Drones en privacy

Handleiding voor een gebruik van drones dat voldoet aan de waarborgen voor bescherming van de privacy

Ministerie van Veiligheid en Justitie

25 november 2015

Inleiding

Het gebruik van drones maakt een stormachtige ontwikkeling door. Drones zijn op afstand bestuurde, onbemande luchtvaartuigen. Zij staan ook wel bekend als "Remotely Piloted Aircraft Systems" (RPAS) of "Unmanned Aerial Vehicles" (UAV).

Door deze stormachtige ontwikkeling rijzen steeds meer vragen omtrent de privacy-aspecten die aan het gebruik van drones zijn verbonden. Het gebruik daarvan kan immers een inbreuk op de privacy opleveren en daardoor consequenties hebben. Doel van deze handleiding is om op een aantal van deze vragen antwoord te geven.

Voordat bij deze vragen wordt stilgestaan, is het van belang onderscheid te maken tussen bescherming van de privacy en bescherming van persoonsgegevens. Het recht op bescherming van de persoonlijke levenssfeer ("privacy") is onder meer neergelegd in het Europees Verdrag tot bescherming van de Rechten van de Mens (EVRM) en onze Grondwet. Dit recht beschermt meer dan alleen persoonsgegevens. Het beschermt ook onze ruimtelijke, relationele en lichamelijke privacy. Het recht op bescherming van persoonsgegevens als onderdeel van het recht op privacy is eveneens vastgelegd in Grondwet. Dit recht is op basis van de zgn. Europese Privacyrichtlijn uitgewerkt in onder meer de Wet bescherming persoonsgegevens (Wbp). Voor specifieke categorieën van persoonsgegevens zijn aparte wetten gemaakt, zoals de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens. Dergelijke wetten worden in deze handleiding vanwege hun wel zeer specifieke karakter verder buiten beschouwing gelaten.

De vragen die hierna, gegroepeerd naar thema, achtereenvolgens aan de orde komen, zijn:

Risico's voor onze privacy

- Met welke instrumenten kunnen drones zijn uitgerust die onze privacy kunnen raken?
- Voor welke doelen kunnen drones worden ingezet die onze privacy kunnen raken?
- Welke risico's levert het gebruik van drones op voor onze privacy?
- Op welke manieren kunnen de risico's voor onze privacy worden verminderd?

Luchtvaartregelgeving

- In hoeverre is bij het gebruik van drones de luchtvaartregelgeving relevant met het oog op onze privacy?

EVRM en Grondwet

- Wanneer is bij het gebruik van drones sprake van een inbreuk op het recht op privacy?
- Wanneer kan een inbreuk op het recht op privacy door het gebruik van drones gerechtvaardigd zijn?

Strafrecht

Wet bescherming persoonsgegevens

Gebruik door politie voor uitvoering van de politietaak

Gebruik door gemeenten, burgers of bedrijven voor cameratoezicht

Methoden om de privacy te beschermen

- Hoe kan bij het gebruik van drones een Privacy Impact Assessment de risico's voor onze privacy verminderen?
- Hoe kunnen bij het gebruik van drones "Privacy by Design" en "Privacy by Default" de risico's voor onze privacy verminderen?
- Hoe kunnen gedragscodes bij het gebruik van drones de risico's voor onze privacy verminderen?
- Hoe kan certificering bij het gebruik van drones de risico's voor onze privacy verminderen?
- Hoe kunnen privacy audits bij het gebruik van drones de risico's voor onze privacy verminderen?

Deze handleiding is bestemd voor zowel bedrijven als overheidsorganisaties die drones gebruiken, en ook voor degene die recreatief met een drone vliegt. Het hangt van de gebruiker af welke vragen en antwoorden voor hem het meest relevant zijn.

In de antwoorden op bovengenoemde vragen wordt soms uitgegaan van een situatie waarin een drone boven mensenmenigten en gebouwen vliegt. Het is van belang daarbij rekening te houden met het feit dat de luchtvaartregelgeving dat vooralsnog slechts in zeer beperkte mate toestaat. Dit impliceert dat, als men zich aan de huidige luchtvaartregelgeving houdt, de kans dat mensen in beeld komen, niet erg groot is Zie in dat verband het woord op de vraag "In hoeverre is bij het gebruik van drones de luchtvaartregelgeving relevant met het oog op onze privacy?"

Tot slot nog dit. De privacywetgeving is naar haar aard tamelijk abstract, omdat het niet mogelijk is voor elke situatie waarin de privacy in het geding is, een specifieke regel te geven. Zij bevat daarom vooral criteria aan de hand waarvan in een concrete situatie een nadere afweging dient plaats te vinden. Deze handleiding beoogt meer houvast te bieden bij afwegingen die bij het gebruik van drones moeten worden gemaakt. Gelet op het karakter van de privacywetgeving is het echter maar zelden mogelijk in deze handleiding een zodanig antwoord op een vraag te geven dat geen enkele nadere afweging meer nodig zou zijn. Anders gezegd, de omstandigheden van het specifieke geval zullen toch veelal moeten worden meegewogen om een vraag van een definitief antwoord te kunnen voorzien.

Deze handleiding is opgesteld door het ministerie van Veiligheid en Justitie. Zij zal periodiek worden geactualiseerd, als ontwikkelingen in het recht of de technologie daartoe aanleiding geven.

Aan het slot van deze handleiding is een overzicht opgenomen van de voornaamste geraadpleegde bronnen.

Risico's voor onze privacy

Met welke instrumenten kunnen drones zijn uitgerust die onze privacy kunnen raken?

Op drones kunnen allerlei instrumenten als zgn. "payloads" zijn gemonteerd. Deze instrumenten kunnen – op zichzelf of in combinatie met elkaar - op verschillende wijze en in verschillende mate informatie over personen opleveren en daarmee hun privacy raken. Te denken valt aan:

- Camera's,
- Sensoren voor onderschepping van telecommunicatieverkeer,
- Microfoons,
- Radars,
- Global Positioning Systems (GPS),
- Wifi-routers.

Camera's vormen de instrumenten die vooralsnog het meest op drones worden gebruikt. Om die reden wordt nog wat dieper ingegaan op de verschillende types camera's en gebruiksmogelijkheden:

- Camera's kunnen van het volgende type zijn: fotocamera, "gewone" videocamera, nachtzichtcamera, infraroodcamera, ultravioletcamera, warmtebeeldcamera etc.[1]
- Camera's kunnen, al naar gelang hun technische mogelijkheden, als monitor worden gebruikt, maar ook beelden opslaan of beelden versturen naar een grondstation.
- Camera's kunnen technieken bevatten waarmee kan worden ingezoomd, zodat zij een gedetailleerd beeld kunnen geven van personen of objecten op de grond.
- Camera's kunnen "intelligent" zijn, zodat zij individuen, kentekens, voorwerpen of situaties kunnen herkennen of bepaalde gedragingen als "abnormaal" identificeren.
- Een drone kan met verschillende camera's zijn uitgerust, zodat het mogelijk wordt een 360°-beeld te scheppen.

Het gebruik van andere sensoren kan mogelijk ook de privacy raken, maar alleen als de data die zij opleveren, worden gecombineerd met andere data. Gedacht kan worden aan sensoren voor het detecteren van biologische, chemische of nucleaire sporen. Dergelijke sporen kunnen mogelijk worden verbonden met mensen die deze hebben achtergelaten.

Voor welke doelen kunnen drones worden ingezet die onze privacy kunnen raken?

Oorspronkelijk werden drones gebruikt voor militaire doeleinden, maar zij worden in toenemende mate ook voor civiele doeleinden gebruikt. Te denken valt aan:

- Veiligheid (opsporing, handhaving van de openbare orde, "search and rescue", calamiteiten, branden en rampen, hulpverlening);

[1] Sommige types hebben deels dezelfde functies. Zo kan een infraroodcamera als nachtzichtcamera worden gebruikt.

- Infrastructuur (inspectie van windmolens, dijken, bruggen, hoogspanningsmasten, bovenleidingen, grote installaties);
- Bewaken en beveiligen (beveiligen publieke en private objecten, grensbewaking);
- Onderzoek (cartografie, milieu, weer en klimaat);
- Land- en tuinbouw, veeteelt (inspectie landbouwgronden, kassen, bemesting, detectie dierziekten en locaties);
- Media en journalistiek (fotografie en filmopnames, bijvoorbeeld ten behoeve van (sport)evenementen, (onderzoeks)reportages, speelfilms, tv-drama en documentaires)
- Hobbyvliegen (eventueel voor maken van foto's en filmopnames).[2]

Bij gebruik voor al deze doeleinden is het mogelijk dat personen "in beeld" komen of objecten die met bepaalde personen in verbinding kunnen worden gebracht. Daarmee kan de privacy van betrokkenen in het geding zijn.

Bij het ene doel is de kans daarop wat groter dan bij een ander doel. Zo zal bij het gebruik van drones ten behoeve van de opsporing al snel de privacy in het geding zijn, omdat opsporing gericht is op het vinden van daders. Daarentegen zal het min of meer toeval zijn dat bij een inspectie van een windmolen ook mensen in beeld komen.

Welke risico's levert het gebruik van drones op voor onze privacy?[3]

Drones kunnen door hun kleine formaat en door de hoogte waarop zij vliegen, soms bijna niet zichtbaar en hoorbaar zijn. Een mens kan zich om die redenen er niet van bewust zijn dat een drone boven hem vliegt die opnamen van hem maakt of op andere wijze gegevens over hem vastlegt. Drones kunnen om deze redenen zeer wel worden ingezet om iemand te bespieden. Denk hierbij aan gebruik van drones door paparazzi die de gangen van bekende Nederlanders willen volgen, of door privédetectives.

Drones kunnen ook worden gebruikt in situaties waarin ze wel worden waargenomen, maar niet worden verwacht. Mensen die in een drukke woonwijk op de begane grond wonen, kunnen erop bedacht zijn dat anderen bij hen wel eens naar binnen kijken. Zij kunnen daartegen desgewenst maatregelen hebben genomen, zoals het aanbrengen van vitrage. Mensen die op bijvoorbeeld een twintigste etage van een flatgebouw wonen, hoeven er echter geen rekening mee te houden dat er bij hen naar binnen wordt gekeken. Als dan een drone met een camera voor hun ramen verschijnt, moet al gauw worden aangenomen dat hun redelijke verwachtingen omtrent hun privacy zijn geschonden.

Het feit dat de piloot van de drone een soms forse afstand kan bewaren tot een persoon die hij met behulp van bijvoorbeeld een camera op de drone filmt, verlaagt de mentale drempel om deze persoon te filmen. Dit wordt wel het "dehumanisation effect" van het gebruik van drones genoemd. Dit effect kan ook ongemerkt tot een groei van dit gebruik leiden.

---

[2] Vgl. Kamerstukken II 2014-2015, 30806, nr. 28, blz. 3.
[3] Zie ook Finn, blz. 23-52; Custers, blz. 75-77; WP 29, blz. 7-8.

Drones kunnen veel intrusiever voor de privacy zijn dan andere methodes om gegevens te verzamelen. Dat wil zeggen dat zij op een indringender wijze in het leven van burgers kunnen binnendringen dan met andere instrumenten mogelijk is. De mogelijkheden van bij voorbeeld camera's op een drone overstijgen die van een camera op de grond, omdat een drone grenzen kan overschrijden die een private ruimte afbakenen (muren, ramen, traliewerk etc.). Zo kan met een camera op een drone iemand worden gefilmd die niet of schaars gekleed in zijn of haar ommuurde achtertuin ligt te zonnen, waar dat met een camera op de grond niet mogelijk is.

Een drone kan niet alleen een ruimte binnendringen, daar waar dat met andere methodes onmogelijk is, maar hij kan ook zijn uitgerust met technologie die het mogelijk maakt informatie te verzamelen die met diezelfde technologie niet gemakkelijk op andere wijze is te verzamelen. Te denken valt aan technologie om informatie te verzamelen door muren, daken of wolken heen, niet alleen overdag maar ook 's nachts.

Zelfs als een drone niet met een camera of andere sensor is uitgerust, kan het vliegen van een drone boven mensen een inbreuk op iemands privacyverwachtingen geven. Mensen kunnen immers vaak niet zien of een drone met een camera is uitgerust. Dat kan ertoe leiden dat iemand zich onder invloed van zo'n overvliegende drone toch anders gaat gedragen. Dat wordt wel het "chilling effect" van drones genoemd: je gaat je minder vrij gedragen dan anders het geval zou zijn. Dat kan, afhankelijk van de situatie, ook betrekking hebben op de uitoefening van je grondrechten, zoals de vrijheid van meningsuiting of het recht van vereniging en vergadering.

Het gebruik van drones is weinig transparant. Terwijl helicopters vaak een "striping" hebben waardoor zij herkenbaar zijn (denk aan politie- en traumahelicopters), heeft een drone meestal geen onderscheidingstekens. Als zij deze wel zou hebben, is het zeer de vraag of deze, gelet op het formaat van de drone, vanaf de grond zichtbaar zouden zijn. Daarnaast kan het ook moeilijk zijn om de persoon waar te nemen die de drone bestuurt, en de organisatie te kennen waartoe deze persoon eventueel behoort. En kan het moeilijk zijn om te weten welke doeleinden met het gebruik van de drone worden nagestreefd of welke gegevens worden ingezameld.

Een drone kan in potentie informatie inzamelen over zeer grote gebieden: de mobiliteit van drones maakt het mogelijk om zeer grote zones te beslaan, van meerdere vierkante kilometers. Zo kan een drone ook van veel mensen tegelijk gegevens opslaan.[4]

Drones kunnen met behulp van verschillende sensoren een zeer breed scala aan verschillende informatie verzamelen. Zo kan een drone niet alleen videobeelden of foto's ontvangen, maar hij kan ook, al naargelang de technologie waarmee hij is uitgerust, communicatiesignalen afluisteren, personen opsporen en identificeren, hun bewegingen opnemen of verplaatsingen signaleren die als abnormaal worden beschouwd.

Denkbaar is dat een drone op termijn een individu gedurende een langere periode kan volgen, zonder de nadelen die aan andere methoden van observatie met behulp van bijvoorbeeld een voertuig, een helicopter of alleen visuele waarneming zijn verbonden

[4] Dit risico is vooralsnog laag, omdat de luchtvaartregelgeving de piloot van een drone verplicht zijn drone binnen gezichtsafstand te houden en vliegen boven mensenmenigten in beginsel niet is toegestaan.

(gebrek aan snelheid, hogere kosten, moeilijke toegang, gebrekkige discretie).

Drones kunnen een enorme hoeveelheid informatie over personen verzamelen zonder deze personen te onderscheiden. Anders gezegd: de verzameling van informatie zal meestal plaatsvinden zonder enig onderscheidend criterium en zonder een voorafgaande sortering van informatie die relevant is voor de doeleinden waarvoor de drone wordt ingezet.

Sensoren op drones kunnen ook leiden tot "function creep". Dat is het verschijnsel dat voor een bepaald doel sensoren op – in dit geval – drones worden gemonteerd die vervolgens ook voor een ander doel worden gebruikt. Te denken valt aan de situatie dat een makelaar met behulp van een drone huizen filmt die hij wil verkopen, maar "en passant" ook mensen, huizen, tuinen en auto's in de naaste omgeving filmt om een beeld te krijgen van de welvaart van de bewoners van de wijk. Daarmee is de privacy van die andere mensen in het geding.

Tot slot wordt gewezen op het risico van datalekken. Omdat de data die een drone met behulp van sensoren vastlegt, meestal via een draadloze verbinding naar een grondstation gaan, bestaat het risico dat deze data worden onderschept. Aldus ontstaat ook een risico voor de privacy van mensen van wie de data zijn vastgelegd.

Welke consequenties de wetgeving aan deze risico's voor onze privacy verbindt, komt in antwoorden op volgende vragen tot uiting.

Op welke manieren kunnen de risico's voor onze privacy worden verminderd?

Personen of organisaties die drones gebruiken, kunnen de risico's die dit meebrengt voor onze privacy, op verschillende manieren wegnemen of verminderen. Daarbij kan worden gedacht aan:

- het uitvoeren van een Privacy Impact Assessment[5],
- het toepassen van "Privacy by Design" en "Privacy by Default"[6],
- het uitvoeren van beveiligingsmaatregelen[7],
- gedragscodes[8],
- certificering[9],
- transparantie[10],
- het uitvoeren van privacy audits[11].

---

[5] Zie nader: Hoe kan bij het gebruik van drones een Privacy Impact Assessment de risico's voor onze privacy verminderen?
[6] Zie nader: Hoe kunnen bij het gebruik van drones "Privacy by Design" en "Privacy by Default" de risico's voor onze privacy verminderen?
[7] Zie nader: Hoe moeten persoonsgegevens die met behulp van drones zijn verzameld, worden beveiligd?
[8] Zie nader: Hoe kunnen gedragscodes bij het gebruik van drones de risico's voor onze privacy verminderen?
[9] Zie nader: Hoe kan certificering bij het gebruik van drones de risico's voor onze privacy verminderen?
[10] Zie nader: In hoeverre moeten personen van wie met behulp van drones gegevens zijn verwerkt, daarover worden geïnformeerd? en Hoe kunnen bij het gebruik van drones "Privacy by Design" en "Privacy by Default" de risico's voor onze privacy verminderen?, onder "transparantie".
[11] Zie nader: Hoe kunnen privacy audits bij het gebruik van drones de risico's voor onze privacy verminderen?

Elk van deze manieren kan afzonderlijk worden toegepast. Sommige manieren liggen echter in elkaars verlengde, zodat het logisch is deze cumulatief toe te passen. Zo kunnen de resultaten van een Privacy Impact Assessment richting geven aan het toepassen van "Privacy by Design".

Luchtvaartregelgeving

In hoeverre is bij het gebruik van drones de luchtvaartregelgeving relevant met het oog op onze privacy?

De luchtvaartregelgeving met betrekking tot drones is bedoeld voor het bevorderen van de luchtvaartveiligheid. Toch bevat deze regelgeving ook bepalingen die als neveneffect hebben dat de privacy wordt beschermd.

In de luchtvaartregelgeving wordt een onderscheid gemaakt tussen drones van maximaal 25 kg die uitsluitend worden gebruikt voor luchtvaartvertoning, recreatie of sport (modelluchtvaartuigen), en drones van maximaal 150 kg, niet zijnde modelluchtvaartuigen (RPA). "Recreatieve" drones tot 25 kg vallen onder de Regeling Modelvliegen, beroepsmatig gebruikte drones van 0 tot 150 kg onder de Regeling op afstand bestuurde luchtvaartuigen.

Op grond van artikel 2 van de Regeling Modelvliegen[12] is het, voor zover relevant in relatie tot de bescherming van de privacy, verboden modelluchtvaartuigen te laten vliegen:

1. hoger dan 120 meter boven de grond of het water,
2. boven gebieden met aaneengesloten bebouwing of kunstwerken, industrie- en havengebieden daaronder begrepen, dan wel boven mensenmenigten of boven spoorlijnen of voor motorrijtuigen toegankelijke verharde openbare wegen, met uitzondering van wegen in 30 km-zones binnen de bebouwde kom en wegen in 60 km-gebieden buiten de bebouwde kom,
3. wanneer er vanaf de grond tijdens de gehele vlucht geen goed zicht is op het modelluchtvaartuig en het luchtruim daaromheen,
4. wanneer de bestuurder tijdens de gehele vlucht geen goed zicht op het modelluchtvaartuig houdt.

In afwijking van onderdeel 1 zijn:

a. vluchten binnen het verband van een bij de Koninklijke Nederlandse Vereniging voor Luchtvaart of de Federatie Limburgse Radio Controle Vliegers aangesloten vereniging toegestaan tot een hoogte van maximaal 300 meter boven de grond of het water en,
b. vluchten toegestaan tot een hoogte van maximaal 450 meter boven de grond of het water, mits dit gebeurt binnen een aerodrome traffic zone van een militaire luchthaven waarop modelvliegen is toegestaan en dit gebied exclusief voor modelvliegen wordt gebruikt of met de andere gebruiker(s) sluitende afspraken zijn gemaakt inzake separatie in het luchtruim.

[12] Laatstelijk gewijzigd bij regeling van 23 april 2015, Stcrt. 2015, nr. 12034.

Op grond van de artikelen 14 en 15 van de Regeling op afstand bestuurde luchtvaartuigen[13] is het, behoudens enkele mogelijkheden van ontheffing, verboden RPA te laten vliegen:

1. hoger dan 120 meter boven de grond of het water,
2. op een horizontale afstand van minder dan 150 meter tot mensenmenigten, aaneengesloten bebouwing, in gebruik zijnde autosnelwegen, autowegen of wegen waar een maximale snelheid van 80 kilometer per uur geldt,
3. op een horizontale afstand van minder dan 50 meter tot industrie- en havengebieden,
4. op een horizontale afstand van minder dan 50 meter tot vaartuigen, voertuigen, kunstwerken en spoorlijnen, mits zij zich niet in gebieden als bedoeld onder 2 bevinden.

Een en ander impliceert dat beide categorieën drones niet dicht in de buurt mogen komen van plaatsen waar zich mensenmenigten of doorgaans mensen bevinden. In gebieden waar zij wel mogen worden gebruikt, zullen zich slechts incidenteel en dan nog in kleinen getale mensen bevinden. Te denken valt in dit verband aan weilanden en natuurgebieden. Bij het gebruik van drones in dergelijke gebieden zal om die reden de privacy niet snel in het geding zijn.

Op grond van artikel 5.5 van de Wet luchtvaart kan de Minister van Infrastructuur en Milieu een ontheffing (voor een bepaalde periode) of vrijstelling (permanent) verlenen van de hier genoemde verboden met betrekking tot het vliegen met drones. Aan de ontheffing of vrijstelling kunnen voorschriften of beperkingen worden verbonden. Dat impliceert dat met een ontheffing of vrijstelling toch mag worden gevlogen boven plaatsen waar zich mensenmenigten of doorgaans mensen bevinden.

Het voornemen bestaat in de regelgeving de volgende drie categorieën van op afstand bestuurde luchtvaartuigen te introduceren:

- Mini-drones tot 4 kg waarvoor de piloot geen brevet nodig heeft en de drone niet behoeft te worden gekeurd maar het gebruik ten behoeve van de veiligheid wordt beperkt;
- Lichte drones 4-150kg waarbij een gebruiker een brevet moet hebben, de drone gekeurd moet zijn en de operatie in een goed te keuren handboek beschreven moet zijn;
- Modelvliegtuigen tot 150 kg die op afgebakende modelvliegterreinen mogen vliegen.

De mini-drone zal tot maximaal 50 m hoogte mogen vliegen. Verder zal de mini-drone minstens 50 meter horizontale afstand moeten houden van mensenmenigten, aaneengesloten bebouwing, in gebruik zijnde autosnelwegen, autowegen of wegen, industrie- en havengebieden, vaartuigen, voertuigen, kunstwerken en spoorlijnen. Uitvoering van dit voornemen impliceert dat de mogelijkheden voor beroepsmatig gebruik van mini-drones aanzienlijk zullen worden verruimd, terwijl de mogelijkheden voor recreatief gebruik buiten afgebakende gebieden zullen worden ingeperkt. Zo zullen recreanten buiten deze gebieden nog slechts met mini-drones mogen vliegen en dan

[13] Stcrt. 2015, nr. 12034.

slechts tot 50 meter hoogte in plaats van de huidige hoogte van 120 meter en met een horizontale afstand van 50 meter tot eerdergenoemde gebieden en objecten, waar die afstand nu nog nihil mag zijn.

De toekomstige regelgeving voor de mini-drone zal uiteindelijk mede afhankelijk zijn van de Europese plannen op dit punt.

Voor meer informatie:

- http://www.rijksoverheid.nl/onderwerpen/luchtvaart/veiligheid-luchtvaart/veiligheid-drones
- http://www.internetconsultatie.nl/veiligheidsregelgeving_drones

EVRM en Grondwet

Wanneer is bij het gebruik van drones sprake van een inbreuk op het recht op privacy?

Voorop gesteld zij dat, wanneer er sprake is van een inbreuk op het recht op privacy, dit nog niet betekent dat die inbreuk niet is toegestaan. De vraag wanneer een inbreuk al dan niet gerechtvaardigd kan zijn, komt pas in de volgende paragraaf aan de orde.

Op grond van artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM) heeft een ieder recht op respect voor zijn privé leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie. Daarnaast bepaalt artikel 10 van de Grondwet dat een ieder, behoudens bij of krachtens de wet te stellen beperkingen, recht heeft op eerbiediging van zijn persoonlijke levenssfeer. Dat betekent dat een beperking van dit recht een grondslag moet hebben in een wet.

Voor een antwoord op de vraag wanneer het gebruik van een drone inbreuk maakt op het recht op privacy, zoals neergelegd in artikel 8 EVRM, is in de eerste plaats van belang of het gebruik de privésfeer raakt. De privésfeer is afgebakend van de publieke sfeer door fysieke grenzen, zoals de muren van de woning, persoonlijke relaties (met familie en vrienden) en door bepaalde categorieën van informatie (persoonlijk, gevoelig, gênant). Het gebruik van een drone om iemand binnen zijn privésfeer te volgen, impliceert ontegenzeggelijk een inbreuk op artikel 8 EVRM.[14]

Of het gebruik van een drone in de publieke sfeer een inbreuk op artikel 8 EVRM oplevert, hangt af van de omstandigheden. Daarbij moet rekening worden gehouden met de "redelijke verwachting van privacy" van mensen in het openbare leven. Afhankelijk van de omstandigheden van het geval wordt de inbreuk op het recht op privacy dan als meer of minder ingrijpend beoordeeld.[15]

Wat "een redelijke verwachting van privacy" is, kan bij het gebruik van bijvoorbeeld een camera op een drone anders uitpakken dan wanneer het om een vaste camera op de grond gaat. Immers, wanneer er tijdens een evenement beelden worden gedraaid met een vaste camera, zal het voor een persoon meestal gemakkelijk zijn om de

[14] Finn, blz. 58.
[15] Custers, blz. 107-108.

aanwezigheid van die camera op te merken, zich te richten tot de persoon die filmt of tot zijn eventuele collega's, de doeleinden van de beeldopnames te kennen of om ten minste te kunnen vragen waaruit ze bestaan (journalistiek, beeldopname, documentaire, audiovisuele realisatie, promotiefilm enz.), en om zich ertegen te verzetten dat hij wordt gefilmd. Daarentegen zijn de omstandigheden totaal anders wanneer een drone de beelden maakt. De betrokken personen zijn er zich immers niet altijd van bewust of zijn er niet altijd van op de hoogte gesteld dat ze door een drone worden gefilmd, noch dat hun afbeelding kan worden hergebruikt op diverse media (internet, televisie, geschreven pers) of voor andere doeleinden (reportage, journalistiek, promoten van evenementen enz.). Ook als ze zich wel bewust zijn van de drone, kan het uitermate lastig zijn de operator van de drone te ontdekken en deze om informatie te vragen.

Op grond van deze overwegingen is het plausibel om bij het gebruik van drones het begrip "redelijke verwachtingen" een strikte interpretatie te geven. Naarmate het gebruik van drones in het luchtruim verder wordt geliberaliseerd, mag uit de mogelijkheid dat een individu in de openbare ruimte door een drone wordt gefilmd, niet automatisch de conclusie worden getrokken dat de beeldopnames binnen de redelijke verwachtingen van het individu vallen. Anders gezegd, de technologische evolutie dient er niet toe te leiden dat de verwachtingen van de burgers inzake privacy worden verminderd omwille van het feit dat de inzameling van hun persoonsgegevens gemakkelijker, discreter en minder omkaderd is geworden.[16]

Tegen deze achtergrond kan uit jurisprudentie met betrekking tot artikel 8 EVRM worden afgeleid dat het gebruik van drones in de publieke sfeer een inbreuk op het recht op privacy geeft, indien

1. een drone wordt gebruikt die gegevens over personen op een systematische of duurzame wijze vastlegt, ongeacht de vraag of dit heimelijk of openlijk gebeurt;
2. een geavanceerde camera wordt gebruikt, zoals een infrarood-camera, een nachtcamera, een warmtebeeldcamera of een camera met ingebouwde analysetechnieken, ook als deze camera slechts monitort en geen beelden van personen vastlegt;[17]
3. de met de drone verzamelde informatie openbaar wordt gemaakt.[18]

Van een inbreuk op de privacy in de publieke sfeer zal dus alleen dan geen sprake zijn, indien het gebruik uitsluitend uit het monitoren van activiteiten bestaat, zonder dat beelden worden vastgelegd, beelden openbaar worden gemaakt of gebruik wordt gemaakt van geavanceerde camera's.

Uit de jurisprudentie met betrekking tot artikel 8 EVRM valt verder af te leiden dat het gebruik van drones die met behulp van GPS locaties kunnen bepalen, als minder indringend worden beschouwd dan het gebruik van drones die met camera's opnames maken, of drones die communicatie intercepteren.[19]

---

[16] http://www.privacycommission.be/nl/faq-page/7340#t7340n16583.

[17] Als de camera waarmee wordt gemonitord, een digitale camera is, zal er, indien zij personen herkenbaar in beeld brengt, wel sprake zijn van verwerking van persoonsgegevens. Zie: Wanneer is bij gebruik van een drone sprake van verwerking van persoonsgegevens?

[18] Finn, blz. 61.

[19] Finn, blz. 63.

Wanneer kan een inbreuk op het recht op privacy door het gebruik van een drone gerechtvaardigd zijn?

De overheid mag geen inbreuk op het recht op privacy plegen anders dan voor zover dit bij de wet is voorzien en in een democratische samenleving noodzakelijk is (art. 8, tweede lid, EVRM).

Als de overheid met het gebruik van een drone inbreuk maakt op artikel 8 EVRM, kan dat rechtmatig zijn, indien wordt voldaan aan de voorwaarden die het tweede lid van dat artikel stelt. Deze voorwaarden zijn:

1. dat een van de doelen, zoals genoemd in dat artikellid, wordt nagestreefd,
2. de inbreuk bij wet is voorzien en
3. de maatregel noodzakelijk is in een democratische samenleving.

Aan de eerste voorwaarde kan betrekkelijk eenvoudig worden voldaan, omdat het doel van het gebruik hoogstwaarschijnlijk wel onder één van de genoemde doelen is te scharen: het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

In het kader van de openbare veiligheid of ter voorkoming van wanordelijkheden en strafbare feiten kunnen gemeenten en de politie drones inzetten als vorm van cameratoezicht. Ook hulpverleningsdiensten kunnen voor de bescherming van de gezondheid of de rechten en vrijheden van anderen drones inzetten. Daarbij kan worden gedacht aan de inzet van drones bij bijvoorbeeld calamiteiten of voor het opsporen van vermiste personen.[20]

De inzet van drones door de overheid die de privacy beperkt, moet tevens bij de wet zijn voorzien. Daarbij zal in ogenschouw moeten worden genomen dat verschillende sensoren onder drones verschillende inbreuken op het recht op privacy maken. Afhankelijk van de intensiteit van de inbreuk op het recht op privacy kan meer gedetailleerde regelgeving met beperkingen voor het gebruik van drones op zijn plaats zijn. Daarbij kan worden benadrukt dat het voor burgers duidelijk moet zijn onder welke omstandigheden de inzet van drones mogelijk is en op welke manier het gebruik van drones een inbreuk op de persoonlijke levenssfeer kan maken. De eis van voorzienbaarheid speelt een nadrukkelijke rol bij technologieën die steeds geavanceerder en indringender worden.[21]

Het vereiste dat de inzet van drones die de privacy beperkt, noodzakelijk moet zijn in een democratische samenleving houdt in dat er een dringende maatschappelijke behoefte moet bestaan voor de inzet van drones. De maatregel dient daarbij tevens proportioneel te zijn, dat wil zeggen dat de inbreuk op de privacy van de betrokkene

[20] Custers, blz. 108-109.
[21] Custers, blz. 109.

niet onevenredig mag zijn in verhouding tot het doel dat met de inbreuk wordt verwezenlijkt (proportionaliteitstoets). De overheid zal dus moeten motiveren welke toegevoegde waarde de inzet van drones zal opleveren en hoe deze inzet opweegt tegen het belang van het recht op privacy. Zij zal ook moeten nagaan of er geen minder ingrijpende middelen voorhanden zijn (de subsidiariteitstoets).[22]

Het EVRM stelt grenzen aan beperkingen op het recht op privacy door de overheid. Als het gaat om gebruik van drones door particulieren, zijn uit een oogpunt van bescherming van de privacy de voorschriften van belang die in de Wet bescherming persoonsgegevens zijn vastgelegd. Deze komen verderop aan bod.

Strafrecht

Welke grenzen stelt het strafrecht aan het gebruik van camera's op drones?

Bij het gebruik van drones met camera's zijn in de eerste plaats de bepalingen in het Wetboek van Strafrecht (Sr) over het heimelijk maken van afbeeldingen relevant.

In artikel 139f Sr is het heimelijk filmen in een woning en op niet voor het publiek toegankelijke plaatsen strafbaar gesteld. Bij het gebruik van drones kan dan worden gedacht aan een drone die enige tijd voor een raam of boven een tuin zweeft om opnames van een persoon in een besloten plaats te maken. De tuin wordt in de toelichting op het artikel uitdrukkelijk als een besloten plaats aangemerkt waar iemand zich in principe onbespied mag wanen.[23]

Een persoon die in een besloten plaats filmt met een camera op een drone is ingevolge artikel 139f pas strafbaar, als hij bij het filmen opzettelijk en wederrechtelijk een afbeelding van een persoon heeft gemaakt. Het bestanddeel "wederrechtelijk" brengt tot uitdrukking dat opsporingsinstanties of inlichtingendiensten die voor de uitoefening van hun taak binnen de daarvoor geldende kaders heimelijk gebruik maken van camera's op drones, niet strafbaar zijn. Onder omstandigheden geldt hetzelfde met betrekking tot journalisten die heimelijk opnames met drones maken. Dit houdt verband met het recht op vrije nieuwsgaring. Omstandigheden die daarbij een rol spelen, zijn het belang van het onderwerp van berichtgeving dat door middel van een verborgen camera aan het licht moet worden gebracht, de vraag of voor de journalist ook andere mogelijkheden om de noodzakelijke inlichtingen te vergaren openstonden dan het gebruik van een verborgen camera, en de aard en mate waarin met de verborgen camera een inbreuk op de persoonlijke levenssfeer van de afgebeelde personen is gemaakt.[24]

Van een "afbeelding" is slechts sprake, wanneer de gefotografeerde of gefilmde persoon herkenbaar in beeld wordt gebracht.[25] Het is de vraag of bij het fotograferen of filmen

---

[22] Custers, blz. 109, 122.
[23] Kamerstukken II 2000-2001, 27732, nr. 3, blz. 10-11.
[24] Kamerstukken II 2000-2001, 27732, nr. 3, blz. 5-6, 9, 12.
[25] Kamerstukken II 2000-2001, 27732, nr. 3, blz. 9, en nr. 5, blz. 12.

van mensen van bovenaf mensen herkenbaar in beeld komen[26]. Het filmen is heimelijk indien de aanwezigheid van een camera niet op duidelijke wijze kenbaar is gemaakt. De opzet moet zijn gericht op het vervaardigen van een afbeelding en het vervaardigen van een afbeelding van een persoon. Onder het vervaardigen van een afbeelding" vallen ook vormen van digitaal "streamen", zonder opslag of bewaring van beelden.[27] Mogelijk is een persoon niet strafbaar indien een groot maatschappelijk belang wordt gediend bij het heimelijk maken van opnames met drones.[28]

Het heimelijk afbeeldingen maken van personen met een aangebracht technisch hulpmiddel op publiekelijk toegankelijke plaatsen is strafbaar gesteld in artikel 441b Sr. Hiervoor geldt een lagere straf dan voor het heimelijk filmen in besloten plaatsen. Het element van "daartoe aangebracht technisch hulpmiddel" wordt in de wetsgeschiedenis breed geïnterpreteerd. Het technisch hulpmiddel kan ook worden verstopt in een voorwerp, zoals een koffer.[29] Naar analogie kan daarom ook een camera op een drone als een aangebracht technisch hulpmiddel worden gekwalificeerd. Met betrekking tot "heimelijk", "afbeelding" en "wederrechtelijk" geldt hetzelfde als bij artikel 139f is opgemerkt. Van opzet behoeft echter geen sprake te zijn. 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.

Andere bepalingen uit het Wetboek van Strafrecht die onder omstandigheden relevant kunnen zijn bij het gebruik van drones, zijn de artikelen 139c en 139d. In die artikelen is het afluisteren van telecommunicatie en het plaatsen van afluisterapparatuur strafbaar gesteld. Ook bij deze artikelen lijkt de voorwaarde dat er sprake is van een "daartoe aangebracht technisch hulpmiddel" breed te moeten worden geïnterpreteerd, zodat ook het gebruik van drones voor afluisteren daaronder valt.

Verder kan worden gedacht aan de situatie waarin met behulp van camera's op drones naaktfoto's worden gemaakt, die vervolgens worden verspreid of openbaar gemaakt. Dat kan strafbaar zijn als aanranding van iemands goede naam en eer (artikelen 261-262 Sr).

Tot slot valt te wijzen op de situatie dat iemand met een drone stelselmatig een ander belaagt. Dan kan sprake zijn van stalking. Dat is strafbaar op grond van artikel 285b Sr.

---

[26] Van "herkenbaar in beeld komen" kan al sprake zijn, indien iemand louter kan worden herkend aan de hand van een kledingstuk.
[27] Kamerstukken II 2000-2001, 27732, nr. 3, blz. 11 en 4.
[28] Kamerstukken II 2000-2001, 27732, nr. 3, blz. 6.
[29] Kamerstukken II 2000-2001, 27732, nr. 3, blz. 7.

Wet bescherming persoonsgegevens

Wanneer zijn gegevens die met behulp van een drone worden verzameld, persoonsgegevens?

Op grond van artikel 1, onder a, van de Wet bescherming persoonsgegevens (Wbp) is een persoonsgegeven elk gegeven over een geïdentificeerde of identificeerbare natuurlijke persoon.

Een persoon is identificeerbaar indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning, kan worden vastgesteld. Er kan een onderscheid worden gemaakt in direct en indirect identificeerbare gegevens. Direct identificerende gegevens zijn gegevens die betrekking hebben op een persoon waarvan de identiteit zonder veel omwegen eenduidig is vast te stellen, zoals een naam, eventueel in combinatie met het adres en de geboortedatum. Van indirect identificeerbare gegevens is sprake wanneer zij via nadere stappen in verband kunnen worden gebracht met een bepaalde persoon, bij voorbeeld een kenteken. Een gegeven is geen persoonsgegeven, indien doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten.[30]

Bij het gebruik van camera's op drones kunnen personen in beeld komen. Daarmee is nog niet gezegd dat er sprake is van persoonsgegevens. Daarvoor is nodig dat de desbetreffende personen identificeerbaar zijn. Dat kan het geval zijn, indien een gezicht van een persoon herkenbaar in beeld komt. Maar ook een opvallend kledingstuk kan iemand al herkenbaar maken. Een opname door een camera op een drone die alleen de bovenkant van personen laat zien en zonder gebruik van geavanceerde middelen niet tot identificatie van deze personen kan leiden, is geen persoonsgegeven.[31]

Kentekengegevens die met een camera op een drone zijn vastgelegd, zijn persoonsgegevens, als men in staat is de kentekengegevens te vergelijken met gegevens uit het kentekenregister. Dan zijn deze kentekengegevens immers herleidbaar tot een individu. Ook andere informatie die drones kunnen verzamelen en verwerken, zoals biometrische gegevens, locatiegegevens en verkeersgegevens, kunnen worden aangemerkt als persoonsgegevens, indien die informatie betrekking heeft op een geïdentificeerde of identificeerbare persoon.[32]

Of ook opnames van huizen als persoonsgegevens zijn aan te merken, hangt van af van de omstandigheden. Mogelijk is een huis indirect tot een persoon herleidbaar, indien ook het huisnummer zichtbaar is of als een afbeelding of video van een huis samen met andere informatie openbaar wordt gemaakt.[33] Opnames met drones van de leefomstandigheden van vee kunnen onder omstandigheden ook persoonsgegevens opleveren. Als dergelijke opnames worden gemaakt door een organisatie tegen

---

[30] Kamerstukken II 1997-1998, 25892, blz. 47-49.
[31] Finn, blz. 69.
[32] Finn, blz. 68.
[33] Custers, blz. 125.

dierenleed en deze organisatie publiceert de opnames met de naam van de boer, zijn het persoonsgegevens.[34]

Wanneer is bij gebruik van een drone sprake van verwerking van persoonsgegevens?

De Wet bescherming persoonsgegevens (Wbp) is van toepassing op iedere geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens (art. 2 Wbp). Onder "verwerking" wordt verstaan: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens. Hieronder valt in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens (art. 1, onder b, Wbp).

Als een camera op een drone beelden van geïdentificeerde of identificeerbare personen digitaal verwerkt, is er sprake van een verwerking van persoonsgegevens waarop de Wbp van toepassing is. De digitale verwerking is immers een vorm van geautomatiseerde verwerking als bedoeld in artikel 2 van de Wbp. Daarvan is ook sprake, indien men dergelijke beelden maakt en de persoonsgegevens op de beelden pas later bij publicatie of uitzending van de beelden onzichtbaar heeft gemaakt.

Wie is bij gebruik van drones de verantwoordelijke voor de verwerking van persoonsgegevens?

Bij gebruik van drones die persoonsgegevens verwerken, is van belang te bepalen wie de verantwoordelijke is voor de verwerking daarvan. Tegenover deze verantwoordelijke kan een burger om wiens persoonsgegevens het gaat, desgewenst zijn rechten uitoefenen, zoals het recht op inzage in die gegevens. Op de verantwoordelijke rust ook een aantal verplichtingen, zoals het informeren van een burger dat over hem persoonsgegevens worden verwerkt.

De verantwoordelijke is degene die, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (art. 1, onder d, Wbp). Het gaat dus om degene die bepaalt welke persoonsgegevens op welke wijze en voor welk doel worden verwerkt.

Bij gebruik van drones kan de verantwoordelijke bijvoorbeeld een ondernemer, een journalist of een officier van justitie zijn. De verantwoordelijke hoeft niet de piloot van de drone te zijn. De piloot zal immers niet altijd het doel en de middelen van de verwerking bepalen. Hij kan ook optreden in opdracht van een klant of als werknemer van een bedrijf. Als de piloot overeenkomstig de instructies van de klant of de baas van het bedrijf en onder diens verantwoordelijkheid zijn werk doet, is de klant of de baas de verantwoordelijke voor de gegevensverwerking. De piloot is in dat geval de "bewerker" (art. 1, onder e, Wbp).

---

[34] Vgl. Finn, blz. 275.

In situaties waarin verschillende personen bij het gebruik van drones betrokken zijn, is het van belang goed van te voren te bepalen wie welke rol daarbij heeft en wie uiteindelijk als verantwoordelijke is aan te merken.[35]

In hoeverre dient het verwerken van persoonsgegevens met behulp van een drone een bepaald doel te hebben?

Persoonsgegevens mogen slechts worden verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (art. 7 Wbp). Dit betekent dat de verantwoordelijke, bijvoorbeeld het bedrijf dat voor beveiligingsdoeleinden drones inzet, van te voren moet vaststellen voor welk doel persoonsgegevens worden verwerkt. Dat doel mag niet zo vaag of ruim zijn dat het tijdens het verwerkingsproces geen kader kan bieden waaraan getoetst kan worden of de desbetreffende persoonsgegevens voor dat doel nodig zijn. Bovendien dient het doel gerechtvaardigd te zijn. Dit houdt in dat het belang van de verantwoordelijke redelijkerwijs aanleiding dient te geven om de desbetreffende persoonsgegevens voor dat doel te mogen verwerken. Ook mag de verwerking van de persoonsgegevens niet in strijd zijn met enige wet, de openbare orde of de goede zeden.[36] Daaruit vloeit voort dat het bespioneren van derden, illegale controles, schending van de intimiteit van anderen geen aanvaardbare doeleinden zijn. Dat de verwerking van persoonsgegevens niet in strijd mag zijn met enige wet, impliceert dat, voor zover het gebruik van drones in een specifiek geval in strijd is met de luchtvaartregelgeving, de verzameling van persoonsgegevens tijdens de desbetreffende vlucht als onrechtmatig valt aan te merken.[37]

Op welke grondslagen mogen persoonsgegevens met behulp van een drone worden verwerkt?

De verwerking van persoonsgegevens door middel van een drone mag alleen plaatsvinden, indien daarvoor een grondslag aanwezig is. Artikel 8 Wbp noemt zes algemene grondslagen.[38] Deze zijn, kort weergegeven:

a. ondubbelzinnige toestemming van de betrokkene;
b. uitvoering van een overeenkomst;
c. wettelijke verplichting;
d. vrijwaring van een vitaal belang van de betrokkene;
e. publiekrechtelijke taak;
f. gerechtvaardigd belang, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene prevaleert.[39]

De meest voor de hand liggende verwerkingsgrondslag voor het gebruik van drones door particulieren voor commercieel of beroepsmatig gebruik ligt in het "gerechtvaardigde belang" om persoonsgegevens te verwerken. Het is daarbij te allen tijde noodzakelijk om

---

[35] Finn, blz. 282; WP 29, blz. 8-9.
[36] Kamerstukken II 1997-1998, 25892, blz. 78-79.
[37] WP 29, blz. 13.
[38] Daarnaast bestaan ook specifieke wettelijke grondslagen voor het verwerken van persoonsgegevens. Te denken valt aan artikel 126gg van het Wetboek van Strafvordering, dat een grondslag geeft voor stelselmatige observatie door de politie.
[39] Zie nader voor de uitleg van deze grondslagen in relatie tot drones: WP29, blz. 12-13.

een belangenafweging te maken tussen enerzijds het gerechtvaardigde belang van de verantwoordelijke, en anderzijds het belang van de persoon ten aanzien van wie persoonsgegevens worden verwerkt. De aard en de zwaarte van de belangen zijn dan relevant in die afweging; bij een zwaarder belang kan de belangenafweging sneller in het voordeel van de verantwoordelijke uitvallen dan bij een licht belang, en vice versa. Ter beveiliging van een terrein of voor de inspectie van een gebouw is bijvoorbeeld sprake van een economisch belang, waarbij het onder omstandigheden onvermijdelijk kan zijn om persoonsgegevens in de vorm van opnames van personen te verwerken. Dit economische belang moet worden afgewogen tegenover het recht op privacy van de betrokkene.[40]

De vraag wat de verwerkingsgrondslag is, kan ook rijzen bij bijvoorbeeld concerten en festivals. Als daar met behulp van een drone wordt gefilmd, kunnen de organisatoren niet volstaan met de aanwezige mensen daarvan op de hoogte te stellen. Dan zal dat filmen ook moeten zijn opgenomen in de voorwaarden voor de aankoop van een toegangsbewijs voor het concert of festival.[41]

Onder welke voorwaarden mogen persoonsgegevens die met behulp van drones zijn verzameld, verder worden verwerkt?

Persoonsgegevens mogen alleen verder worden verwerkt op een wijze die niet onverenigbaar is met de doeleinden waarvoor ze zijn verkregen (art. 9, eerste lid, Wbp).

De vraag of er sprake is van verenigbaarheid wordt in ieder geval beoordeeld aan de hand van de volgende factoren:

a. de verwantschap tussen het doel van de beoogde verwerking en het doel waarvoor de gegevens zijn verkregen;
b. de aard van de desbetreffende gegevens;
c. de gevolgen van de beoogde verwerking voor de betrokkene;
d. de wijze waarop de gegevens zijn verkregen en
e. de mate waarin jegens de betrokkene wordt voorzien in passende waarborgen.

Als bijvoorbeeld gebruik wordt gemaakt van een drone bij een openluchtconcert om voor promotiedoeleinden te filmen, mogen deze beelden in beginsel niet worden gebruikt om later personen te identificeren. Dat laatste doel staat in een te ver verwijderd verband tot het eerste doel. De officier van justitie zal dergelijke beelden dan ook alleen in handen kunnen krijgen met toepassing van de bevoegdheid tot het vorderen van informatie die het Wetboek van Strafvordering hem geeft (artikel 126nd).

Een ander voorbeeld betreft de makelaar, die een drone gebruikt om opnames te maken van luxe huizen van zijn klanten. Hij mag deze opnames niet ter beschikking stellen van de gemeente om deze in staat te stellen een controle uit te oefenen op illegale bebouwing.

---

[40] Custers, blz. 126.
[41] Finn, blz. 284.

Hoe moet bij het gebruik van drones het noodzakelijkheidsvereiste met betrekking tot het verwerken van persoonsgegevens worden uitgelegd?

Op grond van artikel 11 Wbp moeten de verwerkte gegevens toereikend, ter zake dienend en niet bovenmatig zijn. Dit betekent dat de gegevens van die verwerking moeten worden beperkt tot het strikt noodzakelijke om het doel van de verwerking te verwezenlijken.

Op grond van dit principe mogen drones, uitgerust met verschillende technologieën voor gegevensverzameling (camera, GPS, hoogtemeter, bewegingssensoren) uitsluitend die informatie verzamelen die noodzakelijk is voor de verwezenlijking van het doel waarvoor dit gebeurt. Zo mag een camera op een drone die moet dienen om luchtfoto's van landschappen te maken, niet gebruikt worden voor het opnemen van gezichten of andere persoonlijke gegevens (zoals bijvoorbeeld de gevels van woningen of privétuinen).[42] Als in zo'n geval onbedoeld toch opnames van personen zijn gemaakt, kan het noodzakelijk zijn de gezichten van deze personen te "blurren".[43] Het argument dat een camera met blur-techniek duurder is dan een gewone camera, is dan niet relevant: de afwezigheid van deze techniek kan tot gevolg hebben dat de verwerking van persoonsgegevens niet voldoet aan het beginsel van proportionaliteit.[44]

In hoeverre mogen met behulp van een drone zogenoemde bijzondere persoonsgegevens worden verwerkt?

De Wbp noemt in artikel 16 persoonsgegevens die, gelet op hun gevoelige karakter, als bijzonder worden aangemerkt. Het betreft de persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven en lidmaatschap van een vakvereniging alsmede strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.

Als hoofdregel geldt dat de verwerking van deze bijzondere persoonsgegevens niet is toegestaan. De artikelen 17 tot en met 23 Wbp bevatten ontheffingen van dit algemene verwerkingsverbod. Eerst worden de bijzondere ontheffingen genoemd (artikel 17 tot en met 22 Wbp). Daarna volgt een bepaling met algemene ontheffingen (artikel 23 Wbp). Zo doorbreekt artikel 22, vierde lid, onder a, Wbp voor particuliere organisaties met een vergunning om beveiligingswerkzaamheden te verrichten het verbod om strafrechtelijke persoonsgegevens te verwerken. Als zo'n organisatie aan de overige bepalingen van de Wbp voldoet en de vereiste ontheffing op basis van de luchtvaartregelgeving heeft, zou zij bij bijvoorbeeld het bewaken van een industrieterrein een camera op een drone mogen gebruiken die beelden met daarop strafrechtelijke persoonsgegevens maakt.

Op camerabeelden die met drones zijn gemaakt, kunnen de fysieke kenmerken van personen zichtbaar zijn. Zo kan bijvoorbeeld zichtbaar zijn of iemand een bril draagt (wat

---

[42] http://www.privacycommission.be/nl/faq-page/7340#t7340n16585.
[43] Dit is een vorm van "privacy by design". Zie ook: Hoe kunnen bij het gebruik van drones "Privacy by Design" en "Privacy by Default" de risico's voor onze privacy verminderen?
[44] Finn, blz. 286.

iets zegt over zijn visuele gezondheid) of een hoofddoek (wat iets kan zeggen over iemands godsdienstige overtuiging). Tevens kan iemands ras van de camerabeelden worden afgeleid.[45] Dit zou in de praktijk betekenen dat camerabeelden van personen veelal bijzondere persoonsgegevens bevatten. Het lijkt evenwel reëel om camerabeelden niet als bijzondere persoonsgegevens aan te merken als:

- het doel van de verwerking niet gericht is op identificatie of het onderscheid maken op grond van een bijzonder persoonsgegeven, en
- het voor de verantwoordelijke redelijkerwijs niet voorzienbaar is dat de verwerking zal leiden tot het maken van onderscheid.[46]

Verder moet worden bedacht dat persoonsgegevens die voortkomen uit cameratoezicht met gebruik van drones ter beveiliging van personen of goederen, op basis van de bovenstaande criteria meestal wel moeten worden aangemerkt als strafrechtelijke gegevens in de zin van artikel 16 Wbp, aangezien het doel van de verwerking (mede) gericht zal zijn op het verwerken van strafrechtelijke gegevens. Het verbod om dergelijke gegevens te verwerken geldt dan (onder meer) niet, als de verantwoordelijke cameratoezicht toepast ter bescherming van zichzelf of een particuliere organisatie is die met een vergunning beveiligingswerkzaamheden verricht (art. 22, tweede lid, onder b, en vierde lid, onder a, Wbp).

In hoeverre moeten personen van wie met behulp van drones gegevens zijn verwerkt, daarover worden geïnformeerd?

De verantwoordelijke in de zin van de Wbp is verplicht betrokkenen zo goed mogelijk te informeren over de verwerking van persoonsgegevens (artt. 33 en 34 Wbp). Bij gebruik van drones zal dit veelal de onderneming of de overheidsinstelling zijn die van drones gebruik maakt of de opdrachtgever voor het gebruik van drones.

Deze informatieplicht geeft uitdrukking aan het transparantiebeginsel dat bij de verwerking van persoonsgegevens dient te worden gehanteerd. Bij het gebruik van drones kan aan dit transparantiebeginsel invulling worden gegeven door ervoor te zorgen dat de drones voldoende zichtbaar en identificeerbaar zijn tijdens hun gebruik. Dit kan bijvoorbeeld worden bereikt door de drone een bepaalde kleur te geven zodat hij van ver kan worden geïdentificeerd, of door ervoor te zorgen dat de camera's indien mogelijk zichtbaar zijn, of door vooraf het mogelijke gebruik van een drone aan te kondigen via de pers, het internet of een aankondiging op de plaats waarboven de drone gaat vliegen.

Daarnaast moeten de betrokken personen de identiteit van de verantwoordelijke voor de verwerking kunnen achterhalen. Dit kan via dezelfde weg als hierboven beschreven om de aanwezigheid van drones aan te kondigen. Dit kan, afhankelijk van het formaat van de drone en de vlieghoogte, ook via een zichtbare identificatie op de drone, of bepaalde

---

[45] Kamerstukken II 1997-1998, 25892, nr. 3, blz. 105.

[46] Deze criteria zijn afgeleid van criteria die het College bescherming persoonsgegevens hanteert bij de vaststelling of beeldmateriaal rasgegevens bevat. Zie College bescherming persoonsgegevens, Onderzoek naar de verwerking van persoonsgegevens van uitzendkrachten door Randstad Nederland B.V., z2013-00790, 2014.

kleuren die naar een onderneming verwijzen of een verantwoordelijke voor de verwerking die algemeen bekend is bij het grote publiek.[47]

De hier beschreven informatieplicht is niet absoluut. Uitgezonderd is de situatie dat de informatieverstrekking aan de betrokkenen onmogelijk blijkt of een onevenredige inspanning kost. In dat geval dient de verantwoordelijke in ieder geval de herkomst van de gegevens vast te leggen (art. 34, lid 4, Wbp). De vraag of er sprake is van een "onevenredige inspanning" is mede afhankelijk van bijvoorbeeld de mate waarin andere wegen openstaan om de betrokkenen op adequate wijze van informatie te voorzien en het medium waarvan mag worden verwacht dat het de betrokkenen voor een groot deel bereikt.[48]

Daarnaast kan voor het opschorten van de informatieplicht in sommige gevallen een beroep worden gedaan op artikel 43 Wbp. Opschorting is mogelijk voor zover dit noodzakelijk is in het belang van – onder meer – de voorkoming, opsporing en vervolging van strafbare feiten, gewichtige economische en financiële belangen van de staat en andere openbare lichamen, het toezicht op de naleving van wettelijke voorschriften die zijn gesteld ten behoeve van eerdergenoemde belangen, en de bescherming van de betrokkene of van de rechten of vrijheden van anderen. Dit artikel dient restrictief te worden geïnterpreteerd. Het geeft om die reden in beginsel alleen ruimte voor incidentele, niet voor structurele vormen van opschorting. Gedacht kan worden aan het tijdelijk toestaan van heimelijk cameratoezicht door drones.[49]

Hoe moeten persoonsgegevens die met behulp van drones zijn verzameld, worden beveiligd?

Opgeslagen persoonsgegevens moeten te allen tijde afdoende worden beveiligd met technische en organisatorische maatregelen (art. 13 Wbp). Met het oog daarop heeft het College bescherming persoonsgegevens (Cbp) richtsnoeren vastgesteld voor de beveiliging van persoonsgegevens.[50] Deze hebben uiteraard ook betekenis voor gegevensverwerking met behulp van drones.

Beveiligingsrisico's kunnen zowel intentioneel zijn – denk aan "hackers" – als non-intentioneel, bijvoorbeeld door middel van onbedoeld lekken. Persoonsgegevens kunnen daartegen worden beschermd door deze met behulp van bepaalde technieken onbruikbaar te maken voor onbevoegden. Daarbij kan worden gedacht aan cryptografische bewerkingen als encryptie (versleuteling) en "hashing" (het omzetten van gegevens in een unieke code). Het toepassen van dergelijke bewerkingen op identificerende gegevens leidt tot pseudonimisering (het identificerend gegeven wordt vervangen door een ander identificerend gegeven). Pseudonimisering is daarmee wat anders dan anonimisering, waarbij gegevens worden omgezet naar een vorm die identificatie niet langer mogelijk maakt.

---

[47] http://www.privacycommission.be/nl/faq-page/7340#t7340n16581.
[48] Kamerstukken II 1997-1998, 25892, blz. 155. Zie nader: Hoe kunnen bij het gebruik van drones "Privacy by Design" en "Privacy by Default" de risico's voor onze privacy verminderen?, onder "transparantie".
[49] Zie hierna: Mogen burgers of bedrijven drones voor cameratoezicht inzetten?
[50] https://cbpweb.nl/nl/richtsnoeren-beveiliging-van-persoonsgegevens-2013.

Naast zulke beveiligingsrisico's "naar buiten" op het terrein van hacken en lekken van signalen zijn er ook beveiligingsrisico's "naar binnen", dat wil zeggen naar ongeautoriseerde medewerkers. Het kan zijn dat medewerkers binnen een organisatie waar met behulp van drones informatie wordt verzameld, graag mee willen kijken naar gegevens van anderen waarin ze zijn geïnteresseerd, bijvoorbeeld van familieleden, buurtgenoten of bekende Nederlanders.[51] Maatregelen om dit tegen te gaan kunnen worden gevonden in een goed stelsel van autorisaties, toegangsbeveiliging en een systeem van "logging" en controle.[52]

Beveiligingsrisico's kunnen ook zijn gelegen in verstoring van de frequentie waarmee een drone of een payload wordt aangestuurd. Zo'n verstoring kan een bewuste actie zijn, bijvoorbeeld door "jamming". Een "jammer" verstoort de ontvangst van signalen van andere zenders door zelf stoorsignalen uit te zenden. Wanneer drones een doelwit zijn, kunnen "jammers" worden gebruikt om drones onbestuurbaar te maken of om de payloadfrequenties te verstoren. De payloadfrequenties betreffen bijvoorbeeld de signalen om camerabeelden, geluidsopnamen of andere sensorische informatie naar de grond te sturen. Wanneer een WiFi-hotspot of telecomapparatuur als "payload" aan een drone wordt gehangen, worden ook bepaalde frequenties gebruikt. Iemand die deze signalen wil verstoren kan daarvoor een "jammer" inzetten.[53] Het is uiteraard ook mogelijk dat een verstoring optreedt zonder menselijke tussenkomst. Tot slot is denkbaar dat een bestuurder met zijn signaal de besturing van de drone van een ander overneemt. Het overnemen van de besturing door zich voor te doen als iemand anders wordt aangeduid als "spoofing". Hiermee wordt het mogelijk een drone te kapen.[54] In al deze gevallen kan de informatie die met de drone is verzameld, in verkeerde handen vallen. Om dat tegen te gaan, is het niet alleen wenselijk maatregelen te nemen die voor beveiliging van de informatie zelf zorgen, maar kan ook worden gedacht aan een voorziening op de drone die ervoor zorgt dat de drone vanzelf terugkeert naar zijn startpunt als het wifi-signaal met de dronepiloot wordt onderbroken (zgn. "failsafe").

Met ingang van 1 januari 2016 zal de Wbp een zgn. meldplicht datalekken kennen, in geval van gebleken doorbrekingen van de getroffen maatregelen ter beveiliging van persoonsgegevens. De verantwoordelijke zal op grond van een nieuw artikel 34a Wbp bij een inbreuk waarvan redelijkerwijs kan worden aangenomen dat die ernstige nadelige gevolgen heeft voor de bescherming van de verwerkte persoonsgegevens, een melding doen bij het Cbp. Daarnaast dient in de meeste gevallen een melding aan de betrokkene te geschieden, indien de inbreuk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer. De meldplicht rust op alle verantwoordelijken voor de verwerking, zowel in de private als publieke sector. Het nalaten aan deze verplichtingen te voldoen kan worden gesanctioneerd met een bestuurlijke boete, op te leggen door het Cbp. Het doel van de meldplicht is het voorkomen van datalekken ten gevolge van doorbreking van beveiligingsmaatregelen en als deze zich toch voordoen, de gevolgen ervan voor de betrokkenen zoveel mogelijk te beperken.

---

[51] Custers, blz. 67.
[52] Zie ook: WP 29, blz. 17.
[53] Custers, blz. 68.
[54] Custers, blz. 67-68.

Hoe lang mogen persoonsgegevens die met behulp van drones zijn verzameld, worden bewaard?

In het algemeen geldt dat persoonsgegevens niet langer mogen worden bewaard dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor zij worden verwerkt (artikel 10, eerste lid, Wbp). Dit impliceert dat bijvoorbeeld beelden die met een drone zijn gemaakt met het oog op de veiligheid op een terrein waar een festival wordt gehouden, slechts bewaard mogen worden voor de duur die nodig is om eventuele klachten over de veiligheid tijdens het festival af te handelen. Waar mogelijk dient na afloop van de bewaartermijn voor automatische vernietiging of anonimisering van de gegevens te worden gezorgd.[55]

De Wbp noemt geen specifieke bewaartermijnen. Het Vrijstellingsbesluit Wbp geeft wel een indicatie van een bewaartermijn voor specifieke gegevens. Ten aanzien van duidelijk zichtbaar cameratoezicht ter beveiliging van personen of goederen die zijn toevertrouwd aan de zorg van de verantwoordelijke, noemt het Vrijstellingsbesluit Wbp een bewaartermijn van maximaal vier weken dan wel tot een geconstateerd incident is afgehandeld (artikel 38, lid 6, Vrijstellingsbesluit Wbp). Hoewel deze bewaartermijn niet dwingend is, geeft zij wel een duidelijke indicatie van de termijn waarbinnen het bewaren van de desbetreffende persoonsgegevens nog noodzakelijk kan worden geacht. Deze indicatie geldt ook voor duidelijk kenbaar gemaakt cameratoezicht met behulp van drones.

Voor persoonsgegevens die onder specifieke regimes vallen, kunnen wel bewaartermijnen zijn voorgeschreven. Zo vallen persoonsgegevens die de politie met behulp van drones heeft verzameld, onder de regeling van bewaartermijnen in de in artikel 14 van de Wet politiegegevens genoemde artikelen.

In welke gevallen moet het verwerken van persoonsgegevens met behulp van drones worden gemeld aan het College bescherming persoonsgegevens?

De Wbp bepaalt in het algemeen dat een voorgenomen verwerking van persoonsgegevens dient te worden gemeld bij het College bescherming persoonsgegevens (Cbp) of een functionaris voor de gegevensbescherming[56] (artikel 27 Wbp). De melding dient te geschieden alvorens met de verwerking wordt aangevangen. Dit geldt ook voor verwerking van persoonsgegevens met behulp van drones.

In een aantal gevallen kan een melding achterwege blijven. Dit geldt onder meer voor verwerking van persoonsgegevens door middel van cameratoezicht, indien is voldaan aan de vereisten van artikel 38 Vrijstellingsbesluit Wbp. De belangrijkste vereisten die dit artikel noemt zijn: het cameratoezicht is ingesteld ter beveiliging van personen en goederen die zijn toevertrouwd aan de zorg van de verantwoordelijke, het cameratoezicht is duidelijk zichtbaar en de persoonsgegevens worden verwijderd uiterlijk

---

[55] WP 29, blz. 17.

[56] Een functionaris voor de gegevensbescherming ziet toe op de rechtmatigheid van de verwerking van persoonsgegevens door een bepaalde verantwoordelijke, die hem daartoe heeft benoemd (artt. 62-64 Wbp).

vier weken nadat de video-opnames zijn gemaakt, dan wel na afhandeling van geconstateerde incidenten.

Een voorgenomen verwerking van persoonsgegevens door middel van heimelijk cameratoezicht dient altijd te worden gemeld bij het Cbp. Daarbij dient bovendien een voorafgaand onderzoek te worden aangevraagd. Het voorafgaand onderzoek houdt in dat het Cbp de rechtmatigheid van de voorgenomen verwerking zal onderzoeken. Met de verwerking mag niet worden begonnen totdat het Cbp dit onderzoek heeft afgerond dan wel heeft besloten om geen onderzoek in te stellen.

Is de Wbp van toepassing wanneer een drone uitsluitend voor een persoonlijk of huishoudelijk doel wordt gebruikt?

De Wbp is niet van toepassing op de verwerking van persoonsgegevens met gebruik van een drone ten behoeve van activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden (art. 2, tweede lid, onder a, Wbp). Aangenomen mag worden dat tot dergelijke activiteiten ook gerekend mag worden het maken van beelden met een camera op een drone, als deze beelden louter voor privégebruik zijn. Te denken valt aan het vliegen met een drone voor recreatieve doeleinden, waarbij persoonsgegevens worden verwerkt door gebruik van foto- of videoapparatuur.[57]

De hier bedoelde uitzondering geldt niet in het geval dat men de beelden die men met een drone aanvankelijk voor persoonlijke of huishoudelijke doeleinden heeft gefilmd, vervolgens aan een onbepaald aantal personen verstrekt. Hiervan is bijvoorbeeld sprake, indien de beelden op internet worden geplaatst en voor iedereen toegankelijk zijn.[58] In dat geval dienen de bepalingen van de Wbp volledig te worden nageleefd. Als een website of een profiel op een sociale netwerksite echter alleen toegankelijk is voor een beperkte kring mensen, mag iemand daarop een met een drone gemaakte foto of film plaatsen zonder toestemming van de personen die op die foto of film staan.

Het doel waarvoor men met een camera op een drone beelden maakt, is ook van belang voor het bepalen van de locatie waar men mag filmen. Als iemand die beelden maakt met het oog op de beveiliging van zijn gezin of eigendommen en daartoe uitsluitend de eigen woning en tuin filmt, valt dat te rangschikken onder activiteiten met uitsluitend persoonlijke doeleinden. Zodra de camera echter ook een deel van de openbare weg filmt, moet de bestuurder van de drone voldoen aan de bepalingen van de Wbp.[59]

Is de Wbp volledig van toepassing als een drone wordt gebruikt voor journalistieke doeleinden of voor audiovisuele producties?

In de journalistiek kan gebruik gemaakt worden van een drone. Hetzelfde geldt voor audiovisuele producties voor artistieke doeleinden. Met een drone is het immers

---

[57] Zie ook Antwoorden op Kamervragen van het lid Oosenbrug over de regelgeving met betrekking tot drones van staatssecretaris Teeven op 26 juni 2013, *Kamerstukken II* 2012/13, nr. 2691.
[58] Hof van Justitie 6 november 2003, C-101/01, overweging 47 (Arrest Lindqvist).
[59] Hof van Justitie 11 december 2014, C-212/13, overwegingen 33 en 35.

gemakkelijk om op moeilijk toegankelijke plaatsen beelden op te nemen of locaties te zoeken voor filmopnames.

Indien sprake is van de verwerking van persoonsgegevens voor dergelijke doeleinden zijn bepaalde bepalingen uit de Wbp niet van toepassing (art. 3, eerste lid, Wbp). Het gaat daarbij in het bijzonder om de informatieplicht aan betrokkenen, de meldingsplicht voor de verwerking van persoonsgegevens aan het Cbp en de rechten van betrokkenen, zoals het inzage- en correctierecht. Deze exceptie rechtvaardigt dus geen ongelimiteerde verwerking van persoonsgegevens.[60]

Het Cbp heeft de journalistieke exceptie afgebakend in een richtlijn door onder andere te vereisen dat het om een (objectieve) informatieverzameling en een regelmatige bezigheid moet gaan.[61] Deze vereisten staan er niet aan in de weg dat de vraag wie zich journalist mag noemen, ruim mag worden uitgelegd. Daartoe kunnen ook relatief nieuwe typen journalisten worden gerekend, zoals bloggers, paparazzi, Youtubers, "burger-journalisten", zolang als het doel van de gegevensverwerking maar gericht is op openbaarmaking van informatie, opinies of ideeën aan het publiek.[62]

Welke rechten hebben burgers met betrekking tot de verwerking van hun persoonsgegevens met behulp van drones?

Burgers van wie met behulp van een drone persoonsgegevens zijn verwerkt, hebben, de hiervóór genoemde uitzonderingssituaties daargelaten, verschillende rechten.

Een burger kan in de eerste plaats zich tot de verantwoordelijke wenden met het verzoek hem mee te delen welke persoonsgegevens over hem worden verwerkt, voor welke doeleinden en aan welke derden deze gegevens zijn verstrekt (inzagerecht). De verantwoordelijke moet betrokkene daarop binnen vier weken antwoord geven (art. 35 Wbp). In het geval dat met de drone videobeelden zijn gemaakt en deze beelden zonder vermelding van identificerende gegevens in een digitaal archief zijn opgeslagen, lijkt het redelijk betrokkene om informatie te vragen die kan helpen bij de uitvoering van het inzageverzoek.

Een burger over wie persoonsgegevens worden verwerkt, heeft daarnaast het recht de verantwoordelijke te verzoeken persoonsgegevens over hem te verbeteren, aan te vullen, af te schermen of te verwijderen bij feitelijke onjuistheden, bij verwerkingen ten behoeve van onvolledige of niet ter zake doende doelen of bij verwerkingen die in strijd zijn met een wettelijk voorschrift (artt. 36 tot en met 38 Wbp). Indien gegevens het voorwerp zijn van verwerking op grond van artikel 8, onder e en f, Wbp[63], kan de betrokkene daartegen bij de verantwoordelijke te allen tijde verzet aantekenen in verband met zijn bijzondere persoonlijke omstandigheden (art. 40 Wbp).

---

[60] Custers, blz. 127.
[61] Zie de CBP Richtsnoeren voor publicatie van persoonsgegevens op internet, blz. 42-47.
[62] Finn, blz. 264-268.
[63] Zie: Op welke grondslagen mogen persoonsgegevens met behulp van een drone worden verwerkt?

Als het om persoonsgegevens gaat die de politie met behulp van drones heeft verzameld, gelden met betrekking tot het inzage- en correctierecht bijzondere regelingen die in de artikelen 25 tot en met 31 van de Wet politiegegevens zijn vastgelegd.

Aan welke voorwaarden moet worden voldaan om persoonsgegevens te verstrekken aan landen buiten de EU?

Met behulp van drones kunnen persoonsgegevens zijn verzameld die de verantwoordelijke wil doorgeven aan personen of organisaties in landen buiten de Europese Unie. Voor zo'n situatie bevat de Wbp bijzondere bepalingen.

Persoonsgegevens mogen slechts naar dergelijke landen worden doorgegeven, indien die landen een passend beschermingsniveau waarborgen (art. 76 Wbp). Onder bepaalde voorwaarden kunnen gegevens ook worden doorgegeven aan landen die dergelijke waarborgen niet bieden. En als zelfs niet aan die voorwaarden wordt voldaan, kan de Minister van Veiligheid en Justitie, gehoord het Cbp, een vergunning afgeven voor doorgifte van persoonsgegevens naar een derde land dat geen waarborgen voor een passend beschermingsniveau biedt (art. 77 Wbp).

Gebruik door politie voor uitvoering van de politietaak

Op welke wettelijke gronden mag de politie drones met camera's inzetten?

Voor de inzet van drones met camera's voor opsporing van strafbare feiten bestaat geen specifieke wettelijke basis. Op grond van jurisprudentie van de Hoge Raad mag evenwel worden aangenomen dat de inzet daarvan kan worden gebaseerd op artikel 3 van de Politiewet 2012 als algemeen taakstellend artikel voor de politie en op artikel 141 van het Wetboek van Strafvordering, waarin de opsporingsbevoegdheid voor de politie is vastgelegd. Daarbij geldt dan wel als voorwaarde dat de inzet van drones met camera's in het desbetreffende geval slechts "een beperkte inbreuk op grondrechten van burgers" maakt en "niet zeer risicovol is voor de integriteit en beheersbaarheid van de opsporing"[64].

Als het cameragebruik verder reikt en het karakter van stelselmatige observatie krijgt, moet aan de daarvoor geldende voorwaarden van artikel 126g, 126o c.q. 126zd van het Wetboek van Strafvordering worden voldaan. Van stelselmatige observatie is sprake, als de inzet van drones met camera's voor de opsporing "in verband met de duur, intensiteit en frequentie ervan geschikt is om een min of meer compleet beeld te verkrijgen van bepaalde aspecten van het persoonlijk leven van de betrokkene"[65]. Verder zou men kunnen denken aan de inzet van een drone voor het opnemen van vertrouwelijke communicatie met een technisch hulpmiddel (art. 126l Sv) en het uitvoeren van een inkijkoperatie in een besloten plaats (art. 126k Sv).

Overigens kunnen de camera's op drones die thans voor de opsporing worden gebruikt, wel beelden produceren waarop personen zijn te zien, doch geen beelden waarop de

---

[64] Vgl. HR 1 juli 2014, ECLI:NL:HR:2014:1569.
[65] Kamerstukken II, 1996-1997, 25 403, nr. 3, blz. 26 en 27.

gezichten van deze personen herkenbaar zijn. De ontwikkelingen op dit punt staan echter niet stil: het is zeer wel denkbaar dat een nieuwe generatie camera's op drones in de toekomst personen bij de opsporing van strafbare feiten wel herkenbaar in beeld kunnen brengen.[66]

Behalve voor opsporingsdoeleinden kan de politie drones met camera's ook inzetten voor de handhaving van de openbare orde in gevallen waarin sprake is van een "concrete verstoring van de openbare orde dan wel een concrete dreiging daarvan". De inzet daarvan kan dan eveneens worden gebaseerd op artikel 3 van de Politiewet 2012.[67]

Verder is denkbaar dat de politie drones inzet ter uitvoering van haar hulpverlenende taak, bijvoorbeeld in het geval van calamiteiten. Ook dan kan artikel 3 van de Politiewet 2012 als basis voor de inzet daarvan dienen. De eventuele privacyinbreuk die in het kader van de hulpverlening plaatsvindt, zal dan al snel proportioneel kunnen worden geacht door het belang van de slachtoffers dat daar tegenover staat.

Tot slot valt erop te wijzen dat het gebruik van drones door de politie moet passen binnen de kaders van de luchtvaart- en privacyregelgeving. In dat verband zijn ook antwoorden op andere vragen in deze handleiding relevant.[68] Meer in het bijzonder geldt dat drones, gelet op hun intrusieve karakter, niet mogen worden ingezet voor willekeurige surveillance, verwerking van bulk data, koppeling van data en "profiling"[69]. Surveillance met behulp van drones mag ook niet worden gebruikt voor het signaleren van subjecten op basis van louter data-analyses.[70] Het gebruik van drones door de politie zal in ieder geval moeten worden beperkt naar plaats en in tijd. Met het oog op het "chilling effect" van het gebruik van drones op de vrijheid van meningsuiting en het recht van vereniging en vergadering, verdient het bijzondere aandacht dat, voor zover mogelijk, bij demonstraties geen surveillance met behulp van drones plaatsvindt.[71]

Gebruik door gemeenten, burgers of bedrijven voor cameratoezicht

Mogen gemeenten drones voor cameratoezicht inzetten?

Gemeenten mogen op grond van artikel 151c van de Gemeentewet in het belang van de handhaving van de openbare orde gebruik maken van cameratoezicht op openbare plaatsen, zoals uitgaanscentra. De gemeente mag dit alleen doen als andere maatregelen niet voldoende zijn gebleken.

---

[66] Kamerstukken II 2013–2014, 26 643, nr. 298, blz. 14.
[67] Kamerstukken I 2014–2015, 33 582, F, blz. 6.
[68] Voor zover in die antwoorden wordt gerefereerd aan de Wet bescherming persoonsgegevens, moet worden bedacht dat deze wet niet van toepassing is op persoonsgegevens die worden verwerkt in het kader van de uitvoering van de politietaak. Daarvoor geldt de Wet politiegegevens. In deze handleiding wordt die specifieke wet evenwel buiten beschouwing gelaten.
[69] Het gaat er dus om dat genoemde activiteiten vooraf zijn getoetst aan het noodzakelijkheidsvereiste en de eisen van proportionaliteit en subsidiariteit.
[70] Er zal, anders gezegd, altijd een vorm van menselijke tussenkomst dienen te zijn, voordat data-analyses tot een bepaald gevolg met enige impact voor betrokken burgers leiden.
[71] WP 29, blz. 10-11.

Op dit moment is cameratoezicht op grond van artikel 151c alleen mogelijk voor zover daarvoor vaste camera's worden gebruikt. Bij het parlement is een wetsvoorstel flexibel cameratoezicht in behandeling dat het mogelijk moet maken voor cameratoezicht binnen gemeenten ook "losse" camera's in te zetten.[72] Dit kan de vraag oproepen of het dan ook wordt toegestaan om op basis van artikel 151c Gemeentewet camera's op drones in te zetten.

Vanwege de ruimere mogelijkheden en de inherente privacygevaren kan de inzet van vliegende camera's als een zwaarder middel worden aangemerkt dan de inzet van vaste camera's. Het ligt om die reden voor de hand dat de inzet van vliegende camera's minder snel toelaatbaar is dan de inzet van statisch opgestelde camera's.[73] Inzet van camera's op drones op grond van het voorgestelde artikel 151c Gemeentewet is dan ook hoogstens denkbaar in situaties waarbij rond evenementen met een verhoogd risico op ordeverstoringen grote mensenmassa's bijeen zijn in de publieke ruimte en waar het uit het oogpunt van het toezicht op de handhaving van de openbare orde noodzakelijk zou kunnen worden geacht om vanuit de lucht te monitoren hoe groepen mensen zich binnen dat gebied verplaatsen. In die gevallen kan uit proportionaliteitsoverwegingen worden volstaan met een camera waarop geen gezichten kunnen worden herkend, zoals warmtebeeldcamera's.[74]

Het wetsvoorstel schrijft voor dat het cameratoezicht voor burgers kenbaar is. Voor vliegend cameratoezicht betekent dit dat in ieder geval aan de randen van het cameragebied de inzet van drones kenbaar wordt gemaakt.[75]

Tot slot valt erop te wijzen dat het gebruik van drones door gemeenten voor cameratoezicht moet passen binnen de kaders van de luchtvaart- en privacyregelgeving.

Geconcludeerd kan worden dat de ruimte voor inzet van camera's op drones op basis van artikel 151c Gemeentewet zeer beperkt zal zijn. Daarbij moet ook worden aangetekend dat het wetsvoorstel flexibel cameratoezicht niet zozeer beoogt om camera's op drones in te zetten, maar veeleer om het rigide regime van "vast" cameratoezicht "aan de grond" te flexibiliseren, zodat beter kan worden ingespeeld op zich snel verplaatsende overlast, veroorzaakt door bijvoorbeeld hangjongeren, drugsgebruikers, drugsdealers, straatrovers, zakkenrollers en vandalen.

Mogen burgers of bedrijven drones voor cameratoezicht inzetten?

Burgers of bedrijven mogen alleen dan drones voor cameratoezicht inzetten, als dat echt nodig is. Dat kan het geval zijn, als op een bepaald terrein dat eigendom van die burger of dat bedrijf is, regelmatig diefstal plaatsvindt of zaken worden vernield. Dan moet ook duidelijk zijn dat andere, minder ingrijpende maatregelen, zoals het aanbrengen van een hek of verlichting, het uitvoeren van extra surveillances door bewakingspersoneel of het

---

[72] Wetsvoorstel tot wijziging van de Gemeentewet in verband met de verruiming van de bevoegdheid van de burgemeester tot de inzet van cameratoezicht (Kamerstukken II 2012-2013, 33582, nrs. 1-3).
[73] Kamerstukken II 2012-2013, 33582, nr. 3, blz. 12, en nr. 6, blz. 9.
[74] Kamerstukken I 2014–2015, 33582, B, blz. 4.
[75] Kamerstukken II 2012-2013, 33582, nr. 3, blz. 5.

gebruik van bewakingscamera's op de grond, onvoldoende hebben geholpen. Verder zal de verantwoordelijke duidelijk moeten aangeven dat hij met behulp van drones cameratoezicht uitvoert. Is dat niet kenbaar gemaakt, dan is hij strafbaar.

Methoden om de privacy te beschermen

Hoe kan bij het gebruik van drones een Privacy Impact Assessment de risico's voor onze privacy verminderen?

Een Privacy Impact Assessment (PIA) is een methode waarmee op een gestructureerde en transparante wijze zichtbaar kan worden gemaakt wat de eventuele effecten van het gebruik van drones voor de bescherming van persoonsgegevens zijn, en welke maatregelen kunnen worden genomen om die effecten te verminderen.

Op grond van de komende Algemene verordening gegevensbescherming (AVG) van de Europese Unie is uitvoering van een PIA verplicht, wanneer verwerking van persoonsgegevens met behulp van drones waarschijnlijk een hoog risico oplevert voor de rechten en vrijheden van personen. De AVG noemt als voorbeelden van dergelijke risico's: discriminatie, identiteitsdiefstal of -fraude, financiële verliezen, reputatieschade, ongeoorloofde ongedaanmaking van pseudonimisering, verlies van vertrouwelijkheid van door een beroepsgeheim beschermde gegevens, of elke andere aanzienlijke economische of maatschappelijke schade (art. 33, eerste lid).

In aanvulling op deze algemene gevallen kan een PIA in het specifieke geval van het gebruik van drones ook wenselijk zijn, indien:

- de verantwoordelijke onbedoeld het risico loopt persoonsgegevens te verwerken,
- de drone wordt gebruikt voor het maken van beelden op openbare plaatsen,
- de drone wordt gebruikt voor heimelijke surveillance,
- de verzamelde gegevens worden gebruikt om profielen op te stellen of om direct marketing uit te voeren.[76]

Met betrekking tot de eerste twee gevallen geldt nog dat een PIA alleen dan wenselijk kan zijn, indien het om beroepsmatig gebruik van drones gaat. Het maken van beelden van personen voor louter persoonlijke of huishoudelijke doeleinden, valt immers buiten de werking van de Wbp (zie art. 2, onder a).

Het uitvoeren en publiceren van een PIA bij gegevensverwerking door drones kan bijdragen aan de transparantie van deze verwerking en daarmee aan het begrip bij het publiek van de wijze waarop en de reden waarvoor deze gegevens worden verwerkt. Aldus kan een PIA ook bijdragen aan het vertrouwen van het publiek in het gebruik van drones. Verder kan een PIA helpen voorkomen dat op een drone een payload wordt gebruikt die in onvoldoende mate aan de wettelijke voorschriften ter bescherming van persoonsgegevens voldoet. Dat vermindert het risico dat de payload later tegen hoge kosten moet worden aangepast of door een andere moet worden vervangen.

Voor de uitvoering van een PIA binnen de rijksdienst is een toetsmodel ontwikkeld, dat in het zgn. Integraal Afwegingskader (IAK) is opgenomen.[77]

---

[76] Finn, blz. 337-338.

Hoe kunnen bij het gebruik van drones "Privacy by Design" en "Privacy by Default" de risico's voor onze privacy verminderen?

Toepassing van het principe van *"privacy by design"* houdt in dat een verantwoordelijke passende technische en organisatorische maatregelen, zoals minimalisering en pseudonimisering van gegevens, neemt om aan de voorschriften met betrekking tot de bescherming van persoonsgegevens te voldoen. Met inachtneming van de beschikbare technologie en de uitvoeringskosten dient de verantwoordelijke daarbij rekening te houden met de aard, de context, de omvang en de doelen van de gegevensverwerking evenals de waarschijnlijkheid en de ernst van het risico voor de rechten en vrijheden van personen die voortvloeien uit de verwerking.[78]

"Privacy by default" houdt in dat de verantwoordelijke passende maatregelen treft om ervoor te zorgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking. Dit geldt voor de hoeveelheid verzamelde gegevens, de mate waarin zij worden verwerkt, de periode waarin zij worden opgeslagen en de toegankelijkheid ervan.[79]

In het geval van drones impliceren beide principes dat al bij het ontwerpen van de drone en van de payload waarmee persoonsgegevens worden verwerkt, rekening wordt gehouden met privacyrisico's en dientengevolge met de noodzaak van het treffen van technische en organisatorische maatregelen om deze risico's zoveel mogelijk te mitigeren. Daarvoor is nodig dat al vanaf de beginfase van het ontwerp sprake is van multidisciplinaire samenwerking tussen ICT-ers en privacy-juristen. De ICT-ers kunnen daarbij privacy beschermende technologieën inbrengen. Met "privacy by design" kan worden voorkomen dat later hoge kosten moeten worden gemaakt om systemen zo aan te passen dat zij alsnog in voldoende mate aan de vereisten met betrekking tot bescherming van persoonsgegevens beantwoorden.

"Privacy by Design" gaat uit van zeven principes die zich als volgt naar het ontwerpen en gebruiken van drones en hun payloads laten vertalen[80]:

- *De maatregelen moeten pro-actief zijn*, d.w.z. helpen voorkomen dat zich een onnodige inbreuk op de privacy voordoet. Bij het gebruik van drones impliceert dit dat het gebruik, al naar gelang het doel daarvan, moet worden beperkt naar plaats en tijd. Daarvoor dienen dat doel, de locatie van het gebruik en degenen die geautoriseerd zijn de drone te besturen en toegang tot de payload te hebben, vooraf worden gespecificeerd. Het verzamelen, gebruik, openbaren en bewaren van gegevens dient te worden beperkt tot het minimum.

---

[77] Kamerstukken II 2012-2013, 26643, nr. 282 herdruk; Integraal Afwegingskader, onderdeel "verplichte kwaliteitseisen".
[78] In de komende Algemene verordening gegevensbescherming van de Europese Unie wordt dit principe expliciet vastgelegd. Zie daartoe artikel 23, eerste lid, van de concept-verordening, versie 11 juni 2015 (2012/0011 (COD), 9565/15).
[79] Zie het tweede lid van artikel 23 van het voorstel voor de komende Algemene verordening gegevensbescherming van de Europese Unie, versie 11 juni 2015 (2012/0011 (COD), 9565/15).
[80] Zie ook: Cavoukian, blz. 17-21; WP 29, blz. 13-15.

- *Drone en payload moeten standaard zijn ingesteld op bescherming van de privacy ("Privacy by Default").* Dit impliceert dat een camera op een drone die wordt gebruikt voor cameratoezicht, zoveel mogelijk zo moet zijn ingesteld dat alleen beelden worden gemaakt van die plaatsen waarop dat toezicht nodig is. Mogelijkheden om de camera bijvoorbeeld te laten inzoomen op plaatsen die buiten het toezicht vallen, dienen zoveel mogelijk te worden beperkt. Camera's en andere sensoren dienen niet automatisch gegevens te gaan verwerken en alleen te worden aangezet, als dat noodzakelijk is.
- *Privacy moet ingebed zijn in het ontwerp.* Dit impliceert dat privacybescherming geïntegreerd is in het systeem, zonder dat de functionaliteit daarvan vermindert. Als een drone wordt gebruikt voor bijvoorbeeld inspectie van infrastructuur, kan de payload worden uitgerust met technologie om beelden van gezichten te verwijderen of te "blurren". Afhankelijk van het doel van het gebruik van de drone kan er ook voor worden gekozen beelden onmiddellijk te encrypteren (versleutelen) nadat zij zijn verzameld, en alleen te decrypteren (ontsleutelen) in het geval dat dit noodzakelijk is en dan alleen door daartoe geautoriseerde personen.[81] Als een camera op een drone alleen maar bedoeld moet zijn voor de bediening van het toestel, behoort men de drone niet uit te rusten met een camera waarmee kan worden ingezoomd en dienen de beelden niet te worden opgeslagen.
- *Privacy en bedrijfsbelang als positieve optelsom.* Privacy en bedrijfsbelangen behoeven geen tegenstelling te zijn. De legitieme belangen van zowel de organisatie die een drone gebruikt, als het publiek kunnen worden gewaarborgd als ervoor wordt gezorgd dat persoonsgegevens veilig worden opgeslagen en niet langer bewaard dan noodzakelijk is. De toegang tot de opgeslagen gegevens moet technisch zijn beveiligd, bijvoorbeeld door een code of een biometrisch kenmerk, en alleen zijn toegestaan aan daartoe geautoriseerde personen. Alle gevallen waarin personen toegang tot de opgeslagen gegevens hebben verkregen en deze hebben verwerkt, dienen gelogd te zijn, zodat de toegang en verwerking naderhand bij een audit kunnen worden gecontroleerd.
- *Bescherming van start tot finish.* Persoonsgegevens dienen tijdens de gehele verwerkingscyclus te worden beschermd. Dit vergt aandacht vanaf het moment dat gegevens met behulp van drones worden verzameld, tot aan het moment dat zij worden vernietigd. Om te verzekeren dat persoonsgegevens tijdens de gehele verwerkingscyclus in voldoende mate worden beschermd, is nodig dat vooraf een Privacy Impact Assessment wordt uitgevoerd.[82]
- *Transparantie.* Alle belanghebbenden bij het verwerken van persoonsgegevens met behulp van een drone moeten erop kunnen vertrouwen dat de verwerking plaatsvindt overeenkomstig het doel daarvan en dit, zo nodig, kunnen verifiëren. Dit vergt dat het verwerkingsproces voldoende transparant is. Organisaties die drones gebruiken, dienen burgers heldere informatie te verschaffen over vluchten in hun gebied, de doelen waarvoor deze plaatsvinden, de eventuele verwerking van persoonsgegevens tijdens en na deze vlucht en de identiteit en

[81] Article 29 Data Protection Working Party, Remotely Piloted Aircraft Systems (RPAS) – Response to the Questionnaire, European Commission, Brussels, 2013, blz. 3.

[82] Zie: Hoe kan bij het gebruik van drones een Privacy Impact Assessment de risico's voor onze privacy verminderen?

contactgegevens van de piloot en de organisatie. Zij kunnen dit doen via "klassieke" media als de krant, een brochure of posters, maar ook via meer eigentijdse media als websites, push-berichten naar personen die daarvoor hebben ingetekend, "social media" of mobiele applicaties.[83] Aldus kunnen deze organisaties aan vele risico's met betrekking tot de privacy van burgers bij het gebruik van drones tegemoet komen ("chilling effect", "function creep", uitoefening inzagerecht door betrokken burger etc.). Organisaties die drones gebruiken, doen er ook goed aan discussies met belanghebbenden aan te gaan over wat aanvaardbare en minder aanvaardbare vormen van gebruik zijn. Daarmee kunnen zij het risico verminderen dat er onvrede over het gebruik van drones ontstaat.[84]

- *Plaats het data-subject centraal.* Ontwerpers en gebruikers van drones en payloads dienen de belangen van personen over wie gegevens worden verwerkt, centraal te stellen. Dit dient door te klinken in de mate van transparantie die zij betrachten, de gedragscodes die zij hanteren, de keuzemenu's in het gebruikte verwerkingssysteem en de verdere inrichting van het verwerkingsproces.

Hoe kunnen gedragscodes bij het gebruik van drones de risico's voor onze privacy verminderen?

Organisaties die met drones vliegen, kunnen gedragscodes vaststellen waarin zij de wettelijke voorschriften met betrekking tot de bescherming van persoonsgegevens uitwerken met betrekking tot de specifieke verwerking van dergelijke gegevens door hun organisaties. Deze organisaties kunnen aan het Cbp verzoeken te verklaren dat hun gedragscode een juiste uitwerking vormt (art. 25 Wbp).[85]

Als het gaat om de productie en het gebruik van drones en payloads, is denkbaar dat een gedragscode wordt opgesteld door een brancheverenigingvoor professionele productie en gebruik van onbemande luchtvaartuigsystemen. Verder is denkbaar dat gedragscodes worden opgesteld door bijvoorbeeld een belangenbehartigende organisatie als de Nederlandse Vereniging van Journalisten (NVJ).[86] Ook kan worden gedacht aan een inzetinstructie bij bijvoorbeeld de politie.

Gedragscodes voor de productie en het gebruik van drones en payloads kunnen wettelijke voorschriften met betrekking tot de bescherming van persoonsgegevens vertalen naar maatwerk voor de gebruikte technologie en voorzien van praktische voorbeelden. Aldus kan een meer praktisch en levend instrument voor de desbetreffende organisatie(s) ontstaan. Zo'n gedragscode voor de producenten zou bijvoorbeeld kunnen voorschrijven dat zij privacy-instructies in de verpakking van de drone bijsluiten en op hun website plaatsen. Vaststelling van een gedragscode door bedrijven die drones

---

[83] De "Article 29 Data Protection Working Party" (WP 29) spreekt in dit verband van de noodzaak van een "multi-channel approach". Zie nader WP 29, blz. 15-16.
[84] Finn, blz. 256.
[85] Ingevolge artikel 38 van de komende Algemene verordening gegevensbescherming kunnen verenigingen en andere organen die categorieën verantwoordelijken of verwerkers vertegenwoordigen, gedragscodes opstellen, teneinde de toepassing van bepalingen van de verordening nader toe te lichten, met betrekking tot in dat artikel genoemde onderwerpen.
[86] Zie voor buitenlandse voorbeelden van gedragscodes: Finn, blz. 135-137.

produceren of exploiteren, kan bijdragen aan het vertrouwen dat het publiek in de aangesloten bedrijven heeft, en daarmee ook een commercieel belang vertegenwoordigen.[87]

Hoe kan certificering bij het gebruik van drones de risico's voor onze privacy verminderen?

Certificering en het gebruik van keurmerken kunnen laten zien dat bedrijven die drones laten vliegen, aan de wettelijke voorschriften over de bescherming van persoonsgegevens voldoen. Daartoe gespecialiseerde accreditatie-organisaties kunnen aan dergelijke bedrijven certificaten en keurmerken uitreiken. Uitreiking kan afhankelijk worden gesteld van de uitvoering van een Privacy Impact Assessment.[88] Voor bedrijven die een certificaat of keurmerk hebben, kan een bijkomend voordeel zijn dat zij een concurrentievoordeel hebben ten opzichte van bedrijven die een dergelijk certificaat of keurmerk niet hebben.

Hoe kunnen privacy audits bij het gebruik van drones de risico's voor onze privacy verminderen?

Privacy audits zijn instrumenten om op een systematische en onafhankelijke wijze na te gaan of de verwerking van persoonsgegevens plaatsvindt overeenkomstig de wet en het privacybeleid van de betrokken organisatie. Zo'n audit onderscheidt zich van een Privacy Impact Assessment door uit te gaan van bestaande standaarden waaraan de verwerking moet worden getoetst. Privacy audits bij organisaties die drones laten vliegen, kunnen bijdragen aan de transparantie van het gebruik van de drones en daarmee aan de geloofwaardigheid van de desbetreffende organisatie. De mogelijkheid van een privacy audit kan ook stimuleren dat een organisatie handelt in overeenstemming met de wettelijke voorschriften met betrekking tot de bescherming van persoonsgegevens.[89]

---

[87] Finn, blz. 344-345.
[88] Finn, blz. 349; WP 29, blz. 18. Ingevolge artikel 39 van de komende Algemene verordening gegevensbescherming zullen lidstaten de vaststelling van certificeringsmechanismes dienen te bevorderen.
[89] Finn, blz. 339-342.

Gebruikte afkortingen:

AGV: Algemene verordening gegevensbescherming;
Cbp: College bescherming persoonsgegevens;
EVRM: Europees Verdrag voor de Rechten van de Mens;
GPS: Global Positions System;
PIA: Privacy Impact Assessment;
Sr: Wetboek van Strafrecht;
Sv: Wetboek van Strafvordering;
Wbp: Wet bescherming persoonsgegevens;
WP 29: Article 29 Data Protection Working Party.

Geraadpleegde bronnen (o.a.):

Article 29 Data Protection Working Party (WP 29), *Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones,* 2015 (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf);
Cavoukian, Ann, Privacy Commissioner of Ontario, *Privacy and Drones: Unmanned Aerial Vehicles*, 2012 (http://www.ipc.on.ca/images/Resources/pbd-drones.pdf);
College bescherming persoonsgegevens (Cbp), *Richtsnoeren voor publicatie van persoonsgegevens op internet*, 2007;
College bescherming persoonsgegevens (Cbp), *Richtsnoeren voor beveiliging van persoonsgegeven*, 2013;
Commissie voor de bescherming van de persoonlijke levenssfeer (Privacycommissie), (http://www.privacycommission.be/nl/faq-themas/drones?page=1);
Custers, B.H.M, Oerlemans J.J. & Vergouw, S.J., *Het gebruik van drones. Een verkennend onderzoek naar onbemande luchtvaartuigen*, 2014 (http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2015/03/03/tk-rapport-het-gebruik-van-drones.html);
Finn, R.L., Wright, D., Donovan, A., Jacques, L. & De Hert, P. *Study on privacy, data protection and ethical risks in civil Remotely Piloted Aircraft Systems operations - Final Report*, 2014 (http://ec.europa.eu/DocsRoom/documents/8550/attachments/1/translations).