur strafbaar, met maximaal twee jaar gevangenisstraf of geldboete van de vierde categorie, indien dit gebeurt met het oogmerk[312] dat een gesprek, telecommunicatie of computergegevens wederrechtelijk worden afgeluisterd, afgetapt of opgenomen. Artikel 139e Sr stelt het bezit of bekendmaken van wederrechtelijk gemaakte opnames strafbaar, met gevangenisstraf van maximaal zes maanden of geldboete van de vierde categorie.

Voor spionageproducten in enge zin is wellicht de interessantste aanpalende bepaling de overtreding van artikel 441a Sr. Dit artikel stelt het reclame maken[313] voor afluisterapparatuur strafbaar, als daarbij de aandacht wordt gevestigd 'op de geschiktheid daarvan als technisch hulpmiddel voor het heimelijk afluisteren, aftappen of opnemen van gesprekken, telecommunicatie of andere gegevensoverdracht'. De maximumstraf hiervoor is hechtenis van ten hoogste twee maanden of een geldboete van de derde categorie. Op basis van dit artikel zouden bijvoorbeeld bepaalde reclame-uitingen van spy-webshops kunnen worden vervolgd.

5.4.4 Heling van gegevens

Art. 139g Sr stelt heling van gegevens strafbaar (vooral in verband met informationele privacy), met een maximale gevangenisstraf van een jaar of geldboete van de vierde categorie. Heling van gegevens is het verwerven of voorhanden hebben van gegevens waarvan men op het moment van verkrijgen wist of redelijkerwijs had moeten vermoeden dat deze door misdrijf zijn verkregen (lid 1 onder a). Als men op een later tijdstip erachter komt dat de gegevens uit misdrijf zijn verkregen, is het voorhanden hebben niet strafbaar; wel levert dan het verspreiden, bekendmaken of uit winstbejag gebruiken van deze gegevens nog strafbare heling van gegevens op (lid 1 onder b). Een uitzondering geldt voor situaties waarin deze handelingen te goeder trouw in het publiek belang geschieden, bijvoorbeeld door klokkenluiders (lid 2).

Indien bij het gebruik van spionageproducten in enge of in brede zin (dus inclusief hobbydrones) beelden worden vastgelegd op een manier die onder art. 139f Sr valt (dus heimelijk op een

---

[312] Oogmerk is de sterkste vorm van opzet, waarbij de wil van de persoon bewust gericht is op het bewerkstelligen van het effect van een handeling; het omvat daarmee niet het zogenoemde voorwaardelijk opzet, waarbij iemand de kans dat een bepaald effect optreedt voor lief neemt. Zie J. De Hullu, *Materieel strafrecht*, vijfde druk, Deventer: Kluwer 2012, p. 243-244.

[313] De bepaling spreekt van 'verspreiding van enig geschrift', maar hieronder zullen ook elektronische uitingen vallen, gezien de gangbare interpretatie in het strafrecht dat 'geschriften' niet tot papieren dragers beperkt zijn. Het zal wel moeten gaan om schriftelijke reclame; gesproken commerciële uitingen vallen vermoedelijk niet onder de term 'geschrift'.

besloten plaats, zie par. 5.4.1), dan is het bezit van deze beelden vervolgens ook strafbaar. Dit was van oudsher een zelfstandig onderdeel van art. 139f (onder 2°) Sr-oud, maar is bij de Wet computercriminaliteit III per 1 maart 2019 opgegaan in een algemenere strafbaarstelling van heling van gegevens in art. 139g Sr: bezit of verspreiding van niet-openbare gegevens waarvan men weet (of redelijkerwijs moet vermoeden) dat die uit misdrijf zijn verkregen. Heimelijk gemaakte foto's, filmpjes of geluidsopnamen die verder worden verspreid scheppen dus ook strafbaarheid voor de ontvanger en verdere verspreider daarvan. Een beperking daarbij is wel dat heling alleen misdrijven betreft: het verwerven of voorhanden hebben van wederrechtelijk op publiek toegankelijke plaatsen gemaakte beelden is niet strafbaar, omdat artikel 441 Sr een overtreding is en geen misdrijf.

5.4.5 Locatietracking

Bij locatietracking onderscheiden we tussen hardwarematige vormen (zoals GPS-trackers) en softwarematige vormen (zoals locatietracker-apps). Veelal zullen dergelijke spionageproducten heimelijk bij een te volgen persoon worden aangebracht, zoals bij de casus van locatietracking van een partner om diens gangen na te gaan. Voor softwarematige locatietracking zal dan snel de strafbaarstelling van gegevensbeschadiging in artikel 350a Sr van toepassing zijn.

> **Artikel 350a Sr**
>
> 1. Hij die opzettelijk en wederrechtelijk gegevens die door middel van een geautomatiseerd werk of door middel van telecommunicatie zijn opgeslagen, worden verwerkt of overgedragen, verandert, wist, onbruikbaar of ontoegankelijk maakt, dan wel andere gegevens daaraan toevoegt, wordt gestraft met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie.'

Belangrijk is vooral het element 'toevoegen' van gegevens: dit omvat ook het plaatsen van software op iemands draagbare computer of smartphone.[314] Zulk plaatsen is strafbaar als dit wederrechtelijk gebeurt, wat meestal het geval zal zijn als het heimelijk en dus zonder toestemming plaatsvindt. In sommige gevallen, bijvoorbeeld ouders die software op de smartphone van hun kind plaatsen om diens bewegingen te volgen zonder zijn toestemming, kan het heimelijk plaatsen wel rechtmatig zijn, al hangt dat mogelijk ook af van de leeftijd van het kind. Omdat we ons in dit rapport richten op puur horizontale privacy en de familierechtelijke implicaties van ouder/kind-verhoudingen buiten beschouwing laten, gaan we ervan uit dat het zonder toestemming plaatsen van tracking-software op iemands computer of smartphone zonder diens toestemming wederrechtelijk zal zijn en dit dus onder de strafbare gegevensbeschadiging van art. 350a Sr valt.

---

[314] Een smartphone valt ook onder de definitie van geautomatiseerd werk in artikel 80sexies Wetboek van Strafrecht.

Bij hardwarematige vormen van locatietracking ligt dit anders, omdat de fysieke equivalent van gegevensbeschadiging – zaakbeschadiging – geen element 'toevoegen' bevat. Artikel 350 Sr stelt, met dezelfde straf als artikel 350a Sr, strafbaar het opzettelijk en wederrechtelijk vernielen, beschadigen, onbruikbaar maken of wegmaken van een goed dat geheel of ten dele aan een ander toebehoort. Bij computers vormt het toevoegen van gegevens een aantasting omdat de integriteit van het systeem als geheel in het geding is; bij fysiek eigendom wordt het vermeerderen van een goed niet gezien als een vorm van zaakbeschadiging. Het stiekem plaatsen van een GPS-tracker op een auto valt daarom als zodanig niet onder artikel 350 Sr. Niettemin kan bij het plaatsen van zo'n tracker wel enige beschadiging ontstaan, zoals een krasje op de auto, zodat dan alsnog kan worden vervolgd voor zaakbeschadiging; omdat zo'n krasje niet de kern uitmaakt van de spionagehandeling, is het maar de vraag of het Openbaar Ministerie hiervoor zou vervolgen. Interessant is dat in de Verenigde Staten in de GPS-trackingzaak *Jones*[315] (geen horizontale privacy, maar verticale privacy in de verhouding opsporingsinstantie-verdachte) het Hooggerechtshof het plaatsen van een GPS-tracker niet benaderde als een inbreuk op het privacyrecht in de zin van de redelijke privacyverwachting, maar teruggreep op het eigendomsrecht, waarbij het zonder toestemming plaatsen van een object op een auto als zodanig werd gezien als een vorm van eigendomsaantasting, ongeacht of daarbij enige vorm van beschadiging optrad. In het Nederlandse strafrecht wordt daarentegen een aantasting van het eigendomsrecht alleen als strafwaardig beschouwd als enige beschadiging optreedt. Anders dan softwarematige tracking kan fysieke locatietracking daarom niet, of in elk geval niet goed, via de band van beschadiging worden aangepakt.

Men zou bij fysieke tracking nog kunnen denken aan belaging (*stalking*). Dit betreft volgens artikel 285b Sr het wederrechtelijk stelselmatig opzettelijk inbreuk maken op iemands privacy met het oogmerk die ander te dwingen iets te doen, niet te doen of te dulden dan wel vrees aan te jagen; dit is strafbaar met een gevangenisstraf van ten hoogste drie jaren of een geldboete van de vierde categorie. Locatietracking (bijvoorbeeld met GPS-tracker of een smartphone-app) maakt het mogelijk om iemand geautomatiseerd systematisch te volgen. Dit volgen zal bij spionageproducten in enge zin echter normaliter niet gebeuren met de bedoeling om de gevolgde persoon vrees aan te jagen of haar gedrag te doen veranderen, maar juist heimelijk geschieden. Belaging is daarmee geen geschikt middel om locatiespionage aan te pakken. (Locatietracking kan overigens wel een versterkend of faciliterend effect hebben in gevallen waarin iemand al wordt gestalkt. Dat vergt mogelijk beleidsinterventies gericht op het voorkomen van het gebruik van locatietrackers door stalkers, maar dat staat los van de strafwaardigheid van spionageproducten.)

[315] United States v. Jones, 565 U.S. 400 (2012).

Voor zover wij kunnen zien, valt het heimelijk plaatsen van fysieke locatietrackers ook niet onder een andere strafbaarstelling, zodat hiertegen, anders dan softwarematige trackers, geen strafrechtelijke bescherming bestaat. Men kan deze discrepantie tussen software en hardware wel verklaren vanuit de historische ontwikkeling en de enigszins andere dynamiek van zaakbeschadiging en gegevensbeschadiging, maar voor de privacyrisico's van het bespioneren van iemands bewegingen lijkt het weinig uit te maken of dit met hardware of software plaatsvindt. Wij concluderen daarom dat er een mogelijke lacune zit in de wetgeving (deelvraag 4) ten aanzien van heimelijke (of anderszins non-consensuele) hardwarematige locatietracking, ten opzichte van vergelijkbare locatietracking die met spionagesoftware plaatsvindt. Een oplossing hiervoor – met betrekking tot reguleringsmogelijkheden (deelvraag 8) – zou kunnen zijn om een gelijke benadering van fysieke en softwarematige locatietracering in te voeren.

5.4.6 Deelconclusie en discussie: mogelijke strafrechtelijke lacunes en reguleringsmogelijkheden

Op basis van bovenstaande discussie bieden we hier een samenvatting van de geïdentificeerde mogelijke lacunes (antwoord op deelvraag 4) en bespreken we verder de mogelijkheden voor hun regulering (antwoord op deelvraag 8).

De strafwetgeving kent belangrijke bepalingen die duidelijke grenzen stellen aan het visueel of auditief bespioneren van medeburgers. Het gebruik van heimelijk aangebrachte camera's om afbeeldingen te maken is strafbaar, evenals het met een technisch hulpmiddel afluisteren of opnemen van gesprekken, telecommunicatie of gegevensverkeer. Daarmee wordt een belangrijk deel van de privacyrisico's van hobbydrones en spionageproducten afgedekt. Toch laat onze analyse zien dat er enkele mogelijke lacunes in het strafrecht zijn door de manier waarop de strafbepalingen zijn vormgegeven.

Bij visuele observatie is het belangrijkste struikelblok dat het moet gaan om *heimelijk aangebrachte* camera's. De strafbepalingen omvatten niet het heimelijk *gebruik* van camera's waarvan de *aanwezigheid* wel kenbaar is. Dat betekent dat het visueel spioneren met zichtbare draagbare camera's en met hobbydrones vaak buiten de strafbaarstelling zal vallen, hoewel dit wel substantiële privacyrisico's oplevert, met name voor relationele en gedragsprivacy, en soms, zoals bij Kinderdijk, voor de lichamelijke en ruimtelijke privacy. Dit is een mogelijke lacune in de wetgeving gezien de alomtegenwoordigheid van draagbare camera's en het gebruik van drone-camera's, waarbij burgers nauwelijks handelingsmogelijkheden hebben om zich te verweren tegen ongewenste afbeeldingen. Er is politieke en maatschappelijke discussie nodig over de omstandigheden waarin burgers in het huidige tijdperk zich voldoende vrij zouden moeten kunnen voelen van observatie door anderen. Bij smartphones en drones speelt vooral de onzekerheid of anderen de camerafunctie gebruiken om iemand te observeren een rol, evenals het gegeven dat burgers zich vaak moeilijk kunnen verweren tegen het maken van ongewenste afbeeldingen. Het zou echter te ver gaan om alle niet-consensuele afbeeldingen van personen

gemaakt door smartphone- en dronecamera's te verbieden. Waar de grenzen precies moeten liggen, is een politieke keuze die op basis van een geïnformeerd politiek en maatschappelijk debat moet worden gemaakt. Factoren die in dat debat aan de orde kunnen komen, zijn onder andere de plaatsen en contexten waarin mensen onbevangen zichzelf moeten kunnen zijn, kenbaarheid, het gebruik van de afbeeldingen, en de mogelijkheden voor mensen om zich te verweren tegen ongewenste afbeeldingen.

Een andere mogelijke lacune is dat de strafbaarstelling van heimelijke observatie beperkt is tot personen, en daarmee niet het observeren van objecten (woningen, schuren, loodsen) omvat ter voorbereiding van inbraak, terwijl dat ook niet duidelijk onder strafbare voorbereidings-handelingen (art. 46 Sr) zal vallen. Als dit fenomeen vaak genoeg voorkomt om tot strafrechtelijke aanpak te nopen (wat wij in deze verkennende studie niet kunnen inschatten), dan zou de wetgever kunnen overwegen om aan de strafbaarstelling van heimelijke observatie een lid toe te voegen dat specifiek ziet op het observeren van objecten (in plaats van personen) met het oogmerk bepaalde misdrijven voor te bereiden.

Bij auditieve observatie – wederrechtelijk afluisteren – moet ook de vraag worden gesteld of in het verleden gemaakte normatieve keuzes nog steeds voldoende grondslag hebben. Twee aspecten van de strafbaarstelling van het 'direct afluisteren' of opnemen van mondelinge gesprekken veroorzaken daarbij een mogelijke lacune: de uitsluiting van strafbaarheid van het opnemen van een gesprek door een gespreksdeelnemer zelf, en de beperking tot gesprekken (waar in zichzelf praten en andere niet-communicatieve geluiden buiten vallen). Vooral het eerste aspect is belangrijk in het licht van spionageproducten in brede zin, aangezien de opnamefunctionaliteit van alomtegenwoordige smartphones betekent dat het risico dat een gesprekspartner zonder iemands medeweten een mondeling gesprek opneemt, aanzienlijk groter is geworden. Daarnaast vraagt ook de onderlinge consistentie van strafmaxima aandacht.

Bij locatietracking hebben we een verschil geconstateerd tussen softwarematige en hardwarematige methoden. Het heimelijk plaatsen van fysieke locatietrackers valt niet onder een strafbaarstelling (tenzij bij het plaatsen een object wordt beschadigd), zodat hiertegen, anders dan softwarematige trackers, geen strafrechtelijke bescherming bestaat. Voor de privacyrisico's van het bespioneren van iemands bewegingen lijkt het weinig uit te maken of dit met hardware of software plaatsvindt. Daarom signaleren wij een mogelijke lacune ten aanzien van heimelijke hardwarematige locatietracking, die zou kunnen worden opgelost door een gelijke benadering van de twee typen te hanteren.

5.5 Gemeentewetgeving: Algemene Plaatselijke Verordeningen

De Algemene Plaatselijke Verordening (APV) is een wetgevend instrument op gemeentelijk niveau dat alleen in de desbetreffende gemeente van kracht is.[316] Het regelt de onderwerpen die tot het gemeentelijke publieke domein kunnen worden gerekend voor zover deze niet nader zijn uitgewerkt in bijzondere verordeningen zoals de Marktverordening, de Afvalstoffenverordening en de Verordening op het binnenwater. De APV is daarmee bij uitstek een verordening die de gemeenteraad op basis van artikel 149 Gemeentewet (Gw) in het belang van de gemeente kan maken.[317] Het grootste deel van de bepalingen in de APV berust op de autonome bevoegdheid van gemeenten conform artikel 149 Gw.[318] Met autonomie wordt bedoeld dat het gemeentebestuur de bevoegdheid heeft, om binnen de grenzen van de gemeente, de regeling van onderwerpen die tot de huishouding van de gemeente behoren uit te voeren.[319] De APV is dus een autonome verordening doordat het gemeentebestuur de vrijheid heeft om de huishouding vast te stellen, bijvoorbeeld het prostitutiebeleid of regels omtrent evenementen, maar ook het strafbaar stellen van het bespieden van personen.

De APV is een verordening met primair externe werking waardoor de burgers of instellingen rechtstreeks geraakt worden.[320] Door middel van bindende regels in de APV proberen gemeenten gebiedend en verbiedend het gedrag van haar inwoners te beïnvloeden. Daarnaast kunnen in de APV-bevoegdheden worden toegekend. De burgemeester kan bijvoorbeeld een bevel opleggen of categorieën van inrichtingen voor een vergunningplicht aanwijzen.[321] Als zodanig kan de APV ook worden gezien als een gemeentelijke verordening die ook de rol van een soort lokaal Wetboek van Strafrecht vervult. Het voordeel van lokaal strafrecht is dat rekening kan worden gehouden met plaatselijke omstandigheden. Een nadeel daarvan zou kunnen zijn dat het strafrecht plaatselijk verschilt.

Artikelen 108 en 149 van de Gw geven aan dat de gemeenteraad geen volledige vrijheid heeft bij het vaststellen van een gemeentelijke verordening. De gemeenteraad moet zich beperken tot de gemeentelijke huishouding. De gemeentelijke huishouding wordt op drie manieren begrensd: de geografische grens, de benedengrens en de bovengrens. Vooral de benedengrens is hier relevant. De benedengrens geeft aan dat wat buiten de openbaarheid ligt, buiten de wetgevende

---

[316] D.L. Zwagerman, *Basisboek APV en bijzondere wetten*, Hilversum: Concept uitgeverij 2016, p. 9.
[317] Art. 149 Gemeentewet: 'De raad maakt de verordeningen die hij in het belang van de gemeente nodig oordeelt.'
[318] De APV bevat ook bepalingen die gebaseerd zijn op het zgn. 'medebewind', maar dit is niet relevant voor het lopende onderzoek.
[319] De grondslag voor de autonome bevoegdheid voor het gemeentebestuur is weggelegd in artikel 124, eerste lid van de Grondwet en wordt herhaald in artikel 108, eerste lid van de Gemeentewet; D.L. Zwagerman, *Basisboek APV en bijzondere wetten*, Hilversum: Concept uitgeverij 2016, p. 10-11.
[320] A.E. Schilder & J.G. Brouwer, *Staats- en bestuursrecht: Gemeentelijke verordeningen*, Nijmegen: Ars Aequi Libri 2015, p. 5.
[321] A.E. Schilder & J.G. Brouwer, *Staats- en bestuursrecht: Gemeentelijke verordeningen*, Nijmegen: Ars Aequi Libri 2015, p. 14.

bevoegdheid van de gemeenteraad valt. Dit betreft vooral het recht op privacy. Men mag in de privésfeer doen en laten wat men wil in 'volle' vrijheid, behoudens ieders verantwoordelijkheid volgens de wet.[322] De verordende bevoegdheid beperkt zich tot het openbaar belang. Dit betekent dat de gemeenteraad niets mag regelen over handelingen in de privésfeer, tenzij de handelingen een uitstraling hebben of kunnen hebben naar de openbaarheid.

Voor dit onderzoek naar burgers die elkaar bespioneren via drones of spionageproducten in enge zin zijn twee soorten bepalingen uit de APV's relevant: een bepaling over het bespioneren van personen en een bepaling over overlast in de openbare ruimte. Andere soorten bepalingen in de APV's reguleren andere zaken en zijn dus niet relevant voor dit onderzoek. In het kader van dit rapport zullen deze bepalingen worden onderzocht in de model-APV, die we als basis gebruiken, en de APV's van Amsterdam, Rotterdam, Utrecht en Westvoorne om te kijken of hun lokale regelgeving specifieke aanknopingspunten biedt voor regulering van hobbydrones. De APV's van Amsterdam, Rotterdam en Utrecht zijn om verschillende redenen gekozen. Ten eerste behoren zij tot de grootste steden van Nederland, die tot taak hebben het gedrag van grote aantallen mensen in de openbare ruimte te reguleren. Ten tweede bevatten hun APV's een verklarende tekst, die extra inzicht biedt in de bepalingen. En ten derde hebben de APV's van Amsterdam en Rotterdam bepalingen over spionage die sterk afwijken van de tekst van de modelverordening, wat mogelijk extra inzicht biedt in de regulering van spionageproducten. Ten vierde is gekozen voor de APV van Westvoorne omdat deze gemeente de twee relevante bepalingen uit de model-APV specifiek heeft aangepast met de bedoeling de mogelijke spionage en overlast voor burgers door middel van drones aan te pakken. Omdat de APV's van veel andere Nederlandse steden gewoon de model-APV volgen, gaan we, door naar de model-APV te kijken, worden die indirect ook behandeld in dit overzicht.

5.5.1 De modelverordening van de Vereniging van Nederlandse Gemeenten

De Vereniging van Nederlandse Gemeenten (VNG) is de koepelorganisatie van alle gemeenten. De rol van de VNG is het ondersteunen van het functioneren van gemeenten, ook door het verstrekken van modelverordeningen. Deze modellen zijn een leidraad voor de gemeenten en om die reden niet bindend. Door middel van de modelverordeningen probeert de VNG te voorkomen dat gemeentebesturen opnieuw het wiel moeten uitvinden en wordt uniformiteit in de gemeentelijke regelgeving bevorderd.[323] De modelverordeningen worden regelmatig aangepast aan het geldend recht (inclusief nieuwe wet- en regelgeving, jurisprudentie en de praktijkervaringen van gemeenten).

---

[322] G. Klompmaker, A.M.M. Sluijters en J. Veenstra, Inleiding gemeentewet van wet naar praktijk, Den Haag: Sdu uitgevers 2008, p. 78.
[323] A.E. Schilder & J.G. Brouwer, *Staats- en bestuursrecht: Gemeentelijke verordeningen*, Nijmegen: Ars Aequi Libri 2015, p.13.

In de praktijk wordt de tekst van de model-APV vaak gebruikt door gemeenten, die de modelbepalingen (dat wil zeggen bepalingen uit de model-APV) vaak gewoon in hun eigen APV kopiëren. Dit geldt ook voor de twee bepalingen (over bespioneren van personen en over overlast) die relevant zijn voor dit onderzoek. Ze zijn ook van toepassing ongeacht de AVG. Het is daarom nuttig om de twee modelbepalingen kort te bespreken als basis voor de beoordeling van de wijzigingen die de genoemde gemeenten hebben aangebracht om overlast en spionage aan te pakken.

Zowel de bepaling die spionage van personen verbiedt als de bepaling over overlast in de openbare ruimte zijn te vinden in de afdeling over 'Maatregelen ter voorkoming van overlast, gevaar voor schade' in de model-APV.

a) Bespieden van personen

Artikel 2:53 Bespieden van personen

1. Het is verboden zich in de nabijheid van een persoon of een gebouw, woonwagen of woonschip op te houden met de kennelijke bedoeling deze persoon of een persoon die zich in dit gebouw, deze woonwagen of dit woonschip bevindt, te bespieden.

2. Het is verboden door middel van een verrekijker of enig ander optisch instrument een persoon die zich in een gebouw, woonwagen of woonschip bevindt te bespieden.

Met artikel 2:53 wordt beoogd ongemerkte en als ongewenst ervaren verstoring van de privacy tegen te gaan. Als zodanig is deze bepaling duidelijk van toepassing op situaties waarin burgers andere burgers door optische instrumenten bespioneren. Meerdere gemeenten, zoals Utrecht, Den Haag, Eindhoven en Dordrecht, hebben deze modelbepaling in hun APV's overgenomen. Het is dus niet nodig om deze APV’s afzonderlijk te onderzoeken.

Deze bepaling stelt in het eerste lid dat het verboden is om zich in de nabijheid te bevinden van een persoon of een gebouw, woonwagen of woonboot met de kennelijke bedoeling om daar iemand te bespioneren. Het blijft openstaan wat kan worden beschouwd als 'kennelijke intentie om iemand te bespioneren', maar men kan zich voorstellen dat langdurige of voortdurende aanwezigheid of het op de loer liggen bij een huis of appartement als zodanig zou kunnen gelden. De reikwijdte van deze bepaling is beperkt tot het bespioneren van iemand die zich in de buurt bevindt of zich op een afgesloten privéplek bevindt, zoals een gebouw, een woonwagen of een woonboot. Met betrekking tot het bespioneren van personen in de omgeving kan worden begrepen dat het de bedoeling was om gedrag te verbieden zoals 'down-blousing' (het kijken in de blouse van een vrouwelijk persoon) of het kijken naar wat iemand op zijn telefoon typt,

waarvoor men - aangezien er geen technische instrumenten worden gebruikt - dicht bij de bespioneerde persoon moet zijn.

In het tweede lid is het specifiek verboden om 'verrekijkers en andere optische instrumenten' te gebruiken om personen te bespioneren die op een privéplek zijn, zoals in een gebouw, woonwagen of woonboot. Het toepassingsgebied van de tweede alinea is duidelijk beperkt tot visuele waarneming. De toelichting van deze bepaling in de model-APV bevestigt dit door te stellen dat het heimelijk afluisteren wordt geregeld in de paragrafen 139a e.v.[324]en 441a Sr (zie daarover par. 5.4.3). Echter, het van afstand met behulp van verrekijkers of zoom-lenzen bespieden van iemand die zich in de openbare ruimte of in een niet-afgesloten privéruimte bevindt, lijkt buiten de reikwijdte te vallen.

Het doel van deze bepaling is het verbieden van onopgemerkte inbreuken op de privacy van mensen, die door iedereen als ongewenst worden ervaren, en het nemen van maatregelen tegen voyeurs. Volgens de toelichting van de model-APV zal deze bepaling echter alleen worden toegepast in excessieve situaties. Anders dan bij het delict belagen (‘stalking’) uit artikel 285b Sr is hier geen oogmerk vereist om iemand ergens toe brengen of van af te houden dan wel vrees aan te jagen (zie par. 5.4.5). Met dit lid kan bijvoorbeeld worden opgetreden tegen het ongewenst via een kijkgaatje begluren van personen in kleedhokjes. Dit artikel is daar dus een aanvulling op. De politie zal dus in het algemeen pas optreden indien burgers klachten hebben geuit over voyeurs.[325] Bovendien is artikel 2:53 facultatief omdat, volgens de model APV, het zeer weinig wordt toegepast en is gericht op excessieve situaties. Volgens de toelichting in de model-APV kan een situatie van spionage waarbij iemand klaagt bij de politie echter al als buitensporig worden beschouwd.

b) Hinderlijk gedrag in voor het publiek toegankelijke ruimten

> *Artikel 2:50 Hinderlijk gedrag in voor het publiek toegankelijke ruimten*
>
> *Het is verboden zich zonder redelijk doel en op een voor anderen hinderlijke wijze op te houden in of op een voor het publiek toegankelijke ruimte, dan wel deze te verontreinigen of te gebruiken voor een ander doel dan waarvoor deze ruimte is bestemd. Onder deze ruimten worden in elk geval verstaan portalen, telefooncellen, wachtlokalen voor het openbaar vervoer, parkeergarages en rijwielstallingen.*

Op basis van artikel 2:50 kan tegen vormen van onnodige hinder of overlast worden opgetreden. Volgens de toelichting bij de model-APV moet deze bepaling worden gezien als een aanvulling op een aantal bepalingen in het Wetboek van Strafrecht, zoals de artikelen 424

[324] Dit artikel wordt vervangen door 273d Wetboek van Strafrecht.
[325] Model-APV, Toelichting.

("straatschenderij") en 426bis ("belemmeren van anderen op de openbare weg"). De bepalingen in Sr zijn 'strakker', in die zin dat de desbetreffende 'baldadigheid' van een hoger niveau moet zijn, wat verder gaat dan wat mensen gewoonlijk bedoelen als ze de term in het dagelijkse taalgebruik gebruiken. Wanneer het gedrag niet het niveau van overlast bereikt dat nodig is om een beroep te doen op het strafrecht, kan daarom artikel 2:50 model-APV worden gebruikt.

Waar het enigszins moeilijk zou zijn om het gebruik van spionageproducten in enge zin te omschrijven als 'hinderlijk gedrag', vooral in gevallen waarin de spionage onopgemerkt blijft, kan deze bepaling wel relevant zijn met betrekking tot hobbydrones. Het vliegen van drones kan namelijk gemakkelijk overlast veroorzaken door onophoudelijk boven mensen te vliegen (die ook niet kunnen bepalen of ze gefilmd of op een andere manier geobserveerd worden door de drone; zie par. 5.4.1) en vooral door het zoemende geluid dat door de drone wordt geproduceerd en dat de meeste mensen erg irritant vinden. In de toelichting bij de model-APV wordt echter niet op deze kwestie ingegaan.

5.5.2 Privacy: ‘bespieden van personen’

In deze sub-paragraaf zullen we de bepalingen over het bespioneren van personen in drie gemeenten onderzoeken: Westvoorne, Amsterdam en Rotterdam.[326] Deze gemeenten hebben namelijk een bepaling met betrekking tot bespieden van personen die op verschillende manieren afwijkt van de modelbepaling. Deze bepalingen hebben dan ook merkbare gevolgen voor de bescherming van de horizontale privacy van burgers.

a) APV Westvoorne

De spionagevoorziening in APV Westvoorne was aanvankelijk vrijwel gelijk aan die in de model-APV. Naar aanleiding van het toenemende gebruik van drones door burgers heeft de gemeente deze bepaling in 2016 echter aangepast (evenals de bepaling over 'hinderlijk gedrag in de openbare ruimte' zoals besproken in par. 5.5.3).

Al vóór het amendement werd in de tweede alinea verwezen naar "verrekijkers of andere (optische) instrumenten" - dat wil zeggen met "optische" tussen haakjes. Dit zou kunnen impliceren dat technische apparatuur die geschikt is voor andere soorten waarnemingen (bv. audio of locatiebepaling) ook onder het toepassingsgebied kan vallen, althans in beginsel. Bovendien is in het amendement van 2016 'op niet-openbaar toegankelijk gebied' toegevoegd aan de lijst van plaatsen waar een persoon niet mag worden bespioneerd.

In de gewijzigde bepaling staat nu:

---

[326] In deze paragraaf gaan we de Utrecht-APV niet onderzoeken aangezien de bepaling over bespieden van personen dezelfde is als in de model-APV.

Artikel 2:53 Bespieden van personen

1. *Het is verboden zich in de nabijheid van een persoon of een gebouw, woonwagen of woonschip op te houden met de kennelijke bedoeling deze persoon of een persoon die zich in dit gebouw, deze woonwagen of dit woonschip bevindt, te bespieden.*
2. *Het is verboden door middel van een verrekijker of enig ander (optisch) instrument een persoon die zich in een gebouw, woonwagen, woonschip of op niet-openbaar toegankelijk gebied bevindt te bespieden.*

Het opnemen van 'op niet-openbaar toegankelijk gebied' betekent dat het privégebied rond woningen die geen deel uitmaken van aaneengesloten bebouwing, zoals het erf van vrijstaande boerderijen en landbouwgrond, nu ook onder het toepassingsgebied vallen. De redenering van de gemeente voor deze wijziging was dat er binnen Westvoorne veel buitengebied met vrijstaande woningen en boerderijen is, waar personen ook bespioneerd zouden kunnen worden.[327] Door het beperkte toepassingsgebied van de bepaling in de model-APV zouden dergelijke niet-afgesloten plaatsen anders buiten het toepassingsgebied zijn gevallen.

b) APV Amsterdam

De APV Amsterdam heeft een wezenlijk andere tekst dan de model-APV. Deze tekst van de bepaling is in 2010 ingevoerd. Ten eerste heet de bepaling 'Bescherming van de privacy' en niet 'Bespieden van personen'. De titel impliceert dus al een wat bredere reikwijdte dan de model-APV. Zoals kort besproken in het literatuuroverzicht in het eerste deel van dit rapport, gaat het bij spionage om heimelijke observatie van personen. Privacy kan echter ook worden beïnvloed door openlijke observatie (d.w.z. surveillance).

Bovendien verschillen de volgorde en de inhoud van de bepaling ook van de modelbepaling. In de APV Amsterdam staat in het tweede lid dat het verboden is om zich op of nabij een weg te bevinden met de kennelijke bedoeling om anderen te bespioneren op of nabij de weg, in een gebouw of een vaartuig. Volgens de toelichting, dient het tweede lid hier ter eerbiediging van de persoonlijke levenssfeer. Het verbiedt het begluren van personen vanaf de weg. Hoewel de tekst van dit lid afwijkt van de model-APV, lijkt de reikwijdte ervan min of meer gelijk te zijn. Ook al verwijst dit lid niet expliciet naar personen in de omgeving, het bespioneren van iemand zonder technisch gereedschap, dat wil zeggen alleen met de ogen, oren en neus, kan alleen worden gedaan als de persoon relatief dichtbij is.

Er is echter een opmerkelijk verschil in de reikwijdte in de eerste paragraaf van de APV Amsterdam. Het eerste lid van deze bepaling verbiedt namelijk het gebruik van

[327] Agenda van de gemeenteraad op 15/12/15.

'bewakingsapparatuur' voor het observeren van personen in een ander gebouw, vaartuig of besloten erf dan waar de bewakingsapparatuur is geïnstalleerd:

Artikel 2.25 Bescherming van de privacy

1. *Het is verboden bewakingsapparatuur te gebruiken wanneer daarmee personen kunnen worden waargenomen in een ander gebouw, vaartuig of besloten erf dan waar de bewakingsapparatuur staat opgesteld.*

Deze bepaling is dus ruimer en omvat alle soorten bewakingsapparatuur (in plaats van alleen optische apparatuur die visuele waarneming mogelijk maakt) en "besloten erven", dat wil zeggen afgescheiden plaatsen die niet voor het publiek toegankelijk zijn, maar die toch vanuit de openbare ruimte kunnen worden waargenomen, omdat ze niet bebouwd of overdekt zijn. In tegenstelling tot de uitbreiding van het territoriaal bereik in APV Westvoorne is de Amsterdamse bepaling niet van toepassing op landbouwgrond. Volgens de toelichting van de APV Amsterdam, gaat het eerste lid een te ruim gebruik van bewakingsapparatuur tegen. Op basis hiervan kan bijvoorbeeld worden gevraagd om een afschermkap aan te brengen op bewakingsapparatuur.[328] Hoewel deze bepaling dus het verbod omvat op het toezicht op personen in dergelijke privéplaatsen met behulp van bewakingsapparatuur, met inbegrip van visuele, audio- of andere soorten observatie, valt dergelijke surveillance in de openbare ruimte nog steeds buiten het toepassingsgebied.

c) APV Rotterdam

De Rotterdamse APV is over het algemeen vergelijkbaar met de tekst van de model-APV. De bepaling in de APV Rotterdam wijkt echter ook op een aantal punten af van de modeltekst. Ten eerste heeft het een andere titel: 'Bespieden en heimelijk fotograferen/filmen van personen', wat al een bredere strekking heeft. En ten tweede bevat deze bepaling drie in plaats van twee leden. De eerste twee zijn dezelfde als die in de model-APV. Het derde lid verruimt echter het toepassingsgebied van deze bepaling en verbiedt het in het geheim filmen of fotograferen van personen op een voor het publiek toegankelijke plaats met behulp van een technisch hulpmiddel, op voorwaarde dat dit de eer aantast of een inbreuk op de persoonlijke levenssfeer vormt.

Artikel 2:53 Bespieden en heimelijk fotograferen/filmen van personen

3. *Het is verboden op of aan de openbare weg dan wel in een voor publiek toegankelijke ruimte een persoon heimelijk te filmen of heimelijk te fotograferen door middel van een technisch hulpmiddel wanneer dit een aantasting van de eerbaarheid of een inbreuk op de persoonlijke levenssfeer oplevert.*

[328] Toelichting APV Amsterdam.

Dit betekent dat het in het geheim opnemen van beelden van personen met behulp van technische apparatuur ook verboden kan zijn wanneer personen zich in de openbare ruimte bevinden, zoals op straat of in parken. Om de reikwijdte van deze bepaling te beperken, zal er echter alleen sprake zijn van een overtreding, wanneer de handeling de eer aantast of inbreuk maakt op de privacy. Hoe nauw of breed een dergelijke 'aantasting van de eer' of 'inbreuk op de privacy moet worden opgevat, wordt echter aan de gemeente, de rechtshandhaving en ten slotte de rechtbanken overgelaten om te beslissen. Wat wel gezegd kan worden is dat de bepaling niet de voorwaarde bevat van verdere verspreiding van de film of de foto, bijvoorbeeld door deze online te plaatsen of te delen met vrienden. Met andere woorden, er hoeft geen sprake te zijn van verdere verwerking of verspreiding van informatie, het verzamelen van informatie kan voldoende zijn voor strafbaarheid; ook dat kan immers al snel gepaard gaan met een inmenging in andere vormen van privacy (bijvoorbeeld gedragsmatige).

Het is echter de vraag of deze bepaling het toepassingsgebied van artikel 441b Sr daadwerkelijk verruimt, aangezien dit laatste geen aantasting van de eer of de privacy vereist (zie par. 5.4.1). Toch kunnen de termen 'heimelijk te filmen of heimelijk te fotograferen' in bredere zin worden opgevat dan het ietwat beperkte begrip van de eis dat de aanwezigheid van het technische hulpmiddel niet duidelijk kenbaar is gemaakt in artikel 441b Sr. Dit lijkt inderdaad te worden geïmpliceerd door de toelichtende tekst, waarin staat: 'Onder "heimelijk" filmen of fotograferen wordt verstaan dat dit zonder instemming van de betrokkene heeft plaatsgevonden.'[329] Als zodanig valt geheim filmen of fotograferen met een smartphone of drone, wanneer er geen bijzondere inspanning is gedaan om de smartphone of drone te verbergen (maar wanneer het filmen of fotograferen nog onopvallend was, omdat het vaak niet duidelijk zal zijn of er wel of niet wordt opgenomen), wellicht gemakkelijker onder het toepassingsgebied van de APV-bepaling. De bepaling zou ook van toepassing zijn in gevallen waarin het filmen of het maken van foto's duidelijk wordt aangekondigd, als geobserveerde personen geen toestemming geven (en kunnen geven, met name in het geval van drones) voor de waarneming.

5.5.3 Overlast: 'hinderlijk gedrag op openbare plaatsen'

Een andere mogelijk relevante bepaling, in ieder geval met betrekking tot de overlast door het vliegen van drones, is de bepaling betreffende 'hinderlijk gedrag op openbare plaatsen'. Zoals uitgelegd in paragraaf 4.1 is overlast een vorm van inmenging in het privéleven van een persoon door bijvoorbeeld lawaai of stank.

Deze bepaling kan dus een aanvulling vormen op het bovengenoemde verbod op spionage in de APV. Dit zal met name relevant zijn met betrekking tot drones, die - in ieder geval voorlopig –

[329] APV Rotterdam toelichting artikel 2:53.

meestal groot genoeg zijn om door personen op de grond te worden gezien en een zeer specifieke en (vaak als) vervelend ervaren vorm van zoemen uitzenden. Mensen zijn zich er dan ook van bewust dat een drone boven hen vliegt en kunnen zelfs vermoeden dat de drone ook aan het filmen is of een ander soort lading heeft. Naast de significante (horizontale) privacyrisico's die een dergelijke min of meer heimelijke observatie met zich meebrengt, zullen mensen zich ook vaak ergeren als een drone langere tijd boven hen vliegt, vooral als dit boven hun privé-eigendom gebeurt,[330] maar ook als dit gebeurt in de natuur of in de stedelijke openbare ruimte. Dan kan de bepaling over hinderlijk gedrag op openbare plaatsen in de APV een relevante en waardevolle aanvulling zijn op de bestaande strafrechtelijke en civielrechtelijke bepalingen.

Terwijl de tekst van deze bepaling in de model-APV slechts één lid bevat, hebben alle voor dit rapport onderzochte APV's (d.w.z. Amsterdam, Rotterdam, Utrecht en Westvoorne) bepalingen met een dergelijke of een vergelijkbare titel met meerdere leden en verschillende inhoud. Zoals uit het Westvoorne-amendement met betrekking tot deze bepaling volgt, is hier met name één sub-lid relevant. In het geval van de APV's Rotterdam en Westvoorne is dit sub b van het eerste lid. De bepaling in APV Amsterdam is echter anders en vereist een andere analyse.

a) APV Utrecht en APV Rotterdam

Ondanks enkele stilistische verschillen hebben de relevante subparagrafen in de APV's van Utrecht en Rotterdam dezelfde inhoud; daarom zullen ze samen worden bekeken.

Beide bepalingen verbieden gedrag dat overlast of ongemak veroorzaakt voor anderen in de openbare ruimte of voor gebruikers en bewoners van gebouwen in de buurt. In de APV Rotterdam wordt gesproken over 'weg', maar dit wordt zeer breed opgevat en omvat in principe alle soorten openbare ruimten, waaronder parken, pleinen, straten en bossen.[331]

APV Utrecht

Artikel 2:27 Hinderlijk gedrag op openbare plaatsen

1. *Het is verboden: (…)*
    b. *zich op een openbare plaats zodanig op te houden dat aan gebruikers van de openbare plaats of gebruikers of bewoners van nabij de openbare plaats gelegen woningen onnodig overlast of hinder wordt veroorzaakt (…).*

APV Rotterdam

[330] Neem bijvoorbeeld de gemeenschap in Kinderdijk.
[331] Artikel 1:1 (1) APV Rotterdam.

Artikel 2:47 Hinderlijk gedrag op openbare plaatsen

1. *Het is verboden: (…)*
    b. *zich op of aan de weg zodanig op te houden dat aan weggebruikers of gebruikers van nabij de weg gelegen gebouwen onnodig overlast of hinder veroorzaakt wordt;*

Volgens de toelichting van de APV Utrecht is het eerste lid, onder b, met name van belang. Dit onderdeel biedt de mogelijkheid om op te treden tegen personen en groepen die door hun gedrag hinder veroorzaken voor derden. In de toelichting wordt uitgelegd dat deze sub-paragraaf niet gericht is op actief gedrag (zoals straatschenderij, belemmering in vrijheid van beweging of hinderlijk opdringen of volgen, nachtrustverstorend rumoer en burengerucht; dat is geregeld in Art. 2:2 - verstoring van de openbare orde) maar tegen meer passief gedrag dat toch vervelend is, bijvoorbeeld het in een groepje bij elkaar zitten. Als zodanig zou deze sub-paragraaf inderdaad een geschikte voorziening kunnen zijn om de overlast aan te pakken die wordt veroorzaakt door het vliegen van drones in de openbare ruimte, zowel bij het observeren van anderen in de openbare ruimte als in gebouwen, ook in gevallen waarin dit vliegen eerder als 'passief' gedrag zou kunnen worden opgevat.

Zonder verdere aanwijzingen over wat onder het toepassingsgebied van deze bepaling zou vallen, kunnen we niet definitief concluderen dat deze bepaling gebruikt zou kunnen worden om personen te verbieden hun drones te vliegen met mogelijke ladingen en met constant gezoem in de openbare ruimte. Indien de bepaling ruim zou worden geïnterpreteerd, lijkt een dergelijke conclusie wel mogelijk.

b) APV Westvoorne

Zoals gezegd heeft de APV Westvoorne ook de bepaling over 'hinderlijk gedrag op openbare plaatsen' aangepast om de overlast en spionage door het recreatief vliegen van drones aan te pakken. Concreet wijzigde de APV Westvoorne lid 1, onder b, door het volgende toe te voegen: ‘al dan niet met gebruikmaking van instrumenten, toestellen of machines’. De bepaling luidt nu als volgt:

Artikel 2:47 Hinderlijk gedrag op openbare plaatsen

1. *Het is verboden op een openbare plaats: (..)*
    b. *zich, al dan niet met gebruikmaking van instrumenten, toestellen of machines, op te houden op een wijze die aan andere gebruikers of aan bewoners van nabij die openbare plaats gelegen woningen onnodig overlast of hinder berokkent.*

Volgens lid 1, onder b, is het nu verboden zich in de openbare ruimte, met of zonder gebruik van instrumenten, apparaten of machines, te gedragen op een wijze die overlast of ongemak veroorzaakt voor andere gebruikers van de openbare ruimte of voor bewoners van nabije woningen. Gezien het strafrechtelijke karakter van deze bepaling draagt het specificeren van de mogelijke oorzaak van overlast door het gebruik van instrumenten, apparaten of machines bij aan de in het strafrecht vereiste rechtszekerheid en voorzienbaarheid. In de toelichting bij de APV kunnen echter aanvullende aanwijzingen worden gegeven over de mogelijke toepasselijkheid van deze bepaling op drones.

c) APV Amsterdam

De APV Amsterdam heeft geen algemene bepaling over ‘hinderlijk gedrag op openbare plaatsen’. De dichtstbijzijnde bepalingen kan gevonden worden in Artikel 2.18: ‘hinderlijk gedrag in of bij gebouwen’.

Artikel 2.18 Hinderlijk gedrag in of bij gebouwen

1. *Het is anderen dan de bewoners of gebruikers van een gebouw of vaartuig verboden:*
    a. *zonder redelijk doel tegen een deur, raam of vensterbank te leunen of zich anderszins hinderlijk op te houden in de onmiddellijke omgeving van dat gebouw of vaartuig;*
    b. *zonder redelijk doel of op voor anderen kennelijk hinderlijke wijze zich op te houden in de voor gemeenschappelijk gebruik bestemde ruimten van dat gebouw.*
2. *Het is verboden zonder redelijk doel of op voor anderen kennelijk hinderlijke wijze zich op te houden in of bij een portiek, een portaal, een telefooncel, een parkeergarage of een soortgelijke, voor publiek toegankelijke ruimte dan wel deze ruimte te verontreinigen of te gebruiken voor een ander doel dan waarvoor zij is bestemd.*

Het meest vergelijkbare deel van de bepaling is te vinden in het tweede lid, dat verbiedt om zich te gedragen op een manier die duidelijk vervelend is voor anderen in of bij een portiek, een portaal, een telefooncel, een parkeergarage, een bushalte of een soortgelijke ruimte die toegankelijk is voor het publiek. Deze bepaling is vooral van toepassing op "passief" gedrag, zoals het doelloos rondhangen van personen of groepen in ruimten die bestemd zijn voor het publiek, wat kan leiden tot sterke gevoelens van onbehagen en onveiligheid, waardoor het normale gebruik van deze ruimten wordt belemmerd. Door gebruik van het woord ‘kennelijk’ kan zo nodig tegen hinderlijk gedrag in publieksruimten worden opgetreden zonder dat daarover door belanghebbenden is geklaagd.

Net als de bepaling in de model-APV is de reikwijdte van dit lid dus beperkt tot openbare ruimten met een specifieke functie, zoals de bushalte of een parkeergarage. Deze paragraaf lijkt dan ook niet bijzonder geschikt om de overlast van drones die over de 'algemene' openbare ruimte vliegen, zoals straten of parken, aan te pakken.

He eerste lid, onder a, zou echter voor dit doel kunnen worden gebruikt. Met name het laatste deel van deze bepaling, "zich op een anderszins vervelende manier te gedragen in de onmiddellijke nabijheid van een gebouw of vaartuig", kan van belang zijn. Net als in het geval van de APV Westvoorne is de bepaling duidelijk beperkt tot de overlast voor personen in een gebouw of vaartuig; overlast voor personen in de openbare ruimte valt buiten de reikwijdte. De reikwijdte van de bepaling is hier dus beperkter dan in het geval van de APV's van Utrecht en Rotterdam, en kan niet worden gebruikt door personen die zich ergeren aan het vliegen van drones om hen heen in de openbare ruimte.

In de toelichting bij de APV Amsterdam wordt echter ingegaan op de openheid van het begrip 'hinderlijk' gedrag:

> 'Hoewel het uit oogpunt van rechtszekerheid gewenst is om voorschriften zo specifiek mogelijk te formuleren, is het in sommige situaties echter onvermijdelijk dat gewerkt wordt met regels die een algemene typering van het verboden gedrag inhouden, omdat er een zo grote variëteit is aan gedragingen die de delictsomschrijving kunnen vervullen, dat het praktisch niet mogelijk is om deze concreet op te sommen.'

Dit zou een aanwijzing kunnen zijn dat een dergelijke bepaling wel kan worden gebruikt als een middel tegen het vervelende vliegen van drones, zij het beperkt tot het geografische toepassingsgebied van de bepaling.

5.5.4 Vergunningsplicht voor fysieke spyshops

Een andere mogelijk relevante gemeentelijke bepaling voor het doel van dit onderzoek is het vereiste van een vergunning voor het runnen van een fysieke spionagewinkel (dat wil zeggen fysieke winkels die gespecialiseerd zijn in de verkoop van spionageproducten in enge zin). Deze bepaling is in september 2019 ingevoerd in de APV van Amsterdam en blijft, voor zover ons bekend op het moment van schrijven van dit rapport, het enige voorbeeld van een dergelijke eis.

De burgemeester kan op grond van artikel 2.16A van de APV een gebied, straat of gebouw aanwijzen waarin het verboden is zonder vergunning als bedoeld in artikel 3.64 van de APV bepaalde categorieën bedrijfsmatige activiteiten uit te oefenen die naar haar oordeel de openbare orde verstoren, het woon- en leefklimaat aantasten of anderszins ondermijning veroorzaken.

Artikel 2.16a Aanwijzing als gebied, straat of gebouw waar vergunningplicht geldt voor bepaalde bedrijvigheid

1. *De burgemeester kan een gebied, straat of gebouw aanwijzen waarin het is verboden om zonder vergunning als bedoeld in artikel 3.64 bepaalde categorieën bedrijfsmatige activiteiten uit te oefenen die naar zijn oordeel de openbare orde verstoren, het woon- en leefklimaat aantasten of anderszins ondermijning veroorzaken.*
2. *Hij wijst in het besluit de activiteiten aan waarvoor de vergunningplicht geldt en geeft desgewenst aan welke specifieke voorwaarden aan de vergunningplicht worden verbonden.*
3. *De burgemeester kan de aanwijzing intrekken zodra deze bedrijfsmatige activiteiten naar zijn oordeel niet langer de openbare orde verstoren, het woon- en leefklimaat aantasten of anderszins ondermijning veroorzaken.*

Om georganiseerde en ondermijnende criminaliteit te voorkomen, te ontwrichten en te beëindigen, besloot de burgemeester van Amsterdam om dergelijke vergunningen te eisen voor het runnen van spionagewinkels in Amsterdam (zodat bijvoorbeeld iemand met een strafblad geen vergunning zou krijgen om een spyshop te runnen).[332] Volgens de lokale politie worden de – op zich legale – producten die in de spyshops te koop zijn (dat wil zeggen spionageproducten in enge zin) vaak door misdadigers gekocht en gebruikt voor zware criminaliteit en buitensporig geweld.[333] Bovendien hebben spyshops veel criminele klanten, aan wie ze de anonimiteit garanderen en die grote hoeveelheden contant geld verwerken. De lokale politie beschouwt de spionage-industrie dan ook als faciliterend voor de georganiseerde en ondermijnende criminaliteit met een risico op incidenten op het gebied van de openbare orde. Volgens de gemeente Amsterdam maakt het besluit om de bedrijfsactiviteiten van spyshops te onderwerpen aan een vergunningsplicht het mogelijk om toezicht te houden op de spionage-industrie en deze af te dwingen.[334]

Deze bepaling is echter beperkt tot fysieke spyshops, zodat dezelfde producten nog steeds beschikbaar zijn voor (legale) aankoop in webwinkels. Het doel van deze nieuwe eis is echter niet om een licentie te eisen voor alle verkopen van spionageproducten in enge zin (wat een belangrijk middel zou zijn om privacyrisico's van deze producten te beperken), maar om de georganiseerde misdaad aan te pakken, die vaak wordt gefaciliteerd door dergelijke fysieke winkels, die de criminele klanten anonimiteit geven. Deze ontwikkeling heeft dus geen invloed op het kopen van dezelfde producten bij online retailers door burgers die niet betrokken zijn bij

[332] Aanwijzingsbesluit vergunningsplicht voor spyshops, gemeente Amsterdam: https://zoek.officielebekendmakingen.nl/gmb-2019-224376.html.
[333] Ibid.
[334] Ibid.

(georganiseerde) criminaliteit. Een dergelijke regeling van online retailers zou de problemen echter niet oplossen, zeker gezien het geglobaliseerde bereik van het internet (waar men altijd spionageproducten kan bestellen bij een retailer uit een ander land).

5.5.5 Strafbepaling

Op grond van artikel 154 van de Gemeentewet kan de gemeenteraad op overtreding van zijn verordeningen straf stellen. Deze straf mag niet zwaarder zijn dan hechtenis van ten hoogste drie maanden of een geldboete van de tweede categorie, al dan niet met openbaarmaking van de rechterlijke uitspraak. In artikel 23 Sr zijn de maxima van de zes boetecategorieën opgenomen. Het maximum van een boete van de eerste categorie bedraagt EUR 435 en van de tweede categorie EUR 4.350.[335] Het is overigens uiteindelijk de strafrechter die de soort en de maat van de straf in een concreet geval bepaalt, tot de maximumgrens van de door de gemeenteraad gekozen boetecategorie. Hierbij dient de rechter op grond van artikel 24 Sr rekening te houden met de draagkracht van de verdachte. Het algemeen geldende minimum van de geldboete bedraagt EUR 3,00 (artikel 23, tweede lid, Sr).

Het bovenstaande is niet van toepassing op de schending van Art. 2.16A APV Amsterdam, dat wil zeggen het exploiteren van een spyshop zonder vergunning. Het tweede lid van artikel 1.6 APV Amsterdam regelt dat het niet-naleven van een voorschrift of een beperking een zelfstandige overtreding van de APV oplevert. Als reactie op deze overtreding zijn verschillende bestuursrechtelijke handhavingsinstrumenten beschikbaar, zoals het intrekken van een vergunning of een ontheffing. Strafrechtelijke handhaving is – via de strafbepalingen van hoofdstuk 6 APV – eveneens mogelijk.

5.5.6 Deelconclusie en discussie: mogelijke lacunes en reguleringsmogelijkheden

Op basis van bovenstaande discussie bieden we hier een samenvatting van de geïdentificeerde mogelijke lacunes (antwoord op deelvraag 4) en bespreken we verder de mogelijkheden voor hun regulering (antwoord op deelvraag 8).

Een APV kan bepalingen bevatten die een aanvulling vormen op die in het Wetboek van Strafrecht, wat vooral belangrijk is als het gaat om de bescherming van privacy in de openbare ruimte (die over het algemeen minder beschermd is in Sr in vergelijking tot privéruimten). Dit is echter afhankelijk van de specifieke bepaling zoals die door een bepaalde gemeente met haar eigen specifieke behoeften wordt uitgevoerd. In bovenstaande paragraaf zijn diverse verschillen in de reikwijdte van de bepalingen inzake spionage en overlast in de openbare ruimte vastgesteld.

---

[335] De tarieven worden echter elke twee jaar aangepast.

Met betrekking tot de bepalingen inzake spionage van burgers constateerden we verschillen, zowel wat betreft het type bewakingsapparatuur als wat betreft het type plaats dat binnen het toepassingsgebied valt. De model-APV (evenals de APV Utrecht) beperkt de reikwijdte van de bepaling (in het tweede lid) tot optische instrumenten, dat wil zeggen apparaten die visueel toezicht mogelijk maken, en tot particuliere verblijfplaatsen, zoals gebouwen en woonboten. Zo valt het bespioneren van iemand met een zoomlens in de openbare ruimte en zelfs besloten erven buiten de reikwijdte. Een dergelijke beperking kan wijzen op een mogelijke lacune. In APV's van Amsterdam, Rotterdam en Westvoorne vinden we een iets bredere reikwijdte. Aan de ene kant omvat de APV Amsterdam het gebruik van alle soorten bewakingsapparatuur, maar deze beperkt de plaats tot privéplekken, inclusief besloten erven. In Rotterdam daarentegen is de beperking tot optische instrumenten gehandhaafd, maar is de reikwijdte van de plaats specifiek uitgebreid naar de openbare ruimte, althans voor zover de eerbaarheid wordt aangetast of een inbreuk op de persoonlijke levenssfeer wordt gemaakt. Ten slotte heeft Westvoorne ook het toepassingsgebied van de bepaling over de plaats van de geobserveerde persoon verruimd met het privégebied rond niet-aaneengesloten gebouwen en landbouwgrond ('niet-openbaar toegankelijk gebied'). Deze gemeenten hebben dus gebruik gemaakt van de mogelijkheid om de bepaling aan te passen aan haar eigen behoeften.

In ieder geval met betrekking tot stedelijke gemeenten (in plaats van gemeenten waar landbouwgrond de overhand heeft) zou het misschien wenselijk zijn om het toepassingsgebied van de bepaling betreffende spionage uit te breiden tot spionage van personen in de openbare ruimte (met betrekking tot deelvraag 8). Dit zou inderdaad in overeenstemming zijn met het Wetboek van Strafrecht, in het bijzonder met Art. 441b, dat het heimelijke visuele toezicht op personen in de openbare ruimte al strafbaar stelt. Bovendien zou een dergelijke bepaling in de APV niet per se een vereiste van aantasting van de eer of de privacy hoeven te bevatten, zoals in de Rotterdamse APV wel het geval is. Een dergelijke inmenging is niet vereist volgens artikel 441b Sr, omdat de enkele daad van het heimelijk maken van afbeeldingen moreel onwenselijk wordt geacht. Een dergelijke bepaling in de APV zou dan inderdaad een aanvulling zijn op de bestaande bepaling in Sr, met name als 'heimelijke waarneming' ruimer opgevat - bijvoorbeeld het onopvallend opnemen van iemand met een smartphonecamera zonder actief te proberen dit te verbergen. Dit lijkt ons een goede reguleringsmogelijkheid, wat de regulering in de APV's meer in overeenstemming zou brengen met het strafrecht.

Verder zou met betrekking tot reguleringsmogelijkheden de beperking van het type bewakingsapparaat tot optische instrumenten kunnen worden afgeschaft, zoals dat het geval is in Amsterdam. Zoals in hoofdstukken 3 en 4 van dit rapport is besproken, kan de privacy van personen (ernstig) worden aangetast door een breed scala aan spionageproducten in enge en brede zin, niet alleen visueel. Terwijl Art. 139b Sr al strafbaar stelt voor het afluisteren en opnemen van gesprekken buiten privé-plaatsen, kan een aanvullende bepaling in de APV

wenselijk zijn, met name vanuit een praktisch perspectief. Aangezien het bespioneren van personen in de openbare ruimte over het algemeen wordt beschouwd als een geringere vorm van inbreuk op de persoonlijke levenssfeer, zou het minder waarschijnlijk kunnen leiden tot de handhaving van het strafrecht (het Openbaar Ministerie heeft immers de bevoegdheid om te beslissen welke zaken worden vervolgd en welke niet). Met betrekking tot reguleringsmogelijkheden (deelvraag 8), kunnen we constateren dat een administratieve vorm van bestraffing zoals hechtenis of een boete de handhavingsmogelijkheden zou kunnen versterken, ook wat betreft kleinere inbreuken op de persoonlijke levenssfeer. Daarbij moeten we ons ook realiseren dat de inbreuk op de persoonlijke levenssfeer in de openbare ruimte soms groot kan zijn.

Ten slotte maken APV's het ook mogelijk om drones te reguleren door middel van een bepaling over overlast in de openbare ruimte ('hinderlijk gedrag op openbare plaatsen'). Hoewel deze bepaling niet bijzonder relevant lijkt voor spionageproducten in enge zin (of andere spionageproducten in brede zin), wordt het vliegen van drones boven personen, inclusief het specifieke zoemende geluid dat ze produceren, vaak als zeer hinderlijk ervaren. Als zodanig kan deze bepaling een aanvullende basis bieden om het vliegen van drones te beperken (met betrekking tot deelvraag 8). Dit kan ook nuttig zijn als vangnet in gevallen waarin de drone zonder lading vliegt.

5.6 Luchtvaartwetgeving: drone regulering

De Europese Unie (EU) is begonnen met harmonisatie van luchtvaartregelgeving, wat tevens gevolgen zal hebben voor de regelgeving voor drones. Hierbij zal de European Union Aviation Safety Agency (EASA) een belangrijke rol spelen.[336] Deze harmonisatie is echter nog niet voltooid (ze zal met ingang van 1 juli 2020 ten uitvoer worden gebracht), dus op het moment van schrijven is de Nederlandse regelgeving nog van toepassing. In 2015 is reeds een verkennend onderzoek gepubliceerd naar het gebruik van drones (hierna ook: het drones-rapport 2015).[337] In onze beoordeling zullen we ons gedeeltelijk baseren op de bevindingen van dit rapport, maar gezien de veranderingen die voortvloeien uit de komende EU-verordening inzake drones, doen we dat in beperkte mate.

Hieronder wordt kort enige relevante wetgeving weergegeven die van toepassing is op (recreatief gebruik van) drones voor particulieren. Eerst zal gekeken worden naar regelgeving voor recreatief dronegebruik van Nederlandse bodem. Daarna zal gekeken worden naar de geldende Europese wetgeving, alsmede de komende Europese wetgeving. Noch op het niveau van de EU, noch op het niveau van de Raad van Europa bestaan er al relevante arresten over

[336] De website van de EASA: Easa.europa.nu.
[337] B.H.M Custers e.a., *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Amsterdam: Boom Lemma Uitgevers 2015.

drones. De Nederlandse uitspraken over drones en privacy zijn behandeld in de paragraaf over privaatrecht (par. 5.2.2). We beperken ons hier daarom tot de tekst van de regelgeving.

5.6.1 Huidige Nederlandse regelgeving over drones

De Wet luchtvaart is een belangrijke bron van luchtvaartwetgeving in Nederland, samen met het Besluit bewijzen van bevoegdheid voor de luchtvaart, het Besluit luchtvaartuigen 2008 en het Besluit luchtverkeer 2014. Daarnaast is voor recreatief gebruik van drones in het bijzonder de Regeling modelvliegen van belang.

a) Vluchteisen

In Nederland mag er niet met luchtvaartuigen gevlogen worden zonder een bewijs van bevoegdheid of zonder een bewijs van luchtwaardigheid van het luchtvaartuig op basis van de Wet luchtvaart.[338] Deze beperkingen gelden echter niet voor drones die gerekend worden tot modelluchtvaartuigen, zijnde luchtvaartuigen, niet in staat een mens te dragen, en uitsluitend gebruikt voor luchtvaartvertoning, recreatie of sport.[339] Modelluchtvaartuigen, mits niet zwaarder dan 25kg, worden immers uitgezonderd van deze beperkingen.[340]

Afgezien van de uitzondering op het verbod op vliegen zonder de nodige bewijzen, gelden er wel andere eisen voor het vliegen met (lichte) modelluchtvaartuigen c.q. drones.[341] Het karakter van deze regels is gericht op het waarborgen van de veiligheid, maar deze regels kunnen ook gevolgen hebben voor het waarborgen van het recht op privacy. Allereerst leidt de bovengenoemde limiet van 25kg tot op zeker hoogte tot een beperking van de mogelijkheden voor spionage met hobbydrones, maar dit betreft slechts een theoretische beperking, namelijk tegen het gebruik van uiterst geavanceerde en zware drones. Drones met spionage-capaciteiten hoeven bij lange na niet in de buurt van dit maximale gewicht te komen, zeker nu er steeds kleinere en lichtere sensoren op de markt beschikbaar zijn. Verder moet de drone gedurende de hele vlucht goed zichtbaar zijn voor de bestuurder, wat meebrengt dat de bestuurder van een drone die, bijvoorbeeld, gebruikt wordt om een ander te bespieden niet te ver weg kan zijn zonder in overtreding te zijn van de regels voor modelluchtvaart. Tevens mag er alleen overdag gevlogen worden.[342] Het feit dat drones beter zichtbaar zijn overdag komt niet alleen ten goede aan de veiligheid, maar ook aan het recht op privacy. Mensen zullen drones immers overdag sneller opmerken dan 's nachts. Daarnaast mag er niet gevlogen worden boven aaneengesloten bebouwing,[343] mensenmenigten en wegen, hoewel wegen in 30km-zones binnen de bebouwde

[338] Artikel 2.1 lid 1 & artikel 3.8 lid 1 Wet luchtvaart.
[339] Artikel 1 Regeling modelvliegen.
[340] Artikel 11 lid 1 Besluit bewijzen van bevoegdheid voor de luchtvaart en artikel 2 lid 2 Besluit luchtvaartuigen 2008.
[341] Artikel 2 Regeling modelvliegen.
[342] Dit is tevens opgenomen in artikel 18 lid 1 Besluit luchtverkeer 2014.
[343] Het Ministerie van Infrastructuur en Waterstaat omschrijft 'aangesloten bebouwing' als 'elk gebied in relatie tot stad, dorp of gehucht dat in belangrijke mate wordt gebruikt voor huisvesting, commerciële activiteiten of

kom en wegen in 60km-zones buiten de bebouwde kom een uitzondering vormen (over deze uitzondering meer in de volgende paragraaf).[344] Deze eisen brengen mee dat drones dus op een bepaalde afstand moeten blijven van mensen, wat tot op zekere hoogte de bescherming van het recht op privacy ten goede doet.

Deze eisen brengen mee dat drones dus op een bepaalde afstand moeten blijven van mensen, wat tot op zekere hoogte de bescherming van het recht op privacy ten goede komt. Deze ongespecificeerde 'veilige' afstand is echter wat betreft bescherming van privacy niet van grote betekenis als een drone is uitgerust met een HD-camera met zoomfunctie die het mogelijk maakt om beelden van hoge kwaliteit te maken vanaf 'veilige' afstand. Zoals blijkt uit onze interviews met hobbydronevliegers, zijn de meeste camera's op drones op dit moment niet van zo'n hoge kwaliteit dat ze enkele tientallen meters verderop duidelijke en gedetailleerde beelden kunnen weergeven; het perspectief van de observatie – van boven naar beneden (c.q. 'vogelvluchtperspectief) – beperkt ook wat er te zien is. Dit kan echter in de nabije toekomst veranderen, wanneer camera's en microfoons waarschijnlijk steeds krachtiger worden.

De bovengenoemde eisen bieden niet alleen een zekere mate van bescherming voor ruimtelijke en lichamelijke privacy (die vooral betrekking heeft op de privéruimte; denk aan gevallen waarin drones door de ramen in iemands appartement gluurden), maar ook voor de gedragsmatige en relationele privacy. Deze laatste twee typen spelen vooral bij drones die over openbare of semi-private ruimten vliegen en die het gedrag van mensen en interacties tussen mensen vastleggen.

Tenslotte mogen drones slechts tot 120m vliegen boven grond of water in luchtruim met klasse G.[345] Deze maximale hoogte van 120m brengt mee dat, zelfs met een HD-camera, het vogelvluchtperspectief dat door een drone geboden wordt in zekere (doch niet bijzonder HD) mate wordt beperkt. Een limiet van 300m wordt ook gehanteerd, doch slechts indien gevlogen wordt in verband met een vereniging die is aangesloten bij de Koninklijke Nederlandse Vereniging voor de Luchtvaart of de Federatie Limburgse Radio Controle Vliegers,[346] wat niet binnen de scope van dit onderzoek valt.

Wat betreft de uitzondering dat drones wel mogen vliegen boven wegen in 30km-zones binnen de bebouwde kom en wegen in 60km-zones buiten de bebouwde komen (uit art. 2 sub e Regeling Modelvliegen), is in het drones-rapport 2015 volgens ons terecht opgemerkt dat het onduidelijk is hoe wel op straat binnen een 30km-zone of in een achtertuin mag worden

---

recreatie (een zogenaamde congested area)', aldus: 'Particulier en recreatief gebruik van drones', Ilent.nl 13 april 2020.

[344] Artikel 2 sub e Regeling modelvliegen.

[345] De maximale vlieghoogte van 120m is opgenomen in artikel 2 Regeling Modevliegen, evenals de beperking tot klasse G luchtruim. Klasse G is het gedeelte van het luchtruim waarvoor vrijwel geen regels gelden. Op de volgende website van het kadaster wordt aangegeven waar het al dan niet is toegestaan om te vliegen met drones: Godrone.nl (overzichtskaart vliegen met drones).

[346] Artikel 2 sub i Regeling modelvliegen.

gevlogen, maar niet boven bebouwing of andere mensen. Er werd tevens afgevraagd of dan alleen in een rechte lijn naar boven gevlogen zou mogen worden.[347] Vermoedelijk is in de praktijk het antwoord op deze vraag 'nee', maar hier zijn door de rechter noch door de wetgever verdere uitlatingen over gedaan. Overtreding van bovenstaande eisen is op straffe van een hechtenis van ten hoogste zes maanden of een geldboete van ten hoogste de derde categorie.[348]

5.6.2 Europese regelgeving over drones

Wat betreft Europese regelgeving zijn in eerste instantie op alle luchtvaartuigen de regels voor de 'Single European Sky' van toepassing, dus ook op drones.[349] Recentelijk is echter Verordening (EU) 2018/1139 van kracht geworden, die betrekking heeft op burgerluchtvaart, waaronder het gebruik van civiele luchtvaart (inclusief recreatief dronegebruik door burgers), en die harmonisering van luchtvaartwetgeving binnen de EU bewerkstelligt: Verordening (EU) 2018/1139.[350] Het hoofddoel van deze verordening is het tot stand brengen van een hoog niveau van veiligheid.[351] De Verordening bevat derhalve veel regels die betrekking hebben op de veiligheid van het gebruik van onbemande luchtvoertuigen. In deze paragraaf worden alleen die regels besproken die indirect relevant zijn ook voor de bescherming van privacy. Deze Verordening moet tevens uitdrukkelijk bijdragen aan de eerbiediging van het privéleven en van het familie- en gezinsleven, en de bescherming van persoonsgegevens conform respectievelijk artikelen 7 en 8 Handvest van de Grondrechten van de Europese Unie (eerbiediging van het privéleven en bescherming van persoonsgegevens).[352] Daarnaast is in art. 56 lid 8 Verordening (EU) 2018/1139 opgenomen dat lidstaten ook nog nationale regels kunnen vaststellen om voorwaarden te verbinden aan het mogen vliegen met onbemande luchtvaartuigen, bijvoorbeeld ter bescherming van privacy en persoonsgegevens.

Deze nieuwe Europese wetgeving maakt geen onderscheid meer in recreatief of beroepsmatig gebruik van drones, zoals dat nu in Nederland (en in de meeste andere Europese landen) wel

---

[347] B.H.M Custers e.a., *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Amsterdam: Boom Lemma Uitgevers 2015, p. 94.
[348] Artikelen 5.5 & 11.9 lid 1 sub b onder 4 Wet luchtvaart en artikel 33 Besluit luchtverkeer 2014.
[349] Uitvoeringsverordening (EU) nr. 932/2012 van de Commissie van 26 september 2012 tot vaststelling van gemeenschappelijke luchtverkeersregels en operationele bepalingen betreffende luchtvaartnavigatiediensten en -procedures en tot wijziging van Uitvoeringsverordening (EU) nr. 1035/2011 en Verordeningen (EG) nr. 1265/2007, (EG) nr. 1794/2006, (EG) nr. 730/2006, (EG) nr. 1033/2006 en (EU) nr. 255/2010 (*PbEU* 2012, L 281).
[350] Verordening (EU) 2018/1139 van het Europees Parlement en de Raad van 4 juli 2018 inzake gemeenschappelijke regels op het gebied van burgerluchtvaart en tot oprichting van een Agentschap van de Europese Unie voor de veiligheid van de luchtvaart, en tot wijziging van de Verordeningen (EG) nr. 2111/2005, (EG) nr. 1008/2008, (EU) nr. 996/2010, (EU) nr. 376/2014 en de Richtlijnen 2014/30/EU en 2014/53/EU van het Europees Parlement en de Raad, en tot intrekking van de Verordeningen (EG) nr. 552/2004 en (EG) nr. 216/2008 van het Europees Parlement en de Raad en Verordening (EEG) nr. 3922/91 van de Raad (*PbEU* 2018 L 212) hierna: Verordening (EU) 2018/1139.
[351] Artikel 1 lid 1 Verordening (EU) 2018/1139.
[352] Overweging 28 Verordening (EU) 2018/1139.

nog wordt gedaan, maar maakt onderscheid op basis van het risiconiveau (vooral met betrekking tot veiligheid) van de vluchten.[353] Hierbij hangt het risico niet slechts af van het type machine en diens kenmerken (gewicht, snelheid, etc.) maar ook van de gebieden waarboven gevlogen wordt, de hoogte, de ervaring van de bestuurder, het soort vluchtuitvoering en de mogelijkheid van de bestuurder om te reageren op onvoorziene omstandigheden.[354] Overige factoren die herkend kunnen worden in de beschrijving van de verschillende klassen van onbemande luchtvaartuigsystemen zijn de maximale hoeveelheid energie die overgedragen kan worden bij een botsing met het menselijk hoofd, en de hoeveelheid elektrische spanning die op het luchtvaartuig mag staan alsmede het stroomstoot-gevaar als het luchtvaartuig beschadigd is.[355] Ten slotte wordt ook uitdrukkelijk de bescherming van privacy en de bescherming van persoonsgegevens (alsmede beveiliging en het milieu) genoemd bij de situaties wanneer een drone vlieger zich dient te registreren.[356] Met ingang van 1 juli 2020 zal Verordening (EU) 2018/1139 van kracht worden middels Uitvoeringsverordening (EU) 2019/947.[357] De huidige Nederlandse drone-wetgeving wordt dan vervangen door de Europese wetgeving.

a) Vluchteisen

Deze nieuwe Europese regelgeving is strenger dan de regelgeving die nu toepasselijk is in Nederland, zowel op het gebied van veiligheid als op het gebied van privacy, omdat er meer eisen verbonden zullen worden aan zowel de productie van de drones (bijvoorbeeld met betrekking tot bepaalde materialen die moeten worden gebruikt in relatie tot het unieke ID-nummer op de drone en privacy-by-design) als het uitvoeren van vluchten met drones.

Recreatief gebruik van lichte drones (met een maximaal gewicht van 25 kg) zal voortaan vallen onder de categorie ‘open’ vluchtuitvoering.[358] Echter, om in deze categorie te vallen moet een vluchtuitvoering aan een lijst van overige eisen genoemd in art. 4 Uitvoeringsverordening voldoen. Een piloot moet er bijvoorbeeld voor zorgen dat de drone op een veilige afstand blijft van mensen en niet over bijeenkomsten van mensen heen vliegt,[359] dat de drone te allen tijde in het zicht blijft (behalve wanneer deze vliegt in de ‘follow-me’ modus, waarin de drone kan worden ingesteld om autonoom de vlieger te volgen)[360] en dat de drone niet meer dan 120m boven de grond vliegt.[361] Dergelijke eisen zijn al bekend van de huidige Nederlandse wetgeving.

---

[353] Overweging 6 Uitvoeringsverordening (EU) 2019/947 van de Commissie van 24 mei 2019 inzake de regels en procedures voor de exploitatie van onbemande luchtvaartuigen (PbEU 2019 L 152), hierna: Uitvoeringsverordening (EU) 2019/947.
[354] Overweging G Europees Parlement (2015), *Veilig gebruik van systemen van op afstand bestuurde luchtvaartuigen (RPAS) op het gebied van burgerluchtvaart*, donderdag 29 oktober 2015.
[355] Bijlage Deel 1 sub 6 en Deel 2 sub 1 Gedelegeerde Verordening (EU) 2019/945 van de Commissie van 12 maart 2019 inzake onbemande luchtvaartuigsystemen en uit derde landen afkomstige exploitanten van onbemande luchtvaartuigsystemen (*PbEU* 2019 L 152), hierna: Gedelegeerde Verordening (EU) 2019/945.
[356] Overweging 14 & artikel 14 lid 1 Uitvoeringsverordening (EU) 2019/947.
[357] Artikel 23 lid 1 Uitvoeringsverordening (EU) 2019/947.
[358] Artikelen 3 & 4 Uitvoeringsverordening (EU) 2019/947.
[359] Artikel 4 lid 1 sub c Uitvoeringsverordening (EU) 2019/947.
[360] Artikel 4 lid 1 sub d Uitvoeringsverordening (EU) 2019/947.
[361] Artikel 4 lid 1 sub e Uitvoeringsverordening (EU) 2019/947.

De genoemde ‘follow-me’-modus is echter nieuw. Deze modus houdt in dat het onbemande luchtvaartuig constant de piloot volgt binnen een vooraf bepaalde straal, zijnde maximaal 50 meter in de ‘open’ categorie.[362] De Verordening zwijgt over de bijzonderheden van deze modus, behalve dat de piloot weer de controle na het inschakelen van de modus moet kunnen hervatten.[363] Dit is opmerkelijk, want dit suggereert een volkomen vertrouwen in het correcte functioneren van deze modus en gaat voorbij aan mogelijkheden om een dergelijke modus te misbruiken (bijvoorbeeld een drone onopvallend rond laten vliegen in follow-me-modus met de camera ingeschakeld terwijl de piloot probeert zich onopvallend te gedragen). Deze ‘open’ vorm van dronegebruik is de enige die geen voorafgaande exploitatievergunning nodig zal hebben. De overige categorieën die bestaan zijn ‘specifiek’ en ‘gecertificeerd’, en zijn bedoeld voor commercieel gebruik van onbemande vluchtvoertuigen, gebruik van onbemande vluchtvoertuigen door de politie of privaat gebruik van onbemande vluchtvoertuigen met grotere drones. Vluchten met een hoger risiconiveau vallen onder deze categorieën. Het uitvoeren van dergelijke vluchten zonder een exploitatievergunning is dus niet toegestaan.

Een ander toevoeging van de nieuwe Europese regelgeving die nog niet bestaat in de Nederlandse wetgeving, is de registratieplicht. Ieder die met een drone van meer dan 250g, of een drone van minder dan 250g én een sensor die persoonsgegevens kan registreren, wil vliegen, zal zich dienen te registreren in het daartoe bestemde register (behalve indien het wordt beschouwd als speelgoed in de zin van Richtlijn 2009/48/EC).[364] Een dergelijk register van dronevliegers maakt het dan gemakkelijker om ook die vliegers te identificeren die inbreuk hebben gemaakt op de privacy van anderen. De nieuwe EU-verplichting om drones te registreren met elk type sensor dat persoonsgegevens kan vastleggen, beschermt verschillende soorten privacy, afhankelijk van wat er precies wordt waargenomen (de woning, het lichaam, het gedrag en/of de relaties), maar richt zich op de informationele privacy – dat wil zeggen de gevaren die voortkomen uit de mogelijkheid om alle soorten informatie die direct of indirect betrekking heeft op personen te registreren en te verspreiden. Het drone-register omvat: de volledige naam en geboortedatum van natuurlijke personen (of naam en identificatienummer voor rechtspersonen), het adres van de dronevlieger, het e-mailadres, telefoonnummer, nummer van de verzekeringspolis voor het luchtvaartuig (indien vereist volgens toepasselijke regelgeving) en de nodige vergunningen of certificaten (wat niet het geval zal zijn voor hobbydrones).[365] Dit brengt dus mee dat eenieder die een drone wil gebruiken die is uitgerust met een camera (of een ander type sensor dat persoonsgegevens kan registreren), zichzelf dient te registreren, ook als

---

[362] Bijlage A over subcategorie A1 Uitvoeringsverordening (EU) 2019/947 jo. Artikel 3 lid 30 Gedelegeerde Verordening (EU) 2019/945.
[363] Bijlage Deel 1 sub 7 en Bijlag Deel 2 sub 17 Gedelegeerde Verordening (EU) 2019/945.
[364] Artikel 14 lid 5 Uitvoeringsverordening (EU) 2019/947.
[365] Artikel 14 lid 2 Uitvoeringsverordening (EU) 2019/947. Bepaalde drones zelf zullen ook moeten worden geregistreerd (in een apart register), maar dit geldt alleen voor drones die zijn gecertificeerd, dit zijn zeer grote drones die over het algemeen niet relevant zijn voor hobbydronevliegers (Artikel 14 lid 3 & lid 7 Uitvoeringsverordening (EU) 2019/947).

het om niet-beroepsmatig gebruik van de drone gaat. De registratieplicht houdt ook in dat gebruikers het registratienummer op hun drone moeten weergeven (bijv. door een speciale sticker op hun drone te plakken).[366] Zo'n sticker heeft echter weinig zin als iemand een vliegende drone vanaf de grond observeert en het nummer niet kan onderscheiden.

Daarnaast dienen er regels opgesteld te worden voor de markering en identificatie van drones, hoewel niet iedere drone hiervoor in aanmerking komt.[367] Drones met een gewicht van minder dan 250 gram, ongeacht of ze een sensor hebben (drone met label C0),[368] zullen niet hoeven te worden voorzien van een uniek serienummer, maar alle drones met een hoger gewicht zullen wel een dergelijke verplichting hebben.[369] Gezien een gestage afname van het gewicht van hobbydrones met een camera of een andere sensor die op de markt komen (bijvoorbeeld een nieuw type DJI-drone met camera die 249g weegt),[370] kan dit worden gezien als een mogelijke lacune (met betrekking tot deelvraag 4). Deze beperking vloeit waarschijnlijk voort uit de perceptie van veiligheidsrisico's, waarbij wordt aangenomen dat kleine en lichte drones (tot 250 g) een zeer laag veiligheidsrisico vormen. Gezien mogelijke inbreuken op privacy, kan het echter beter zijn om de verplichting met betrekking tot een serienummer niet te beperken tot een bepaald gewicht, aangezien daarmee geen rekening wordt gehouden met de technologische vooruitgang (met betrekking tot deelvraag 8). Desalniettemin lost een uniek serienummer zonder een technologische oplossing voor het observeren ervan niet het probleem op van hoe burgers die een drone die in strijd met bovenstaande bepaling vliegt, hebben opgemerkt, de bestuurder kunnen identificeren of het serienummer kunnen bemachtigen.

Ten slotte dienen personen met een drone met een gewicht tussen de 250g en de 900g een online training theorie-examen af te leggen,[371] en dienen personen met een drone zwaarder dan 900g en lichter dan 4kg ook nog een aanvullend theorie-examen af te leggen en moeten zij verklaard hebben een praktische zelfopleiding voltooid te hebben.[372] Over het algemeen dienen deze middelen ertoe te voorkomen dat drones onrechtmatig gebruikt worden en dienen ze het gemakkelijker te maken om te kunnen optreden tegen iemand die vermoedelijk wel onrechtmatig gebruik maakt van een drone.

De Verordening geeft aan dat, indien dit nodig is om risico's ten aanzien van onder andere privacy en bescherming van persoonsgegevens te beperken, drones over functionaliteiten moeten beschikken die rekening houden met de principes van privacy en bescherming van

---

[366] Artikel 14 lid 8 Uitvoeringsverordening (EU) 2019/947.
[367] Overweging 13 Uitvoeringsverordening (EU) 2019/947.
[368] 'EU droneregels: in welke (sub)categorie kom je op 1 juli 2020 terecht?', Dronewatch.nl 13 april 2020.
[369] Artikel 6 lid 5 Gedelegeerde Verordening (EU) 2019/945.
[370] 'DJI introduceert Mavic Mini: drone van nog geen 250 gram met 30 minuten vliegtijd', Dronewatch.nl 13 april 2020.
[371] Bijlage A over subcategorie A1 Uitvoeringsverordening (EU) 2019/947.
[372] Bijlage A over subcategorie A2 Uitvoeringsverordening (EU) 2019/947.

persoonsgegevens 'by design' en 'by default'.[373] Wat betreft geografische zones is er al eerder gesproken over een 'geofencingsysteem' waardoor drones niet op bepaalde plekken kunnen komen (bijv. luchthavens en gevangenissen), wat niet alleen een middel zou kunnen zijn om de veiligheid te bewaken, maar ook om privacy te waarborgen.[374] Zo zouden bijvoorbeeld delen van stadscentra of overige toeristische attracties (zoals Kinderdijk), waar dronegebruik tot ernstige overlast of tot hoge inbreuk van de privacy (van verschillende types, vooral ruimtelijke, lichamelijke, gedragsmatige, relationele en informationele, afhankelijk van het type indringing) van anderen kan leiden, zouden simpelweg afgesloten kunnen worden. Daarnaast moet het mogelijk zijn om de drone, evenals de aard en het doel van de vlucht, te identificeren. Deze mogelijkheid is in het bijzonder van belang in de context van spionage met behulp van hobbydrones. Op deze technologische manieren moet verzekerd worden dat voorwaarden en verboden gehandhaafd kunnen worden, in het bijzonder die voorwaarden en verboden die verband houden met vluchten in bepaalde geografische zones, en voorbij bepaalde afstanden van de bestuurder.

Dit is klaarblijkelijk moeilijk om te handhaven, maar de Gedelegeerde Verordening noemt al een technische mogelijkheid (een voorbeeld van 'data protection by design') om identificatie op afstand toe te staan. Zo wordt er verwezen naar een systeem voor 'directe identificatie op afstand' waarmee zonder fysieke toegang drones geïdentificeerd kunnen worden.[375] Dit systeem zendt het registratienummer van de bestuurder uit, het unieke serienummer van de het luchtvaartuig, de geografische positie van het luchtvaartuig, het traject, en de geografische positie van de piloot of, indien niet beschikbaar, het opstijgpunt.[376] Tevens moet het systeem gebouwd zijn om ervoor te zorgen dat de bestuurder de genoemde gegevens niet kan wijzigen.[377] In de praktijk wordt gewerkt aan verschillende systemen voor directe identificatie op afstand via een smartphone-app, gebaseerd op het Bluetooth-protocol en Wi-Fi-protocollen.[378] Deze mogelijkheid zal, mits goed geïmplementeerd, het benaderen van een drone-bestuurder in geval van verdenking van spionage of ander onrechtmatig handelen sterk moeten versimpelen.

---

[373] Bijlage IX 1.3 Verordening (EU) 2018/1139; Bedrijven/organisaties worden aangemoedigd om technische en organisatorische maatregelen te nemen, in de vroegste stadia van het ontwerp van de dataverwerkingsactiviteiten, zodat de beginselen van privacy en gegevensbescherming vanaf het begin worden gewaarborgd; bijv., het gebruik van pseudonimisering en encryptie ('data protection by design'). Bedrijven/organisaties dienen er standaard voor te zorgen dat persoonsgegevens met de hoogste privacybescherming worden verwerkt (bijvoorbeeld alleen de noodzakelijke gegevens dienen te worden verwerkt, korte opslagtijd, beperkte toegankelijkheid), zodat persoonsgegevens niet standaard voor een onbepaald aantal personen toegankelijk worden gemaakt ('data protection by default'). Zo moet een sociale-mediaplatform worden aangemoedigd om de profielinstellingen van gebruikers in de meest privacy-vriendelijke instelling te zetten door bijvoorbeeld de toegankelijkheid van het gebruikersprofiel vanaf het begin te beperken, zodat het niet standaard toegankelijk is voor een onbepaald aantal personen; zie 'What does data protection 'by design' and 'by default' mean?', Ec.europa.eu 13 april 2020.
[374] *Kamerstukken II* 2016/2017, 30 806, nr. 41, p. 5 en *Aanhangsel Handelingen II* 2017/18, 520, p. 2.
[375] Artikel 3 lid 31 Gedelegeerde Verordening (EU) 2019/945.
[376] Bijlage Deel 2 sub 17 onder b Gedelegeerde Verordening (EU) 2019/945.
[377] Bijlage Deel 2 sub 17 onder c Gedelegeerde Verordening (EU) 2019/945.
[378] News Byte, 'Intel Advances the Safe Integration of Drones into US Airspace', Newsroom.intel.com 13 april 2020. '*DJI Demonstrates Direct Drone-To-Phone Remote Identification'*, Dji.com 13 april 2020.

Het beschikken over een dergelijk systeem is niet gekoppeld aan het type vluchtuitvoering, maar aan de classificatie van het luchtvaartuig. Alle categorieën onbemande luchtvaartuigen, behalve de categorie drones van minder dan 250g (ongeacht of ze een sensor hebben), moeten een dergelijk systeem bevatten.[379] Dit zou echter betekenen dat een drone met sensor van minder dan 250g niet een systeem voor directe identificatie op afstand hoeft te hebben, wat een mogelijke lacune betekent (met betrekking tot deelvraag 4). Om deze beperking te ondervangen, zou het wenselijk kunnen zijn om de toepassing van een dergelijk identificatiesysteem op afstand ook uit te breiden tot drones met sensoren die persoonlijke gegevens kunnen vastleggen (met betrekking tot deelvraag 8).

Tot slot moet nog opgemerkt worden dat, indien een drone persoonsgegevens vastlegt, de Algemene Verordening Gegevensbescherming van toepassing is, hoewel men er bedacht op moet zijn dat indien deze gegevens zijn vastgelegd bij enkel recreatief dronegebruik hiervoor mogelijk de uitzondering voor zuiver persoonlijke of huishoudelijke activiteit kan gelden (zie paragraaf 5.1 over grondrechten en gegevensbescherming).[380]

5.6.3 Deelconclusie en discussie: mogelijke lacunes en reguleringsmogelijkheden

Op basis van bovenstaande discussie bieden we hier een samenvatting van de geïdentificeerde mogelijke lacunes (antwoord op deelvraag 4) en bespreken we verder de mogelijkheden voor hun regulering (antwoord op deelvraag 8).

Met inachtneming van de komende Europese regelgeving inzake drones kan men spreken van zowel lacunes als van verschillende mogelijkheden tot nadere bescherming van de privacy, waaronder mogelijkheden voor verdere regelgeving op nationaal niveau die deze verordeningen met zich meebrengen. Hoewel de meeste regels met betrekking tot drones in de eerste plaats gericht zijn op het waarborgen van veiligheid, kunnen ze toch een belangrijk effect hebben op de privacybescherming.

Met betrekking tot reguleringsmogelijkheden (deelvraag 8), bepaalt Art. 56 (8) Verordening (EU) 2018/1139 dat de lidstaten ook nationale regels kunnen vaststellen voor het vliegen met drones om de privacy en persoonsgegevens te beschermen. De Gedelegeerde Verordening (EU) 2019/945 introduceert zelf echter al een aantal nieuwe verplichtingen die deze doelen dienen. Ten eerste wordt een nieuwe registratieplicht ingevoerd voor eigenaars die willen vliegen met drones van meer dan 250 gram, alsook met drones van minder dan 250g met een sensor die persoonsgegevens kan vastleggen. Het instellen van een register van dronevliegers verbetert

[379] Zie bijvoorbeeld Bijlage Deel 2 sub 12 Gedelegeerde Verordening (EU) 2019/945.
[380] *Artikel 2 lid 2 sub c Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (PbEU 2016 L 119) (algemene verordening gegevensbescherming).*

volgens ons de identificatiemogelijkheden van dronevliegers die hun drone tegen de regels vliegen (bijv. over drukke stedelijke gebieden of achtertuinen), wat relevant is in het licht van de privacy van personen (voornamelijk op gedragsmatig, relationeel, ruimtelijk en lichamelijk gebied). Als gemaakte beelden vervolgens online zijn gezet of op een andere manier zijn verspreid, kan ook de informationele privacy in sterkere mate zijn aangetast.

Niet alle nieuwe verplichtingen gelden echter voor drones onder de 250 gram, zelfs niet als ze een sensor hebben. Terwijl de meeste drones met een type sensor, vooral een camera, op dit moment meer dan 250g wegen, zal dit naar verwachting in de nabije toekomst veranderen (dit is al het geval met de eerdere genoemde DJI-drone met camera van 249 gram).[381] Dit leidt dus tot een aantal mogelijke lacunes. De verplichte online cursus en examen gelden bijvoorbeeld niet voor dergelijke drones, ook al is dit misschien een goede manier om dronevliegers bewust te maken van hun mogelijke impact op de privacy van anderen. Drones onder de 250g zijn ook niet verplicht om een uniek serienummer te hebben. Bovendien is de technische mogelijkheid van 'directe identificatie op afstand' niet voorzien voor dergelijke drones.

Betreffende de reguleringsmogelijkheden, zou het wenselijk zijn om dergelijke eisen ook verplicht te stellen voor drones onder de 250 gram met een sensor die persoonlijke gegevens kan registreren, omdat daarmee de dronevlieger die inbreuk maakt op de persoonlijke levenssfeer beter kan worden geïdentificeerd. Bovendien zouden er aanvullende technische maatregelen (in de zin van privacy en gegevensbescherming 'by design en by default') kunnen worden genomen om de drone (en daarmee de eigenaar) daadwerkelijk herkenbaar te maken voor burgers of wetshandhavers op de grond. In dit verband wordt in de Gedelegeerde Verordening (EU) 2019/945 al melding gemaakt van een technische mogelijkheid om identificatie op afstand mogelijk te maken. Er wordt gesteld dat in elke drone met een gewicht van meer dan 250 gram een 'direct identificatiesysteem op afstand' moet worden ingebouwd, dat het registratienummer van de piloot, het unieke serienummer van de drone, de geografische positie, het traject en de geografische positie van de piloot (of, indien niet beschikbaar, het opstijgpunt) kan doorgeven, op een manier dat de piloot de genoemde gegevens niet kan wijzigen. In de praktijk wordt al gewerkt aan verschillende systemen voor dergelijke directe identificatie op afstand via een smartphone-app, gebaseerd op het Bluetooth-protocol en WiFi-protocollen. Deze mogelijkheid zal, mits goed geïmplementeerd, het confronteren van een drone-bestuurder in geval van verdenking van spionage of ander onrechtmatig handelen sterk moeten versimpelen. Gezien de bestaande en naar verwachting toenemende toekomstige drones met een sensor die minder dan 250 g wegen, lijkt de verplichte toepassing van een dergelijk systeem ook op deze drones misschien wenselijk (deelvraag 8). Er moet echter worden opgemerkt dat een dergelijke technische eis op zich ook een verstoring van de privacy kan zijn; de positie van de

[381] De MAVIC-mini van DJI: 'Mavic mini The everyday flycam', Dji.com 13 april 2020.

desbetreffende dronevlieger wordt immers voortdurend geregistreerd en doorgegeven. Een dergelijk systeem moet dus op proportionele wijze worden toegepast.

Met name met betrekking tot privacy-by-design en privacy-by-default is er ruimte om (vooral inter- en supranationale) standaarden te ontwikkelen met betrekking tot drones. Bestaande suggesties voor geo-fencing kunnen ook worden uitgevoerd voor bepaalde soorten plaatsen waar niet alleen veiligheid voorop staat (bijvoorbeeld luchthavens, gevangenissen), maar waar ook privacy een belangrijk aandachtspunt is, bijvoorbeeld bij bepaalde toeristische attracties zoals Kinderdijk.

6 Inventarisatie van andere reguleringsopties in het binnen- en buitenland

In dit hoofdstuk richten wij onze blik op de deelvragen uit Deel 2 en 3 over de inventarisatie van praktische waarborgen van bedrijven en organisaties, overheidsregulering uit het buitenland en mogelijke aanvullende reguleringsopties voor Nederland. Wij verkennen daarvoor hoe bedrijven, burgers en overheden van andere landen de mogelijke privacyrisico's van spionageproducten in de horizontale relatie trachten te beperken.

In paragraaf 6.1 en 6.2 adresseren wij vraag 5 en 7: *Met betrekking tot overheidsregulering: hoe trachten de ons omringende landen om privacy-inbreuken door het gebruik van spionageproducten door burgers te voorkomen of te beperken via vergunningstelsels of andere vormen van overheidsregulering? Welke maatregelen zijn succesvol en welke niet?* En: *Zijn er buiten de ons omringende landen nog interessante voorbeelden te vinden van succesvolle of juist mislukte vormen van overheidsregulering of zelfregulering om privacy-inbreuken door spionageproducten te voorkomen of te beperken?*

Zoals beschreven in paragraaf 2.5.2 hebben wij ervoor gekozen, om Duitsland en Frankrijk te belichten ter beantwoording van deze deelvragen, omdat uit de Internet quickscan bleek dat deze landen voorbeelden geven van regulering van spionageproducten in enge zin die in Nederland niet bestaan. Paragraaf 6.1 belicht Frankrijk als enige land met een vergunningsregeling voor specifieke soorten spionageproducten in enge zin (vraag 5). Duitsland staat centraal in paragraaf 6.2 als enige land met een verbod op de verkoop, distributie, het bezit en de reclame voor specifieke soorten spionageproducten in enge zin (beide als gevolg van onze beperkte internetquickscan) (vraag 7). Bij de beantwoording van beide vragen blikken wij ook al vast vooruit naar de mogelijke oplossingsrichtingen voor het Nederlandse beleid en geven daarmee alvast een aanzet voor het antwoord op deelvraag 8. De analyse in beide paragrafen hebben wij uitgevoerd middels klassiek juridisch-dogmatisch onderzoek en analyse van wetenschappelijke literatuur (zie par. 2.5.1). Voor hobbydrones als spionageproducten in brede zin hebben wij op basis van de Internet quickscan naar internationale wetgeving geen interessante voorbeelden kunnen vinden van overheidsregulering (zie paragraaf 2.2.3).

In paragraaf 6.3 richten wij onze blik op de praktische waarborgen die bedrijven en organisaties hebben ontwikkeld ter beperking van de privacyrisico's in horizontale relaties van zowel spionageproducten in enge zin als hobbydrones. In deze paragraaf beantwoorden wij aldus vraag 6: *Wat zijn succesvolle, praktische waarborgen van binnen- en buitenlandse bedrijven en organisaties om privacy-inbreuken door spionageproducten te voorkomen of te beperken? En waarom zijn andere waarborgen niet succesvol?* Hierbij hebben wij ons gebaseerd op de literatuurstudie, de interviews en focusgroepen (zie hoofdstuk 2).

6.1 Het Franse vergunningenstelsel voor sommige soorten spionageproducten[382]

Het Franse vergunningenstelsel voor spionageproducten is vastgelegd in het Franse Wetboek van Strafrecht (CP; Code pénal). In deze paragraaf beantwoorden we deelvraag 5. Het vergunningenstelsel kan worden gekwalificeerd als een tweeledig systeem. De eerste relevante bepaling is art. 226-3 CP. Dit artikel heeft betrekking op een aantal producten en apparaten die mondelinge gesprekken kunnen opnemen, elektronische communicatie kunnen onderscheppen of computergegevens kunnen vastleggen. Dit zijn de soorten spionageproducten in enge zin. Het op de markt brengen, verkopen, verhuren, verwerven, bezitten of gebruiken van deze producten wordt geregeld door middel van een vergunningsregeling of een ex ante toestemmingsregeling.

Het gebruik van art. 226-3 CP wordt echter beperkt door het Wetboek van Strafrecht. Met name door een aantal bepalingen die het recht op privéleven en de daarmee samenhangende rechten vastleggen. Art. 226-1 verbiedt inbreuken op het recht op privéleven, en in het bijzonder het opnemen van privégesprekken of het vastleggen van beelden in privéruimtes. In dit verband is art. 226-3 een verzwarende omstandigheid: wanneer de overtreding wordt begaan met een van de apparaten die onder art. 226-3 vallen, zullen de straffen aanzienlijk hoger zijn. In die zin voorziet art. 226-3 zowel in een op zichzelf staande vergunningsregeling voor spionageproducten als in een aanvullend verbod op - de handeling van - spionage, waarvan de reikwijdte grotendeels wordt bepaald door art. 226-1. Wat bepaalde vormen van privacy betreft, wordt de belangrijkste bescherming geboden aan de communicatieve privacy (met betrekking tot de opname van privégesprekken) en de ruimtelijke en lichamelijke privacy (met betrekking tot het vastleggen van beelden in privéruimtes). Deze bescherming heeft echter ook betrekking op de gedragsmatige en relationele privacy, die ook door een dergelijke observatie kunnen worden beïnvloed.

6.1.1 Art. 226-1: een algemeen verbod op inbreuken op de persoonlijke levenssfeer en daarmee verband houdende bepalingen

Art. 226-1 is de algemene bepaling van het Wetboek van Strafrecht die het recht op privéleven handhaaft. Dit artikel straft met een jaar gevangenisstraf en een boete van 45.000 euro iedereen die vrijwillig en op welke manier dan ook inbreuk maakt op de intimiteit van het privéleven van andere mensen. Meer in het bijzonder definieert het artikel ook de soorten handelingen die als een inbreuk gelden. Het gaat onder meer om het volgende:

- het vastleggen, opnemen of doorgeven, zonder toestemming van de auteur, van woorden die privé of vertrouwelijk zijn gesproken;[383] en

[382] Vertaling van bepalingen door R. Gellert en T. van Delden.
[383] Deze kunnen zowel in de privé- als in de openbare ruimte worden uitgesproken, zie 'Atteintes à la vie privée', Cabinetaci.com 14 april 2020.

- het vastleggen, opnemen of doorgeven, zonder toestemming van deze laatste, van het beeld van een persoon in een privéruimte.[384]

Op basis van de formulering van deze bepaling is het duidelijk dat de nadruk ligt op de bescherming van de meest intieme delen van het privéleven. In termen van de typologie van Koops et al. heeft dit vooral betrekking op het linker bovenste deel van de typologie: lichamelijke, ruimtelijke en communicatieve privacy, die we al hebben geïdentificeerd als de belangrijkste privacyrisico's die het gebruik van spionageproducten met zich meebrengt.

Art. 226-1 is het algemene verbod en wordt aangevuld met een aantal bepalingen. Zo kan men artikel 226-2 noemen. Dit artikel bepaalt dat het houden, dragen of aan het publiek bekendmaken (ook via de media) of aan derden of het op enigerlei wijze gebruiken van elke opname of elk document dat is verkregen door middel van een van de in art. 226-1 bedoelde handelingen, eveneens met dezelfde straf wordt bestraft.

Ook moet art. 226-15 worden genoemd, dat de geheimhouding van correspondentie waarborgt (die vaak wordt gezien als onderdeel van het recht op privéleven, zoals het geval is met art. 8 EVRM). Dit artikel straft met een gevangenisstraf van één jaar en een boete van 45.000 euro de volgende handelingen te kwader trouw: het openen, onderdrukken, vertragen of omleiden van al dan niet op de plaats van bestemming aangekomen en aan derden geadresseerde correspondentie, of het op frauduleuze wijze kennisnemen van de inhoud ervan. Dit geldt ook voor de uitvoering (te kwader trouw) van de volgende inbreuken op het elektronisch briefgeheim: het onderscheppen, omleiden, gebruiken of openbaar maken van elektronisch verzonden, verzonden of ontvangen correspondentie, of het installeren van apparaten die het mogelijk maken dergelijke onderscheppingen te realiseren.

6.1.2 Art. 226-3: de regulering van spionageproducten als verzwarende omstandigheid

Art. 226-3 is de bepaling die het gebruik van spionageproducten regelt. Het houdt rechtstreeks verband met art. 226-1 en art. 226-15. In beide gevallen werkt het als een verzwarende omstandigheid.

Volgens deze bepaling wordt, wanneer de in artikel 226-1 bedoelde strafbare feiten worden gepleegd met behulp van een technisch apparaat waarmee gesprekken op afstand kunnen worden gedetecteerd, de straf voor een dergelijke inbreuk verhoogd tot vijf jaar gevangenisstraf en een boete van 300.000 euro. De spionageapparaten die leiden tot de toepassing van deze bepaling zijn opgenomen in een lijst, die deel uitmaakt van een decreet (*Arrêté*), dat door de minister-president is aangenomen. Iedereen die een van deze toestellen vervaardigt, invoert,

[384] Het artikel gaat er ook van uit dat wanneer de in dit artikel bedoelde handelingen zijn verricht in de wetenschap en de wetenschap van de betrokkenen zonder dat zij daartegen bezwaar hebben gemaakt, ook al waren zij daartoe in staat, de instemming van de betrokkenen wordt verondersteld.

bezit, tentoonstelt, aanbiedt, verhuurt of verkoopt, moet hiervoor toestemming (d.w.z., een vergunning) hebben. Iedereen die met behulp van deze apparaten art. 226-1 overtreedt wanneer dergelijke handelingen buiten de grenzen van de vergunning vallen of niet zijn toegestaan, zal worden onderworpen aan de in deze bepaling voorziene sanctie.

Wat art. 226-15 betreft, heeft art. 226-3 betrekking op het gebruik van specifieke apparatuur voor het verstoren van elektronische communicatie. Artikel 226-3 verbiedt ook het gebruik van dergelijke apparaten voor het vastleggen van computergegevens zonder toestemming van het slachtoffer, zoals in het geval van keylogging, screenshot, enz., die vallen onder de artikelen 706-102-1 en 706-102-2 van het Franse Wetboek van Strafvordering. Bovendien straft artikel 226-3 ook het feit dat er reclame wordt gemaakt voor deze apparaten, wanneer de reclame kan worden opgevat als een aansporing tot het plegen van de in de artikelen 226-1 en 226-15 bedoelde strafbare feiten. Dit laatste deel van de bepaling was in 2017 in het geding bij de zogenaamde "Fireworld"-zaak. Dit bedrijf moedigde mensen aan om zijn spionageproducten te kopen om hun zonen te surveilleren om zo te ontdekken "of ze homo waren".[385]

6.1.3 Het vergunningenstelsel van art. 226-3 CP

Het Franse Wetboek van Strafrecht bestaat uit twee delen. Het wetgevende deel, dat de eigenlijke wettelijke bepalingen bevat, en het regelgevende/administratieve deel. Het laatste bevat de decreten die de wettelijke bepalingen aanvullen. De decretale bepalingen worden voorafgegaan door een "R" (bv. R. 226-1).

a) De lijst van spionageproducten

Volgens R. 226-1 maakt de in art. 226-3 bedoelde lijst deel uit van een besluit van de minister-president. Het betreft het "Decreet van 4 juli 2012 tot vaststelling van de lijst van apparaten en technische inrichtingen bedoeld in artikel 226-3 van het Wetboek van Strafrecht". Het werd gewijzigd op 1 oktober 2016 (een nieuwe wijziging wordt verwacht voor oktober 2021).[386] De uitvoering ervan is gedelegeerd aan het Nationaal Agentschap voor Cyberveiligheid – ANSSI (Agence nationale de la sécurité des systèmes d'information).[387]

Volgens art. 1 van het decreet is de lijst van apparaten waarvoor een vergunning overeenkomstig artikel 226-3 van het Wetboek van Strafrecht is vereist, opgenomen in Bijlage I bij het decreet. De lijst is opgenomen in Bijlage I, punt 2. Het is echter niet strikt genomen een lijst, zoals een lijst die een aantal specifieke hulpmiddelen zou bevatten. Het is meer een uitgebreide en diepgaande definitie van de soorten producten die in het geding zijn.

---

[385] Zie, 'La vente ou l'usage d'outils intrusifs face au droit français', Nextinpact.com 14 april 2020.
[386] Zie,' Arrêté du juillet 2012 fixant la liste d'appereils et de dispoitifs techniques prévue par l'article 226-3 du code pénal', Legifrance.gouv.fr.
[387] Decreet van 4 juli 2012 tot vaststelling van de lijst van apparaten en technische inrichtingen als bedoeld in artikel 226-3 van het wetboek van strafrecht, artikel 4.

Bijlage I, punt 2 richt zich op:

> ‘apparaten die speciaal zijn ontworpen om gesprekken op afstand te detecteren om, zonder medeweten van de spreker, de onderschepping, het afluisteren of de heruitzending van spraak, direct of indirect, met akoestische, elektromagnetische of optische middelen te realiseren, [waardoor] het mogelijk [wordt] om de overtreding van art. 226-1 van het Wetboek van Strafrecht te realiseren.’

De Bijlage specificeert deze lijst/uitgebreide definitie met de volgende hulpmiddelen/apparaten. Micro-zenderapparaten die de hertransmissie van de stem mogelijk maken via draadloze, optische of bedrade middelen, zonder medeweten van de spreker; toestellen voor het onderscheppen van geluid op afstand van het type microcanon of uitgerust met akoestische versterkingsapparaten; systemen voor het afluisteren van geluid op afstand via laserstralen.

Wanneer een apparaat op de lijst staat, hebben verkopers van dergelijke apparaten een periode van drie maanden om een licentie aan te vragen (R. 226-12). De Franse vergunningsplicht geldt dus alleen voor audio-spionageproducten in enge zin.

b) Het vergunningenstelsel

Volgens R. 226-1 verleent de minister-president de machtigingen/vergunningen. Ingevolge een decreet van 2 juni 2005 delegeert de minister-president zijn bevoegdheid tot het verlenen van vergunningen aan de secretaris-generaal van Landsverdediging. Hij wordt bijgestaan door een raadgevend comité (R. 226-2), waarvan het advies verplicht is (R. 226-3). Het is samengesteld uit een aantal vooraanstaande personen zoals de directeur-generaal van het Nationaal Agentschap voor Cyberveiligheid (of zijn vertegenwoordiger), alsook de vertegenwoordigers van verschillende ministeries (justitie, binnenlandse zaken, defensie, enz.) (R. 226-2).

De commissie kan deskundigen horen in de loop van het verlenen van de licentie. Een andere administratieve wet, de Instructie van 5 september 2006 betreffende het op de markt brengen en het verwerven of het vasthouden van apparatuur die inbreuk kan maken op de intimiteit van het privéleven of het geheim van correspondentie, vormt een aanvulling op de verschillende regelgevende/administratieve bepalingen van het Wetboek van Strafrecht.[388] Volgens artikel 3 van deze instructie moeten in ieder geval technische deskundigen worden geraadpleegd die nagaan of de technische bijzonderheden van het hulpmiddel overeenstemmen met het beoogde gebruik en of de aspirant-gebruiker zijn materiaal op adequate wijze heeft beschreven in zijn aanvraag voor een vergunning. Daarnaast is het verplicht om zogenaamde "moraaladviezen" over de aanvrager te verzamelen. Deze laatste worden afgegeven door verschillende ministeries, zoals die van justitie, binnenlandse zaken of defensie.

[388] Zie de preambule van deze instructie.

In het vergunningenstelsel wordt een onderscheid gemaakt tussen twee soorten vergunningen. Die welke betrekking hebben op de verkopers van apparaten, en die welke betrekking hebben op de kopers. In beide gevallen moet een vergunning worden verkregen (R. 226-3 en R. 226-7). De aanvragen voor beide soorten vergunningen moeten worden ingediend bij de directeur-generaal van de ANSSI. Deze eisen moeten een aantal elementen bevatten.

De verzoeken van de verkopers om een vergunning moeten voor elk apparaat de volgende elementen bevatten (R. 226-4):

> 1 ° De naam en het adres van de aanvrager, indien hij een natuurlijk persoon is, of zijn naam en zetel indien hij een rechtspersoon is;
>
> 2 ° De in artikel R. 226-3 genoemde transactie(s) waarvoor een vergunning wordt aangevraagd [d.w.z. vervaardiging, invoer, tentoonstelling, aanbieding, verhuur of verkoop] en de beschrijving van de betrokken contracten;
>
> 3 ° Het doel en de technische kenmerken van het type apparaat, vergezeld van een gedetailleerde technische documentatie met een beschrijving van:
>
> - de mogelijkheid om zonder toestemming van de auteurs woorden die onderhands of vertrouwelijk zijn gesproken vast te leggen, op te nemen of door te geven;
>
> - de mogelijke middelen van cryptologie die in de hardware zijn geïntegreerd of integreerbaar zijn;
>
> - de middelen en methoden om het ongeoorloofde gebruik van de apparatuur te voorkomen;
>
> 4 ° De plaats van vervaardiging van het apparaat of voor de andere in artikel R. 226-3 genoemde handelingen. In geval van invoer, de naam van het product van oorsprong, de handelsnaam en de plaats van vervaardiging;
>
> 5 ° De verbintenis om de nodige controles te ondergaan om na te gaan of de in de vergunningsaanvraag vermelde gegevens worden nageleefd. Om de daadwerkelijke band tussen de ondertekenaar van de verbintenis en de onderneming die aan de oorsprong van de aanvraag ligt te verifiëren, wordt het dossier aangevuld met een "K bis"-uittreksel van minder dan een maand.[389]

De aanvragen van de kopers (d.w.z. de verwerving of het bezit per R. 226-7) voor een vergunning moeten voor elk apparaat de volgende elementen bevatten (R. 226-8):

---

[389] In Frankrijk fungeert de K-bis als de identiteitskaart voor ondernemingen, zie ‘Extrait Kbis’, Infogreffe.fr 14 april 2020.

1 ° De naam en het adres van de aanvrager, indien hij een natuurlijk persoon is, of zijn naam en zetel indien hij een rechtspersoon is;

2 ° De in artikel R. 226-3 genoemde transactie(s) waarvoor een vergunning wordt aangevraagd [d.w.z. vervaardiging, invoer, tentoonstelling, aanbieding, verhuur of verkoop] en de beschrijving van de betrokken contracten;

3 ° Het doel en de technische kenmerken van het type apparaat, vergezeld van een gedetailleerde technische documentatie met een beschrijving van:

- de mogelijkheid om zonder toestemming van de auteurs woorden die onderhands of vertrouwelijk zijn gesproken vast te leggen, op te nemen of door te geven;

- de mogelijke middelen van cryptologie die in de hardware zijn geïntegreerd of integreerbaar zijn;

- de middelen en methoden om het ongeoorloofde gebruik van de apparatuur te voorkomen;

3 ° Het aantal apparaten voor het bezit waarvan de toestemming wordt gevraagd;

4 ° Het beoogde gebruik en het algemeen kader van gebruik;

5 ° De verbintenis om zich te onderwerpen aan de controles die nodig zijn om na te gaan of de in de vergunningsaanvraag vermelde gegevens in acht worden genomen.

Vergunningen kunnen worden verleend voor een periode van maximaal 6 jaar voor verkopers (R. 226-5), en voor kopers voor een periode van maximaal 3 jaar (R. 226-9). De vergunningen kunnen ook voorwaardelijk zijn. Voor verkopers kan de minister-president voorwaarden stellen aan de wijze waarop de verschillende verkooptransacties [d.w.z. productie, invoer, tentoonstelling, aanbieding, verhuur of verkoop] kunnen worden uitgevoerd, en het maximumaantal toegestane apparaten beperken (R. 226-5). Voor kopers kan de minister-president voorwaarden stellen aan het gebruik van de apparaten met het oog op het "voorkomen van misbruik" (R. 226-9). In beide gevallen wordt de vergunning automatisch verleend wanneer de aanvraag voor een vergunning wordt ingediend door staatsambtenaren binnen de grenzen van hun prerogatieven (R. 226-5 en R. 226-9).

Licenties kunnen op verzoek worden verlengd. Dergelijke verzoeken moeten ten minste drie maanden voor het einde van de licentie worden ingediend. Anders moet een verzoek om een nieuwe licentie worden ingediend (artikel 2, lid 2, van de Instructie van 5 september 2006).

Voor de licenties van de verkopers gelden ook aanvullende eisen. Volgens R. 226-6 moet elk apparaat dat is gefabriceerd, geïmporteerd, tentoongesteld, aangeboden, gehuurd of verkocht, voorzien zijn van een verwijzing naar de verleende licentie, alsmede van een uniek identificatienummer. Spionageproducten kunnen alleen worden verkocht aan actoren die ook een licentie hebben (hetzij als koper, hetzij als verkoper) (R. 226-10). Verkopers hebben ook een registratieplicht. Zij moeten een register bijhouden waarin alle handelingen met betrekking tot deze materialen worden getraceerd (R. 226-10). De kenmerken van het register worden verder uitgewerkt in het "Besluit van 16 augustus 2006 betreffende het register bedoeld in artikel R. 226-10 van het Strafwetboek".[390] Het register is een rooster in een notitieboekje dat door de licentiehouder moet worden ondertekend (art. 2).

Op basis van de bijlage van het decreet is hier een modelregister opgenomen:[391]

Datum van de transactie (A)	*[INFORMATIE INVOEGEN]*
Aard van de transactie (B)	[*INFORMATIE INVOEGEN*]
Beschrijving van het apparaat (d.w.z. wat voor een apparaat is het) (C)	[*INFORMATIE INVOEGEN*]
Identificatienummer van het apparaat (D)	[*INFORMATIE INVOEGEN*]
Licentienummer (E)	[*INFORMATIE INVOEGEN*]
Identificactie van de cliënt of de aanbieder (F)	[*INFORMATIE INVOEGEN*]
Verwijzing naar de eigen licentie van de cliënt/leverancier (G)	[*INFORMATIE INVOEGEN*]
Naam van de persoon die verantwoordelijk is voor de naleving van de vergunning (H)	[*INFORMATIE INVOEGEN*]

De naleving van de vergunningen is onderworpen aan controle (R. 226-4 en R. 226-8). In het kader van deze controles kan het register worden geïnspecteerd. Ook de toegang tot de apparaten is mogelijk. Ook de inspectie van de apparaat-beschrijving en de toegang tot relevante documentatie (zoals die met betrekking tot de beveiliging, de traceerbaarheid of het gebruik van de apparaten) behoort tot de mogelijkheden. Deze controles kunnen plaatsvinden op

[390] Vertaling door R. Gellert.
[391] Gebaseerd op de persoonlijke bewerking en vertaling door R. Gellert.

het moment dat de aanvraag voor een vergunning wordt ingediend, of op elk verrassingsmoment daarna (Art. 2 lid 3 Instructie van 5 september 2006).

Volgens R. 226-11 kunnen de vergunningen in een aantal gevallen worden ingetrokken:

> "1 In geval van valse aangifte of valse informatie;
>
> 2 In geval van wijziging van de omstandigheden op basis waarvan de vergunning is afgegeven;
>
> 3 Indien de begunstigde van de vergunning niet heeft voldaan aan [R. 226-1 tot en met 12], of aan de specifieke verplichtingen die in de vergunning zijn voorgeschreven;
>
> 4 Wanneer de begunstigde van de vergunning de uitoefening van de activiteit waarvoor de vergunning is afgegeven, stopzet."

Volgens art. 4 (Instructie van 5 september 2006) zijn in punt 3 van R. 226-11 de volgende motieven opgenomen:

> "de weigering om zich te onderwerpen aan de controles die nodig zijn om na te gaan of de in de vergunningsaanvraag vermelde gegevens worden nageleefd;
>
> - niet-naleving van de aan de vergunning verbonden verplichtingen;
>
> - voor houders van een fabricage-, invoer-, tentoonstellings-, aanbiedings-, verhuur- of verkoopvergunning:
>
> - het feit dat er geen register wordt bijgehouden of dat wordt geweigerd het aan de onderzoeksinstanties te presenteren (R. 226-10);
>
> - het feit dat op elk gefabriceerd, ingevoerd, tentoongesteld, aangeboden, gehuurd of verkocht apparaat niet de referentie van het type dat overeenkomt met de vergunningsaanvraag (R. 226-6) is aangebracht;
>
> - het feit dat zij apparaten hebben voorgesteld, overgedragen, verhuurd of verkocht aan onbevoegde personen of bedrijven (R. 226-10);
>
> - het maken van een advertentie ten gunste van een apparaat dat de verwezenlijking van de in artikel R. 226-1 [privéleven] en de tweede alinea van artikel 226-15 [geheimhouding van

> correspondentie] van het Wetboek van Strafrecht bedoelde strafbare feiten mogelijk maakt, wanneer deze advertentie een aansporing vormt om deze strafbare feiten te plegen".

Behalve in geval van urgentie kan de intrekking pas plaatsvinden nadat de licentiehouder op de intrekking heeft kunnen reageren. Bovendien kunnen de vergunningen automatisch worden ingetrokken indien de houder ervan wordt veroordeeld voor een van de overtredingen van de artikelen 226-1, 226-15, dat wil zeggen inbreuken op het recht op privéleven en/of het beroepsgeheim (R. 226-11).[392]

De intrekking van de licentie wordt aan de licentiehouder gemeld. Deze laatste heeft twee opties. Ofwel kan hij het toestel vernietigen (in het bijzijn van politieagenten), ofwel kan hij het toestel aan een andere persoon overdragen, op voorwaarde dat dit gebeurt binnen de hierboven onderzochte wettelijke vereisten (art. 4 Instructie van 5 september 2006).

6.1.4 Discussie: Het Franse vergunningenstelsel en reguleringsmogelijkheden voor Nederland

Op basis van bovenstaande juridische analyse waarin we deelvraag 5 beantwoorden, geven we in deze paragraaf alvast een aanzet voor het antwoord op deelvraag 8 over de reguleringsmogelijkheden voor Nederland.

Over het algemeen kan men concluderen dat het Franse vergunningenstelsel kan worden beschouwd als een nuttige bron van inspiratie, met name wat betreft de juridische constructie ervan (d.w.z. als een aanvulling op het recht op een privéleven). Wij zijn het eens met de keuze van de Franse wetgever om de regulering van spionageproducten in enge zin te verankeren in het recht op privéleven in plaats van in de bescherming van persoonsgegevens. Dat is niet alleen conceptueel gezien geschikter, het vermijdt ook enkele van de valkuilen rond de toepassing van het recht op gegevensbescherming op personen (de zogenaamde huishoudvrijstelling; zie het stuk over Grondrechten in par. 5.1).[393]

Vanuit een meer praktisch perspectief kan een dergelijk licentiesysteem, dat ook een uniek identificatienummer van het gekochte spionageapparaat vereist, de identificatie van de persoon die de spionage uitvoert, mogelijk maken. Dit zal relevant zijn in die gevallen waarin de bespioneerde persoon een microfoon of een ander type afluisterapparaat vindt. In dat geval kan de politie het unieke identificatienummer koppelen aan de koper. Dit zou echter alleen het geval zijn wanneer de koper inderdaad een licentie zou verwerven, wat echter niet erg waarschijnlijk is,

---

[392] En ongeoorloofde toegang tot het informatiesysteem met het oog op het vastleggen van gegevens, zie artikel 432-9 Franse Wetboek van Strafrecht.
[393] Voor enkele regels over het toepassingsgebied van de huishoudvrijstelling, zie R. Gellert, 'Case Note Door-to-Door Preaching by Jehovah's Witnesses Community', *4 European Data Protection Law Review* 3, 4–5.

aangezien men dergelijke apparatuur gemakkelijk online kan kopen van een buitenlandse aanbieder en het licentiesysteem kan omzeilen (dit wordt hieronder verder besproken).

Er zijn echter verschillende beperkingen van het Franse vergunningensysteem. De eerste beperking heeft betrekking op een gebrek aan gebruiksvoorwaarden. Hoewel het vergunningenstelsel zeer gedetailleerd is wat betreft de procedure en de formele vereisten, zijn aan de autorisatie geen inhoudelijke gebruiksvoorwaarden verbonden. Zo zijn er in het vergunningenstelsel bijvoorbeeld geen aanwijzingen opgenomen over gebruiksvoorwaarden die in de licentie gesteld kunnen worden, zoals type activiteit, het type actor, het type actie, enz. die ondernomen kunnen worden. Dit betekent dat de minister-president een grote mate van discretie heeft. Het ontbreken van duidelijk vastgestelde criteria is met name problematisch omdat de betrokken activiteiten, die bestaan uit het gebruik van spionageproducten, in veel gevallen een inbreuk vormen op de grondrechten (waaronder het privéleven). Het zijn juist de voorwaarden voor het gebruik zoals bepaalt in de licentie, die het gebruik binnen de grenzen van de legaliteit moeten houden.[394]

De tweede opmerking gaat over uiteenlopende toepassingsgebieden van art. 226-1 en art. 226-3. Zoals aangegeven heeft artikel 226-1 in een notendop betrekking op twee soorten acties. Aan de ene kant gaat het over wat in essentie de opname is van gesproken of geschreven woorden die bedoeld waren om vertrouwelijk te zijn (of het nu in de openbare- of de privéruimte is). Anderzijds omvat het de opname van het beeld van een persoon, maar enkel in de privéruimte.

Hoewel art. 226-3 geacht wordt deze bepaling aan te vullen, lijkt de aandacht uitsluitend uit te gaan naar de opname van gespreken in art. 226-1. Dit komt duidelijk naar voren uit de formulering van de bepaling zelf, die alleen verwijst naar de "detectie van gesprekken op afstand". Het vloeit ook voort uit het decreet van 4 juli 2012 dat de lijst bevat van wat als een spionageapparaat wordt beschouwd. De vergunningsverplichting heeft dus alleen betrekking op apparatuur die privégesprekken kan vastleggen. Dit betekent dat er een discrepantie bestaat tussen het toepassingsgebied van de twee bepalingen. Deze bepaling beschermt dus vooral communicatieve en, gedeeltelijk, relationele privacy (aangezien de gesprekspartners ook worden onthuld door mee te luisteren naar de gesprekken). Andere vormen van privacy die met het gebruik van andere soorten spionageapparatuur in gevaar komen, met name ruimtelijke en lichamelijke privacy (bijv. bij het opnemen van beelden van personen in de woning), worden met dit licentiestelsel niet beschermd. Om deze door de wet te beschermen, indien geïmplementeerd in Nederland, zou het toepassingsgebied van het licentiestelsel kunnen worden verbreed (met betrekking tot deelvraag 8).

---

[394] Dit wordt bevestigd door de formulering van artikel 226-3, dat bepaalt: "Eenieder die met behulp van deze hulpmiddelen artikel 226-1 overtreedt, wanneer dergelijke handelingen buiten de grenzen van de vergunning vallen of in eerste instantie niet zijn toegestaan, zal worden onderworpen aan de in deze bepaling voorziene sanctie".

Ten slotte zijn er ook kwesties die betrekking hebben op het enkele artikel 226-1, en die dus een gevolg hebben voor artikel 226-3, aangezien het om een verzwarende omstandigheid gaat. Er kan worden gesteld dat dit traditionele beperkingen zijn van de rechtsbescherming van het recht op een privéleven. Om deze reden zullen ze korter worden vermeld, aangezien ze geen betrekking hebben op het vergunningenstelsel als zodanig.

Art. 226-1 voorkomt geen inbreuken op het recht op privéleven als in Artikel 8 EVRM, maar inbreuken op de *intimiteit* van het privéleven van anderen. Met andere woorden, het eenvoudigweg bespioneren van mensen om hun privégesprek of hun beeltenis (in een privéruimte) vast te leggen, zal als zodanig geen inbreuk maken op hun recht op een privéleven. De handelingen moeten bovendien inbreuk maken op de intimiteit van dat privéleven.[395]

Het begrip intimiteit van het privéleven omvat alle elementen van het privéleven van een persoon die deze gewoonlijk zeer belangrijk vindt en die als zodanig het verdienen om te worden behouden en beschermd tegen inmenging, door ontoegankelijk te worden gemaakt voor anderen.[396] Om deze reden heeft de Franse rechtspraak geoordeeld dat de intimiteit van het privéleven het echtelijke en sentimentele leven omvat, of de relatie van een persoon met anderen die emotioneel dicht bij hem of haar staan. Het strekt zich ook uit tot familierelaties, of tot gevoelens en (geheime) verlangens.[397] Met andere woorden, niet elke opname van privé- of vertrouwelijke gesprekken (met of zonder spionageproducten in enge zin) zal kwalificeren als een inbreuk op het privéleven op grond van het Franse Wetboek van Strafrecht. Dit is met name het geval geweest in de context van de werkgelegenheid. Het vastleggen van werknemers die hun ongenoegen uiten tijdens een vergadering met werkgeversvertegenwoordigers wordt niet beschouwd als een inbreuk op de intimiteit van hun privéleven.[398] Wat de risico's voor de privacy betreft, lijken alleen de risico's die gepaard gaan met de meest intieme delen van het privéleven van een persoon te worden beschermd (bijvoorbeeld communicatieve (intieme gesprekken) en beslissings-privacy (geheime wensen). Andere soorten risico's voor de persoonlijke levenssfeer, die geen betrekking hebben op het intieme privéleven, maar plaatsvinden in de semi-private en publieke context (met name wat betreft de gedragsmatige en relationele privacy), lijken niet binnen de reikwijdte van deze bescherming te vallen. Als het vergunningensysteem in Nederland zou worden geïmplementeerd (met betrekking tot deelvraag 8), zou de reikwijdte dus beter kunnen worden verbreed tot het 'privéleven' (wat dan in overeenstemming zou zijn met de jurisprudentie van het EHRM).

---

[395] Zie Gassin, R., Rép. pén. Dalloz*, V° Vie privée. Atteintes,* 1974, § 63, p. 5*.* Deze interpretatie is bevestigd door de Franse wetgever destijds, zie *JOAN,* première session ordinaire de 1969-1970, n° 1147, p. 10*.*
[396] Zie, F. Cordier, 'L'atteinte à l'intimité de La Vie Privée En Droit Pénal et Les Médias', 20 *LÉGICOM* 85 1999.
[397] Zie, V. Fitoussi, 'Doctrine Jurisprudence Droit Pénal de La Vie Privée : Les Images, Les Mots, Les Photos Volées, Quelles Sanctions Au Pénal ?' (*Dossier complet : doctrine jurisprudence droit pénal de la vie privée*, 2010) 12 1 <https://www.fitoussi-avocat.com/2010/04/21/dossier-complet-doctrine-jurisprudence-droit-penal-de-la-vie-privee/>.
[398] Cass. crim., 14 februari 2006, n° 05-84.384.

Een andere belangrijke beperking van art. 226-1 is dat, in tegenstelling tot de opname van gesprekken die zowel in de privé- als in de openbare ruimte kunnen plaatsvinden, de vastlegging, opname of uitzending van beelden beperkt is tot die welke in een privéruimte zijn gemaakt.

Het onderscheid tussen openbare en private ruimte is echter niet scherp. Er wordt algemeen aangenomen dat de privéruimte moet worden opgevat als een ruimte die voor niemand toegankelijk is, tenzij de persoon die de plaats permanent of tijdelijk bezet, daarvoor toestemming heeft gegeven.[399] Daarentegen is een openbare ruimte een ruimte die voor iedereen toegankelijk is, zonder speciale toestemming van wie dan ook, ongeacht of de toegang permanent en onvoorwaardelijk is, of onder bepaalde voorwaarden.[400] In die zin worden zwembaden,[401] auto's,[402] boten,[403] of zelf winkels,[404] als privéruimten beschouwd.[405] De straat (en soortgelijke plaatsen zoals stranden) blijft echter een openbare ruimte.[406] Dus zelfs als de vergunningsregeling van artikel 226-3 wel betrekking zou hebben op het vastleggen van beelden, dan nog zou een dergelijke vastlegging in ieder geval geen betrekking hebben op de openbare ruimte. In die zin is de reikwijdte van het vergunningensysteem vrij beperkt en is het niet duidelijk of het voldoende is uitgerust om het hoofd te bieden aan de huidige uitdagingen als gevolg van het toenemende gebruik van spionageapparatuur (met verschillende soorten sensoren) tussen burgers, met name in openbare ruimten.

Tot slot zijn er kwesties over de mogelijkheden voor de handhaving van een dergelijk vergunningensysteem. Hoewel handhaving met betrekking tot fysieke spyshops binnen Frankrijk mogelijk is (hoewel dit heel veel middelen zou vergen), lijkt dit niet mogelijk met betrekking tot online spyshops, met name die welke buiten Frankrijk zijn gevestigd. Bijgevolg kan een Franse burger gemakkelijk en zonder vergunning een soort afluisterapparatuur kopen bij een online spyshop die evenmin over een vergunning beschikt. Het licentiestelsel wordt dus gemakkelijk omzeild. Het Franse licentiestelsel zegt niets over deze kwesties, waarvoor waarschijnlijk geen eenvoudige oplossing bestaat.

---

[399] Besançon, 5 janv. 1978 : D. 1978. 357, note Lindon ; JCP 1980. II. 19449 (1 re esp.), note Bécourt; Aix-en-Provence, 9 janv. 2006 : JCP 2007. IV. 1499.
[400] TGI Paris, 23 oct. 1986 : Gaz. Pal. 1987. 1. 21.
[401] TGI Paris, 17e ch., 6 juill. 1995, P : 94 167 200029.
[402] Cass. crim., 12 avr. 2005.
[403] CA Paris, 5 juin 1979 : JCP G 1980, II, 19343.
[404] Cass. crim., 14 mars 1984 : Bull. crim. 1984, n° 110.
[405] Zie ook: geschreven vraag n° 00425 van Mme Esther Sittler (Bas-Rhin - UMP), gepubliceerd in het Publicatieblad van de Franse Senaat, 12/07/2012 - pagina 1562, en het antwoord van het ministerie van Justitie, gepubliceerd in het Publicatieblad van de Senaat, 27/12/2012 - pagina 3086.
[406] T. corr. Aix-en-Provence, 16 oct. 1973; TGI Paris, 18 mars 1971: D. 1971. 447.

6.2 Het Duitse verbod op zenders en andere telecommunicatieapparatuur[407]

In deze paragraaf richten we ons op het Duitse verbod op zenders en andere telecommunicatieapparatuur ter beantwoording van deelvraag 7. Naast de reguliere bepalingen over inbreuken op iemands privacy met behulp van visuele en audiobewakingsapparatuur in het Wetboek van Strafrecht (art. 201 en 201a van het Duitse Wetboek van Strafrecht; 'StGB'), heeft Duitsland ook een specifieke bepaling die bepaalde soorten zenders en andere telecommunicatieapparatuur verbiedt in artikel 90 van de Telecommunicatiewet (Telekommunikationsgesetz; 'TKG'). Dit verbod, ook wel 'het verbod op mini-spionnen'[408] genoemd, werd oorspronkelijk al in 1986 ingevoerd, maar heeft sindsdien verschillende wijzigingen ondergaan. In deze paragraaf zullen we deelvraag 5 beantwoorden.

Het algemene doel van art. 90 TKG is het voorkomen van misbruik van zenders of andere telecommunicatieapparatuur voor het onopgemerkt onderscheppen van gesprekken van anderen en het onopgemerkt opnemen van beelden van andere personen.[409] De bepaling is gericht op iedereen en is niet beperkt tot het commerciële gebruik van zenders of andere telecommunicatieapparatuur. Artikel 90 beschermt rechtstreeks de persoonlijke levenssfeer (*Privatsphäre*) en beschermt het algemene recht op privacy (artikel 1, lid 1, juncto artikel 2, lid 1, van de *Grundgesetz*; GG), alsmede het recht van personen op informationele zelfbeschikking, dat is ontwikkeld door het Bundesverfassungsgericht (BVerfG 65, 1 (41)). Meer in het bijzonder omvat dit recht het recht op de eigen beeltenis en het recht op de vertrouwelijkheid van het woord. Dit betekent dat men zelf kan beslissen, binnen bepaalde grenzen, wie haar woord mag opnemen en of en door wie haar stem, opgenomen op een geluidsdrager, mag worden afgespeeld.[410] In die zin dient art. 90 dient ook ter bescherming van het telecommunicatiegeheim (met inbegrip van zowel de inhoud als de metadata, zoals verkeersdata,[411] die anders door art. 88 lid 1 en Art. 206 lid 5 StGB geregeld wordt).

Als zodanig dient dit fundamentele verbod ter bescherming van alle soorten privacy die in gevaar kunnen komen door het gebruik van dergelijke spionageapparatuur die in staat is om gesprekken of beelden van mensen heimelijk op te nemen. Wanneer bijvoorbeeld een bug of een spycam in een huis wordt gebruikt, kunnen die vormen van privacy die betrekking hebben op de meest intieme zone van een persoon (zoals te vinden in het type linksboven van de Koops et al. typologie) worden aangetast: met name de ruimtelijke en lichamelijke privacy. Wanneer

---

[407] Vertalingen van bepalingen door M. Galič en T. van Delden.
[408] T. Schwenke, '§ 90 TKG - Anwendbarkeit des Verbotes von "Minispionen" im Zeitalter smarter Geräte', 5 Kommunikation & Recht 2017.
[409] A. Dierlamm & M. Cordes, '§ 90 Missbrauch von Sende- oder sonstigen Telekommunikationsanlagen', in: K.D. Scheurle & T. Mayen (red.) *Scheurle/Mayen Telekommunikationsgesetz Kommentar*, 2018, A., para 1.
[410] BVerfGE 34, 238, 31 januari 1973 (*Tonband*).
[411] A. Dierlamm & M. Cordes, '§ 90 Missbrauch von Sende- oder sonstigen Telekommunikationsanlagen', in: K.D. Scheurle & T. Mayen (red.) *Scheurle/Mayen Telekommunikationsgesetz Kommentar*, 2018, A., para 1.

dergelijke spionageapparatuur wordt gebruikt in een semi-private of openbare ruimte, zoals in een school (denk aan het casus met ouders die de les van de leraar afluisteren via de smartwatch van hun kind), in een café of een park, dan komt met name de communicatieve, relationele en gedragsmatige privacy in het gedrang. Gezien het feit dat met het gebruik van dergelijke apparatuur informatie wordt vastgelegd, waardoor het mogelijk is deze op enigerlei wijze verder te verspreiden, is ook de informationele privacy altijd in gevaar.

Art. 90 TKG vormt dus een aanvulling op de bestaande bepalingen in het StGB. Volgens de wetgever was de bepaling een reactie op de verspreiding en miniaturisering van opname- en transmissietechnologie ('mini-spionnen'). Een aanvullende bepaling werd nodig geacht omdat degenen wiens vertrouwelijkheid van woord en beeld zijn geschonden, vaak niet op de hoogte waren van de schending en zelfs in het geval dat zij op de hoogte waren, vaak niet konden bewijzen wie de dader was.[412] Als er bijvoorbeeld inderdaad afluisterapparatuur bij de slachtoffers werd gebruikt, was het meestal erg moeilijk te bewijzen wie de systemen had geïnstalleerd en bediend. De wetgever heeft erkend dat, als apparatuur die geschikt is voor ongeoorloofde afluister- en opnamepraktijken in toenemende mate wordt verspreid, de vereiste bescherming van de persoonlijke, zakelijke en beroepsgeheime levenssfeer niet meer voldoende gewaarborgd is, aangezien het gevaar van het gebruik van dergelijke apparatuur voor ongeoorloofde afluisterpraktijken overduidelijk is.[413] Voldoende bescherming tegen het onderscheppen en opnemen door onbevoegden kon dus niet alleen door het strafrecht worden gewaarborgd. Daarom vond de wetgever het noodzakelijk het bezit, de verkoop, de reclame etc. van dergelijke apparatuur te controleren en te beperken, om de verspreiding van de apparatuur die voor het onopgemerkt onderscheppen en opnemen van beelden wordt gebruikt, tegen te gaan.[414] Art. 90, lid 1, eerste zin, verruimde dus de strafrechtelijke aansprakelijkheid die voortvloeit uit art. 201 en art. 201a StGB.

6.2.1 Het algemene verbod

Volgens art. 90 TKG is het verboden om zenders of andere telecommunicatieapparatuur, die in hun vorm een ander voorwerp nabootsen of gekleed (dat wil zeggen bedekt) zijn met voorwerpen voor dagelijks gebruik, in eigendom te hebben,[415] te vervaardigen te distribueren, in te voeren of anderszins onder het toepassingsgebied van deze wet te brengen. Vanwege deze omstandigheden of vanwege hun werkingswijze is, volgens de Duitse wetgever, dergelijke apparatuur bijzonder geschikt en bedoeld om het niet-openbaar gesproken woord van andere

---

[412] T. Schwenke, '§ 90 TKG - Anwendbarkeit des Verbotes von "Minispionen" im Zeitalter smarter Geräte', 5 Kommunikation & Recht 2017.
[413] Ibid.
[414] M. Bock, 'TKG § 90 Missbrauch Bock von Sende- oder sonstigen Telekommunikationsanlagen', in: M. Geppert & R. Schütz (red.), *Beck'scher TKG-Kommenta*r, 2013, A., paragraaf 5; T. Schwenke, '§ 90 TKG - Anwendbarkeit des Verbotes von "Minispionen" im Zeitalter smarter Geräte', 5 Kommunikation & Recht 2017.
[415] Op strafrechtelijk gebied wordt exclusief bezit ook beschouwd als eigendom.

personen te beluisteren of om hun beeld op een door hen onopgemerkte manier vast te leggen. Deze wet heeft dus gevolgen voor zowel fabrikanten, verkopers als kopers van dergelijke apparatuur.

Art. 90 TKG stelt:

> *Het is verboden om in het bezit te zijn van, te vervaardigen, te distribueren, in te voeren of op andere wijze binnen het toepassingsgebied van deze wet te brengen van zenders of andere telecommunicatieapparatuur die door hun vorm een ander voorwerp nabootsen of die bedekt zijn met voorwerpen voor dagelijks gebruik en die door deze omstandigheden of door de wijze waarop zij functioneren bijzonder geschikt en bedoeld zijn om ongemerkt te luisteren naar het niet publiekelijk gesproken woord van een andere persoon of om het beeld van een andere persoon ongemerkt door deze persoon op te nemen.*

Oorspronkelijk was deze bepaling alleen een aanvulling op Art. 201 StGB, dat de schending van de vertrouwelijkheid van het woord strafbaar stelt. De Duitse wetgever vond namelijk de bescherming van het gesproken woord belangrijker dan de bescherming van het beeld.[416] Met andere woorden, het criminaliseerde alleen onopgemerkte inbreuken op de privacy door middel van audiosurveillance. Het ging hierbij om het onderscheppen van niet-openbaar gesproken woorden, die alle menselijke geluiden omvatten met een intellectuele eigenaar waarvan de sprekende persoon terecht kon verwachten dat zij alleen door een kring van personen die tot haar beperkt waren, zou worden gehoord.[417] Ze worden onderschept wanneer de woorden die door het apparaat worden gehoord, akoestisch worden waargenomen, of het nu gaat om opnames die op hetzelfde moment worden gemaakt of die later worden opgeslagen.[418]

In 2004 werd echter de bepaling in art. 90, lid 1, eerste zin, gewijzigd om het verbod op het onopgemerkt opnemen van beelden te omvatten, waardoor ook artikel 201a StGB werd aangevuld.[419]

a) Zender en telecommunicatieapparatuur

Een essentieel onderdeel van de bepaling betreft de wijze waarop de termen ‘zender’ (Sendenalage) en "telecommunicatieapparatuur" (Telekommunikationsanlagen) worden gedefinieerd.

De term ‘zender’ wordt niet gedefinieerd in de TKG, maar in plaats daarvan wordt een definitie uit de vroegere Wet op de telecommunicatieapparatuur (*Gesetz über Fernmeldeanlagen*; FAG)

---

[416] S. Ernst, ‘Gleichgang des Persönlichkeitsrechtsschutzes im Bild- und Tonbereich?‘, 1277 NJW 2004.
[417] T. Schwenke, ‘§ 90 TKG - Anwendbarkeit des Verbotes von "Minispionen" im Zeitalter smarter Geräte’, 5 Kommunikation & Recht 2017.
[418] Ibid.
[419] M. Bock, ‘TKG § 90 Missbrauch Bock von Sende- oder sonstigen Telekommunikationsanlagen’, in: M. Geppert & R. Schütz (red.), *Beck’scher TKG-Kommentar*, 2013, A., paragraaf 1.

gebruikt. Art. 1, lid 1, tweede zin FAG definieerde "radiosystemen", die elektrische transmissie- en ontvangstapparatuur omvatten, als apparatuur "waarin de transmissie of ontvangst van berichten, tekens, beelden of geluiden [werd gedaan] zonder verbindingslijnen of met behulp van elektrische trillingen die langs een ladder worden gedragen".[420] Zenders zijn dus technische apparaten voor het genereren en uitzenden van radiogolven, bijvoorbeeld met behulp van wifi of Bluetooth-technologie. Als zodanig bestaat een zender uit ten minste één oscillator en één zendantenne, waarbij een apparaat voor het moduleren van de oscillatie altijd nodig is voor het gebruik voor het verzenden van berichten. Zo kunnen spraak, geluid, tekens en beelden worden verzonden. De term is bedoeld voor systemen die zowel kunnen verzenden als ontvangen, maar niet voor zuivere ontvangers of bedrade systemen. Objecten die alleen maar reproductie mogelijk maken zonder een aparte overdrachtsfunctie zijn, volgens de bewoordingen van art. 90, lid 1, eerste zin, dus geen zenders.[421] Dit betekent dat de overdracht van gegevens via USB (bijvoorbeeld spycams die de gegevens opnemen en later op een computer moeten worden aangesloten om de bestanden over te dragen), niet onder deze definitie zou vallen.

In 2012 vond de laatste wijziging van de bepaling plaats, toen het toepassingsgebied werd uitgebreid door de tekst "en andere telecommunicatieapparatuur" toe te voegen aan lid 1 eerste zin. Telecommunicatieapparatuur wordt gedefinieerd in Art. 3(23) TKG en betekent technische apparaten of systemen die elektromagnetische of optische signalen kunnen verzenden, overdragen, bemiddelen, ontvangen, controleren of monitoren die als boodschappen herkenbaar zijn. Deze toevoeging werd ingevoerd om de bepaling zo open mogelijk te maken en gelijke tred te houden met de snelle ontwikkeling van de technologie.[422] De toegevoegde bewoording dekt bijvoorbeeld lasermicrofoons, die het mogelijk maken om gesprekken in gesloten ruimtes op afstand te volgen door de trillingen van de ruiten die door de geluidsgolven van het gesproken woord worden opgewekt, en deze om te zetten in verstaanbare spraak.[423]

b) Camouflage en bijzondere geschiktheid voor spionage

In het amendement van 2012 is deze brede definitie van zenders en andere telecommunicatieapparatuur echter ook vernauwd. Dit werd gedaan door de invoering van een extra eis, volgens welke een object niet alleen geschikt moet zijn voor het onderscheppen van een niet-openbaar woord[424] of het vastleggen van iemands beeld op een onopgemerkte manier, maar ook *bedoeld* voor een dergelijk gebruik. De bepaling is dus gericht op apparatuur die niet

---

[420] Zie § 3, nr. 4 TKG 1996.
[421] M. Bock, 'TKG § 90 Missbrauch Bock von Sende- oder sonstigen Telekommunikationsanlagen', in: M. Geppert & R. Schütz (red.), *Beck'scher TKG-Komment*ar, 2013, marginal 8; A. Dierlamm & M. Cordes, '§ 90 Missbrauch von Sende- oder sonstigen Telekommunikationsanlagen' in: K.D. Scheurle & T. Mayen (red.) Scheurle/Mayen Telekommunikationsgesetz Kommentar, 2018, B., para 1.
[422] M. Bock, 'TKG § 90 Missbrauch Bock von Sende- oder sonstigen Telekommunikationsanlagen', in: M. Geppert & R. Schütz (red.), *Beck'scher TKG-Komment*ar, 2013, A., paragraaf 3.
[423] Ibid.
[424] Het gesproken woord is niet openbaar als het niet tot het grote publiek of tot een onbepaald aantal personen is gericht.

bedoeld is om van meet af aan een waardig doel te dienen; in plaats daarvan is het duidelijk bedoeld voor het in het geheim afluisteren of vastleggen van beelden van anderen.[425] Met andere woorden, het apparaat moet specifiek zijn gecamoufleerd - de *vorm* en de *functie* ervan moeten zodanig zijn ontworpen dat de privacy zonder toestemming wordt geschonden.[426] Mobiele telefoons of andere spionageproducten in brede zin die geschikt zijn voor het onopgemerkt opnemen van geluid of beeld, zouden als zodanig niet onder deze definitie vallen, aangezien zij niet in de eerste plaats voor dergelijk gebruik bestemd zijn. Wat het eerste deel van dit verslag betreft, vallen alleen bepaalde soorten spionageproducten in enge zin onder deze definitie, zoals bijvoorbeeld spycams in de vorm van een klok of afluisterapparaten in de vorm van een pen.

Een dergelijke intentie wordt relatief beperkt opgevat, met inbegrip van alleen objecten die een ander object nabootsen (bijvoorbeeld een camera in de vorm van een knoop of een pen) of zijn bekleed - dat wil zeggen bedekt - met voorwerpen voor dagelijks gebruik (bijvoorbeeld een kleine microfoon die verborgen is binnenin een lampenkap). Richtingsgevoelige microfoons,[427] baby- of nanny-cams zijn uitgesloten omdat ze niet nabootsen en niet met een ander voorwerp zijn bekleed.[428] Apparaten die alleen door hun kleine afmetingen bijzonder goed en onopvallend in een ruimte kunnen worden verborgen – dat wil zeggen, 'verborgen in het volle zicht' – en daarom ook bijzonder geschikt zijn voor onopgemerkte onderschepping of opname, vallen niet onder het verbod.[429] Bijgevolg zou een miniatuurcamera of -microfoon (ter grootte van een knoop) die niet vermomd is in de vorm van een ander voorwerp of verborgen is via een ander voorwerp voor dagelijks gebruik, niet onder deze definitie vallen, ook al zou de camera of de microfoon door zijn kleine formaat in feite even moeilijk te detecteren zijn.

Dit is bekritiseerd in wetenschappelijke literatuur. Schwenke verwoordde het als volgt: '[d]e veronderstelling dat verboden apparaten een noemenswaardig doel zouden kunnen missen, is een inschatting tegen de achtergrond van de technologie van de jaren tachtig van de vorige eeuw.'[430] Hoewel zo'n duidelijke differentiatie misschien geschikt was voor 'spionageproducten' uit het verleden, hebben apparaten in de tijd van 'Internet of Everything' meestal geen

---

[425] M. Bock, 'TKG § 90 Missbrauch Bock von Sende- oder sonstigen Telekommunikationsanlagen', in: M. Geppert & R. Schütz (red.), *Beck'scher TKG-Kommen*tar, 2013, A., paragraaf 2.
[426] T. Schwenke, '§ 90 TKG - Anwendbarkeit des Verbotes von "Minispionen" im Zeitalter smarter Geräte', 5 Kommunikation & Recht 2017.
[427] S. Ernst, 'Gleichgang des Persönlichkeitsrechtsschutzes im Bild- und Tonbereich?', NJW 2004, p. 1278; A. Dierlamm & M. Cordes, '§ 90 Missbrauch von Sende- oder sonstigen Telekommunikationsanlagen' in: K.D. Scheurle & T. Mayen (red.) Scheurle/Mayen Telekommunikationsgesetz Kommentar, 2018, B., para 3.
[428] M. Bock, 'TKG § 90 Missbrauch Bock von Sende- oder sonstigen Telekommunikationsanlagen', in: M. Geppert & R. Schütz (red.), *Beck'scher TKG-Kommen*tar, 2013; A. Dierlamm & M. Cordes, '§ 90 Missbrauch von Sende- oder sonstigen Telekommunikationsanlagen' in: K.D. Scheurle & T. Mayen (red.) Scheurle/Mayen Telekommunikationsgesetz Kommentar, 2018, B., paragraaf 3.
[429] M. Bock, 'TKG § 90 Missbrauch Bock von Sende- oder sonstigen Telekommunikationsanlagen', in: M. Geppert & R. Schütz (red.), *Beck'scher TKG-Kommen*tar, 2013, B., paragraaf 3.
[430] T. Schwenke, '§ 90 TKG - Anwendbarkeit des Verbotes von "Minispionen" im Zeitalter smarter Geräte', 5 Kommunikation & Recht 2017.

afgebakende en gesloten reeks functies en, daarmee verbonden, vormen.[431] Integendeel, met 'embedded' minicomputers worden hedendaagse apparaten gekenmerkt door een verscheidenheid aan functies, mobiliteit en kleinschaligheid.[432] Veel huishoudelijke of alledaagse voorwerpen kunnen tegenwoordig worden gebruikt voor onopgemerkte spionage, zoals smartwatches, slimme tv's die meeluisteren met gesprekken[433] of Amazon's Alexa.

Bovendien, Art. 90 introduceert een fundamenteel verbod. Dit betekent dat een criminele dreiging niet nodig is en dat het niet nodig is dat het object daadwerkelijk wordt gebruikt. Het object hoeft alleen geschikt en bedoeld te zijn voor het onopgemerkt onderscheppen van communicatie of het opnemen van beelden. Het is ook onmogelijk om zenders alleen te legaliseren door waarschuwingen aan de verborgen camera of het verborgen afluisterapparaat te bevestigen.[434]

6.2.2 Vrijstellingscatalogus

Lid 1, zin 2 van art. 90 TKG bevat de catalogus met vrijstellingen van het verbod. Deze omvatten bijvoorbeeld onderzoeks- of handhavingsactiviteiten van rechtshandhavingsinstanties en gerechtelijke uitvoerders (bijvoorbeeld deurwaarders; nr. 1, 2 en 3), de tijdelijke verwerving door of voor een eiser (nr. 4), het geval van commercieel vervoer of opslag van transmissieapparatuur (nr. 5), het geval van een opvolger, in welk geval het voorwerp onmiddellijk moet worden overgedragen aan het vermogen van een eiser of het permanent onbruikbaar moet worden gemaakt (nr. 7) of de verwerving van permanent onbruikbare voorzieningen voor verzamelaarsdoeleinden (nr. 8).[435] Deze vrijstellingen zijn over het algemeen niet van toepassing op het geval van burgers die daadwerkelijk spionageproducten gebruiken of bezitten om andere burgers te bespioneren, wat het doel van dit onderzoek is, dus het zal niet verder worden onderzocht.

Lid 2 van art. 90 TKG stelt dat de bevoegde hoogste federale- of staatsautoriteiten uitzonderingen zullen toestaan indien dit in het algemeen belang noodzakelijk is, met name om redenen van openbare veiligheid.[436]

---

[431] Cf. T. Schwenke, '§ 90 TKG - Anwendbarkeit des Verbotes von "Minispionen" im Zeitalter smarter Geräte', 5 Kommunikation & Recht 2017.
[432] Ibid.
[433] 'Samsung Smart TV's listening to Your Private Conversations', sites.suffolk.edu 17 april 2020.
[434] 'Miss-brauch von Sen-de-an-la-gen', Bundesnetzagentur.de 17 april 2020.
[435] De aankoop moet schriftelijk aan BNA worden gemeld met vermelding van de persoonlijke gegevens, het type uitrusting, de fabrikant of het handelsmerk en, indien van toepassing, het fabrikantnummer. De koper moet ook het doel van de aankoop geloofwaardig maken.
[436] Deze paragraaf maakt de export van zenders of andere telecommunicatieapparatuur mogelijk.

6.2.3 Reclameverbod

Art. 90 bevat een reclameverbod in para. 3. Dit verbod werd ingevoerd in de wijziging van 2004.[437] Art. 90 stelt in lid 3:

> *Het is verboden om in het openbaar of in mededelingen bestemd voor een grotere groep personen reclame te maken voor zenders of andere telecommunicatie-uitrusting door te verklaren dat zij geschikt zijn om ongemerkt naar het niet in het openbaar gesproken woord van een andere persoon te luisteren of om zijn of haar beeld ongemerkt op te nemen.*

Volgens lid. 3 is het dus verboden om in het openbaar of in mededelingen die bestemd zijn voor een grotere groep mensen (bijvoorbeeld mededelingen of reclamefolders, met inbegrip van berichten die achtereenvolgens naar een groep mensen worden gestuurd), reclame te maken voor zenders en andere telecommunicatieapparatuur door erop te wijzen dat de apparatuur in staat is om het niet-openbare gesproken woord van anderen te onderscheppen of foto's van anderen te maken op een manier die onopgemerkt blijft. Dit betekent dat het ook niet mogelijk is om dit verbod te omzeilen door te beweren dat het apparaat bedoeld is voor spionage met een positief doel, zoals het behoud van de veiligheid van kinderen; als het apparaat het mogelijk maakt om beelden of gesprekken heimelijk op te nemen, mag er geen reclame voor worden gemaakt. Advertenties kunnen in elke vorm van mondelinge of schriftelijke kennisgeving zijn. Het verbod geldt ook voor degenen die verantwoordelijk zijn voor de pers, d.w.z. uitgevers en redacteuren.

6.2.4 Bestraffing

De overtreding van het verbod volgens lid 1 zin 1 is overeenkomstig artikel 148, lid 1 TKG strafbaar als een strafbaar feit. De overtreding van het reclameverbod volgens lid 3 kan worden gesanctioneerd als een overtreding met een boete op grond van Art. 149 lid 1 sub 15. Aangezien de persoonlijke rechten van derden nog niet zijn geschonden door de schending van art. 90, zijn civiele schadeclaims tegen de dader uitgesloten.[438]

Strafrechtelijke aansprakelijkheid vloeit voort uit art. 148, lid 1, nr. 2, volgens welke een schending van art. 90 leidt tot een gevangenisstraf van maximaal twee jaar of een boete. In geval van nalatigheid is de straf een gevangenisstraf van maximaal één jaar of een boete volgens artikel 148, lid 2. Volgens art. 149 lid, nr. 15, kan iedereen die reclame maakt voor een

---

[437] M. Bock, 'TKG § 90 Missbrauch Bock von Sende- oder sonstigen Telekommunikationsanlagen', in: M. Geppert & R. Schütz (red.), *Beck'scher TKG-Kommen*tar, 2013, A., paragraaf 3.
[438] A. Dierlamm & M. Cordes, '§ 90 Missbrauch von Sende- oder sonstigen Telekommunikationsanlagen' in: K.D. Scheurle & T. Mayen (red.), *Scheurle/Mayen Telekommunikationsgesetz Kommentar*, 2018, A., paragraaf 4.

transmissie- of ander telecommunicatiesysteem die in strijd is met art 90 lid 3 worden gestraft met een boete van maximaal honderdduizend euro (art. 149, lid 2, eerste zin).

6.2.5 Aangewezen autoriteit: het federaal netwerkagentschap

Het federaal netwerkagentschap (Bundesnetzagentur; BNA) is de aangewezen instantie, waarvan een deel van de kerntaak erin bestaat de naleving van de TKG te waarborgen.[439] Volgens art. 115 TKG kan de BNA de distributie verbieden en de vernietiging van de verboden voorwerpen eisen van zowel de verkopers als de kopers.

Om de doelstellingen van de BNA op het gebied van regelgeving te bereiken, beschikt zij over effectieve procedures en instrumenten, waaronder het recht op informatie en onderzoek, en de bevoegdheid tot het opleggen van geleidelijke sancties. De BNA heeft ook een duidelijk aanspreekpunt, waar burgers gebruik van kunnen maken om vermeende schendingen van art. 90 TKG te melden.[440] Personen worden aangemoedigd om verdachte aanbiedingen op het internet, in speciaalzaken of via andere middelen te melden. Bij de melding worden zij verzocht enige informatie te verstrekken:

- Welk voorwerp is het? (korte beschrijving)
- Wie is de aanbieder?
- Wanneer en waar is het aanbod gevonden (indien nodig, internetlink toevoegen).

Als de BNA door eigen onderzoek of informatie op de hoogte komt van dergelijke aanbiedingen, kan zij op basis van art. 115 TKG passende maatregelen nemen om de inbreuk op art. 90 TKG te stoppen. Zij kan de platformexploitanten met name verzoeken het aanbod te annuleren om de verdere verkoop onmiddellijk stop te zetten. De verkopers kunnen via een administratieve procedure worden gecontacteerd, zodat zij in de toekomst afzien van de verkoop van de goederen. De BNA kan ook de vernietiging van de goederen eisen van zowel de verkopers als de kopers. Hiervoor moet bewijs worden geleverd (bijvoorbeeld een vernietigingscertificaat in de vorm van een bevestigingsbrief van een afvalverwerkingsstation waar het te vernietigen artikel is afgeleverd). De BNA verstrekt een formulier van het certificaat van vernietiging.[441]

Indien de betrokkenen vrijwillig weigeren om aan de verzoeken van de BNA te voldoen, kunnen zij daartoe door de BNA verplicht worden door middel van een bestuurshandeling. Deze verplichting kan worden afgedwongen met een boete van maximaal € 25.000. In dit kader heeft de BNA ook het recht om bedrijfsruimtes te betreden en te inspecteren; illegale

---

[439] 'The Bundesnetzagentur's duties', Bundesnetzagentur.de 14 april 2020.
[440] Missbrauch von Sendeanlagen, Bundesnetzagentur, Tulpenfeld 4, 53113 Bonn; e-mail: spionagegeraete@bnetza.de.
[441] Ook foto's (niet groter dan 15 megabyte) die duidelijk de vernietiging van de betreffende spyware laten zien, zijn toegestaan als bewijs van vernietiging. Er moet echter wel op worden gelet dat het apparaat niet werkt en dat het voorwerp in kwestie is.

spionageapparatuur die tijdens de inspectie wordt aangetroffen, kan ook in beslag worden genomen.

Met betrekking tot art. 90 TKG, is de BNA relatief actief geweest. Begin 2008 verbood de BNA de slimme kinderpop 'My friend Cayla' die heimelijk gespreken kan opnemen op grond van art. 90 TKG (en verwees daarbij ook naar risico's met betrekking tot gegevensbeschermingswetgeving).[442] Hoewel de BNA geen gedetailleerde analyse heeft gedaan van de manier waarop de pop binnen het bereik van art. 90 TKG valt, werd dit wel gedaan door verschillende Duitse geleerden. Ten eerste moet worden opgemerkt dat zo'n pop het vaakst in huis aanwezig zal zijn en geluiden en gesprekken die men thuis heeft kan vastleggen, wat meestal leidt tot risico's voor de ruimtelijke en communicatieve privacy (hoewel ook de intellectuele privacy in gevaar kan komen, als maatschappelijk onpopulaire ideeën worden besproken). De Duitse wetenschappers merkten eerst op dat de pop een microfoon en een luidspreker had die via Bluetooth en een app op de smartphone konden worden bediend. Aangezien Bluetooth, een gestandaardiseerde radiotechniek, wordt gebruikt voor de communicatie tussen de pop en de mobiele telefoon, worden de gegevens verzonden en voldoet de pop aan de criteria van een 'zender'.[443] Wat betreft de camouflage-eis zitten de microfoon en andere technische componenten in de pop (en de luidspreker is bedekt met de kleding), zodat de pop in eerste instantie de indruk geeft gewoon kinderspeelgoed te zijn zonder technische functies. Er moet ook worden opgemerkt dat de ketting van de pop oplichtte wanneer de microfoon werd ingeschakeld. De gloed van de ketting fungeert echter alleen voor degenen die bekend zijn met de technische mogelijkheden van de pop; speelgoed dat oplicht (maar geen geluid opneemt) is namelijk niet ongewoon. Volgens de fabrikant werkt deze functie niet met sommige Android-toestellen.[444] Bovendien biedt de officiële app van de pop de mogelijkheid om de lichtgevende ketting uit te schakelen.[445] Daarom kan de pop, ondanks de gloeiende ketting, beschouwd worden als een zender (conform art. 90) die geschikt is om privégesprekken van personen te beluisteren zonder dat ze het merken. Wat betreft het intentievereiste voor onopgemerkt luisteren, kan men stellen dat het doel dat de fabrikant van de pop nastreeft waarschijnlijk niet het onderscheppen van het niet-publieke woord is. Men mag echter niet vergeten dat de fabrikant door het ontwerp en de constructie van de pop ruime mogelijkheden voor misbruik biedt en dat daarom een functie voor onopgemerkte onderschepping in het functionele bereik van de pop is opgenomen.

---

[442] T. Schwenke, '§ 90 TKG - Anwendbarkeit des Verbotes von "Minispionen" im Zeitalter smarter Geräte', 5 Kommunikation & Recht 2017; S. Vogelgesang & S. Hessel, 'Spionagegeräte im Kinderzimmer?', 6 Zeitschrift für Datenschutz 2017; G. Hornung, 'Mitlauschen bei den lieben Kleinen: Kindeswohl oder Kindesgefährdung?', 41 VuR 2018.
[443] S. Vogelgesang & S. Hessel, 'Spionagegeräte im Kinderzimmer?', 6 Zeitschrift für Datenschutz 2017.
[444] Ibid.
[445] Ibid.

De BNA is ook van mening dat smartwatches met een geïntegreerde camera onder art. 90 TKG kunnen vallen.[446] Hiervoor is het van cruciaal belang of er een onopgemerkte opname mee mogelijk is, die naar een ontvangend apparaat kan worden gestuurd. Volgens de BNA is dit bijvoorbeeld niet het geval als het opgenomen beeld parallel aan de opname op het display van de klok wordt weergegeven. Als de camera alleen voor videotelefonie wordt gebruikt, is er ook geen sprake van een schending van art. 90 TKG. Over het algemeen vallen horloges met een geïntegreerde mobiele telefoon niet onder art. 90 TKG. Als het horloge echter naast de normale telefoonfunctie ook een monitoringfunctie heeft (vaak aangeduid als "voice monitoring", "babyfoonfunctie", "eenrichtingsgesprek"), is het verboden. In deze gevallen kan de microfoon van het horloge worden geactiveerd via een eerder in de app ingevoerd telefoonnummer of via een SMS-commando. In dit geval kunnen alle stemmen en geluiden rond het horloge worden afgeluisterd zonder te bellen. Noch de drager van het horloge, noch de gesprekspartner van de drager van het horloge kan dit in het algemeen opmerken.

In 2017 verbood de BNA ook een speciaal ontworpen smartwatch voor kinderen, geadverteerd als een product ontworpen voor educatieve doeleinden.[447] De reden voor het verbod was dat de smartwatch was uitgerust met een SIM-kaart en een telefoonnummer kon bellen, ongemerkt door de drager van het horloge. Zo was het mogelijk om de gesprekken in de omgeving van de horlogedrager uit te zenden, zonder dat dit herkenbaar was voor de deelnemers aan die gesprekken.[448] Volgens de BNA zijn dergelijke horloges ook gebruikt door ouders om docenten te bespioneren tijdens de les door middel van het slimme horloge van hun kind (zoals meer in detail beschreven in het scenario in Hoofdstuk 1). In dit geval kan worden gesteld dat het gedragsmatige, communicatieve en de intellectuele privacy (in de zin van het bepalen van wat er precies aan haar of zijn leerlingen wordt geleerd en op welke manier) van de docent mogelijk werd verstoord.

Volgens de BNA kunnen drones niet worden beschouwd als zenders of telecommunicatieapparatuur volgens art. 90 TKG, aangezien het bekend is dat drones camera's hebben, en dus kunnen ze niet op een speciale manier geschikt worden geacht voor onopgemerkte opname. In dit verband zou het ook goed zijn om te stellen dat drones niet onder het toepassingsgebied van artikel 90 TKG moeten vallen, omdat ze kunnen worden beschouwd als spionageproducten in brede zin – ze zijn niet in de eerste plaats voor spionage ontworpen of aangepast.

Ten slotte zijn volgens de BNA GPS en GSM-trackingapparaten niet in strijd met art. 90 TKG, als ze alleen de locatie-tracking functie hebben.[449] Dit is echter niet in overeenstemming met een

---

[446] Zie ‘Hinweise zu einzelnen Produktkategorien’, Bundesnetzagentur.de 14 april 2020.
[447] Ibid.
[448] G. Hornung, ‘Mitlauschen bei den lieben Kleinen: Kindeswohl oder Kindesgefährdung?’, 41 VuR 2018.
[449] Zie ‘Hinweise zu einzelnen Produktkategorien’, Bundesnetzagentur.de 14 april 2020.

rechtszaak over GPS-tracking, waarin de regionale rechtbank Mannheim concludeerde dat een GPS-tracker in de vorm van een in de handel verkrijgbare draadtelefoon met ontvanger wel degelijk een zender in de zin van Art. 90 TKG is.[450] Dit was echter slechts een kanttekening in de zaak, zodat er geen sprake was van een behoorlijke bespreking van de zaak.

6.2.6 Discussie: Het Duitse verbod en reguleringsmogelijkheden voor Nederland

Op basis van bovenstaande discussie waarin we deelvraag 7 beantwoordden, geven we hieronder een aanzet voor het beantwoorden van deelvraag 8.

Het Nederlandse Wetboek van Strafrecht (Sr) kent reeds enkele bepalingen di gedeeltelijk samenvallen met de reikwijdte van Art. 90 TKG. Zoals besproken in de paragraaf over het Nederlandse strafrecht (zie 1.4.4 (c)), bepaalt Art. 139d (1) Sr dat het plaatsen van afluisterapparatuur, indien dit gebeurt met de bedoeling om illegaal af te luisteren, strafbaar is met maximaal twee jaar gevangenisstraf of een boete van de vierde categorie. Artikel 441a Sr stelt ook reclame voor afluisterapparatuur strafbaar, indien daarin de aandacht wordt gevestigd op ‘de geschiktheid ervan als technisch hulpmiddel voor het heimelijk afluisteren, aftappen of opnemen van communicatie, telecommunicatie of andere vormen van datatransmissie’.

Art. 90 TKG is echter veel ruimer dan deze twee bepalingen. In de eerste plaats wordt onder art. 90 TKG reeds het enkele bezit (in de zin van exclusieve controle), de productie en de distributie van soorten spionageproducten strafbaar gesteld. Het apparaat hoeft nog niet hoeft te worden gebruikt en er hoeft geen bijzondere bedoeling te zijn, aangezien een dergelijke bedoeling kan worden afgeleid uit het loutere feit dat men een product bezit of verkoopt, dat in de eerste plaats voor spionage is bedoeld en ontworpen. Ten tweede worden zenders en andere telecommunicatieapparatuur die geschikt zijn voor het onopgemerkt onderscheppen van het niet publiekelijk gesproken woord van anderen of het onopgemerkt opnemen van het beeld van anderen, verboden. Het toepassingsgebied omvat dus ook apparaten die bedoeld zijn voor spionage door middel van visuele bewakingsapparatuur. Ten slotte wordt in de Duitse bepaling ook duidelijk het *Bundesnetzagentur* (BNA) als instantie aangewezen met duidelijk afgebakende bevoegdheden en een duidelijk aanspreekpunt voor, bijvoorbeeld, de behandeling van klachten, het uit de handel nemen van producten, het uitgeven van boetes of het gelasten van de vernietiging van producten. Dit is met name van belang in verband met de handhaving, waardoor een betere handhaving van de bepalingen mogelijk wordt.

Zoals uit ons onderzoek blijkt kent de Duitse bepaling echter ook enkele beperkingen. De eerste betreft apparaten die niet draadloos gegevens verzenden (bijvoorbeeld een miniatuurmicrofoon

[450] LG Mannheim 18 oktober 2012, 4 KLs 408 Js 27973/08; hoewel de zaak betrekking had op privédetectives, betreft de conclusie met betrekking tot het locatievolgsysteem ook de focus van dit rapport.

in de vorm van een hanger, die geen gegevens verzendt, maar via een USB-poort op een computer moet worden aangesloten om toegang te krijgen tot de gegevens). Hoewel spionageproducten die draadloos gegevens kunnen verzenden inderdaad een groter risico voor de privacy kunnen vormen (aangezien men in real-time kan luisteren of video's kan bekijken), is er weinig anders dat pleit voor het uitsluiten van spionageproducten, die op een computer moeten worden aangesloten om toegang te krijgen tot de gegevens (behalve om redenen van systematisering, aangezien een dergelijke bepaling dan wellicht beter past bij een andere wet, bijvoorbeeld met betrekking tot consumentenbescherming). De Nederlandse wetgever zou dus kunnen overwegen om de reikwijdte van een dergelijk verbod in deze zin te verbreden, indien dit in de wet zou zijn opgenomen (met betrekking tot deelvraag 8).

De tweede beperking betreft spionageproducten in enge zin die een vorm van inbreuk op de privacy mogelijk maken die noch visueel, noch auditief is. De Nederlandse wetgever zou kunnen overwegen om locatievolgsystemen (hardware; software valt al onder de relevante bepalingen inzake cybercriminaliteit – zie het stuk over strafrecht, par. 5.4) in het toepassingsgebied op te nemen. Hiervoor zou moeten worden beoordeeld of dergelijke apparaten geschikt zijn en in de eerste plaats bedoeld zijn om personen te bespioneren. Er zijn goede redenen om dit als zodanig te beschouwen.

De laatste beperking betreft de eis dat de zender of het telecommunicatieapparaat de vorm van een alledaags voorwerp moet hebben of bekleed met een alledaags voorwerp moet zijn (bijvoorbeeld een camera in de vorm van een knop of een microfoon die aan de binnenkant van een lamp zit). Gezien de steeds kleinere afmetingen van spionageproducten is het niet nodig om de apparaten in de vorm van een ander alledaags voorwerp te ontwerpen, zodat ze geschikt zijn en in de eerste plaats bedoeld zijn om te worden gebruikt voor spionage – een camera ter grootte van een knop is in eerste instantie ontworpen om 'in het zicht te worden verborgen' en net zo goed te worden gebruikt voor spionage. Bij rechtmatig gebruik van bewakingstechnologieën, bijvoorbeeld voor de bescherming van particuliere eigendommen of voor de verzorging van een baby, kan gebruik worden gemaakt van bewakingsinstrumenten. Maar om aan deze doeleinden te voldoen, hoeven de instrumenten zelf niet in het klein te zijn (bij de bescherming van eigendommen kan een grotere en zichtbare camera zelfs sommige inbrekers afschrikken). Zo kan men zeggen dat miniatuurmicrofoons of camera's die overal verborgen zijn (bijvoorbeeld achter een bed of onder een tafel) niet alleen geschikt zijn, maar ook bedoeld zijn voor het heimelijk onderscheppen van woorden of het opnemen van beelden.

Wat ten slotte nog moet worden onderzocht, is de daadwerkelijke impact van deze bepaling op de beschikbaarheid van dergelijke spionageproducten voor de burgers. Dit gaat echter verder dan de reikwijdte van deze verkennende studie. Wat gezegd kan worden, is dat het werk van de BNA wel degelijk tot enkele tastbare effecten leidt, waardoor bepaalde soorten producten (zoals

de Cayla-pop of soorten slimme horloges) niet (even gemakkelijk) beschikbaar zijn op de Duitse markt.

6.3 Praktische waarborgen van bedrijven en organisaties

In deze paragraaf staat deelvraag 6 centraal: *Wat zijn succesvolle, praktische waarborgen van binnen- en buitenlandse bedrijven en organisaties om privacy-inbreuken door spionageproducten te voorkomen of te beperken? En waarom zijn andere waarborgen niet succesvol?* Wij kijken eerst naar praktische waarborgen van bedrijven en organisaties op het gebied van spionageproducten in enge zin en bespreken daarna dergelijke waarborgen op het gebied van hobbydrones als spionageproducten in brede zin.

6.3.1 Spionageproducten in enge zin

In deze verkenning hebben wij weinig voorbeelden kunnen vinden van praktische waarborgen ontwikkeld door bedrijven die spionageproducten in enge zin verkopen. Uit de Internet quickscan van het aanbod van spionageproducten in enge zin ontstaat een beeld waarin er weinig uitleg wordt gegeven aan kopers van dergelijke producten over wat wel en niet geoorloofd is in termen van privacy. Sommige online webwinkels geven een disclaimer dat zij zelf niet aansprakelijk kunnen worden gehouden voor onjuist en onrechtmatig gebruik van de bij hen gekochte producten. Zo vermeldt de webshop van Sitcon bijvoorbeeld bij de webpagina over horloge camera's:

> Sitcon accepteert geen aansprakelijkheid voor het onjuist of onwettig gebruik van de door ons aangeboden spionageproducten. Sitcon adviseert iedereen voor aankoop en gebruik na te gaan of inzet van een door Sitcon aangeboden spy product legaal is in het land voor het gewenste gebruik en toepassing. Doordat wij ook exporteren kan het zijn dat onze spyshop producten niet in Nederland gebruikt mogen worden![451]

Op de blog van de webwinkel zijn enkele artikelen te vinden over wetgeving rondom spionageproducten, zoals "Afluisterapparatuur gebruiken: wat mag wel en wat mag niet?"[452] Deze blogposts geven een beknopt overzicht van de wetgeving en onder welke voorwaarden de producten gebruikt mogen worden. Deze informatie wordt niet bij de producten zelf gegeven. Verder is er weinig informatie over privacy te vinden op de website (op de privacyverklaring van de site zelf na). Tegelijkertijd vermeldt de site bij de beschrijving van spycamera's het volgende:

> Zekerheid in het leven is belangrijk. Soms is het hierbij nodig om iemands doen en laten na te trekken. Met een spy camera volgt u onopgemerkt alle bewegingen in

[451] Zie bijvoorbeeld'Horloge camera's', Sitconsecurity.nl 14 april 2020.
[452] 'Afluisterapparatuur gebruiken: wat mag wel en wat mag niet?', Sitconsecurity.nl 14 april 2020.

> een woning, vergaderzaal en op het werk. Deze spycam beelden kunt u bijvoorbeeld gebruiken als bewijsmateriaal mocht dit nodig zijn.[453]

Dergelijke uitspraken lijken ogenschijnlijk illegaal gebruik aan te moedigen.

Op de site van een andere webwinkel spyshop4u.nl staat helemaal geen direct zichtbare informatie over het legaal gebruik van de producten. Deze site schrijft zelfs bij het overzicht van spycamera's dat deze camera's ook gebruikt kunnen worden om gesprekken af te nemen waar het eigenlijk niet mag:

> Een spycam kan je in veel situaties gebruiken. Bijvoorbeeld om misstanden op de werkvloer aan te tonen zoals diefstal, fraude en ongewenste intimiteiten. Dankzij de onopvallende camera die goed verborgen zit in het gebruiksvoorwerp kun jij dat bewijzen. Wat veel mensen vergeten is dat je een spionage camera [sic] niet alleen kunt gebruiken om bewijs te verzamelen, maar ook om ongemerkt gesprekken op te nemen of te filmen waar dat meestal niet mag. Denk aan een belangrijk gesprek met een arts of leidinggevende. Je krijgt veel informatie en wil dat later terug kunnen zien en horen als je niet precies meer weet wat er gezegd is. Het filmen van een college is ook handig![454]

Naast disclaimers, enkele waarschuwingen en blogposts, hebben wij weinig initiatieven om privacy-inbreuken te voorkomen, kunnen vinden bij bedrijven die spionageproducten in enge zin verkopen. Wel bieden deze bedrijven, zoals beschreven in paragraaf 3.3, doorgaans ook anti-spionageproducten aan waarmee burgers zelf inbreuken op hun privacy zouden kunnen beperken.

Burger hebben ook toegang tot technische maatregelen met betrekking tot *spyware* of *stalkerware*. Onderzoek uitgevoerd door Canadese onderzoekers toont bijvoorbeeld aan dat het mogelijk is om door een technische beoordeling van de netwerkactiviteit van spionage-applicaties (die via het internet, in plaats van de App store worden gedownload) een lijst van netwerkindicatoren te genereren, die mogelijk door gebruikers of netwerkbeheerders kan worden benut om te bepalen of deze applicaties op hun netwerk draaien. [455] Dit onderzoek toont aan dat antivirusprogramma's kunnen worden gebruikt om spyware op de smartphone te detecteren, onder meer door netwerkverkeer te analyseren. Android-telefoons met de Google Play Store zijn, bijvoorbeeld, al beschermd tegen schadelijke toepassingen met behulp van een systeem genaamd Google Play Protect, een antivirusachtige dienst die applicaties scant die van buiten de

---

[453] 'Spy camera's', Sitconsecurity.nl 14 april 2020.
[454] 'Spy camera', Spyshop4u.nl 14 april 2020.
[455] C. Parsons e.a., *The predator in your pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry* Munk school of global affairs & public policy, University of Toronto (2019); C. Khoo e.a., *Installing fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications* Munk school of global affairs & public policy, University of Toronto (2019).

Google Play Store op de telefoon zijn geïnstalleerd. Google Play Protect scant toepassingen met een zijwaartse belasting voordat ze worden geïnstalleerd en voorkomt, indien ze als kwaadaardig worden aangemerkt, dat ze worden geïnstalleerd. Google Play Protect kan echter worden uitgeschakeld vanuit de Google Play Store, zodat iemand met toegang tot de telefoon de beperkingen van Play Protect kan omzeilen. Play Protect kan wel opnieuw worden ingeschakeld om het te activeren om handmatig geïnstalleerde toepassingen te scannen en de gebruiker te vragen om alle toepassingen die zijn geïdentificeerd als kwaadaardig te verwijderen. Aangezien de regulering van spyware niet centraal staat in deze verkenning, zullen we hier niet verder op ingaan. Wat hier wel gezegd kan worden is dat de overheid zou kunnen proberen om de risico's en de prevalentie van spyware en het belang van het gebruik van dergelijke anti-virus programma's (zowel de reeds geïnstalleerde als de gekochte) op de smartphones onder de aandacht te brengen.

6.3.2 Hobbydrones als spionageproducten in brede zin

Als het gaat om hobbydrones (spionageproducten in brede zin), is er meer informatie van bedrijven beschikbaar over privacy. Bij sommige websites gespecialiseerd in de verkoop van drones is informatie te vinden over privacy en relevante wetgeving. Zo is bij de website droneland.nl - aanbieder van drone opleidingen en producten - een apart deel van de site gewijd aan de nieuwe EU-wetgeving. De webwinkel droneshop.nl heeft daarentegen weer geen informatie over privacy en wetgeving. Online winkels met een breder assortiment die drones verkopen hebben in sommige gevallen ook een gedeelte van de website gewijd aan goed gebruik van drones.[456]

Verschillende makers van drones bieden op hun website wel informatie aan over wetgeving en soms ook privacy. DJI en Yuneec hebben beide bijvoorbeeld een pagina over veilig vliegen met tips en links naar lokale wetgeving. Daarin komt privacy terloops ter sprake, maar het merendeel gaat over veiligheid. Op de website van het Franse bedrijf Parrot is informatie te vinden over de privacyoverwegingen bij het vliegen met drones bij specifieke drone modellen. Zo geeft het bedrijf bij een model een aantal *common sense* vuistregels waaronder:

> 7. Ik respecteer de privacy van anderen
>
> Mensen, om mij en mijn drone heen, moeten op de hoogte worden gebracht van wat ik doe, vooral als mijn drone is uitgerust met een camera of een ander apparaat dat gegevens over hen kan opnemen. Ik informeer de aanwezigen, beantwoord hun vragen en respecteer hun recht op privacy. Ik onthoud me van het opnemen

[456] Zie bijvoorbeeld https://www.coolblue.nl/advies/wet-regelgeving-drones-nederland.html

van beelden die het mogelijk zouden maken om mensen (gezichten, nummerplaten, etc.) te herkennen of te identificeren zonder hun toestemming.

8. Ik respecteer de privacy van anderen, ik verzend de beelden die ik vastleg niet zonder toestemming van de betrokkenen en ik gebruik de laatste niet voor commerciële doeleinden

Afbeeldingen mogen niet worden uitgezonden zonder toestemming van de betrokken personen of de eigenaar in het geval van een privéruimte (huis, tuin, enz.) en een dergelijke publicatie moet voldoen aan de geldende wetgeving (inclusief de Franse wet van 6 januari 1978, gewijzigd, de zogenaamde "Informatique et Libertés"). Elk gebruik van een drone om foto's te maken voor commerciële of professionele doeleinden is onderworpen aan specifieke vereisten, en, in Frankrijk, geldt dat een vergunning moet zijn afgegeven door de Franse burgerluchtvaartautoriteit (DGAC).[457]

Naast dat dronemakers gebruikers informeren over privacy, zijn er diverse fabrikanten, zoals DJI en Parrot, die privacybeschermende technieken inbouwen in de drones zelf, zoals geofencing, identificatie op afstand, data-minimalisatie en encryptie. Zo zijn de drones van DJI bijvoorbeeld standaard uitgerust met een geofencing functionaliteit.[458] Dit is vooral uit veiligheidsoverwegingen (om drones uit de buurt te houden van aanvliegroutes bijvoorbeeld), maar kan ook gebruikt worden om drones te weren uit gebieden die zijn aangemerkt als no-fly zone om privacy redenen (zie paragraaf 5.5) Dataminimalisatie technieken kunnen ingezet worden om bijvoorbeeld mensen en gezichten onherkenbaar te maken in beeld of beelden met mensen niet op te slaan. Encryptie is vooral bedoeld om de privacy van de dronevlieger te beschermen.

Hierbij moet worden opgemerkt dat vooralsnog technieken als “identificatie op afstand” en *geofencing* met enkele simpele ingrepen uitgeschakeld kunnen worden. Volgens een van de geïnterviewde experts kan een *geofencing* systeem met wat handig geplaatste aluminiumfolie worden omzeild. Er bestaat zelfs een speciale website met manieren om ingebouwde beperkingen van drones te verwijderen.[459] Deze technische oplossingen zullen de gemiddeld dronegebruiker helpen om het risico op privacy-inbreuken te verminderen, maar mensen met de bedoeling om heimelijk te spioneren, kunnen dan alsnog onopgemerkt blijven of gebieden binnen vliegen die ‘omheind’ zijn.

---

[457] Vertaald vanuit het Engels door A. Verhagen.
[458] *Drones and Privacy by Design: Embedding Privacy Enhancing Technology in Unmanned Aircraft*, Future of Privacy Forum 2016.
[459] Zie Nolimitdronez.com. Zie ook M. Huttunen, ‘Civil unmanned aircraft systems and security: The European approach’ *Journal of Transportation Security* (12) 2019, p. 83-101.

Ook bij andere spionageproducten in brede zin, zoals smartphones, komt het voordat technische maatregelen al snel omzeild worden. Relevant voor dit onderzoek is bijvoorbeeld de ervaring in Japan om het gebruik van smartphones voor 'upskirt'-foto's (foto's van onder de rok gemaakt) te reguleren. Om dit gebruik aan banden te leggen werd verplicht gesteld om een sluiter-geluid (als van een camera) af te spelen als een telefoon een foto maakt. Hierdoor merken omstanders wanneer iemand een foto maakt, waarmee hopelijk heimelijke observatie wordt voorkomen. Vervolgens werden echter al snel apps of technieken ontwikkeld om dit geluid te onderdrukken, waardoor het doel van de regulering niet meer werd bereikt.[460]

Naast de makers en aanbieders van drones, zijn er ook bij andere bedrijven initiatieven te vinden om privacy-inbreuken te beperken. Zo zijn er bedrijven, zoals Droneland Academy, die opleidingen verzorgen voor recreatieve en professionele dronevliegers, waarin privacy een rol speelt. Met de nieuwe regelgeving over drones zal de vraag naar opleidingen waarschijnlijk toenemen, omdat deze het voor bijna alle dronevliegers verplicht stelt om minimaal een theorie-examen af te leggen. Niet alle nieuwe verplichtingen gelden echter voor drones onder 250 gram, zelfs niet als ze een sensor hebben. Dit is al het geval met de eerdere genoemde nieuwe DJI-drone met een camera, die 249 gram weegt. Het verplichte theorie-examen geldt bijvoorbeeld niet voor dergelijke drones, ook al is dit misschien een goede manier om dronevliegers te leren over hun mogelijke impact op de privacy van anderen.

In het kader van bewustwording en educatie zijn er ook verschillende apps op de markt gebracht waarop voor dronevliegers eenvoudig te zien is waar het is toegestaan om te vliegen. Zo heeft de verzekeringsmaatschappij a.s.r. de app Vlieg Veilig ontwikkeld die aangeeft of je op een bepaalde locatie mag vliegen.[461] De app biedt ook een checklist waarin onder meer wordt gevraagd of de gebruiker rekening houdt met andermans privacy. Ook in de focusgroepen werd positief gereageerd op dergelijke apps.

Maatschappelijke organisaties, verenigingen en individuen spelen ook een belangrijke rol bij de bewustwording over de privacyrisico's van vliegen met hobbydrones. Zo geven een aantal van geïnterviewde experts en de hobbydronevliegers uit de focusgroep aan dat beginnende dronevliegers, al snel op een website als dronewatch.nl - gestart en beheerd door Wiebe de Jager - terechtkomen om informatie in te winnen over wat wel en niet kan of mag met drones. Ook fora waarin hobbydronevliegers met elkaar praten en in discussie gaan zijn veel gebruikte bronnen van informatie.[462] Bovendien spreken mensen elkaar aan op hun vlieggedrag in deze fora. Of zoals Wiebe de Jager het in een interview met ons verwoordt: "Als je op een facebook groep een filmpje post dat je boven Amsterdam vliegt, dan struikelt iedereen binnen no-time over

[460] Zie bijv. 'How to turn off camera sound on Iphone to take a silent photo', Unlockboot.com 8 april 2020.
[461] Vlieg Veilig-app van a.s.r. toont waar je wel en niet mag vliegen met je drone #adv', Dronewatch.nl 14 april 2020.
[462] Zie bijvoorbeeld Dronepilots.nl.

je heen: kan niet, mag niet. Dus er is behoorlijk wat sociale control aan het ontstaan". Hij merkt daarbij wel op: "Terwijl er ook mensen zijn die zeggen: Nederland is 16 miljoen politieagentjes, ik bepaald zelf wel wat ik doe. Die hebben daar weer lak aan."

kunnen mensen ook op lokaal niveau worden gewaarschuwd, zoals bijvoorbeeld ten aanzien van dronegebruik in toeristische gebieden. Uit de focusgroepen blijkt bijvoorbeeld dat de bewoners van Kinderdijk van lieverlee zelf maar een waarschuwingsbord hebben geplaatst om hinderlijke drones van toeristen tegen te gaan (zie Figuur 6.1).

FIGUUR 6.1 WAARSCHUWINGSBORD KINDERDIJK

Samenvattend en in antwoord op deelvraag 6 hebben wij vooral op het gebied van voorlichting en educatie praktische waarborgen van bedrijven en organisaties om privacy-inbreuken te beperken, gevonden. Uit onze verkenning blijkt dat op deze terreinen meer initiatieven te vinden zijn die hobbydrone vliegers proberen bewust te maken van de privacyrisico's van het vliegen met drones en over wat verantwoord vliegen inhoudt. Daarnaast vonden wij initiatieven van buitenlandse drone makers om privacybeschermende technieken in te bouwen in drones. Het is niet mogelijke geweest om binnen het bestek van deze verkenning te beoordelen of deze maatregelen voldoende waarborgen bieden voor het beperken van de privacyrisico's. Dit zou verder onderzoek vergen naar het effect van dergelijke zelfregulering.

7 Conclusie en reflectie

De hoofdvraag in dit rapport is in hoeverre met betrekking tot het gebruik van hobbydrones en spionageproducten in enge zin door medeburgers de huidige regelgeving is toegerust op de uitdagingen van de 21ste eeuw en in hoeverre aanpassingen mogelijk en wenselijk kunnen zijn om de privacy van burgers te beschermen. Om deze vraag te beantwoorden zijn een aantal methoden gehanteerd: literatuurstudie, internetquickscans, interviews, focusgroepen en rechtsverkenning. In navolging van de onderzoeksopdracht vanuit het WODC hebben wij in dit verkennende onderzoek zowel gekeken naar producten die specifiek gemaakt zijn voor heimelijke observaties, zoals minicamera's en locatietrackers, als naar hobbydrones. Maar in plaats van een strikte scheiding tussen deze twee aan te brengen, hebben wij hobbydrones opgevat als een soort spionageproduct. In beide gevallen gaat het immers om technologie waarmee burgers heimelijk informatie kunnen verzamelen over andere burgers. Ook al zijn drones niet hoofdzakelijk gemaakt om te bespioneren, zij kunnen wel als spionageproduct worden gebruikt. Producten als minicamera's noemen we in dat licht spionageproducten in enge zin, terwijl hobbydrones spionageproducten in brede zin kunnen worden genoemd. De analyse van de privacyrisico's van deze verschillende typen spionageproducten kan dan ook grotendeels hetzelfde zijn.

Spionageproducten zijn momenteel over het algemeen vrijelijk verkrijgbaar in Nederland, zowel via fysieke spyshops als via webshops. Dat burgers eenvoudig toegang hebben tot dergelijke producten en elkaar zodoende, in ieder geval technisch gezien, voortdurend zouden kunnen bespioneren is op zich niet nieuw. Al sinds de opkomst van de fotografie bestaan er zorgen over de waarborging van het recht om met rust gelaten te worden in horizontale verhoudingen en zeker sinds de jaren '60 van de vorige eeuw zijn kleine spionageproducten, zoals richtmicrofoons, zoomlenzen en diverse typen camera's, op de consumentenmarkt verschenen. In het verleden zijn reeds tal van maatregelen getroffen om mogelijke privacyrisico's te beperken, zoals door strafrechtelijke bepalingen in te voeren over heimelijke observaties en het afluisteren van gesprekken.

De beschikbaarheid van spionageproducten is op zich dus niet nieuw. Wel is een aantal belangrijke ontwikkelingen waar te nemen. Ten eerste zijn de producten steeds eenvoudiger en algemener beschikbaar. Waar dergelijke producten vroeger nog met name in gespecialiseerde (fysieke) winkels te koop waren, is spionageapparatuur momenteel eenvoudig te bemachtigen via Bol.com, Amazon.de en vele Chinese webshops. Het feit dat ze nu verkrijgbaar zijn in algemene winkels kan ook leiden tot een normalisering van dergelijke producten en het gebruik ervan in het dagelijks leven. Ten tweede zijn de kosten steeds verder gedaald, zodat economische belemmeringen voor de aanschaf en het gebruik van deze producten vrijwel volledig zijn komen te vervallen. Beide ontwikkelingen hebben een democratisering van

spionageproducten ten gevolg gehad. Niet alleen kunnen spionageproducten eenvoudig worden aangeschaft, steeds meer alledaagse voorwerpen, zoals smartphones, zijn uitgerust met geluids- en beeldsensoren die het heimelijk fotograferen en filmen van anderen mogelijk maken.

Naast een sterke kwantitatieve stijging van het gebruik van spionageproducten door burgers zijn ook de nodige kwalitatieve veranderingen zichtbaar. Ten eerste worden spionageproducten steeds kleiner, zodat zij onder meer in alledaagse objecten, zoals een shampoofles of een knuffel, kunnen worden verstopt of ingebouwd. Dit maakt het steeds eenvoudiger om anderen in alle ruimtes, ook binnen intieme en persoonlijke ruimtes en sferen, te monitoren. Ten tweede worden de opnametechnieken steeds preciezer, waardoor niet alleen de kwaliteit en resolutie van het opgenomen beeld en geluid beter worden; ook maakt de techniek het mogelijk om anderen op steeds grotere afstand te bespieden. Ten derde kunnen spionageproducten steeds eenvoudiger fysieke barrières omzeilen; een drone kan bijvoorbeeld simpelweg over het tuinhek heen vliegen of op de tweede verdieping in iemands slaap- of badkamer kijken. Het heimelijkheidspotentieel van spionageproducten neemt daarmee exponentieel toe.

Daarnaast is ook de informatie-infrastructuur waarbinnen de opname en eventuele verspreiding van heimelijk verzamelde informatie geschiedt, de afgelopen decennia structureel veranderd. De opnameproducten zelf kunnen steeds langer opnemen zonder dat de batterij of accu moet worden vervangen. Ook maken de producten het mogelijk om de opnames van afstand en in real-time uit te lezen. Dergelijke opnames kunnen eenvoudig worden gepubliceerd en verspreid via het internet. Technologische of economische barrières om beelden of geluidsopnames openbaar te maken via Youtube, Instagram, Facebook of andere fora zijn er nauwelijks. Een bijkomend punt is dat, los van de doelbewuste opnames en publicatie daarvan door burgers, technologische producten vaak slecht beveiligd zijn, zodat bijvoorbeeld beveiligingscamera's soms beelden, zonder medeweten van de burger die ze heeft geïnstalleerd, live beelden uitzenden op het internet.

Spionageproducten maken het niet alleen mogelijk om op specifieke momenten op specifieke plaatsen specifieke burgers heimelijk te monitoren; dit kan ook op een structurele wijze gebeuren. Zo kan door middel van GPS-trackers niet alleen de handel en wandel van huisdieren worden gemonitord, ook kinderen of (voormalige) partners en echtgenoten kunnen nauwgezet in de gaten worden gehouden. Ook is het technisch eenvoudig om permanente registraties te maken van privéruimtes, openbare ruimtes en publiek toegankelijke plaatsen, zoals cafés en sauna's. Verkooppunten prijzen producten dan ook niet zelden aan als gericht op het heimelijk afluisteren of bespieden van bekenden of vreemden. Daarbij moet wel worden gezegd dat er vaak ook *anti*-spionage apparatuur wordt aangeboden, zoals zender- en tracker-detectoren, stemvervormers, ruisgenerators en signaalblokkeerfolie. Maar lang niet elke burger die wordt of kan worden bespied zal zulke hulpmiddelen gebruiken, als ze al op de hoogte zijn van het bestaan ervan.

In dit afsluitende hoofdstuk geven we eerst een korte samenvatting van de antwoorden op de overkoepelende vraagstelling van dit rapport en op de verschillende deelvragen 1, 2, 3 en 4 (paragraaf 7.1). We beginnen met een korte samenvatting met betrekking tot de classificatie van spionageproducten (7.1.1), vervolgens richten we ons op de belangrijkste privacyrisico's (7.1.2) en tot slot identificeren we de belangrijkste lacunes in de bestaande wet- en regelgeving (7.1.3).

In het tweede deel (7.2) richten we ons op de reguleringsmogelijkheden voor Nederland en beantwoorden we deelvragen 5, 6, 7, 8 en 9. Om een breed scala aan oplossingsperspectieven te bieden, benaderen we de reguleringsmogelijkheden vanuit een breed perspectief en maken gebruik van de door Lessig onderscheiden reguleringsinstrumenten: markt (7.2.1), sociale normen (7.2.2), code (7.2.3) en recht (7.2.4). In de respectievelijke paragrafen geven we aan waar welke deelvraag beantwoord wordt.

7.1 Algemene conclusie en samenvatting van de antwoorden op de overkoepelende vraagstelling

7.1.1 Classificatie van spionageproducten

Met betrekking tot deelvraag 2 (welke spionageproducten zijn te koop of anderszins beschikbaar voor burgers), zien we dat winkels diverse spionageproducten verkopen, zoals objecten met een GSM-zender of GPS-trackers die op objecten of personen kunnen worden vastgemaakt, rookmelders met camera's, pennen met de mogelijkheid om geluidsopnames te maken, camera's die in camouflagekleuren worden geleverd en opritverklikkers die kunnen worden ingezet om beweging, bijvoorbeeld in of rondom het huis, te registreren. Naast dergelijke hardware wordt ook software verkocht om spionage mogelijk te maken ('spyware'). Zo wordt controlesoftware met diverse mogelijkheden aangeprezen als instrument om kinderen en werknemers in de gaten te houden.

Wat betreft deelvraag 1 (hoe kunnen spionageproducten worden gedefinieerd en geclassificeerd), is een aantal punten van belang, voor het definiëren en het classificeren van niet alleen de spionageproducten, maar ook van de privacyrisico's en mogelijke aangrijpingspunten voor regulering.

Allereerst is het van belang om een onderscheid te maken tussen enerzijds producten die hoofdzakelijk ontworpen of geschikt zijn gemaakt zijn om specifiek voor spionage te worden gebruikt en anderzijds producten met diverse toepassingsmogelijkheden, waaronder spionage. Onder de eerste categorie vallen mini-camera's en -microfoons die ontworpen zijn met het oog op heimelijke spionage; ook al kunnen zulke producten soms ook voor niet spionage-doeleinden worden gebruikt, zoals een GPS-tracker voor het volgen van een persoon met dementie, zijn ze hoofdzakelijk bedoeld voor heimelijke spionage. Een smartphone en een drone vallen in de tweede categorie. Een smartphone kan bijvoorbeeld worden gebruikt voor bellen, appen en het

maken van selfies, maar ook voor het maken van geheime opnames, bijvoorbeeld van privégesprekken. Een drone kan worden gebruikt voor mooie natuurfoto's, maar ook om buren te bespioneren. Het onderscheid betreft uiteraard twee ideaaltypes: veel producten, zoals de toenemend beschikbare locatietrackers en Internet of Things-producten (dat wil zeggen producten die zijn aangesloten op het internet), zijn lang niet altijd eenduidig in de ene of de andere groep onder te brengen.

Het gebruik van spionageproducten in brede zin kan een grote variëteit aan doeleinden hebben, waarvan vier het meest prominent aan bod zijn gekomen in deze studie. Ten eerste is er het recreatief gebruik. Veel van de producten worden vooral als leuke gadgets voor hobbyisten gezien. Drones zijn daarvan het voorbeeld bij uitstek, maar ook producten die het mogelijk maken om op grote afstand beeld- en geluidsopnames te maken worden vaak gebruikt voor hobbydoeleinden, zoals het filmen van een buurtfeest, een verjaardag of de carnavalsoptocht. Het gebruik van alledaagse producten met spionagemogelijkheden, zoals smartphones, is voor het grootste deel ook in deze categorie te plaatsen. Ten tweede gaat het om het beveiligen van personen en objecten. Een evident voorbeeld in dit verband is het filmen van het erf vanaf het huis door een camera (voor het beveiligen van privé-eigendom) en het monitoren van het kind, zoals door middel van apps of trackers met een GPS-signaal. Voor deze doeleinden worden typisch spionageproducten in enge zin gebruikt. Ten derde gaat het om de inzet van spionageproducten voor professionele doeleinden, wat buiten het bereik van dit onderzoek valt. Hierbij valt te denken aan de inzet van drones om dijken te inspecteren en aan boeren die hun landbouwgrond met drones inspecteren. Ten vierde en tot slot gaat het om het heimelijk en vaak wederrechtelijk doelbewust bespioneren van personen. Dit geldt voor spionageproducten in brede en enge zin; bij de laatste categorie zal dit een belangrijk deel van het gebruik uitmaken. Hierbij valt te denken aan het in de gaten houden van iemand door een jaloerse (voormalige) partner, het plaatsen van minicamera's in sauna's of kleedkamers en het afluisteren van gesprekken van de buren.

Niet alle spionageproducten bieden de mogelijkheid om individuele personen te identificeren of om al dan niet gevoelige informatie over hen te vergaren. Sommige drones zijn bijvoorbeeld niet uitgerust met sensoren, of enkel met zulke grofkorrelige sensoren dat daar geen herleidbare informatie mee kan worden vergaard. Andere producten kunnen bijvoorbeeld slechts worden ingezet om te registreren of er beweging is, bijvoorbeeld om automatisch de buitenverlichting aan te doen of om een signaal te geven aan de eigenaar van een woning dat er zich iemand rond of in het huis begeeft, zoals een potentiele inbreker. Toch kan over het algemeen worden gezegd dat de meeste drones en spionageproducten het wel degelijk mogelijk maken om, en sterker nog in hoge mate gericht zijn op, het verzamelen van persoonlijke informatie over anderen en dat de opnametechnieken daarvoor steeds beter, preciezer en gedetailleerder worden.

Opnames kunnen worden gemaakt met de intentie gegevens over anderen te verzamelen, maar zulks kan ook onbewust gebeuren of een bijvangst zijn. Hiervan kan bijvoorbeeld sprake zijn als een persoon met een drone een landschapsfilm wil maken en een toevallige wandelaar in beeld verschijnt. De opnames die worden gemaakt met spionageapparatuur, zoals mini-cameras die in rookmelders zijn verstopt, zijn doelbewust heimelijk, maar dat geldt niet voor alle producten. Zo is het voor veel hobbyisten met een drone niet de bedoeling om mensen heimelijk te filmen, maar – zo geven de hobbydronevliegers in de focusgroep aan – het is praktisch vaak niet mogelijk om iedereen over wie zij gegevens verzamelen daarvan individueel op de hoogte te stellen. Daarbij is van belang dat het bij een traditionele camera duidelijk was voor eenieder die de camera zag dat de persoon met de camera daar opnames mee zou kunnen maken. Dit geldt mogelijk ook voor drones, maar een verschil is dat het vaak niet duidelijk zal zijn door wie de opnames gemaakt worden. Voor sensoren die in alledaagse objecten zijn geplaatst is het helemaal niet evident dat er opnames gemaakt worden en door wie. Het is dan nauwelijks mogelijk voor burgers om bezwaar te maken en opnames te voorkomen, of om achteraf om verwijdering van opnames te vragen.

Daarnaast is het van belang dat, alhoewel spionageproducten vaak zonder toestemming van de bespioneerde(n) gebruikt zullen worden, er ook een aantal belangrijke uitzonderingen zijn. Een voorbeeld zijn drones die opnames van een verjaardagsfeest maken, waarbij alle bezoekers hiervan op de hoogte zijn en daarmee instemmen. Een ander voorbeeld kan worden gevonden in kinderen die zelf een app downloaden op hun telefoon of een smartwatch om doen, om hun ouders zodoende in staat te stellen hen steeds te lokaliseren. Daarbij moet worden evenwel worden bedacht dat wetenschap van en instemming met het maken van beelden in beginsel onafhankelijk is van de legitimiteit van het eventuele latere gebruik van de beelden, bijvoorbeeld de verspreiding ervan. Wraakporno is daarvan het meest navrante voorbeeld.

Tot slot is het van belang een onderscheid te maken tussen sensoren die in of aan een bepaalde plaats worden bevestigd en sensoren die mobiel zijn. De eerste categorie producten maken vaak permanent of semipermanent opnames mogelijk, maar zijn naar hun aard gericht op een specifieke plek. De tweede categorie producten wordt vaak ingezet voor meer tijdelijke en kortstondige opnames, maar zijn naar hun aard wel in staat om personen te volgen in hun dagelijkse handel en wandel. Daarbij moet worden opgemerkt dat door de technologische ontwikkelingen het steeds makkelijker wordt om ook mobiele sensoren permanente opnames te laten maken.

7.1.2 De belangrijkste privacyrisico's

Uit deze beschrijving van de soorten van spionageproducten, wordt duidelijk dat de inzet van spionageproducten de privacy van burgers op een aantal fronten onder druk kan zetten. Naarmate deze producten steeds wijdverbreider raken, vaker gebruikt worden, kleiner worden en

tegelijkertijd steeds betere en langere opnames kunnen maken, zal daarbij zowel het aantal als de ernst van de inbreuken toenemen. Met betrekking tot de tweede vraag van deelvraag 3 (hoe kan het gebruik van spionageproducten door burgers een inbreuk vormen op de privacy van andere burgers en wat zijn de belangrijkste privacyrisico's), zijn de belangrijkste bevindingen van deze studie (zie hoofdstuk 4) de volgende.

Allereerst kunnen middels spionageproducten opnames worden gemaakt in de privéruimte van anderen. Daarbij gaat het om spionageproducten die heimelijk beeld of geluid opnemen zowel binnenin als van buiten de woning. Niet alleen infraroodcamera's of geluidssensoren met een groot bereik kunnen door muren heen informatie registreren; ook drones kunnen worden gebruikt om over iemands heg heen te kijken of door het raam van een woning naar binnen te kijken. Hiermee komt het idee van de woning als afgesloten privéruimte, en dus *ruimtelijke privacy* (waarbij de bewoner bepaalt wie toegang heeft tot die ruimte), onder druk te staan: binnen komen zonder te kloppen, noemen molenbewoners van Kinderdijk dit bij een voor deze studie gehouden focusgroep.

Daarbij kunnen ook intieme zaken en gedragingen worden bekeken. Zo kunnen drones de slaapkamer of de badkamer binnenkijken en kunnen opnames worden gemaakt in iemands achtertuin waar een persoon schaars gekleed ligt te zonnen. Daarbij moet evenwel worden opgemerkt dat dergelijke intieme beelden ook kunnen worden opgenomen in de publieke en semipublieke sfeer. Hierbij valt te denken aan een drone die over een naaktstrand zweeft of aan verborgen camera's in sauna's en kleedruimtes van fitnessgelegenheden. Hierbij komt vooral de *lichamelijke privacy* onder druk te staan. Door het plaatsen van microfoons in de woning kunnen echter ook privégesprekken door de aanwezigen of via de telefoon worden afgeluisterd. Dit heeft gevolgen voor de *communicatieve privacy*.

Het opnemen van beelden en geluiden in de privésfeer, de publieke en de semipublieke ruimte, gecombineerd met het verlies aan controle door burgers en de onmogelijkheid om zeker te weten of en zo ja wanneer zulke opnames worden gemaakt, kan leiden tot gedragsverandering. Mensen die zich bespied wanen in hun privéomgeving gaan zich anders gedragen, aarzelen om vrienden thuis uit te nodigen en kleden zich kuiser of treffen voorzorgsmaatregelen om opnames te voorkomen. *Gedragsmatige en relationele privacy* zijn dus in de eerste plaats in gevaar. Ook blijkt uit de focusgroepen dat mensen soms, tegen hun zin in, agressief worden als zij zich continu bespied wanen, zoals mensen die wonen in toeristische trekpleisters als Kinderdijk. Wellicht is dit een voorbode voor andere delen van het land waar op termijn een toename in het gebruik van spionageproducten is te verwachten. Een dergelijke reactie zou kunnen voortkomen uit het feit dat, in tegenstelling tot lichamelijke en ruimtelijke privacy (waarbij personen tot op zekere hoogte anderen kunnen uitsluiten, bijvoorbeeld door deuren te vergrendelen en zich alleen op goed afgeschermde locaties uit te kleden), een dergelijke uitsluiting vaak nauwelijks mogelijk is met betrekking tot de gedragsmatige en relationele privacy in de openbare of publiek

toegankelijke ruimte. Iemand kan immers niet uitsluiten dat anderen haar, haar relaties of haar gedrag in de openbare ruimte observeren. Waar het vroeger tot op zekere hoogte nog mogelijk was om op te gaan in de menigte en onopvallend door afgelegen delen van de stad te bewegen, behoort dit steeds minder tot de mogelijkheden in het licht van hedendaagse spionageproducten. Zo'n verlies aan privacy leidt echter niet tot een verlies aan behoefte aan privacy, maar leidt doorgaans tot een gedragsverandering en zelfs tot agressief gedrag uit frustratie vanwege het gebrek aan controle over de handelingen van anderen.

Hierbij zijn nog twee zaken van belang. Ten eerste worden gedragsveranderingen niet alleen veroorzaakt door het daadwerkelijk maken van opnames; ook als een drone niet filmt, maar mensen denken dat dit gebeurt of weten dat niet zeker, kan dit leiden tot angst en een gevoel van controleverlies. Ten tweede is de intentie van degene die opneemt niet doorslaggevend voor de vraag of het maken van opnames als problematisch moet worden gezien. Ook het met de beste bedoelingen filmen van mensen kan als storend of indringend worden ervaren, net als het geluid dat drones maken als overlast kan worden ervaren.

Bij heimelijk filmen is een belangrijk privacy-probleem dat er informatie over een persoon wordt verzameld tegen haar zin en zonder haar medeweten. Dit is dus een kwestie van *informationele privacy* zoals besproken in het model van Koops et al. en uitgewerkt in de taxonomie van Solove (zie sectie 4.1.2). Dit is extra problematisch als het geheimen of privézaken betreft. De verzamelde informatie kan uiteraard worden ge- of misbruikt, ook op een later tijdstip. Het kan daarbij gaan om het publiceren van de informatie op het internet of het delen daarvan met derden. Dit kan betekenen dat privéinformatie in het publieke domein komt, wat reputatieschade kan aanrichten of iemands eer en goede naam kan aantasten. Het dreigen met dergelijke handelingen kan worden gebruikt voor chantage, voor geldelijk gewin of om andere zaken gedaan te krijgen. In extreme gevallen kan het gaan om het doorverkopen van informatie, zoals sekstapes of -foto’s van bekende Nederlanders.

Het is belangrijk om op te merken dat de gegevens niet hoeven te worden ge- of misbruikt om privacyrisico’s met zich mee te brengen. Het enkele feit dat de buurjongen met een drone de privéruimte heeft bekeken en de buurvrouw naakt heeft gezien kan als problematisch worden ervaren, ook al was dat niet zijn bedoeling en wist hij meteen de beelden. Het enkele verzamelen van informatie over anderen brengt al een machtsverschuiving met zich mee, omdat een burger meer weet van de ander dan de ander over de een. Zelfs als de informatie wordt gebruikt voor vriendelijke of beschermende doeleinden kan dit privacydilemma’s met zich meebrengen, zoals de in paragraaf 4.2.3 beschreven casus van de moeder die haar zoon een smartwatch meegeeft om hem te beschermen tegen de leraar.

Tot slot is het bij een beschrijving van de privacyrisico’s van drones en spionageproducten van belang om oog te hebben voor het *cumulatieve effect van privacyschendingen*. Daarbij zijn met name twee punten van belang. Ten eerste kan elke opname op zich relatief weinig (al dan niet

intieme) informatie blootgeven, maar als tientallen of honderden verschillende onschuldige informatiebronnen bij elkaar worden gevoegd, dan kunnen zij samen een zeer pregnant beeld van iemands privéleven schetsen. Zo kan de informatie die door middel van locatietracking voor een langere periode wordt verzameld (bijvoorbeeld een week) al veel onthullen over het professionele en persoonlijke leven van een persoon: waar zij woont en werkt, hoe zij haar tijd doorbrengt 's avonds en in het weekend, met wie zij omgaat, enz. Ten tweede geldt datzelfde voor de overlast en angst die mensen ervaren. De wetenschap dat er een kleine kans bestaat dat iemand een duur en hooggespecialiseerd product heeft aangeschaft om je te volgen, zoals tot enkele jaren geleden het geval was, is wezenlijk anders dan de wetenschap dat je voortdurend zou kunnen worden bekeken door elke medeburgers die weer een goedkope gadget heeft aangeschaft. Een keer per jaar een drone over je achtertuin zien vliegen is overkomelijk; gebeurt dat meerdere keren per week dan kan er een permanent gevoel van ongemak in iemands leven sluipen.

7.1.3 Wet- en regelgeving: welke risico's worden geadresseerd en waar er nog lacunes zijn

Uit dit rapport blijkt dat de huidige wet- en regelgeving de meeste van deze privacyrisico's reeds adresseert. Sterker nog, veel van de huidige inzet van drones en spionageproducten is in strijd met al bestaande wetten. In beantwoording van deelvraag 4 (welke risico's worden geadresseerd door de huidige wet- en regelgeving en waar bestaan er nog lacunes) zijn een veelheid van punten naar voren gekomen. De belangrijkste zijn de volgende.

De AVG vereist dat als burgers opnames van anderen maken, zij diegenen daarvan op de hoogte stellen en wel uiterlijk op het moment dat de persoonsgegevens worden verzameld. Bij daadwerkelijk heimelijk spioneren van anderen zal daar per definitie geen sprake van zijn. Ook bij niet-heimelijk gebruik van drones en opnames door smartphones blijkt dat het vaak als ondoenlijk en niet noodzakelijk wordt beschouwd om mensen hiervan op de hoogte te stellen, en dat als dat al gebeurt, dan geschiedt dit vaak nadat de opnames reeds zijn gemaakt. Alhoewel het niet is uitgesloten dat er in specifieke gevallen een uitzondering geldt op deze informatieplicht, zal dat in het algemeen slechts zo zijn in zoverre er een algemeen belang met de gegevensverzameling is gemoeid, zoals bij journalisten die heimelijk gegevens verzamelen om onthullingen te kunnen doen, of in zoverre de gegevens op kleine schaal voor puur persoonlijke doeleinden worden gebruikt.

Bij drones geldt daarbij nog dat binnen flink wat gebieden al niet mag worden gevlogen, hetzij vanwege het feit dat het een Natura 2000-gebied betreft, hetzij omdat het een bebouwde kom betreft, dan wel omdat er omwille van lucht- en verkeersveiligheidsredenen restricties gelden. Daarnaast gelden er nog tal van andere regelingen, zoals dat er niet in het donker mag worden gevlogen, dat de drone zelf niet zwaarder dan 25 kilogram mag wegen (anders gelden – nog – strengere regels) en niet hoger dan 120 meter boven de grond of het water mag vliegen. Uit de

gehouden focusgroepen en interviews komt een beeld naar voren waarin zowel gebruikers van drones als mensen die in gebieden wonen waar drones worden gebruikt, aangeven dat deze bepalingen regelmatig worden overtreden, al zijn er uiteraard ook veel hobbyisten die zich keurig aan de regels houden. Ook geven de dronevliegers uit onze focusgroep aan dat als zij beelden van anderen maken, zoals van een optocht van de lokale carnavalsvereniging, en die met hen delen, die anderen daar vaak blij mee zijn.

Bij spionageproducten in enge en brede zin gelden daarbij echter twee belangrijke beperkingen. Ten eerste vereist de AVG onder meer dat degene die persoonsgegevens over anderen verwerkt daarvoor een legitiem doel moet hebben. Als de spionageproducten worden ingezet om mensen heimelijk te filmen zal daar in principe geen sprake van zijn, uitzonderingen, zoals bij babyfoons of beveiligingscamera's die uitsluitend op het eigen erf zijn gericht, daargelaten. Ten tweede gelden er tal van strafbepalingen, zowel in het strafrecht als in de APV's. Het met behulp van spionageproducten heimelijk en wederrechtelijk beeldmateriaal verzamelen binnen woningen en andere besloten ruimtes kan tot een gevangenisstraf van een jaar leiden. Voor het heimelijk en wederrechtelijk maken van afbeeldingen op niet-besloten plaatsen geldt een hechtenis van ten hoogste twee maanden. Het belangrijkste struikelblok hier is dat het moet gaan om *heimelijk aangebrachte* camera's. De strafbepalingen omvatten niet camera's waarvan de *aanwezigheid* wel kenbaar is maar op een heimelijke manier worden *gebruikt*. Dat betekent dat het visueel spioneren met zichtbare mobiele camera's (zoals bij hobbydrones) vaak buiten de strafbaarstelling zal vallen, hoewel dit wel substantiële privacyrisico's oplevert voor relationele en gedragsprivacy, en soms voor de lichamelijke en ruimtelijke privacy. Dit is een mogelijke lacune in de wetgeving gezien de alomtegenwoordigheid van mobiele camera's, waarbij burgers nauwelijks handelingsmogelijkheden hebben om zich te verweren tegen ongewenste afbeeldingen.

Daarnaast zijn er nog bijzondere strafbepalingen die het gebruik van spionageproducten verbieden, zoals het verbod op het heimelijk maken van afbeeldingen van seksuele aard, bijvoorbeeld *upskirt*-foto's, en het verbod op het opnemen van gesprekken tussen derden. Wel is bij dat laatste een mogelijke lacune dat het opnemen van een gesprek door een gespreksdeelnemer zelf (zonder medeweten van de gesprekspartner) niet strafbaar is.

Uit het voor dit rapport uitgevoerde onderzoek blijkt dat het grootste probleem ten aanzien van drones en spionageproducten niet zozeer is gelegen in juridische lacunes en onduidelijkheden, die er overigens wel op relatief beperkte schaal zijn en die later in deze conclusie aan bod zullen komen (onder meer in paragraaf 7.2.4), maar in een gebrek aan naleving en handhaving van de bestaande regels. Dat ligt aan een combinatie van factoren. Ten eerste is bij heimelijk opnames het evidente probleem dat behalve de dader vaak niemand weet van de opnames; ook als bijvoorbeeld het slachtoffer hier wel van op de hoogte geraakt, bijvoorbeeld omdat beelden zijn gepubliceerd op het internet, is niet altijd eenvoudig te achterhalen en achteraf te bewijzen wie

de beelden heeft geplaatst. Zelfs als dit wel lukt en het slachtoffer kan een causaal verband aantonen tussen die daad en eventuele schade, dan nog worden ter compensatie van onrechtmatige daden (als privaatrechtelijk middel) met privacy-inbreuken tot gevolg vaak slechts zeer minimale bedragen toegekend. Dat betekent dat het voor veel mensen niet loont of zelfs een extra (emotionele) belasting kan vormen om deze juridische route te bewandelen. Ten tweede zullen de relevante strafbepalingen vermoedelijk slechts worden toegepast op de inzet van spionageproducten bij ernstige inbreuken; in gevallen die wel strafbaar zijn maar die niet ingrijpende privacyschade opleverden zal er niet snel aangifte worden gedaan en zal vanwege het opportuniteitsbeginsel ook niet snel worden vervolgd. Ten derde is de organisatie die belast is met het toezicht op en de naleving van de Algemene Verordening Gegevensbescherming, de Autoriteit Persoonsgegevens, niet genoeg geëquipeerd om zich over ieder mogelijk incident in burger-burger-relaties te buigen. Tot slot, zoals blijkt uit onze interviews en focusgroep, zijn er ook signalen dat het voor gemeentes lastig is om eventuele regels uit de APV te handhaven; zelfs bij drones, die van alle spionageproducten het best zichtbaar zijn, kan een buitengewone opsporingsambtenaar (boa) moeilijk constant de straten en de lucht in de gaten houden om drones te spotten en die te volgen naar hun bestuurder, terwijl dat wel nodig is om de overlast te kunnen vaststellen.

De handhaving van de regels is ook onrealistisch zolang er onbekendheid met en onduidelijkheid over de huidige regelgeving is, of als regels wel bekend zijn maar niet aansluiten bij de belevingswereld van de mensen die de spionageproducten inzetten. Burgers zijn weliswaar over het algemeen op de hoogte dat er privacynormen bestaan, maar er lijkt tevens bij velen een gevoelen te bestaan dat opnames door middel van bijvoorbeeld smartphones of drones moeten kunnen als er geen compromitterende or anderszins belastende informatie mee wordt verzameld. Hoewel je mensen eigenlijk om toestemming moet vragen en hen van tevoren op de hoogte moet brengen van het feit dat ze zullen worden gefilmd, brengt dat wel erg veel gedoe met zich mee. Terwijl je eigenlijk een vergunning voor bepaalde typen producten en gebruik moet aanvragen, kom je er in de praktijk ook zonder vergunning vaak mee weg. Terwijl je eigenlijk niet boven de bebouwde kom of in Natura 2000-gebieden mag vliegen, zijn juist hier de mooiste beelden met drones te maken. En bij het veelvuldig gebruik van spionageproducten voor heimelijke en illegale opnames kan een oorzaak van gebrek aan naleving worden gevonden in de constatering dat de pakkans erg laag is.

Dat er tot nu toe relatief weinig grote privacy-incidenten door of vanwege het gebruik van spionageproducten zijn (ten minste voor zover incidenten bekend zijn gemaakt), zal dan ook niet zozeer te danken zijn aan technologische of economische beperkingen of aan een effectief gehandhaafd juridisch normenstelsel, maar eerder of evenzeer aan het feit dat de meeste mensen die aan de slag gaan met spionageproducten daar prudent mee om gaan. Uit de focusgroepen blijkt bijvoorbeeld dat hobbydronevliegers wel vaak het gesprek aangaan met

mensen die bezwaar maken tegen opnames en dat zij stoppen met vliegen als deze mensen persisteren in hun wens. Ook als er per ongeluk gevoelig materiaal wordt verzameld, zoals iemand die langs de kant van de weg staat te plassen, wordt dit materiaal onmiddellijk verwijderd.

Toch leidt deze prudente omgang met spionageproducten niet altijd tot een adequate bescherming van de privacyrechten van medeburgers. Zo zijn er altijd mensen die wel doelbewust de regels aan hun laars lappen of die kwade intenties hebben, en ook is bekend dat sommige mensen die aanvankelijk wel prudent met opnames omgaan, dit later soms nalaten, zoals bij wraakporno. Uiteraard staat ook niet ieders morele kompas ten aanzien van wat wel en niet kan gelijk, wat een van de redenen is waarom de huidige gegevensbeschermingswetgeving ervan uitgaat dat mensen niet tegen hun zin en zonder dat te weten mogen worden bespied door hun medeburgers. Voor het versterken en in lijn brengen van ieders normbesef zou het recht, met name het strafrecht, een belangrijke aanvullende normerende rol kunnen spelen, maar dat zal gelet op de criteria voor strafbaarstelling en het principe van 'ultima ratio' of 'ultimum remedium' slechts de ondergrens van maatschappelijk onwenselijk of schadelijk gedrag kunnen betreffen.

Uit de focusgroepen en interviews die voor deze studie zijn gehouden blijkt bovendien dat een van de punten waarop het morele kompas uiteenloopt is dat veel gebruikers van hobbydrones en spionageproducten in enge zin met name een gevaar zien in het gebruik of misbruik van verzamelde informatie (dat wil zeggen informationele privacyrisico's), terwijl de mensen over wie gegevens worden verzameld met name wijzen op de privacyproblemen die samenhangen met het opnemen van beeld en geluid zelf (oftewel andere types van privacyrisico's, zoals lichamelijke en gedragsmatige privacy).

Om deze gaten tussen wet en praktijk te dichten, zullen wij in de volgende paragraaf bekijken welke reguleringsopties er binnen de Nederlandse context voorhanden zijn om privacy in deze context te beschermen.

7.2 Reguleringsmogelijkheden voor Nederland

In deze paragraaf kijken we naar de verschillende mogelijkheden voor regulering van drones en andere spionageproducten in Nederland. Tevens bespreken wij praktische waarborgen die wij zijn tegengekomen in binnen- en buitenland. Dit wordt gedaan aan de hand van de vier klassieke, door Lawrence Lessig onderscheiden, reguleringsmogelijkheden: marktregulering/zelfregulering (paragraaf 7.2.1), maatschappelijke regulering/sociale normen (paragraaf 7.2.2), technische regulering/code (paragraaf 7.2.3) en het recht (paragraaf 7.2.4). Hiermee beantwoorden wij de deelvragen 5 tot en met 9.

Deelvraag 5, betreffende de regulering in de ons omringende landen waar Nederland wellicht van kan leren, wordt specifiek in paragraaf 7.2.4 behandeld. Deelvraag 6, aangaande praktische

waarborgen die bedrijven hebben geïmplementeerd ter bescherming van de privacy, wordt in paragraaf 7.2.1 behandeld. Deelvraag 7, aangaande voorbeelden van verschillende vormen van overheidsregulering of zelfregulering om privacy-inbreuken door spionageproducten te voorkomen of te beperken, en deelvragen 8 en 9, betreffende de oplossingsrichtingen voor het Nederlandse beleid, zullen in alle sub-paragrafen aan bod komen al naar gelang het om marktregulering, sociale normering, technische regulering of juridische maatregelen gaat.

7.2.1 Markt: zelfregulering

Het tegengaan van privacy-inbreuken zou aan de markt zelf kunnen worden overgelaten. Uit deze studie komt naar voren dat vrijwel alle websites en winkels die spionageproducten verkopen, ook anti-spionageproducten aanbieden. Een optie is om het aan burgers zelf te laten om zich te beschermen tegen spionerende medeburgers, bijvoorbeeld door stoorzenders aan te schaffen of apparaten die opnameapparatuur van anderen kunnen ontdekken. Daarbij is evenwel de vraag of het wenselijk is om een wapenwedloop op dit punt tussen burgers onderling te laten bestaan, waarbij de mate waarin iemands privacy adequaat wordt beschermd afhangt van hoe veel zij investeert in anti-spionageproducten.

Voor wat betreft de praktische waarborgen van bedrijven en verkooppunten zelf zijn weinig bruikbare resultaten verkregen als het gaat om het beperken van de privacyrisico's van burgers door spionageproducten, met name spionageproducten in enge zin. Uit de verkenning ontstaat bijvoorbeeld een beeld waarin er weinig uitleg wordt gegeven aan kopers van dergelijke producten over wat wel en niet geoorloofd is in termen van privacy. Sterker nog, soms lijken privacyschendingen te worden aangemoedigd en benadrukt men de capaciteiten van producten om hiervoor te worden ingezet.

Als het gaat om hobbydrones (spionageproducten in brede zin), is er meer informatie van bedrijven beschikbaar over privacy. Op verschillende websites gespecialiseerd in de verkoop van drones is informatie te vinden over privacy en relevante wetgeving. Daarnaast hebben dronemakers ook zelf initiatieven genomen om privacybeschermende technieken in te bouwen in drones (waarover in 7.2.3 meer).

Tot slot zijn er ook bedrijven die opleidingen verzorgen voor recreatieve en professionele dronevliegers, waarin privacy een rol speelt. Het verplichte theorie-examen geldt bijvoorbeeld niet voor dergelijke drones, ook al is dit misschien een goede manier om dronevliegers bewust te maken van hun mogelijke impact op de privacy van anderen.

7.2.2 Maatschappelijke normen: bewustwording

Naast zelfregulering zou kunnen worden ingezet op het creëren van meer bewustwording bij burgers omtrent de privacyrisico's van spionageproducten. Zo zouden burgers op landelijke schaal bewust kunnen worden gemaakt van de gevaren van spionageproducten en het normatief

kader waarbinnen eventueel gebruik is toegestaan. Dit is momenteel al het geval bij drones. De Nederlandse overheid heeft in de afgelopen jaren meerdere initiatieven genomen op het gebied van veilig vliegen met drones, zoals een website met regels voor recreatief gebruik van drones.[463] Hier komen ook privacyaspecten ter sprake. Ook de EU probeert – in aanloop naar de inwerkingtreding van de nieuwe wetgeving – dronevliegers op meerdere manieren te informeren, waaronder de website dronerules.eu en een filmpje van de European Union Aviation Safety Agency.[464] Ook hier wordt privacy genoemd.

Dergelijke bewustwordingscampagnes zullen vermoedelijk voornamelijk effectief zijn voor wat betreft de inzet van spionageproducten waar mensen niet de intentie hebben de privacy van anderen te schenden. Voor spionageproducten die erop zijn gericht om mensen heimelijk in de gaten te houden, zoals een spionageapp die al het gedrag van iemand op de smartphone registreert of een camera die is verstopt in een rookmelder, zullen dergelijke bewustwordingscampagnes vermoedelijke minder effect sorteren, omdat onbekendheid met het vigerende kader daarbij vermoedelijk niet het probleem is. Eventueel kan er ook in bewustwording van potentiële slachtoffers worden geïnvesteerd, zoals nu op beperkte schaal wordt gedaan bij seksuele opnames in de privésfeer of via webcams. Daarbij is evenwel de vraag of dit wenselijk en effectief is, zeker bij verborgen spionageproducten; als burgers achter elke rookmelder een camera gaan vermoeden en hun gedrag daaraan aanpassen, werkt een bewustwordingscampagne averechts.

Tot slot constateerden wij in paragraaf 5.4.6 dat er een politieke en maatschappelijke discussie nodig is over de omstandigheden waarin burgers in het huidige tijdperk zich voldoende vrij zouden moeten kunnen voelen van observatie door anderen.

7.2.3 Code: technische oplossingen

Er kunnen ook technische oplossingen (ook wel ‘technoregulering’ genoemd) worden ingezet. Daarbij is het belangrijk een onderscheid te maken tussen producten die ten doel hebben en ontworpen of aangepast zijn om personen heimelijk te bespieden (spionageproducten in enge zin) en producten die daarvoor kunnen worden gebruikt, maar waarvan dat niet het hoofddoel is (spionageproducten in brede zin). Voor die laatste categorie zou voor een aantal oplossingen kunnen worden gekozen. Zo kunnen mobiele telefoons, drones en soortgelijke producten als technische eis hebben dat zij een duidelijk hoorbaar geluid maken of een lichtsignaal geven voordat zij opnames maken, zodat de omstanders hiervan op de hoogte geraken. Dergelijke technische oplossingen zijn echter gemakkelijk te omzeilen.

---

[463] ‘Regels voor recreatief gebruik drone’, Rijksoverheid.nl 14 april 2020. Er zijn ook andere initiatieven met website gesteund door verschillende organisaties, zoals Vliegveilig.nl en Vliegjedroneveilig.nl.
[464] ‘EASA Drones – Safe drone operations – Meet Donnie & Paul’ *EASA, YouTube* 14 april 2020.

Technische oplossingen kunnen een belangrijk onderdeel te zijn van het behoud van de horizontale privacy met betrekking tot drones (als typisch voorbeeld van een spionageproduct in brede zin). Zo kunnen drones standaard met locatietrackers en logging-mechanismen worden uitgerust (waardoor ‘directe identificatie op afstand’ mogelijk wordt), op een manier dat deze niet kunnen worden omzeild of uitgeschakeld, zodat duidelijk is waar de apparaten wanneer wat hebben opgenomen. Tot slot zou kunnen worden gewerkt met het zogenoemde *geofencing*, waardoor drones momenteel al simpelweg niet binnen bepaalde aangewezen zones, zoals luchthavens, kunnen komen. In hoeverre het realistisch is om alle gebieden in en rond een bebouwde kom tot zo’n automatisch afgedwongen no-fly-zone te maken, zou kunnen worden onderzocht. Een dergelijke maatregel is wellicht beter haalbaar voor specifieke kleinere gebieden, zoals Kinderdijk.

De komende EU-verordening inzake drones (met inbegrip van de uitvoeringsverordening) voorziet reeds in het gebruik van deze twee maatregelen voor de regulering van drones. Voor drones onder 250g (zelfs als ze een sensor hebben die persoonlijke gegevens kan registreren) is de technische mogelijkheid van 'directe identificatie op afstand' echter niet voorzien. Ze hoeven ook geen uniek serienummer te hebben. Terwijl de meeste drones die langere tijd buiten kunnen vliegen met een sensor op dit moment nog steeds meer dan 250g wegen, zijn er al drones met een hoogwaardige camera op de markt die minder wegen. Te overwegen valt dergelijke eisen ook verplicht te stellen voor drones onder 250g met een sensor die persoonlijke gegevens kan registreren, zodat de mogelijkheid om de dronepiloot te identificeren wordt vergroot. Juridisch gezien hoeft daar geen belemmering voor te zijn, nu de verordening lidstaten de mogelijkheid biedt om aanvullende maatregelen ter bescherming van de persoonlijke levenssfeer te treffen, waaronder technische oplossingen. Met name met betrekking tot *privacy-by-design* en *privacy-by-default* is er voorts ruimte om (met name inter- en supranationale) standaarden te ontwikkelen met betrekking tot drones.

Technische maatregelen om privacy-inbreuken te voorkomen liggen minder voor de hand bij fysieke apparatuur die is gebouwd of klaargemaakt met als hoofddoel om personen heimelijk te kunnen bespieden, zoals kleine camera’s of microfoons, GPS-trackers die op auto’s of andere objecten kunnen worden geplaatst en sensoren die in alledaagse objecten, zoals een horloge of wandklok, zijn of kunnen worden ingebouwd. Deze apparaten zijn veelal bedoeld om heimelijk en zonder toestemming gegevens over anderen te verzamelen. Daarom zouden bovengenoemde technische eisen de *raison d'être* van dergelijke producten tenietdoen. Op dit punt liggen dan ook eerder juridische regels voor de hand, zoals verbodsbepalingen bij misbruik, die hieronder (7.2.4) aan bod zullen komen.

7.2.4 Recht

Privacybescherming ten aanzien van spionageproducten kan worden verbeterd door middel van regulering en handhaving. Daarbij zijn momenteel met name in het strafrecht een aantal punten die opheldering zouden behoeven. Zo is het twijfelachtig of onder de verbodsbepaling van heimelijke observatie (art. 139f en 441b Sr) ook een opname valt met zichtbare of kenbare mobiele camera's, zoals een drone waarvan men kan verwachten dat die een camera draagt. De beperking van de strafbaarstelling tot heimelijk aangebrachte camera's zou kunnen worden heroverwogen, omdat bij drones niet zozeer de heimelijkheid problematisch is maar de onzekerheid of men wordt geobserveerd en het gebrek aan handelingsmogelijkheden om zich te verweren tegen ongewenste afbeeldingen.

Een ander punt dat mogelijk tegen het licht kan worden gehouden is het feit dat het opnemen van gesprekken, dat wil zeggen auditieve observatie, momenteel alleen verboden is (art. 139a en 139b Sr) als het gaat om het opnemen van gesprekken van anderen, dus gesprekken waarbij de persoon die spioneert zelf niet betrokken is. Als het gaat om een gesprek waaraan de persoon zelf deelneemt, maar de opname geschiedt zonder medeweten en toestemming van de gesprekspartner, dan is dit onder het huidige juridische kader in principe niet strafbaar. Hierbij zou kunnen worden overwogen om van een zogenoemd *one-party consent*-model naar een *all-party consent*-model over te stappen. Verder zou de wetgever ook de mogelijkheid kunnen overwegen om aan de strafbaarstelling van heimelijke observatie een lid toe te voegen dat specifiek ziet op het observeren van objecten zoals woningen, schuren, loodsen (in plaats van personen) met het oogmerk bepaalde misdrijven voor te bereiden. Drones worden namelijk ook gebruikt voor het plegen van inbraken (bijvoorbeeld door rond het huis te vliegen en te controleren of er iemand thuis is of dat er een raam openstaat). Tot slot is, in tegenstelling tot het heimelijk plaatsen van softwarematige locatietrackers, het heimelijke plaatsen van fysieke locatietrackers, zoals een GPS-tracker op de auto van een medeburger, momenteel niet als zodanig strafbaar; dat is alleen het geval als een object tijdens de installatie wordt beschadigd. De wetgever zou kunnen overwegen om softwarematige en hardwarematige locatietracking in dit opzicht gelijk te trekken.

Een ander punt waarbij er mogelijk meer juridische duidelijkheid en harmonisering kan plaatsvinden is op het gebied van de Algemene Plaatselijke Verordening. Uit de voor dit rapport uitgevoerde studie (zowel in het juridisch als in het empirisch onderzoek) blijkt dat gemeenten een vrij gevarieerde aanpak hebben, dat er onduidelijkheid bestaat over hoe nieuwe spionageproducten zoals drones kunnen en moeten worden gereguleerd en dat er twijfels bestaan in hoeverre nieuw ingevoerde regels stand zullen houden bij de rechter. Op dit punt zou de Vereniging van Nederlandse Gemeentes enige aanwijzingen kunnen geven, met name over de mogelijkheden om drones te reguleren – zowel met betrekking tot de mogelijkheid om ze te verbieden (in gebieden waar ze nog mogen vliegen, zoals Kinderdijk) als met betrekking tot de

mogelijkheid om overlast vast te stellen buiten de directe waarneming van de overlast door een buitengewoon opsporingsambtenaar (boa) zelf. Dit zou als voorbeeld kunnen dienen voor alle Nederlandse gemeenten, vooral voor gemeenten met bijzondere kenmerken, zoals toeristische trekpleisters. Tot slot zou de Autoriteit Persoonsgegevens een richtsnoer kunnen uitgeven of een illustratieve zaak behandelen als het gaat om de inzet van drones en smartphones voor het al dan niet heimelijk filmen van medeburgers, om zo meer helderheid te geven over de toepasselijkheid van de huidige gegevensbeschermingsregels op het gebruik van deze apparaten en om meer aandacht te vragen voor dit onderwerp.

Zoals eerder geconstateerd is het ontbreken van, of onduidelijkheid over, juridische bepalingen echter niet de grootste uitdaging als het gaat om het inperken van privacyrisico's ten aanzien van de inzet van drones en spionageproducten. Veeleer gaat het om de handhaving en naleving van het huidige juridische kader. Deze lacune zou *grosso modo* op twee manieren kunnen worden geadresseerd: meer inzet op ex post-handhavings- en restitutiemogelijkheden en een grotere nadruk op ex ante-regulering van producten en de verkoop daarvan. Het eerste zal vooral van belang zijn met betrekking tot spionageproducten in brede zin, zoals drones, terwijl het tweede vooral van toepassing zal zijn op spionageproducten in enge zin, die aan de bron kunnen worden gereguleerd (bijvoorbeeld de invoering van een licentiesysteem of een verbod op de productie of verkoop).

Voor een versterking van het ex-post-toezicht kan allereerst worden gekeken naar het feit dat de privaatrechtelijke schadevergoedingen voor burgers bij privacyschendingen momenteel erg laag zijn. De moeite en kosten die met een rechtszaak gemoeid zijn, wegen voor veel burgers niet op tegen de mogelijke toegekende schade. Het neerleggen van een minimumbedrag voor privacyschendingen door spionagetechnieken zou hiertoe een oplossingen kunnen bieden.[465] Anderzijds zou hierdoor een praktijk van massaschadeclaims kunnen worden aangemoedigd. Als een drone bijvoorbeeld onbevoegd beelden maakt boven een festival en de zeg 10.000 bezoekers een beroep doen op een schade van 1.000 euro, dan zou zo'n claim kunnen oplopen tot 10 miljoen euro. Toch zal zo'n massaclaim slechts in uitzonderlijke gevallen soelaas bieden, namelijk als zeer grote groepen mensen schade ondervinden van eenzelfde feit, en zal het in veel gevallen lastig zijn om de identiteit van de dader te achterhalen.

Realistischer lijkt het dus als de overheid het voortouw neemt in ex-post-toezicht en handhaving. Daarbij liggen globaal drie trajecten voor de hand: de bestuurlijke boete die door de Autoriteit Persoonsgegevens kan worden opgelegd, de strafoplegging door de strafrechter en handhaving door de gemeente. Toch geldt voor elk van deze vormen van handhaving het probleem dat het vaak gaat om relatief kleine incidenten die op relatief grote schaal plaatsvinden. Het kan niet van

[465] Zie uitgebreider voor deze oplossingsrichting: B. van der Sloot & S. van Schendel, 'De Modernisering van het Nederlands Procesrecht in het licht van Big Data: Procedurele waarborgen en een goede toegang tot het recht als randvoorwaarden voor een data-gedreven samenleving', *Tilburg University (TILT),* WODC 2019.

de Autoriteit Persoonsgegevens worden verwacht iedere met een drone gemaakte foto of video waarop een andere burger staat afgebeeld, te onderzoeken en op rechtmatigheid te toetsen; het kan niet van buitengewoon opsporingsambtenaren worden gevraagd om constant alert te zijn op drones en die te volgen naar hun eigenaar; en het kan niet van het Openbaar Ministerie worden verlangd om iedere heimelijke en wederrechtelijke opname te vervolgen. Ex post-toezicht en handhaving door de overheid zal soelaas bieden voor de meer ingrijpende incidenten, waarbij bijvoorbeeld de lichamelijke en ruimtelijke privacy van mensen duidelijk in het geding is.

Daarom zou ook kunnen worden gekeken naar de mogelijkheden van ex-ante-regulering en toezicht. Dit is met name van belang in verband met spionageproducten in enge zin. Ex ante-maatregelen zijn overigens ook mogelijk met betrekking tot drones, als een spionageproduct in brede zin. Een voorbeeld is de registratieplicht van drones van meer dan 250 gram of drones met een sensor die persoonlijke gegevens kan verzamelen. Een dergelijke verplichting bestaat reeds (en zal in werking treden met de komende EU-verordening inzake drones in juli 2020) en zal hier dus verder onbesproken blijven. In het hiernavolgende richten we ons dus op spionageproducten in enge zin. Daarbij liggen vooral twee instrumenten voor de hand die we in de internationale rechtsverkenning hebben onderzocht.

Naar het voorbeeld van Frankrijk is ten eerste het neerleggen van een vergunningsstelsel voor kopers en verkopers van spionageproducten in enge zin een mogelijkheid. Een dergelijk licentiesysteem vereist dat elk spionageproduct een uniek identificatienummer heeft, wat de identificatie van de personen die de spionage uitvoeren kan vergemakkelijken. Terwijl de Franse licentieverplichting alleen geldt voor spionageproducten in enge zin die geluidsopname mogelijk maken, zou de Nederlandse wetgever kunnen overwegen of een verbreding van zo'n vergunningsplicht wenselijk is. Gezien de verschillende soorten belangrijke privacyrisico's die met spionageproducten gemoeid zijn, zou zo'n vergunningenstelsel ook visuele observatie en registratie en locatietracking kunnen omvatten. Er zouden ook aanvullende regels kunnen worden ingevoerd, zoals een verplichte uitleg bij de verkoop van wat wel of niet is toegestaan bij het gebruik van dergelijke producten, vergelijkbaar met apothekers die het juiste gebruik, de gevaren en de risico's van hun producten moeten uitleggen. Uiteraard moet een dergelijk licentiesysteem niet worden gezien als een panacee voor het spionageprobleem, aangezien de verkopers of kopers van spionageproducten de licentieverplichting vrij gemakkelijk kunnen omzeilen door een product te bestellen bij een buitenlandse webwinkel (zoals Alibaba.com) of door hun bedrijf op te zetten in een land waar een dergelijke verplichting niet geldt.

Ten tweede zou, naar het voorbeeld van Duitsland, kunnen worden ingezet op het beperken van de productie, de distributie en het gebruik van spionageproducten in enge zin, met name van zenders en andere telecommunicatieapparatuur die geschikt zijn voor het onopgemerkt onderscheppen van privégesprekken van anderen of het onopgemerkt opnemen van beelden van anderen. Het Duitse model leidt tot een betere handhaving, door het aanwijzen van een

instantie (*Bundesnetzagentur*; BNA) met duidelijk afgebakende bevoegdheden en een duidelijk aanspreekpunt voor de behandeling van klachten, het uit de handel nemen van producten, het opleggen van boetes of het gelasten van de vernietiging van producten. Het werk van de BNA leidt heeft duidelijk enkele tastbare effecten, waardoor bepaalde soorten producten (zoals de Cayla-pop of soorten slimme horloges) niet beschikbaar zijn op de Duitse markt. De Nederlandse wetgever zou, als hij besluit om dit model te volgen, kunnen overwegen om het verbod, dat in het Duitse kader alleen geldt voor producten die draadloos gegevens verzenden, te verruimen met spionageproducten die via een USB-aansluiting functioneren. Ten slotte zou de Nederlandse wetgever kunnen overwegen om zo'n verbod iets ruimer te formuleren. Het Duitse verbod heeft alleen betrekking op producten die de vorm van een alledaags voorwerp hebben of zijn ingebed in een alledaags voorwerp, en omvat dus niet spionageproducten die door hun miniatuurformaat 'in het volle zicht' kunnen worden verborgen. Ook al is het niet uitgesloten dat dergelijke producten worden gebruikt voor legitieme doeleinden, de aard en het design van deze producten zijn dusdanig dat ze aanmoedigen tot wederrechtelijk gebruik, of dit in ieder geval in hoge mate faciliteren. Voor legitiem gebruik van afluister- en opnameapparatuur, zoals babyfoons, is het vaak geen bezwaar om een groter apparaat aan te schaffen, dat duidelijk zichtbaar voor iedereen is. Deze twee aanvullingen zouden het moeilijker maken om een verbod op bepaalde spionageproducten in enge zin in de praktijk te omzeilen.

Met dit overzicht van reguleringsmogelijkheden heeft de wetgever en beleidsmaker een breed scala aan opties om de privacyrisico's van hobbydrones en spionageproducten in enge zin te adresseren. Aangezien het om een veelzijdige problematiek gaat – met diverse soorten producten, verschillende typen privacy, uiteenlopende risico's en verschillende gebruikerscontexten – zal er geen 'one size fits all'-aanpak mogelijk zijn. Eerder zal een combinatie aangewezen zijn van diverse stappen die op verschillende manieren helpen om privacy in horizontale relaties te waarborgen in het licht van de toenemende beschikbaarheid en gebruik van spionageproducten.

* * *

Op basis van het voorgenoemde zou de regelgever de volgende stappen kunnen zetten (zie de flowchart op de volgende pagina). Daarbij gaan de stappen van ex ante-vormen van regulering naar ex post-vormen van regulering, en van strikte verboden (bijvoorbeeld ingebed in de techniek) naar meer flexibele regelgeving. De mogelijkheden kunnen stapsgewijs worden doorlopen. Als de Nederlandse regelgever bijvoorbeeld zou besluiten de verkoop of productie van bepaalde producten te verbieden, dan hoeft er, in ieder geval voor wat betreft privacyschendingen die met die producten kunnen worden begaan (stap 1), niet meer te worden bekeken of er een bewustwordingscampagne dient te worden ingezet (stap 7).


1: Verbod
• Ten eerste zou kunnen worden bekeken of en zo ja welke producten zouden kunnen worden verboden, ofwel bij de productie ofwel bij de verkoop.
• Daarbij zou met name kunnen worden gekeken naar alledaagse producten met sensoren en naar mini-microfoons en –camera's die in alledaagse objecten kunnen worden verstopt.
2: Certificering
• Ten tweede zou kunnen worden onderzocht in hoeverre de verkoop en het gebruik van niet-verboden producten zouden kunnen worden gecertificeerd.
• Daarbij zou met name moeten worden gekeken naar de mogelijke certificering van fysieke en virtuele spyshops en naar het gebruik van drones in gebieden met woonhuizen.
3: Technische eisen I
• Ten derde zou kunnen worden onderzocht in hoeverre technische eisen kunnen worden gesteld om bepaalde opnames onmogelijk te maken (of, in ieder geval, veel moeilijker), zoals geo-fencing ten aanzien van no-flyzones of het automatisch blurren van gezichten of personen bij drones.
4: Technische eisen II
• Ten vierde zou kunnen worden onderzocht in hoeverre er technische eisen kunnen worden gesteld aan producten om de heimelijkheid van opnameapparatuur te verkleinen.
• Hierbij kan worden gedacht aan het verplicht afgeven van een geluidssignaal of lichtsignaal als producten opnames starten of maken.
5: Strafrecht
• Ten vijfde zou kunnen worden bekeken in hoeverre strafrechtelijke bepalingen aanpassing behoeven, met name in hoeverre opnames door middel van zichtbare camera's onder het verbod op heimelijk observatie moeten vallen, in hoeverre het heimelijk opnemen van gesprekken door een gespreksdeelnemer zelf ook verboden zou moeten zijn, en in hoeverre het plaatsen van hardwarematige locatietrackers strafbaar moet zijn.
6: Richtlijnen
• Ten zesde zou kunnen worden onderzocht in hoeverre er meer duidelijkheid kan worden geven omtrent de interpretatie van het huidige regelgevende kader ten aanzien van spionageproducten en drones.
• Daarbij kan in het bijzonder worden gedacht aan het ontwikkelen van een modelbepaling in de Algemene Plaatselijke Verordening door de Vereniging van Nederlandse Gemeenten en aan een richtsnoer door de Autoriteit Persoonsgegevens ten aanzien van de gegevensbescherming.
7: Bewustwording
• Ten zevende zou kunnen worden onderzocht in hoeverre kan worden ingezet op het creëren van meer bewustwording, bijvoorbeeld door landelijke campagnes, door lokale signalen en verbodsborden te plaatsen of door het ontwikkelen van een app waarmee dronegebruikers snel en eenvoudig kunnen zien waar zij wel en niet mogen vliegen.
8: Audits en controles
• Ten achtste zou kunnen worden onderzocht in hoeverre drones en andere spionageapparatuur standaard zouden kunnen worden uitgerust met mechanismen die audits en controles mogelijk maken, zoals het loggen van het gebruik en de locatie van het apparaat.
9: Handhaving
• Ten negende zou kunnen worden onderzocht hoe de handhaving van het juridische kader kan worden versterkt, door het ontwikkelen van een gezamenlijke strategie door de gemeenten, de Autoriteit Persoonsgegevens en het Openbaar Ministerie.
10: Vergoeding
• Tot slot zou kunnen worden onderzocht in hoeverre het mogelijk is om burgers een standaardvergoeding toe te kennen bij onrechtmatige gegevensverzameling door medeburgers door middel van drones en spionageproducten.

Bijlage

I Lijst Experts

Wiebe de Jager	Dronewatch.nl
Rachel Finn	Trilateral Research
Sander Flight	sanderflight.nl
Bart Custers	Leiden Universiteit
Tim de Boer	Droneland
Tjeerd Tiedemann	Luchtvaartpolitie
Denise Eikelenboom	Public Air Services
Wille-Anne van 't Zelfde	Gemeente Molenlanden
Mathilda Poirot	Gemeente Molenlanden
Jan-Dirk Verheij	Werelderfgoed Kinderdijk verantwoordelijke

II Interviewleidraad

INTRO:

Voorstellen, doel interview, aanpak, toestemming, tijdsduur

ALGEMENE VRAGEN:

1. **Op welke manier houd jij je bezig met hobbydrones?**
2. **Welk ervaring heb jij met het vliegen van drones?**
3. **Hoe lang houd jij je al bezig met drones?**

Hobbydrones:

1. **Welke kwesties op het gebied van drones verdienen volgens jouw aandacht op dit moment?**
2. **Hoe zie jij de ontwikkeling van drones en het gebruik veranderen in de komende**
3. **5-10 jaar?**

Uitdagingen privacy

1. **Denk je dat het gebruik van hobbydrones op zich privacyrisico's met zich meebrengt voor mensen in de maatschappij en zo ja, welke?**
2. **Op welke manier beïnvloeden de ontwikkelingen op het gebied van drones deze risico's?**
3. **In welke situatie(s) zou je je zelf ongemakkelijk voelen als je weet dat anderen je opnemen en afluisteren?**
4. **Zou je meer ondersteuning willen op het gebied van privacy? Zo ja, uit welke hoek zou die idealiter moeten komen?**
5. **Zijn er bepaalde toepassingen van drones die verboden moet zijn/blijven/worden?**

Privacy en gegevensbescherming wetgeving

1. **Op welke manier speelt privacy een rol bij jouw eigen drone activiteiten? (En in die van je bedrijf?)**
2. **Kan je een voorbeeld geven van een moment waarop privacy een duidelijke rol speelde?**
3. **Hoe speelt wet- en regelgeving rondom privacy een rol in jouw activiteiten? Kan je daar een voorbeeld van geven?**
4. **Hoe blijven jij en andere op de hoogste van relevante wet- en regelgeving?**
5. **Helpt deze wet -en regelgeving bij de ontwikkeling en/of gebruik van drones?**
6. **Verhindert of bemoeilijkt deze wet -en regelgeving de dingen die je zou willen ondernemen?**

7. **Als je het voor het zeggen had, wat voor regelgeving zou je dan invoeren/aanpassen/afvoeren?**

Best Practices privacy

1. **In hoeverre worden er technische maatregelen genomen om privacyrisico's te beperken?**
2. **Welke partijen houden zich bezig met privacy en in hoeverre zijn zij succesvol in het beperken van de risico's?**
3. **Welke andere maatregelen helpen bij het beperken van de privacyrisico's?**
4. **Wat vind jij in jouw domein het beste voorbeeld van een privacy-vriendelijk gebruik van drones? Wat maakt dat dit succesvol is?**

Overige

1. **Wat hebben we nog niet besproken wat zeker nog moet genoemd worden?**
2. **Waar zou je met het bedrijf over 5 jaar willen staan?**

III Vignetten voor focusgroep met hobbydronevliegers

1.

Menno is een jonge man die samen met zijn moeder op de 7e verdieping van een flatgebouw woont met uitzicht op een charmant kanaaltje en een rij hoge bomen. Hij is al een tijdje verliefd op Sophie, zijn mooie buurvrouw. Hij is echter te verlegen om haar in de lift aan te spreken en haar mee uit te vragen.

Twee maanden geleden besloot Menno een goedkope drone met een camera te kopen. Zijn bedoeling was om Sophie te bespioneren om te weten te komen wat haar interesses zijn: welke programma's kijkt ze op tv, wat voor eten vindt ze lekker, of ze graag leest en zo verder. Hij dacht dat hij haar hierdoor beter zou leren kennen en betere gesprekken met haar zou kunnen beginnen, als hij haar in het gebouw tegenkwam. Bovendien zou dit haar ervan kunnen overtuigen dat ze veel gemeen hebben waardoor ze misschien met hem op een date gaat. Hij zocht op het web naar een 'mini drone met camera' en kocht er een voor 80 euro. Met een vliegtijd van twaalf minuten, een vliegbereik van honderd meter, de grootte van een kleine vogel (10x10x10x10 cm) en een degelijke camera (720p HD, 2 megapixel) die live-streaming mogelijk maakt, leek deze drone het ideale spionageproduct.

Gedurende twee maanden heeft Menno de drone gebruikt om de activiteiten van Sophie vast te leggen. Hoewel hij slechts tien minuten per dag (de vliegtijd van de drone) 's avonds (wanneer Sophie terugkomt van haar werk) opneemt, doet hij dit de laatste twee maanden meerdere keren per week. Meer concreet, vroeg in de avond ging hij naar het kanaal voor het gebouw en vloog de drone op de hoogte van de ramen van de 7e verdieping (ca. 21m). Hij hield de drone meestal op 15m afstand van haar ramen en verscholen achter de hoge bomen op straat. Hij observeerde dan het gedrag van Sophie via de livestream van de drone op zijn smartphone. Als hij echter zou merken dat ze bijvoorbeeld iets op tv kijkt of een boek leest, zou hij zijn kleine drone heel dicht bij haar ramen vliegen om de show of het boek te herkennen.

Op een van die momenten, na twee maanden spionage door Menno, zag Sophie de drone voor het eerst voor haar raam. Ze schreeuwde en rende de kamer uit. Menno parkeerde de drone snel en verstopte zich van de straat. Daarna waren de gordijnen van Sophie’s kamer vaker dicht dan niet dicht; iets wat haar helemaal niet beviel, vooral omdat ze genoot van haar uitzicht over het kanaal. Eigenlijk voelde ze zich een tijdje erg ongemakkelijk in haar eigen huis, bang voor de volgende keer dat een drone haar thuisleven zou binnendringen.

Door Sophie twee maanden lang op deze manier te bespioneren, kon Menno heel wat informatie verzamelen over haar privéleven. Menno concludeert dat hij genoeg geleerd heeft en besluit te stoppen met zijn spionage. Als hij Sophie de volgende keer in de lift ontmoet, knoopt hij een praatje met haar aan over een tv-show waarvan hij inmiddels weet dat zij die vaak kijkt. Sophie is aangenaam verrast en begint enthousiast te discussiëren over de laatste episode. Ze blijven zo

doorkletsen wanneer ze elkaar de komende maanden in het gebouw tegenkomen. Ze hebben een goede relatie opgebouwd. Tot slot heeft Menno de moed bij elkaar verzameld om haar om haar mee uit te vragen en Sophie stemt hier mee in.

2.

Eelco is een techneut van middelbare leeftijd die gelooft dat de klimaatverandering niet echt is. Hij brengt zijn tijd graag door met het bezoeken van websites die alternatieven perspectieven op de actualiteit geven die doorgaans niet in de huidige nieuws media worden besproken. Hij maakt zich zorgen over een kleine groep mensen in zijn stad die elke vrijdag (een onderdeel van de wereldwijde 'Fridays for Future' beweging[466]) voor het gebouw van de lokale overheid bijeenkomen om op vreedzame wijze te protesteren tegen de opwarming van de aarde, het meest recentelijk in verband gebracht met de Amazonebranden in Brazilië. Eelco ziet de activisten als gevaarlijk. Om het nog erger te maken, hebben de lokale nieuwsfeiten melding gemaakt van hun protesten, waardoor de 'leugens' over de klimaatverandering verder worden verspreid. Eelco besluit dan ook de zaak in eigen hand te nemen en de demonstranten te stoppen. Hij kan dus worden omschreven als een verontruste burger die zijn eigen moraal aan anderen wil opleggen.

Eelco weet dat de groep een wettelijk recht heeft om zich op deze manier te verzamelen, dus hij wil een andere manier bedenken om hun protest te voorkomen. Hij besluit hen in diskrediet te brengen door negatieve informatie over hen te verkrijgen. Om dat te doen, bedenkt hij een plan met onder meer een klein drone met een microfoon. Door te googelen ontdekt hij dat drones meestal met camera's worden geleverd, maar zonder microfoon. Hij ondervindt dat het monteren van een externe microfoon op een drone de goedkoopste oplossing met het beste geluid is. Hij vindt een website, die hem stap voor stap laat zien hoe hij dit moet doen. Hij bestelt dus een goedkoop drone met een camera en een vliegtijd van twintig minuten (minder dan 150 euro) en monteert hier een externe microfoon op. Dit stelt hem in staat om de video- en audio-feed van de drone (video en audio) door te sturen naar zijn smartphone en deze vervolgens op te nemen.

Op een vrijdag, wanneer de kleine groep zich op hun gebruikelijke plaats voor het gebouw van de lokale overheid bevindt, verstopt Eelco zich achter enkele struiken, ongeveer 150 meter van de groep. Hij vliegt zijn drone met de microfoon relatief dicht bij de groep, maar zorgt ervoor dat hij af en toe wegvliegt om niet al te veel argwaan te wekken. Na een korte tijd merkt de groep de drone op, maar ze maken zich geen zorgen. Ze gaan er niet van uit dat aan de drone een microfoon gemonteerd is (de microfoon is inderdaad niet zichtbaar) en deze in staat is om hun gesprekken op te nemen. Door gebruik te maken van een extra batterij die bij de drone is

[466] Zie Fridaysforfuture.org

geleverd, is Eelco in staat om een volle veertig minuten de gesprekken van de groep af te luisteren en heimelijk op te nemen. Tot Eelco's teleurstelling is het grootste deel van het gesprek van de groep niet nuttig voor zijn doel. Om hun karakter bloot te leggen, besluit hij daarom de opnames te bewerken door in de opname te knippen en bepaalde delen van het gesprek te combineren. Hierdoor wil hij de milieuactivisten laten klinken alsof ze vleesliefhebbers zijn die niet-milieuvriendelijk gedrag vertonen, zoals vliegen. Om hen en hun beweging in diskrediet te brengen, stuurt Eelco al het bewerkte materiaal naar het lokale nieuws.